第二届“未来工业互联网”学术论坛

2024 2nd Future Industrial Internet Symposium

会议论文集

广东·深圳

2024 年 8 月

目 录

Data/Model Jointly Driven Routing and Resource Allocation Algorithms for Large-scale Self-organizing Networks for New Power Systems ····· *Chuanfang Jing*, *et al*（1）

AIoT for the Aircraft Final Assembly Line: A Cloud-Edge-Terminal Collaborative Framework ····· *Cheng Ren*, *et al*（12）

面向工业互联网装备预测性维护的跨域预测方法综述 ····· 贾子翟，等（24）

Energy-aware Remanufacturing Process Planning and Scheduling Problem Using Particle Swarm Optimization Algorithm ····· *Jun Wang*, *et al*（35）

绿色集成炼钢炉次计划研究 ····· 王敬博，等（64）

轻量级区块链辅助的工业互联网端边协同调度 ····· 张培风，等（81）

FCLA-DT: Federated Continual Learning with Authentication for Distributed Digital Twin-based Industrial Internet of Things ····· *Yingjie Xia*, *et al*（96）

基于保序缓存的时间敏感网络 FRER 机制 ····· 胡绍柳，等（109）

基于“微服务+中台”内核的航天离散协同制造工业互联网平台构建及其应用 ····· 钟珂珂，等（123）

面向工业互联网的推–抓协作式机械臂精细化自主抓取方法 ····· 何自明，等（136）

考虑工人移动性的人员排班和生产调度研究 ····· 毛照昉，等（153）

减小系统控制成本的双阈值水印添加策略用于重放攻击检测 ····· 朱琦琳，等（168）

基于多视野感知的多智能体协同策略融合方法 ····· 王彬锐，等（183）

Relay Selection for Multi-Source Cooperation in Wireless Powered Industrial Sensor Networks ····· *Min Li*, *et al*（194）

An empirical analysis of RIS phase quantization effect in an IIoT scenario ····· *PAN Junjian*, *et al*（202）

Industrial process monitoring based on multi-block graph convolutional network ····· *Chen Xufei*, *et al*（210）

知识图谱驱动的船舶管件加工车间制造资源推荐方法……田思思，等（220）

基于数据驱动的转炉能耗建模与工艺参数节能优化……敬培锋，等（232）

3DGLS: A Location Scheme based on 3D Geo-Magnetic Sensors for Multi-Workshop and Multi-Production Line Optimization …… *Yu Tang*, *et al*（245）

Edge Intelligence-based Collaborative Device Authentication and Localization for Industry 5.0 …… *Li Xu*, *et al*（261）

Application of Embedded Soft-PLC in Residential Photovoltaic System …… *Zhiwu Tang*, *et al*（272）

UEMA: An Symmetric-key AKA Scheme for Industrial Internet Multi-Cloud Applications in Untrusted Edge Environments Based on ECDH …… *Guiliang Chen*（279）

面向 Eclipse 工业互联网开源软件的安全漏洞分析……李增扬，等（287）

适应工业互联网的低延迟分组密码研究综述……杨金玲，等（302）

Empowering Industrial Fault Detection via Self-Supervised Learning Techniques …… *Qianwen Meng*, *et al*（315）

Recursive residual convolutional neural network with attention mechanism based on U-Net (Attention R2U-Net) for surface minor defect detection …… *Yongwen Zhang*, *et al*（325）

基于过程挖掘的多维度过程分析方法……汤珺雅，等（338）

面向柔性制造的通信感知控制协同系统优化方法……周　映，等（352）

5G-TSN 融合网络中面向负载均衡的资源分配技术……苏　慧，等（363）

Rolling Bearings Intelligent Fault Diagnosis Method Based on TTS-GAN Model Transfer Learning …… *Shuang Liu*, *et al*（381）

确定性系统功能安全确保技术：挑战与趋势……张志为，等（393）

面向工业互联的星地传输性能评估方法……汪文静，等（407）

绿色集成连铸中包计划研究 ……魏俊杰，等（416）

智能配电网不平衡问题的主动定位与调控恢复……李一泓，等（428）

工业互联网 AI 安全的挑战与发展趋势 ……周晓茂，等（441）

基于蒙特卡洛树搜索的自组织制造车间任务调度优化……王立平，等（450）

面向低功耗嵌入式设备的可信软件栈设计与应用……杨　轩，等（468）

基于多特征融合的工业时序异常检测方法……乔怡群，等（481）

融合注意力机制的 3D 打印缺陷检测算法……张俊杰，等（489）

Data-Driven Raw Material Dynamic Procurement Optimization Method Based on Industrial Internet of Things and Application……*LUO Jiang*, *et al*（507）

基于 ZOA-ShareSpace 的多模态数据共享子空间方法……许云晋，等（519）

面向工业的数据空间构建 ……王　晨，等（528）

A High-Performance Data Collaborative Analysis Chain with Privacy Protection……*Haonan Yan*, *et al*（534）

Image semantic transmission method for downstream tasks of industrial Internet……*LU Yanpeng*, *et al*（542）

Modeling and Collaborative Control for Networked Heterogeneous Re-Entrant Manufacturing Systems ……*Chenguang Liu*, *et al*（550）

基于多源特征融合的飞机翼身交点孔精密镗削刀具磨损状态监测 ……杨展鹏，等（556）

Improvement of Visual Sensing System via Dual Attention YOLOv5 in Calcium Carbide Factory ……*ZHU Haijiang*, *et al*（579）

Resource-Efficient Consensus for Large-Scale Industrial Multi-Agent Systems: An Event-Triggered Approach ……*Ruchao Su*, *et al*（592）

基于随流检测的确定性网络混合时敏流量调度技术研究……王圣恺，等（598）

YOLO_LSK: A Sintered Surface Defect Detection Model Based on Large Selective Kernel Network ……*YANG Yi*, *et al*（613）

A Review of Steelmaking and Continuous Casting Scheduling Based on Intelligent Optimization Methods ……*SONG Xinbo*, *et al*（624）

TD3-based Stochastic Workload Offloading for 5G-based Cloud Control System……*LI Sha*, *et al*（634）

Data/Model Jointly Driven Routing and Resource Allocation Algorithms for Large-scale Self-organizing Networks for New Power Systems

Chuanfang Jing, Xiaorong Zhu, and Xu Liu

***Abstract*—The large-scale self-organizing networks (LSNs) for new power systems are the multi-mode mesh networks combining high speed power line communication and radio-frequency communication (HPLC/RF), which are a promising means to solve the "last mile" problem of ubiquitous access. Due to the complex network topology and communication environment, and rapid service iteration, it is challenging to improve transmission efficiency. In this paper, we proposed the routing and resource allocation algorithms based on graph attention network (GAT) and model for new power systems. First, according to historical data such as delay, reliability, SINR, load ratio, betweenness centrality and level, GAT can calculate different probabilities for nodes with higher level than the central node and select the optimal next hop with the largest probability. This process is executed multiple times on different central nodes to get the best end-to-end path. Secondly, considering the wired and wireless channel interference, packets priority and quality of service (QoS) comprehensively, a dynamic resource allocation model based on the optimal next hop generated by GAT is established, which is aimed to maximize the number of successfully transmitted packets between node pairs. And then a packet priority-based resource allocation algorithm is presented for LSNs for new power systems. Simulation results show that the proposed routing and resource allocation algorithms outperform baselines in terms of throughput, end-to-end delay, hop count and network reliability.**

***Index Terms*—New power systems, Large-scale self-organizing networks, Routing, Resource allocation, Graph attention network and model.**

I. Introduction

NEW power systems take the smart grid as the hub, and the energy-network-load-storage coordination and multi-type energy complementation as the support, aiming to accelerate carbon peaking and carbon neutrality [1]. With the widespread access of distributed energy and new services, the scale of data and terminals collected and controlled will reach millions, and new power systems will gradually extend to the power distribution side and user side. Due to the explosive growth of information and the scattered distribution of equipment, it is necessary to realize real-time and efficient transmission of measurements and control commands among sampling/measurement devices and control centers, so as to facilitate fast and automatic operation.

This work was supported by Natural Science Foundation of China (92367102), Key R&D plan of Jiangsu Province (BE2021013-3) and Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX22_0944).(*Corresponding author: Xiaorong Zhu*)

The authors are all with the Wireless Communication Key Lab of Jiangsu Province, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, China

Large-scale self-organizing networks (LSNs), as the essential tool for IoT to capture data in the "last mile" [2], can fully sense and connect complex and diverse terminals, and support the on-demand access of various devices in new power systems. The primary objective of LSNs for new power systems is to efficiently transfer bi-directional energy and communication signals from the source to the target, enabling timely and accurate decision-making [3]. However, the changes in distributed resources and load modes add complexity to optimizing routing and resource allocation in LSNs. Specifically, the presence of large power load fluctuations and numerous scattered users introduces strong time-varying line impedance and serious long-distance line interference [4]. Moreover, building occlusion and intermittent terminal access contribute to severe channel attenuation and node congestion within LSNs. Therefore, maintaining high transmission efficiency in LSNs for new power systems becomes exceptionally challenging if routing and resource allocation strategies remain fixed amidst changing channel environments and load distributions. Thus, the development of intelligent and real-time approaches to optimize routing and resource allocation in LSNs is urgently needed to ensure their optimal performance for new power systems.

Currently, researchers are actively studying routing and resource allocation in new power systems, with a focus on model-driven approaches based on mathematical optimization techniques. Numerous applications and methods have been proposed in this field [5]-[7]. To meet specific routing requirements in challenging environments, the Internet Engineering Task Force (IETF) introduced the Low Power and Lossy Network (RPL) routing protocol [8][9]. RPL establishes an optimal path between source and sink nodes based on objective functions (OFs) or path metrics. The OFs aim to optimize specific network parameters, such as energy, latency, or throughput [10]. Resource allocation is typically treated as an optimization problem, which is addressed through two categories: centralized methods and distributed methods. Due to the distributed nature of resources that require control and coordination in new power systems, traditional centralized solutions face significant complexity [11][12].

These studies become impractical in the context of new power systems. The reason is that different subsystems within a given application may exhibit varying topologies, and the involved domains describe the environments in different ways. The overall network's performance optimization heavily relies on system operators and manual procedures, making it

challenging to manage and maintain efficiently. Moreover, the emergence of massive terminals presents obstacles in obtaining accurate mathematical models for actual LSNs. Furthermore, the solution process is burdened with cumbersome and over-simplified assumptions, adding complexities to determining optimal strategies for resource allocation and routing. As a promising paradigm of LSNs for new power systems, machine learning seems well suited to develop the accurate and lightweight routing and resource allocation algorithms. However, LSNs are fundamentally represented as a graph. These methods of fully-connected neural networks [13], convolutional neural networks [14], and recurrent neural networks [15] are not designed to learn graph structural information and lack generalization to network topology, resulting in limited accuracy of the final trained model [16]-[18].

One of the potential methods to solve the above challenges is the GAT and model driven approach, which intelligently and quickly achieves optimization of routing and resource allocation of LSNs. Here, GAT-based routing algorithms collect and learn historical information for new power systems with the advantages of globality, high efficiency and versatility. In addition, GAT expresses the relationship between different neighbor nodes and central node without any complicated matrix operations (such as inversion) and prior knowledge of the graph structure [19]. As a novel neural network for learning graph-structured data, GATs are very suitable for developing routing optimization algorithms for LSNs. On the contrary, the most critical advantage of the model-based approach is to obtain accurate results through mathematical optimization techniques. And the distributed method of resource allocation with good robustness and fast computing speed is an ideal choice for LSNs. The historical data obtained based on the model can be used to train GATs to improve the accuracy.

Therefore, this paper proposes the GAT and model joint driven routing and resource allocation algorithms to improve the transmission efficiency for LSNs for new power systems. The main contributions of this article are concluded as follows.

1) We systematically develop a GAT and model joint driven framework of routing and resource allocation (GMRR) for LSNs for new power systems, which can help improve the intelligence and practicability of universal schemes of optimization of routing and resource allocation.

2) In GMRR, GATs are used to adaptively find optimal end-to-end path. First, the parameters of delay, reliability, SINR, load ratio, betweenness centrality and level are normalized and input into GAT. Then, the self-attention mechanism of GAT is used to compute different probabilities for high-level neighbor nodes of the central node. The high-level node with the largest probability is selected as the optimal next hop, which is also the central node of the next GAT. The optimal end-to-end path is obtained through executing GATs multiple times on different central nodes.

3) In GMRR, the model driven method for resource allocation is proposed to effectively utilize the limited channel resources. First, we divide packets into high, medium, and low priorities according to latency tolerance. Considering SINR and capacity of high speed power line carrier (HPLC) and radio-frequency (RF) channels and delay requirements of packets, a resource allocation model is established to maximize the number of successfully transmitted packets between node pairs. In addition, a packets priority-based resource allocation algorithm is proposed to solve the 0-1 integer linear programming problem.

4) Finally, we conduct extensive experiments on LSNs with different packets transmission amounts and network scales to evaluate the feasibility and performance of the proposed algorithms. The results indicate that the proposed resource allocation and routing algorithms are more effective and accurate than the existing researches on LSNs in terms of hop count, delay, reliability and throughput.

The rest of the paper is organized as follows: Section II introduces the system model and GMRR of LSNs for new power systems. In Section III, a routing algorithm for LSNs based on GAT is provided. Section IV presents the problem description, the dynamic resource allocation model, and the algorithm PBRA. Section V gives the simulation results and related discussions. Finally, Section VI concludes the paper.

II. A GAT And Model Joint Driven Framework Of Routing And Resource Allocation For LSNs For New Power Systems

A. System Overview

LSNs for new power systems consist of three types of nodes, namely, a border router node, multiple router nodes and leaf nodes [20]. As shown in Fig. 1, the border router is the center of LSNs. The functions of the three types of nodes are as follows.

Border router node: It is a key element in LSNs, accessing WAN via Ethernet, serial, and microwave to provide multiple services. Its function is to transmit the data collected by router nodes to the control center through WAN, and convey the commands of the control center to router nodes.

Router node: It is composed of routers with constant power supply. Multiple router nodes form a mesh network to provide uplink and downlink data forwarding. They are not only responsible for data collection but also serve as relay nodes for adjacent nodes. A router node with fewer hops to the border router node has a higher level.

Leaf node: It is mainly composed of various low-power devices, such as smart meters, electric vehicle charging piles, gas/water metering and various sensors. Leaf nodes generate all kinds of data and form a star network with router nodes.

As depicted in Fig. 1, LSNs for new power systems utilize a combination of wired and wireless communication methods. Wired communication is facilitated by HPLC, while wireless communication involves 470MHz-RF and low-power wireless technologies like Bluetooth, ZigBee, and WiFi [21]. Different types of nodes in LSNs integrate various communication modes based on their specific requirements to achieve optimal communication effectiveness. For instance, router nodes are equipped with dual-mode (HPLC+470MHz-RF) or single-mode (HPLC or 470MHz-RF only), ensuring comprehensive geographical coverage. On the other hand, leaf nodes are configured with low-power wireless communication technologies. The seamless integration of wired and wireless communication

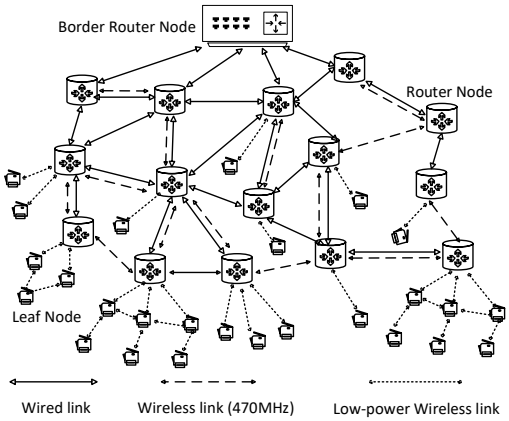


Fig. 1. System model of LSNs.

complements each other, ensuring reliable communication between nodes in LSNs as long as one of the communication methods remains connected. In this paper, we assume that numerous nodes employing different communication methods have been pre-deployed, and the data generated by leaf nodes is transmitted to the border router through the mesh network formed by the router nodes.

B. GMRR framework

Due to the surge in the number of terminals and services, and the time-varying characteristics of resources and communication environments in new power systems, it is necessary to generate accurate and real-time routing and resource allocation optimization strategies. The proposed GMRR framework of LSNs is shown in Fig. 2, which consists of data integration module, GAT-based end-to-end path generation module and model-driven resource allocation module.

In GMRR, the data integration module is used to collect historical data and input historical data into the path generation module and the resource allocation module. In the end-to-end path generation module, GATs are used to generate efficient routing algorithm, which can fully consider the characteristics of network topology and the requirements of multi-dimensional metrics and quickly process the combination of hyperscale parameters. In the resource allocation module, a complete distributed resource allocation model is presented to select the exact number of time-varying channels for data transmission between the central node and the optimal next hop. Moreover, the delay, reliability and SINR obtained by the optimal resource allocation strategy are used as historical data to update the database and input the GAT-based end-to-end path generation module. Finally, the end-to-end path generation module and the resource allocation module jointly obtain the optimal routing and resource allocation strategies for LSNs for new power systems. The implementation process of the two modules will be described in section III and IV respectively.

III. GAT-based Routing Algorithm Of LSNs For New Power Systems

A. Routing representation of GAT

In this section, we construct a graph structure for LSNs and build a mathematical model for routing task based on GAT. First, LSNs are described as the graph structure $G^{'}(\mathcal{V}, \mathcal{E}, \{f^{node}(i)\}, \{f^{e}(i,j)\})$, where $\mathcal{V}$ is the set of router nodes, $\mathcal{E}$ is the set of communication links between router nodes, $\{f^{node}(i)\}$ is the set of router node features, and $\{f^{e}(i,j)\}$ is the set of link features, $i, j \in \mathcal{V}$, $e(i,j) \in \mathcal{E}$. $\{s, d\}$ represents the routing task from source s to destination d. The process of finding the optimal end-to-end path is described as selecting the node sequence from $\mathcal{V}$ and link sequence from $\mathcal{E}$ when $\{f^{node}(i)\}$ and $\{f^{e}(i,j)\}$ are satisfied. The forwarding node sequence of the routing task $\{s, d\}$ is expressed as:

$$\{s, d\} = [v_0, v_1, v_2, \cdots v_L] \tag{1}$$

where $v_0 = s$, $v_L = d$. The th node of the forwarding sequence is:

$$\{s, d\}_l = v_l \tag{2}$$

We assume that P represents the process of finding the optimal route from the source s to the destination d, and $P(v_l, d, G^{'})$ indicates that v_l selects the next hop v_{l+1} from $G^{'}$. The process P is expressed as:

$$P(v_l, d, G^{'}) \rightarrow v_{l+1} \tag{3}$$

Combining (2) and (3), the relationship between the routing task $\{s, d\}$ and the process P is obtained, i.e.

$$P(\{s, d\}_l, d, G^{'}) \rightarrow \{s, d\}_{l+1} \tag{4}$$

Our goal is to find a process P based on GAT to solve the optimal end-to-end path generation problem of LSNs. There are two key factors to get the optimal end-to-end path based on GAT, one is feature representation and processing. GAT takes a set of high-quality features as input. And the other is the establishment of GAT routing architecture for LSNs. GAT utilizes a graph-aware structure customized for routing, and generates the optimal next hop by the self-attention layer. Hence, we illustrate the GAT-based routing scheme of LSNs from the two factors.

B. Feature representation and processing

To find the optimal end-to-end path, routing algorithms require not only topological information such as the adjacency matrix but also additional details about nodes and links. The GAT must comprehend the relationship between these performance metrics and the network status derived from the data plane to optimize crucial performance parameters within the network [22]. By utilizing a comprehensive set of high-quality features that encompass various routing indicators and possess strong expressive power, the need for an extensive training dataset can be mitigated while improving the model's efficiency.

In our analysis of the optimal routing formation and operational state of LSNs, we have identified load ratio, betweenness

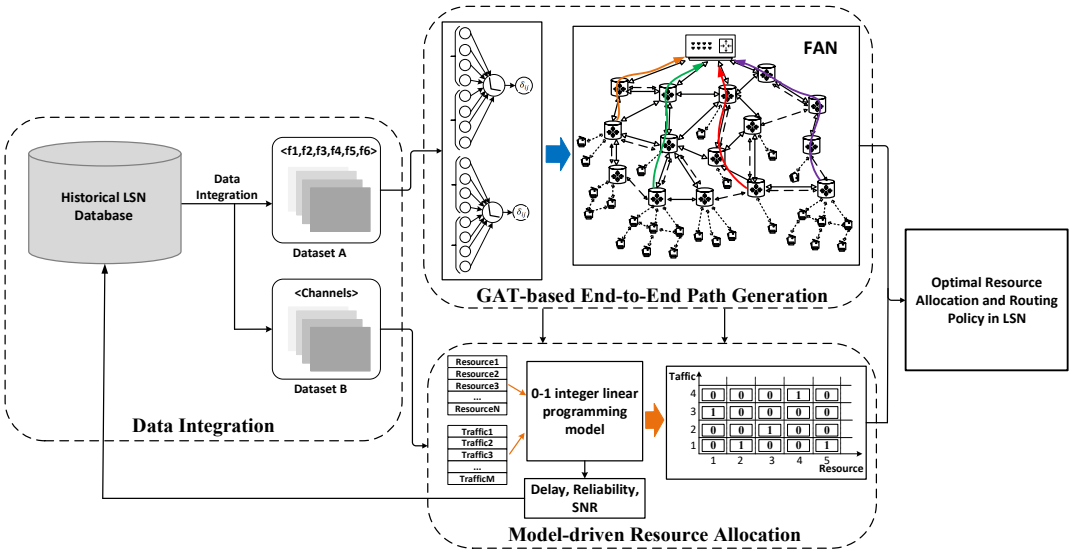


Fig. 2. The GMRR framework.

centrality, and hierarchy as the node features to be incorporated into GATs. Additionally, delay, reliability, and SINR are selected as the link features. As these features have different dimensionalities, directly inputting them into GATs for training is not feasible. For example, reliability, SINR, and betweenness centrality are advantageous features, and higher values indicate better network performance. Conversely, latency, load ratio, and hierarchy are considered cost-type features, and lower values correspond to better network performance. To address this discrepancy, we employ a normalization method [23] to process the data without dimensionality, ensuring compatibility across the various features. Assume that q_{iu} is the uth feature of node i, and $q_{u,\min}$ and $q_{u,\max}$ represent the minimum and maximum values of the uth feature, respectively. The normalization process of benefit-type features is:

$$h_{iu} = \frac{q_{iu} - q_{u,\min}}{q_{u,\max} - q_{u,\min}} \tag{5}$$

The normalization process of cost-type features is:

$$h_{iu} = \frac{q_{u,\max} - q_{iu}}{q_{u,\max} - q_{u,\min}} \tag{6}$$

Combining (5) and (6), the input feature set of GAT is:

$$\mathbf{h} = \{\overrightarrow{h_1}, \overrightarrow{h_2}, \cdots, \overrightarrow{h_i}\}, \overrightarrow{h_i} \in R^F \tag{7}$$

where $\overrightarrow{h_i}$ is the feature of the node i, and F is the number of input features.

C. Establishment of GAT routing architecture for LSNs

GAT is a new class of neural networks operating on graph-structured data, which utilizes hidden self-attention layers to address the shortcomings of graph convolution-based or other similar previous methods [22]. The implementation of GAT is relatively simple, which only needs neighborhood information and uses neighbor features to update the information of central node.

The GAT routing architecture for LSNs is shown in Fig. 3. We decompose the routing process P, i.e. (4), into the process of finding the optimal next hop. And then the best end-to-end path is obtained hop by hop from source to destination. Therefore, the key is to construct an optimal next-hop selector according to different network conditions based on GAT. In this way, we treat the probabilities generated by each self-attention layer for the optimal next hop as an intermediate result, and mainly focus on the formation of the best end-to-end paths. As shown in Fig. 3, the orange nodes represent the central node of GAT, and the gray and yellow nodes represent the neighborhood nodes lower and higher than the hierarchy of the central node respectively in the self-attention layers. We only calculate different probabilities to neighborhood nodes with higher levels to avoid loops and reduce complexity.

Hereafter, we introduce the specific implementation process of generating the optimal end-to-end path based on GATs for LSNs. First, according to (7), we normalize the six high-quality features of delay, reliability, SINR, load ratio, betweenness centrality, and level, and input them into the hidden self-attention layers of GATs. The central node of the first self-attention layer is regarded as the source. A shared weight matrix W for all nodes in LSNs is trained as a mapping between the input features and the output features. The results of the feature maps of each node are spliced and input to a feed-forward neural network to convert the concatenated vectors into a value [24]. Then through the activation function, the absolute attention coefficient between nodes i and j is obtained:

$$\delta_{ij} = LeakyReLU(\overrightarrow{\mathrm{a}}^T[\mathrm{W}\overrightarrow{h_i}||\mathrm{W}\overrightarrow{h_j}]) \tag{8}$$

where $||$ is a splicing operation, W is the node shared weight matrix, $\mathrm{W} \in R^{F \times F'}$, and $\overrightarrow{\mathrm{a}}$ is the weight matrix of the feed-forward neural network, $\overrightarrow{\mathrm{a}} \in R^{2F'}$, F' is the number of output features. δ_{ij} also indicates the importance of node j to node i.

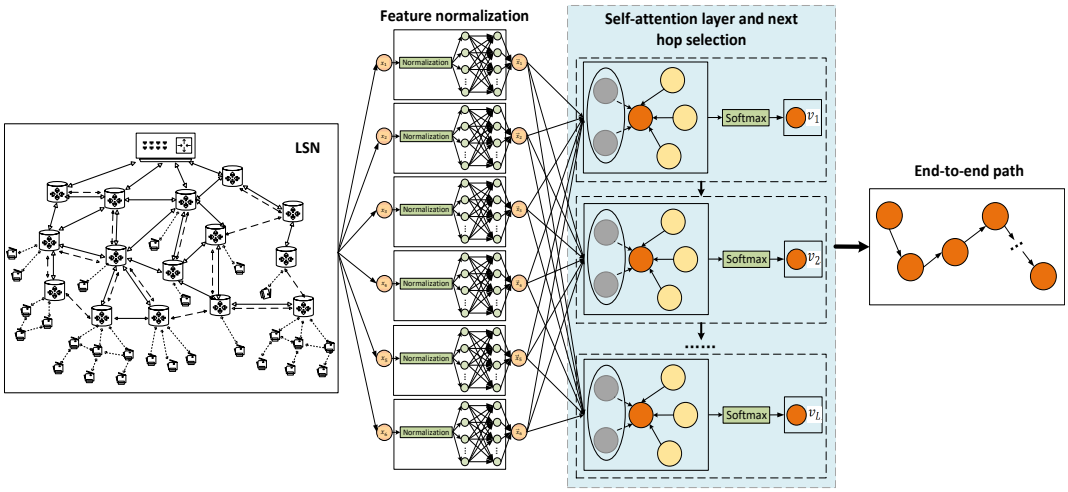


Fig. 3. GAT routing architecture for LSNs.

Second, the high-level neighbor nodes of the central node are filtered by hierarchical features, and the probability that the high-level neighbor nodes belong to the optimal next hop is generated through the self-attention layers. In order to make the coefficients easier to compare between different nodes, we use the softmax function to normalize the absolute attention coefficients of high-level neighborhood nodes to calculate the relative attention coefficient between nodes i and j :

$$\alpha_{ij} = softmax(\delta_{ij}) = \frac{exp(\delta_{ij})}{\sum_{i \neq k, k \in \mathcal{N}_i} exp(\delta_{ik})} \tag{9}$$

where $\mathcal{N}_i$ is the set of high-level neighbors of node i (including i), $j, k \in \mathcal{N}_i$.

The relative attention coefficients are used to compute the linear combination of features as the final output of each node. The calculated relative attention coefficients of the high-level neighbors of the central node, i.e. (9), are weighted and summed. And then we obtain the feature representation of node i

$$\overrightarrow{h_i}' = \sigma(\sum_{j \in \mathcal{N}_i} \alpha_{ij} \mathrm{W} \overrightarrow{h_j}) \tag{10}$$

Through (8), (9) and (10), the output of the central node contains the probability that the high-level neighbor nodes are selected as the optimal next hop. Similarly, each self-attention layer will generate the probability that the high-level neighbor nodes of the central node belong to the optimal next hop and the high-level neighbor node with the largest probability value is selected as the central node of the next self-attention layer. (8) (9) and (10) are terminated until the destination is included in the high-level neighbor nodes. Therefore, the optimal route from source s to destination d is found through $L-1$ hidden self-attention layers.

IV. Resource Allocation Of Lsns For New Power Systems

In order to effectively utilize the limited channel resources, an accurate resource allocation algorithm is proposed, which is performed directly between the central node and optimal next hop generated by GATs in section III. It is worth noting that the SINR, reliability and delay obtained by the resource allocation strategy are collected into the historical database for GAT training.

A. System Overview

The packets transmitted in LSNs mainly include alarms, power outages, real-time charging loads, water and gas meter settlement, station area identification, temperature and humidity, etc. [25], which come from different leaf nodes and are generated at different times. In this paper, we assume that the types of packets transmitted have been predefined and classified into high, medium, and low priorities based on the delay tolerance of packets. The leaf nodes generate the priority label (high, medium, and low) and the router nodes identify the packets type based on the label. When packets need to be transmitted, router nodes confirm their priority and size and check the available resources so that router nodes can adaptively manage and allocate wired and wireless resources (i.e., channels).

The available HPLC and wireless channel resources of the node i (i.e., the optimal next hop) are indexed as $\mathbf{CR}_i = \{cr_{i,1}, cr_{i,2}, ..., cr_{i,U}\}$, where $cr_{i,u}$ is composed of two parameters denoted as $cr_{i,u} = \{wc_{i,u}, pc_{i,u}\}$, $wc_{i,u}$ indicates the capacity of the uth channel of node i, $pc_{i,u} = 0$ indicates that the uth channel is a wired channel, and $pc_{i,u} = 1$ indicates that the uth channel is a wireless channel. The high, medium, and low priority packets at node i are listed in set $\mathbf{SR}_i = \{sr_{i,1}, sr_{i,2}, ..., sr_{i,K}\}$, where $sr_{i,k}$ is composed of two parameters denoted as $sr_{i,k} = \{ws_{i,k}, ps_{i,k}\}$, $ws_{i,k}$ represents the size of the kth packet at node i, and $ps_{i,k}$ represents the priority of the kth packet at node i. Priorities of packets are mapped to a single number (0, 1 or 2). For example, when a packet has high priority, $ps_{i,k} = 0$. The lower the packet priority, the greater the value of $ps_{i,k}$. Without loss of generality, it is assumed that packet with the same priority have the same maximum acceptable waiting time, and $T_1^{\max}$, $T_2^{\max}$, $T_3^{\max}$ are the maximum acceptable waiting time of high, medium and low priority packets respectively.

B. Problem Formulation

According to the difference between HPLC and wireless channel models [25], we assume that $\gamma_{i,j}^{HPLC}$ and $\gamma_{i,j}^{RF}$ are the SINR of the PLC and wireless link between nodes i and j, which could be expressed as

$$\gamma_{i,j}^{HPLC} = \frac{E_b|h_{i,j}^{HPLC}|^2}{\sigma_b^2(1+\eta)} \tag{11}$$

$$\gamma_{i,j}^{RF} = \frac{Pd_{i,j}^{-\alpha}|h_{i,j}^{RF}|^2}{\sum_{k\in\mathcal{V}_j} pd_{k,j}^{-\alpha}|h_{k,j}^{RF}|^2+\sigma_0^2} \tag{12}$$

where E_b is the average energy of the signal, $h_{i,j}^{HPLC}$ and $h_{i,j}^{RF}$ are the PLC and wireless channel fading gain between nodes i and j respectively, $\eta = \sigma_i^2/\sigma_b^2$ is the noise ratio of IMN and BGN, P is the node transmit power, α is the channel fading coefficient, $d_{i,j}$ is the distance between nodes i and j, and σ_0^2 is the Gaussian white noise with zero mean variance.

The SINR of HPLC and wireless links between node pairs should be greater than SINR thresholds, indicating that node pairs can communicate with each other. Thus, the SINR constraints of the HPLC and wireless links are as follows:

$$\gamma_{i,j}^{HPLC} \geq \gamma_0 \tag{13}$$

$$\gamma_{i,j}^{RF} \geq \gamma_1 \tag{14}$$

where γ_0 is the SINR threshold of HPLC links, γ_1 is the SINR threshold of wireless links.

The channel capacity of the link between nodes i and j is

$$w_{e_{ij}} = \begin{cases} B^{HPLC}log_2(1+\gamma_{i,j}^{HPLC}), & pc_{i,u}=0 \\ B^{RF}log_2(1+\gamma_{i,j}^{RF}), & pc_{i,u}=1 \end{cases} \tag{15}$$

where B^{PLC} and B^{RF} are the channel bandwidth of HPLC and wireless links, respectively.

Assume that $\mathbf{X} = \{X_{1,1}^i, X_{1,1}^i, ..., X_{U,K}^i\}$ indicates HPLC and wireless channel allocation, where $X_{u,k}^i = 1$ means that the kth packet is allocated the uth channel, otherwise the uth channel is not allocated to the kth packet. When node i transmits packets, the channel capacity constraints are

$$\sum_{k=1}^{K} X_{u,k}^i ws_{i,k} \leq wc_{i,u}, 1 \leq u \leq U \tag{16}$$

Due to the limited number of available channels of the PLC and wireless links, the number of channels allocated to all packets cannot exceed the sum of the available channels at node i

$$\sum_{u=1}^{U}\sum_{k=1}^{K} X_{u,k}^i \leq \sum_{u=1}^{U} wc_{i,u} \tag{17}$$

At the same time, a packet should only be assigned one communication method, i.e.:

$$\sum_{u=1}^{U} X_{u,k}^i \leq 1, 1 \leq k \leq K \tag{18}$$

Furthermore, the actual queuing time of each packet at node i should be less than or equal to the maximum acceptable waiting time. Assuming that the actual queuing time of the kth packet at node i is t_k^i, t_k^i is expressed as

$$t_k^i = \sum_{u=1}^{U}\sum_{k=1}^{K} X_{u,k}^i \cdot \frac{wc_{i,u}}{ws_{i,k}} \tag{19}$$

Combined with (19), the delay constraints of three priority packets can be obtained

$$t_k^i \leq \begin{cases} T_1^{\max}, ps_{i,k}=0 \\ T_2^{\max}, ps_{i,k}=1 \\ T_3^{\max}, ps_{i,k}=2 \end{cases} \tag{20}$$

Our target is to find out the optimal channels allocation between the central node and the optimal next hop and maximize the amounts of transmitted packets. Therefore, the formula for the above problem is as follows:

$$\mathbf{P_1} : \max_{\mathbf{X}} \sum_{u=1}^{U}\sum_{k=1}^{K} X_{u,k}^i$$

subject to

$$C1 : \gamma_{i,j}^{HPLC} \geq \gamma_0$$

$$C2 : \gamma_{i,j}^{RF} \geq \gamma_1$$

$$C3 : \sum_{k=1}^{K} X_{u,k}^i ws_{i,k} \leq wc_{i,u}, 1 \leq u \leq U$$

$$C4 : \sum_{u=1}^{U}\sum_{k=1}^{K} X_{u,k}^i \leq \sum_{u=1}^{U} wc_{i,u}$$

$$C5 : \sum_{u=1}^{U} X_{u,k}^i \leq 1, 1 \leq k \leq K$$

$$C6 : t_k^i \leq \begin{cases} T_1^{\max}, ps_{i,k}=0 \\ T_2^{\max}, ps_{i,k}=1 \\ T_3^{\max}, ps_{i,k}=2 \end{cases}$$

In $\mathbf{P1}$, the optimization variable $\mathbf{X}$ only takes the value of 0 or 1. The inequality constraints of $C4$, $C5$ can be expressed as the form of $0 \leq \mathbf{X} \leq \mathbf{q}$, where $\mathbf{q}$ is a constant vector. The inequality constraints of $C3$, $C6$ can be expressed as the form of $0 \leq \mathbf{g}(\mathbf{X}) \leq \mathbf{p}$, where $\mathbf{g}(\mathbf{X})$ is a linear function with the variable $\mathbf{X}$ and $\mathbf{p}$ is a constant vector. Obviously, $\mathbf{P1}$ conforms to the general form of 0-1 programming problem [26]. For this kind of optimization problem, if all feasible variable combinations are listed by exhaustive method, the time complexity of the resource allocation algorithm will be very high. It is worth noting that the method of allocating available resources to packets according to the high, medium and low priorities is actually a special case of the feasible variable combination of the optimization problem $\mathbf{P1}$. Therefore, we propose a packet priority-based dynamic resource allocation algorithm (i.e., **Algorithm 1**) to solve the optimization problem $\mathbf{P1}$.

Algorithm 1 Packets Priority-Based Dynamic Resource Allocation Algorithm (PBRA)

Input: **SR**; $ws_{i,k}$; $ps_{i,k}$; **CR**; $wc_{i,u}$; $pc_{i,u}$; $T_1^{\max}$; $T_2^{\max}$; $T_3^{\max}$; γ_0; γ_1

Output: The number of packets successfully transmitted at the central node

for each k, $k \in \{1, 2, ..., K\}$ **do**
  for u, $u \in \{1, 2, ..., U\}$ **do**
    if $ps_{i,k} = 0$ **then**
      if $\sum_{k=1}^{K} ws_{i,k} \leq \sum_{u=1}^{U} wc_{i,u}$ **then**
        if There exits u that satisfies the conditions: $C1$, $C2$, $C4$, $C5$, $C6$ **then**
          $X_{u,k}^{i} = 1$;
        end if
      else if $\sum_{k=1}^{K} ws_{i,k} > \sum_{u=1}^{U} wc_{i,u}$ **then**
        if There exits u that satisfies the conditions: $C1$, $C2$, $C4$, $C5$, $C6$ **then**
          $X_{u,k}^{i} = 1$;
        end if
      end if
    else if $ps_{i,k} = 1$ **then**
      if $\sum_{k=1}^{K} ws_{i,k} \leq \sum_{u=1}^{U} wc_{i,u}$ **then**
        if There exits u that satisfies the conditions: $C1$, $C2$, $C4$, $C5$, $C6$ **then**
          $X_{u,k}^{i} = 1$;
        end if
      else if $\sum_{k=1}^{K} ws_{i,k} > \sum_{u=1}^{U} wc_{i,u}$ **then**
        if There exits u that satisfies the conditions: $C1$, $C2$, $C4$, $C5$, $C6$ **then**
          $X_{u,k}^{i} = 1$;
        end if
      end if
    else
      if $\sum_{u=1}^{U} wc_{i,u} \neq 0$ **then**
        if There exits u that satisfies the conditions: $C1$, $C2$, $C4$, $C5$, $C6$ **then**
          $X_{u,k}^{i} = 1$;
        end if
      end if
    end if
  end for
end for
return $\sum_{u=1}^{U} \sum_{k=1}^{K} X_{u,k}^{i}$;

In **Algorithm 1**, we dynamically perform resource allocation of LSNs for new power systems based on packet priorities. The packets belong to different priorities, there are different processing methods. First, if the available resources of the central node i can meet the transmission performance requirements of packet k, that is, $C1$, $C2$, $C4$, $C5$, $C6$, the central node i will immediately allocate resources to the packet k. Then, if the resources at the central node i are insufficient or there are no available resources, the resources occupied by packets with a lower priority will be allocated to packet k, and the interrupted packets will wait for the central node i to allocate resources again. Considering the maximum waiting time (delay tolerance) of high, medium and low priority packets, these packets exceeding the maximum waiting time will be deleted by the central node i.

TABLE I
SIMULATION PARAMETERS

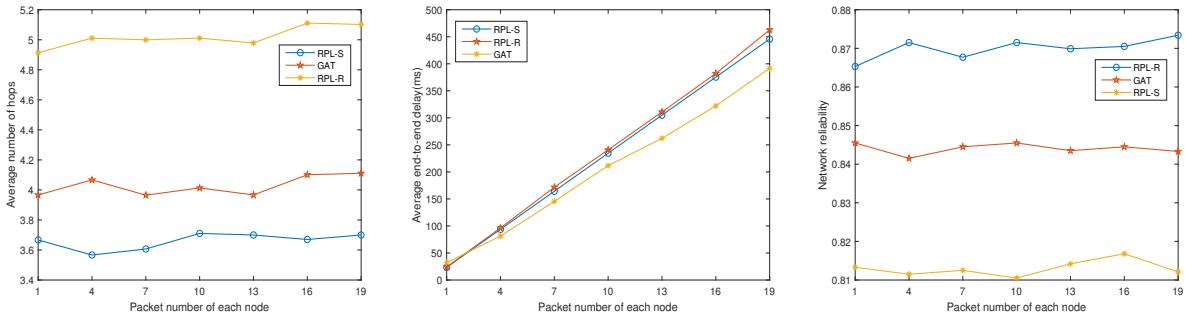
Parameter	Value
Bandwith of PLC link(B^{PLC})	1.1 Mbps
Bandwith of 470MHz-RF link (B^{RF})	250 kbps
Signal average energy of PLC link (E_b)	1.5
Channel fading gain of PLC link ($h_{i,j}^{PLC}$)	-0.8dB
BGN noise power (N_0)	2
Ratio of IMN to BGN (α)	3
Channel fading gain of 470MHz-RF link ($h_{i,j}^{RF}$)	1dB
Channel fading coefficient of 470MHz-RF link (α)	2
Transmission power of 470MHz-RF link (P)	(0.03, 0.06]
Learning rate	0.005
Loss rate	0.5
RELU parameter	0.00025
Number of input features (F)	6
Number of output features ($F^{'}$)	1

V. SIMULATION

A. Experimental Setting

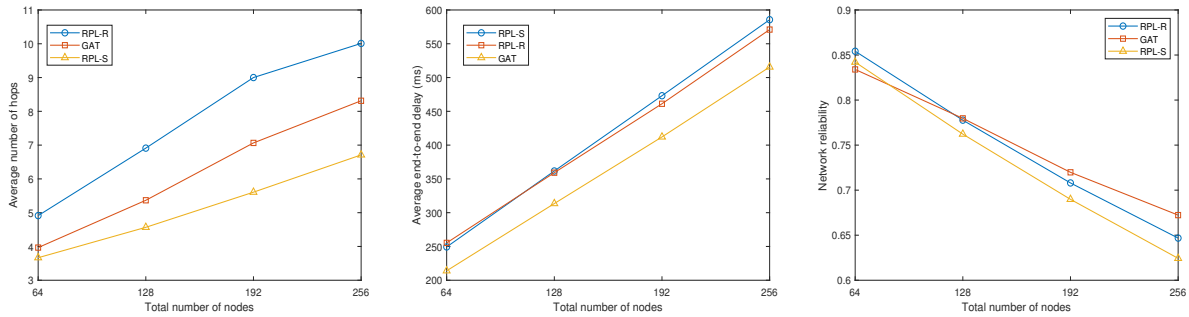
In this section, we describe the experimental environment and evaluate the performance of the algorithms proposed by Matlab and Python. Firstly, we evaluate the performance of the proposed routing algorithm in a small-scale scenario (i.e., 1 border router node and 63 router nodes), where nodes are randomly and evenly distributed within an area of $150*150\mathrm{m}^2$. The links between router nodes are equipped with dual-mode (HPLC+470MHz-RF) or single-mode (only HPLC or 470MHz-RF). The links between router nodes and border router nodes are composed of HPLC links. In our simulations, we set the maximum radio transmission range to 12 m and the interference range to 15 m. We use the log-distance path loss model which is suitable for outdoor propagation such as in urban areas, and set the path loss exponent to 2 [25]. The node transmission power is set to 23.0306dB. The data traffic is sent from the source using the User Datagram Protocol (UDP) and the packet size is 1024 bytes. The simulation parameters are shown in Table 1.

We simulate 64 nodes network topology and collect data on network performance to train GATs based on Matlab. The specific process is to randomly generate the positions of a border router node and 63 router nodes and set the number of packets transmitted by 63 router nodes to 1, 4, 7, 10, 13, 16, and 19, respectively. All packets are generated by leaf nodes, collected by router nodes and transmitted to the border router node. Performance values (i.e., delay, reliability, SINR, load ratio, betweenness centrality, and hierarchy) between 63 source-destination node pairs are collected for training. Then the values are normalized according to (5) and (6). GATs are implemented based on the deep learning framework of Pytorch. The labels are generated based on the features of the



(a)　　(b)　　(c)

Fig. 4. Comparison of the performance of three routing strategies with different packets number transmitted by router nodes.(a) Average number of hops. (b) Average end-to-end delay. (c) Network reliability.



(a)　　(b)　　(c)

Fig. 5. Comparison of the performance of three routing strategies with different number of nodes.(a) Average number of hops. (b) Average end-to-end delay. (c) Network reliability.

nodes for LSNs and GATs are trained in a supervised manner. During the training process, the number of iterations of GATs is set to 2000. We set 2 self-attention layers in GATs to better predict the optimal next hop. The number of attention heads in the first layer is 3, and the activation function is ELU. The number of attention heads in the second layer is 1, and the activation function is RELU. Moreover, we have tried multiple pairs of hyperparameters to achieve better performance, and the values are shown in Table I.

B. Performance Evaluation

Currently, the routing protocol widely used in new power systems is RPL [8]. Therefore, we choose RPL algorithms based on the shortest hops (RPL-S) and the highest reliability (RPL-R) as baselines for performance comparison with the proposed GAT-based routing algorithm. In Fig. 4, we compare the average number of hops, average end-to-end delay, and network reliability of the three routing strategies. All router nodes transmit packets to the border router node at the same time.

In Fig. 4(a), when the number of packets increases from 1 to 19, the average number of hops of three routing algorithms basically keep balance, and the performance of the proposed GAT-based routing algorithm is close to RPL-S. As depicted in Fig. 4(b), as the number of packets increases, the average end-to-end delay of the three routing algorithms all show an upward trend. The average end-to-end delay of the proposed GAT-based routing algorithm is significantly smaller than the other two routing algorithms. The main reason is that when the number of packets increases, congestion gradually occurs in the network, and the queuing delay of packets at nodes gradually increases, resulting in growth in end-to-end delay. RPL-S and RPL-R only select the optimal path based on hops and reliability, while the GAT-based routing algorithm comprehensively considers packets number and network conditions (e.g, load ratio, SINR) to select the optimal end-to-end path. In addition, the greater the packet number, the greater the performance difference between the three algorithms, and the proposed GAT-based routing method can obtain the best performance. As shown in Fig. 4(c), even with the increase in the number of packets, the network reliability of the three routing algorithms remains basically unchanged. The performance of the GAT-based routing algorithm is close to RPL-R.

Then we illustrate the impact of different network scales on the proposed routing algorithm performance. Our simulations are conducted on multiple scenarios, which consist of 64-nodes, 128-nodes, 192-nodes and 256-nodes. All router nodes transmit packets to the border router node at the same time. And the performance values between different

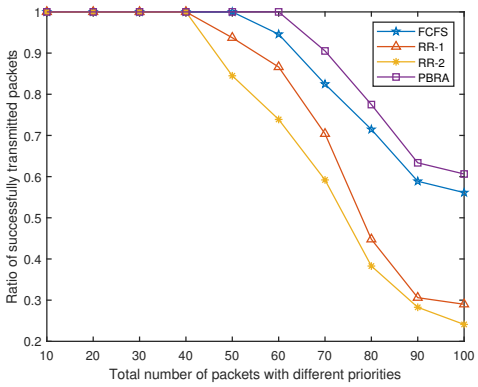


Fig. 6. Ratio of packets successfully transmitted with different number of nodes.

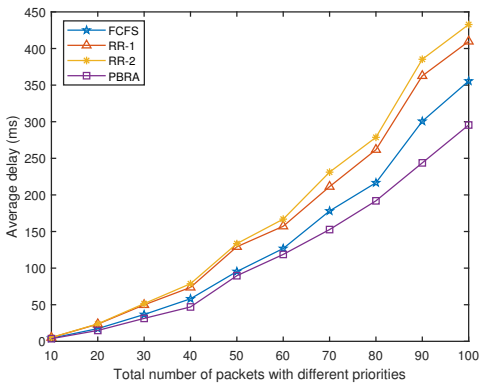


Fig. 7. Network reliability with different number of nodes.

source-destination node pairs under four network topological scales, namely delay, reliability, SINR, load ratio, betweenness centrality, and hierarchy, are collected to train GATs.

In Fig. 5, the curves with different colors and shapes represent the network performance of three routing strategies under different network scales. Fig. 5(a) and Fig. 5(b) display that the average number of hops and the average end-to-end delay of the three routing algorithms tend to go upward. As the total number of nodes increases, the number of hops from source to destination grows, so that the average number of hops and average end-to-end delay of end-to-end paths becomes larger. The average number of hops of our proposed GAT-based routing algorithm is smaller than that of RPL-R and greater than that of RPL-S. However, the average end-to-end delay of our proposed GAT-based routing algorithm is significantly smaller than the other two routing algorithms. And the more the total number of nodes, the greater the performance difference between the three algorithms. Fig. 5(c) exhibits that the network reliability of the three routing algorithms gradually decreases with the increase of the total number of nodes. The network reliability of the GAT-based routing algorithm is close to that of RPL-R. The results show that under different packets number transmitted by router nodes and different network scales, the proposed GAT-based routing algorithm performs well in terms of the average number of hops, average end-to-end delay and network reliability.

Then, we compare the packets priority-based dynamic resource allocation algorithm (PBRA) with two other different methods, which are as follows:

(1) First-in-first-out (FCFS): When a node transmits packets to multiple nodes at the same time, the channel resources at the node are allocated to the first-in packet in chronological order.

(2) Round-Robin (RR): When a node transmits packets to multiple nodes at the same time, each packet occupies a time slice in turn and channel resources are allocated according to the order in which the packets arrive at the queue. If the packet does not complete transmission within a time slice, channel resources are released and the packet is placed at the end of the queue.

In this paper, the proportion of successfully transmitted packets is defined as the ratio of the maximum number of packets successfully transmitted between node pairs to the total number of packets within 50 ms. Two time slices are set in RR, which are 30ms (RR-1) and 10ms (RR-2) respectively. We focus on the amounts of packets successfully transmitted from the central node to the optimal next hop node, where throughput and latency are the most critical performance metrics.

As illustrated in Fig. 6, with the number of different priority packets at nodes increases, the proportion of packets successfully transmitted by PBRA is consistently better than the other three algorithms. FCFS, RR-1 and RR-2 suffer from uneven variation/fluctuation in resource allocation. Since FCFS allocates resources completely according to the order of packets' arrival, it logically shows the irregular use of resources. RR-1 and RR-2 also face unbalanced resource utilization. Ensuring packet transmission fairness consumes a significant amount of time, which, in turn, reduces the number of successfully transmitted packets. In cases where the time slice size is unreasonable, RR scheduling experiences even higher volatility when compared to FCFS. Conversely, PBRA enhances resource utilization in comparison to FCFS and RR, enabling a higher volume of transmitted packets. PBRA considers the priority of packets in the queue at nodes and achieves adaptive and efficient management of resources. This approach optimizes the utilization of resources, resulting in improved packet transmission efficiency.

The average delay of different packets number is shown in Fig. 7. It depicts that the trend of all curves is upward, that is, when the number of different priority packets increases, the average delay of PBRA, FCFS, RR-1 and RR-2 will be extended because the available resources of nodes cannot satisfy more packets transmission requests, and these packets cause congestion at nodes, which will eventually lead to a surge in queuing time. FCFS, RR-1 and RR-2 perform almost similarly and well when the number of packets is low. However, as the number of different priority packets at nodes increases, the average delay will be greatly affected. FCFS allocates resources according to the order in which the packets arrive, regardless of the priority. When the resources

are unavailable, the packets that arrive later must wait. In RR, router nodes allocate available resources to each packet fairly according to the time slice cycle, so the packets waiting time is longer, and the size of the time slice has a significant impact on the average delay. In PBRA, packets are managed according to resource requirements and packet priorities. PBRA attempts to allocate available resources to packets as quickly as possible. Therefore, as the number of packets increases, the average delay of PBRA is significantly smaller than the other three algorithms, which proves the effectiveness of PBRA.

VI. Conclusion

This paper studies the optimization of routing and resource allocation for Large-Scale Networks (LSNs) for new power systems. First, we proposed a GAT and model driven framework, where GATs are executed periodically multiple times on different nodes to generate optimal end-to-end paths. Then, we established a resource allocation optimization model.Theoretical analysis demonstrates that our proposed GAT-based routing algorithm achieves an efficient balance between the average number of hops, average end-to-end delay, and network reliability. Moreover, our packets priority-based resource allocation algorithm, based on the optimal next hop found by GATs, ensures The optimal throughput and average delay. Comparative experiments are conducted to verify the effectiveness of our proposed routing and resource allocation algorithms for LSNs for new power systems. Future work includes evaluating the performance of our proposed alogorithms in extreme environmental scenarios to improve their adaptability and scalability in new power systems.

References

[1] V. Dehalwar, A. Kalam, M. L. Kolhe and A. Zayegh,“Compliance of IEEE 802.22 WRAN for field area network in smart grid,” *2016 IEEE International Conference on Power System Technology* (POWERCON), Wollongong, NSW, Australia, 2016, pp. 1-6, doi: 10.1109/POWERCON.2016.7754046.

[2] T. Qiu, L. Zhang, N. Chen, S. Zhang, W. Liu and D. O. Wu, “Born This Way: A Self-Organizing Evolution Scheme With Motif for Internet of Things Robustness,” in *IEEE/ACM Transactions on Networking*, vol. 30, no. 6, pp. 2644-2657, Dec. 2022, doi: 10.1109/TNET.2022.3178408.

[3] “IEEE Standard for Wireless Smart Utility Network Field Area Network (LSN),” in *IEEE Std 2857-2021* , vol., no., pp.1-182, 25 June 2021, doi: 10.1109/IEEESTD.2021.9464888.

[4] J. Jagannath, S. Furman, T. Melodia and A. Drozd, “Design and Experimental Evaluation of a Cross-Layer Deadline-Based Joint Routing and Spectrum Allocation Algorithm,” in *IEEE Transactions on Mobile Computing*, vol. 18, no. 8, pp. 1774-1788, 1 Aug. 2019, doi: 10.1109/TMC.2018.2866093.

[5] J. Wang, F. Zhang, Z. Xie, Z. Wen and G. Zhang, “Joint Bandwidth Allocation and Path Selection in WANs with Path Cardinality Constraints,” in Journal of Communications and Information Networks, vol. 6, no. 3, pp. 237-250, Sept. 2021, doi: 10.23919/JCIN.2021.9549120.

[6] H. Kordbacheh, H. Dalili Oskouei and N. Mokari, “Robust Cross-Layer Routing and Radio Resource Allocation in Massive Multiple Antenna and OFDMA-Based Wireless Ad-Hoc Networks,” in *IEEE Access*, vol. 7, pp. 36527-36539, 2019, doi: 10.1109/ACCESS.2019.2904673.

[7] C. Pan, R. Liu and G. Yu, “Joint User Association and Resource Allocation for mmWave Communication: A Neural Network Approach,” in *Journal of Communications and Information Networks*, vol. 6, no. 2, pp. 125-133, June 2021, doi: 10.23919/JCIN.2021.9475122.

[8] A. Shabani Baghani and M. Khabbazian, “RPL Point-to-Point Communication Paths: Analysis and Enhancement,” in *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 166-179, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3201177.

[9] M. Park, G. Jeong, H. Son and J. Paek, “Performance of RPL Routing Protocol over Multihop Power Line Communication Network,” 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 1918-1920, doi: 10.1109/ICTC49870.2020.9289175.

[10] P. Janani, V. C. Diniesh and M. J. Auxilius Jude, “Impact of Path Metrics on RPL’s Performance in Low Power and Lossy Networks,” 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2018, pp. 0835-0839, doi: 10.1109/ICCSP.2018.8524141.

[11] B. Liu, C. Liu and M. Peng, “Resource Allocation for Energy-Efficient MEC in NOMA-Enabled Massive IoT Networks,” in IEEE Journal on Selected Areas in Communications, vol. 39, no. 4, pp. 1015-1027, April 2021, doi: 10.1109/JSAC.2020.3018809.

[12] Z. Sharif, L. T. Jung, I. Razzak and M. Alazab, “Adaptive and Priority-Based Resource Allocation for Efficient Resources Utilization in Mobile-Edge Computing,” in IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3079-3093, 15 Feb.15, 2023, doi: 10.1109/JIOT.2021.3111838.

[13] D. Talbi and Z. Gal, “Impact of Multi-Layer Recurrent Neural Networks in the Congestion Analysis of TeraHertz B5G/6G MAC Mechanism,” *2022 International Conference on Software, Telecommunications and Computer Networks* (SoftCOM), Split, Croatia, 2022, pp. 1-6, doi: 10.23919/SoftCOM55329.2022.9911500.

[14] M. Chen, U. Challita, W. Saad, C. Yin and M. Debbah, “Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial,” in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3039-3071, Fourthquarter 2019, doi: 10.1109/COMST.2019.2926625.

[15] B. Jia and Y. Zhang, “Spectrum Analysis for Fully Connected Neural Networks,” in *IEEE Transactions on Neural Networks and Learning Systems*, doi: 10.1109/TNNLS.2022.3164875.

[16] S. Li, Y. Sun, G. G. Yen and M. Zhang, “Automatic Design of Convolutional Neural Network Architectures Under Resource Constraints,” in *IEEE Transactions on Neural Networks and Learning Systems*, doi: 10.1109/TNNLS.2021.3123105.

[17] M. Xu et al., “Recurrent Neural Network Based Link Quality Prediction for Wireless Sensor Networks,” *2021 IEEE 6th International Conference on Computer and Communication Systems* (ICCCS), Chengdu, China, 2021, pp. 905-909, doi: 10.1109/ICCCS52626.2021.9449134.

[18] M. Wang, Y. Cui, X.Wang, S. Xiao, and J. Jiang, “Machine learning for networking: Workflow, advances and opportunities,” *IEEE Netw.*, vol. 32, no. 2, pp. 92–99, Mar. 2018.

[19] Y. Liang, Y. Zhang, D. Gao and Q. Xu, “An End-to-End Multiplex Graph Neural Network for Graph Representation Learning,” in *IEEE Access*, vol. 9, pp. 58861-58869, 2021, doi: 10.1109/ACCESS.2021.3070690.

[20] E. Y. Song, G. J. FitzPatrick, K. B. Lee and E. Griffor, “A Methodology for Modeling Interoperability of Smart Sensors in Smart Grids,” in *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 555-563, Jan. 2022, doi: 10.1109/TSG.2021.3124490.

[21] “IEEE Approved Draft Guide for Smart Distribution Applications Guide,” in *IEEE P1854/D008, July 2018*, vol., no., pp.1-99, 13 June 2019.

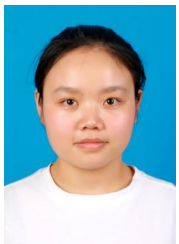
[22] M. Shi, Y. Tang, X. Zhu, Y. Zhuang, M. Lin and J. Liu, “Feature-Attention Graph Convolutional Networks for Noise Resilient Learning,” in *IEEE Transactions on Cybernetics*, vol. 52, no. 8, pp. 7719-7731, Aug. 2022, doi: 10.1109/TCYB.2022.3143798.

[23] Meng J, Tang W, Tang H, et al. A Comprehensive Evaluation System Urban Distribution Network[C]//*2018 IEEE 4th Information Technology and Mechatronics Engineering Conference* (ITOEC). IEEE, 2018: 1139-1143.

[24] Y. Shao, R. Li, B. Hu, Y. Wu, Z. Zhao and H. Zhang, “Graph Attention Network-Based Multi-Agent Reinforcement Learning for Slicing Resource Management in Dense Cellular Network,” in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 10792-10803, Oct. 2021, doi: 10.1109/TVT.2021.3103416.

[25] L. Yang, X. Yan, S. Li, D. B. da Costa and M. -S. Alouini, “Performance Analysis of Dual-Hop Mixed PLC/RF Communication Systems,” in *IEEE Systems Journal*, vol. 16, no. 2, pp. 2867-2878, June 2022, doi: 10.1109/JSYST.2021.3088096.

[26] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.



Chuanfang Jing was born in Jiaxian County, Pingdingshan City, Henan Province, China in 1997. She received the B.E. degree in Tianjin University of Technology in 2019. And she is currently pursuing the D.S. degree in Nanjing University Of Posts And Telecommunications.

From 2015 to 2019, she served as the party secretary of the class. And she holds two patents. Her research interests include 5G/6G networks and Internet of Things.

Xiaorong Zhu received the Ph.D. degree in wireless communications in 2008 from Southeast University, Nanjing, China.

She was a post-doctor in The Chinese University of Hong Kong in 2008 and 2009. She is currently a Professor with College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. Her current research interests include 5G/6G networks, swarm intelligence, as well as Internet of Things.

Xu Liu received the Ph.D. degree in communication and information system in 2010 from Nanjing University of Aeronautics and Astronautics, Nanjing, China.

He is currently an associate professor in College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include mobile communication system and Internet of Things.

AIoT for the Aircraft Final Assembly Line: A Cloud-Edge-Terminal Collaborative Framework

Cheng Ren, *Graduate Student Member, IEEE*, Xiaojing Wen, *Graduate Student Member, IEEE*
Xinping Guan, *Fellow, IEEE*, Yehan Ma, *Member, IEEE*, and Cailian Chen, *Member, IEEE*

***Abstract*—The aircraft final assembly line (AFAL) comprises thousands of processes that must be completed prior to delivery. However, the heavy dependence on manual labor in most assembly processes affects the assembly quality and prolongs the delivery time. The advent of Artificial Intelligence of Things (IoT) technologies has brought advancements to some AFAL scenarios, but systematically improving the intelligence level of the AFAL and promoting AI technology deployment remain significant challenges. To address these challenges, we propose the intelligent and collaborative aircraft assembly (ICAA) framework, which integrates AI technology into a cloud-edge-terminal architecture. The ICAA framework aims to support AI-enabled applications in the AFAL, targeting improved assembly efficiency at both individual process and multiple process levels. We analyze the specific demands in different assembly scenarios and introduce corresponding AI technologies to meet those demands. The three-tier ICAA framework consists of the assembly field, edge data platform, and assembly cloud platform. It facilitates the collection of heterogeneous terminal data and the deployment of AI technologies. The framework enhances assembly efficiency by reducing reliance on manual labor for individual processes and fostering collaboration among multiple processes. We provide detailed descriptions of how AI functions at each level of the framework. Furthermore, we apply the ICAA framework to a real AFAL, explicitly focusing on the functional testing process of the flight control system. This practical implementation demonstrates the effectiveness of the framework in improving assembly efficiency and promoting the adoption of AIoT technologies.**

***Index Terms*—Aircraft Final Assembly Line, AIoT, Cloud-Edge-Terminal, Collaborative Framework**

I. Introduction

Various aircraft equipment and systems are installed and tested in the aircraft's final assembly line (AFAL) before delivery to the customer [1]. As depicted in Fig.1, AFAL spans a wide area, typically exceeding 500 meters in length and 100 meters in width. The multi-manned AFAL comprises a sequential arrangement of workstations [2]. Each workstation is subdivided into several sub-stations, each encompassing multiple installation or testing processes. The details of these processes are outlined in one or several assembly outlines (AOs). Once the designated processes are completed at each workstation, aircraft are simultaneously transferred to the subsequent workstation at the end of the takt time [3]. The takt time represents the maximum duration required for workers at each workstation to carry out all designed processes [4]. To improve assembly efficiency, there is a compelling need to reduce both the takt time and delivery period [5].

However, most aircraft final assembly processes still heavily rely on manual labor, which significantly hinders the improvement of assembly efficiency [6]. On the one hand, many installation and testing procedures require manual intervention, resulting in prolonged assembly times and extended delivery periods. On the other hand, issues such as resource allocation between workstations and process scheduling are also subject to manual decision-making, making it difficult to consider multiple factors across different workstations and processes along the entire production line. This could lead to erroneous decision-making and, in severe cases, interrupt the assembly process. To improve the assembly quality and efficiency, there are mainly three challenges as follows:

1) How can we improve the efficiency of each single installation or testing process?
2) How can we coordinate various resources among different processes within the same workstation?
3) How can we cooperate with the demands of different processes among workstations to reduce the workstation cycle time?

With the rise of Internet of Things (IoT) technologies, various types of terminals are deployed in the AFAL to improve the efficiency of installation and testing processes [7]–[10]. For example, combining contact and non-contact sensors with estimation can significantly enhance the accuracy of aircraft control surface angle monitoring [7]. Humanoid robots, deployed in areas inaccessible to wheeled robotic platforms, enable the execution of assembly operations [8]. During the installation of large equipment, vision-based assembly tools are used to boost precision and efficiency [9]. Additionally, numerous robots and sensors are interconnected to manage heterogeneous processes by sharing limited communication and computing resources [10]. Although integrating these IoT terminals reduces reliance on manual labor in the AFAL, it introduces new challenges, such as data collection and fusion from diverse terminals, coordination and management of limited communication-computing resources, and collaborative scheduling of multiple processes. Traditional algorithms and human-based decision-making are inadequate to address these complexities. Consequently, artificial intelligence (AI) has emerged as a viable solution to these challenges [11].

C. Ren, X. Wen, X. Guan, and C. Chen are with the Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China; Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China; Shanghai Engineering Research Center of Intelligent Control and Management, Shanghai 200240, China(e-mail: rencheng, xiaojingwen, xpguan, cailianchen@sjtu.edu.cn).

Y. Ma is with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: yehanma@sjtu.edu.cn).

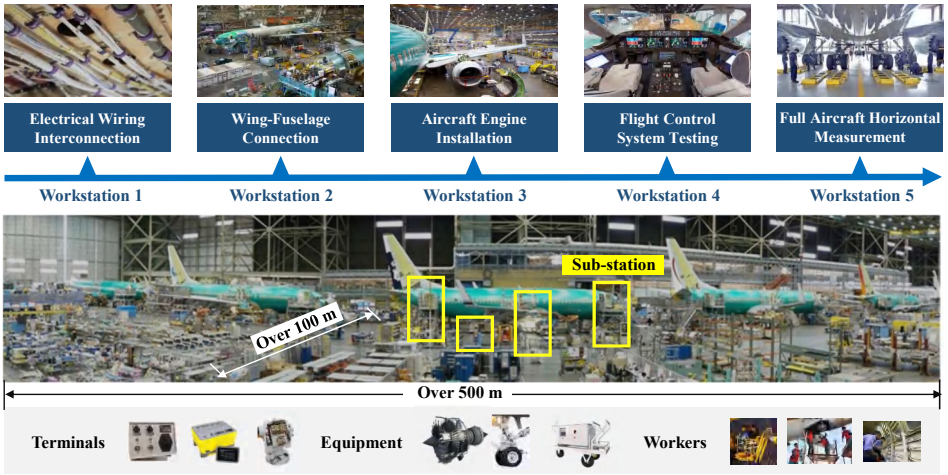


Fig. 1: The overview of the aircraft final assembly line.

The integration of AI technology continues to have a significant impact on the AFAL, with various AI techniques being employed, such as pointnet [12], dual Q-learning [13], transfer learning [14], double-layer Q-learning [15], and XGBoost [16]. These AI technologies are used to address various needs in the AFAL, including human-robot collaboration in wiring installation [14], automatic surface segmentation in aircraft painting [12], and display board information recognition in the testing process [17]. Although IoT terminals and AI technologies have been applied in individual scenarios of the AFAL, the challenge still lies in coordinating multiple AI technologies to improve overall assembly efficiency and quality. Therefore, it is necessary to design a framework to facilitate the implementation of AI technology and achieve collaborative management in the AFAL.

Thee AFAL consists of three structural levels: workshops, workstations, and processes, which collaborate to complete assembly tasks [2]. This unique structure necessitates the adoption of a three-tier architecture to ensure unified management of the AFAL. With the emergence of cloud manufacturing and edge computing technologies, the cloud-edge-terminal collaboration framework is expected to address this issue [18], [19]. While significant research has been conducted in the fields of industrial IoT [20], [21] and connected vehicles [22], the architecture of the AFAL remains relatively underexplored. Moreover, existing research mainly analyzes different functional levels without delving into more detailed discussions. Some studies have focused on specific issues, such as target localization [23] and data processing [24]. However, these single-function designs are insufficient since the AFAL is a complex system with multiple workstations conducting multiple processes simultaneously while competing for limited resources, equipment, and workers. Thus, a comprehensive design is necessary to simultaneously ensure the smooth progress of multiple tasks. Given the labor-intensive nature of aircraft assembly, integrating AI technology into the architecture design to improve assembly efficiency and quality is a viable solution. However, existing frameworks that incorporate AI technologies, such as deep learning [25] and reinforcement learning [23], tend to focus on generic scenarios or single-technology enhancements. These do not apply to aircraft assembly with complex environments, process coupling, and strict quality requirements. Therefore, it is necessary to customize a cloud-edge-terminal framework based on the specific requirements of aircraft assembly to assist the implementation of multiple AI technologies and achieve better performance guarantees, which is still unresolved.

To address the requirements of various scenarios in the AFAL, this paper presents a collaborative framework that integrates AI technologies with a cloud-edge-terminal IoT architecture. The proposed framework aims to improve assembly efficiency and quality by effective data processing and resource management. In addition, the framework is validated through its application in the flight control system functional testing (FCSFT) process. The main contributions of this paper are summarized as follows:

1) To address the characteristics and demands of the AFAL, we propose an intelligent and collaborative aircraft assembly (ICAA) framework. This framework integrates AI technology with a cloud-edge-terminal IoT architecture, enabling the systematical intelligence level of the AFAL and contributing to the overall improvement of assembly quality and efficiency. The ICAA framework consists of an assembly field, edge data middle platform, and assembly cloud platform.
2) We conduct a in-depth analysis of the demands in several aircraft assembly scenarios and discuss related AI technologies that can enhance assembly efficiency. These AI methods include transfer learning, PointNet, and reinforcement learning, among others. We discuss how these AI technologies can play a role in different scenarios, including human-robot collaboration, heterogeneous data collection and fusion, resource management, and object identification and tracking.
3) We demonstrate the practical implementation of the ICAA framework in a real AFAL, with a focus on the FCSFT process. We specifically address the challenges of arranging multiple AOs, and discuss the feasibility and necessity of utilizing reinforcement learning algorithms to optimize the AO arrangement.

The rest of the paper is organized as follows. Section II gives a literature review of advanced technologies in the AFAL and IIoT architecture. Section III analyzes the demands of several scenarios and discusses the application of related AI technologies in depth. Section IV presents the design and detailed description of the proposed ICCA framework. Section V focuses on implementing the ICAA framework, and finally, Section VI concludes this paper.

II. Related Works

A. Advanced Technologies in the AFAL

Many scholars have researched the application of IoT technology in the AFAL, exploring its potential benefits and implications [2], [6], [26]–[29]. Roy and Asada proposed a nonlinear feedback control scheme for a gravity-assisted underactuated manipulator to facilitate the installation of aircraft wing-boxes [26]. Ottogalli *et al.* utilized virtual reality technologies to develop a simulator for the assembly process of cabins and cargo, incorporating human-robot collaboration [6]. Zhu *et al.* adopted knowledge-based engineering and optimization methods to solve the 3D routing automation as an optimization problem satisfying all relevant design rules and constraints [27]. Tereshchuk *et al.* designed an efficient scheduling method to distribute tasks among multiple robots in the assembly of aircraft structures, specifically applying it to solve the aircraft wing hole drilling problem [28]. Mei *et al.* developed a dual-machine drilling and riveting cell, incorporating laser displacement sensors and cameras for precise cell positioning using a multi-sensor serving technique [29]. Fang *et al.* presented a modified genetic algorithm to solve a worker allocation problem with the multistage workstation [2]. Bao *et al.* conducted a study on a robust resource investment problem aimed at minimizing the cost of resource investment considering uncertain budgets and varying processing times [30]. These efforts showcase the immense potential of IoT technology in revolutionizing the aircraft assembly process and enhancing the efficiency and reliability of aircraft.

Besides, many researchers have explored the application of AI technology in the AFAL, encompassing various areas such as productivity forecasting [5], intelligent surface segmentation [12], preventive maintenance [15], human-machine collaboration [14], and more. Long *et al.* employed diverse approaches to investigate the productivity prediction for the AFAL and compare the performance of each approach [5]. Wang *et al.* proposed a parallel PointNet approach to achieve automated surface segmentation for painting various types of aircraft [12]. Yan *et al.* designed an improved double-layer Q-learning algorithm for an integrated optimization problem involving assembly scheduling, worker assignment, and flexible preventive maintenance in a flexible assembly line [15]. Li *et al.* proposed a multi-modal transfer-learning-enabled approach for predicting actions, ensuring proactive human-robot collaborative assembly. To demonstrate its effectiveness, an aircraft bracket assembly task was conducted in a laboratory environment [14]. Han *et al.* designed a vision-based aircraft display and control board statute recognition method to replace the manual reading and recording operation during the aircraft assembly testing stage [17]. Monferran *et al.* proposed a machine learning model capable of predicting the currents in the fastening assemblies of an aircraft fuel tank within a matter of seconds [16]. While the works above have successfully applied IoT or AI technologies to specific scenarios in aircraft assembly, achieving overall intelligence in the AFAL requires more than just advanced technologies in individual scenarios. It necessitates an intelligent framework design for the AFAL at the system level.

B. IIoT Architecture

In recent years, the cloud-edge-terminal collaborative framework has gained significant attention as a research hotspot due to its capability to address the challenges of high latency in centralized cloud computing [31] and limited computing capabilities in edge computing [32]. This framework is well-suited for meeting the multi-level cooperation demands of the workshop-workstation process in the AFAL. It can be a practical approach for systematically managing production lines in AFAL and beyond. This kind of three-tier framework has been applied to various application scenarios, including IIoT [20], connected vehicles [22], smart grids [33], healthcare IoT [34], and AFAL [10]. For instance, Qiu *et al.* [20] proposed a reference architecture that comprehensively considers the characteristics of IIoT, focusing on the functions of each layer and communication between layers. Wang *et al.* [22] conducted a comprehensive literature survey on existing architectural design alternatives for connected vehicles. Chen *et al.* [33] designed an edge computing hardware and software architecture for power systems to foster the digitalization of intelligent grids through cloud-edge collaboration. These architectures are typically proposed based on technical, business, and service requirements for a specific scenario to determine the number and functionality of layers. Ren *et al.* [10], [35] proposed a digital twin-enabled heterogeneous process coordination framework to manage various devices and resources in a workstation of the AFAL. However, the framework design of the AFAL is still in its early stages and needs further exploration.

Some existing collaborative framework researches mainly focus on practical issues, such as data fusion [25], anomaly detection [36], and target localization [23], [37]. Wu *et al.* [25] presented a three-layer cloud-edge-terminal architecture that optimizes terminals and multi-edge nodes to achieve low latency, energy consumption, and load balancing. Ren *et al.* [36] studied a cloud-edge collaborative adaptive fault diagnosis method in which the global fault diagnosis model in the cloud is further refined and used for scenario-specific and real-time prediction in each edge. There are some papers addressing pervasive problems such as computing offloading [38], resource allocation [32], [39], and data processing [24]. Thai *et al.* [38] introduced a terminal-edge-cloud architecture that aims to provide vertical and horizontal offloading among service nodes while minimizing system computing and communication costs. Yuan *et al.* [39] maximized the profit of system providers by ingeniously scheduling incoming tasks between cloud computing and edge computing layers while

strictly ensuring their response time limits. However, these solutions mainly focus on the decision-making behavior of a single target and may not be suitable for more complex cases like the AFAL, where processes are coupled and affect each other. Therefore, we need to comprehensively analyze the requirements of each workstation and even each AO in the AFAL to design a comprehensive framework.

Meanwhile, the rise of AI technologies in recent years has prompted researchers to explore integrating it into frameworks for further optimization and performance improvements. Some and federated learning [40], [41] in the framework. For instance, Yang *et al.* [34] proposed a framework that maximizes the intelligence level of healthcare IoT through optimized data processing and node deployment efficiency. Similarly, Bhuiyan *et al.* [23] presented a mobile target tracking framework that utilizes collaborative deep reinforcement learning Edge-IoT for high-quality tracking and resource-efficient network performance. In addition, Wang *et al.* [37] combined a collaborative cloud-edge-terminal structure with machine learning-oriented localization to form a federated scheme that outperformed traditional methods in terms of performance. However, these works mainly introduce a few applications and do not delve into the characteristics of application scenarios, which can significantly affect the design of AI algorithms. Hence, it is necessary to design a customized cloud-edge-terminal framework specifically tailored to the needs of the AFAL. Combining this framework with AI technologies can significantly enhance the overall assembly quality and efficiency.

III. Demand Analysis and AI Technologies

In this section, we introduce several typical scenarios within the AFAL and analyze their specific demands. On the one hand, we focus on selected installation and testing processes to illustrate the current assembly status and the specific requirements of individual processes. On the other hand, we address common challenges and analyze the needs arising from multiple processes within one or more workstations. Furthermore, we conduct an in-depth analysis of potential AI technologies that can offer solutions to meet the requirements of the aforementioned processes and scenarios.

A. Electrical Wiring Interconnected System Installation

The electrical wiring interconnection system (EWIS) is a complex network comprising electrical wiring, connectors, cables, and associated components that facilitate the interconnection of various electrical systems and equipment within an aircraft, as shown in Fig. 2. The EWIS is responsible for transmitting electrical power, signals, and data between different systems and components, such as avionics, lighting, communication systems, control systems, among others. In the context of commercial airliners, the EWIS plays a vital role, as evidenced by the substantial scale of its deployment. A typical commercial airliner consists of approximately 530 kilometers of cables, 100,000 wires, and 40,300 connectors. Moreover, more than 90 design areas are involved in the installation of the EWIS throughout the entire aircraft [27].

[1]This image was captured from a video, and the link is https://www.youtube.com/watch?v=B014XuPljjY.

Fig. 2: Diagram of aircraft electrical wiring distribution[1].

In the AFAL, the installation of wiring harnesses constitutes a significant portion of the overall assembly process. This process entails precise adherence to spacing requirements, bending radius guidelines, and slack management, while also considering limited spatial constraints in certain areas. However, currently, the installation of wiring harnesses in the AFAL still relies primarily on manual labor. This manual installation process is highly complex and time-consuming, requiring workers to meticulously adhere to installation precision and follow the predefined routing plans.

Unfortunately, the efficiency of manual installation methods for the entire aircraft wiring harness is relatively low, and it becomes challenging to ensure consistent and quantifiable levels of quality throughout the process. To address these limitations, alternative approaches that leverage advanced technologies or equipment, such as AI and robot, are being explored to improve efficiency and enhance the quality assurance of wiring harness installation in the AFAL. By incorporating AI technologies into the wiring installation process, several improvements can be achieved:

1) Automated Routing and Optimization: AI technologies can analyze the aircraft's design specifications, routing plans, and structural constraints to automatically generate optimized wiring routes. This not only reduces the time required for manual routing but also ensures the efficient utilization of limited space.

2) Human-Robot Collaboration Assembly: In order to meet the flexible and complex process characteristics of aircraft wiring installation, AI-powered robotics and automation systems can be employed to assist in the physical installation of wiring harnesses. Robots can work alongside human operators, performing repetitive or physically demanding tasks, thereby increasing installation speed and reducing fatigue.

Furthermore, the emergence of humanoid robots in aircraft manufacturing has paved the way for human-robot collaboration assembly (HRCA) [8]. HRCA incorporates the advantages of bionic design, environmental perception, and AI learning, creating a new process flow for wiring installation. With the addition of collaborative robots, work efficiency and assembly quality can be improved. In the future, HRCA will develop toward a proactive manner, and transfer learning is a potential method to support this transition [14].

B. Flight Control System Functional Testing

The flight control system is one the most critical systems inside an aircraft, like many other embedded systems, its size and complexity has grown in recent years [42]. Each aircraft

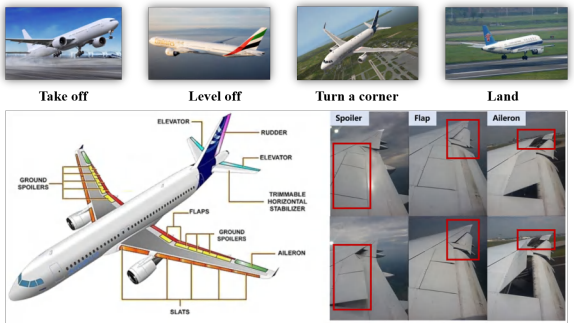


Fig. 3: Flight Attitudes and Flight Control Surfaces

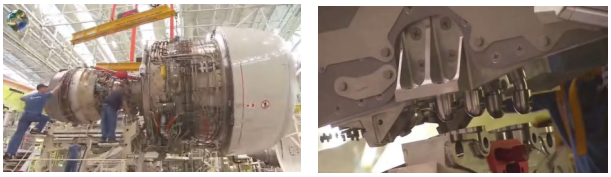
has more than 20 flight control surfaces, including flaps and slats, ground spoilers, ailerons, horizontal stabilizers, rudder, elevator, etc as shown in Fig.3. These flight control surfaces are installed and tested in the AFAL. During flight, different flight control surfaces move to the specified position according to the control command from flight control system, so as to adjust the aircraft attitude, as shown in Fig.3. The FCSFT process is is crucial for verifying whether each flight control surface can correctly executes the control instructions and reaches the required position.

1) Heterogeneous Data Fusion: After data collection, effectively transmitting and fusing heterogeneous raw measurement data to obtain accurate testing data is another challenge. AI techniques can be used to fuse data from multiple sensors and sources, thereby enhancing the accuracy and reliability of the FCSFT. Deep multimodal learning, for instance, is a potential method to address this challenge [43]. By integrating information from different sensors, such as accelerometers, gyroscopes, and position sensors, this method can obtain a more comprehensive understanding of the flight control surface behavior, resulting in more accurate testing data.

2) Virtual Testing and Simulation: AI technologies empower the creation of virtual environments and simulations for testing flight control systems. By leveraging physics-based models, machine learning algorithms, and real-time data integration, virtual testing can simulate various scenarios and evaluate the performance of flight control surfaces under different conditions. This approach aids in diminishing the dependency on physical testing, resulting in time and resource savings.

C. Aircraft Engine Installation

On aircraft, there are some large equipment that needs to be installed, such as the main landing gear and engines [44]. During the installation process, precision and accuracy are crucial to ensure a proper fit and alignment. When the engine is transported to the designated installation area, it needs to be rotated to a position where it can be lifted or suspended, as depicted in the Fig. 4 (a). Throughout the lifting process, the engine's attitude is continuously adjusted to align the locating pin on the engine with the locating hole on the fuselage, as shown in Fig. 4 (b). The alignment accuracy requirement is as high as 0.1 millimeters. Achieving such high-precision installation through manual labor-intensive processes



(a) The lifted engine　　(b) The locating pin and hole

Fig. 4: Diagram of Aircraft Engine Installation[1].

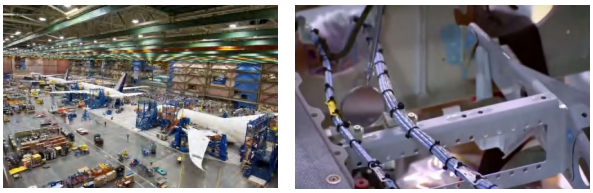
poses significant challenges. Therefore, the introduction of intelligent terminals and the utilization of AI technologies can greatly enhance the efficiency and accuracy of the installation process.

1) Accurate Positioning and Alignment: To ensure the proper fit and function of the engine, it is crucial to position and align it precisely with the aircraft's mounting structure. Computer vision algorithms can analyze real-time images or videos captured during the installation process to detect and track the position and orientation of the equipment. Specifically, AI algorithms can accurately identify the location of installation points and the equipment itself, providing visual feedback to guide operators in achieving precise positioning and alignment. This integration of computer vision and AI technologies greatly enhances the efficiency and accuracy of the installation process.

2) Real-time Monitoring and Feedback: AI technologies facilitate the fusion of data from diverse sensors like cameras, lidar, and proximity sensors, enabling real-time monitoring of equipment movement and alignment during installation. By integrating and analyzing data from multiple sources, AI algorithms enhance the perception capabilities of the system and improve the accuracy of equipment installation. In addition, augmented reality (AR) technology can provide real-time visual overlays of digital information onto the physical environment, aiding technicians in equipment installation. AR can offer step-by-step guidance, highlighting the correct positions, angles, and alignments for each installation step. This interactive visual feedback improves accuracy and minimizes the risk of errors during the installation process.

D. Assembly Objects Identification and Tracking

The aircraft assembly process requires real-time monitoring and management of various production elements, such as the position information, motion state, and attitude information of aircraft components, assembly equipment, and workers. This is vital for improving production efficiency and ensuring production safety. However, the aircraft assembly line encompasses a vast area, posing challenges for vision-based target tracking and positioning. The large field of view and narrow field of vision make it difficult to discern small and indistinct elements. Moreover, the complex environment of the assembly site, as depicted in Fig. 5(a)), diminishes the visibility of originally existing features due to factors like camera distance and resolution. Notably, aircraft components have smooth surfaces with minimal texture information. If the surface color of the target to be detected is monotonous and lacks rich texture details, it can result in a significant



(a) The complex site environment (b) The similar target and background

Fig. 5: Characteristics of Assembly Objects Identification[2].

resemblance between the target and the background, as shown in Fig. 5 (b). Additionally, occlusions caused by machinery and other equipment can further weaken the distinctiveness of the target features. Furthermore, variations in lighting conditions can affect the extraction of target features, leading to incomplete feature representation and potential tracking loss during the positioning and tracking process.

1) Identification: The assembly line involves handling various aircraft components, tools, and equipment. Accurate identification and classification of these objects are crucial to ensure the correct assembly sequence and prevent errors. Computer vision techniques, including object detection and recognition algorithms, can be applied to analyze visual data from cameras or sensors. Deep learning models, such as convolutional neural networks (CNNs), can be trained to identify different objects with high accuracy, even in complex or cluttered environments.

2) Tracking: To ensure objects' real-time monitoring, tracking their positions and movements is crucial as they move along the assembly line. Object tracking enables the observation of object trajectories, detection of any deviations, and coordination with other assembly operations. Multiple object tracking algorithms, such as Kalman filters or particle filters, can be utilized to estimate the positions and velocities of objects based on sensor data. These algorithms can handle occlusions, track objects across frames, and provide reliable object tracking information.

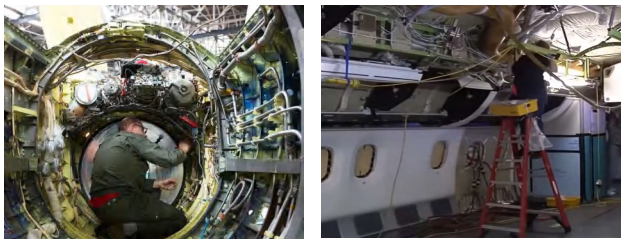
E. Worker Allocation

In the aircraft final assembly line, optimizing the allocation of workers is crucial for improving production efficiency and assembly quality. The objective is to achieve a smooth workflow, balanced workloads, and efficient utilization of resources, as depicted in Fig. 6. However, traditional optimization methods may struggle to effectively address worker allocation problems due to the complexity and interdependencies among different processes. AI technologies may provide some new solution to this issue. AI technologies can optimize worker allocation strategies by analyzing various factors in the assembly process, such as interdependencies between processes, workers' skills and experience, and workload considerations. Here are some examples of AI technologies that can be applied to worker allocation in the AFAL:

1) Skill Matching: Efficient worker allocation requires matching workers with the appropriate skills to specific tasks

[2]The picture is from https://www.sohu.com/a/298739232_628944.

[3]The picture is from http://www.bbkgps.com/blog/?p=270.



(a) The electrical system testing (b) The electrical wiring installation

Fig. 6: Workers in different workstation with different tasks[3].

based on their expertise and qualifications. AI technologies can play a crucial role in analyzing worker profiles, including their skills, experience, and certifications, to match them with suitable tasks or workstations. Machine learning (ML) algorithms can be used to analyze and match worker skills with the requirements of each task. By training ML models on historical data, the system can learn patterns and correlations between worker skills and task performance. The ML models can take into account various factors, such as workers' past performance, feedback from supervisors, and real-time data from the assembly line. This enables accurate matching of workers to tasks based on their competencies, increasing efficiency and reducing errors.

2) Optimization of worker allocation: AI algorithms can optimize worker schedules to minimize conflicts, reduce waiting time, and improve task sequencing. By considering factors such as worker availability, shift patterns, and task dependencies, AI can generate optimized schedules that maximize productivity. For example, reinforcement learning (RL) techniques can be applied to learn optimal policies for assigning workers to tasks. RL-based allocation method can observe the current state of the assembly line, including worker availability, task complexity, and resource constraints, and make decisions on task assignments to maximize productivity.

F. Multi-Process Cooperation

In the AFAL, the coordination of multiple processes is a critical issue. Different processes need to collaborate within the same workstation or across different workstations to ensure smooth assembly processes. AI technologies offer solutions to address the multi-process coordination challenges in the AFAL, improving assembly efficiency and optimizing the coordination between processes.

1) Multi-AO Arrangement: AI technologies can be used to schedule and optimize the sequence and timing of processes based on factors such as process dependencies, time requirements, and resource constraints. By considering the dependencies between processes and resource utilization, AI can help develop optimal process scheduling plans that minimize waiting time and maximizing process execution efficiency.

2) Resource Management: In the AFAL, the effective allocation of resources, including tools, equipment, and personnel, is essential to ensure smooth operations and maximize productivity. AI technologies can be employed for resource coordination management, including material delivery, equipment scheduling, and worker allocation. AI can intelligently

TABLE I: Demand Analysis and Related AI Technologies for Typical Scenarios

Assembly Scenario / Problem	Requirements	Related AI Technology	Reference	Relevance to level
EWIS Installation	Human-Robot Collaboration	Transfer Learning	[14], [45]	E-T
FCS Functional Testing	Image Data Processing	6D Pose Estimation	[46], [47]	C-E-T
Engine Installation	Accurate Position	Multimodal Learning	[48]	E-T
Objects Management	Identification and Tracking	DNN, pointnet	[12], [49]	C-E-T
Worker Allocation	Skill Matching	Reinforcement Learning	[2], [50]	C-E
Multi-Process Cooperation	Workstation Cycle Minimization	Fedrated Learning	[30]	C-E-T

allocate the required materials and equipment based on real-time data and demand predictions, ensuring timely availability of resources for each process. Additionally, AI can optimize the allocation of human resources based on the complexity and urgency of each process, ensuring sufficient workforce participation and completion.

3) Data Sharing: Various processes may generate and require access to data such as design specifications, quality standards, and work instructions. Seamless data sharing and communication are necessary to enable real-time information exchange and collaboration among different processes. AI technologies can facilitate data sharing and communication between workstations, ensuring the flow of information and collaboration between processes. AI can integrate data from different workstations and provide real-time status updates and sharing, promoting collaborative operations and information flow between processes.

G. Heterogeneous Protocol Conversion

In order to achieve efficient application of AI algorithms, in addition to algorithm design, data collection and transmission are the foundation for supporting all algorithm applications. In the AFAL, there are numerous types of installation and testing terminals. For example, during the FCSFT process, multiple heterogeneous testing terminals are deployed, including atmospheric data simulation devices, contact-type wireless angle sensors, non-contact visual sensors, and so on. The data formats of these devices usually vary, including numerical data, image data, and video data. Managing data flow and ensuring the quality of data transmission for various types of data is a challenge.

These terminals utilize various protocols. For wired protocols, Ethernet, PROFINET, RS485, and fieldbus protocols are widely applied to meet the requirements for deterministic low latency, low jitter, and tight synchronization. In addition, industrial wireless protocols such as Bluetooth and WiFi are widely used for extensive data acquisition due to their low maintenance costs and flexible deployment. However, these wired and wireless protocols cannot directly communicate with each other, which makes it challenging to establish unified data collection and transmission.

IV. ICAA Framework Design

In the previous section, we selected multiple scenarios and analyzed the demands in aircraft assembly, as summarized in Table I. In Table I, the second column summarizes the demands that exist not only in the six typical scenarios mentioned in Section III but also throughout the AFAL. We identify relevant AI technologies as potential solutions for each demand listed in Table I—applications in the AFAL. However, our analysis thus far has focused on the relationship between demands and AI technologies, and we need further clarification on how to deploy AI technologies in such a complex system as the AFAL.

Therefore, in this section, we propose the ICAA framework, which combines cloud-edge-terminal architecture, to facilitate the implementation of AI technologies in the AFAL, as shown in Fig. 7. The proposed framework comprises three layers: the Assembly Filed, the Edge Data Middle Platform, and the Assembly Cloud Platform. Unlike the previous framework discussed in other papers, our proposed framework considers the specific requirements of aircraft assembly and the corresponding AI technologies. We will discuss three aspects: the functionality modules included in each level, how AI technologies are leveraged at each level, and how coordination and collaboration are achieved among the different levels.

A. Assembly Field

In the Assembly Field, multiple workstations are set up, each with various assembly terminals such as sensors, robots, and other actuators located geographically dispersed within the workstation. Each workstation comprises around 3-6 substations, each with several installation or testing processes. To enhance assembly quality and efficiency, monitoring these processes through state perception is necessary. The data generated and collected by these massive terminals have a set of critical features, including multimodes and heterogeneity. In essence, these data must be transmitted to a computing terminal for data processing and fusion, eventually leading to autonomous decision-making for installation or testing processes. To improve the efficiency of each single installation or testing process, it is necessary to adopt AI technologies for several general demands in the AFAL.

Each workstation is equipped with one edge server to support the implementation of AI algorithms and meet other

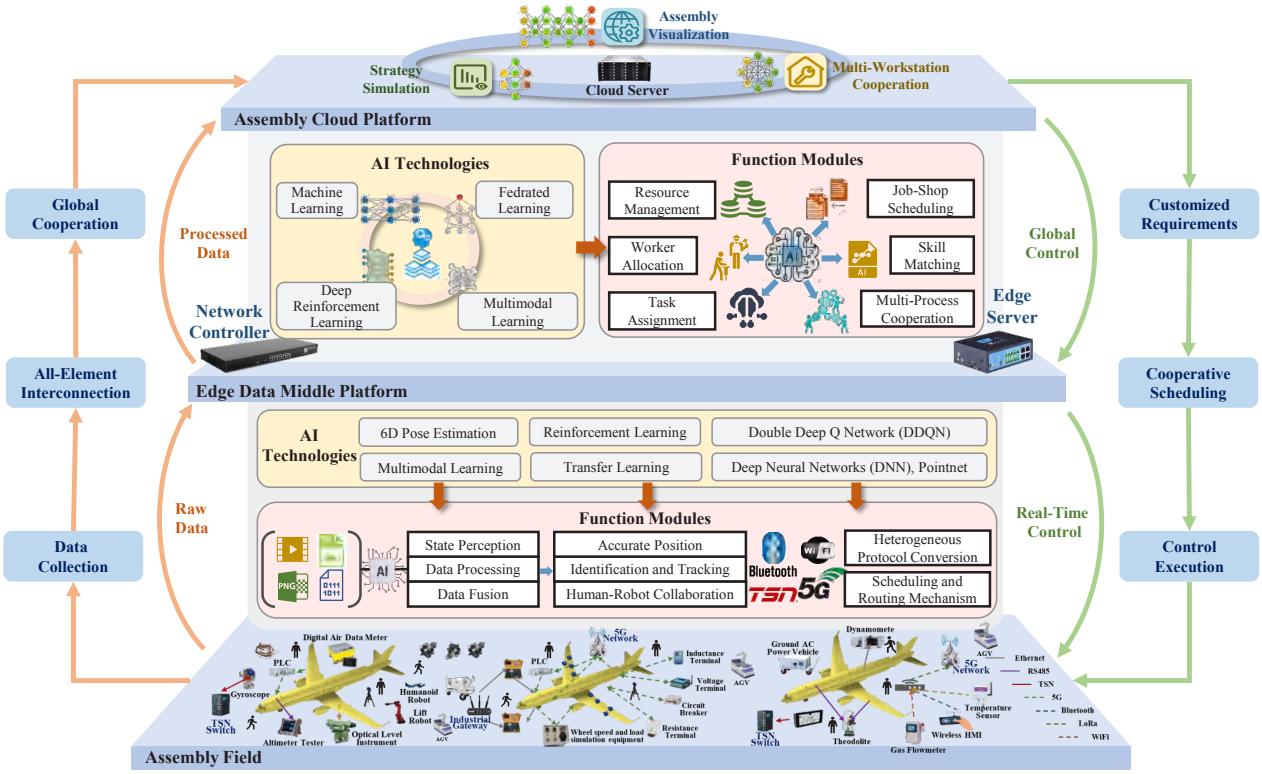


Fig. 7: Intelligent and collaborative Aircraft Assembly (ICAA) Framework.

processing demands. We utilize AI technologies such as 6D pose estimation and multimodal learning to improve the accuracy of image data processing and heterogeneous data fusion. Additionally, due to the heterogeneity of the processes within the sub-station, as discussed in Table I, partial scenarios during the assembly process require high perception precision and low latency sensitivity, such as accurate position, identification, and tracking, and human-robot collaboration. To address these challenges, we design different AI modules according to the characteristics of each process to meet the demands. For instance, we employ DNN and pointnet for high-quality identification and reliable tracking of assembly objects in the face of weak target detection and environmental complexity. For the human-robot collaborative installation, we utilize force control and trajectory planning to enhance work efficiency and assembly quality and minimize the risk of errors or injuries. Meanwhile, deep multimodal learning can effectively integrate heterogeneous raw measurement data and extract accurate information for special scenarios involving multiple types of data (e.g., numerical value, image, and video).

In addition, as all types of terminals are interconnected through heterogeneous communication networks to achieve dynamic information interaction, ensuring the reliable transmission of data is a critical issue that needs to be addressed. To achieve this, we deploy various types of conversion devices, such as TSN switches, 5G networks, and industrial gateways, and utilize double deep Q-network (DDQN) to improve network load balancing. Additionally, we design appropriate scheduling and routing mechanisms to achieve determinism and real-time communication [51]. These methods combine classification and graph-based clustering to enhance schedulability based on the flow data sets characterized according to the actual demands in Table I.

B. Edge Data Middle Platform

In the AFAL, workstations are crucial assembly units where multiple installation or testing processes are carried out simultaneously within each workstation [10]. And the assembly of all workstations also progresses in parallel. It is evident that workstation-level management plays a critical role in the entire AFAL. If all the data and information from the each process are transmitted to a centralized server, it would significantly impact data processing efficiency and make it challenging to support the implementation of numerous AI algorithms. Leveraging edge computing technology, deploying an edge server in each workstation becomes an effective solution. Therefore, in the ICAA architecture, we design the Edge Data Middle Platform to handle real-time requirements and lower computing capacity demands in various workstations of the assembly site.

Unlike the Assembly Field, which performs a single-target task, the edge platform has more storage and computing resources to handle the collected data. The heterogeneous data collected from the site are first pre-processed, fused, and cached on this platform. When sufficient data is obtained, the edge servers execute the steps of data processing deployed in the embedded system or lightweight container, using traditional extensive data analysis or emerging edge intelligence

technologies such as multimodal learning, federated learning, and deep reinforcement learning (DRL). The data analysis logs are also saved for future reference. The edge data middle platform ensures efficient resource utilization, smooth workflow, and balanced workloads.

As multiple processes take place simultaneously in a workstation and all must be completed within a fixed takt time, it is essential to coordinate various resources and workers' different processes to ensure seamless task implementation. To achieve this, network slicing and AI-powered scheduling methods like DRL can be employed for resource management to adjust to changing environments and real-time data dynamically. DRL can also help solve job-shop scheduling problems, particularly related to AO arrangements during FCS testing. Furthermore, to achieve multi-process cooperation within the workstation, we can utilize federated learning to minimize the workstation cycle time.

In addition, many tasks often shift within the workstation, resulting in frequent movement of workers in the multimanned assembly line. At the edge, allocating workers among the sub-stations while satisfying precedence relations and limited worker resources is another problem to solve. As the number of assembly elements considered increases, professional domain knowledge in assembly lines becomes increasingly essential for worker allocation. Machine learning can accurately match workers to tasks based on their competencies, increasing efficiency and reducing errors. It can predict future demand, optimize worker scheduling, and minimize delays or disruptions. Furthermore, we use reinforcement learning to improve the effectiveness of task assignments based on feedback and performance evaluation, ensuring smooth workflow, balanced workloads, and efficient resource utilization.

C. Assembly Cloud Platform

In the AFAL, each aircraft moves to the next workstation simultaneously, known as the cycle time of each workstation. To reduce the cycle time of each workstation and improve assembly efficiency, the workstations must cooperate with their respective demands and achieve line balancing. To address this, drawing inspiration from the industrial cloud platform in the cloud-edge-end architecture, we design the assembly cloud platform in the ICAA framework as shown in Fig.7. The assembly cloud platform plays a critical role in unlocking the potential value of massive data to support AI technologies, realizing the optimal management of whole workshop resources.

The platform acquires data from the Edge Data Middle Platform through the industrial network to achieve this. It supports upper-layer applications like multi-workstation cooperation, strategy simulation, and assembly visualization. Due to the multitude of resources and complex coupling relationships between multiple workstations, traditional optimization methods or heuristic algorithms often struggle to solve optimization and scheduling problems with such complexity effectively. Therefore, we have designed corresponding functional modules in the assembly cloud platform and utilized relevant AI technologies to solve these problems. For example, we explore deep reinforcement and federated learning for global resource management and data sharing to achieve multi-workstation cooperation.

The platform is also responsible for overall long-term data planning for global strategy simulation, decision optimization, and visualization of assembly processes. To achieve this, deep integration of AI and digital twin (DT) technology is necessary [52]. On the one hand, multidimensional and heterogeneous manufacturing process data can be processed through big data and AI to support intelligent decision-making and precise execution of digital twin. On the other hand, the analytical decision results of AI models can be thoroughly simulated and verified through the twin model, providing zero-cost trial-and-error methods for AI decision-making results and improving their reliability. By leveraging virtual simulation and visualization, the resource management of the framework can be improved, trial and error costs can be reduced, and efficiency can be enhanced.

In addition, due to the limited storage and computing capacity of edge computing devices or servers, the platform can provide data storage space and computing power for various workstations. For instance, edge servers at different workstations can offload their entire or partial training tasks to the assembly cloud platform for training. Once the training is completed on the cloud platform and the assembly plans or strategies are obtained, they can be distributed to different workstations for execution. Moreover, the Assembly Cloud Platform can offer a platform for sharing data and resources between different workstations and processes, increasing efficiency and flexibility across the AFAL.

In conclusion, our proposed three-layer architecture perfectly matches the characteristics and requirements of the process, workstation, and workshop structures in the AFAL. It enables the practical application of AI technologies in different scenarios. It achieves the organic integration of various AI technologies through collaboration between the cloud layer, the edge layer, and the terminal layer. This promotes the improvement of assembly quality and efficiency throughout the AFAL.

V. ICAA Framework Implementation

A. DT-enabled Framework Implementation

We deploy the three-tier framework in the AFAL through DT technology, covering applications at the workshop, workstation, and process levels as shown in Fig.8. From top to bottom, we have the Assembly Cloud Platform, the Edge Data Middle Platform for a specific workstation, and IoT terminals in the Assembly Field.

It can be seen from Fig.8 that several workstations are displayed at the assembly cloud platform, realizing the visualization of the AFAL. The operation information of different processes and resources can be displayed at the workstation in the UI panel for monitoring. Each process's relevant process operation information is displayed on the left part of the panel. The resource usage information is shown on the right part of the panel. Besides, the IoT Terminals such as wireless sensors, vision-based robots, workers, and other devices are all displayed in the system.

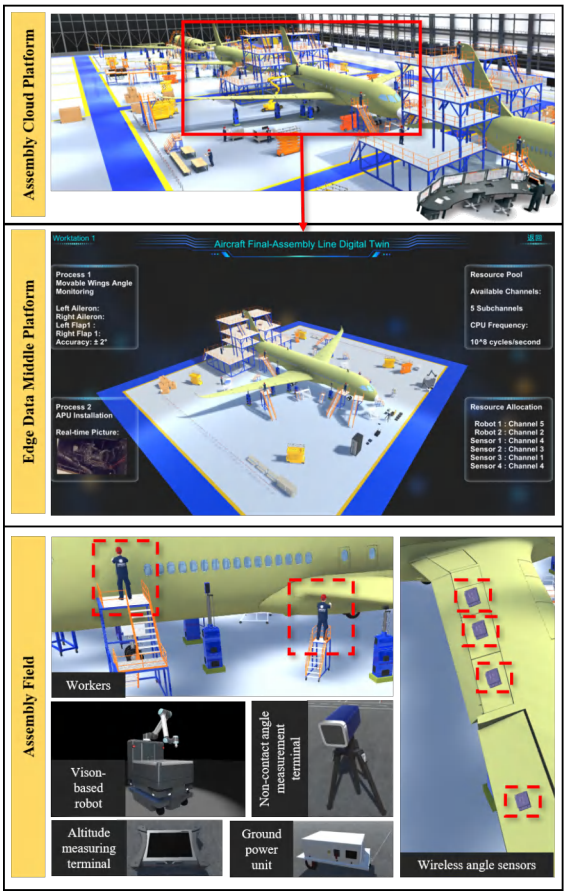


Fig. 8: ICAA Framework Implementation

B. ICAA Framework for FCSFT Process

In Section III, we discussed the significance of the FCSFT process, which verifies the correct execution of control instructions and the attainment of required positions by each flight control surface. This process involves multiple testing terminals, such as atmospheric data simulation devices, inertial navigation testing platforms, altitude measuring terminals, and wireless angle sensors. However, these devices operate on different communication protocols, including Ethernet, RS485, TSN, and 5G, making it challenging to manage them uniformly and exchange data directly.

We apply the proposed ICAA framework to the FCSFT process to address this issue, as illustrated in Fig. 9. In the assembly field, we employ protocol conversion technology to enable data interaction among diverse testing terminals. Additionally, we integrate AI technologies to achieve accurate perception and data processing of the testing state. For example, to precisely monitor the angle of aircraft movable surfaces, we utilize both wireless angle sensors and non-contact-based angle measurement terminals, as depicted in Fig. 8. Network slicing techniques are applied to meet the distinct requirements of these heterogeneous devices. Furthermore, we leverage DNN technology to enhance precise identification and tracking of the wing's installed calibration points and utilize 6D pose estimation and multimodal learning to analyze wing

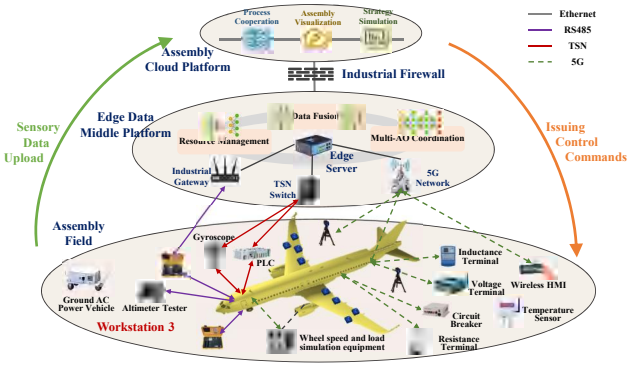


Fig. 9: ICAA Framework for the FCSFT Process

attitude and obtain accurate angle information.

At the edge data middle platform, we implement multimodal data fusion and online cooperative optimization of communication and computing resources to facilitate testing data fusion and multi-AO coordination. Since the FCSFT process requires worker cooperation, we use RL-based allocation strategies to observe the current state of the process and make informed decisions about task assignments. This approach aims to maximize testing accuracy and collaboration by efficiently assigning tasks to workers based on real-time observations and learned policies.

At the assembly cloud platform, we perform offline scheduling and simulation of multiple testing tasks to optimize the allocation of resources and ensure efficient utilization. Using big data processing techniques, we enable seamless data interaction between the assembly cloud platform and other workstations, facilitating real-time information exchange and collaborative decision-making. To enhance the performance of the FCSFT process, we leverage deep reinforcement learning techniques. We can make timely adjustments and optimize the testing processes by continuously monitoring and analyzing actual production conditions. This approach ensures that the FCSFT process is completed within the specified takt time, and efficiency.

Based on the analysis above, it can be concluded that our proposed three-layer framework integrates different AI technologies into the testing process, facilitating effective resource management, timely adjustments, and proactive decision-making. This integration ensures the successful completion of the FCSFT process while enabling continuous improvement and optimization.

C. RL-based AO Arrangement for FCSFT Process

Multiple wireless sensors are applied in the test process to measure the rotation angle of each surface. The FCSFT process comprises multiple monitoring tasks corresponding to various flight attitudes, each corresponding to an AO. The arrangement of these AOs directly affects the testing time. As mentioned in [30], the processing times of testing processes are usually uncertain owing to the fact that possible test failure brings about additional rounds of tests. Therefore, a proper AO arrangement is crucial for the efficient and accurate completion of the testing process. Moreover, different flight attitudes

require the activation of different control surfaces, and the frequency of sensor activation corresponding to each control surface varies. Some sensors may be used more frequently, resulting in higher energy consumption. However, sensors are always battery-supported, and the reduction of battery power will affect the available transmission power and, thus, affect the monitoring quality. Therefore, arranging the order of AOs cooperatively considering the testing accuracy and energy budget is therefore very challenging.

For the whole testing process, there are M monitoring tasks denoted by $\mathcal{M} = \{\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_M\}$, where $\mathcal{M}_1$ denotes the monitoring task 1 and $\mathcal{M}_M$ indicates the monitoring task M. For such an AO arrangement demand, the current decisions will influence following monitoring performances. It can be found there are total $M!$ arrangement strategies of monitoring tasks. Furthermore, due to the complex interdependencies among various terminals required for different monitoring tasks, traditional scheduling algorithms struggle to provide theoretically optimal arrangement strategies.

Deep reinforcement learning is a powerful tool for solving job-shop schedulingproblems [53] and is particularly suitable for the AO arrangement problem in the testing process. Therefore, We employed reinforcement learning techniques to address this problem. We defined the reward function as the negative value of the monitoring accuracy for each arrangement strategy. We trained the DQN network offline and generated real-time arrangement strategies based on different aircraft models. Moreover, we deploy the RL-based arrangement in the constructed system as shown in Fig.10. We consider ten function tests, including in the FCSFT process, and the flight control surfaces involved in each test are intuitively displayed on the panel. When we click the button of any test task, the involved control surfaces will move to indicate which control surfaces need to be called for that monitoring task. We also apply different colors to indicate various surfaces. Typically, we select four of these tests to demonstrate the visualization of flight control surfaces as shown in Fig.10. When we click the button corresponding to this algorithm, the system will run the RL-based task arrangement algorithm and provide the obtained sequencing order on the panel to guide subsequent test tasks.

VI. Conclusion and Future Directions

In this paper, we analyzed the various demands for improving the assembly efficiency of the AFAL and integrated AI technology with cloud-edge-terminal architecture to propose the ICAA framework. We identified the application scenarios of AI technologies at three levels: single process, workstation, and workshop. Then we designed corresponding AI modules in the ICAA framework to provide the required services. Furthermore, We applied the ICAA framework to a real AFAL and specifically described the DT-enabled framework implementation, ICAA framework for FCSFT process and RL-based AO arrangement. In the future, we will further explore the implementation of AI technologies in the AFAL and deploy our ICAA framework in multiple assembly scenarios.

Fig. 10: Multi-AO Coordination for FCSFT Process

References

[1] B. Xin, Y. Li, J. Yu, and J. Zhang, “An adaptive bpso algorithm for multi-skilled workers assignment problem in aircraft assembly lines,” *Assembly Automation*, 2015.

[2] P. Fang, J. Yang, Q. Liao, R. Y. Zhong, and Y. Jiang, “Flexible worker allocation in aircraft final assembly line using multiobjective evolutionary algorithms,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7468–7478, 2021.

[3] M. Şahin and T. Kellegöz, “Balancing multi-manned assembly lines with walking workers: problem definition, mathematical formulation, and an electromagnetic field optimisation algorithm,” *International Journal of Production Research*, vol. 57, no. 20, pp. 6487–6505, 2019.

[4] O. Battaïa, X. Delorme, A. Dolgui, J. Hagemann, A. Horlemann, S. Kovalev, and S. Malyutin, “Workforce minimization for a mixed-model assembly line in the automotive industry,” *International Journal of Production Economics*, vol. 170, pp. 489–500, 2015.

[5] T. Long, Y. Li, and J. Chen, “Productivity prediction in aircraft final assembly lines: Comparisons and insights in different productivity ranges,” *Journal of Manufacturing Systems*, vol. 62, pp. 377–389, 2022.

[6] K. Ottogalli, D. Rosquete, J. Rojo, A. Amundarain, J. María Rodríguez, and D. Borro, “Virtual reality simulation of human-robot coexistence for an aircraft final assembly line: process evaluation and ergonomics assessment,” *International Journal of Computer Integrated Manufacturing*, vol. 34, no. 9, pp. 975–995, 2021.

[7] X. Wen, C. Chen, C. Ren, L. Lyu, and X. Guan, “Resource allocation for coupled slices in edge-assisted industrial iot systems,” in *2023 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2023, pp. 1–6.

[8] A. Kheddar, S. Caron, P. Gergondet, A. Comport, A. Tanguy, C. Ott, B. Henze, G. Mesesan, J. Englsberger, M. A. Roa *et al.*, “Humanoid robots in aircraft manufacturing: The airbus use cases,” *IEEE Robotics & Automation Magazine*, vol. 26, no. 4, pp. 30–45, 2019.

[9] J. Tang, W. Zhu, and Y. Bi, “A computer vision-based navigation and localization method for station-moving aircraft transport platform with dual cameras,” *Sensors*, vol. 20, no. 1, p. 279, 2020.

[10] C. Ren, C. Chen, X. Wen, Y. Ma, S. Zhu, and X. Guan, “Joint design of communication and computing for digital twin enabled aircraft final assembly,” *IEEE Internet of Things Journal*, 2023.

[11] I. K. Nti, A. F. Adekoya, B. A. Weyori, and O. Nyarko-Boateng, “Applications of artificial intelligence in engineering and manufacturing: a systematic review,” *Journal of Intelligent Manufacturing*, vol. 33, no. 6, pp. 1581–1601, 2022.

[12] G. Wang, X. Hua, J. Xu, L. Song, and K. Chen, “A deep learning based automatic surface segmentation algorithm for painting large-size aircraft with 6-dof robot,” *Assembly Automation*, vol. 40, no. 2, pp. 199–210, 2020.

[13] H. Wang, B. R. Sarker, J. Li, and J. Li, "Adaptive scheduling for assembly job shop with uncertain assembly times based on dual q-learning," *International Journal of Production Research*, vol. 59, no. 19, pp. 5867–5883, 2021.

[14] S. Li, P. Zheng, J. Fan, and L. Wang, "Toward proactive human–robot collaborative assembly: A multimodal transfer-learning-enabled action prediction approach," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 8, pp. 8579–8588, 2021.

[15] Q. Yan and H. Wang, "Double-layer q-learning-based joint decision-making of dual resource-constrained aircraft assembly scheduling and flexible preventive maintenance," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 6, pp. 4938–4952, 2022.

[16] P. Monferran, C. Guille-Escuret, C. Guiffaut, and A. Reineix, "Prediction of lightning currents on fastening assemblies of an aircraft fuel tank with machine learning methods," *IEEE Transactions on Electromagnetic Compatibility*, 2023.

[17] H. Bing, L. Gongping, H. Ju, D. Kunpeng, W. Yanzhe, and W. Yanding, "Automatic recognition of display and control board status for aircraft assembly testing based on machine vision," *Measurement and Control Technology*, vol. 41, no. 10, pp. 38–45, 2022.

[18] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 4, pp. 2322–2358, 2017.

[19] X. Wen, C. Chen, M. Li, L. Lyu, and X. Guan, "Age-of-task aware sampling rate optimization in edge-assisted industrial network systems," in *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021, pp. 1–6.

[20] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial internet of things: Architecture, advances and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2462–2488, 2020.

[21] X. Wen, C. Chen, C. Ren, Y. Ma, M. Li, L. Lyu, and X. Guan, "Age-of-task aware co-design of sampling, scheduling and control for industrial iot systems," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 4227–4242, 2024.

[22] H. Wang, T. Liu, B. Kim, C.-W. Lin, S. Shiraishi, J. Xie, and Z. Han, "Architectural design alternatives based on cloud/edge/fog computing for connected vehicles," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2349–2377, 2020.

[23] J. Zhang, M. Z. A. Bhuiyan, X. Yang, A. K. Singh, D. F. Hsu, and E. Luo, "Trustworthy target tracking with collaborative deep reinforcement learning in edgeai-aided iot," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1301–1309, 2021.

[24] Y. Wu, "Cloud-edge orchestration for the internet of things: Architecture and ai-powered data processing," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 792–12 805, 2020.

[25] H. Wu, Z. Zhang, C. Guan, K. Wolter, and M. Xu, "Collaborate edge and cloud computing with distributed deep learning for smart city internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8099–8110, 2020.

[26] B. Roy and H. H. Asada, "Nonlinear feedback control of a gravity-assisted underactuated manipulator with application to aircraft assembly," *IEEE Transactions on Robotics*, vol. 25, no. 5, pp. 1125–1133, 2009.

[27] Z. Zhu, G. La Rocca, and M. Van Tooren, "A methodology to enable automatic 3d routing of aircraft electrical wiring interconnection system," *CEAS Aeronautical Journal*, vol. 8, pp. 287–302, 2017.

[28] V. Tereshchuk, J. Stewart, N. Bykov, S. Pedigo, S. Devasia, and A. G. Banerjee, "An efficient scheduling algorithm for multi-robot task allocation in assembling aircraft structures," *IEEE Robotics and Automation Letters*, vol. 4, no. 4, pp. 3844–3851, 2019.

[29] B. Mei and W. Zhu, "Accurate positioning of a drilling and riveting cell for aircraft assembly," *Robotics and Computer-Integrated Manufacturing*, vol. 69, p. 102112, 2021.

[30] Z. Bao, L. Chen, and K. Qiu, "A robust optimization approach for the resource investment problem of an aircraft final assembly line," *IEEE Transactions on Automation Science and Engineering*, 2022.

[31] H. Liu, F. Eldarrat, H. Alqahtani, A. Reznik, X. De Foy, and Y. Zhang, "Mobile edge cloud system: Architectures, challenges, and approaches," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2495–2508, 2017.

[32] S. Sardellitti, G. Scutari, and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 1, no. 2, pp. 89–103, 2015.

[33] S. Chen, H. Wen, J. Wu, W. Lei, W. Hou, W. Liu, A. Xu, and Y. Jiang, "Internet of things based smart grids supported by intelligent edge computing," *IEEE access*, vol. 7, pp. 74 089–74 102, 2019.

[34] Z. Yang, B. Liang, and W. Ji, "An intelligent end–edge–cloud architecture for visual iot-assisted healthcare systems," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 16 779–16 786, 2021.

[35] C. Ren, C. Chen, P. Li, X. Wen, Y. Ma, and X. Guan, "Digital twin enabled task scheduling for state monitoring in aircraft testing process," *IEEE Internet of Things Journal*, 2024.

[36] L. Ren, Z. Jia, T. Wang, Y. Ma, and L. Wang, "Lm-cnn: A cloud-edge collaborative method for adaptive fault diagnosis with label sampling space enlarging," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 9057–9067, 2022.

[37] Z. Wang, S. Wang, Z. Zhao, and M. Sun, "Trustworthy localization with em-based federated control scheme for iiots," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1069–1079, 2022.

[38] M.-T. Thai, Y.-D. Lin, Y.-C. Lai, and H.-T. Chien, "Workload and capacity optimization for cloud-edge computing systems with vertical and horizontal offloading," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 227–238, 2019.

[39] H. Yuan and M. Zhou, "Profit-maximized collaborative computation offloading and resource allocation in distributed cloud and edge computing systems," *IEEE Transactions on Automation Science and Engineering*, vol. 18, no. 3, pp. 1277–1287, 2020.

[40] G. Bao and P. Guo, "Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges," *Journal of Cloud Computing*, vol. 11, no. 1, p. 94, 2022.

[41] S. Xu, Y. Li, S. Guo, C. Lei, D. Liu, and X. Qiu, "Cloud–edge collaborative sfc mapping for industrial iot using deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4158–4168, 2021.

[42] T. Bochot, P. Virelizier, H. Waeselynck, and V. Wiels, "Model checking flight control systems: The airbus experience," in *2009 31st International Conference on Software Engineering-Companion Volume*. IEEE, 2009, pp. 18–27.

[43] D. Ramachandram and G. W. Taylor, "Deep multimodal learning: A survey on recent advances and trends," *IEEE signal processing magazine*, vol. 34, no. 6, pp. 96–108, 2017.

[44] A. Magrini, E. Benini, H.-D. Yao, J. Postma, and C. Sheaf, "A review of installation effects of ultra-high bypass ratio engines," *Progress in Aerospace Sciences*, vol. 119, p. 100680, 2020.

[45] J. F. Arinez, Q. Chang, R. X. Gao, C. Xu, and J. Zhang, "Artificial intelligence in advanced manufacturing: Current status and future outlook," *Journal of Manufacturing Science and Engineering*, vol. 142, no. 11, 2020.

[46] D. Fu, S. Han, B. Liang, and W. Li, "The 6d pose estimation of the aircraft using geometric property," *IEEE Transactions on Circuits and Systems for Video Technology*, 2022.

[47] D. Fu, S. Han, W. Li, and H. Lin, "The pose estimation of the aircraft on the airport surface based on the contour features," *IEEE Transactions on Aerospace and Electronic Systems*, 2022.

[48] Z. Kong, J. Mao, J. Wang, and X. Lu, "Mmpd-net: An aircraft deformation prediction network based on multimodal fusion," 2022.

[49] H. Si, J. Qiu, and Y. Li, "A review of point cloud registration algorithms for laser scanners: applications in large-scale aircraft measurement," *Applied Sciences*, vol. 12, no. 20, p. 10247, 2022.

[50] X. Wang, L. Zhang, Y. Liu, F. Li, Z. Chen, C. Zhao, and T. Bai, "Dynamic scheduling of tasks in cloud manufacturing with multi-agent reinforcement learning," *Journal of Manufacturing Systems*, vol. 65, pp. 130–145, 2022.

[51] L. Xu, Q. Xu, J. Tu, J. Zhang, Y. Zhang, C. Chen, and X. Guan, "Learning-based scalable scheduling and routing co-design with stream similarity partitioning for time-sensitive networking," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13 353–13 363, 2022.

[52] J.-L. Grégorio, C. Lartigue, F. Thiébaut, and R. Lebrun, "A digital twin-based approach for the management of geometrical deviations during assembly processes," *Journal of Manufacturing Systems*, vol. 58, pp. 108–117, 2021.

[53] L. Wang, X. Hu, Y. Wang, S. Xu, S. Ma, K. Yang, Z. Liu, and W. Wang, "Dynamic job-shop scheduling in smart manufacturing using deep reinforcement learning," *Computer Networks*, vol. 190, p. 107969, 2021.

面向工业互联网装备预测性维护的跨域预测方法综述

贾子翟，董家宝，王海腾，李世祥，王宇清，任磊

摘　要：复杂装备的预测性维护(Predictive Maintenance)是工业互联网中的主要任务之一，对于保障工业设备的安全运行起着至关重要的作用。深度学习等人工智能方法的突破性创新也在驱动着预测性维护方法的不断发展。然而现代制造任务、设备和过程日益复杂导致监控数据分布不断变化，甚至不可见，导致工业设备状态难以精准监控。近年来各种跨域预测方法逐渐进入人们的视野，这类方法可以通过无监督的手段将有标签数据域的知识迁移至未标记的数据域。基于此，本文调研了跨域预测的各种方法，包括领域自适应、无源领域自适应、领域泛化，分别针对这些方法的问题设定和代表性方法进行了介绍。最后，本文对工业装备预测性维护的未来发展趋势做了展望。

关键词：工业互联网；预测性维护；深度学习；跨域预测

A review of cross-domain prediction methods for predictive maintenance of Industrial Internet equipment

Zidi Jia, Jiabao Dong, Haiteng Wang, Shixiang Li, Yuqing Wang, Lei Ren

Abstract: Predictive maintenance of complex equipment is one of the key tasks in the Industrial Internet and plays a vital role in ensuring the safe operation of industrial assets. Breakthrough innovations in artificial intelligence methods, such as deep learning, are also driving the continuous development of predictive maintenance methods. However, the increasing complexity of modern manufacturing tasks, equipment, and processes has resulted in a constantly changing and even invisible distribution of monitoring data, resulting in challenges in accurately monitoring of industrial equipment. In recent years, cross-domain prediction methods have gradually come to the fore. Such methods can transfer knowledge from labeled data domains to unlabeled data domains in an unsupervised manner. Based on this, this paper investigates various cross-domain methods, including domain adaptation, source-free domain adaptation, and domain generalization, and introduces the problem settings and representative methods of these methods, respectively. Finally, this paper outlooks the future development trend of predictive maintenance of industrial equipment.

Key words: Industrial Internet, predictive maintenance, deep learning, cross-domain prediction

1　引言

复杂装备的预测性维护(Predictive Maintenance, PdM)是工业互联网的主要应用之一，也是保障工业设备安全、可靠运行的重要手段之一。工业生产中设备逐渐向大型化、复杂化、综合化和智能化的趋势发展，这对设备运行的可靠性、安全性和经济性提出了更高的需求。实时的感知设备的健康状态及其退化趋势，制定合理的维护计划，进而最大化设备的可用性、安全性和可靠性，是当前一个重要的议题。预测性维护

是预测设备中即将发生的故障或剩余使用寿命，并在最优的时间点采取维护措施，从而降低故障发生率和故障危害程度。在工业制造智能化过程中，复杂装备的预测性维护也是至关重要的一个环节，可以使重大装备的运行智能化水平大大提高。

随着智能时代的到来，人工智能促进了多个领域的快速发展和深度整合[1]。近年来，由于一些关键技术的突破，基于深度学习的方法[2]已成为预测性维护的主要方法。尽管深度学习方法在工业互联网设备预测性维护中显示出了巨大的潜力，但现代制造任务、设备和过程日益复杂的性质已经带来了重大挑战。从监控数据的低质性和分布偏移的角度出发，基于深度学习的装备预测性维护面临以下瓶颈挑战问题。首先，由于工业任务的复杂多变，被监控设备的工况可能是未知的，难以采集足够的高质量信号。然而，当前设备预测性维护中所使用的数据分析模型大多服从有监督的建模范式，即需要高质量的有标签数据来分析数据和标签的线性或非线性映射关系。这导致现有的大多数工业数据分析模型难以满足对利用无标签监控数据来训练健康指标预测模型的需求。其次，出于对于私有性和安全性的考虑，工业互联网产业联盟中的成员一般都不希望将自己工厂的监控数据和其他成员分享，只能将健康指标预测模型以“黑盒”的形式共享。这导致在跨域知识迁移时，只能访问源域数据训练好的预训练模型，而无法访问源域数据。这导致难以直接从历史数据中获取信息。最后，装备的工况往往是复杂多变的，导致从工业互联网中采集而来的传感数据在特征空间中的分布可能存在差异。这对工业时序分析模型所需求的数据独立同分布假设带来了挑战，传统设备健康指标预测方法可能无法适应工况突然变化或是渐变演化过程进而导致可靠性下降。

一些跨域预测方法可以利用来自源域的标记数据和来自相关但不同目标域的未标记数据进行训练模型，并使其在目标域表现良好。许多典型的同质无监督深度领域适应方法被开发，将深度学习中强大的层次表示与跨域迁移方法相结合，以减少对潜在昂贵的目标数据标签的依赖。因此，基于领域自适应（Domain Adaptation）以及领域泛化（Domain Generalization, DG）的方法成为了研究者关注的重点。

鉴于此，本文献综述主要围绕面向工业互联网装备预测性维护的跨域预测方法具体展开。首先介绍领域自适应问题设定；之后介绍DA方法的研究现状，包括有源领域自适应、无源领域自适应（Source-Free Domain Adaptation, SFDA）以及领域泛化；最后分析工业互联网下PdM跨域预测方法的研究趋势。

2 跨域预测问题设定

2.1 有源领域自适应

为了便于描述，这里采用 DA 的基本标准符号。将一个数据域表示为$D = \{\mathcal{X}, P(X)\}$，$\mathcal{X}$为特征空间，$X \in \mathcal{X}$，$P(X)$是数据在特征空间中的边际分布。给定一个有标签的源域$D^{\mathbb{S}} = \{X^{\mathbb{S}}, P^{\mathbb{S}}(X)\}$和一个未标记的目标域$D^{\mathbb{T}} = \{X^{\mathbb{T}}, P^{\mathbb{T}}(X)\}$，$D^{\mathbb{S}}$和$D^{\mathbb{T}}$是不同但相关的分布。无监督 DA 尝试将在$D^{\mathbb{S}}$中学习到的知识转移到$D^{\mathbb{T}}$中，从而使目标域的预测获得良好的效果。尝试将$D^{\mathbb{S}}$中学习到的数据与标签之间的相关性转移到$D^{\mathbb{T}}$中，

使预测模型在未知条件$D^{\mathbb{T}}$下也能具有良好的性能。将源域数据表示为$\{X_i^{\mathbb{S}}, Y_i^{\mathbb{S}}\}_{i=1}^{n^{\mathbb{S}}}$，$X_i^{\mathbb{S}} \in R^{m\times k}$是源域的第 i 个样本，是 m 个传感器在 k 个采样时刻采集的监控信号，Y 是 X 的标签，$n^{\mathbb{S}}$是源域中样本的数量。同样，$\{X_i^{\mathbb{T}}\}_{i=1}^{n^{\mathbb{T}}}$为未标记的目标域数据，$X_i^{\mathbb{T}} \in R^{m\times k}$，$n^{\mathbb{T}}$是目标域内的样本数。对于 DA，目标是学习源域$D^{\mathbb{S}}$上的预测函数$f: x \to \hat{y}$，并将它迁移到目标域，以获得在目标域$D^{\mathbb{T}}$上的最小误差。

2.2　无源领域自适应

由于要解决隐私保护下的工业数据预测问题，所以只有在源域训练的源模型和未标记的目标数据可用。SFDA 尝试采用无监督学习方法，将在源域训练的预测模型$M^{\mathbb{S}}$中的知识转移到目标域，从而在目标域保持满意的预测性能。目标域内的数据定义为$\{X_i^{\mathbb{T}}\}_{i=1}^{n^{\mathbb{T}}}$，$X_i^{\mathbb{T}} \in R^{m\times k}$，表示 m 个传感器收集的 k 个时间步长的信号。SFDA 的学习目标是将源域中的映射关系$f: x \to \hat{y}$迁移到目标域，使其在目标域中服从最小的损失。

2.3　领域泛化

领域泛化使模型通过学习不同领域的不变知识，在处理更广泛分布的数据时保持较高的鲁棒性。设 X 表示数据，Y 表示其对应的标签。一个域，表示为$D^{\mathbb{T}} = \{X^{\mathbb{T}}, y^{\mathbb{T}}(X)\}$，由从一个联合分布$P_{Xy}$采样的数据组成。传统方法在特征空间通过经验风险最小化（ERM）获得一个预测函数$f: x \to \hat{y}$应用于训练集 D。然而，当训练和测试集不服从独立同分布的假设时，ERM 不鲁棒并且难以推广，尽管它很高的计算效率。这里考虑了多源 DG 技术。给定一个训练集$D = \{D^k\}_{k=1}^{K}$包含 K 个源域，$D^k \sim P_{Xy}^k$，服从不同分布P_{Xy}^k，DG 的目标是通过最小化预期误差在任何看不见的目标域$D^{\mathbb{T}}$中获得一个鲁棒的和可推广的预测函数f，作用于不同于P_{Xy}^k（$k = 1, \ldots, K$）的联合分布P_{Xy}^T。

3　领域自适应方法

3.1　有源领域自适应

为区别于无源领域自适应，这里将一般的DA方法称为有源领域自适应方法。根据研究路线和建模思路的不同，这些方法可以被概括为：基于域分布对齐的方法、基于域映射的方法、基于归一化统计的方法、基于集成的方法和基于决策边界的方法。此外，DA也可以通过深度生成模型实现，并且这些方法的组合也可以带来更有效的知识迁移。

3.1.1 基于域分布对齐的方法

基于域分布对齐的方法通过创建一个域不变的特征表示来对齐源域和目标域，通常以特征提取器的形式实现。如果特征遵循相同的分布，那么无论数据来自源域或目标域，特征都是域不变的[3]。如果一个模型能够使用域不变特征进行训练，并在源数据上表现出良好的性能，那么该模型很可能能够很好地推广到目标域。这是因为目标数据的特征与训练源域模型所学到的特征相匹配。然而，这些方法的有效性基于一个假设，即存在一种特征表示方式，使得在不同域上的标签分布没有明显的差异。

域对齐分布的最常用方法，通过最小化度量分布之间的距离的散度来实现。代表性的散度度量的选择方法包括最大平均差异(Maximum mean discrepancy, MMD)、相关对齐(Correlation alignment, CORAL)[4]、对比域差异(Contrastive domain discrepancy, CCD)[5]和图匹配损失[6]等。MMD是基于两个分布的样本对两个分布相等的假设进行的双样本统计检验，由两个域样本上平滑函数的平均值的差计算的。CORAL类似于具有多项式内核的MMD，通过计算源域和目标域特征的二阶统计量之间的距离以最小化距离。CDD是另一类常用域对齐方式，通过最小化类内差异并最大化类间边际实现。另一种散度度量来自于图匹配，即在图之间寻找最优对应关系的问题。对一批样本的表征可以看作是一个无向图，其中相似的样本是邻接的。给定源数据的图表征，以及来自一批目标数据的图表征，那么对齐这些图的成本可以用作散度。

特征级的对抗性DA方法是学术界研究的重点之一[7]。对齐组件通常是一个域分类器。域分类器是一种用于判别特征表示是源数据还是目标数据生成的分类器。在生成对抗网络中，判别器被设计用来准确预测一个样本是真实数据分布还是生成器生成的数据。同样地，域分类器可以被设计成判别源分布和目标分布的判别器。域分类器的训练目标是正确地对域进行分类。在这种情况下，特征提取器被训练以产生无法被域分类器准确分类的特征表示。这样的训练过程形成了一种零和博弈。通常情况下，这些网络通过在这两个步骤之间交替进行反向训练。特征提取器的权重通过反向传播进行更新，以最大程度地混淆域分类器。

3.1.2 基于域映射的方法

创建域不变特性表示的另一种替代方法是从一个域映射到另一个域。映射通常是在特征级和特征级（即特征级的对抗性DA）创建的。这个映射可以通过一个有条件的生成对抗网络来完成。生成器通过将源输入数据转换为与目标分布非常相似的数据，在特征级执行自适应。之后，分类器可以使用已知的源标签[8]对映射到目标域的源数据进行训练，或与生成对抗网络[9]联合训练。与原始的生成对抗网络不同，条件生成对抗网络引入了额外的输入信息，如类标签或其他数据[10]。这样，生成器可以根据这些额外的信息来生成特定类型的数据。通过将类标签作为条件输入，生成器可以根据指定的类别生成与该类别相对应的图像样本。另一个应用是数据偏移，将输入数据从一个域映射到另一个域[11]。

虽然上述方法主要用于域间的数据映射和转换，但它们也可以用于DA任务。常见的方法是通过训练一个模型将源域实例映射到目标域实例，并在源域上进行监督学习，然后将该模型应用于目标域上的分类任务[12]。此外，可以学习从目标域到源域的映射。训练源域模型后，使用已知的源域标签进行监督学习。之后，在测试阶段，将目标域实例输入到实例转换模型中，将其转换为源域数据类似的样式，然后使用在源域上训练的模型对转化后的数据分析[13]。

3.1.3 基于归一化统计的方法

大多数神经网络中都使用批归一化batch norm等数据标准化处理[14]。这些处理的好处包括允许更高的学习率，从而加快训练速度，减少初始化的敏感性，平滑优化的景观并提供更清晰的梯度，以及允许更深

层次的网络聚合[15]。然而，这些标准化技术都没有考虑到DA的问题。在DA的情况下，每个数据域的标准化统计数据可能会有所不同。Li等人[16]提出了一个假设，即神经网络可以学习任务知识，而batch norm可以学习领域知识。

3.1.4 基于集成的方法

基于多个模型构建的集合通常可以对模型输出进行综合考量[17]，从而优于单个模型。这些方法利用集成预测来指导学习，或使用集成来衡量对目标数据的伪标记预测置信度。一种常用于DA的集成方法是对一个模型在训练过程中多个时间点的参数进行评估，将预测或网络权重进行平均[18]，这被称为自集成。然而，由于集成通常需要不同的模型，这些自集成方法需要在网络中引入高度的随机性。同时，还可以对单个模型的不同预测进行比较，以确定集成对该预测的置信度。集成中一致的模型越多，集成对该预测的可信度就越高。这就引出了伪标签这项技术的使用。将其应用于DA，可以使用对源数据进行训练的不同集成来标记目标数据。如果集成的伪标签是高置信的，那些被标记的目标样本就可以用来训练目标模型。这种方法可以提供一种有效的方式来利用集成的置信度来增强DA的性能。

3.1.5 基于决策边界移动的方法

可以将决策边界移动到较低密度的区域（即数据点较少的区域），实现自适应的域对齐[19]。这基于大多数聚类方法的一个基本假设，即数据点分布在单独的聚类中，每个聚类中的样本都有一个共同的标签；同时决策边界应该位于特征空间的低密度区域。这通常由对抗性训练实现。

3.2　无源领域自适应

在传统的DA方法中，通常假设在自适应过程中同时可以访问源域和目标域数据。然而，这在许多应用程序中都是不现实的[20]。由于隐私、保密性和私有性问题，源域数据无法使用。这阻碍了DA的进一步发展。近年来提出了无源领域自适应[21]，并已迅速成为DA的重点被广泛研究。在DA方法的基础之上，SFDA方法可以被分为两类：基于数据的方法和基于模型的方法。

3.2.1 基于数据的无源领域自适应方法

出于不同的动机，基于数据的SFDA方法的可以分为基于领域重建和基于实例信息提取两类。

(1) 基于领域重建的方法

在考虑源域数据不可用的情况下，一种直观的方法是通过利用源域模型中的隐含信息来模拟源域数据，或者重建一个中间域或另一个域来弥补源域数据的缺失。这种方法被称为基于领域重建的方法。这样做的目的是弥补源域数据不足的问题。一般而言，构造新的领域可以采用以下三种方法：生成虚拟源域、构造扰动目标域进行鲁棒学习，以及将目标域划分为类源域和类目标域并进行域内对抗。

由于模型已在源域上进行了预训练，因此可以通过探索模型的输出来模拟域的分布。虚拟域生成可以通过基于对抗性生成或基于高斯分布两种方式。基于对抗性生成的方法重点在于约束跨域的语义一致性的

一致性损失的设计[22]。也可以利用预训练模型中的隐式知识，基于高斯分布模拟源域的分布[23]。

构造扰动目标域的方法基于源域和目标域的特征都来自于一个域不变的特征空间的假设，即源域和目标域实际上是由域不变特征和一些域偏置因子形成的[24]。从扰动的角度来看，通过利用目标域数据对源域数据进行语义增强，可以指导模型学习域不变的特征。即使在没有源域数据的情况下，也可以在模型训练过程中对未标记的目标数据添加一些适当的域相关扰动。如果模型能够抵抗这些与域相关的扰动，就有可能获得域不变的特征。在这一技术路线上的方法仍然很少，但由于其独特的技术特点，它仍是一个与基于领域重建中的其他两类方法并行，并值得研究的类别。

基于域内对抗的方法在目标域内执行二进制分割，在保持源模型知识的同时，在两个数据域之间进行对抗性学习[25]。它与基于虚拟源域的方法不同，前者注重域内的对抗性分布对齐，而后者注重构建虚拟源域。域内对抗对齐主要使用不同的分类器和特征提取器进行对抗。可以通过冻结一个分类器的参数来保留源特定的分类器，并可以在未标记的目标数据上训练目标特定的分类器。此外，根据源特定分类器的预测置信度或其他标准，可以将目标域分为源相似和源不同样本，从而通过目标特定分类器和源特异性分类器对两个数据域的预测，可以实现域内对抗对齐。

(2) 基于实例信息提取的方法

另一类方法旨在探索未标记的目标域数据中的潜在数据结构或聚类信息，从而使得可以单独使用目标域数据来执行DA任务。这种方法的目标是利用目标域数据中的内在信息，使得DA任务能够在没有标注数据的情况下进行。这种方法可被称为基于实例的信息提取的方法。一个实例中所包含的信息可以分为与标签相关的信息和特定于领域分布的信息[26]。基于此，可以使用近邻聚类和实例分布转换等SFDA方法。实例分布转换方法将目标实例转换为源实例的特征表示，而不改变其内在特征[27]，使源领域的模型能够更好地识别目标实例。由于它主要应用在视觉领域，因此本文不做过多评价。近邻聚类方法利用目标数据本身的内容信息建立一个清晰的结构和聚类，通过增加类内距离并减少类间距离来增强特征空间中相邻节点的一致性。这样做可以减少分类的困难，因为误分类主要发生在模型的决策边界上。

3.2.2 基于模型的无源领域自适应方法

与专注于数据生成或探索数据属性的基于数据的方法不同，基于模型的方法将模型分离为几个子模块，然后调整其中一些参数以进行领域适应。自监督学习是这一类SFDA最流行的范式。自监督学习方法大多使用辅助模块来提高模型的鲁棒性，并与其他方法结合保持源域知识。在SFDA中，大多数的自监督学习方法都是基于伪标签、熵最小化的思想来进行的。

在无监督的情况下，一种直观的方法是根据源模型的预测对目标样本进行标注，之后利用这些伪标签进行自监督学习。这个过程可以分为三个步骤来进行：原型生成，使用一些高置信样本或所有样本来生成类原型；伪标签分配，给未标记的目标域样本分配伪标签；伪标签过滤，对分配的伪标签进行过滤，以去

除噪声标签，从而保持标签的纯度（第一步和第三步不是必须的）。原型生成的最简单方法之一是通过自熵[28]来选择类原型，即在每个类中选择自熵大于一定阈值的样本。但是，以这种方式选择的类原型可能没有代表性。同样，受到主动学习的启发，一些方法[29]认为具有较高自由能的目标样本更能代表目标域分布，可以作为类原型。另一种流行的方法是基于深度集群计算各类的质心。一些研究认为只使用一个原型并不能完全描述类，因此在每个类中生成多个原型。一般来说，这个步骤的目的是获得一个可以表示目标域中每个类别的分布的类原型。一旦得到类原型，每个样本就可以通过与不同类原型的相似性或距离进行比较得到伪标签。伪标签直接由模型输出中最复杂的类别分配。

通过对齐源域和目标域的特征分布的DA方法在没有源域数据的情况下是不可行的。因此，假设得到了一个具有自适应能力的模型，那么每个样本的模型输出应该是确定性的，即熵最小化，这个理想的结果约束可以反向指导模型的优化[21]。由于熵最小化损失很容易实现，可以很容易地结合其他方法如伪标记方法作为损失函数。然而，熵最小化损失在训练过程中可能会导致一个简单的解决方案，即所有的预测都偏向于某一类，所以可以利用批熵最大化损失来确保预测的多样性[30]。

3.3　领域泛化

领域泛化是指利用一种或多种源域数据训练深度学习模型，以使其在未知的目标域上展现良好的性能[31]。基于DA的方法已经受到了广泛的关注，然而DA依赖于目标数据可用于模型自适应的假设，而这在实践中并不总是成立的。在许多应用程序中，在部署模型之前，目标数据是很难获得，甚至很难感知的。为了克服领域偏移问题以及目标数据的缺失，引入了领域泛化。近年来，DG方法主要面向多源域场景。现有的方法可分为三类：数据操纵、表征学习和学习策略。这些方法有着明显的差异，但并不冲突，可以相互集成，以实现更好的效果。

3.3.1 基于数据操纵的领域泛化方法

基于数据操纵的DG关注于对输入数据进行特定的处理和操作使得这些数据有利于学习具有强泛化能力表征。对于复杂的DG任务而言，基于数据操纵的DG方法通常是最简单有效的。此类方法通常以提升输入数据的多样性为目标进行数据的增强或生成。数据操纵的经典手段之一是领域随机化[32]，提升数据及标签的多样性。领域生成是另一种经典方法[33]，旨在构建一个新的数据域对模型的训练进行增强，通过设定一定的约束，使新生成的数据域能够对模型的泛化能力有所提升。

3.3.2 基于表征学习的领域泛化方法

基于表征学习的DG方法是研究最广泛的一类方法，通过领域不变性表征和特征解耦，提取对于源域和未知目标域有着共同特性的特征向量[34][35]。基于表征学习的方法有对抗训练、显式的特征对齐、因果关系表征等技术。这些方法可以提取对于源域和未知目标域有着共同特性的特征向量。领域对抗训练是一种常用的表征学习方法，用于学习领域无关的表示。显式对齐技术用相比于对抗学习等对齐方式更为直接，

其直接使用特定的约束手段对不同域的特征进行规范对齐。因果关系是比联合分布更细致的变量关系描述方式。它提供了系统在干预条件下如何行为的信息，因此在DG任务中适用，因为域偏移可以看作是一种干预操作。特别是在考虑因果关系的情况下，期望的表征是标签的真实属性，这样就不会因为对相关但语义无关的特征进行干预而对预测结果产生影响。

3.3.3 基于学习策略的领域泛化方法

基于学习策略的DG主要包含三种思路，即集成学习[36]、元学习[37]和分布式鲁棒优化[38]。集成学习的方法通常通过混合多个模型和专家系统来进行联合预测，以提升模型的能力。集成学习的基本假设是任何一个样本都可以被视为由多个数据域采样得到的综合样本，因此该样本的真实预测值也应该通过使用由多个数据域训练得到的模型进行集成预测。元学习DG方法引入了元学习的思想框架，通过将多个源域数据划分为元训练集和元测试集，并在训练过程中利用这些数据集来模拟分布偏移现象。元学习的目标是通过利用元数据集在模型训练期间学习对元测试集的泛化能力，从而在真实的目标域数据上实现泛化。基于元学习的DG方法能够在具备多源域的情况下实现优秀的知识迁移，从而提升对未知领域的泛化能力。除了前面提到的方法，基于梯度操作的DG也是值得讨论的。这种方法主要利用梯度的各种信息来强制模型学习具有泛化能力的表示。分布式鲁棒优化(DRO)[161]通过学习在最坏分布情况下的模型，并将其推广到测试数据，以实现领域泛化。

4 未来研究趋势

4.1 基于联邦学习的分布式建模

由于隐私方面的考虑，传统的集中式训练方法可能不适用于敏感数据驱动的工业场景。为了进行集中式训练而收集大量数据可能带来严重的隐私风险。因此，在大规模工业应用中，有效且协同地实现人工智能提出了新的要求。联邦学习是一种可行的方案，它可以使参与者通过协作学习一个共享模型，而不需要暴露其本地数据。参与联邦学习的主要动机是获得更好的模型。没有足够私有数据的客户将从联邦学习的模型中获益最多。然而，对于那些拥有足够私有数据来训练精确的本地模型的客户来说，参与联邦学习的好处存在争议。研究表明，由于全局共享模型的准确性不如他们自己训练的本地模型，一些参与者可能无法从中获得任何好处。此外，一些研究质疑全局模型的效用，因为它与用户的典型使用方式差距较大。因此，对于个性化方面的研究变得十分必要。一种方法是利用迁移学习将通过联邦学习得到的全局模型在本地数据上进行再训练，进行全部或部分参数更新。另一种方法是利用多任务学习构建个性化联邦模型，并开发相应的算法来解决与通信、掉队和容错相关的挑战。

4.2 基于工业基础模型的预测性维护

近年来出现的各种设备预测性维护技术大多是“小模型”，与源自特定工业领域的应用需求的特定领域问题有很强的相关性。随着先进信息技术与工业制造的融合，以及日益复杂的工业网络物理系统的形成，

预测性维护将在系统层面上面临日益复杂的问题。现有的针对特定领域单一问题的“迷你模型”技术无法解决这一问题，迫切需要针对大型和复杂的工业系统问题探索新的工业智能技术。基础模型（foundation model）技术为这个问题提供了一个潜在的解决方案。基础模型作为深度学习领域的最新研究热点，提供了一种基本的、同质的“基石”建模技术，可以支持模型的预训练和快速适应下游任务，并可以突破当前小模型在结构层面上的精度限制。目前，在工业制造业，基础模型探索上仍存在差距，工业智能基础模型有望成为解决未来工业制造过程中各种高度复杂问题的颠覆性技术之一。

5　结束语

本文针对工业互联网中由于监测数据分布不断变化导致的预测性维护方法精度有限的问题，调研了跨域预测方法，包括有源领域自适应，无源领域自适应以及领域泛化。分别介绍了问题设定和典型方法。最优，对未来的研究趋势做出了展望。

参考文献：

[1] Zhao R, Yan R, Chen Z, et al. Deep learning and its applications to machine health monitoring[J]. Mechanical Systems and Signal Processing. 2019, 115:213-37.
[2] Sharma P, Jain S, Gupta S, et al. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications[J]. Ad Hoc Networks. 2021, 123:102685.
[3] Wilson G, Cook D J. A Survey of Unsupervised Deep Domain Adaptation[J]. ACM Transactions on Intelligent Systems and Technology, 2020, 11(5):1-46.
[4] Sun B, Feng J, Saenko K. Correlation alignment for unsupervised domain adaptation[C]. Computer Vision–ECCV 2016 Workshops: Amsterdam, The Netherlands, 2016, 443-450.
[5] Kang G, Jiang L, Yang Y, et al. Contrastive adaptation network for unsupervised domain adaptation[C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019.
[6] Chen L, Gan Z, Cheng Y, et al. Graph optimal transport for cross-domain alignment[C]. In International Conference on Machine Learning, 2020, 1542-1553.
[7] Ganin Y, Ustinova E, Ajakan H, et al. Domain-adversarial training of neural networks[J]. Journal of Machine Learning Research, 2016, 59:1–35
[8] Shrivastava A, Pfister T, Tuzel O, et al. Learning from simulated and unsupervised images through adversarial training[C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017.
[9] Bousmalis K, Silberman N, Dohan D, et al. Unsupervised pixel-level domain adaptation with generative adversarial networks[C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017.
[10] Denton E, Chintala S, Szlam A, et al. Deep generative image models using a Laplacian pyramid of adversarial networks[C]. Advances in Neural Information Processing Systems 2015, 28:1486–1494.
[11] Isola P, Zhu J Y, Zhou T, et al. Image-to-image translation with conditional adversarial networks[C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017.
[12] Li P, Liang X, Jia D, et al. Semantic-aware GRAD-GAN for virtual-to-real urban scene adaption[J]. arXiv preprint arXiv:1801.01726, 2018.
[13] Chen C, Dou Q, Chen H, et al. Semantic-aware generative adversarial nets for unsupervised domain adaptation in chest X-ray segmentation[C]. Machine Learning in Medical Imaging, 2018, 143–151.
[14] Santurkar S, Tsipras D, Ilyas A, et al. How does batch normalization help optimization? Advances in Neural Information Processing Systems[C]. 2018, 31, 2483–2493.
[15] Theis L, Oord A, Bethge M. A note on the evaluation of generative models[C]. Proceedings of the

International Conference on Learning Representations, 2016.
[16] Ioffe S, Szegedy C. Batch normalization: Accelerating deep network training by reducing internal covariate shift [C]. Proceedings of the 32nd International Conference on Machine Learning, 2015, 37, 448–456.
[17] Daho M, Settouti N, Lazouni M, et al. Weighted vote for trees aggregation in random forest[C]. Proceedings of the 2014 International Conference on Multimedia Computing and Systems, 2014, 438–443.
[18] Laine S, Aila T. Temporal ensembling for semi-supervised learning[C]. Proceedings of the International Conference on Learning Representations, 2017.
[19] Miyato, T, Maeda, S I, Koyama, M, et al. Virtual adversarial training: a regularization method for supervised and semi-supervised learning[J]. IEEE transactions on pattern analysis and machine intelligence, 2018, 41(8), pp.1979-1993.
[20] Yu Z, Li J, Du Z, et al. A Comprehensive Survey on Source-free Domain Adaptation[J]. arXiv preprint arXiv:2302.11803. 2023.
[21] Liang J, Hu D, Feng J. Do we really need to access the source data? source hypothesis transfer for unsupervised domain adaptation[C]. International Conference on Machine Learning, 2020, 6028–6039.
[22] Kurmi V K, Subramanian V K, Namboodiri V P. Domain impression: A source data free domain adaptation method[C]. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2021, 615–625.
[23] Yeh HW, Yang B, Yuen PC, et al. Sofa: Source-data-free feature alignment for unsupervised domain adaptation[C]. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2021, 474–483.
[24] Li S, Lv F, Xie B, et al. Bi-classifier determinacy maximization for unsupervised domain adaptation[C]. Proceedings of the AAAI Conference on Artificial Intelligence, 2021, 35(10):8455-8464.
[25] Xia H, Zhao H, Ding Z. Adaptive adversarial network for source-free domain adaptation[C]. Proceedings of the IEEE/CVF International Conference on Computer Vision, 2021, 9010–9019.
[26] Gatys L A, Ecker A S, Bethge M. Image style transfer using convolutional neural networks[C]. Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, 2414–2423.
[27] Luan F, Paris S, Shechtman E, et al. Deep photo style transfer[C]. Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, 4990–4998.
[28] Huang Y, Yang X, Zhang J, et al. Relative alignment network for source-free multimodal video domain adaptation[C] Proceedings of the 30th ACM International Conference on Multimedia, 2022, 1652–1660.
[29] Xie B, Yuan L, Li S, et al. Active learning for domain adaptation: An energy-based approach[C]. Proceedings of the AAAI Conference on Artificial Intelligence, 2022, 36(8):8708–8716.
[30] Jabi M, Pedersoli M, Mitiche A, et al. Deep clustering: On the link between discriminative models and k-means[J]. IEEE transactions on pattern analysis and machine intelligence, 2019, 43(6):1887–1896.
[31] Zhou K, Liu Z, Qiao Y, et al. Domain generalization: A survey[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(4):4396–4415.
[32] Peng X, Qiao F, Zhao L. Out-of-Domain Generalization From a Single Source: An Uncertainty Quantification Approach[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022.
[33] Zhou K, Yang Y, Hospedales T, et al. Learning to generate novel domains for domain generalization[C]. European conference on computer vision, 2020: 561-578.
[34] Motiian S, Piccirilli M, Adjeroh D.A, et al. Unified deep supervised domain adaptation and generalization[A]. Proceedings of the IEEE international conference on computer vision[C], 2017: 5715-5725.
[35] Arjovsky M, Bottou L, Gulrajani I, et al. Invariant risk minimization[J]. arXiv preprint arXiv:1907.02893, 2019.
[36] Zhou K, Yang Y, Qiao Y, et al. Domain adaptive ensemble learning[J]. IEEE Transactions on Image Processing, 2021, 30: 8008-8018.
[37] Finn C, Abbeel P, Levine S. Model-agnostic meta-learning for fast adaptation of deep networks[C]. International conference on machine learning, 2017: 1126-1135.
[38] Rahimian H, Mehrotra S. Distributionally robust optimization: A review[J]. arXiv preprint arXiv:1908.05659, 2019.

[作者简介]

贾子翟（1994-），男，北京航空航天大学博士研究生。主要研究方向：工业人工智能、领域自适应、领域泛化等。

董家宝（1998-），男，北京航空航天大学博士研究生。主要研究方向：工业人工智能、具身智能、机械臂抓取等。

王海腾（1999-），男，北京航空航天大学博士研究生。主要研究方向：工业大模型与生成式人工智能。

李世祥（1995-），男，北京航空航天大学博士研究生。主要研究方向：模型量化，剪枝，知识蒸馏，FPGA 神经网络加速。

王宇清（1999-），男，北京航空航天大学博士研究生。主要研究方向：工业大数据，机器人视觉以及计算机图形学。

任磊（1979-），男，博士，北京航空航天大学教授。主要研究方向：工业互联网，工业人工智能，工业大模型。

Energy-aware Remanufacturing Process Planning and Scheduling Problem Using Particle Swarm Optimization Algorithm

Jun Wang, Chunhua Tang, *Qiang Zhang

Jun Wang
Postgraduate Student
Key Laboratory of Process Optimization and Intelligent Decision-making, Ministry of Education, the School of Management, Hefei University of Technology
Hefei, China 230009
Email: wangjunkyle@mail.hfut.edu.cn

Chunhua Tang
Postgraduate Student
Key Laboratory of Process Optimization and Intelligent Decision-making, Ministry of Education, the School of Management, Hefei University of Technology
Hefei, China 230009
Email: chunhuatang@mail.hfut.edu.cn

Qiang Zhang (Corresponding author)
Ph.D., Professor
Key Laboratory of Process Optimization and Intelligent Decision-making, Ministry of Education, the School of Management, Hefei University of Technology
Hefei, China 230009
Email: qiang_zhang@hfut.edu.cn

Abstract

Solving remanufacturing process planning and scheduling problem collaboratively, leveraging the complementary attributes of process planning and shop scheduling to attain improved production flow and process routes, is crucial for further enhancing the environmental and economic benefits of remanufacturing. Most of the existing works regard these two segments as independent and solve them separately, which hinder the further improvements of remanufacturing system performance. Besides studies on energy-aware remanufacturing scheduling have all employed machine turn on/off strategy to achieve energy reduction, but not all machines are suitable for turn on/off strategy. Therefore, a new energy-aware remanufacturing process planning and scheduling model with process sequence flexibility is proposed. This model not only solves the remanufacturing process planning and scheduling problem collaboratively, but also employs machine speed-switching strategy to reduce energy waste. To solve this model, a reinforcement learning-based particle swarm optimization algorithm with an efficient multi-dimensional encoding scheme is proposed, in which, a hybrid population initialization strategy, a novel reinforcement learning-based multi-directional guide position-updating mechanism, a local search strategy, and a restart mechanism are devised to enhance the performance. A comprehensive experiment of the proposed algorithm against other

advanced algorithms is conducted. Experimental results confirm the superiority of the presented algorithm.

Key words: Energy-aware; Particle swarm optimization; Reinforcement learning; Remanufacturing process planning; Remanufacturing scheduling

1. Introduction

With the worsening of environmental pollution and energy crisis, the sustainability development of industrial civilization has been increasingly emphasized around the world. In view of this, remanufacturing has received extensive attention from both academia and industry as a significant approach to achieving sustainable development (Du and Li 2014; Fu et al. 2021). Remanufacturing is a complicated industrial process that restores end-of-life (EOL) products to like-new status through the implementation of various operations (Guide 2000). Compared with traditional manufacturing, remanufacturing not only provides like-new product quality and saves resources, but also reduces emissions of various toxic substances, offering considerable economic and environmental benefits.

Process planning and scheduling problem in remanufacturing have been regarded as two critical components when achieving the economic and environmental benefits of remanufacturing (Zhang et al. 2015). Remanufacturing process planning aims to optimize the procedures and steps involved in EOL product remanufacturing, including determining production flow, process routes, and related considerations. Scheduling involves systematically organizing the sequence of practical remanufacturing processing tasks, allocating machinery, and optimizing resource utilization to satisfy process planning constraints and achieve predefined optimization objectives (Li et al. 2018; Lin et al. 2020). The relationship between process planning and scheduling is interdependent and complementary. Most of the existing works regard the remanufacturing process planning and scheduling problem as two independent problems to be solved separately. For example, Wang et al. (2017) proposed a method to characterize the failure features of remanufactured products for obtaining an optimal remanufacturing process plan. Jin et al. (2024) focused on the dynamics of machine efficiency (degradation and learning) when solving the remanufacturing system scheduling problem. Although optimizing remanufacturing process planning or scheduling problem individually can improve remanufacturing efficiency to some extent, it still prevents further improvements in resource utilization and may contribute to problems such as unbalanced machine loads, and bottleneck resources (Zhang et al. 2023a).

The development of intelligent manufacturing, Internet of Things, and digitalization technologies has established a foundational framework conducive to achieving integrated optimization of process planning and scheduling. By facilitating data exchange, information interchange effectively coordinates and integrates process planning and scheduling, ensuring the efficient operation of remanufacturing systems. Several works have acknowledged the necessity of collaboratively optimizing remanufacturing process planning and scheduling problem and addressed them through different approaches (Zhang et al. 2015; Gong et al. 2020; Zhang et al. 2023a). Remanufacturing is a complicated industrial process with not only machine flexibility and process plan flexibility, but also process sequence flexibility (i.e., sometimes there is no priority in the sequence of processes). Neglecting any flexibilities may contribute to the inefficiency and energy wastage in the remanufacturing scheduling scheme obtained with process planning constraints. These works did not comprehensively express the flexibility of remanufacturing process planning and inadequately acknowledge the significance of energy-aware scheduling. With the potential pressure of global warming and resource scarcity, energy-aware scheduling is becoming increasingly important (Agrawal and Rao, 2014). All current work on energy-aware remanufacturing scheduling applies the machine turn on/off strategies. Energy consumption can be reduced by turning off non-bottleneck machines during idle times (Mouzon and Yildirim, 2007), but not all machines are suitable for the turn on/off strategies, and frequently switching machine states will shorten their lifetime.

Thus, to tackle the limitations of these works, a new energy-aware remanufacturing process planning and scheduling (ERPPS) model with process sequence flexibility is proposed to obtain a more efficient and environment-friendly remanufacturing scheduling scheme. Moreover, the proposed model incorporates a speed-switching strategy capable of adjusting machine speed based on actual demand to reduce energy waste when the machine is running at low load or idling without shortening the service life of the machine.

ERPPS problem is a typical NP-hard problem, and metaheuristic algorithms have been widely used to solve it. Particle swarm optimization (PSO) algorithm was proposed by Kennedy and Eberhardt (1995) as a population-based algorithm that has been widely applied to solve scheduling problem due to its efficiency and stability (Behnamian 2014; Shi et al. 2021). Nevertheless, the basic PSO algorithm still contains some inherent shortcomings, such as tendency to converge prematurely and poor population diversity. Reinforcement learning (RL) is one of the most important machine learning methods that learns from the interaction between the agent and

environment to solve various problems (Chen et al. 2020), and has been used in several works for adjusting and controlling parameters in metaheuristic algorithms to address their inherent shortcomings. Thus, a novel RL-based multi-directional guide position-updating mechanism is proposed in this study, which overcomes the inherent shortcomings of the basic PSO by solving the particle movement direction selection problem. On this basis, the reinforcement learning-based particle swarm optimization algorithm (RL-PSO) is proposed and five improvements are adopted to enhance the performance of the algorithm.

The remainder of this study is organized as follows. Section 2 reviews the relevant literatures. Section 3 describes the proposed ERPPS model. The proposed RL-PSO algorithm is presented in Section 4. Section 5 discusses and analyzes the experimental results. Section 6 presents the conclusion and future work.

2. Related work

In this section, two aspects of related works are briefly reviewed: process planning and scheduling in remanufacturing and metaheuristic algorithm.

2.1 Process planning and scheduling in remanufacturing

Compared to conventionally manufactured products, remanufactured raw materials are EOL products with significant differences in quality, which complicate both process planning and scheduling problem. Van et al. (2017) designed an additive and subtractive combinatorial process approach to solve the remanufacturing process planning problem. In our previous work (Anonymous Authors 2019), the adoption of advanced repair techniques in engine remanufacturing has been explored to improve the efficiency of the remanufacturing process. Kimita et al. (2021) proposed a design method for remanufacturing process planning based on the concept of loosely coupled systems. Chen et al. (2021) constructed a failure description set for EOL products by combining attribute features and failure features, and proposed an integrated process-tolerance design optimization model. Lv et al. (2021) proposed a remanufacturing process planning model to improve remanufacturing efficiency and minimize costs by addressing the uncertainty and fuzziness involved in the remanufacturing process.

For the remanufacturing scheduling problem, initial works focused on developing various scheduling rules (Daniel and Guide, 1997), choosing appropriate scheduling strategies (Zhou et al. 2006), or adopting diverse practical constraints (Jeon et al. 2006) to determine a reasonable remanufacturing scheduling scheme. Afterwards, more and more works addressed the

remanufacturing scheduling problem with different configurations of remanufacturing systems. For example, Kim et al. (2015) developed an integer planning model to solve the remanufacturing system scheduling problem with a single disassembly/reassembly workstation, parallel flow-shop-type reprocessing lines. Yu and Lee (2018) addressed the remanufacturing system scheduling problem with component matching requirements under parallel disassembly/reassembly workstations, job-shop-type reprocessing shop configurations. With the objective of minimizing manufacturing and remanufacturing costs, installation costs, inventory holdings, and backlog costs within the planning horizon while minimizing machine energy costs and processing time, Roshani et al. (2022) proposed a large-bucket mixed integer planning model.

The aforementioned works addressed the optimization problem from the perspective of remanufacturing process planning or scheduling, respectively. However, optimizing process planning without considering the scheduling problem may result in wasting resources during the scheduling process, whereas just optimizing the scheduling problem based on the predefined processing routes may result in the lack of processing flexibility and imbalance of machine loads etc. In summary, it is necessary to solve remanufacturing process planning and scheduling problem collaboratively. Peng et al. (2019) applied the Petri net algorithm to formulate the cylinder block of engine remanufacturing process planning and developed a scheduling model with the objective of minimizing the completion time. After summarizing four common remanufacturing routes, Gong et al. (2020) proposed a mathematical model that simultaneously considers the remanufacturing process planning and scheduling problem. Zhang et al. (2023a) designed an extended network graph to solve the remanufacturing process planning and scheduling problem between the remanufacturing disassembly, reprocessing, and reassembly subsystems. However, these works mainly focused on handling route flexibility in process planning problem, ignoring process sequence flexibility.

In addition, with the increasing pressure of global warming and resource scarcity, more and more scholars are focusing on remanufacturing energy-aware scheduling. For example, Giglio et al. (2017) proposed a mixed-integer planning model to solve the energy-efficient job shop scheduling problem for hybrid manufacturing and remanufacturing. Shi et al. (2020) constructed an environment-aware remanufacturing scheduling model that aims to minimize the maximum completion time and carbon emissions. Wang et al. (2023) proposed an energy-aware remanufacturing scheduling model to minimize the total energy consumption and applied turn on/off strategy for pursuing remanufacturing environmental benefits. Most existing works about

energy-aware remanufacturing scheduling problem employed turn on/off strategies to reduce energy consumption, but turn on/off strategies cannot be applied to all machines, and frequently switching machine states will shorten their lifetime.

For the purpose of overcoming the aforementioned drawbacks, this study proposes a new ERPPS model that incorporates processing sequence flexibility. The primary objective of this model is to minimize both the makespan and energy consumption. And a speed-switching strategy is applied to reduce the remanufacturing energy consumption additionally, thereby striking a balance between remanufacturing efficiency and environmental benefits.

2.2 Metaheuristic algorithm

With the increasing scale of the problem, classical exact solution methods such as integer programming and branch-and-bound method struggle to effectively solve NP-hard problem such as remanufacturing process planning and scheduling problem. Consequently, a number of metaheuristic algorithms have been developed in the last decade for solving NP-hard problem. For instance, Gao et al. (2016) proposed a two-stage artificial bee colony algorithm to solve the remanufacturing scheduling and rescheduling problem with new job insertion constraints. Wang et al. (2023) applied genetic algorithms that integrated variable neighborhood search technique to solve the remanufacturing scheduling problem aiming at minimizing total energy consumption. Wang et al. (2024) proposed an iterative greedy algorithm that embeds reinsertion and re-destruction strategies to solve the distributed flow shop scheduling problem.

Besides the aforementioned metaheuristics, PSO algorithm has received a lot of attention due to its fast convergence and favorable stability in solving NP-hard problem. Shi et al. (2021) proposed a discrete PSO algorithm that integrates position update mechanism and multi-directional guiding strategy to enhance the population diversity and convergence rate of the algorithm. To solve multi-attribute group decision-making problem, tournament selection operator guided PSO algorithm has been proposed in our previous work (Anonymous Authors 2022). A hybrid differential evolution algorithm and PSO algorithm was proposed for solving the remanufacturing scheduling optimization problem with rework risk (Zhang et al. 2023b). In addition, as artificial intelligence technology continues to evolve, more and more works have explored the integration of RL with metaheuristic algorithms to overcome the inherent shortcomings of metaheuristic algorithms. For example, Chen et al. (2020) proposed a self-learning genetic algorithm with RL to intelligently adjust critical parameters of the genetic algorithm to solve the flexible job shop scheduling problem. Durgut et al. (2021) embed RL in an artificial bee algorithm, which

dynamically selects operators to generate new candidate solutions through RL, thereby balancing the global and local search capabilities of the algorithm.

The PSO algorithm is applied for solving the ERPPS problem in this study. However, the one-dimensional encoding scheme of the basic PSO algorithm is not appropriate for encoding the solution of the proposed model. Moreover, both the convergence rate and the exploitation and exploration capabilities of the proposed algorithm have further potential to be enhanced. Therefore, an RL-PSO algorithm is proposed to address the ERPPS problem which embeds an efficient multi-dimensional encoding scheme and a novel RL-based multi-directional guide position-updating mechanism to overcome the shortcomings of the basic PSO algorithm. In Section 4 all the improvements of the algorithm are described in detail.

3. Mathematical model

This section details the problem definition and develops a new ERPPS model.

3.1 ERPPS problem description

During the remanufacturing process, all EOL products will undergo a quality inspection. Following this, specific remanufacturing process plans will be developed based on the quality of product. By performing the remanufacturing operation corresponding to the process plan, the EOL product will be restored to a like-new status. It is worth noting that there is often more than one process plan for a EOL product, e.g., if the product has relatively severe abrasion, there are two typical surface restoration process plans: grinding, chromium electroplating or grinding, cold welding, fine grinding. The flow shop is ideally suited to handling large volumes of similar products via a pre-determined process plan. However, it is not ideally suited for the ERPPS problem proposed in this study, where the EOL products qualities varies widely. In contrast, the flexible job shop can develop one or more process plans to remanufacture EOL products based on the quality of each product. Therefore, in this study, the flexible job shop with machine and process plan flexibility is employed to remanufacture products. In addition, the remanufacturing process for some products may also have process sequence flexibility, such as the surface restoration process for some less worn products involves welding and grinding operations, which do not have specific sequence.

To clearly describe the proposed problem, an illustrative example of the fundamental framework that characterizes the remanufacturing process planning and scheduling problem is given in Fig.1. The upper part of Fig. 1 illustrates the remanufacturing process planning for three

distinct EOL products. Specifically, there are three process plans to remanufacture P_1 to a like-new status, where PR_{11} and PR_{13} are distinguished by the fact that O_1 and O_3 have process sequence flexibility. Furthermore, P_2 comprises two process plans, while P_3 solely adheres to a specific process plan. Then, on the basis of solving the remanufacturing process planning selection problem for each product, this study determines the sequence of products to be processed on each operation, the specific machine designated to perform the operation, and its corresponding processing speed to balance remanufacturing efficiency and environmental benefits. Finally, a scheduling scheme with superior performance is obtained by solving the above decision, illustrated at the bottom of Fig. 1. In this scheme, P_2 selected RP_2 for remanufacturing while M_3 is assigned to perform O_1 (machines capable of performing O_1 include M_1, M_2, M_3), and processing at speed V_1.

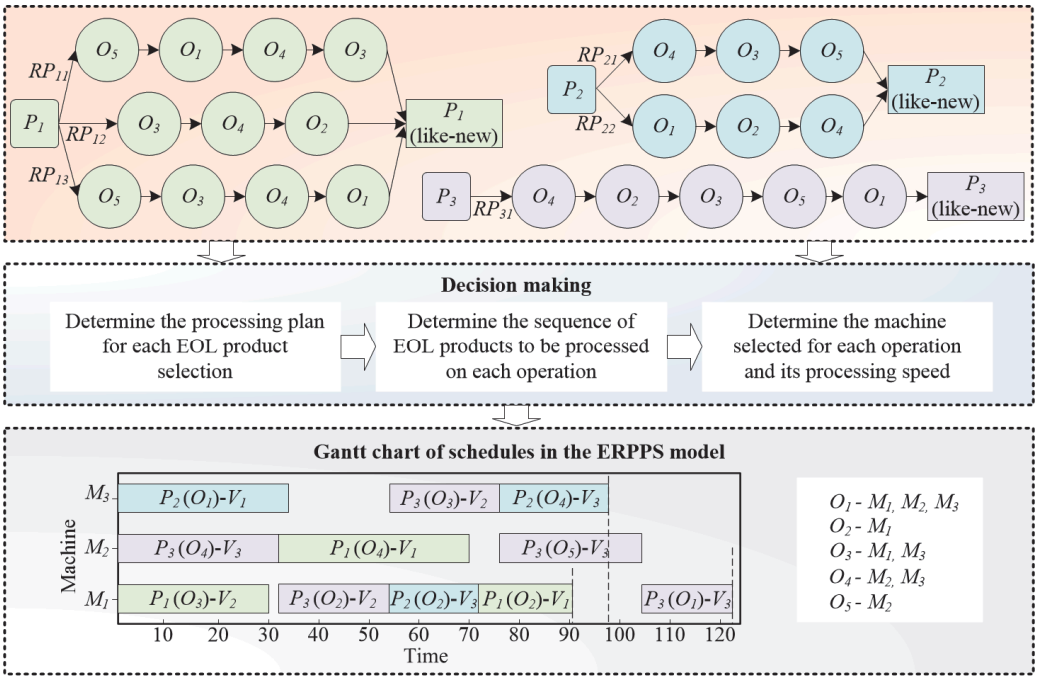


Fig.1. An illustrative example of the fundamental framework for ERPPS problem.

3.2 Modeling of ERPPS

Five assumptions were made to abstract the proposed ERPPS problem as follows:

1) Priority is not considered during the remanufacturing process.

2) When the scheduling optimization begins, all EOL products and machines are ready.

3) Once a machine starts an operation, it must finish it without interruption.

4) The setup time for machines is negligible.

5) Each machine can process only one product at a time.

3.2.1 Notations

For the purpose of explicitly describing the mathematical model of ERPPS, the following notations are defined.

P_i	ith EOL product, i = 1, …, I, where I is the number of remanufacturing products
O_l	lth operation, l = 1, …, L, where L is the number of operations
M_n	nth machine, n = 1, …, N, where N is the number of machines
PR_{ij}	jth process plan, j = 1, …, J_i, where J_i is the number of remanufacturing process plans of P_i
V_k	kth machine processing speed, k = 1, …, K, where K is the type of machine processing speed
T_{ij}^{ln}	standard processing time of O_l performed by M_n in PR_{ij}
S_{ij}^{ln}	starting time of O_l performed by M_n in PR_{ij}
E_{ij}^{ln}	ending time of O_l performed by M_n in PR_{ij}
RPC_{ij}^{ln}	remanufacturing power consumption of M_n at running mode per unit time perform O_l in PR_{ij}
SPC^n	remanufacturing power consumption of M_n at standby mode per unit time to perform O_l in PR_{ij}
REC_{ij}^{ln}	remanufacturing energy consumption when M_n runs at running mode to perform O_l in PR_{ij}
SEC^n	remanufacturing energy consumption when M_n runs at standby mode to perform O_l in PR_{ij}
TCT	total completion time of P_i
TEC	total energy consumption of P_i
α_{ij}	binary variable which equals 1 if P_i selects the jth process plan for remanufacturing, and 0 otherwise
β_{ij}^{l}	binary variable which equals to 1 if O_l is the first operation in PR_{ij}, and 0 otherwise
δ_{ij}^{ln}	binary variable which equals to 1 if M_n performing O_l in PR_{ij} is starting for the first time, and 0 otherwise
γ_{ij}^{ln}	binary variable which equals to 1 if O_l in PR_{ij} selects M_n for processing, and 0 otherwise

3.2.2 Mathematical model

In this study, the optimization objective of the proposed ERPPS model is to minimize *TCT* and

TEC to achieve the best economic and environmental benefits. Relevant mathematical formulas for *TCT* are as follows:

$$S_{ij}^{ln}=\begin{cases}0 & ,\beta_{ij}^{l}=1\ ,\delta_{ij}^{ln}=1\\ E_{ij}^{l'n'} & ,\beta_{ij}^{l}=0\ ,\delta_{ij}^{ln}=1\\ \max\left(E_{i'j'}^{l'n}\right) & ,\beta_{ij}^{l}=1\ ,\delta_{ij}^{ln}=0\\ \max\left[E_{ij}^{l'n'},\max\left(E_{i'j'}^{l'n}\right)\right] & ,\beta_{ij}^{l}=0\ ,\delta_{ij}^{ln}=0\end{cases} \tag{1}$$

$$E_{ij}^{ln}=S_{ij}^{ln}+\left(T_{ij}^{ln}/V_k\right)\times\gamma_{ij}^{ln} \tag{2}$$

$$TCT=\max_{\substack{1\le i\le I,1\le j\le J_i\\1\le l\le L,1\le n\le N}}\left(E_{ij}^{ln}\right) \tag{3}$$

where Eqs. 1 and 2 indicate the starting time and the ending time, respectively, of O_l performed in PR_{ij} by M_n. $E_{ij}^{l'n'}$ is the ending time of the preceding operation of P_i in PR_{ij}, $E_{i'j'}^{l'n}$ is the ending time for another product that was processed on the same machine as P_i, T_{ij}^{ln}/V_k is the actual processing time of M_n running at V_k. Eq. 3 is developed to calculate the total completion time which aims to minimize the makespan.

Inspired by Wang and Wang (2021), the relevant mathematical formulae for *TEC* are as follows:

$$REC_{ij}^{ln}=RPC_{ij}^{ln}\times\left(T_{ij}^{ln}/V_k\right)\times\gamma_{ij}^{ln} \tag{4}$$

$$SEC^{n}=SPC^{n}\times\left[\max_{1\le i\le I,1\le j\le J_i,1\le l\le L}\left(E_{ij}^{ln}\times\gamma_{ij}^{ln}\right)-\min_{1\le i\le I,1\le j\le J_i,1\le l\le L}\left(S_{ij}^{ln}\times\gamma_{ij}^{ln}\right)-\sum_{i}^{I}\sum_{j}^{J_i}\sum_{l}^{L}\left[\left(T_{ij}^{ln}/V_k\right)\times\gamma_{ij}^{ln}\right]\right] \tag{5}$$

$$TEC=\sum_{i}^{I}\sum_{j}^{J_i}\sum_{l}^{L}\sum_{n}^{N}\left(REC_{ij}^{ln}\times\gamma_{ij}^{ln}\right)+\sum_{n}^{N}SEC^{n} \tag{6}$$

where Eqs. 4 and 5 indicate the energy consumed by M_n to remanufacture P_i on O_l in PR_{ij}, and the energy consumed by the M_n at standby mode during the remanufacturing process, respectively. Eq. 6 is developed to calculate the total energy consumption which aims to achieve maximum environmental benefits.

This model is developed to obtain the scheduling scheme with maximum combined utility by minimizing *TCT* and *TEC*. In this study, normalization method proposed by Zeng et al. (2004) is employed to directly calculate the combined utility of the scheduling scheme. This method

transforms the multi-objective problem into a single-objective problem through selecting appropriate weighting coefficients for *TCT* and *TEC*. Here, manager can flexibly adjust the weighting coefficients for each objective based on actual needs. The normalized *TCT* and *TEC* are shown in Eqs. 7 and 8.

$$TCT' = \begin{cases} \dfrac{TCT_{\max} - TCT}{TCT_{\max} - TCT_{\min}}, TCT_{\max} - TCT_{\min} \neq 0 \\ 1 \qquad\qquad , TCT_{\max} - TCT_{\min} = 0 \end{cases} \tag{7}$$

$$TEC' = \begin{cases} \dfrac{TEC_{\max} - TEC}{TEC_{\max} - TEC_{\min}}, TEC_{\max} - TEC_{\min} \neq 0 \\ 1 \qquad\qquad , TEC_{\max} - TEC_{\min} = 0 \end{cases} \tag{8}$$

where TCT' and TEC' indicate the values of *TCT* and *TEC* after normalization, respectively. $TCT_{\max}$ and $TEC_{\max}$ indicate the maximum *TCT* and *TEC* to accomplish the remanufacturing task with all the constraints satisfied, respectively, while $TCT_{\min}$ and $TEC_{\min}$ indicate the minimum *TCT* and *TEC*.

In summary, the objective function of this study is constructed as follows:

$$\max f = w_t TCT' + w_c TEC' \tag{9}$$

where w_t and w_c are the weighting coefficients of *TCT* and *TEC*, respectively, and their sum is 1. And *f* is the fitness value of the proposed algorithm.

All the above formulas are subject to the following constraints:

$$\sum_{j=1}^{J_i} \alpha_{ij} = 1, \forall\ 1 \le i \le I \tag{10}$$

$$\sum_{i=1}^{I} \sum_{j=1}^{J_i} \beta_{ij}^{l} \le 1, \forall\ 1 \le l \le L \tag{11}$$

$$\sum_{i=1}^{I} \sum_{j=1}^{J_i} \sum_{l=1}^{L} \delta_{ij}^{ln} \le 1, \forall\ 1 \le n \le N \tag{12}$$

where constraint (10) ensures that at most one process plan is selected at a time for remanufacturing P_i, constraint (11) is to guarantee that no more than one product on O_l can be remanufactured first, and constraint (12) is to guarantee that no more than one product on M_n can be remanufactured first.

4. RL-PSO algorithm

In this study, the proposed problem is a discrete optimization problem, while the basic PSO algorithm is not applicable to solve this problem directly. Thus, in pursuit of obtaining a more optimal solution for this problem, an RL-PSO algorithm is explored. And five improvements are embedded in the RL-PSO algorithm including: 1) an efficient multi-dimensional encoding scheme is proposed to adapt the ERPPS model; 2) a hybrid population initialization strategy is proposed to speed up the convergence of the algorithm; 3) a novel RL-based multi-directional guide position-updating mechanism is proposed to maintain population diversity; 4) a local search strategy is employed for improving the exploration capability of the algorithm; and 5) a restart mechanism is applied to prevent algorithm from converging prematurely. The framework of the RL-PSO algorithm is shown in Fig. 2.

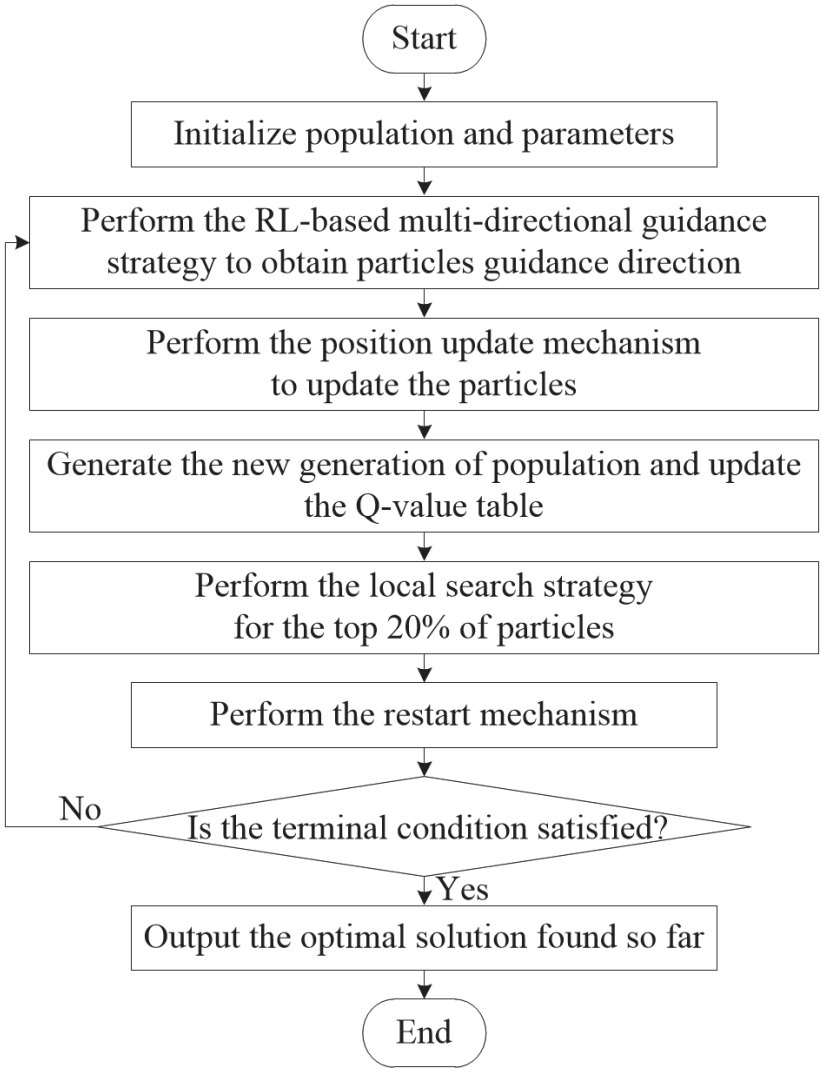


Fig. 2. Framework of the RL-PSO algorithm.

4.1 Multi-dimensional encoding scheme

A reasonable encoding scheme adopted to the ERPPS model can enhance the efficiency of the algorithm in solving problem. Therefore, in this study, a multi-dimensional encoding scheme that accurately maps the EOL product remanufacturing process planning (RP), operation sequence (OS), machine allocation (MA) and machine processing speed (MS) information to the RL-PSO algorithm is proposed according to the characteristics of the ERPPS model.

To explain the encoding scheme more clearly, there is an illustrative example presented through three EOL products remanufacturing process in Fig. 1 (as shown in Fig. 3). The first dimension of the example incorporates the process planning selection information for the three products, e.g., P_3 selected RP_1 for remanufacturing. The remaining dimensions encode the OS, MA, and MS information, and their length depends on the sum of operations when the process planning with the maximum number of operations is selected for each product, which is 12 (4+3+5) in this example. In the second dimension the second appearance of element 3 indicates the second operation (O_2) of P_3, while the corresponding elements in the third and fourth dimensions are the machine that performs the operation (M_1) and its processing speed (V_2), respectively. In addition, positions in each dimension that are not assigned any information will be filled with 0.

RP	2	2	1									
OS	1	2	3	1	3	2	3	1	2	3	3	0
MA	1	3	2	2	1	1	3	1	3	2	1	0
MS	2	1	3	1	2	3	2	1	3	3	3	0

Fig. 3. An illustrative example of multi-dimensional encoding scheme.

4.2 Hybrid population initialization strategy

Considering the initial population has a direct impact on the convergence and solution quality of the algorithm (Tian and Shi, 2018). Therefore, a hybrid population initialization strategy involving random generation rule, minimum number of operation rule, minimum time rule, and minimum energy consumption rule is proposed to accelerate the convergence of the algorithm. The specific implementation is detailed as follows:

Step 1: Randomly generate particles that reach the population size.

Step 2: Randomly select 60% of the particles to determine whether the product has multiple process plans. If it does, the minimum number of operations is selected for remanufacturing.

Step 3: Randomly select half of the particles from the 60% above to apply the minimum time rule, which means selecting the shortest processing time machine for each operation.

Step 4: Apply the minimum energy consumption rule to the other half of the particles, which

means selecting the minimum energy consumption machine for each operation.

4.3 RL-based multi-directional guide position-updating mechanism

(1) RL-based multi-directional guidance strategy

The particles in traditional PSO algorithms engage in evolution along two movement vectors, namely *pbest* and *gbest*. This simple learning model may result in poor population diversity. Although Shi et al. (2021) proposed a PSO algorithm equipped with a multi-directional guidance mechanism. Each particle in this algorithm is randomly assigned different guidance directions based on probabilities, which renders it challenging to effectively balance the exploitation and exploration capabilities of the algorithm.

Therefore, five guidance directions were designed in this study based on the characteristics of the ERPPS model, which are *pbest*, *gbest*, *tbest*, *ebest*, and *rand*, where *tbest*, *ebest*, and *rand* are particles with the smallest total completion time, the smallest total energy consumed and the randomly selected particle, respectively. Furthermore, Q-learning is employed at each iteration to steer the evolutionary trajectory of individual particles, maintaining population diversity and effectively balancing the capabilities of the algorithm in exploitation and exploration. Q-learning is a simple and efficient RL method proposed by Watkins and Dayan (1992). It consists of five components: agent (*A*), environment (*E*), action set (*As*), state set (*S*), and reward (*R*). This method effectively uses all kinds of information generated by the metaheuristic algorithm during the iterative process, thereby enhancing the performance of the algorithm (Chen et al. 2020).

Fig. 4 illustrates the interaction between the agent and the environment in Q-learning. Specifically, at time *t*, the agent performs an action (A_t) based on the state of the environment (S_t). Subsequently, the agent receives a reward denoted as R_{t+1}, and state of the environment will then change to S_{t+1}. In this study，the epsilon greedy policy is adopted. That means if the randomly generated number within 0-1 is bigger than greedy factor ε then the agent will choose the action with the biggest Q value, otherwise the agent will choose a random action. The Q-value will be updated according to Eq. (14):

$$Q(S_t, A_t) \leftarrow (1-\alpha)Q(S_t, A_t) + \alpha\left[R_{t+1} + \gamma \times \max_a Q(S_{t+1}, A_{t+1})\right] \tag{14}$$

where $Q(S_t, A_t)$ is the Q-value for performing action A_t at state S_t and R_{t+1} is the reward obtained after performing action A_t; α is the learning rate and γ is the discount rate, both of which are located at [0,1]; $\max_a Q(S_{t+1}, A_{t+1})$ indicates the highest expected Q value in the Q-value

table that can be obtained by performing the action A_{t+1} at state S_{t+1}.

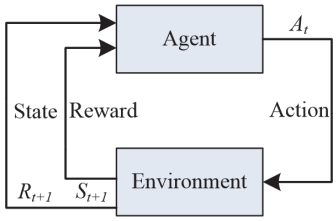


Fig. 4. The interaction between agent and environment of Q-learning.

Inspired by Li et al. (2019), this study divides each particle in the population into nine states according to the objective function of the ERPPS model, as shown in Fig. 5. Specifically, the result of each objective function can be sorted into three levels in descending order: the first level (denoted as 1) ranging from 0-33%, the second level (denoted as 2) ranging from 33%-67%, and the third level (denoted as 3) ranging from 67%-100%. Therefore, considering the two objective functions of *TCT* and *TET* in the ERPPS model, the states in this study are divided into nine, denoted as $\left[(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (2,\ 1),\ (2,\ 2),\ (2,\ 3),\ (3,\ 1),\ (3,\ 2),\ (3,\ 3)\right]$. The action set that is the five guidance directions of the particle is denoted as *p*, *g*, *t*, *e* and *r*. If the state of a particle changes for the better after performing an action, e.g., from $(2,\ 2)$ to $(1,\ 1)$ then the reward is 2 ($(2+2) - (1+1) = 2$), otherwise the reward is -1, e.g., from $(2,\ 2)$ to $(3,\ 3)$. It is worth noting that for better learning the appropriate guidance direction at different stages of the algorithm iteration process, the algorithm will initialize the q-value table after every one hundred iterations are completed.

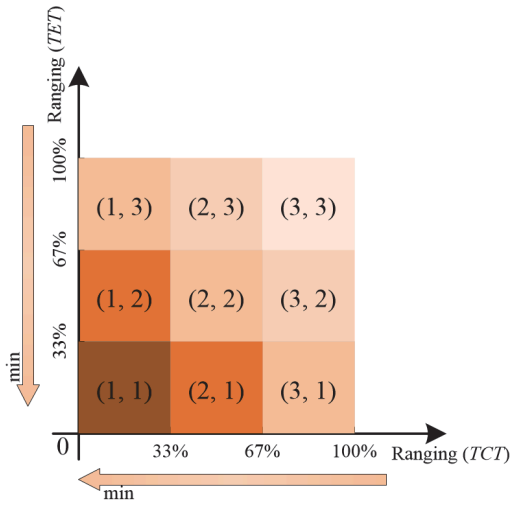


Fig. 5. An illustrative example of state levels based on *TCT* and *TET*.

(2) Position-updating mechanism

Given that it is primarily designed for solving continuous optimization problems, the basic PSO algorithm is not appropriate for direct application to solving the proposed ERPPS problem.

Thus, this study proposes a new position-updating mechanism based on the RL-based multi-directional guidance strategy. First, the space around the particle (e.g., particle *a*) is searched by using a mutation operator to avoid the algorithm converging to local optimum. Then, the action (e.g., *p*) performed by particle *a* is obtained by the RL-based multi-directional guidance strategy, and the particle (*pbest*) corresponding to this action is crossover with particle *a* to get the offspring. This mechanism not only enables the direct application of the algorithm to ERPPS problem, but also broadens the tendency of particles to move in more desirable directions, consequently elevating the likelihood of particles converging towards the optimal solution. Based on this, two mutation operations (swap operator and random operator) and a crossover operation (job-based operator) are employed in this study. The specific descriptions of the operators are as follows：

a) Swap operator

The swap operator, which does not involve the RP column, it means to choose two points at random in particle *a* and swap all the values corresponding to them. An illustrative example of the swap operator is shown in Fig. 6.

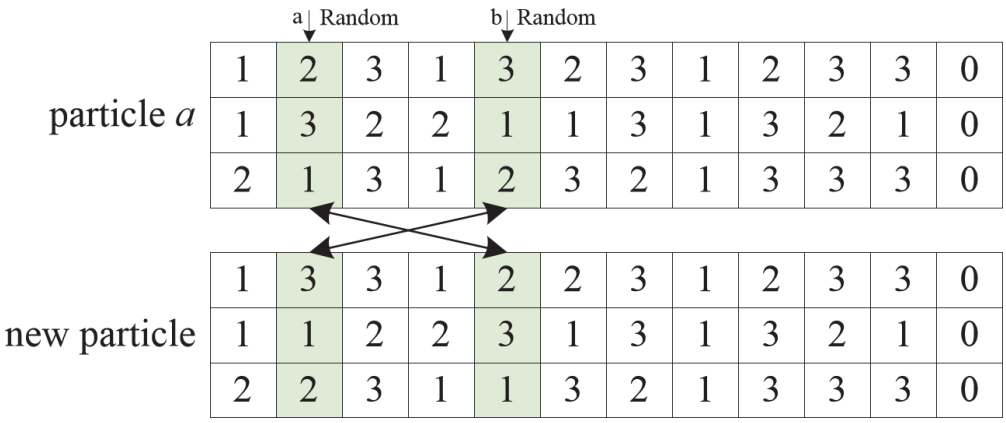


Fig. 6. An illustrative example of swap operator.

b) Random operator

The random operator consists of three components, as depicted in Fig. 7. First, a point is randomly selected within the RP column. If the generated random number is less than the process planning mutation rate λ , a replacement is randomly chosen from the alternative process plans for the product (i.e. the process plan for P_1 has changed from 2 to 1.). For the OS column, two points are randomly selected, and the values corresponding to these points are exchanged. In the case of the MA and MS columns, two points are first randomly selected. If an alternative machine exists for the operation corresponding to the MA column between these two points, one alternative machine is randomly chosen and assigned a random processing speed.

particle *a*

2	2	1									
1	2	3	1	3	2	3	1	2	3	3	0
1	3	2	2	1	1	3	1	3	2	1	0
2	1	3	1	2	3	2	1	3	3	3	0

new particle

1	2	1									
1	2	2	1	3	3	3	1	2	3	3	0
1	3	2	2	1	1	2	2	1	2	1	0
2	1	3	1	2	3	1	2	2	3	3	0

Fig. 7. An illustrative example of random operator.

b) Job-based operator

Fig. 8 shows an illustrative example of a job-based (JBX) operator. Initially, the set of product numbers {1, 2, ..., n} is partitioned into two subsets at random, PS_1 and PS_2. Subsequently, the elements corresponding to PS_1 in particle$_1$ (highlighted in green) are copied to offspring$_1$, while the elements corresponding to PS_2 in particle$_2$ (highlighted in yellow) are copied to offspring$_2$, with their positions maintained. Similarly, the elements corresponding to PS_2 in particle$_1$ are copied to offspring$_1$, and the elements corresponding to PS_1 in particle$_2$ are copied to offspring$_2$, with their order preserved.

PS_1={2}
PS_2={1, 3}

P_1

2	2	1									
1	2	3	1	3	2	3	1	2	3	3	0
1	3	2	2	1	1	3	1	3	2	1	0
2	1	3	1	2	3	2	1	3	3	3	0

P_2

1	3	2									
2	1	2	1	3	1	2	3	2	3	0	0
2	3	1	1	2	2	3	1	3	1	0	0
1	2	3	2	3	3	2	2	3	3	0	0

O_1

1	2	2									
1	2	1	3	1	2	3	3	2	0	0	0
3	3	1	2	2	1	1	1	3	0	0	0
2	1	2	3	3	3	2	3	3	0	0	0

O_2

1	2	2									
2	1	2	1	3	1	2	3	0	3	0	0
3	3	1	1	2	2	3	1	0	1	0	0
1	2	3	2	3	3	3	2	0	3	0	0

Fig. 8. An illustrative example of JBX operator.

4.4 Local search strategy

For the purpose of overcoming the defects of PSO algorithm with weak local search ability and insufficient search accuracy. Three local search operators are designed that depend on the characteristics of the proposed ERPPS model, which are the insertion operator, shift operator and speed adjustment operator. The insertion operator means that select two random points in a particle, then insert the elements contained in the former point in front of the latter. The shift operator

involves randomly selecting two points in a particle and the element contained in the last point is shifted to the first position, and the elements in the remaining positions are sorted sequentially. And the speed adjustment operator refers to randomly adjusting the machine processing speed vector between two randomly selected points in a particle. Fig. 9 shows an illustrative example of three local search operators.

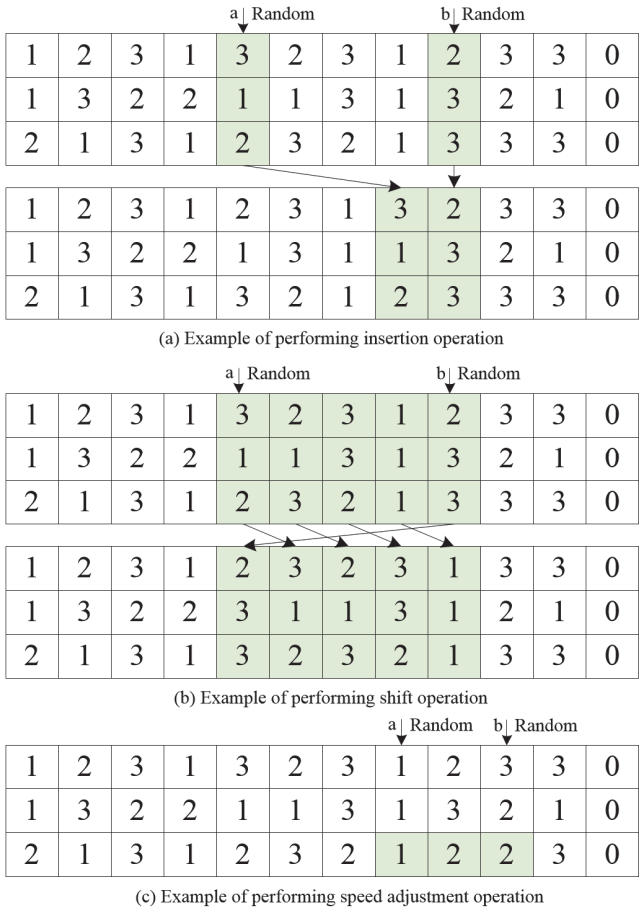


Fig 9. An illustrative example of three local search operators.

4.5 Restart mechanism

Finally, this study applied a restart mechanism to prevent the RL-PSO algorithm from converging prematurely. If the optimal solution does not improve after iterating for i*0.1 generations, 10% of the population will be generated randomly.

5. Experiment

The performance of the RL-PSO algorithm is evaluated by conducting a series of simulation experiments in this section. All simulation experiments were programmed by the Python language on a personal computer featuring 10 64-bits, an Intel® Core™ i5-13400F processor CPU, 16 GB of RAM, and an NVDIA GeForce RTX 3060 GPU.

In the series of simulation experiments, the performance of the proposed algorithm in solving the ERPPS model is evaluated by comparing the RL-PSO algorithm with four other metaheuristic algorithms including hybrid discrete PSO algorithm (HDPSO, Behnamian 2014), extended discrete PSO algorithm (EDPSO, Shi et al. 2021), self-learning genetic algorithm (SLGA, Chen et al. 2020) and hybrid genetic algorithm (HGA, Wang et al. 2023).

5.1 Experimental design

This study extends the simulation instances of Shi et al. (2021) to simulate a realistic remanufacturing scenario through randomly generating multiple sets of instances with different sizes. The number of products, number of operations and number of machines for each instance were randomly generated in the intervals 7-70, 6-30 and 5-23, respectively. Details of all instances are publicly available from the Figshare database (https://doi.org/10.6084/m9.figshare.25460503.v1), and instance takes its name from the number of products, operations and machines. Ins(35/20/10) indicates that the number of product types is 35, the number of operations is 20, and the number of machines is 10. In addition, to ensure the fairness and stability of the experiments, all experiments are conducted 10 times independently, and the results are the average of the 10 experiments.

5.2 Parameter design

Since the parameter settings of Q-learning and the process planning mutation rate will directly affect the obtained solutions. The algorithm proposed in this study involves the following four parameters the learning rate α, the discount rate γ, the greed factor ε, and the process planning mutation rate λ. Therefore, the first experiment was designed to investigate the effect of the above parameters on the performance of the RL-PSO algorithm by performing orthogonal experiments based on the Taguchi method in medium-sized Ins(35/20/10). The levels of the four parameters are shown in Table 1. The maximum number of iterations of the algorithm was set to 1000, and the population size was set to 50. The coefficient weights of the objective function were set to $w_t = 0.5$ and $w_r = 0.5$ for the ERPPS model, respectively. To obtain the optimal parameter combinations, an orthogonal array P16 (i.e., the experiment involves 16 parameter combinations) and the fitness values for each combination are shown in Table 2. The average fitness value for each parameter level in Table 2 was calculated and the trend of each parameter level was obtained as shown in Fig. 10. The figure clearly indicates that best average fitness values were attained for each parameter at specific levels. Specifically, α performed best at level 1, γ at level 2, ε and λ at level 3.

Therefore, the parameters for the RL-PSO algorithm as follows: α = 0.35, γ = 0.55, ε = 0.75, and λ = 0.75 to efficiently address the proposed model in subsequent experiments.

Table 1 Levels of four parameters for the RL-PSO algorithm

parameter	level			
	1	2	3	4
α	0.35	0.55	0.75	0.95
γ	0.35	0.55	0.75	0.95
ε	0.35	0.55	0.75	0.95
λ	0.35	0.55	0.75	0.95

Table 2 Orthogonal array and fitness value

Combination of parameters	parameter level				Fitness value
	α	γ	ε	λ	
P01	1	1	1	1	0.884220
P02	1	2	2	2	0.885020
P03	1	3	3	3	0.885930
P04	1	4	4	4	0.882381
P05	2	1	2	3	0.883538
P06	2	2	1	4	0.883541
P07	2	3	4	1	0.884839
P08	2	4	3	2	0.883178
P09	3	1	3	4	0.883814
P10	3	2	4	3	0.886123
P11	3	3	1	2	0.883534
P12	3	4	2	1	0.883587
P13	4	1	4	2	0.882984
P14	4	2	3	1	0.885391
P15	4	3	2	4	0.884252
P16	4	4	1	3	0.884052

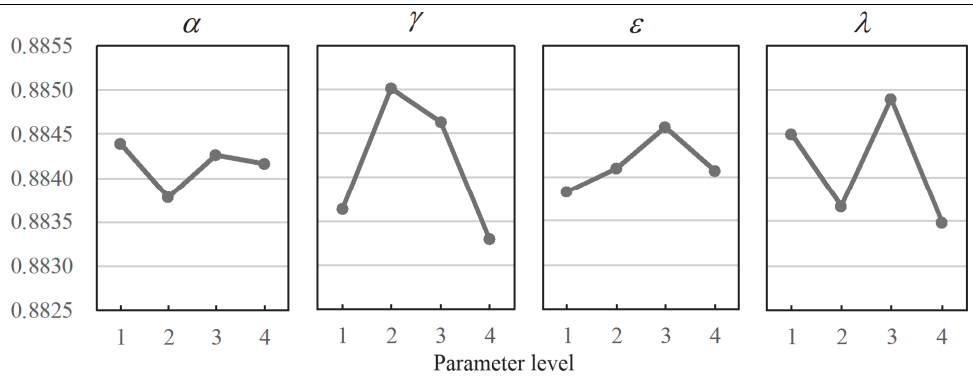


Fig. 10. Trend of each parameter level in the RL-PSO algorithm.

Subsequently, experiments were conducted on Ins(35/20/10) to analyze the iteration count of the algorithms, yielding the reasonable iteration count for all algorithms. The maximum number of iterations and population size for each algorithm was set to 1200 and 50, respectively. Fig. 11 shows the evolution trajectory of all algorithms. It is shown that the convergence of the RL-PSO and SLGA algorithms occurs at approximately 700 generations, the HDPSO algorithm tends to converge around 800 generations. However, the EDPSO and HGA algorithms require approximately 1000 iterations to reach convergence. Furthermore, it is worth noting that the proposed algorithm achieves superior fitness values despite fewer iterations, e.g., the obtained results after 100 iterations are even better than the rest of the baseline algorithms with 1200 iterations. For example, the results RL-PSO algorithm obtained after 100 iterations are even better than the rest of the baseline algorithms with 1200 iterations. This demonstrates that RL-PSO has a strong local search capability and is superior to other baseline algorithms in solving this model. Therefore, to ensure the fairness of the following experiments, the number of iterations for all the algorithms in this study is set to 1000.

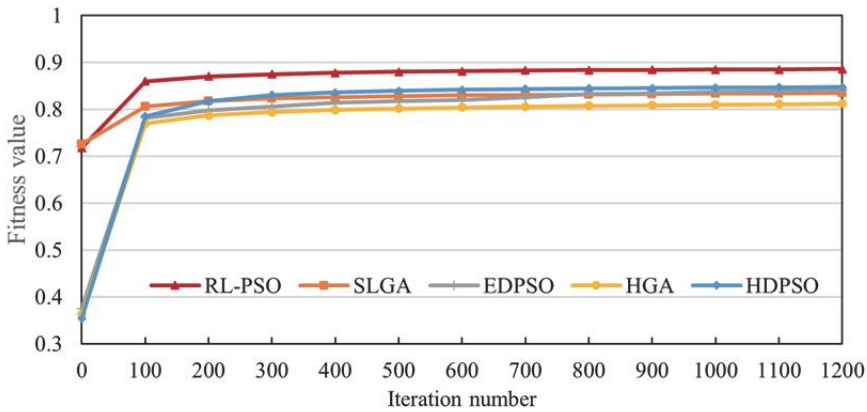


Fig. 11. Evolutionary trajectory of all algorithms.

The following experiment aims to compare the effectiveness of five algorithms on Ins(35/20/10) with different population sizes (15-55) to determine a reasonable population size. It is evident from Fig. 12 that the fitness values achieved by the RL-PSO algorithm are always better than the other algorithms, regardless of the variation of population size, which indicates that the algorithmic performance of the RL-PSO is better than the other baseline algorithms. Moreover, it is evident that the trend of the fitness value for the RL-PSO algorithm remained relatively stable as the population size varied. The fitness values obtained by the HGA and SLGA algorithms improve as the population size increases, and tend to remain stable after the population size reaches 50. In contrast, the performance of the HDPSO and EDPSO algorithms improves with increasing population size, but cannot become stable. Therefore, the initial population size is set to 50 for all

algorithms to ensure fair and efficient comparisons in subsequent experiments, and to keep the computation time within reasonable bounds.

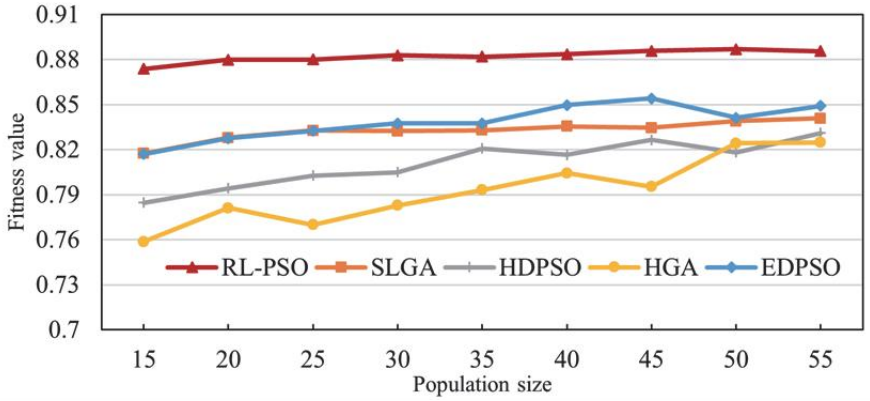


Fig. 12. Comparative experiments by increasing population size from 15 to 55.

5.3 Performance comparison of RL-PSO algorithm

The weight coefficient setting of the objective function has a direct impact on the algorithm effectiveness evaluation. Hence, to evaluate the effectiveness of the RL-PSO algorithm more effectively, this study conducts comparison experiments with other baseline algorithms on 18 instances with varying weight combinations. The comparative results are presented in Table 3-8

Tables 3, 4 and 5 detail the best and average fitness values obtained by all algorithms for different weight combinations, represented as “best” and “mean”, respectively. Table 3 shows that the best and average fitness values obtained by the proposed RL-PSO algorithm are superior to the other baseline algorithms. In addition, most of the best and average fitness values obtained by this algorithm for two different weight combinations in Tables 4 and 5 are also better than the comparison algorithms. It indicates that the proposed algorithm performs better than baseline algorithms in solving the ERPPS model regardless of the combination of weight coefficient.

Table 3 The best and the average fitness value obtained by all algorithms

(weight combination 1: $w_t = 0.3$, $w_c = 0.7$)

Instance	HDPSO		EDPSO		SLGA		HGA		RL-PSO	
	Mean	Best	Mean	Best	Mean	Best	Mean	Best	Mean	Best
Ins(8/8/3)	0.830375	0.839387	0.830064	0.844411	0.742978	0.755254	0.823547	0.837220	**0.842035**	**0.844987**
Ins(9/9/5)	0.763592	0.779570	0.775013	0.783670	0.717208	0.741405	0.757919	0.774158	**0.782101**	**0.785707**
Ins(10/11/4)	0.828495	0.858113	0.851183	0.876173	0.843643	0.852728	0.812987	0.842966	**0.871538**	**0.872562**
Ins(12/9/3)	0.823883	0.841413	0.849584	0.865305	0.785972	0.804507	0.817017	0.827614	**0.871698**	**0.873192**
Ins(16/15/	0.8386	0.8523	0.8367	0.8521	0.8186	0.8296	0.8384	0.8612	**0.8633**	**0.8680**

7)	12	26	14	13	63	45	32	95	**44**	**57**
Ins(20/14/6)	0.826737	0.842281	0.818271	0.830718	0.793642	0.801979	0.823999	0.836941	**0.842687**	**0.859815**
Ins(21/23/10)	0.798424	0.829012	0.789700	0.821323	0.785761	0.804859	0.782774	0.808063	**0.841827**	**0.854528**
Ins(23/19/8)	0.848284	0.863157	0.831718	0.851780	0.855870	0.865291	0.851306	0.873340	**0.879909**	**0.884123**
Ins(25/24/11)	0.797043	0.807669	0.781571	0.807705	0.799999	0.812039	0.796766	0.828164	**0.831366**	**0.841354**
Ins(30/18/6)	0.835288	0.844197	0.818472	0.827748	0.822610	0.829570	0.837749	0.851123	**0.865098**	**0.870147**
Ins(33/17/9)	0.858343	0.872619	0.833355	0.860888	0.861578	0.869324	0.854706	0.869029	**0.882275**	**0.892195**
Ins(35/20/10)	0.808396	0.839423	0.772267	0.791162	0.792501	0.803421	0.756243	0.803990	**0.855001**	**0.858166**
Ins(41/22/13)	0.771439	0.790541	0.758941	0.785146	0.774613	0.787619	0.766071	0.817466	**0.814481**	**0.820249**
Ins(46/10/3)	0.791684	0.803148	0.778457	0.790641	0.768781	0.773324	0.773745	0.790273	**0.829709**	**0.837571**
Ins(49/23/11)	0.807251	0.820453	0.802897	0.820486	0.794815	0.808149	0.801034	0.822269	**0.840733**	**0.852011**
Ins(52/17/5)	0.772607	0.786276	0.756920	0.776638	0.791798	0.799819	0.759705	0.781545	**0.817963**	**0.825888**
Ins(58/21/7)	0.746094	0.756771	0.737537	0.753773	0.747983	0.760732	0.739160	0.754470	**0.783976**	**0.791670**
Ins(70/19/6)	0.780407	0.793118	0.780008	0.800174	0.797199	0.803259	0.781862	0.800208	**0.837743**	**0.847262**

Note: The black mark indicates the optimal result

Table 4 The best and the average fitness value obtained by all algorithms (weight combination 2: $w_t = 0.5$, $w_c = 0.5$)

Instance	HDPSO		EDPSO		SLGA		HGA		RL-PSO	
	Mean	Best	Mean	Best	Mean	Best	Mean	Best	Mean	Best
Ins(8/8/3)	0.826001	0.836873	0.834745	0.839254	0.750375	0.760030	0.817810	0.835771	**0.838509**	**0.841034**
Ins(9/9/5)	0.785405	0.807385	0.793238	0.807811	0.750031	0.767070	0.783572	0.804666	**0.802718**	**0.808298**
Ins(10/11/4)	0.854793	0.881005	0.870131	**0.894270**	0.863783	0.875439	0.838972	0.883021	**0.892435**	0.892602
Ins(12/9/3)	0.829982	0.856355	0.855559	0.873142	0.789417	0.810101	0.827607	0.853996	**0.872528**	**0.879842**
Ins(16/15/7)	0.840753	0.856860	0.835806	0.849296	0.818401	0.822565	0.844955	0.854813	**0.865221**	**0.870577**
Ins(20/14/6)	0.823369	0.840661	0.816580	0.834584	0.809594	0.819410	0.833909	0.849588	**0.845000**	**0.853807**
Ins(21/23/10)	0.795311	0.809749	0.777106	0.806344	0.793589	0.808230	0.797017	0.814006	**0.835917**	**0.852397**
Ins(23/19/8)	0.846595	0.862725	0.833547	0.859478	0.857329	0.865281	0.831967	0.859010	**0.882920**	**0.888312**
Ins(25/24/11)	0.808021	0.827701	0.794448	0.816499	0.815172	0.822877	0.806176	0.819020	**0.849880**	**0.857699**
Ins(30/18/6)	0.826662	0.837978	0.826344	0.846719	0.815045	0.826029	0.833221	0.844975	**0.858257**	**0.866531**

Ins(33/17/9)	0.847742	0.859894	0.827082	0.841968	0.860607	0.871154	0.835849	0.851156	**0.879938**	**0.889878**
Ins(35/20/10)	0.841073	0.854299	0.818207	0.847025	0.838956	0.845235	0.824126	0.855494	**0.886783**	**0.888584**
Ins(41/22/13)	0.765689	0.794884	0.741551	0.770394	0.766322	0.777712	0.764762	0.796937	**0.809796**	**0.826837**
Ins(46/10/3)	0.767114	0.774637	0.758291	0.781336	0.765199	0.774963	0.757976	0.771267	**0.820971**	**0.825695**
Ins(49/23/11)	0.805939	0.828612	0.794530	0.820605	0.796036	0.807337	0.794550	0.826325	**0.838723**	**0.848476**
Ins(52/17/5)	0.769083	0.780435	0.750466	0.763842	0.794656	0.800670	0.758283	0.772725	**0.819450**	**0.824716**
Ins(58/21/7)	0.748541	0.766910	0.729795	0.758760	0.759698	0.772066	0.736212	0.765861	**0.790850**	**0.799982**
Ins(70/19/6)	0.767693	0.780251	0.760074	0.776115	0.782615	0.788460	0.770145	0.783523	**0.823744**	**0.830303**

Note: The black mark indicates the optimal result

Table 5 The best and the average fitness value obtained by all algorithms

(weight combination 3: $w_t = 0.7$, $w_c = 0.3$)

Instance	HDPSO		EDPSO		SLGA		HGA		RL-PSO	
	Mean	Best	Mean	Best	Mean	Best	Mean	Best	Mean	Best
Ins(8/8/3)	0.828852	0.842408	**0.840846**	**0.845445**	0.766475	0.776203	0.821131	0.844628	0.840273	**0.845445**
Ins(9/9/5)	0.811163	0.823993	0.819605	0.833302	0.788543	0.807696	0.809211	0.829799	**0.833281**	**0.835087**
Ins(10/11/4)	0.880996	0.903956	0.904777	0.918027	0.894984	0.901494	0.883895	0.909301	**0.915910**	**0.920023**
Ins(12/9/3)	0.846436	0.868145	0.867221	0.881867	0.801566	0.811207	0.838272	0.874535	**0.884917**	**0.893905**
Ins(16/15/7)	0.839178	0.853387	0.831413	0.838554	0.813073	0.824188	0.841245	0.863527	**0.864468**	**0.871883**
Ins(20/14/6)	0.852701	0.862629	0.827799	0.850000	0.826310	0.833004	0.847236	0.860928	**0.861576**	**0.866005**
Ins(21/23/10)	0.816865	0.830068	0.791845	0.818860	0.806959	0.817869	0.805008	0.830436	**0.845754**	**0.856605**
Ins(23/19/8)	0.853473	0.868618	0.836556	0.847638	0.865680	0.875472	0.846803	0.874894	**0.889135**	**0.892996**
Ins(25/24/11)	0.825377	0.835952	0.819850	0.834636	0.832103	0.840686	0.817195	0.851012	**0.863650**	**0.869029**
Ins(30/18/6)	0.825732	0.847668	0.810143	0.822408	0.808795	0.827005	0.822867	0.832856	**0.859725**	**0.867489**
Ins(33/17/9)	0.845645	0.853828	0.825607	0.842885	0.858681	0.869753	0.826234	0.841810	**0.882270**	**0.888075**
Ins(35/20/10)	0.886487	0.902845	0.867355	0.890964	0.881019	0.883248	0.858018	0.883248	**0.916230**	**0.920145**
Ins(41/22/13)	0.780119	0.804564	0.764209	0.786461	0.758748	0.769544	0.758348	0.795781	**0.821110**	**0.829654**
Ins(46/10/3)	0.760579	0.769692	0.733226	0.747696	0.769186	0.774923	0.747557	0.766330	**0.819599**	**0.825154**
Ins(49/23/11)	0.815596	0.835054	0.808665	0.830912	0.795856	0.805088	0.803794	0.833176	**0.853728**	**0.858800**
Ins(52/17/5)	0.759896	0.773407	0.746565	0.763267	0.800232	0.805370	0.755774	0.773079	**0.827168**	**0.834486**

Ins(58/21/7)	0.753830	0.763748	0.746324	0.757403	0.770000	0.778535	0.733562	0.756635	**0.805921**	**0.810947**
Ins(70/19/6)	0.751675	0.764599	0.746530	0.767521	0.771473	0.776500	0.742521	0.768535	**0.817858**	**0.823288**

Note: The black mark indicates the optimal resultConclusion

To achieve the economic and environmental benefits of remanufacturing effectively, this study investigates a new ERPPS problem and develops its mathematical model. This model not only solved the remanufacturing process planning and scheduling problem collaboratively, but also employed machine speed-switching strategy to reduce energy waste. A new RL-PSO algorithm embedded with five improvements was proposed to solve the ERPPS model. In this algorithm, a novel RL-based multi-directional guide position-updating mechanism was proposed to maintain population diversity and effectively balance the capabilities of the algorithm in exploitation and exploration. For the purpose of validating the effectiveness of RL-PSO in addressing the ERPPS model, experimental evaluations were conducted, comparing its performance against four baseline algorithms. The simulation experiments demonstrate that the RL-PSO algorithm outperforms other baseline algorithms in terms of faster convergence, enhanced search capability, and superior stability. When solving the ERPPS model, it attains solutions of superior quality.

In the future work, digital twin technology and dynamic scheduling can be integrated into the ERPPS model to solve the remanufacturing process planning and scheduling problem more effectively and collaboratively.\

References

[1] Agrawal, P., & Rao, S. (2014). Energy-aware scheduling of distributed systems. *IEEE Transactions on Automation Science and Engineering*, 11(4), 1163-1175.

[2] Anonymous Authors (for blind review purpose) (2019). Environmental life cycle assessment of remanufactured engines with advanced restoring technologies. *Robotics and Computer-Integrated Manufacturing*, 59, 213-221.

[3] Anonymous Authors (for blind review purpose) (2022). Linguistic information-based granular computing based on a tournament selection operator-guided PSO for supporting multi-attribute group decision-making with distributed linguistic preference relations. *Information Sciences*, 610, 488-507.

[4] Behnamian, J. (2014). Particle swarm optimization-based algorithm for fuzzy parallel machine scheduling. *The International Journal of Advanced Manufacturing Technology*, 75(5-8), 883-895.

[5] Chen, R. H., Yang, B., Li, S., & Wang, S. L. (2020). A self-learning genetic algorithm based on reinforcement learning for flexible job-shop scheduling problem. *Computers & Industrial Engineering*, 149, 106778.

[6] Chen, Y. X., Jiang, Z. G., Zhang, H., & Yan, W. (2021). Integrated design of process-tolerance for remanufacturing based on failure feature. *Applied Sciences*, 11(14), 6377.

[7] Daniel, V., & Guide Jr, R. (1997). Scheduling with priority dispatching rules and drum-buffer-rope in a recoverable manufacturing system. *International Journal of Production Economics*, 53(1), 101-116.

[8] Du, Y. B., & Li, C. B. (2014). Implementing energy-saving and environmental-benign paradigm: machine tool remanufacturing by OEMs in China. J*ournal of Cleaner Production*, 66, 272-279.

[9] Durgut, R., Aydin, M. E., & Atli, I. (2021). Adaptive operator selection with reinforcement learning. *Information Sciences*, 581, 773-790.

[10] Fu, Y. P., Zhou, M. C., Guo, X. W., & Qi, L. (2021). Stochastic multi-objective integrated disassembly-reprocessing-reassembly scheduling via fruit fly optimization algorithm. *Journal of Cleaner Production*, 278, 123364.

[11] Gao, K. Z., Suganthan, P. N., Pan, Q. K., Tasgetiren, M. F., & Sadollah, A. (2016). Artificial bee colony algorithm for scheduling and rescheduling fuzzy flexible job shop problem with new job insertion. *Knowledge-Based Systems*, 109, 1-16.

[12] Giglio, D., Paolucci, M., & Roshani, A. (2017). Integrated lot sizing and energy-efficient job shop scheduling problem in manufacturing/remanufacturing systems. *Journal of Cleaner Production,* 148, 624-641.

[13] Gong, G. L., Deng, Q. W., Chiong, R. M., Gong, X. R., Huang, H. Z. Y., & Han, W. W. (2020). Remanufacturing-oriented process planning and scheduling: mathematical modelling and evolutionary optimisation. *International Journal of Production Research*, 58(12), 3781-3799.

[14] Guide Jr, R. (2000). Production planning and control for remanufacturing: industry practice and research needs. *Journal of operations Management*, 18(4), 467-483.

[15] Jeon, H. B., Kim, J. G., Kim, H. J., & Lee, D. H. (2006). A two-stage heuristic for disassembly scheduling with capacity constraints. *Management Science and Financial Engineering*, 12(1), 95-112.

[16] Jin, Q. Y., Zhang, S., Xu, J. Y., Jiang, K., Cheng, Y. Z., & Zhang, W. Y. (2024). Remanufacturing system scheduling of batch products with the consideration of dynamic changes in machine efficiency using an improved artificial bee colony algorithm. *Computers & Industrial Engineering*, 187, 109817.

[17] Kennedy, J., & Eberhart, R. (1995). Particle swarm optimization. In *Proceedings of IEEE International Conference on Neural Network*, Perth, Australia, November 27-December 1, pp. 1942-1948.

[18] Kim, M. G., Yu, J. M., & Lee, D. H. (2015). Scheduling algorithms for remanufacturing systems with parallel flow-shop-type reprocessing lines. *International Journal of Production Research*, 53(6), 1819-1831.

[19] Kimita, K., Matschewsky, J., & Sakao, T. (2021). A method for remanufacturing process planning and control using loosely coupled systems. *Journal of Manufacturing Science and Engineering*, 143(10), 101001.

[20] Li, X. Y., Gao, L., Pan, Q. K., Wan, L., & Chao, K. M. (2018). An effective hybrid genetic algorithm and variable neighborhood search for integrated process planning and scheduling in a packaging machine workshop. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(10), 1933-1945.

[21] Li, Z. H., Shi, L., Yue, C. T., Shang, Z. G., & Qu, B. Y. (2019). Differential evolution based on reinforcement learning with fitness ranking for solving multimodal multiobjective problems. *Swarm and Evolutionary Computation*, 49, 234-244.

[22] Lin, C. S., Li, P. Y., Wei, J. M., & Wu, M. C. (2020). Integration of process planning and scheduling for distributed flexible job shops. *Computers & Operations Research*, 124, 105053.

[23] Lv, Y., Li, C. B., Zhao, X. K., Li, L. L., & Li, J. (2021). A novel approach for remanufacturing process planning considering uncertain and fuzzy information. *Frontiers of Mechanical Engineering*, 16(3), 546-558.

[24] Mouzon, G., Yildirim, M. B., & Twomey, J. (2007). Operational methods for minimization of energy consumption of manufacturing equipment. *International Journal of Production Research*, 45(18-19), 4247-4271.

[25] Peng, S. T., Li, T., Zhao, J. L., Guo, Y. C., Lv, S. P., Tan, G. Z., & Zhang, H. C. (2019). Petri net-based scheduling strategy and energy modeling for the cylinder block remanufacturing under uncertainty. *Robotics and Computer-Integrated Manufacturing*, 58, 208-219.

[26] Roshani, A., Paolucci, M., Giglio, D., Demartini, M., Tonelli, F., & Dulebenets, M. A. (2022). The capacitated lot-sizing and energy efficient single machine scheduling problem with sequence dependent setup times and costs in a closed-loop supply chain network. *Annals of Operations Research*, 321(1-2), 469-505.

[27] Shi, J. X., Zhang, W. Y., Zhang, S., & Chen, J. (2021). A new bifuzzy optimization method for remanufacturing scheduling using extended discrete particle swarm optimization algorithm. *Computers & Industrial Engineering*, 156, 107219.

[28] Shi, J. X., Zhang, W. Y., Zhang, S., Wang, W., Lin, J., & Feng, R. J. (2020). A new environment-aware scheduling method for remanufacturing system with non-dedicated reprocessing lines using improved flower pollination algorithm. *Journal of Manufacturing Systems*, 57, 94-108.

[29] Tian, D. P., & Shi, Z. Z. (2018). MPSO: Modified particle swarm optimization and its applications. *Swarm and Evolutionary Computation*, 41, 49-68.

[30] Van, T. L., Paris, H. R., & Mandil, G. (2017). Process planning for combined additive and subtractive manufacturing technologies in a remanufacturing context. *Journal of Manufacturing Systems*, 44, 243-254.

[31] Wang, B. T., Pan, Q. K., Gao, L., Miao, Z. H., & Sang, H. Y. (2024). Modeling and Scheduling a Constrained Flowshop in Distributed Manufacturing Environments. *Journal of Manufacturing Systems*, 72, 519-535.

[32] Wang, H., Jiang, Z. G., Zhang, X. G., Wang, Y. N., & Wang, Y. (2017). A fault feature characterization based method for remanufacturing process planning optimization. *Journal of Cleaner Production*, 161, 708-719.

[33] Wang, J. J., & Wang, L. (2021). A cooperative memetic algorithm with learning-based agent for energy-aware distributed hybrid flow-shop scheduling. *IEEE Transactions on Evolutionary Computation*, 26(3), 461-475.

[34] Wang, W. J., Tian, G. D., Zhang, H. H., Li, Z. W., & Zhang, L. L. (2023). A hybrid genetic algorithm with multiple decoding methods for energy-aware remanufacturing system scheduling problem. R*obotics and Computer-Integrated Manufacturing*, 81, 102509.

[35] Watkins, C. J., & Dayan, P. (1992). Q-learning. *Machine learning*, 8, 279-292.

[36] Yu, J. M., & Lee, D. H. (2018). Scheduling algorithms for job-shop-type remanufacturing systems with component matching requirement. *Computers & Industrial Engineering*, 120, 266-278.

[37] Zeng, L., Benatallah, B., Ngu, A. H., Dumas, M., Kalagnanam, J., & Chang, H. (2004). QoS-aware middleware for web services composition. *IEEE Transactions on software engineering*, 30(5), 311-327.

[38] Zhang, R., Ong, S. K., & Nee, A. Y. (2015). A simulation-based genetic algorithm approach for remanufacturing process planning and scheduling. *Applied Soft Computing*, 37, 521-532.

[39] Zhang, W. K., Zheng, Y. F., & Ahmad, R. (2023a). The integrated process planning and scheduling of flexible job-shop-type remanufacturing systems using improved artificial bee colony algorithm. *Journal of Intelligent Manufacturing*, 34(7), 2963-2988

[40] Zhang, W. Y., Wang, J., Liu, X. Q., & Zhang, S. (2023b). A new uncertain remanufacturing scheduling model with rework risk using hybrid optimization algorithm. *Environmental Science and Pollution Research*, 30(22), 62744-62761.

[41] Zhou, L., Naim, M. M., Tang, O., & Towill, D. R. (2006). Dynamic performance of a hybrid inventory system with a Kanban policy in remanufacturing process. *Omega*, 34(6), 585-598.

绿色集成炼钢炉次计划研究

王敬博[1]，　王庚辰，　王庆，　黄敏*

东北大学 信息科学与工程学院，辽宁 沈阳 110004

摘　要：钢铁行业的集成批量计划对促进钢铁工序间协同，最大化企业收益起到重要作用。本文从炼钢炉次计划问题入手，考虑柔性板坯，着眼于废钢的重新利用，针对炼钢、连铸、热轧集成工艺约束和碳排放问题，致力于在考虑绿色、柔性和集成约束背景下建立一个有效且合理的炉次编制多目标优化模型。鉴于问题的 NP-hard 特性设计了嵌入局部搜索算子的基于分解的多目标进化算法，并根据柔性板坯的特点，设计了基于板坯宽度交集的初始解生成策略。为了验证模型和算法的性能，以国内某钢厂的订单列表为数据源，随机抽取了含有 60 块板坯的某天板坯批量数据作为研究案例，验证了模型和算法的有效性。

关键词：炼钢炉次计划；柔性；集成；碳排放；MOEA/D

Research on the green integrated charge planning of steel making process

*WANG Jing-bo，WANG Geng-chen，WANG Qing，HUANG Min**

College of Information Science and Engineering, Northeastern University, Shenyang 110004, China

Abstract: Integrated batch planning in the steel industry plays an important role in promoting synergies between steel processes and maximizing corporate profitability. In this paper, starting from the steelmaking charge planning problem, considering flexible slabs, focusing on the reuse of scrap, and targeting the integrated process constraints of steelmaking, continuous casting, and hot rolling as well as the carbon emission problem, we are committed to establishing an effective and reasonable multi-objective optimization model of charge preparation under the background of considering the green, flexible, and integrated constraints. A decomposition-based multi-objective evolutionary algorithm embedded with a local search operator is designed in view of the NP-hard nature of the problem, and an initial solution generation strategy based on the intersection of slab widths is designed according to the characteristics of flexible slabs. In order to verify the performance of the model and the algorithm, the order list of a domestic steel mill is used as the data source, and the batch data of slabs containing 60 slabs on a certain day is randomly selected as a study case, and the validity of the model and the algorithm was verified.

Key words: Steelmaking charge planning; Flexible; Integrated; Carbon emissions; MOEA/D

1　引言

钢铁企业的计划调度问题，由于其复杂性和多变性，被认为是工业计划调度领域中极具挑战性的一类

基金项目：国家自然科学基金重大研究计划重点支持项目(92267206)；国家自然科学基金重点项目(62032013)；辽宁省“兴辽英才计划” (XLYC2202045).

作者简介：王敬博（2002-），男，硕士生，从事智能制造、智能算法等研究，E-mail：20205540@stu.neu.edu.cn；王庚辰（2000-），男，博士生，从事智能制造、鲁棒优化等相关研究，E-mail：2310322@stu.neu.edu.cn；王庆（1969-），男，副教授，博士，从事系统建模与优化、供应链与 ERP 系统等研究，E-mail：qwang@mail.neu.edu.cn 黄敏（1968-），女，教授，博士生导师，从事物流与供应链管理、智能算法设计与优化、调度理论与方法等研究，E-mail：mhuang@mail.neu.edu.cn

优化问题。炼钢工序作为钢铁冶炼流程工艺的一环，集成批量计划能够综合考虑炼钢、连铸、热轧（如图1）的生产目标和工艺约束，优化资源配置，提高生产效率，降低成本，增强企业的市场竞争力。柔性制造在制造业中展现出显著的优势[1]，而柔性板坯的引入，可以为炼钢炉次计划带来更高的灵活性和应变能力。

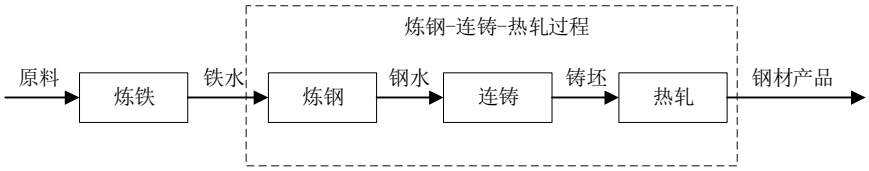


图 1 炼钢、连铸、热轧集成批量计划工艺流程图

作为全球经济体系中不可或缺的一环，钢铁行业是典型的高耗能、高排放产业。对于长流程转炉炼钢工艺，提高废钢比、降低铁水比可实施性较高，将是未来一段时间内长流程炼钢工艺降低碳排放的重要措施之一[2]。

从过往研究来看，炼钢调度问题可分为集成炼钢工艺生产计划问题、柔性炼钢工艺生产计划问题和绿色炼钢工艺生产计划问题。在集成炼钢工艺生产计划问题和柔性炼钢工艺生产计划问题的研究中，大多数研究未考虑绿色因素。而在绿色集成炼钢炉次计划的相关研究大多集中在调度层面、很少有在规划层面对绿色因素进行考虑。在废钢资源再利用的相关研究，未有研究将废钢利用与炉次编制计划综合考虑。同时，大部分研究都是将炉次计划建立成单目标优化模型进行求解。区别于以往研究，本文在使用柔性板坯处理柔性订单的场景下，着眼于废钢再利用与炼钢工艺的集成工艺约束，建立了考虑集成工艺约束，柔性因素，绿色因素的多目标优化模型，针对优化模型设计了嵌入局部搜索算子的 MOEA/D(MOEA/D embedded in Local Search, LS-MOEA/D)求解模型。

2 绿色柔性集成炼钢炉次计划

2.1 问题描述

集成批量计划始于编制炉次计划，炉次计划是一个对板坯进行组批的过程。本文的绿色柔性集成炼钢炉次计划表现为在考虑集成工艺约束条件下，充分利用炉次的最大废钢比，对柔性板坯进行组批，以期达到在确保在炉次容量限制内，最小化每个炉次中板坯之间的属性差异、最大化炉次空间利用率、最小化碳排放量的目标，获得多组可供决策者选择的炉次编制方案。

2.2 集成工艺约束

集成工艺约束表现为炼钢、连铸、热轧各工序间的相互限制条件，本文主要体现在炉次计划的编制过程中对后续流程中工艺约束条件的充分考虑，具体为：

（1）同一炉次中，尽量确保所冶炼的板坯具有相同的钢级，或至少属于同一连续浇铸的组别代码。

（2）每个炉次有其容量上限，为提高生产效率，应尽可能装满炉次，若存在剩余容量，则使用无指定客户的板坯（即无委材）进行填充。

（3）同一炉次中的板坯厚度必须相同。

（4）每块板坯均存在有效的宽度范围。

（5）同一炉次中，所包含的板坯的宽度范围应存在重叠交集，且该交集范围越大越理想。（基于约束

（6）同一炉次中，所包含的板坯优先级尽量接近。

（7）同一炉次中，所包含的板坯的流向尽量相同。

其中（1）和（2）为炼钢约束，（3）和（5）为连铸约束，（4）为热轧约束，（6）为板坯库约束，（7）热轧工序后的其它工序约束。

2.3　基于废钢比的绿色刻画

对于长流程转炉炼钢工艺，提高废钢比、降低铁水比可实施性较高，将是未来一段时间内长流程降低碳排放的重要措施之一[2]。不同钢级钢种对应废钢比不同，而生产每一炉钢产生的碳排放量会随着这一炉次的废钢比的增加而降低，假设能组在同一炉次中板坯的钢级有 A 和 B 且钢级 A 优于钢级 B，则钢级 A 钢种质量更好，工艺要求高，钢级为 A 的炉次能容忍的废钢比低（假设为 10%），钢级为 B 的炉次能容忍的废钢比高（假设为 15%）。当炉次中同时有钢级为 A 和钢级为 B 的板坯时，由于同炉次中的钢水最终生产时仅能采用唯一的钢级，因此某一炉次采用的钢级不可低于任何一个所包含板坯的最低钢级要求，故炉次计划的编制采用以优冲次[3]的原则，炉次最终的钢级为 A，这会导致生产这一炉钢的能使用的最大废钢比低，而提高废钢比有利于降低炼钢过程中的碳排放。设碳排放系数为β，不同钢级炉次对应不同的最大废钢比，根据炉次钢级以优冲次的原则，在编制炉次方案时不同的板坯分配结果会产生不同的碳排放指标。

2.4　模型建立

2.4.1 问题假设

在转炉出钢量不变的条件下，废钢比提升的同时入炉铁水量需减少[2]，若加入废钢过多，入炉铁水量太少，炉温可能达不到工艺温度要求，影响钢产品的品质，为了使模型符合工艺要求对问题做出下列假设：

（1）每种钢级对应的最大废钢比已知。

（2）板坯组成炉次尽量组满，未组满部分使用无委托材料填充。

（3）所组炉次在炼钢过程中均使用最大废钢比进行炼钢。

（4）加入废钢后炼钢过程炉次中所含铁水温度可达到工艺温度要求。

2.4.2 板坯多维属性

相较于传统板坯，柔性板坯可以为炼钢炉次计划带来更高的灵活性，本文特别选择柔性板坯作为组合炉次的基本单位。柔性板坯的属性集包含多个维度，用于标识和描述板坯的特性。其中，i表示板坯的序号，取值范围为$i\epsilon\{1,\cdots n\}$。每个板坯的属性由以下部分组成：$S_i=[SG_i,\ C_i^{\text{code}},\ W_i^{\min},\ W_i^{\max},\ W_i^{\text{R}},\ T_i,\ WT_i^{\min},\ WT_i^{\max},\ AL_i,\ F_i]$，其中各个符号的含义如下：

(1)　SG_i：板坯i的钢级

(2)　C_i^{code}：板坯i的连铸标识

(3)　$W_i^{\min}$：板坯i的宽度下限

(4) $W_i^{\max}$：板坯i的宽度上限

(5) $WT_i^{\min}$：板坯i的重量下限

(6) $WT_i^{\max}$：板坯i的重量上限

(7) AL_i：板坯i的优先级（由板坯的交货期、客户优先级等因素决定）

(8) F_i：板坯i的流向代码（板坯轧制后目的地或用途的标识代码）

(9) T_i：板坯i的厚度

(10) W_i^{R}：板坯i的轧制宽度

2.4.3 模型符号说明

m表示炉次总数；n表示板坯总数；WT表示炉次容量；L表示钢级总数；α_l表示每种钢级在转炉炼钢时对应的最大废钢比$l=1,\cdots,L$；β代表炉次每使用 1%的废钢，生产每吨钢铁碳排放量降低系数；模型的决策变量为 0-1 变量x_{ik}，当$x_{ik}=1$时表示板坯i被指派到炉次k中，否则$x_{ik}=0$；模型的其它变量I_k表示炉次k中的板坯集合；wt_{ik}表示炉次k中板坯i的集合；F_{SG_k}表示炉次k的钢级（炉次中所含板坯的最优钢级）；c_{ik}表示炉次k中板坯i的惩罚即集成工艺约束惩罚，由钢级、宽度、流向和优先级四个惩罚项构成，具体定义如下：

$$c_{ik}=c_{ik}^{\mathrm{SG}}+c_{ik}^{\mathrm{W}}+c_{ik}^{\mathrm{F}}+c_{ik}^{\mathrm{PR}} \tag{1}$$

钢级惩罚项c_{ik}^{SG}定义如下：

$$c_{ik}^{\mathrm{SG}}=\begin{cases}0 & SG_i=SG_{\min\{i_k'\}}\\ \lambda^{\mathrm{SG}} & SG_i\text{与}SG_{\min\{i_k'\}}\text{属于同一钢级序列}\end{cases} \tag{2}$$

宽度惩罚项c_{ik}^{W}定义如下：

$$c_{ik}^{\mathrm{w}}=\begin{cases}\dfrac{\phi}{\sigma} & \sigma\geq 0\\ R & \sigma<0\end{cases} \tag{3}$$

$$w_{ik}^{\mathrm{up}}=\min\{w_i^{\max},w_i^{\mathrm{R}}+200\ \mathrm{mm},\min\left\{w_{i_k'}^{\max}\right\},\min\left\{w_{i_k'}^{\mathrm{R}}\right\}+200\ \mathrm{mm}\}$$

$$w_{ik}^{\mathrm{low}}=\max\{w_i^{\min},w_i^{\mathrm{R}},\min\left\{w_{i_k'}^{\min}\right\},\min\left\{w_{i_k'}^{\mathrm{R}}\right\}\}$$

$$\sigma=w_{ik}^{\mathrm{up}}-w_{ik}^{\mathrm{low}}$$

流向惩罚项c_{ik}^{F}定义如下：

$$c_{ik}^{\mathrm{F}}=\begin{cases}\lambda^{\mathrm{F}} & F_i\notin\left\{F_{i_k'}'\right\}\\ 0 & F_i\in\left\{F_{i_k'}'\right\}\end{cases} \tag{4}$$

优先级惩罚项c_{ik}^{PR}定义如下：

$$c_{ik}^{\mathrm{PR}}=\begin{cases}\lambda^{\mathrm{PR}} & \left|AL_i-\min\left\{AL_{i_k'}\right\}\right|\geq\delta^{\mathrm{PR}}\\ 0 & \left|AL_i-\min\left\{AL_{i_k'}\right\}\right|<\delta^{\mathrm{PR}}\end{cases} \tag{5}$$

引入第 k 个炉次未充分利用板坯的重量惩罚项C_k^{WT}，定义如下：

$$C_k^{\mathrm{WT}}=\begin{cases}\alpha\left(\sum_{i=1}^{n}WT_i^{\max}x_{ik}-WT\right)\sum_{i=1}^{n}WT_i^{\max}x_{ik}\geq WT\\ \frac{\alpha}{2}\left(WT-\sum_{i=1}^{n}WT_i^{\max}x_{ik}\right)\sum_{i=1}^{n}WT_i^{\max}x_{ik}<WT\end{cases}\tag{6}$$

2.4.4 绿色柔性集成炼钢炉次计划多目标优化模型

基于给定的模型参数和变量，构建模型：

$$\min\sum_{k=1}^{m}\sum_{i=1}^{n}c_{ik}x_{ik}\tag{7}$$

$$\min\sum_{k=1}^{m}c_k^{\mathrm{WT}}\tag{8}$$

$$\min\sum_{k=1}^{m}\beta\left(1-\alpha_{F_{SG_k}}\right)WT\tag{9}$$

s.t.

$$\sum_{k=1}^{m}x_{ik}=1\ i=1,2,\cdots,n\tag{10}$$

$$\sum_{i=1}^{n}WT_i^{\min}x_{ik}\leq WT,k=1,2\ldots,m\tag{11}$$

$$m^{\min}\leq m\leq m^{\max},m\in N^*\tag{12}$$

其中，式(7)表示最小化集成工艺约束惩罚；式(8)表示最小化重量惩罚；式(9)表示最小化碳排放量；式(10)表示每个板坯都被唯一分配到一个炉次；式(11)表示炉次背包约束；式(12)表示炉次数量范围，由启发式规则计算炉次数的可能取值范围$m^{\min}\sim m^{\max}$

炉次数下限：

$$m^{\min}=\left\lceil\frac{\sum_{i=1}^{n}WT_i^{\min}}{WT}\right\rceil\tag{13}$$

理想炉次数：

$$m^*=\left\lceil\frac{\sum_{i=1}^{n}WT_i^{\max}}{WT}\right\rceil\tag{14}$$

炉次数上限：

$$m^{\max}=\left\lceil\frac{\sum_{i=1}^{n}WT_i^{\max}}{WT-\delta_k}\right\rceil\tag{15}$$

其中，根据实际炉次生产能力将δ_k设置为常数，算法从$m^{\min}\sim\ m^{\max}$，依次选取炉次数。

3　算法设计

3.1 模型分析

在炉次计划问题中，若板坯的宽度范围均存在交集，则可以归约为容量车辆路径问(Capacitated Vehicle Routing Problem, CVRP)[4]。鉴于 CVRP 已被证实为 NP-hard 问题，炉次计划问题同样被归类为 NP-hard 问

题。由于本模型为多目标优化问题，现有研究验证了 MOEA/D 在求解多目标优化问题和组合优化问题的有效性及优越性[5-7], 本文设计了 LS-MOEA/D，同时针对柔性板坯的特点设计了相应的初始解生成策略。

3.2 板坯的宽度分组策略

该策略旨在将柔性宽度有交集的板坯分为一组，具体流程见图 2。

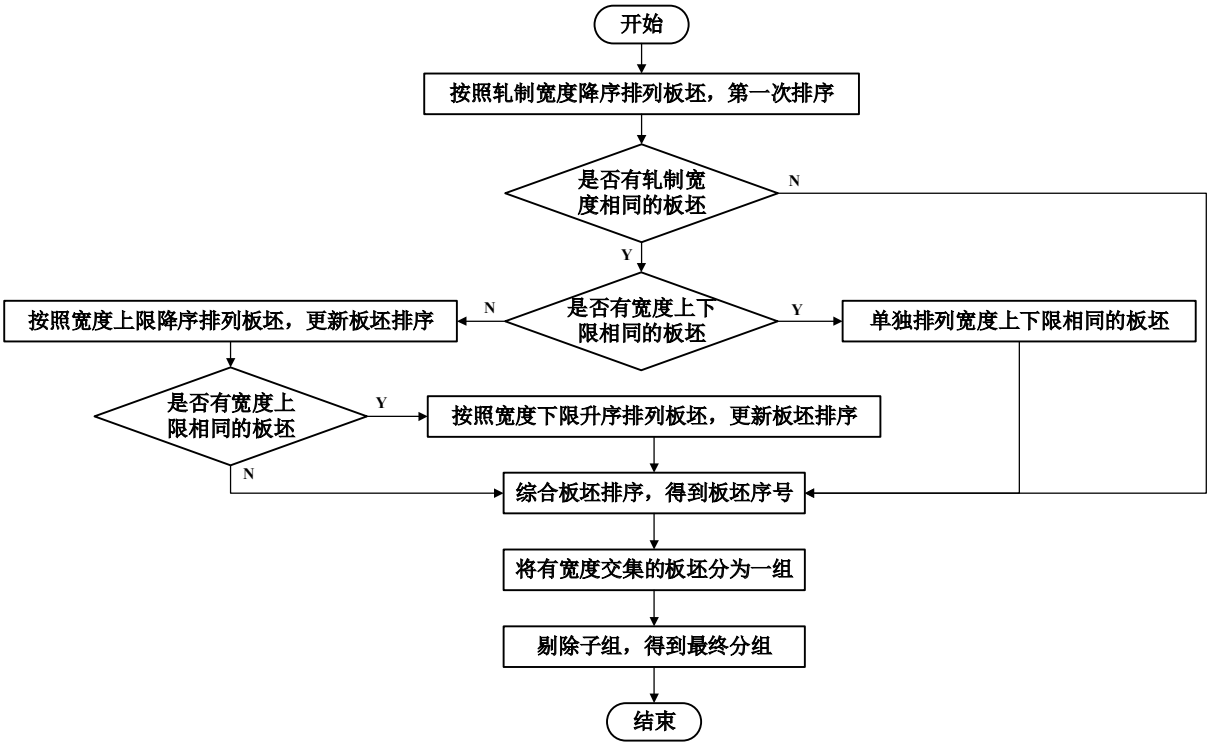


图 2 板坯基于宽度交集分组策略流程图

3.3 LS-MOEA/D 设计

LS-MOEA/D 涉及编码与解码、初始化权重向量、产生初始解群体、初始化邻域个体、初始化参考值、更新种群个体、更新邻域解、更新参考点，具体算法流程如图 5 所示。使用整数编码进行编码，编码中的数字对应板坯序号，个体由 m 条整数编码组成（m 为炉次数）。解码为一个 m 行 n 列的 0-1 矩阵（m 代表炉次数，n 代表板坯数），对应炉次的分配方案，图 3 和图 4 分别对应编码和解码的示意图。

$Code_1$	1	2	5	7	
$Code_2$	3	4	6	8	9

图 3 整数编码示意图

	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8	n_9
m_1	1	1	0	0	1	0	1	0	0
m_2	0	0	1	1	0	1	0	1	1

图 4 解码 0-1 矩阵示意图

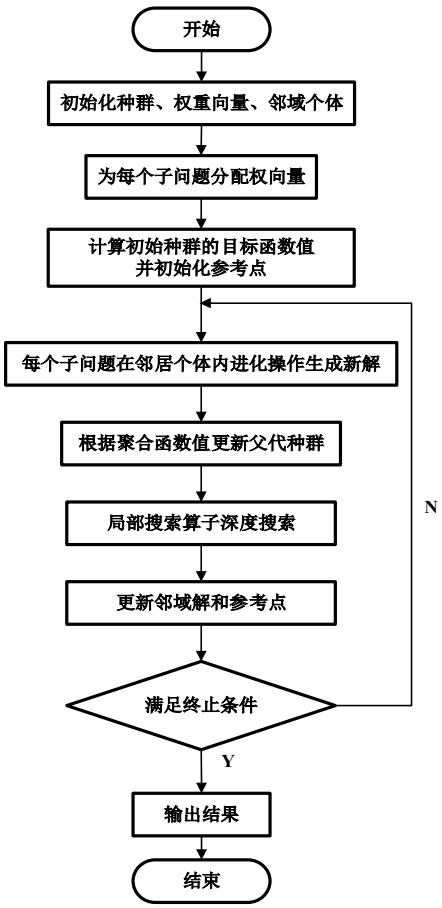


图 5 LS-MOEA/D 流程图

3.3.1 初始化权重向量

在运用基于分解的多目标进化算法时，首要步骤是生成一组权重向量，确保这些向量在解空间内均匀分布，权重向量基于单位超平面产生，生成权重向量个数$N = \mathrm{C}_{H+M-1}^{M-1}$，其中 M 是目标的个数，$H \geq M$是多目标问题中每个维度的坐标轴的间隔数量。

3.3.2 初始化种群

初始化种群采用随机分配和基于宽度交集分配两种方法，其中基于宽度交集分配是利用 3.2 节对板坯根据宽度交集分组的基础上设计的初始化种群的方法，下面给出了该方法的框架，如图 6 所示。

3.3.3 交叉

基于序列的交叉算子(Sequence-based Crossover, SBX)[8]作为一种交叉策略，自 1996 年提出以来，因其高效性和实用性而得到了广泛认可和应用。鉴于其显著优势，本文采用了 SBX 算子作为交叉机制。首先，从两个父代个体随机选取个体P_1和P_2，使用 SBX 算子分别随机选中一个炉次，分别标记为M_1和M_2。接着，针对每个炉次，随机选择两个断点，将炉次中的板坯组合分割成两个独立的集合，如$M_1 = \{M_{11}, M_{12}\}$，$M_2 = \{M_{21}, M_{22}\}$。接下来将M_{11}和M_{22}组合得到一个新炉次$M_{\mathrm{new1}} = \{M_{11}, M_{22}\}$。检查新构建的炉次$M_{\mathrm{new1}}$是否满足背包约束条件，如果组合得到的新炉次$M_{\mathrm{new1}}$满足炉次的背包约束，则用$M_{\mathrm{new1}}$替换掉父代个体$P_1$和中的原炉次$M_1$。若新炉次$M_{\mathrm{new1}}$不满足约束条件，重新在$M_1$和$M_2$中随机选择断点，构建新的炉次。这一过程将重复进行，直至成功找到满足条件的炉次或尝试次数达到 20 次上限。在规定的迭代次数内，若未能寻找到

符合特定条件的炉次，终止针对个体P_1和P_2的交叉操作，随机挑选新的父代个体，并重新启动交叉操作，以确保算法能够持续进行并探索更广泛的解空间。

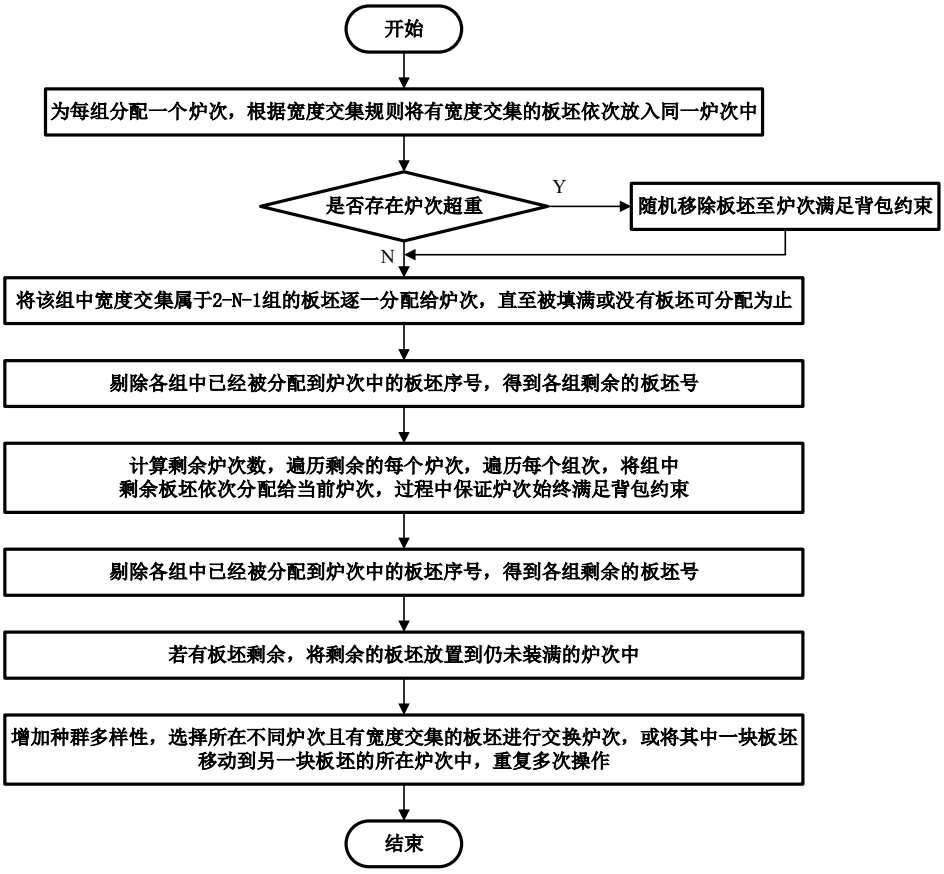


图 6 基于板坯宽度交集的初始解生成策略流程图

3.3.4 变异

Najera 和 Bullinaria[9]提出了一种包含三种基本变异算子的特殊变异算子，融合了三种核心操作与三种变异机制。结合本模型三种操作具体分别为，选择炉次、选择板坯、插入板坯。首先，炉次的选择是从个体中随机选择炉次。板坯的插入为选择满足约束条件的炉次，并且在插入后集成工艺约束惩罚最小的位置进行插入。三种基本算子分别是重新分配算子、交换算子和重新定位算子，考虑到本问题的特殊性，变异操作采用交换算子和重新分配算子。交换算子具体操作为，首先随机选择两个炉次，在每个炉次中随机选择两块板坯，移除两个板坯及其之间的所有板坯，并重新分配到另一个新炉次中。如果在重新分配过程中，有一个或多个板坯不满足新炉次的背包约束，这些板坯将被重新放回至原炉次中。重新定位算子具体操作为，随机选择一个炉次，从炉次中选择一块板坯从原炉次中移除，放入到合适的炉次中。如果不存在合适的炉次，则不移动板坯，因此经过变异操作后的个体同样满足约束条件是可行解。

3.3.5 解的修复

若交叉操作后，出现一块板坯同时现在同一个炉次中，删除重复的板坯序号；若出现一块板坯同时出现在两个炉次中，则将该板坯保留在新出现的炉次中，删除旧炉次中的板坯序号；若出现板坯未被分配到炉次中，则将该板坯随机插入符合背包约束的炉次中，图 7 为交叉算子流程及其修复策略示意图。

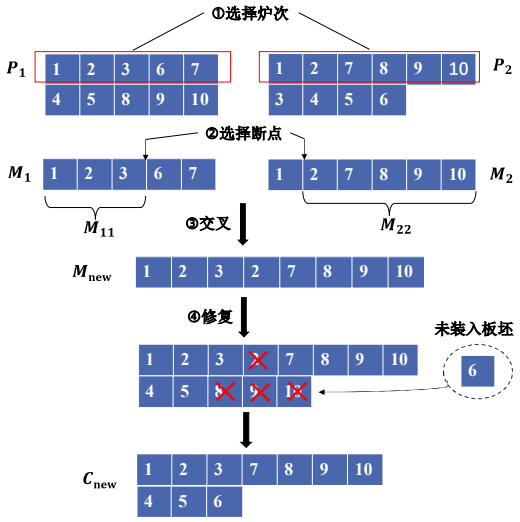


图 7 交叉算子示意图

经过重新分配算子处理后产生的新子代中若存在炉次不满足重量约束，则将移动的板坯放回原炉次中，进行重新变异，最多重复 20 次。图 8 为变异操作中的交换算子与重新分配算子的流程及其修复策略示意图。

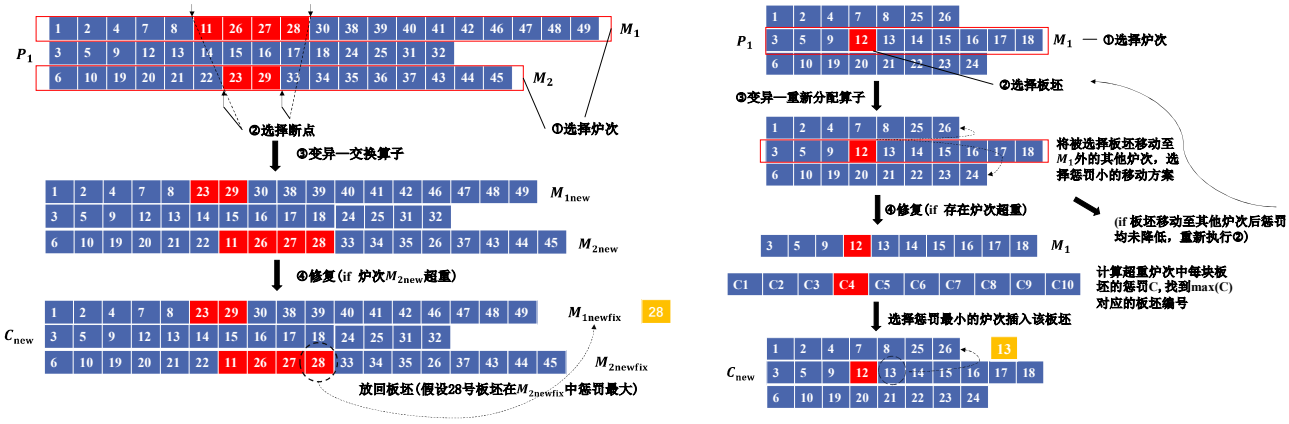


图 8 变异算子示意图

3.3.6 局部搜索

K.C.Tan 指出[10]，针对多目标时间窗车辆路径规划问题的求解，局部搜索算子能够协助全局搜索算法实现更广泛的搜索覆盖，提升问题求解的效率和准确性。对于炉次编制问题，本文为了获得更好的解，设计了两种局部搜索算子，分别是 Swap 算子和 Move 算子，图 9 为两种算子的示意图。

Swap 算子：从两个不同的炉次中选择两块板坯，然后交换这两块板坯的位置，交换后计算所有炉次的质量和，若所有炉次均满足重量约束且集成工艺约束惩罚未上升，则保留这次交换，重复 10 次操作。

Move 算子：在一个炉次中选择一块板坯，将其随机移动至其他炉次，移动后，若所有炉次均满足重量约束且集成工艺约束惩罚惩罚未上升，则保留这次移动，重复 10 次操作。

局部搜索触发概率PQ计算公式为式(16)

$$PQ = \tau\left(\frac{i}{Gen}\right) \tag{16}$$

其中τ为 0-1 之间的数，i表示当前迭代次数，Gen表示总迭代次数。

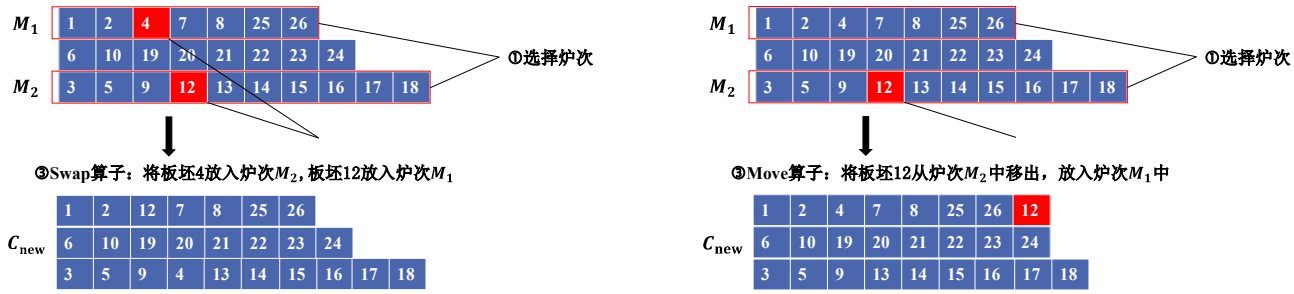


图 9 Swap 算子和 Move 算子示意图

3.3.7 选择

对新解y'给予一定的被选择概率，如果新解被选中，则进行局部搜索策略产生新解y''，如果有$g(y''|\lambda,z) \le g(y'|\lambda,z)$成立，则令$y' = y''$，$F(y') = F(y'')$，并对$y'$继续搜索直至不再获得更好的解，其中$g$为式(17)，更新解后，计算当前种群中各个解的 Z 值，并更新 Z 值。

$$\min g^{\mathrm{te}}(x|\lambda,z^*) = \max\{\lambda|f_i(x) - z_i^*|\} \tag{17}$$

3.3.8 终止条件判定

选择最大迭代次数作为算法的终止条件，当未达到最大迭代次数时算法将继续按照选择、交叉、变异、局部搜索的方式进行迭代，更新父代种群。

4 实例分析

为了验证本文模型与 LS-MOEA/D 的实际应用效果，以国内某钢厂的实际生产数据作为研究案例，从订单列表中随机抽取了包含 60 块板坯的某天板坯批量数据，以此为基础进行深入的实例分析。本文涉及的惩罚参数及其他相关参数的具体设定已详细列于表 1 和表 2 中，此外，$WT = 200$，$\delta_k = 30$。

表 1 惩罚参数表

参数	设定值	说明
δ^{PR}	60	优先级增量阈值
λ^{SG}	1000	相同钢级序列惩罚
λ^{PR}	100	优先级惩罚
λ^{F}	10	不同流向惩罚
β	22.375	碳排放量降低系数
α	1	重量惩罚系数
ϕ	100	宽度惩罚系数

表 2 不同钢级对应的最大废钢比

钢级编号	最大废钢比
2	0.15
3	0.18

4.1 参数分析

为了提升 LS-MOEA/D 的求解效率和精度，采用控制变量法对种群数(NP)、迭代次数(NG)、邻域大小

(NN)、交叉率(PC)、变异率(PM)五个参数试验调试，记录算法运行得到的解所对应三个目标函数值f_1、f_2、f_3的最小值(Min)、平均值(Mean)及运行时间(Time)，引入最大延展性指标[11](Maximum Spread, MS)和间距指标[12](Spacing, SP)对最终得到的解集的延展性和均匀性进行评价。每组参数运行 20 次取平均值，在 60 块板坯数据集下，得到 LS-MOEA/D 的最佳参数组合为，NP=231、NG=200、NN=6、PC=0.8、PM=0.4，表 3 为使用最佳参数得到的各项指标值。

$$MS(S) = \sqrt{\sum_{j}^{m} \max_{y,y' \in S} \left(y_j - y_j'\right)^2} \tag{18}$$

$$SP(S) = \sqrt{\frac{1}{N-1} \sum_{i}^{N} \left(\bar{d} - d\left(y_i, \frac{S}{y_i}\right)\right)^2} \tag{19}$$

表 3 使用最佳参数组合运行算法得到的各项指标值

Min			Mean			*M*	Time(s)	*MS*	*SP*
f_1	f_2	f_3	f_1	f_2	f_3				
659.1	48.2	22420	686.9	52.3	22420	6	1757.1	1.3617	0.1851
291.8	72.3	26089	295.4	74.3	26089	7	1881.6	1.1341	0.2016

4.2 目标分析

由于订单中某些板坯存在属性完全相同的情况，不同的炉次编制方案可能产生相同的效果，故去重处理得到最终的 Pareto 解集，如图 10 所示解的空间分布，决策者根据实际需求可以选择不同的方案，通过 LS-MOEA/D 得到 15 组较优的方案。对模型中的三个目标值分析可知，分配同等数量板坯时，增加炉次数会使集成工艺约束惩罚降低，重量惩罚变大；即增加炉次数量得到的板坯分配方案更加符合集成工艺约束，但是会使一些炉次的空间利用率降低，需要使用更多的无委托材料填充。当炉次数为 6 和 7 时，平均每个炉次的碳排放量为 3736.7 和 3727，表明炉次的平均碳排放量有所下降。

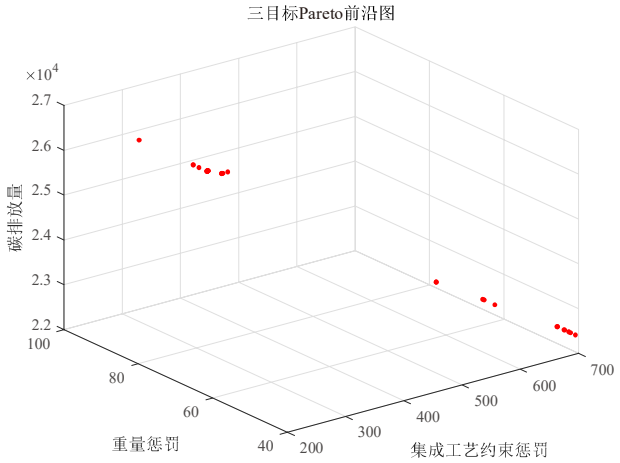


图 10 三目标 Pareto 前沿图

记录算法运行过程中每次迭代各目标的平均值，图 11 为使用七个炉次分配 60 块板坯三个目标函数均值随迭代次数的变化曲线，可见三个目标函数经过一定迭代次数后均现收敛趋势。

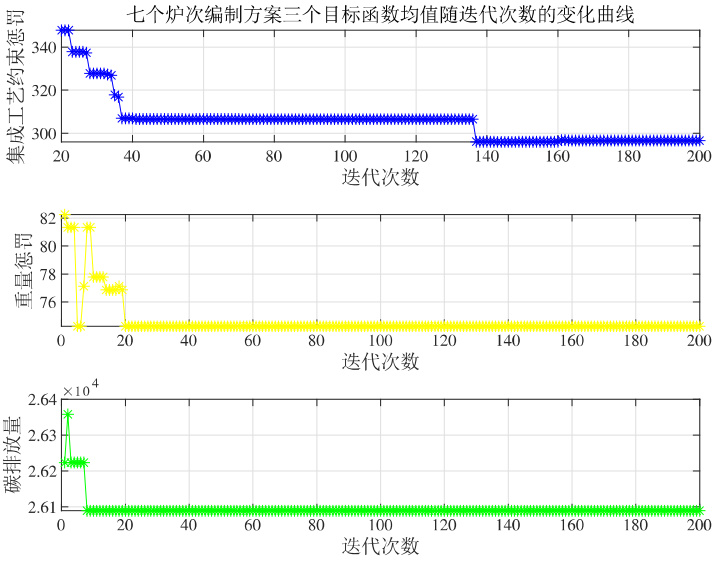


图 11 七个炉次编制方案三个目标函数的收敛性验证图

4.3 算法对比分析

为了体现本文算法的优越性，本文对初始解生成策略进行分析，同时对 LS-MOEA/D 与标准的 MOEA/D 使用相同的算法参数在相同数据集下的运行结果进行对比分析。

4.3.1 初始解生成策略对比

在 3.2 节中给出了使用随机分配（记为方法 A）和基于宽度交集分配（记为方法 B）两种初始解的生成策略，现考虑分别使用两种不同的初始解生成策略以及生成初始种群时，一半使用随机分配，一半使用基于宽度交集分配两种策略生成初始解（记为方法 A&B），使用 60 块板坯订单数据进行分析。由表 4 可以看出，三种初始解生成策略的平均运行时间基本相同，且算法最终均能收敛，且 MS 和 SP 值基本相同，说明得到解集的延展性和均匀性基本相同。

表 4 不同初始解策略对 LS-MOEA/D 算法的影响

初始解生成方法	Min			Mean			M	Time(s)	MS	SP
	f_1	f_2	f_3	f_1	f_2	f_3				
A	660.3	48.1	22420	688.2	52.6	22420	6	1767.4	1.3517	0.1946
	295.8	74.3	26089	296.7	75.6	26089	7	1882.1	1.1296	0.2106
B	659.1	48.2	22420	686.9	52.5	22420	6	1768.3	1.3617	0.1851
	291.8	72.3	26089	295.4	74.3	26089	7	1882.9	1.1341	0.2012
A&B	659.2	48.2	22420	686.5	52.4	22420	6	1768.1	1.3609	0.1886
	295.5	74.3	26089	296.6	75.9	26089	7	1882.6	1.1338	0.2013

由图 12 可见，对比三个目标函数值的收敛速度，使用基于宽度交集分配的初始解生成策略(B)目标函数值的下降速度最快，使用随机生成方法的初始解生成策略(A)目标函数值下降速度较慢。从 A&B 曲线看出，使用基于宽度交集分配的初始解策略寻优能力更强，效果更好。

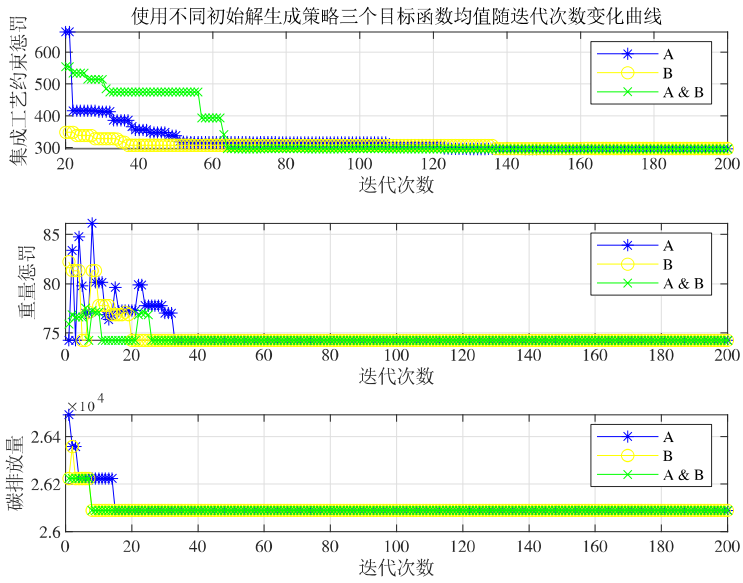


图 12 七个炉次分配 60 块板坯使用不同初始解生生策略三个目标函数的收敛性验证图

4.3.2 LS-MOEA/D 与标准 MOEA/D 对比

从表 5 可以看出标准的 MOEA/D 和 LS-MOEA/D 最终均能收敛且运行时间及各项评价指标基本相同，如图 13 所示本文的 LS-MOEA/D 相较于标准的 MOEA/D 收敛速度更快。

表 5 LS-MOEA/D 与标准 MOEA/D 的指标对比

算法	Min			Mean			M	Time(s)	MS	SP
	f_1	f_2	f_3	f_1	f_2	f_3				
LS-MOEA/D	659.1	48.2	22420	686.9	52.5	22420	6	1768.3	1.3617	0.1851
	291.8	72.3	26089	295.4	74.3	26089	7	1882.9	1.1341	0.2016
MOEA/D	659.2	48.3	22420	686.9	52.5	22420	6	1756.3	1.3621	0.1863
	296.1	74.4	26089	296.7	78.7	26089	7	1868.6	1.1316	0.2124

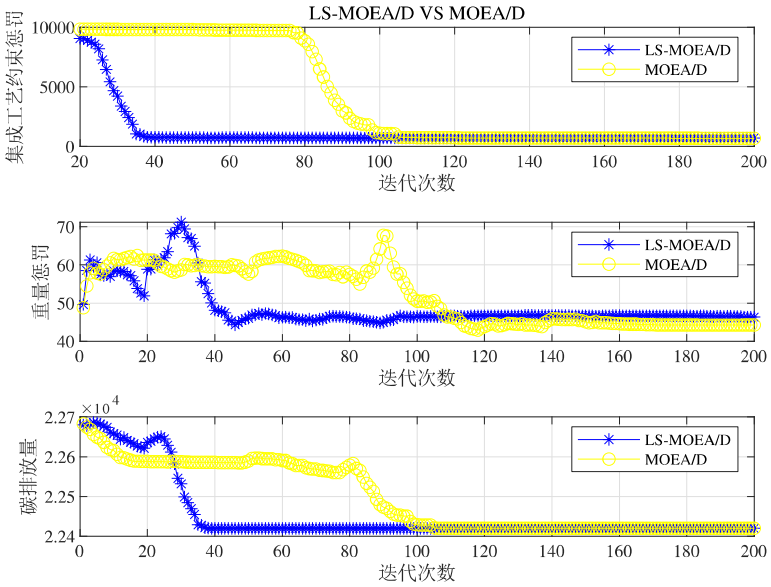


图 13 不同算法三个目标函数的收敛性验证图

5 结束语

本文研究了绿色柔性集成炼钢炉次计划问题，在使用柔性板坯的场景下，建立了以最小化集成工艺约束惩罚、最小化重量惩罚、最小化碳排放量为目标的多目标优化模型，鉴于问题的 NP-hard 特性，设计了 LS-MOEA/D 对模型进行求解。选用某钢厂的 60 块板坯真实数据进行实例分析。研究结果表明，分配同等数量板坯时，增加炉次数会使集成工艺约束惩罚降低，重量惩罚上升，当炉次数为 6 和 7 时，碳排放量分别为 22420 和 26089，平均每个炉次的碳排放量为 3736.7 和 3727，每个炉次的平均碳排放量降低。使用基于宽度交集分配的初始解生成策略会使 LS-MOEA/D 算法收敛速度更快，寻优效果更好，LS-MOEA/D 算法相较于标准的 MOEA/D 算法收敛速度更快，验证了 LS-MOEA/D 能够在综合考虑绿色、柔性、集成因素的条件下为炉次编制提供可行的方案。

参考文献

[1] 邱伏生, 李志强. 柔性生产模式下的制造业物流系统升级[J]. 物流技术与应用, 2024, 29(03): 77-83.

[2] 杨建平, 姚柳洁, 高攀, 等. 面向转炉高废钢比冶炼工艺的废钢比与碳排放理论计算[J]. 中国冶金, 2023, 33(06): 133-140.

[3] 郑忠, 呼万哲, 龙建宇, 等. Charge design method for medium steel plate considering tapping time and capacity[C]//中国金属学会炼钢分会. 第十九届(2016 年)全国炼钢学术会议大会报告及论文摘要集, 2016: 6.

[4] Huang M, Dong H, Wang X, et al. Guided variable neighborhood harmony search for integrated charge planning in primary steelmaking processes[M]//Proceedings of the first ACM/SIGEVO summit on genetic and evolutionary computation. 2009: 231-238.

[5] Tian Y, Feng Y, Zhang X , et al. A Fast Clustering Based Evolutionary Algorithm for Super-Large-Scale Sparse Multi-Objective Optimization[J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10(04): 1048-1063.

[6] 罗顺根, 郭秀萍. 用改进的 MOEA/D 算法求解微电网电力调度多目标优化问题[J]. 系统科学与数学, 2020, 40(01): 81-104.

[7] Do A V, Neumann A, Neumann F, et al. Rigorous runtime analysis of MOEA/D for solving multi-objective minimum weight base problems[J]. Advances in Neural Information Processing Systems, 2023, 36: 36434-36448.

[8] Potvin J Y, Bengio S. The vehicle routing problem with time windows part II: genetic search[J]. INFORMS journal on Computing, 1996, 8(2): 165-172.

[9] Garcia-Najera A, Bullinaria J A. An improved multi-objective evolutionary algorithm for the vehicle routing problem with time windows[J]. Computers & Operations Research, 2011, 38(1): 287-300.

[10] Tan K C, Chew Y H, Lee L H. A hybrid multiobjective evolutionary algorithm for solving vehicle routing

problem with time windows[J]. computational optimization and applications, 2006, 34: 115-151.

[11] 曹嘉乐, 杨磊, 田井林, 等. 面向高维多目标优化的双阶段双种群进化算法[J]. Journal of Computer Engineering & Applications, 2024, 60(9).

[12] 李二超, 张生辉. 基于新评价指标自适应预测的动态多目标优化算法[J]. 计算机应用, 2023, 43(10): 3178-3187.

[作者简介]

王敬博(2002—)，男，硕士生，从事智能制造、智能算法等研究；王庚辰（2000—），男，博士生，从事智能制造、鲁棒优化等相关研究；王庆（1969—），男，副教授，博士，从事系统建模与优化、供应链与 ERP 系统等研究；黄敏（1968—），女，教授，博士生导师，从事物流与供应链管理、智能算法设计与优化、调度理论与方法等研究。

流向	优先级	最大宽度	最小宽度	最大重量	最小重量	钢级	钢级序列	连浇代码
40	1	1450	1394	26.63	20.13	1441	2	140250
75	19	1450	1362	26.63	19.67	1441	2	140250
120	836	1450	1277	26.19	19.44	1441	2	140250
120	836	1450	1274	26.37	19.86	1441	2	140250
120	836	1450	1274	26.37	19.87	1441	2	140250
60	28	1450	1272	26.63	18.37	1441	2	140250
60	28	1450	1272	26.63	18.37	1441	2	140250
60	51	1450	1210	26.63	17.47	1441	2	140250
15	51	1400	1192	26.63	21.43	1441	2	140250
15	51	1400	1192	26.63	21.43	1441	2	140250
15	51	1400	1192	26.63	21.43	1441	2	140250
40	1	1200	1114	24.11	16.97	1441	2	140250
60	51	1300	1062	24.42	18.91	1441	3	140250
15	51	1300	1052	24.19	21.01	1441	2	140250
15	51	1300	1052	24.19	21.01	1441	2	140250
15	51	1250	1042	23.96	21.43	1441	2	140250
15	51	1250	1042	23.96	21.43	1441	2	140250
1	80	1250	1037	15.71	14.97	1441	3	140250
1	80	1250	1037	15.71	14.97	1441	3	140250
1	80	1250	1037	15.71	14.97	1441	3	140250
1	80	1250	1037	15.71	14.97	1441	3	140250
1	80	1250	1037	15.71	14.97	1441	3	140250
1	80	1250	1033	15.64	14.91	1441	3	140250
15	51	1250	1026	23.59	21.43	1441	2	140250
15	51	1250	1026	23.59	21.43	1441	2	140250
15	51	1250	1026	23.59	21.43	1441	2	140250
15	51	1250	1026	23.59	21.43	1441	2	140250
15	51	1250	1026	23.59	21.43	1441	2	140250
15	51	1250	1026	23.59	21.43	1441	2	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250

1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	80	1250	1025	15.52	14.8	1441	3	140250
1	39	1250	1025	15.52	14.8	1441	3	140250
15	51	1200	1019	23.43	21.43	1441	2	140250
15	51	1200	1019	23.43	21.43	1441	2	140250
15	51	1200	1019	23.43	21.43	1441	2	140250
75	80	1200	1013	15.34	14.63	1441	3	140250

轻量级区块链辅助的工业互联网端边协同调度

张培风[1,2,3]，许驰[1,2]

(1. 中国科学院沈阳自动化研究所 机器人学国家重点实验室，沈阳 110016;

2. 中国科学院 网络化控制系统重点实验室，沈阳 110016;

3. 中国科学院大学，北京 100049)

摘　要：针对工业互联网多样化工业任务的端边协同可信处理问题，本文设计了轻量级的区块链机制，提出了基于深度强化学习的任务、资源、区块链联合调度算法。首先，考虑多边缘服务器支持下，多终端的多目的地任务卸载场景，设计了任务卸载与区块链并行的轻量级委托拜占庭容错区块链机制，在保障实时性和安全性的情况下，降低了系统开销。在此基础上，充分考虑端边任务和计算资源分配、任务截止期和区块链稳定性等约束，构建了一个端边任务可信处理时延最小化问题，以联合优化任务卸载比例、计算资源分配和区块生成间隔。考虑问题的非凸性，采用马尔科夫决策过程进行建模，并提出增强软 Actor-Critic 算法来求解最佳调度策略。实验结果表明，所提方法在保障任务端边协同可信处理的同时，降低了任务处理时延，相比 DDPG 算法降低了 51.22%。

关键词：工业互联网；任务卸载；深度强化学习；区块链

Lightweight blockchain-assisted end-edge collaborative scheduling in industrial Internet

Zhang Peifeng[1,2,3], Xu Chi[1,2]

(1. State Key Laboratory of Robotics, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China; 2. Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China; 3. University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: To address the issue of trusted end-edge collaborative processing for diverse industrial tasks in the industrial Internet, this paper designs a lightweight blockchain mechanism and proposes a deep reinforcement learning-based joint scheduling algorithm for tasks, resources, and blockchain. Firstly, considering the scenario of multi-destination task offloading supported by multiple edge servers and end devices, a blockchain mechanism named lightweight-delegated Byzantine fault tolerance is designed to run in parallel with task offloading. This mechanism ensures real-time performance and security while reducing system overhead. On this basis, constraints such as end-edge task and computing resource allocation ratios, task deadlines, and blockchain stability are fully considered. The paper formulates a problem of minimizing the trusted processing delay of end-edge tasks, jointly

国家自然科学基金(92267108,62173322)；辽宁省科学技术计划(2023JH3/10200004,2022JH25/10100005).

optimizing the task offloading ratio, computing resource allocation, and block generation interval. Given the non-convex nature of the problem, a Markov decision process is used for modeling, and an enhanced soft Actor-Critic algorithm is proposed to solve the optimal scheduling policy. Experimental results show that the proposed method reduces task processing delay while ensuring trusted end-edge collaborative processing, achieving a 51.22% reduction compared to the DDPG algorithm.

Key words: industrial Internet, task offloading, DRL, blockchain

1　引言

工业互联网是新一代信息通信网络技术与工业制造深度融合的技术产物，它通过将工业设备、数据和人进行互联互通，显著提升了工业系统的智能化水平，提高了工业生产效率[1]。然而，工业互联网面临着几个关键挑战。首先，工业设备数量庞大且分布广泛，所产生的工业任务也激增，但其计算资源等有限[2]，无法满足日益增长的任务处理需求[3]。其次，工业互联网依赖开放的网络环境，系统的可信度较低，容易受到网络攻击和数据泄露的威胁[4,5]。这些问题对工业互联网的安全性和稳定性构成了严峻挑战。

为了应对这些挑战，基于区块链的端边协同计算成为了一种有效的网络范式[6]。该方案在靠近数据源的地方部署边缘服务器（edge server，ES）以补充算力，工业终端设备（end device，ED）可以选择让任务在本地计算或者将其卸载到算力较高的 ES 上，以处理复杂的计算任务，减少计算延迟，提高终端设备的用户体验质量[7]。此外，通过将 ES 及 ED 都接入区块链系统，利用其去中心化、不可篡改、可追溯等特点，来实现网络内各方的相互认证及任务卸载过程的记录与追溯。

近期有许多相关研究尝试将区块链与边缘计算相结合，以提高边缘计算网络的安全性及可信性[8,9]。文献[8]展示了一种基于区块链的新型平台，其目标是以去中心化的方式系统地解决多接入边缘计算场景内用户与边缘服务器的激励和信任问题。进一步地，还有许多研究工作以优化系统时延、能耗等为目标，在引入区块链机制后，建立关于资源及任务的调度优化问题，并采用深度强化学习等方法对其进行求解[10–16]。文献[11]面向车联网的移动计算卸载场景，提出了一种基于区块链的车辆辅助计算的系统模型，然后通过深度强化学习算法对资源分配策略进行优化,以在保证区块链吞吐量的同时减少系统能耗和时延；文献[12]提出了一个基于实用拜占庭容错（practical Byzantine fault tolerance，PBFT）区块链机制的协作计算卸载框架，以保证多车辆边缘计算环境中的安全数据迁移，并采用异步优势 Actor-Critic 算法来优化任务计算时延；类似地，文献[13]提出了一个集成 PBFT 的移动边缘计算框架来增强数据安全性和完整性，并利用双重深度 Q 网络来最小化总系统成本；文献[14]提出了一种区块链辅助边缘计算网络的资源管理方案，并制定了一个包含任务调度、发射功率控制和计算资源分配的联合任务处理问题，最后采用孪生延迟深度确定性策略梯度（twin-delayed deep deterministic policy gradient，TD3）算法对其进行求解；文献[15]开发了一种声誉证明共识机制，并通过多智能体深度确定性策略梯度（multi-agent deep deterministic policy gradient，

MADDPG）算法联合优化卸载决策、信道选择、发射功率分配和计算资源分配，以最大化基于区块链的多接入边缘计算系统的效用；文献[16]提出了一种区块链辅助的智能边缘协作系统来解决协同边缘计算中不同节点进行资源共享时的信任问题，并采用了长短时记忆来优化系统的性能。

尽管上述融合边缘计算与区块链的研究都对系统性能进行了不同程度的优化，然而，工业互联网相比传统互联网对时延更为敏感，传统的区块链机制需要大量的通信及计算资源，加剧了系统开销；同时，海量工业任务的并发卸载可能会导致网络拥塞和边缘服务器过载等一系列问题。因此，本文针对上述问题做出贡献如下：

（1）针对工业场景时延敏感性的特点，提出了轻量级的委托拜占庭容错（lightweight-delegated Byzantine fault tolerance，L-dBFT）区块链机制，与广泛使用的 PBFT 相比，L-dBFT 可以在保证安全可信的同时，有效降低区块链机制的开销。

（2）针对多终端、多边缘服务器场景下工业任务可信端边协同计算问题，建立多目的地任务卸载模型，充分考虑计算资源、任务截止期和区块链稳定性等约束，建立可信任务处理时延最小化问题，以优化任务迁移比例、计算资源分配、区块生成间隔。

（3）针对高度动态及时变的问题，采用马尔科夫决策过程进行建模，并提出增强的软 Actor-Critic（enhanced soft actor-critic，ESAC）算法，以获取最优策略。相比传统深度强化学习算法，有效提升了优化目标的性能表现。

2 系统模型

2.1 网络模型

如图 1 所示，本文主要考虑了一个工业互联网场景下基于区块链的端边协同计算模型，包含N个 ES 和M个 ED。令$\mathcal{N}=\{1,2,\dots,N\}$和$\mathcal{M}=\{1,2,\dots,M\}$分别表示 ES 和 ED 的集合。其中，ES 配备高性能的计算资源和持续的能源供应，并且彼此之间通过有线连接。而 ED（例如具有计算密集型任务的机器人视觉传感器）则与 ES 无线连接。ED_m的任务由元组$Y_m=\left(D_m^{\text{task}},C_m^{\text{task}},T_m^{max}\right),m\in\mathcal{M}$表示。其中，$D_m^{\text{task}}$表示该任务的数据大小，$C_m^{\text{task}}$表示完成任务所需的计算资源（即 CPU 周期数），T_m^{max}表示任务截止期（即完成任务允许的最大时延）。

由于 ED 的资源有限，在此边缘计算网络架构下，ED 可以将任务划分并卸载到多个 ES 上并行计算，借助 ES 的高性能计算资源来完成复杂任务的计算，提高任务处理效率。具体来说，ED_m将大小为$u_{m,n}D_m^{\text{task}}$的子任务卸载到ES_n。其中，$u_{m,n}$表示ED_m为ES_n划分的任务比例。由此可得

$$\sum_{n=0}^{N}u_{m,n}=1, \tag{1}$$

当$n=0$时，表示该子任务由 ED 执行本地计算。

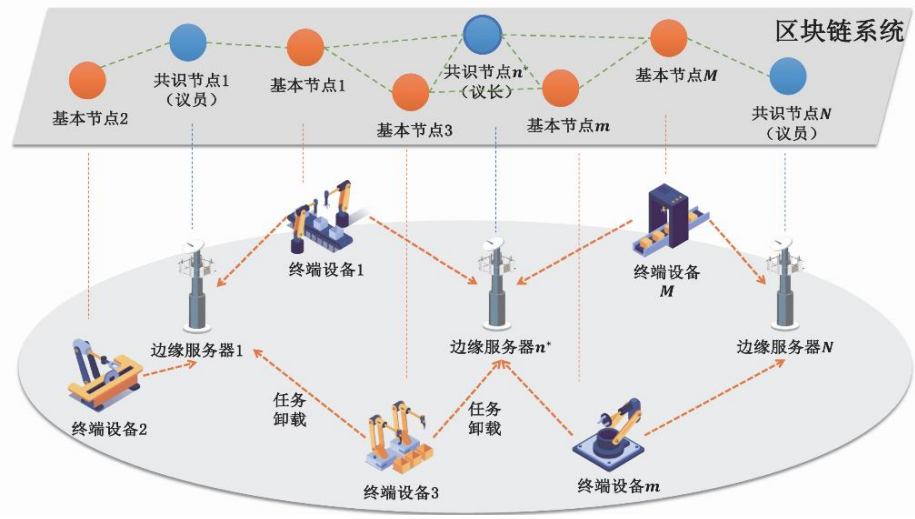


图 1 区块链辅助的端边协同计算模型

2.2 通信模型

ED 执行边缘计算时，会采用正交频分多址（OFDMA）来进行多目的地的任务卸载。根据香农定理，ED_m与ES_n之间的传输速率可以计算为

$$R_{m,n}(t)=W_{m,n}\log_2\left(1+\frac{p_m g_{m,n}}{\sigma^2+I}\right), \tag{2}$$

其中，$W_{m,n}$，$g_{m,n}$，σ^2，I 分别代表ED_m到ES_n之间的信道带宽、信道增益、噪声功率和干扰功率，p_m被设为ED_m的发射功率。

因此，根据公式(2)，我们可以计算出任务卸载时的传输时延为

$$T_{m,n}^{\text{off}}=\frac{u_{m,n}D_m^{\text{task}}}{R_{m,n}}, \tag{3}$$

当完成计算，得到结果后，ES 将结果返回给对应的 ED。但是，由于返回结果数据远小于卸载数据，参考已有研究成果，本文中忽略返回结果的传输时延。

2.3 计算模型

任务的计算由 ES 和 ED 共同完成，以实现端边协同计算。本节将分别介绍边缘计算和本地计算模型。

（1）边缘计算

由于任务可被拆分卸载给多个 ES 进行并行计算，则可以将ES_n针对ED_m卸载子任务的边缘计算时延表示为

$$T_{m,n}^{\text{edge}}=\frac{u_{m,n}C_m^{\text{task}}}{f_{m,n}}, \tag{4}$$

其中，$f_{m,n}$是ES_n为ED_m分配的计算频率，以每秒的计算周期数来衡量，且不能超过ES_n的最大计算频率$F_n^{\max}$，表示为

$$f_{m,n}\le F_n^{\max}. \tag{5}$$

由于多个子任务并行计算，所以最终任务Y_m的边缘计算时延可表示为

$$T_m^{\text{edge}} = \max_{n=1,\dots,N} \{T_{m,n}^{\text{edge}}\}. \tag{6}$$

（2）本地计算

对于未卸载到 ES 的剩余子任务，将由 ED 执行本地计算。假设本地计算资源为 f_m，则其计算时延可表示为

$$T_m^{\text{end}} = \frac{u_{m,0} C_m^{\text{task}}}{f_m}. \tag{7}$$

类似地，对于本地计算资源 f_m 有

$$f_m \le F_m^{\max}. \tag{8}$$

2.4 区块链模型

为了确保 ES 和 ED 之间的互信，实现可信端边协同计算，本文进一步提出轻量级的区块链方法 L-dBFT。区块链系统的部署如图 1 所示。当 ED 的任务需要卸载至 ES 进行端边协同计算时，所有参与边缘计算的 ES 将会在完成计算后生成交易数据，然后通过区块链共识机制将相关进行验证、上链与存储。具体来说，所有 ES 和 ED 都充当区块链节点。其中，ES 为共识节点，负责生成新区块并参与共识；ED 为基本节点，只负责记录链上信息，并可通过智能合约查询历史卸载记录以验证任意 ES 的可信性。

如图 2 所示，端边协同计算与区块链共识并行开展。在共识过程中，假设共识节点数量$N \ge 3s+1$（s为可容忍的最大恶意节点数量），每阶段随机选择一个$ES_{n^*}(n^* \in N)$作为议长，负责广播新区块提案；其余参与共识的节点为议员，负责对新区块提案进行投票。

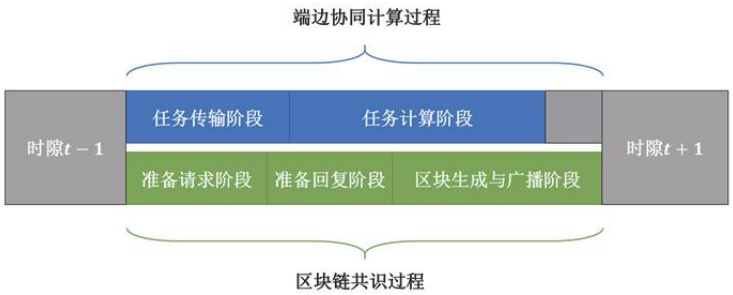


图 2 时隙分配

L-dBFT 算法的具体步骤主要如下：

（1）准备请求阶段：参与边缘计算的 ES 将交易信息和共识请求存入交易内存池，议长ES_{n^*}从内存池内取出交易数据，验证交易信息后生成签名及对应的 MAC，并将其打包为一个新的区块提案作为请求消息。假设验证所需的计算资源为C^{req}，议长ES_{n^*}为其分配的计算资源为

$$T^{\text{req}} = \frac{C^{\text{req}}}{f_{n^*}^{\text{b}}}. \tag{9}$$

然后，议长ES_{n^*}将该请求消息发送给其他议员 ES。因 ES 之间为有线连接，传输稳定且速度快，则共识阶段中的传输时延可被忽略。

（2）准备回复阶段：所有议员 ES 收到区块提案后，都需要对其包含的所有交易的签名及 MAC 进行验证，再生成签名及 MAC 形成回复消息。假设此阶段所需要的计算资源为C^{reply}，议员ES_n为其分配的计算资源为f_n^{b}。由此可得

$$T_n^{\text{reply}} = \frac{C^{\text{reply}}}{f_n^{\text{b}}}. \tag{10}$$

若成功经过验证，议员 ES 则会返回该回复消息给议长ES_{n^*}。

（3）区块生成与广播阶段：本阶段议长收到满足拜占庭容错条件数量的议员回复消息，开始验证其有效性，若验证成功，则生成签名与 MAC，正式生成新区块，并将其广播给其他议员 ES。假设所需计算资源为C^{gen}，则有

$$T^{\text{gen}} = \frac{C^{\text{gen}}}{f_{n^*}^{\text{b}}}. \tag{11}$$

到此就认为本次共识完成，该区块成功上链。

综上所述，整个区块链共识过程包括：准备请求阶段、准备回复阶段和区块生成与广播阶段，其共识过程所耗费的时延可表示为

$$T^{\text{cons}} = T^{\text{req}} + \max_{n=1,\ldots,N} \{T_n^{\text{reply}}\} + T^{\text{gen}}. \tag{12}$$

此外，为了控制区块链数据的增长速度和网络的稳定性，防止区块生成过快导致区块链分叉，还需设置合适的区块生成间隔T^{intv}。所以区块链的最终确定时延T^{LTF}为由两部分组成：共识时延和区块生成间隔，可被表示为

$$T^{\text{LTF}} = T^{\text{cons}} + T^{\text{intv}}. \tag{13}$$

3　问题建模

3.1　问题形成

根据前述系统模型，可以得知可信端边协同计算过程主要包括：任务的卸载与计算、区块链的共识与上链。所以整个系统的总时延为

$$T^{\text{total}} = \max_{m=1,\ldots,M} \{T_m^{\text{end}}, T_m^{\text{edge}}, T^{\text{LTF}}\}. \tag{14}$$

面向工业互联网多样化任务的实时、可信端边协同计算要求，本文以最小化可信任务处理时延T^{total}为目标，构建如下任务、资源和区块链联合调度问题

$$\underset{\mathcal{U},\mathcal{F},\mathcal{I}}{\text{Minimize}} \quad T^{\text{total}}, \tag{15}$$

$$\text{s.t. } (1),(5),(8),$$

$$\sum_{m=1}^{M} f_{m,n} + f_n^{\text{b}} \le F_n^{\max}, \tag{16}$$

$$T_m \le T_m^{\max}, \tag{17}$$

$$T^{\text{LTF}} \le \omega T^{\text{intv}}, \tag{18}$$

其中，$\mathcal{U} = \{u_{m,n}\}_{M\times(N+1)}$是任务划分比例的集合，$\mathcal{F} = \{\{f_{m,n}\}_{M\times N}, \{f_n^{\text{b}}\}_N\}$是计算资源分配比例的集合，$\mathcal{I} = \{T^{\text{intv}}\}$是区块链参数的集合。

在上述问题中，我们考虑了端边任务分配约束(1)，计算资源约束(5)、(8)、(16)，任务截止期约束(17)，区块链的安全性约束(18)。其中$\omega > 1$，代表一个区块应该在多个连续的区块生成间隔内发布和验证，即ω区块生成间隔[4]。

3.2 马尔科夫建模

在工业互联网端边协同计算场景下，涉及到多个不确定的因素，如网络条件的变化、资源的可用性以及任务的动态生成等，且各优化变量间互相耦合，传统方法难以求解。因此，本文将上述任务、资源与区块链的联合调度问题描述为一个马尔科夫决策过程（MDP），以适应动态、高维的环境信息，再利用深度强化学习算法进行求解。

该 MDP 模型包括智能体集合、状态空间、动作空间、奖励函数，具体的定义如下：

（1）智能体集合$\mathcal{N}$：每个 ES 都被当作智能体，可通过观测状态信息做出动作决策。因此，智能体集合被表示为$\mathcal{N} = \{1,2,\dots,N\}$。

（2）状态空间$\mathcal{S}$：状态空间定义了系统在任何给定时间点可能处于的所有状态。状态可被智能体观测后用于做出决策。在上述问题中，每个时刻的状态可表示为

$$S(t) = \left\{\mathbf{D}(t), \mathbf{C}(t), \mathbf{T}^{\max}(t), W_{m,n}(t), g_{m,n}(t), \sigma^2(t), I(t),\ \mathbf{F}^{\text{end}}(t), F_n^{\max}(t)\right\}. \tag{19}$$

其中，$\boldsymbol{D}(t) = \{D_1^{\text{task}},\dots,D_M^{\text{task}}\}$为任务数据大小的集合，$\boldsymbol{C}(t) = \{C_1^{\text{task}},\dots,C_M^{\text{task}},C^{\text{ver}},C^{\text{val}},C^{\text{gen}}\}$为任务所需计算资源及区块链共识各阶段所需的计算资源，$\boldsymbol{T^{max}}(t) = \{T_1^{max},\dots,T_M^{max}\}$表示任务的截止期，$W_{m,n}(t), g_{m,n}(t), \sigma^2(t), I(t)$分别表示带宽、信道增益、噪声功率和干扰功率，$\mathbf{F}^{\text{end}}(t) = \{f_1^{max}, f_2^{max},\dots,f_M^{max}\}$代表 ED 所能分配的最大计算资源，而$F_n^{max}(t)$为 ES 所能分配的最大计算资源。

（3）动作空间$\mathcal{A}$：动作空间定义了所有 ES 的一系列策略。在时隙t，ES 将根据状态$S(t)$做出决策并执行动作$A(t)$，该动作被表示为

$$A(t) = \left\{\mathbf{u}(t), \mathbf{f}(t), \mathbf{f}^b(t), T^{\text{intv}}(t)\right\}, \tag{20}$$

其中，$u(t) = \{u_{1,1},\dots,u_{1,N},\dots,u_{M,N}\}$表示任务的划分比例，$f(t) = \{f_{1,1},\dots,f_{1,N},\dots,f_{M,N}\}$表示 ES 的计算资源分配比例，$f^b(t) = \{f_1^{\text{b}}(t),\dots,f_n^{\text{b}}(t)\}$为分配给区块链共识的计算资源，$T^{\text{intv}}$为区块链的区块产生间隔。

（4）奖励函数$\mathcal{R}$：奖励函数为智能体提供了关于其行为好坏的反馈，是智能体在学习过程中用来评估不同行为的标准，从而指导智能体在复杂环境中学习更优的动作策略以获得最大的长期收益。在上述优化问题中，为了在满足约束条件的情况下最小化时延，本文设计奖励函数如下

$$R = \frac{1}{T^{\text{total}}} + P_{\text{b}}, \tag{21}$$

其中，P_{b}表示未满足约束(18)时产生的惩罚，定义为

$$P_{\text{b}} = \begin{cases} 0, & \text{如果满足约束(18)}, \\ -1, & \text{如果不满足约束(18)}. \end{cases} \tag{22}$$

4 基于 ESAC 的调度算法

依据前述问题特性，本文提出了一种结合 SAC 和优先经验回放（Prioritized Experience Replay， PER）机制的深度强化学习算法 ESAC。ESAC 利用 SAC 的稳定性和高效性，并通过优先经验回放机制提高了样本利用率，从而进一步提升了训练效率和性能。

4.1 算法介绍

ESAC 基于最大熵的思想，在寻求最大化累积奖励的同时，还会同时考虑增加策略的熵，以促进探索和防止过早收敛到次优策略。如图 3 所示，它的网络结构基于 Actor-Critic 架构，具体如下：

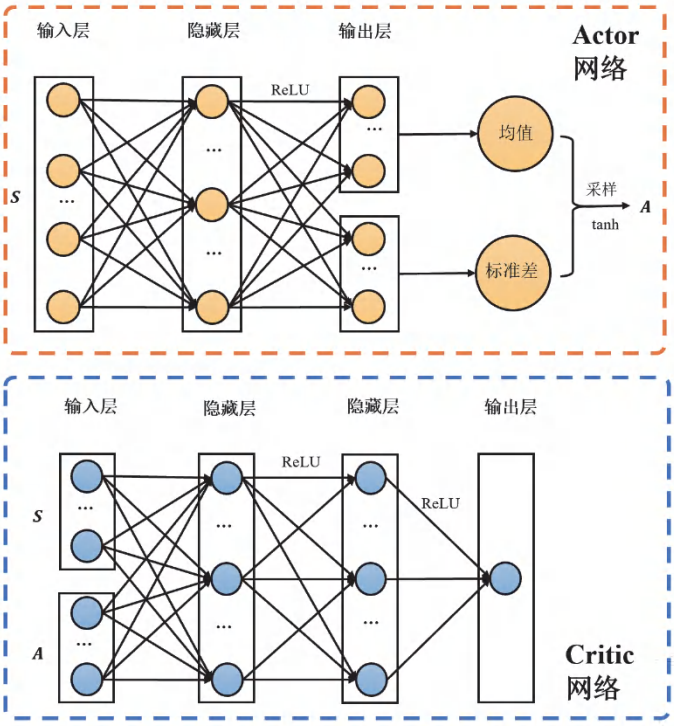


图 3 ESAC 的神经网络架构

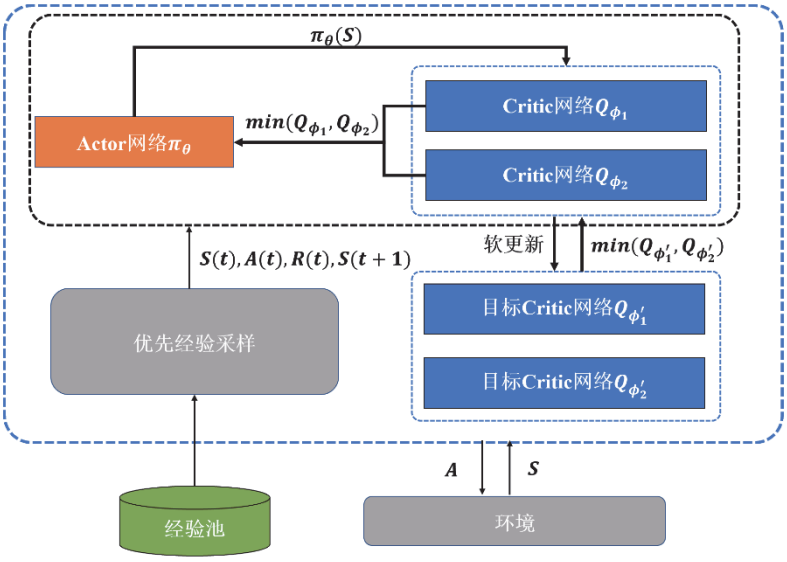


图 4 算法运行过程

（1）Actor 网络：Actor 网络π_θ接收状态输入S，输出动作A。其结构包括两层全连接层，每层包含h个神经元，再连接到 ReLU 激活函数。最后一层使用 tanh 激活函数以保证动作在合理范围内。

（2）Critic 网络：Critic 网络包含两个独立的 Q 网络Q_{ϕ_1}和Q_{ϕ_2}，及两个与其相同结构的目标 Critic 网络$Q_{\phi'_1}$和$Q_{\phi'_2}$，均接收状态S和动作A作为输入，输出相应的 Q 值。由于传统 Q 网络的估计值普遍偏高，所以引入两个 Q 网络取其计算出的较小 Q 值，可以有效减轻由于估值误差带来的偏差。每个 Q 网络也包括两层全连接层，每层包含h个神经元，并连接至 ReLU 激活函数。目标 Q 值Q^t的计算公式如下

$$Q^t = R + \gamma \min(Q_{\phi'_1}(S', A'), Q_{\phi'_2}(S', A')) - \eta \log \pi_\theta(A' \mid S'), \tag{23}$$

其中，γ是折扣因子，η是熵正则化系数，用于平衡算法的平衡和探索。

ESAC 通过引入优先经验回放机制来优先选择重要的经验样本进行训练，从而提高样本利用率和算法性能。PER 的核心思想是通过为每个经验样本分配一个优先级，使得重要样本被更频繁地采样。经验样本

的优先级通常与其时分误差相关，时分误差越大，经验样本越重要。具体而言，样本i的采样概率$P(i)$由其优先级p_i确定，计算公式如下：

$$P(i)=\frac{p_i^{\alpha}}{\sum_{k=1}^{K}p_k^{\alpha}}, \tag{24}$$

其中，α控制优先级对采样概率的影响，K为经验样本数量。然后可计算得到采样性权重w_i，

$$w_i=\left(\frac{1}{K}\cdot\frac{1}{P(i)}\right)^{\beta}, \tag{25}$$

此处，β控制重要性采样的程度。

4.2 算法运行过程

本文所提出的 ESAC 优化算法的具体训练过程如图 4 和算法 1 所示。

算法 1：ESAC 算法训练过程

输入：状态S；

输出：动作A；

初始化 Actor 网络π_θ，Critic 网络 Q_{ϕ_1},Q_{ϕ_2} 和目标 Critic 网络 $Q_{\phi_1'},Q_{\phi_2'}$；
初始化具有优先级权重和超参数 α,β的经验回放缓冲区$\mathcal{D}$；
for 最大迭代次数 do：
    for 最大环境交互步数：
        根据神经网络，选择动作 $A(t)\sim\pi_\theta\big(A\big|S(t)\big)$；
        获得奖励$R(t)$和下一个状态$S(t+1)$；
        将经验$\{S(t),A(t),R(t),S(t+1)\}$存储到$\mathcal{D}$中，使用初始优先级；
    end for
    for 每次梯度更新 do：
        通过公式(25)计算重要性采样权重w_i；
        通过公式(23)计算目标 Q 值Q^{t}；
        计算 Critic 网络的损失：
            $L_Q=E\left[w_i\big(Q_{\phi_1}(S,A)-Q^{\mathrm{t}}\big)^2+w_i\big(Q_{\phi_2}(S,A)-Q^{\mathrm{t}}\big)^2\right]$；
        更新 Critic 网络的参数ϕ_1,ϕ_2；
        计算时分误差δ_i并用其与探索系数ε来更新$\mathcal{D}$中的经验样本优先级：
            $\delta_i=Q^{\mathrm{t}}-Q_{\phi}(S,A)$，
            $p_i=|\delta_i|+\varepsilon$；
        计算 Actor 网络的损失：
            $L_\pi=E\left[\alpha\log\pi_\theta(A|S)-\min\Big(Q_{\phi_1}(S,A),Q_{\phi_2}(S,A)\Big)\right]$；
        更新 Actor 网络的参数 θ；
        根据目标熵$\mathcal{H}$计算熵正则化系数的损失：
            $L_\eta=-E\big[\eta\big(\log\pi_\eta(A|S)+\mathcal{H}\big)\big]$；
        更新熵正则化系数 η；
        软更新目标 Critic 网络的参数；
            $\phi_1'\leftarrow\tau\phi_1+(1-\tau)\phi_1'$，
            $\phi_2'\leftarrow\tau\phi_2+(1-\tau)\phi_2'$；

27:　　end for
28:　end for

训练过程中，对经验池内的经验设置优先级，提高训练效率及训练稳定性，所使用的优先经验回放机制具体如下算法 2 所示。

算法 2：ESAC 算法的优先经验回放机制

输入：经验池D；
输出：经验池D；
1:　初始化回放缓冲区$\mathcal{D}$，容量为 K，优先级参数 α *和* β；
2:　初始化优先级数组 p，其大小为 K；
程序 1 添加：
3:　初始化新经验样本的优先级；
4:　将经验样本及其优先级存储到缓冲区中；
程序 1 end
程序 2 采样：
5:　根据优先级p_i^{α}和公式(24)计算采样概率$P(i)$；
6:　根据概率$P(i)$采样一批经验样本；
7:　通过公式(25)计算重要性采样权重w_i：
8:　将权重w_i归一化；
9:　返回采样的经验样本和归一化权重；
程序 2 end
程序 3 优先级更新：
10:　for K do：
11:　　更新优先级：
12:　　$p_i = |\delta| + \varepsilon$ ；
13:　end for
程序 3 end

5　仿真实验及结果分析

为了证明所提出模型、区块链机制和 ESAC 算法的收敛性和有效性，本章节将采用该算法针对上述时延最小化的优化问题进行仿真实验，并使用同样适用于连续性动作空间的 SAC、DDPG、TD3、PPO 算法作为基准算法进行对比实验。

5.1　环境及参数设置

实验环境部署于配备 Intel Core i9-11700 CPU 和 NVIDIA GTX 4090 GPU 的服务器上进行，系统采用 Ubuntu 18.04 LTS，编译环境采用 Python 3.11.0 和 PyTorch 框架。仿真参数参考文献[12,13,17,18]设置，具体如表 1 所示。

表 1 仿真实验参数表

参数名称	参数数值
最大训练步数	30000
折扣因子γ	0.99
隐藏层宽度$\hbar$	256
学习率ψ	0.001
训练批次大小	256
终端设备数M	20
边缘服务器数N	3

ED_m的最大发射功率p_m	300 mW
ED_m和ES_n之间的最大带宽$W_{m,n}$	20 MHz
ED_m的最大计算资源F_m^{max}	2 GHz
ES_n的最大计算资源F_n^{max}	50 GHz
区块生成间隔数量ω	2
信道增益$g_{m,n}$	-70dB
噪声功率σ^2	(2×10^{-13})mW
干扰功率I	(2×10^{-12})mW
任务所需计算资源C_m^{task}	[0.25, 2.5] GHz
任务大小D_m^{task}	[1, 10] MB
任务截止期T_m^{max}	[0.01, 0.5] s
区块链交易验证所需计算资源C^{req}	0.2 GHz
区块链交易回复所需计算资源C^{reply}	0.1 GHz
区块生成所需计算资源C^{gen}	0.2 GHz
区块生成间隔T^{intv}	[0.2, 2] s

5.2 实验结果分析

图 5 测试了所提出 ESAC 算法在不同学习率情况下的性能表现。我们可以观察到，随着学习率的增加，算法的收敛速度明显提升。这一现象表明，较高的学习率有助于算法快速适应环境变化，从而加速学习过程。然而，过高的学习率也存在风险，可能会导致算法过早地收敛到局部最优解，而忽略了潜在的更优策略，这反映在奖励的减少上。相反，较低的学习率虽然能够避免上述问题，但却可能导致学习过程过于缓慢，使得算法无法充分利用累积的经验。因此，综合考虑收敛性和稳定性，我们采用 0.001 作为训练学习率。

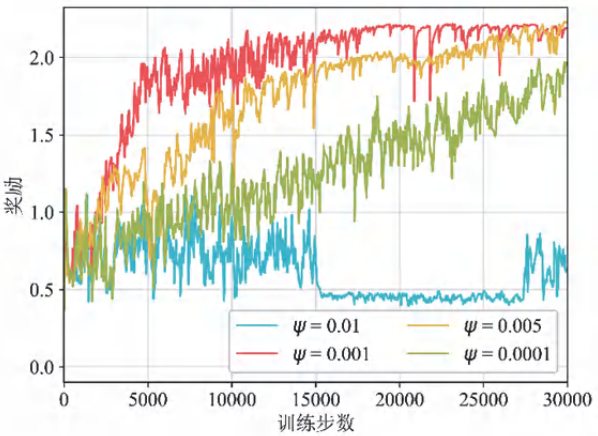


图 5 不同学习率下的奖励对比

如图 6 所示，测试了不同算法所获得的奖励。可以看出，随着训练步数的增加，所有算法最终都能收敛到一个稳定的值，说明了所述时延最小化问题有解，且证明了各算法的可用性。此外，由图可观察到，所提出 ESAC 算法得到的奖励相比 DDPG 得到的奖励分别高出了近 48.17%。显著地，可发现添加优先经验回放机制的 ESAC 相比原始 SAC 算法收敛速度会加快，最终收敛值也更佳。因此，本文所提出的 ESAC 算法的奖励最高，并且训练效率更高、更加稳定。

进一步地，图 7 测试了在不同算法下，所提算法在时延最小化方面的表现。从图中我们可以观察到，所提出的算法 ESAC 在前述问题模型上表现出色，不仅在奖励方面保持了高水平，而且在时延最小化方面也展现了显著的优势，所得时延相比 DDPG 降低了 51.22%。这一测试的性能表现证明了该算法针对时延敏感的工业互联网场景时的有效性和适用性。

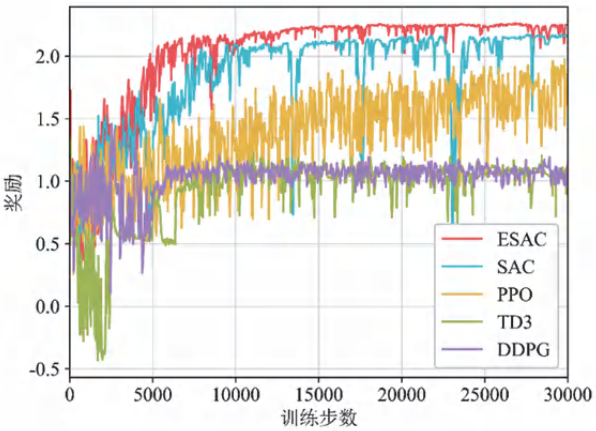


图 6 不同算法的奖励对比

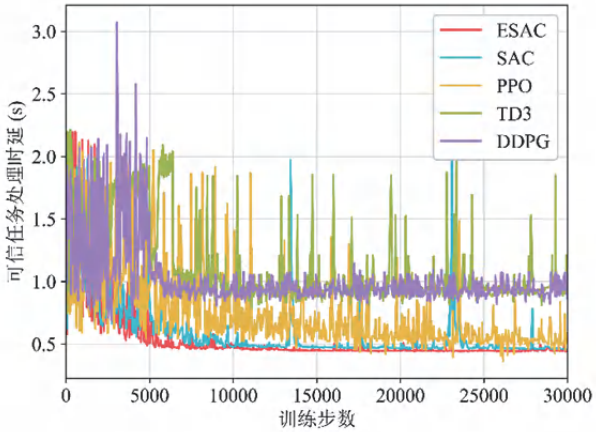


图 7 不同算法的时延对比

图 8 展示不同数量级的 ED 对奖励产生的影响。可以发现，算法获得的奖励随着 ED 数量的增多而递减。其原因是边缘服务器的通信资源及计算资源有限，当工业终端数量增加时，所产生的任务数量也随之增多，可能引发高并发卸载，使得同一边缘服务器下工业终端分得的带宽减小、计算资源减少，造成任务处理时延增加，最终使得所获得奖励减小。但是，在不同数量级终端设备的情况下，所提出的 ESAC 算法始终保持更优的性能。

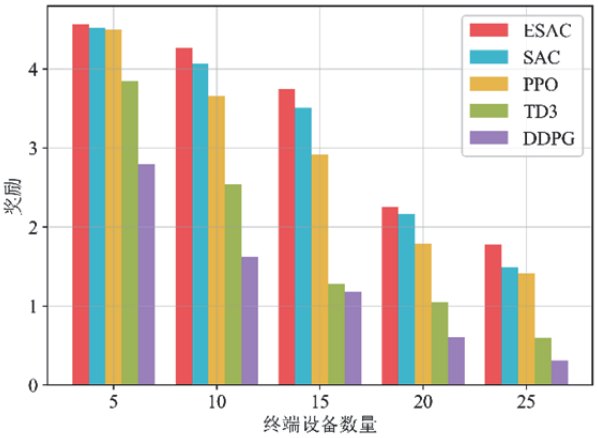


图 8 不同终端设备数量下的奖励对比

此外，图 9 对比了不同数量级的 ED 对时延产生的影响。随着 ED 数量增多，所有算法得到的时延都在下降，且所提出的 ESAC 算法得到的可信任务处理时延也总是低于其他算法，体现了该算法求解所构建问题的高效性和优越性。

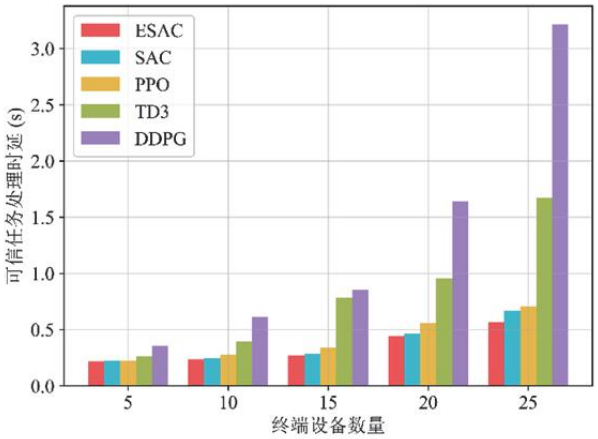


图 9 不同终端设备数量下的时延对比

图 10 描述了边缘服务器不同最大计算资源的情况下，奖励随着训练次数的变化趋势。可以从图中观察到，随着计算资源的增大，边缘服务器针对大量任务请求时可供分配的资源增多，则任务的计算速度及区块链共识速度都能得到提升，所以会导致奖励提升，即总时延降低。且可以看出，所提出 ESAC 算法的性能表现一直优于其他算法。

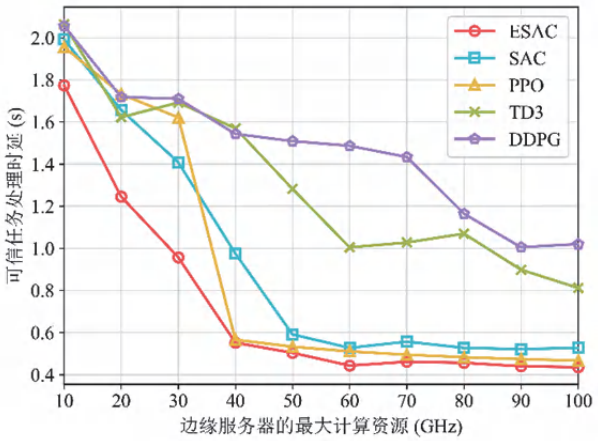


图 10 不同边缘服务器的最大计算频率下的奖励对比

针对区块链机制的高效性，我们设计了所提出的 L-dBFT 与 PBFT 共识机制及原始 dBFT 共识机制的对比。从图 11 中可以看出，随着训练步数的增加，时延都逐渐降低，最后趋于稳定。可以发现，本文中所提出的基于多目的地卸载的 L-dBFT 机制的时延低于 PBFT 和 dBFT，显著降低了区块链共识过程的通信开销，这也证明了其更适用于时延敏感的工业互联网。

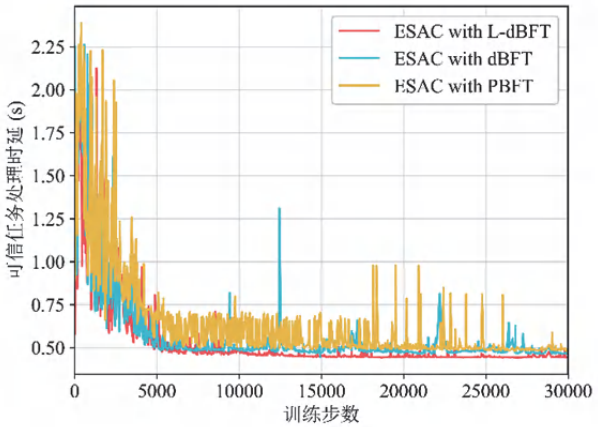


图 11 不同区块链机制的时延对比

6 总结

为解决工业互联网中多终端、多边缘服务器场景下多样工业任务的可信协同处理问题，本文提出了一种基于轻量级区块链机制的端边协同计算网络模型和深度强化学习的调度优化算法。首先，设计了一种轻量级区块链机制L-dBFT，显著降低了系统开销。其次，构建了可信任务处理时延最小化模型，旨在考虑计算资源、任务截止日期和区块链稳定性等约束条件的同时，联合优化任务卸载比例、计算资源分配和区块生成间隔。最后，本文采用马尔可夫决策过程对问题进行建模，并提出了基于最大熵和优先经验回放机制的ESAC算法来求解最优调度策略。广泛的实验结果表明，所提出的方法在确保网络可信度的同时，显著提高了任务处理性能，减少了51.22%的任务处理时延，验证了其高效性。

参考文献：

[1] HUO R, ZENG S, WANG Z, 等. A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges[J]. IEEE Communications Surveys and Tutorials, 2022, 24(1): 88-122. DOI:10.1109/COMST.2022.3141490.

[2] POULARAKIS K, LLORCA J, TULINO A M, 等. Joint service placement and request routing in multi-cell mobile edge computing networks[C]//IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. 2019:. DOI:10.1109/INFOCOM.2019.8737385.

[3] CHAI Z Y, ZHAO Y J, LI Y L. Multitask computation offloading based on evolutionary multiobjective optimization in industrial internet of things[J]. IEEE Internet of Things Journal, 2024, 11(9): 15894-15908. DOI:10.1109/JIOT.2024.3349609.

[4] LIU M, YU F R, TENG Y, 等. Performance optimization for blockchain-enabled industrial Internet of things (IIoT) Systems: a deep reinforcement learning approach[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3559-3570. DOI:10.1109/TII.2019.2897805.

[5] DAI Y, XU D, ZHANG K, 等. Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4312-4324. DOI:10.1109/TVT.2020.2973705.

[6] WANG X, ZHU H, NING Z, 等. Blockchain intelligence for Internet of vehicles: challenges and solutions[J]. IEEE Communications Surveys & Tutorials, 2023, 25(4): 2325-2355. DOI:10.1109/COMST.2023.3305312.

[7] AKHLAQI M Y, MOHD HANAPI Z B. Task offloading paradigm in mobile edge computing-current issues, adopted approaches, and future directions[J]. Journal of Network and Computer Applications, 2023, 212: 103568. DOI:10.1016/j.jnca.2022.103568.

[8] YUAN L, HE Q, TAN S, 等. CoopEdge+: enabling decentralized, secure and cooperative multi-access edge computing based on blockchain[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(3): 894-908. DOI:10.1109/TPDS.2022.3231296.

[9] YUAN L, HE Q, TAN S, 等. CoopEdge: a decentralized blockchain-based platform for cooperative edge computing[C]//Proceedings of the Web Conference 2021. New York, NY, USA: Association for Computing Machinery, 2021: 2245-2257. DOI:10.1145/3442381.3449994.

[10] 许驰, 唐紫萱, 金曦, 等. 基于李雅普诺夫优化和深度强化学习的多任务端边迁移[J]. 控制与决策, 2024, 39(7): 2457-2464. DOI:10.13195/j.kzyjc.2023.1243.

[11] 田琳琳, 李萌, 司鹏搏, 等. 基于边缘计算与区块链的车载计算资源智能调度研究[J]. 高技术通讯,

2023, 33(4): 390-401.

[12] LANG P, TIAN D, DUAN X, 等. Blockchain-based cooperative computation offloading and secure handover in vehicular edge computing networks[J]. IEEE Transactions on Intelligent Vehicles, 2023, 8(7): 3839-3853. DOI:10.1109/TIV.2023.3271367.

[13] MOGHADDASI K, RAJABI S, GHAREHCHOPOGH F S. Multi-objective secure task offloading strategy for blockchain-enabled IoV-MEC systems: a double deep Q-network approach[J]. IEEE Access, 2024, 12: 3437-3463. DOI:10.1109/ACCESS.2023.3348513.

[14] FAN W, HAO Z, TANG B, 等. Resource matching for blockchain-assisted edge computing networks[J]. IEEE Internet of Things Journal, 2024, 11(8): 14460-14471. DOI:10.1109/JIOT.2023.3342439.

[15] NGUYEN D C, DING M, PATHIRANA P N, 等. Cooperative task offloading and block mining in blockchain-based edge computing with multi-agent deep reinforcement learning[J]. IEEE Transactions on Mobile Computing, 2023, 22(4): 2021-2037. DOI:10.1109/TMC.2021.3120050.

[16] DU X, CHEN X, LU Z, 等. A blockchain-assisted intelligent edge cooperation system for IoT environments with multi-infrastructure providers[J]. IEEE Internet of Things Journal, 2023, 10(24): 21227-21239. DOI:10.1109/JIOT.2023.3282954.

[17] CUI L, CHEN Z, YANG S, 等. A secure and decentralized DLaaS platform for edge resource scheduling against adversarial attacks[J]. IEEE Transactions on Computers, 2024, 73(3): 631-644. DOI:10.1109/TC.2021.3074806.

[18] XU C, TANG Z, YU H, 等. Digital twin-driven collaborative scheduling for heterogeneous task and edge-end resource via multi-agent deep reinforcement learning[J]. IEEE Journal on Selected Areas in Communications, 2023, 41(10): 3056-3069. DOI:10.1109/JSAC.2023.3310066.

[作者简介]

张培风 (2000-)，女，硕士，从事工业无线网络、人工智能、边缘计算、区块链等研究，E-mail: zhangpeifeng1@sia.cn;

许驰 (1987−)，男，研究员，博士，从事工业控制系统、工业无线网络、5G、边缘计算等研究，E-mail: xuchi@sia.cn;

FCLA-DT: Federated Continual Learning with Authentication for Distributed Digital Twin-based Industrial Internet of Things

Yingjie Xia, Xuejiao Liu, Yunxiao Zhao, Yun Wang

Abstract* — Digital Twin (DT) technology is currently pervasive in industrial IoT applications, notably in predictive maintenance scenarios. Prevailing digital twin-based predictive maintenance methodologies are constrained by a narrow focus on singular physical modeling paradigms, impeding comprehensive analysis of diverse factory data at scale. This paper introduces an improved method, federated continual learning with authentication for distributed digital twin-based industrial internet of things (FLCA-DT). This decentralized strategy ensures the continuous learning capability vital for adaptive and real-time decision-making in complex industrial predictive maintenance systems. A group signature based authentication scheme is introduced to enable the verification of digital twin identities during inter-twin collaborations, avoiding unauthorized access and potential model theft. Security analysis shows that FLCA-DT can enable numerous nodes to collaborate learning without compromising individual twin privacy, thereby ensuring group authentication in the cooperative distributed industrial internet of things. Performance analysis shows that FCLA-DT outperforms traditional federated learning methods with over 95% fault diagnosis accuracy and ensures the privacy and authentication of digital twins in multi-client task learning.

***Keywords* — federated continual learning, authentication, group signature, digital twin, industrial internet of things**

I. INTRODUCTION

Digital twin is now often utilized in product lifecycle management processes like predictive maintenance as Industry 5.0 develops. By incorporating real-time environmental data and sensor data, including temperature and vibration, the program takes a proactive approach to asset management services by updating the digital twin model. The development of digital twin-based predictive maintenance (DT-PdM), which has applications in many industries including manufacturing and aerospace [2], [3]. Most of existing DT-PdM methodologies are primarily on the single physical modeling, which results in insufficient investigation of different data in the physical field [4].

As shown in Figure 1, it becomes an urgent need to interconnect and integrate massive environmental data from many physical entities in distributed factories for global manufacturing.

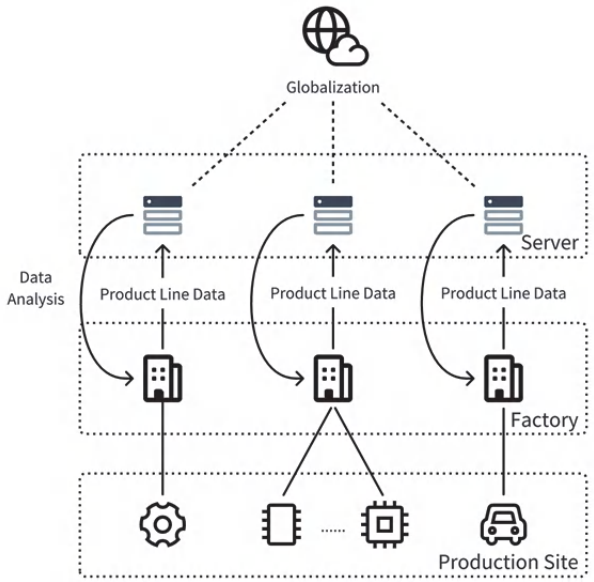


Figure 1　Global manufacturing

Digital twin is a virtual representation of the elements and dynamics of a physical system [5]. It leverages techniques like machine learning and data analytics to comprehensively model and understand the system's dynamics. There exists numerous challenges in implementing large scale digital-twin based predictive maintenance. Firstly, it is costly to process the above data using cloud/edge which requires a huge amount of network bandwidth and has high latency and energy consumption. More

importantly, it causes vital privacy concerns about the data from different physical systems. Sensitive production data is involved in each system, while processing the data on the untrusted server may increase the potential risk of data leakage. If the data is not appropriately secured, an attacker may be able to obtain sensitive information to infer the system, such as the production of a specific factory.

Furthermore, the digital twin-based predictive maintenance allows for efficient information aggregation across large physical/virtual entities, free data sharing, and dynamic mission coordination through the interconnection of gigantic physical entities and their virtual twins through inter-twin communications. When storing and distributing the developed machine learning models for the cloud/edge server of participating entities during inter-twin collaboration, there is a possibility of theft [6]. How to ensure secure communication between the inter-twins to authenticate the valid entities becomes an important issue, especially during the distributed machine learning. Moreover, it holds significant importance for large scale distributed system applications with stringent real-time requirements, including robot control, process monitoring, and automation tasks [7].

To address these challenges, we propose to employ federal continuous learning to ensure that sensitive data processed locally, while the local model parameter updates are transmitted to the server to reduce raw data transmission. Meanwhile, we propose group authentication scheme to authenticate the digital twins. The contributions can be summarized as follows.

(1) We propose a group signature based authentication scheme in digital twin-based predictive maintenance, to ensure the valid identity of different digital twin for aggregation.

(2) We propose federated learning model for large scale digital twin-based predictive maintenance, to avoid data leakage among large scale co-production factories for data sharing.

(3) We propose to combine continuous learning in federated learning to support multiple tasks and ensure the real-time data generated for learning.

II. RELATED WORK

In the section, we will present the related work about the security issues of digital twin-based industrial internet of things and the security technologies.

A. Digital Twin-based Industrial Internet of Things

Digital twin utilizes physical models and historical data to replicate the lifecycle of assets and systems. Its bidirectional, real-time link between the physical and virtual domains facilitates tracking, prediction of system behavior, and resource optimization, thereby augmenting manufacturing efficiency and informing strategic decisions [8]. Therefore, digital twin was pivotal in industrial internet of things [9]. A digital twin-driven method was presented by Zhang et al. to execute rolling bearing fault diagnostics in the absence of enough training data [10]. Rolling bearing twins were set up to produce simulated data. After that, a transformer-based network was constructed and simulated for fault diagnosis.Hu et al. proposed a masked one-dimensional convolutional autoencoder (MOCAE) based on digital twin for bearing defect diagnostics [11] .

B. Privacy Preserving Security Technologies in Digital Twin-based Industrial Internet of Things

There raises vital security issues in the process of machine learning for digital twin-based industrial internet of things, such as data leakage, privacy leakage, identity theft and so on [12].

In the digital twins-based industrial internet of things, how to ensure the data security in data sharing is of great significance. Qu et al. proposed a privacy-protecting local model training scheme that uses generative adversarial networks to enhance differential privacy[13], ensuring optimal data utility while achieving strict differential privacy protection. Wang et al. proposed a data sharing scheme[14] based on the design of knowledge protocol signature and smart contract algorithm, so that vehicles can flexibly impose conditions on data sharing according to specific needs. Shen et al. proposed a framework for secure big digital twin data (BDTD) [15]. The framework proposed that hashes and transaction records of BDTD

bare stored in the blockchain, and BDTD was encrypted and stored in the cloud to achieve the requirements of exponential growth and timely sharing of BDTD.

Authentication is the important protocol to avoid privacy leakage and identity theft in digital twin based industrial internet of things. Gautam et al. proposed a protocol for intra-twin authentication and inter-twin authentication in the networked vehicle environment. This scheme was based on blockchain technology and uses elliptic curve cryptography (ECC) , which realized reliable mutual authentication between the vehicle and the twin and between the twins to ensure secure communication [16]. Chen et al. proposed an authentication mechanism deployed in the digital twin autonomous vehicle environment. This mechanism used bilinear mapping technology for initialization and encryption and decryption, and realized mutual authentication between the user and the twin, as well as between the autonomous vehicle and the twin [17]. Aggarwal et al. proposed a cloud-based digital twin platform security authentication scheme that used blockchain integration and bilinear mapping technology to ensure the verifiable and security of data [18]. Xu et al. proposed a secure in-twin authentication and inter-twin authentication vehicle-mounted digital communication architecture, which used bilinear mapping to design the authentication process to ensure digital twin communication security and facilitate information sharing [19]. Patel et al. proposed a user authorization privacy protection identity authentication protocol based on decentralized identifier (DID) and verifiable credential (VC), which realized the user's complete control over their identity and privacy protection [20].

The above authentication schemes do not take into account the simultaneous authentication of multiple digital twins. While with real-time data integration, how to perform efficiently authenticate for multiple digital twins becomes an urgent issue.

C. Learning Technologies in Digital Twin-based Industrial Internet of Things

Since inter connected devices in industrial internet of things systems grows rapidly, the performance of applications is strongly associated with big data analysis. As artificial intelligence evolves, data-driven predictive maintenance approaches have gained widespread application across diverse industrial settings, particularly excelling in bearing fault diagnostics.

In the practical industrial scenario, collaborative learning technologies have been paid much attention, in which data are collected from different collaborators, and then perform collaborative learning. It raises serious data privacy problems. Therefore, federated learning(FL) scheme was proposed, in which data owners can keep their data locally and upload their training knowledge to a trusted central server during collaborative training process. Zhang et al. [21] proposed a federated learning method to provide the conditions for monitoring requirements for the assessment of the equipment, but the changeable data in production scenario was not considered. Wang et. al [22] proposed a method to reduce the impact of low-quality data. Zhang et al. [23] and Chen et al. [24] introduced federated transfer learning to resolve data differences problems. Wang et al. [25] proposed an adversarial domain generalization network to improve model performance, but problems of knowledge preservation through continual learning process still remains unsolved in those methods.

In summary, learning methods have been widely used in fault diagnosis. However, problems brought by multiple clients and tasks are still not satisfied in most methods.

III. SYSETM MODEL

In this section, as illustrated in Figure 2, the architectural framework of our proposed FCLA-DT scheme, specifically designed for for large scale distributed digital twin-based industrial internet of things. The industrial physical network's foundational data acquisition stratum encompasses a plethora of hardware, encompassing mechanical assemblies, bearing systems, microchips, sensor arrays, and motor units. The signals collected by these devices will be transmitted to the data analysis storage layer. In this layer, digital twins are generated, and the data is

received and stored in the digital twin. This systematic approach facilitates a holistic, real-time representation and analysis of physical assets, pivotal for advanced monitoring and predictive maintenance strategies.

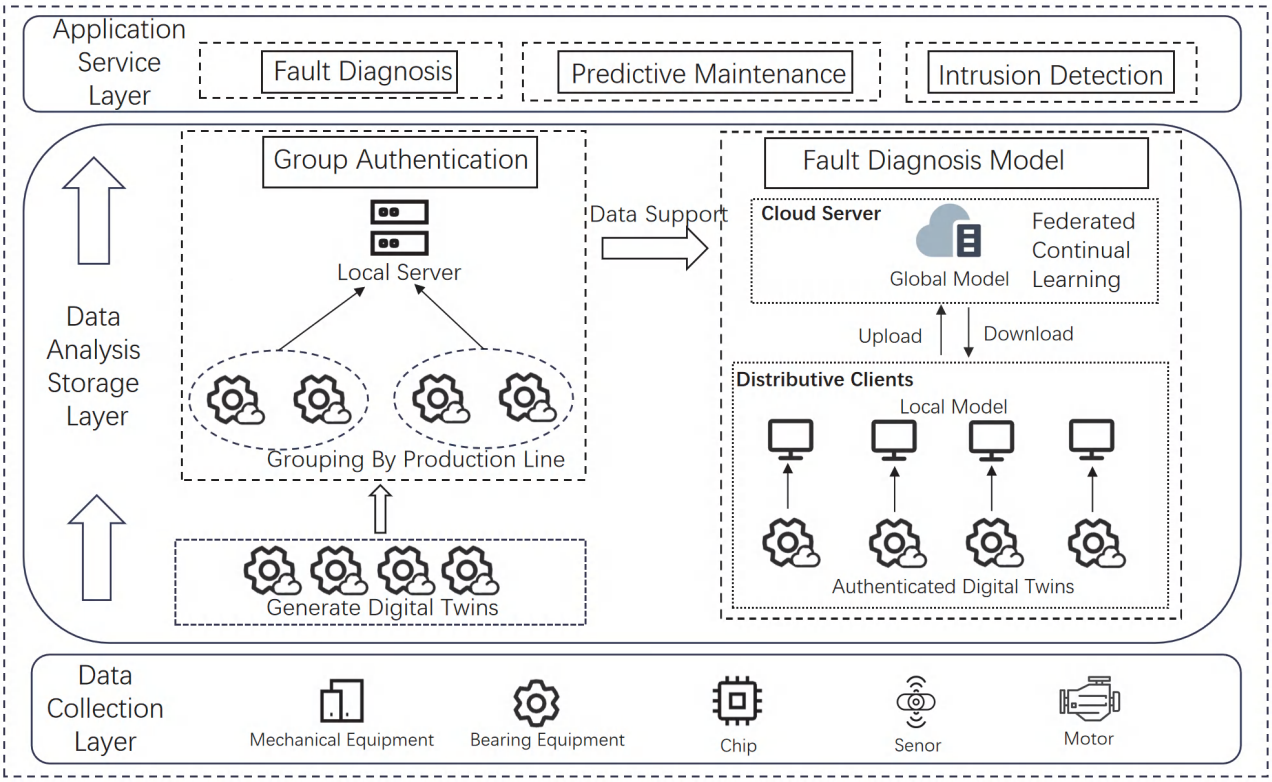


Figure 2 System model of FCLA-DT

The twins will also undergo group authentication, after which the certified twins upload data locally and are trained using federated continuous learning methods and upload parameters.

The global model aggregates these parameters, saves them, and updates them to the local model. At the application service layer, there are fault diagnosis, environmental monitoring, intrusion detection, predictive maintenance of equipment and other operations to manage and maintain plant equipment.

IV. PROPOSED SCHEME

In this section, we present our proposed scheme FCLA-DT in details, which mainly includes two parts, inter-twin authentication based on group signature and federal continuous learning in bearing diagnosis.

In our experiment, we take rolling bearings of rotating equipment for fault diagnosis in large scale factories as an example. As shown in **错误!未找到引用源。**, our system model includes six roles, namely cloud server, distributive clients, local model, local sever, bearing DTs and bearing equipment. Each bearing equipment takes machine learning to train their owner predicative data, and communicates with the bearing DTs, each DT needs to be authenticated and support data for local model. Then local model uploads their parameters and aggregate it at the global model.

A. Inter-twin Authentication based on Group Signature

In order to ensure the secure transmission and storage of bearing data, we propose a group authentication scheme based on digital twins. The scheme requires the bearing to send a registration request to the local server before accessing the system, and after successful verification, the local server will generate a unique public and private key for each bearing as its authentication credentials in the network. In the group authentication stage, we group bearings according to their digital twins in different production lines, and authenticate them based on identity information. This approach can not only improve authentication efficiency, but also can help to achieve

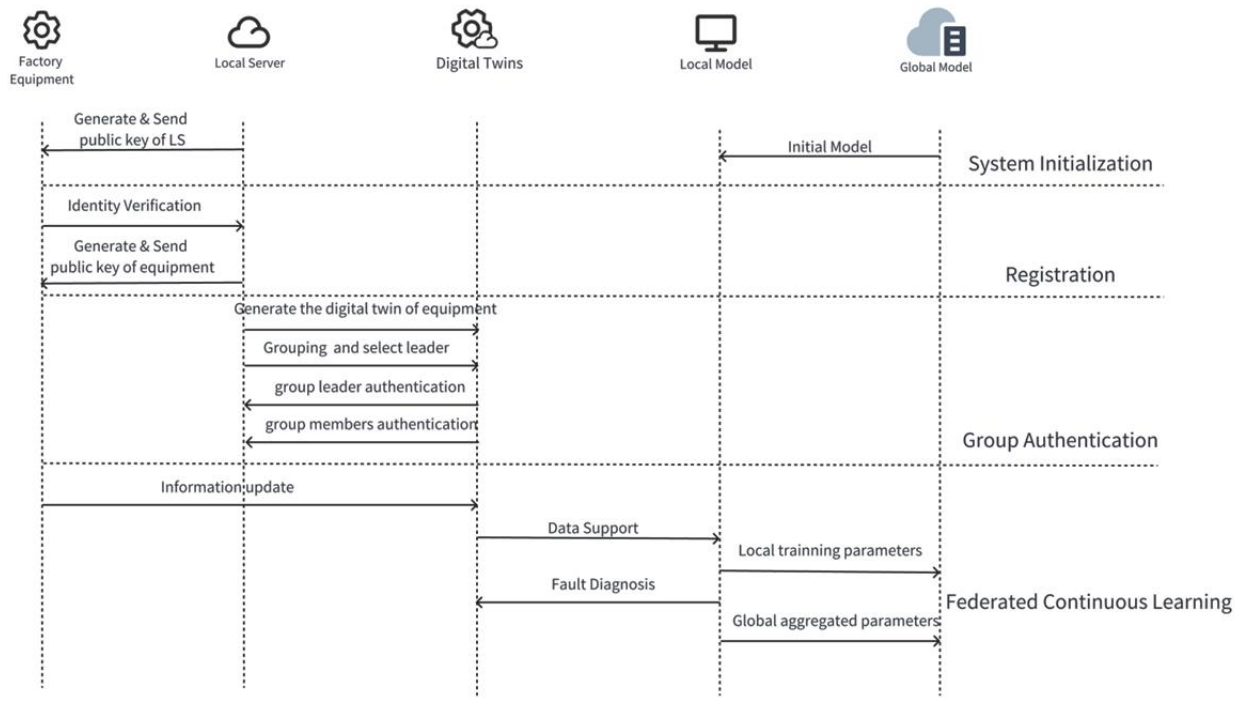


Figure 3　The flow chart of FCLA-DT

granular permission management and data access control. This section mainly consists of the following three parts: system initialization, bearing registration and group authentication. Table Ⅰ contains a list of the notations used in the suggested scheme..

Table Ⅰ　Notations and descriptions

Symbol	Description
LS	Local sever
B_i	Bearing
DT_i	DT of B_i
ID_i	True identity of B_i
RID_i	Pseudo identity of B_i
LN_i	Line number of B_i
PK_{LS}	Public key of LS
s_{LS}	Private key of LS
pp_i	Partial private key of B_i
PK_i	Public key of B_i
Na_i	Number of authentication attempts of B_i
T_i	Current system timestamps
$\|\|$	Concatenation operation

1) System Initialization

In this phase, the Local Server (LS) is responsible for system initialization.

Step 1: To initiate the protocol, the LS selects a non-singular elliptic curve, $y^2 = x^3 + ax + b(\mathrm{mod}\ p)$, over $GF(p)$, ensuring $4a^3 + 27b^2 \neq 0\ (\mathrm{mod}\ p)$. A base point $P \in E_p(a, b)$ is then picked to generate an additive cyclic group E_g of prime order q, optimized to be maximally large yet below p.

Step 2：The LS selects $s_{LS} \in Z_p^*$ as its master key and generates the public key $PK_{LS} = s_{LS} \cdot P$.

Step 3：The LS chooses the collision- resistant one-way cryptographic hash function $H: (0,1)^l \rightarrow Z_p^*$.

Step 4: LS make$\{Ep(a, b), p, P, Eg, PK_{LS}, H(\cdot)\}$as the public system parameters.

2) Bearing Registration

The bearings are required to register with LS as follows:

Step 1: The bearing B_i first selects the identity ID and a random number $r_i \in Z_p^*$. And then calculates the $RID_i = H(ID_i||r_i)$ for each bearing and sends the

registration request {RID} to LS.

Step 2: The LS generates a random secret s_i, and computes $R_i = s_i \cdot P$ and $h_i = H(RID_i||R_i)$ for B_i. Then the LS generates the private key as $pp_i = s_i + s_{LS} * h_i (\mathrm{mod}\ p)$ and send $\{pp_i, R_i\}$ to B_i.

Step 3: When the Bearing B_i receives the message $\{pp_i, R_i\}$, the public key is set as $PK_i = pp_i \cdot P$ if the condition $pp_i \cdot P = R_i + H(RID_i||R_i) \cdot PK_{LS}$ is met. Finally The LS deletes s_i from its database.

3) Group Authentication

After registration is complete, the local server (LS) groups all digital twins (DTs) according to the different production lines to which the bearings belong. After the grouping succeeds, LS compares the generation time of each DT in the group and selects the DT with the earliest generation time as the group leader. Then each DT selected as the leader sends the authentication information to the LS, and after the LS authentication is complete, the DT becomes the HDT. After the election is successful, other group members send authentication messages to the next DT in turn, and the next DT receives the messages and authenticates until the authentication messages are transmitted to the HDT.

Step 1: The DT_i that have been elected as the group leader selects current timestamp T_i. At the same time The DT_i generates a random number $x \in Z_p^*$ and computes:

$$X_i = H(ID_i||x||Na_i||T_i) \cdot P \quad (1)$$

$$Y_i = H(LN_i||ID_i||Na_i||T_i) \cdot PK_i \quad (2)$$

then it makes a signature as: $\delta_i = H(ID_i||x||Na_i||T_i) + pp_i * H(X_i||Y_i||T_i||RID_i)(\mathrm{mod}\ p)$. (3)

After calculating these parameters, the DT_i sends $\{X_i, Y_i, \delta_i, T_i, RID_i\}$ to the DT_{LS}.

Step 2: Upon receiving the $\{X_i, Y_i, \delta_i, T_i, RID_i\}$, the DT_{LS} generates the current timestamp T_i'. If $|T_i' - T_i| \leq \Delta T$, the timestamp T_i is proven valid, otherwise the message is discarded. If valid, the DT_{LS} will verifies the validity of signature. It computes if

$$\delta_i \cdot P = H(X_i||Y_i||T_i||RID_i) \cdot PK_i + X_i. \quad (4)$$

On verifying the validity of signature , It has been verified that this DT_i is authorized to head the group.

Step 3: The prior DT simultaneously sends the authentication data to the next DT during group authentication, and so on, until the DT_n sends the data to the leader.

DT_i selects $r_i \in Z_p^*$, and generates current timestamp T_i, calculates its generation time GT_i. The DT_i computes

$$X_i = H(ID_i||GT_i||LN_i||T_i) \cdot P \quad (5)$$

$$Y_i = H(ID_i||r_i||GT_i||LN_i) \cdot PK_{i+1} \quad (6)$$

then it makes a signature as:

$$\delta_i = H(ID_i||GT_i||LN_i||T_i) + pp_i * H(X_i||Y_i||T_i||RID_i)(\mathrm{mod}\ p). \quad (7)$$

At last, DT_i sends $\{X_i, Y_i, T_i, \delta_i, RID_i\}$ to DT_{i+1}.

Step 4: Upon receiving the $\{RID_i, X_i, Y_i, \delta_i, T_i\}$ from DT_i, the DT_{i+1} generates the current timestamp at T_i'. And then it checks for validity for timestamp T_i by $|T_i' - T_i| \leq \Delta T$. Meanwhile, the LN_i of DT_i also needs checked. If the timestamp and the line number are valid, the DT_{i+1} verifies the δ_i as:

$$\delta_i \cdot P = H(RID_i||X_i||Y_i||T_i) \cdot PK_{i+1} + X_i \quad (8)$$

B. Federated Continuous Learning in Bearing Diagnosis

To provide data privacy and aggregate knowledge from multiple sources, we propose a federated continual learning algorithm based on private digital twin datasets. This scheme raises a global model on server to aggregate local parameters of clients by

weighted average. Then global server sends aggregated global parameters to each client to update their local model. The local model makes a combination of global, task-based and historical parameters to better fit current tasks, and upload new parameters after a round of training. This approach improves diagnosis performance, and provides data privacy protection and adaptation to new tasks. We summarize this scheme into four steps.

Step 1. Initialization: An initial global model is built on the cloud server and also sent to clients as initial local models.

Step 2. Local training: Clients use their data of digital twins to improve local models and send the gradients of parameters to server.

For a specific client with private data source, the deep learning model is assumed to minimize the empirical classification error measured by cross-entropy loss function:

$$L = -\frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{N}[y_i = j]\log\frac{p_{i,j}}{\sum_{j=1}^{N} p_{i,j}} \tag{9}$$

While n denotes the size of input data- set, N denotes the number of categories of bearing health states, y_i refers to the label of *i*th input data sample, and $p_{i,j}$ denotes the probability of sorting *i*th sample into label j. Clients upload the gradients of parameters as long as completing training process, which can be defined as $B^t \odot m^t$, while B^t is the set of base parameters of current task t and m^t denotes a set of sparse vector masks.

Step 3. Global aggregation: Global model aggregates local parameters by computing a weighted average of them, and sends the global parameters θ_G to every client. The weighted aggregation can be defined as follows:

$$\theta_G = \frac{1}{C}\sum_C \widehat{B_C^t} \tag{10}$$

Step 4. Local update: Clients update their local models by selectively combine global parameters and their task-based local parameters. First, Local parameters can be defined as:

$$\theta^t = B^t \odot m^t + A^t + \sum_{i\in C_{\setminus c}}\sum_{j<|t|} \alpha_{i,j}^t A_i^j \tag{11}$$

Where A denotes task-adaptive sparse parameters. Cloud central server saves all the task-adaptive parameters and send a random subset to every client per task, and clients selectively learn from them by taking α-weighted aggregation.

Simply let $B^t = \theta_G$ while updating local parameters and then learn new training parameters θ_t by minimizing target function as follows:

$$\underset{B^t, m^t, A^{1:t}, \alpha}{\text{minimize}}\ L(\theta^t) + \lambda_1\ \Omega(\{m^t, A^{1:t}\})$$

$$+ \lambda_2 \sum_{i=1}^{t-1} ||\Delta B^t \odot m^i + \Delta A^i||_2^2 \tag{12}$$

While L denotes the loss function mentioned above and Ω is a sparsity-inducing regularization term, ΔB^t is the difference between the latest base parameter and the current parameter and ΔA^i is the difference between task-adaptive parameters of former task and the current one. Step 2 to 4 will be repeated until the client decide not need the model anymore.

V. SECURITY ANALYSIS

Our proposed FCLA-DT scheme can avoid data leakage among distributed co-production factories for data sharing and ensure real-time data federal continuous learning in multi-client task learning. To show the advantages of FCLA-DT scheme in industrial internet of things, we compare it with existing schemes as follows.

Gautam et al. **错误!未找到引用源。** proposed a blockchain-based mutual authentication protocol. Chen et al. **错误！未找到引用源。** proposed a privacy-preserving authentication mechanism based on bilinear pairing deployed in digital-twin-enabled autonomous vehicle environments. Aggarwal et al. **错误!未找到引用源。** introduced a secure authentication scheme based on bilinear pairing for cloud-based DT platforms.

Eren et al. [27] used CNN classifier to implement a generic intelligent bearing fault diagnosis system.The model was retrained every task with data of current task on one client (using CNN for short for performance comparison). McMahan et al. [28]

proposed a widely used FL algorithm as FedAvg. It aggregated all the local parameters by taking an average of them. This method was applied under the same parameter settings as the proposed method. Zenke et al. [29] proposed continual learning (CL), an individual continual learning method. Each client trained on local task sequence without knowledge sharing.

The comparative results are presented in Table Ⅱ.

1) DT Authentication: For the authentication scheme and our scheme in digital-based industrial internet of things, they all provide DT authentication between digital twins and their physical entities.

2) Group Authentication: In terms of the simultaneous authentication of multiple twins, our scheme adopts the group authentication mode of key pair authentication. However, Gautam et al. [16], Chen et al. [17] and Aggarwal et al. [18] only proposed the authentication scheme of a single digital twin, and did not elaborate the simultaneous authentication of multiple digital twins.

Table Ⅱ Security analysis by comparing FCLA-DT with other schemes

Scheme	Gautam 错误!未找到引用源。	Chen 错误!未找到引用源。	Aggarwal 错误!未找到引用源。	CNN[27]	FedAvg[28]	CL[29]	FCLA-DT
DT Authentication	√	√	√	—	—	—	√
Group Authentication	×	×	×	—	—	—	√
Mutual Authentication	—	—	—	×	√		√
Client Cooperation	—	—	—	×	√	×	√
Privacy Preservation	—	—	—	√	√	√	√
Continuous Data	—	—	—	×	×	√	√

1) Mutual Authentication: In terms of mutual communication between different source domains, the CNN and CL method is limited by the limited data capacity and the difference in distribution. In contrast to the FedAvg algorithm, which integrates knowledge from multiple source domains to generate a more generalized application model, our scheme is based on a federated continuous learning approach that allows models to be trained collaboratively from local data from multiple actors, allowing for mutual communication.

2) Client Cooperation: The CNN and CL method trains in a local environment without communication among clients. Our scheme uses federated continual learning method to enable cooperation among clients for distributive learning. The FedAvg algorithm also provides distributive learning resources.

3) Privacy Preservation: Our scheme used federated continual learning method to realize privacy protection and data sharing. The CNN, FedAvg and CL algorithm also maintain the privacy of their respective data.

4) Continuous Data: When dealing with changeable datasets, the CNN and FedAvg model usually assumes that the data distribution is stable, and the CL algorithm cannot adapt to multi-client learning. Our proposed scheme uses federated continuous learning to extract shared features from multiple clients with variable data sets.

In the context of large-scale factory bearing fault diagnosis in industrial internet of things, collaboration

or communication among multiple clients is often required. Therefore, ensuring security of information assets for participants in collaborations is crucial, especially concerning data privacy and identity authentication. As factories evolve, more bearing fault diagnosis tasks may emerge. This demands that application models not only support multiple clients cooperation, but also protect their data privacy and adapt to evolving tasks. Common fault diagnosis method like CNN cannot apply to the current production environment. The FedAvg scheme considers only client data privacy under multi-client cooperation. The CL method can adapt to new tasks, but ignored communication between clients. Our proposed FCLA-DT introduces federated continual learning to support multi-client collaborative learning for fault diagnosis, which ensures client data privacy and adaptability to new tasks through distributed task-driven algorithm.

VI. PERFORMANCE ANALYSIS

A. Experimental Settings

To evaluate the performance of our proposed FCLA-DT, we do fault diagnosis experiments under different configurations. We use the CWRU dataset [26], a widely appreciated rolling bearing dataset from the Case Western Reserve University, including four bearing health states: Normal state, ball fault, inner race fault and outer race fault. The faults are seeded on rolling elements running at constant speed for motor loads of 0 to 3 horsepower. The range of fault diameter includes 0.007, 0.014, 0.021 and 0.028. The sample rates were 12kHz and 48kHz. We use part of this dataset ranging in the formal three types of diameter and 12kHz sample rate. We split the classes into 6 non-iiD tasks, each of which contains four different bearing states, that are disjoint from each other. Then we send them in random orders to support current training task.

B. Model Training Efficiency

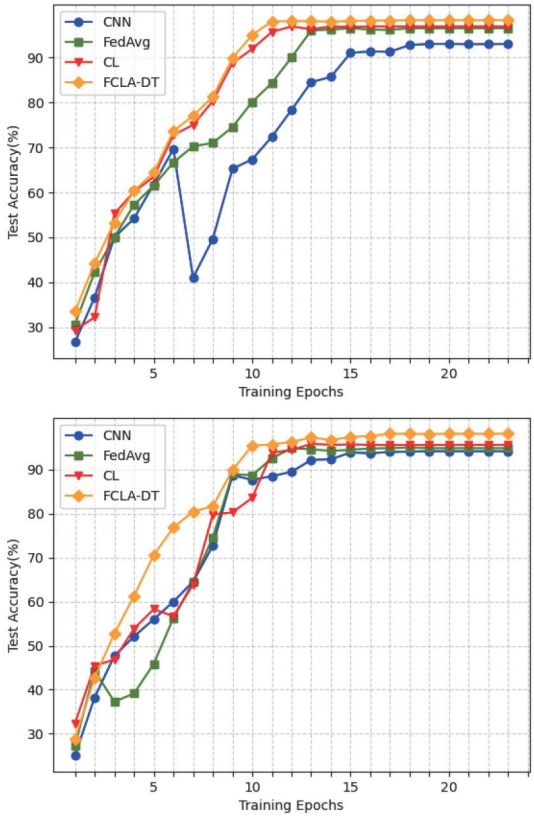


Figure 4　Learning process in two tasks, taking the first client as representative.

Figure 4 illustrates the learning progress of clients by using two tasks as test datasets. It’s evident that our method achieves stable accuracy with fewer epochs compared to other methods, indicating faster convergence and highlighting the efficiency advantage of our approach. Compared to FedAvg, it reveals that leveraging past task parameters enhances model efficiency and accelerates model convergence in subsequent tasks. Moreover, FCLA-DT outperforms the CL method, which demonstrates the positive impact of knowledge sharing from diverse tasks among clients on current task learning. In conclusion, our efficiency advantage can be attributed to inter-client knowledge transfer and learning from previous tasks.

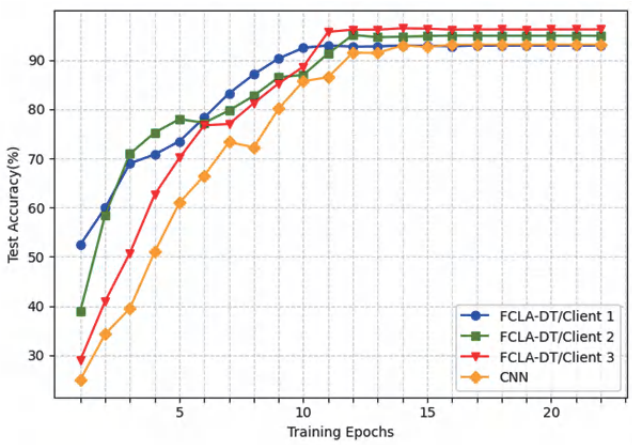


Figure 5 Learning process in the first task

As our model deals with new tasks continually, Figure 5 measures the adaptation of past tasks after learning all tasks in different clients of our FCLA-DT, compared with CNN performance. Better adaptation appears at the beginning epochs, and clients after several rounds of training convergence faster than untrained CNN. This can well reflect the severity of catastrophic forgetting of the model after training several tasks. Due to knowledge acquisition from irrelevant tasks, the final accuracy of old tasks might decrease. As shown in Figure 5, catastrophic forgetting won't happen in our proposed method. The accuracy has only slightly decreased, but still shows better performance than CNN without knowledge transfer.

C. Computation Cost

We evaluate the performance of the authentication protocol. Some notations of the running time are specifically listed as follows. T_{bp}: Time of a bilinear pairing operation. $T_{ecc_{sm}}$: Time of a scalar multiplication to the ECC. T_{sin}: Time of a signature of elliptic curve digital signature. T_{ver} : Time of a verification of elliptic curve digital signature. T_{bcq}: Time of a query operation on the blockchain.

Table Ⅲ Computation cost by comparing FCLA-DT with other schemes

Scheme	Single DT authentication		Multiple DTs authentication (n DTs)
	DT	Server/Physical entity	
Gautam et al.错误!未找到引用源。	$3T_{ecc_{sm}}+T_{bcq}+T_{sin}$	$3T_{ecc_{sm}}+T_{ver}$	$6nT_{ecc_{sm}}+nT_{sin}+nT_{ver}+2nT_{bcq}$
Chen et al.错误!未找到引用源。	T_{bp}	T_{bp}	$6nT_{ecc_{sm}}+2nT_{bp}$
Aggarwal et al.错误!未找到引用源。	$4T_{ecc_{sm}}+2T_{bp}$	$4T_{ecc_{sm}}$	$4nT_{ecc_{sm}}+nT_{bp}$
FCLA-DT	$2T_{ecc_{sm}}+T_{ecc_{pa}}+T_{sin}$	$2T_{ecc_{sm}}+T_{ecc_{pa}}+T_{ver}$	$4nT_{ecc_{sm}}+2nT_{ecc_{pa}}+nT_{sin}+nT_{ver}$

To demonstrate the efficiency of proposed scheme, we choose several existing authentication schemes to compare. As shown in Table Ⅲ, for the digital twin needs to authenticate in intra-twin communication, it needs $2T_{ecc_{sm}}+T_{ecc_{pa}}+T_{sin}$ in our scheme. For the server or the physical entity, it needs $2T_{ecc_{sm}}+T_{ecc_{pa}}+T_{ver}$ in our scheme. Our scheme is more efficient when single digital twin needs to authenticate.

If there are multiple digital twins need to authenticate, we employ group authentication, thus it needs $4nT_{ecc_{sm}}+2nT_{ecc_{pa}}+nT_{sin}+nT_{ver}$, it is more efficient when multiple digital twins need to authenticate.

D. Diagnosis Accuracy

Figure 6 shows the total accuracy of our FCLA-DT and comparing models on the mentioned non-iiD task sequences. Three clients are set in both FCLA-DT and FedAvg to simulate cooperative scenario, all of which is trained with 6 tasks in different random order. The accuracy of each task is calculated independently, and averaged as model evaluation indices. It can be observed that FCLA-DT performs better than other methods in multi-task scenario. The CNN method obtains the lowest accuracy in all tasks due to the limited size of training sample. Our method also achieves higher performance comparing with FedAvg in every different experiments. The comparison validates that our method can improve training performance by sharing knowledge with other

clients, and learning from historical tasks.

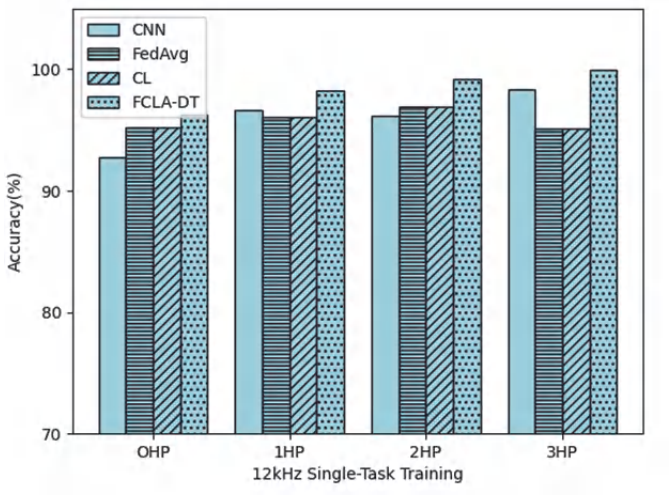


Figure 6　Total accuracy in multi-task training

Figure 7 shows the confusion matrixes for FCLA-DT and FedAvg on the test dataset after training the whole task sequences on FCLA-DT and training across the last parallel tasks on FedAvg clients. FedAvg cannot classify classes not included in the training tasks. In contrast, FCLA-DT recognizes all classes and achieves higher accuracy beacuse it continually gains and retains knowledge throughout all previously learned tasks. In summary, FCLA-DT demonstrates superiority in multi-task learning by continuously learning and accumulating knowledge, enabling it to memorize all classes learned and provide assistance for future training.

Through multi-task continual training, the proposed federated continual learning method extracts shared features from multiple clients with different tasks of changeable datasets and privacy consideration. The knowledge learned from data of different tasks at different clients can be well shared without privacy concern, with fast adaptation to new task and less likely forgetting.

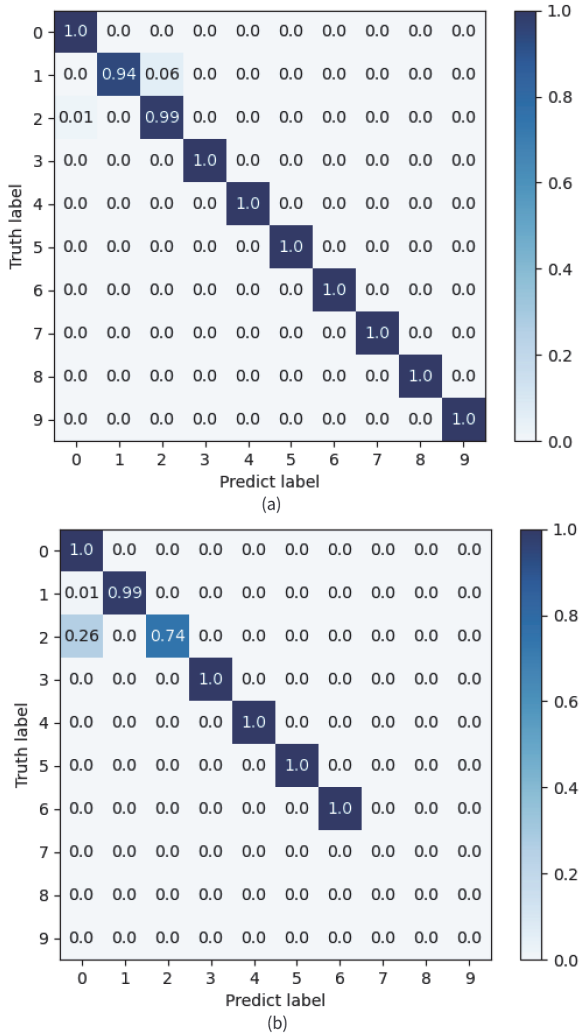


Figure 7　(a) Confusion matrix of FCLA-DT

(b) Confusion matrix of FedAvg

VII. CONCLUSION AND FUTURE WORK

In this paper, we have introduced a bearing fault detection model leveraging federated continual learning (FCLA-DT) for industrial internet of things. The model avoids the pitfalls of centralized data processing and only shares model parameter updates, thereby mitigating privacy concerns, reducing latency, and minimizing energy consumption associated with cloud/edge computing. In addition, we introduced a group signature-based authentication scheme specifically tailored for DT-PdM. It realizes the authentication of digital twin identity during the twin collaboration, allows the exchange of authenticated models, realizes the batch authentication of a large

number of twins at the same time, and improves the efficiency of real-time authentication. The experimental results show that our scheme has high accuracy in fault detection under different bearing health conditions while protecting data privacy.

However, in the real production environment, low-quality data is common to appear, and the performance of the model may be seriously affected when a large number of low-quality data appear. In the future, we will focus on the data analysis of federal learning in digital-based industrial internet of things.

Acknowledgement

This research is supported by Natural Science Foundation of Zhejiang Province of China (LZ22F030004) and Key Research and Development Program Project of Zhejiang Province (2024C01179).

References

[1] Y. You, C. Chen, F. Hu, Y. Liu, Z. Ji. Advances of digital twins for predictive maintenance. Procedia Computer Science. 2022, 200, pp. 1471-1480.

[2] X. Lai, L. Yang, X. He, Y. Pang, X. Song, W. Sun. Digital twin-based structural health monitoring by combining measurement and computational data: an aircraft wing example Journal of Manufacturing System. 2023, 69, pp. 76-90.

[3] H. Mu, F. He, L. Yuan, P. Commins, H. Wang, Z. Pan. Toward a smart wire arc additive manufacturing system: a review on current developments and a framework of digital twin. Journal of Manufacturing System. 2023, 67, pp. 174-189.

[4] C. Chen, H. Fu, Y. Zheng, F. Tao, Y. Liu. The advance of digital twin for predictive maintenance: The role and function of machine learning. Journal of Manufacturing Systems. 2023, 71, pp. 581-594.

[5] W. Kritzinger, M. Karner, G. Traar, J. Henjes, W. Sihn. Digital Twin in manufacturing: A categorical literature review and classification. Ifac-PapersOnline. 2018, 51(11), pp. 1016-1022.

[6] Y. Wang, Z. Su, S. Guo, M. Dai, T. Luan, Y. Liu. A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. IEEE Internet of Things Journal. 2023, 10(17), pp. 14965-14987.

[7] Y. Lu, C. Liu, I. Kevin, K. Wang, H. Huang, X. Xu. Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues. Robotics and computer-integrated manufacturing. 2020, 61, pp. 1-14.

[8] H. Xu, J. Wu, Q. Pan, X. Guan, M. Guizani. A Survey on Digital Twin for Industrial Internet of Things: Applications, Technologies and Tools. IEEE Communications Surveys and Tutorials. 2023, 25(4), pp. 2569-2598.

[9] F. Tao, Q. Qi. Make more digital twins. Nature. 2019, 573(7775), pp. 490-491.

[10] Y. Zhang, J. Ji, Z. Ren, Q. Ni, F. Gu, K. Feng, K. Yu, J. Ge, Z. Lei, Z. Liu. Digital twin-driven partial domain adaptation network for intelligent fault diagnosis of rolling bearing. Reliability Engineering & System Safety. 2023, 234, pp. 1-14.

[11] H. Hu, Y. Feng, Q. Hu, Y. Zhang. A Masked One-Dimensional Convolutional Autoencoder for Bearing Fault Diagnosis Based on Digital Twin Enabled Industrial Internet of Things. IEEE Journal on Selected Areas in Communications. 2023, 41(10), pp. 3242-3253.

[12] C. Alcaraz, J. Lopez. Digital twin: A comprehensive survey of security threats. IEEE Communications Surveys & Tutorials. 2022, 24(3), pp. 1475-1503.

[13] Y. Qu, L. Gao, Y. Xiang, S. Shen, S. Yu. FedTwin: Blockchain-enabled adaptive asynchronous federated learning for digital twin networks. IEEE Network. 2022, 36(6), pp. 183-190.

[14] C. Wang, Y. Ming, H. Liu, J. Feng, N. Zhang. Secure and Flexible Data Sharing With Dual Privacy Protection in Vehicular Digital Twin Networks. IEEE Transactions on Intelligent Transportation Systems. 2024, pp. 1-14.

[15] W. Shen, T. Hu, C. Zhang, S. Ma. Secure sharing of big digital twin data for smart manufacturing based on blockchain. Journal of manufacturing systems. 2021, 61, pp. 338-350.

[16] D. Gautam, G. Thakur, P. Kumar, A. Das, Y. Park. Blockchain Assisted Intra-Twin and Inter-Twin Authentication Scheme for Vehicular Digital Twin System. IEEE Transactions on Intelligent Transportation Systems. 2024, pp. 1-14.

[17] C. Chen, Q. Miao, S. Kumar, T. Wu. Privacy-preserving authentication scheme for digital twin-enabled autonomous vehicle environments. Transactions on Emerging Telecommunications Technologies. 2023, 34(11), pp. 1-17.

[18] P. Aggarwal, B. Narwal, S. Purohit, A. Mohapatra. BPADTA: Blockchain-based privacy-preserving authentication scheme for digital twin empowered aerospace industry. Computers and Electrical Engineering. 2023, 111, pp. 1-13.

[19] J. Xu, C. He, T. Luan. Efficient authentication for vehicular digital twin communications. 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall). 2021, pp. 1-5.

[20] C. Patel, A. Pasikhani, P. Gope, J. Clark. User-empowered secure privacy-preserving authentication scheme for Digital Twin. Computers & Security. 2024, 140, pp. 1-19.

[21] W. Zhang, X. Li, H. Ma, Z. Luo, X. Li. Federated learning for machinery fault diagnosis with dynamic validation and self-supervision. Knowledge-Based Systems. 2021, 213, pp. 1-15.

[22] R. Wang, F. Yan, L. Yu, C. Shen, X. Hu, J. Chen. A federated transfer learning method with low-quality knowledge filtering and dynamic model aggregation for rolling bearing fault diagnosis. Mechanical Systems and Signal Processing. 2023, 198, pp. 1-26.

[23] W. Zhang, X. Li. Data privacy preserving federated transfer learning in machinery fault diagnostics using prior distributions. Structural Health Monitoring. 2022, 21(4), pp. 1329-1344.

[24] J. Chen, J. Li, R. Huang, K. Yue, Z. Chen, W. Li. Federated transfer learning for bearing fault diagnosis with discrepancy-based weighted federated averaging. IEEE Transactions on Instrumentation and Measurement. 2022, 71, pp. 1-11.

[25] R. Wang, W. Huang, M. Shi, J. Wang, C. Shen, Z. Zhu. Federated adversarial domain generalization network: A novel machinery fault diagnosis method with data privacy. Knowledge-Based Systems. 2022, 256, pp. 1-13.

[26] W. A. Smith, R. B. Randall. Rolling element bearing diagnostics using the Case Western Reserve University data: A benchmark study. Mechanical systems and signal processing. 2015, 64, pp. 100-131.

[27] L. Eren, T. Ince, S. Kiranyaz. A generic intelligent bearing fault diagnosis system using compact adaptive 1D CNN classifier. Journal of Signal Processing Systems. 2019, 91(2), pp. 179-189.

[28] B. McMahan, E. Moore, D. Ramage, S. Hampson, B. y Arcas. Communication-efficient learning of deep networks from decentralized data. Artificial intelligence and statistics. 2017, pp. 1273-1282.

[29] F. Zenke, B. Poole, S. Ganguli. Continual learning through synaptic intelligence. International conference on machine learning. 2017, pp. 3987-3995.

About the authors

Yingjie Xia (Member, IEEE) received the Ph.D. degree from the College of Computer Science, Zhejiang University, Hangzhou, China, in 2009. He is currently a Distinguished Professor with Hangzhou Dianzi University, Distinguished Research Fellow with Zhejiang University and the CEO of Hangzhou Yuantiao Technology Company. His research interests cover digital twin and information security. (Email: xiayingjie@zju.edu.cn)

Liu Xuejiao is currently a Professor with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou, China. Her research interests include network security and data security. (Email: liuxuejiao@hznu.edu.cn)

Zhao Yunxiao is currently pursuing the M.S. degree with Hangzhou Normal University, Hangzhou, China. Her research interests include cyberspace security.

Wang Yun is currently pursuing the M.S. degree with Hangzhou Dianzi University, Hangzhou, China. Her research interests include security authentication.

基于保序缓存的时间敏感网络 FRER 机制

胡绍柳　蔡岳平　韩笑

（重庆大学微电子与通信工程学院　重庆　400030）

摘　要：时间敏感网络（Time-Sensitive Networking, TSN）通过帧的复制与消除机制（Frame Replication and Elimination for Reliability, FRER）解决业务可靠通信问题。FRER 机制通过在两条源节点与目的节点相同且不相交的路径上并行传输相同的帧，并在目的节点消除重复帧，提高了时间敏感网络的可靠性。但传统的 FRER 机制通过不同路径传输会导致帧乱序，现有的在接收端进行帧重排序方案容易在高负载下发生拥塞导致帧丢弃。为了解决 FRER 机制帧乱序导致缓存区溢出帧丢弃问题，提出了一种基于相交节点处帧保序缓存的 FRER 机制（FRER based on Frame Preservation Caching at Intersecting Nodes, FRER-FPCIN）。提出的机制包括保序缓存算法以及保序缓存区的分析与设计。在路径对的相交节点处提前对无序帧进行重排序，保序缓存算法通过帧到达事件和定时器超时事件保证帧的有序转发，并减轻保序缓存区中帧排队压力避免缓存区溢出，最后还对保序缓存区的大小和定时器的设置进行了分析。仿真结果表明，提出的机制有效降低了由于缓存区溢出导致的帧丢失率，与传统的在接收端利用滑动窗口法进行帧排序和在接收端用保序缓存算法帧排序相比，提出机制的帧丢失率最高分别降低了 3.2%和 1.4%。

关键词：时间敏感网络；帧的复制与消除；保序缓存

FRER mechanism based on sequence-preserving cache in Time-Sensitive Networking

Shaoliu Hu　Yueping Cai　Xiao Han

（School of Microelectronics and Communication Engineering, Chongqing University，Chongqing　400030）

Abstract: Time Sensitive Networking (TSN) solves the problem of reliable communication in business through the Frame Replication and Elimination for Reliability (FRER) mechanism. The FRER mechanism improves the reliability of time sensitive networks by transmitting identical frames in parallel on the disjoint paths between two source and destination nodes, and eliminating duplicate frames at the destination node. However, the traditional FRER mechanism frames transmitted through different paths can cause frame reordering, and existing frame reordering schemes at the receiving end are prone to congestion and frame dropout under high loads.To solve the

problem of buffer overflow and frame dropout caused by frame disorder in the FRER mechanism, a FRER mechanism based on frame preservation caching at intersecting nodes (FRER FPCIN) is proposed. The proposed mechanism includes the preservation cache algorithm and the analysis and design of the preservation cache area. Resorting unordered frames in advance at the intersection nodes of path pairs, the preservation caching algorithm ensures orderly forwarding of frames through frame arrival events and timer timeout events, and reduces the queuing pressure of frames in the preservation buffer to avoid buffer overflow. Finally, the size of the preservation buffer and the setting of the timer were analyzed. The simulation results show that the proposed mechanism effectively reduces the frame loss rate caused by buffer overflow. Compared with the traditional sliding window method for frame sorting at the receiving end and the preservation caching algorithm for frame sorting at the receiving end, the highest frame loss rates of the proposed mechanism are reduced by 3.2% and 1.4%, respectively.

Key words: time-sensitive network, frame replication and elimination, frame ordering and caching

1　引言

随着工业自动化和智能制造的不断发展，对数据处理和传输的及时性、可靠性要求越来越高。对于实时性和低时延有严格要求的场景[1]，标准以太网无法保证有界低时延和低丢包率，因而无法满足高质量的服务需求[2]。对此，IEEE 标准协会成立了音视频桥接（Audio Video Bridging, AVB）工作组[3]，随后演进为时间敏感网络工作组。时间敏感网络技术的发展体现在两个方面：一方面是这一工作组发展的一系列标准[4]。这些标准通过改良以太网，提高其在音视频传输、工业控制等高实时性和可靠性场景中的性能。时间敏感网络标准提供时间同步、低时延流控、可靠性和网络管控四个技术规范，确保数据传输具有确定性时延、高可靠性和精准时间同步，扩展了以太网的应用范围，如自动驾驶、实时控制系统和音视频流媒体传输等领域[5]。另一方面，学术界的一些学者深入地研究了 IEEE 802.1 工作组所提供的 TSN 标准技术，通过对这些标准技术进行改进和扩展，实现了在不同环境下满足网络的确定性和可靠性需求。

2005 年，AVB 工作组提出流预留协议标准，通过预留带宽减少数据帧丢失和阻塞。2012 年成立的 TSN 工作组致力于提升以太网性能，确保低时延和高可靠性。2018 年，TSN 工作组制定 IEEE 802.1CB 标准，引入帧复制和消除机制，最大程度减少拥塞和故障，提高帧传输可靠性。IEEE 802.1CB 标准中制定的 FRER 机制为以太网提供无缝冗余特性[6]，通过在源节点和网络中继节点中对每个帧进行编号并复制，在目的节点和其他中继节点中消除这些复制帧，为流提供了更高的可靠性，将拥塞和故障影响降到最低。FRER 机制通过在不相交的路径上发送重复的帧，允许关键流量的帧冗余[7][10]。即使工作路径故障，复制帧可通过冗余路径到达目的节点。在两个帧都到达目的地时，提供重复包消除机制。

TSN 在 IEEE 802.1CB-2017 中引入 FRER 作为可靠性标准，重点关注帧传输的可靠性，以预防故障安全和故障操作行为。尽管 FRER 通过帧的空间冗余实现了帧传输的无缝冗余，但在开销、时序、FRER 机制内部以及对网络其他特性的影响等方面仍存在未解决的问题。其中一个关键方面是时序分析，目前在该领域的研究主要有：

- Thomas[11]等人指出，FRER 通过复制功能将帧复制到冗余路径上，之后路径再次合并，消除函数删除重复的帧。这种冗余方案中复制可能导致复制路径上的突发增长和帧乱序，影响冗余和调度机制之间的相互作用。然而，文献未提出具体的帧重排序方法来解决这一问题；
- Mohammadpour[12]等人证明了如果流在其源和重排序缓存区之间是无损的，则重排序缓存区不会增加最坏情况时延和时延抖动。该理论成立的条件较特殊，节点和链路发生故障的时间和位置是不可控的，该文并没有给出帧重排序对流传输时延产生影响时完备的减缓或消除方案；
- Beneš[13]等人针对网络中数据包乱序问题提出了一种高效硬件实现的数据包重排序方案，并给出了提出的解决方案的资源消耗。这种重排序方案是在传输的接收端对数据包进行重排序，且重排序单元使用了最小的现场可编程门阵列（Field Programmable Gate Array, FPGA）资源；
- Tian[14]等人指出 TSN 通过每队列时分复用实现实时通信，无需考虑传入帧的细节。然而，实际转发序列可能与窗口调度不同，因此存在帧乱序问题。为解决此问题，作者提出了一种帧排序整形器（Frame Ordering Shaper, FOS），放置在接收端，以期望的序列对传入的帧进行排序。尽管进行了不同大小帧的仿真验证，但该方案未对帧丢失率和时延进行仿真测试，且 FOS 机制对帧传输的影响需要量化表示；
- Wang[15]等人研究了动态波长和带宽分配（Dynamic Wavelength and Bandwidth Allocation, DWBA）技术对帧重排序的影响，提出了一种不影响带宽利用率并能减轻帧乱序的 DWBA 算法。作者还分析了该算法对帧重排序光网络单元（Optical Network Unit, ONU）数的理论上界，并通过仿真对提出算法的性能进行了评价，包括帧重排序 ONU 数和帧时延。

2 帧乱序及缓存区溢出问题分析

TSN 需要对一定数量的帧进行重新排序，如参考文献[11]中所述，帧的复制与消除机制利用空间冗余实现帧的冗余传输，但由于网络元素的并行性，不同路径路由的帧可能引起排序错误和突发增加。解决方案通常是在接收端设置缓存区，并在源端每帧头部添加序列号，以便接收端根据序列号进行重排序。然而，这种方案存在两个主要问题：一是缓存区中的提前到达帧必须等待所有序列号较小的帧到达后才能转发，可能在网络拥塞时导致缓存区溢出丢弃后续帧；二是所有无序帧均需在接收端缓存区进行重排序处理，增加了接收端缓存区负载，也是网络拥塞导致缓存区溢出的原因之一。缓存区溢出如图 1 所示，序列号大于$N+1$的帧在缓存区中排队等候，当缓存区已满时序列号为$N+1$的帧还未到，新到达的所有其他帧均将被

丢弃。因此，一种新的重排序方法需要被设计，实现在接收端之前对帧的顺序提前进行调整，并重新规划重排序缓存区中帧调度规则以解决缓存区溢出导致的帧丢失问题。

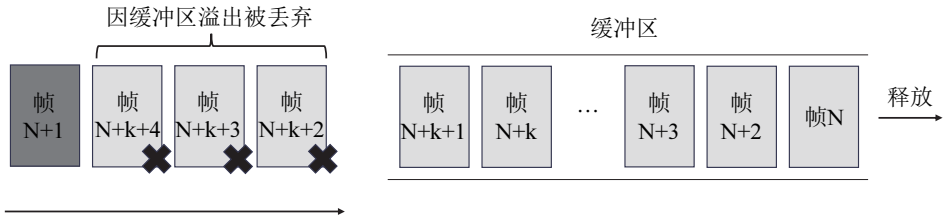


图 1　缓存区溢出示意图

3　相交节点处帧保序缓存机制

3.1　相交节点处帧保序缓存原理

帧的复制与消除机制允许帧通过多条路径传输，这些路径通常不完全不相交。由于网络拓扑和状态的多样性，在源节点和目的节点之间很难找到完全不相交的路径。相交节点具有帧消除能力，但也易发生帧乱序。因此，基于相交节点处帧保序缓存的 FRER 机制在每个路径对的相交节点后设置保序缓存区，提前调整帧顺序，影响帧在下一个相交节点的到达曲线，最终减少接收端的帧无序情况。在保序缓存机制中，源节点在帧头添加递增序列号，帧到达保序缓存区后根据调度规则转发或排队。期望到达的帧直接转发，提前到达的帧设定定时器。当所有比该帧序列号小的帧都到达或定时器超时时，该帧被释放；如果比该帧序列号大的帧定时器超时，该帧也被释放。

由上述可知，在保序缓存区中，有两类事件可以触发保序缓存区的保序规则：帧到达事件，定时器超时事件。

3.2　帧到达事件

当一个新的帧p到达保序缓存区时，执行算法 1。其中，变量buf代表一个保序缓存区列表，包含所有正在等待更小序列号帧到达的帧，变量N代表该保序缓存区期望接收的下一个序列号。

首先判断帧p的序列号pid是否大于等于$N-1$。如果该判断不成立，则该帧是无效的，将该帧丢弃。这是因为N为保序缓存区期望接收的下一个序列号，因此，新到达的帧p的序列号pid要么是序列号为$N-1$的帧的副本，要么是期望的序列号的或更大序列号的帧。如果该判断不成立，传输这种小序列号的帧将违反传输顺序。

其次判断帧p的序列号pid是否大于等于N。由第一个判断得知，此时帧的序列号均是有效值。如果该判断不成立，说明该帧p是序列号为$N-1$的帧的副本，应当释放该帧。

接着判断帧p的序列号pid是否大于N。如果该判断不成立，则该帧p是序列号为N的帧，且序列号是保序缓存区期望到达的帧序列号。因此，将N增加 1 到下一个序列号，并释放该帧。和上面情况不同，此时还需检查保序缓存区中帧的排队情况，若此时保序缓存区中存在序列号为N（此时的N为已经增加 1 后的N）

的帧，则应继续释放这些在保序缓存区中等待的帧。筛选符合序列号条件的帧由 Check.buffer 函数完成，在函数中，首先检查保序缓存区是否有一个序列号等于更新后的值的帧。如果有，就从队列中移除该帧，并增加到下一个序列号。与此同时，相关的定时器也会停止，最后释放符合条件的帧。接着继续调用 Check.buffer 函数对更新后的N值继续判断，这样递归调用函数 Check.buffer，每次执行该函数时，只要有符合序列号条件的帧，都会再次更新N值，直到保序缓存区中没有序列号等于最后更新值N的帧。这样，所有序列号小于新N值的帧都已经从保序缓存区中释放。

最后如果帧p的序列号pid大于N，说明有比期望序列号更大的帧提前到达保序缓存区，应等待较小序列号的帧到达后再处理。然后检查保序缓存区长度，若能容纳当前长度加上该帧，则启动其定时器，表示大序列号的帧提前排队等待。若容量不足，则丢弃该帧。

算法 1 保序缓存算法-帧到达事件

Input: 帧p
Variables: buf,N
1: **if** $p.id \geq N-1$ **then** //如果成立，则p是一个有效的帧
2: **if** $p.id \geq N$ **then**
3: **if** $p.id > N$ **then**
4: **if** $buf.len() + p.len \leq B$ **then**
5: TimerList.start($p.id$, Time() + T)
6: buf.enqueue(p)
7: **else** discard(p) //出现溢出，丢弃帧
8: **end if**
9: **else**
10: $N \leftarrow p.id + 1$
11: release(p)
12: Check.buffer()
13: **end if**
14: **else**
15: release(p)
16: Check.buffer()
17: **end if**
18: **else** discard(p) //出现无效帧
19: **end if**
20: **function** Check.buffer(void)
21: **if** $buf.contains(N)$ **then**
22: $p \leftarrow buf$.dequeue(N)
23: $N \leftarrow p.id + 1$
24: TimerList.stop($p.id$)
25: release(p)
26: Check.buffer()
27: **end if**

```
end function
```

3.3　定时器超时事件

当序列号为pid的帧的定时器超时，执行算法 2。其中变量buf代表一个保序缓存区列表，包含所有正在等待更小序列号帧到达的帧，变量N代表该保序缓存区期望接收的下一个序列号。

根据帧的调度规则，当序列号为pid的帧定时器超时，应该释放序列号为pid的帧。为了提供按顺序传递帧，保序缓存区首先按顺序释放保序缓存区中序列号小于等于pid的所有帧。利用函数buf. contains(N)，将N增加到保序缓存区中存储的帧的最小序列号，如果序列号为N的帧在保序缓存区中，则返回 TRUE，否则返回 FALSE。接着便是按顺序弹出保序缓存区中排队的帧，停止对应的定时器。每次有帧从保序缓存区中释放时，都要有相应的定时器被终止。最后，检查保序缓存区以释放正在等待 id 为pid或更小帧的帧。

算法 2　保序缓存算法-定时器超时事件

```
Input: 帧 id 号pid
Variables: buf,N
while N ≤ pid do
    while !buf.contains(N) do
        N ← N + 1
    end while
    p′ ← buf.dequeue(N)
    N ← p′.id + 1
    TimerList.stop(p′.id)
    release(p′)
end while
Check.buffer()
function Check.buffer(void)
    if buf.contains(N) then
        p ← buf.dequeue(N)
        N ← p.id + 1
        TimerList.stop(p.id)
        release(p)
        Check.buffer()
    end if
end function
```

由此，帧p被保序缓存区释放只存在三种情况：1）所有序列号小于p的帧都已经被保序缓存区接收到；2）帧p的定时器超时；3）保序缓存区中接收到序列号大于帧p的帧，且这个较大的帧定时器超时。

4　保序缓存区分析与设计

4.1　保序缓存区参数设置分析与设计

通过上述算法，可以实现保序缓存区中帧的有序释放。但当保序缓存区已满或到达的帧序列号小于

$N-1$时，帧将被丢弃。这表明要考虑保序缓存区中的两个重要参数：保序缓存区大小 B 和定时器超时值 T。这两个参数直接影响帧在保序缓存区中的处理情况，帧在以下两种情况下会被保序缓存区丢弃：

1）保序缓存区大小 B 太小；

2）定时器超时值 T 太小。

因此，为了避免帧被丢弃，保序缓存区大小和超时值应该设置得足够大。这里引入 RFC4737 中定义的两个包重排序度量：重排序时间偏移（Reordering Time Offset, RTO）和重排序字节偏移（Reordering Byte Offset, RBO），利用它们对帧的重排序进行度量，定义如下：

令在源点观察到的第 n 个帧为帧P_n，E_n为在目的点观察到帧P_n的时间。若帧P_n在两点间丢失，则$E_n=+\infty$。由于网络中不是所有元素都是保序的，所以帧P_n不一定比帧P_{n+1}先到达目的点，那么这种时间上的偏移可以表示为：

$$\lambda_n = E_n - \min_{j|j\geq n, E_j\leq E_n} E_j \tag{4.1}$$

其中λ_n表示帧P_n重排序时间偏移，即序列号大于 n 的帧比帧P_n早到达的最大时间。如果帧P_n丢失，则λ_n无定义。

同样地，对于帧P_n，如果存在帧P_j使得$j>n$且$E_j<E_n$，且帧P_n没有丢失，则帧P_n的重排序字节偏移量可以定义为：

$$\pi_n = \sum_{j|j>n, E_j<E_n} l_j \tag{4.2}$$

其中l_j为帧的字节大小，所以π_n表示帧P_n的重排序字节偏移，即序列号大于 n 的帧比帧P_n早到达的累计字节数。当帧P_n后没有出现乱序时，由重排序字节偏移量π_n为 0。

4.2 定时器超时值 T 的设置

假设保序缓存区中定时器的超时值为 T，考虑保序缓存区大小 B 足够大。λ为源端到目的端的 RTO，π为源端到目的端的 RBO。A_n表示帧 n 到达保序缓存区的时间，D_n表示帧 n 从保序缓存区释放的时间。帧 n 从保序缓存区释放的时间D_n可由下式表示：

$$D_n = \begin{cases} X_n & 若 n=1, \\ \max\{X_n, Y_n\} & 若 n>1 \end{cases} \tag{4.3}$$

其中X_n，Y_n为考虑不同参数情况下帧 n 从缓存区释放的时间。可由式（4.4）和（4.5）给出：

$$X_n = \begin{cases} +\infty & 若 A_n > min_{j\geq n}\{A_j\} + T, \\ A_n & 否则 \end{cases} \tag{4.4}$$

$$Y_n = \min\left(D_{n-1}, \min_{j\geq n}\{A_j\} + T\right), n\geq 2 \tag{4.5}$$

则序列号小于 n 的帧不被缓存区丢弃的情况表示为：

$$D_n \geq \max_{i<n|A_i\neq+\infty} D_i \tag{4.6}$$

假设对于$i < n$式（4.6）成立，则当$n = 1$时，有$D_1 = A_1$。当$n \geq 2$时：

$$D_n = max\{A_n, Y_n\} \tag{4.7}$$

对于集合$\xi_n = \{i < n|A_i \neq +\infty\}$，设 m 为其最大值，$T \geq \lambda$。则有：

$$\forall j > m: \quad A_m \leq A_j + \lambda \leq A_j + T, \tag{4.8}$$

$$A_m \leq T + \min_{j\geq m}\{A_j\}. \tag{4.9}$$

因此帧 m 从保序缓存区中释放的时间可表示为：

$$D_m = \max(Y_m, A_m) \leq \max\{T + \min_{j\geq m}\{A_j\}, A_m\} \overset{\text{公式(4.9)}}{\Rightarrow} D_m \leq T + \min_{j\geq m}\{A_j\} \tag{4.10}$$

这里需要讨论 m 的取值范围，m 的取值范围分为两种情况：$m = n - 1$和$m < n - 1$。

当$m = n - 1$时，因为有$n - 1 < n$，且$\min_{j\geq n-1}\{A_j\} \leq \min_{j\geq n}\{A_j\}$。因此有$D_{n-1} \leq T + \min_{j\geq n}\{A_j\}$。利用公式（4.7），则对帧 n 从保序缓存区中释放的时间有：

$$D_n = \max(Y_n, A_n) \geq Y_n = \min\left(D_{n-1}, T + \min_{j\geq n}\{A_j\}\right) = D_{n-1} \tag{4.11}$$

因此，没有帧被保序缓存区丢弃。

当$m < n - 1$时，因为有$A_{n-1} = +\infty$，且$D_{n-1} = \max\{Y_n, A_{n-1}\} = +\infty$。利用公式（4.7），则帧 n 从保序缓存区中释放的时间可表示为：

$$D_n = \max(Y_n, A_n) \geq Y_n = \min\left(D_{n-1}, T + \min_{j\geq n}\{A_j\}\right) = T + \min_{j\geq n}\{A_j\} \tag{4.12}$$

又因为有$m < n - 1$且$\min_{j\geq m} A_j \leq \min_{j\geq n} A_j$，因此对帧 n 从保序缓存区中释放的时间有：

$$D_n \geq T + \min_{j\geq n}\{A_j\} \geq T + \min_{j\geq m}\{A_j\} \geq D_m \tag{4.13}$$

因此，没有帧被保序缓存区丢弃。由此可知，当$T \geq \lambda$时，保序缓存区不会丢弃帧。现在假设$T < \lambda$且$\lambda > 0$，考虑这样一个场景，帧p_1到达保序缓存区时间为$A_1 = t_0$，帧p_2到达保序缓存区时间为$A_2 = t_0 + \lambda$，由于$A_1 > \min_{j\geq n}\{A_j\} + T = A_2 + T$，则一定有$D_1 = X_1$且$X_1 = +\infty$，即有帧$p_1$被保序缓存区丢弃。因此保证保序缓存区不丢弃帧的最小超时值 T 值应大于等于λ。

4.3　保序缓存区大小 B 的设置

假设保序缓存区的大小$B = +\infty$，帧 n 的大小为l_n，则时间 t 时保序缓存区中帧总大小为：

$$L(t) = \sum_{A_i<t,D_i\geq t} l_i, \tag{4.14}$$

考虑一个帧p_n有$n > 1$且其大小为l_n。则当帧p_n到达保序缓存区时，还在保序缓存区中排队的所有帧集合可由下式定义：

$$S = \{i \in \mathbb{Z}^+ | \quad i < n, D_i \geq A_n\} \tag{4.15}$$

如果 S 为空，不会发生缓存区溢出问题。若 S 不为空，且集合 S 中的最小值为 m，即$m = \min(S)$。则帧p_n到达保序缓存区时，其中帧总大小为：

$$\begin{aligned} L(A_n) + l_n &= \sum_{i,A_i<A_n\leq D_i} l_i + l_n \\ &= \sum_{i<m,A_i<A_n\leq D_i} l_i + \sum_{i\geq m,A_i<A_n\leq D_i} l_i + l_n \\ &= \sum_{i\geq m,A_i<A_n\leq D_i} l_i + l_n \leq \sum_{i\geq m,A_i<A_n} l_i + l \end{aligned} \tag{4.16}$$

因为$m < n$，且$E_m > E_n$，则此时的保序缓存区中帧大小可表示为：

$$\sum_{i\geq m,A_i<A_n} l_i + l_n \leq \sum_{i>m,A_i<A_m} l_i = \pi_m \tag{4.17}$$

综合上式可知，保序缓存区的大小上界为π：

$$L(A_n) + l_n \leq \pi_m \leq \pi \tag{4.18}$$

5 性能分析与评价

本节介绍了所提出的基于相交节点处帧保序缓存的 FRER 机制（FRER-FPCIN）、在接收端利用保序缓存算法进行帧排序以及在接收端使用滑动窗口法的帧排序机制在不同网络负载下的性能评价和对比分析。性能评价指标包括帧丢失率、平均时延和平均时延抖动。

5.1 仿真评价指标

①帧丢失率

帧丢失率指数据传输过程中，帧丢失的数量占总的帧传输的比率。这个比率越低，表示数据传输的可靠性越高，因此本论文将帧丢失率作为仿真评价指标之一。帧丢失率的计算方式如下：

$$\eta = \frac{N_{loss}}{N_{total}} \tag{5.1}$$

其中，N_{loss}表示丢失的帧数量，N_{total}表示发送的帧总数量。

②平均时延

帧传输的端到端时延包括排队时延、发送时延、传播时延和处理时延四部分。排队时延是帧在队列中等待处理的时间，受网络拥塞影响而增大。发送时延取决于帧大小和发送设备带宽。传播时延与链路长度和材质有关。处理时延是帧到达路由器或交换机时进行检查和处理的时间。帧的平均时延计算方式如下：

$$T_{delay} = T_{send} + T_{spread} + T_{process} + T_{queue} \tag{5.2}$$

其中，T_{delay}表示端到端总时延，T_{send}表示发送时延，T_{spread}表示传播时延，$T_{process}$表示处理时延，T_{queue}表示排队时延。

③平均时延抖动

帧的平均时延抖动 J 可计算如下：

$$J = \max\{T_{delay}\} - \min\{T_{delay}\} \tag{5.3}$$

5.2　仿真参数设置

如图 2 所示仿真包含 13 个节点，26 条链路的网络拓扑。其中节点 1 为源节点，节点 9 为目的节点。以 1Gbit/s 作为链路带宽，网络负载取值范围设置为[0.1, 1]。帧的大小设置为服从均匀分布，取值范围在 64 到 500 之间。帧的个数设置为 500000 个。帧的到达过程设置为服从泊松分布，参数设置为 500 帧每秒。帧的间隔时间设置为服从负指数分布，参数设置为 10。仿真的主要参数设置见表 1 所示。

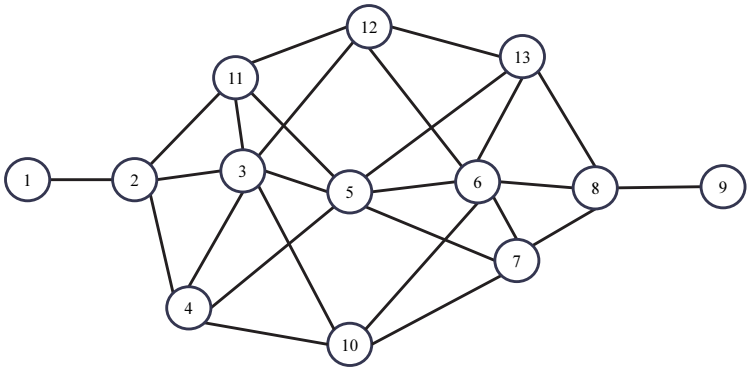


图2　仿真网络拓扑图

表1　仿真参数

参数	分布	值
链路带宽	-	1（Gbit/s）
网络负载	-	[0.1,1]
链路数量	-	26
节点数量	-	13
帧数量	-	5×10^5
帧大小（bytes）	均匀	64~500
帧到达过程	泊松	500
帧间隔时间（μs）	负指数	10

5.3　帧丢失率仿真结果与分析

图 3 显示了接收端滑动窗口帧排序机制、接收端帧保序缓存和在相交节点处帧保序缓存的 FRER 机制（FRER-FPCIN）三种策略的帧丢失率随网络负载变化的情况。随着负载的增加，三种策略的帧丢失率都在

升高，且在负载为 0.6 之后增长幅度加大。接收端滑动窗口帧排序机制在接收到提前到达的帧时，会将其暂存于缓存区，直到序列号较小的帧到达再释放。此方法在网络拥塞和负载较大时，容易导致大量帧丢失，帧丢失率最高。在接收端使用保序缓存算法帧排序，通过定时器 T 改善了网络拥塞时帧丢失的情况。而基于相交节点处帧保序缓存的 FRER 机制，在相交节点提前处理帧顺序，影响下一个节点的帧到达曲线，减少保序缓存区排队等待的帧，降低了帧丢失率。比起接收端滑动窗口帧排序和接收端保序缓存帧排序方案，FRER-FPCIN 机制的帧丢失率最高分别降低了 3.2%和 1.4%。

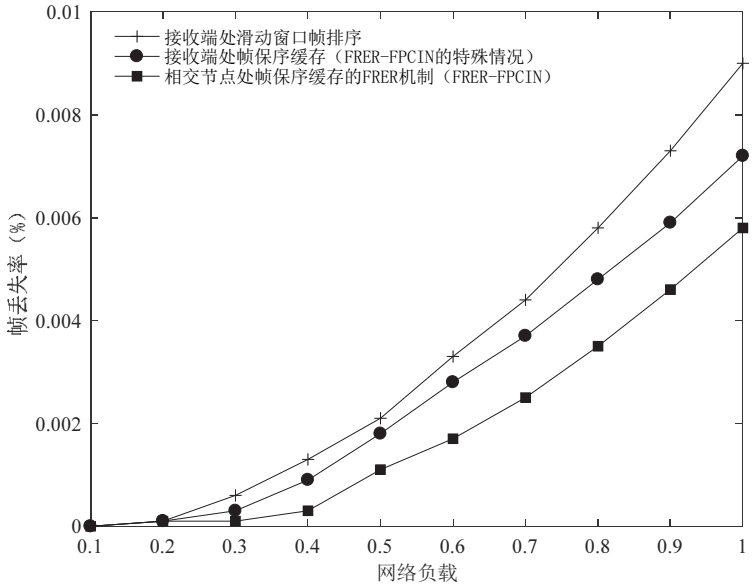


图 3　不同网络负载下的帧丢失率

5.4　平均时延仿真结果与分析

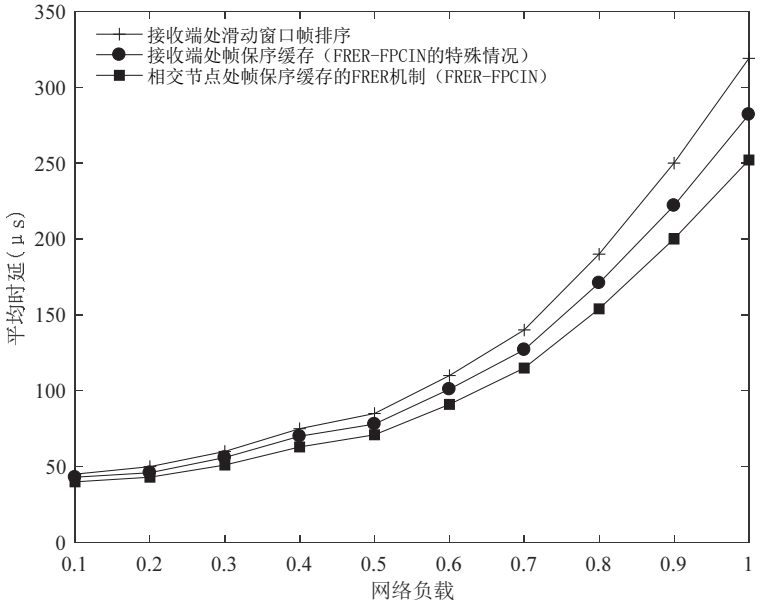


图 4　不同网络负载下的平均时延

图 4 显示了接收端滑动窗口帧排序机制、接收端帧保序缓存和在相交节点处帧保序缓存的 FRER 机制

（FRER-FPCIN）三种策略的平均时延随网络负载变化的情况。随着负载的增加，三种重排序策略的平均时延都在升高。其中在接收端用滑动窗口帧排序的平均时延最高，因为乱序帧均在接收端处理，负载增大会导致网络拥塞和排队时延增加。使用保序缓存算法并设置定时器 T，平均时延稍好。相交节点处帧保序缓存策略提前处理乱序帧，避免重排序时间偏移扩增，降低了平均时延。与接收端滑动窗口帧排序和接收端保序缓存帧排序方案策略相比，FRER-FPCIN 平均时延分别降低了 16.77%和 9.15%。

5.5　平均时延抖动仿真结果与分析

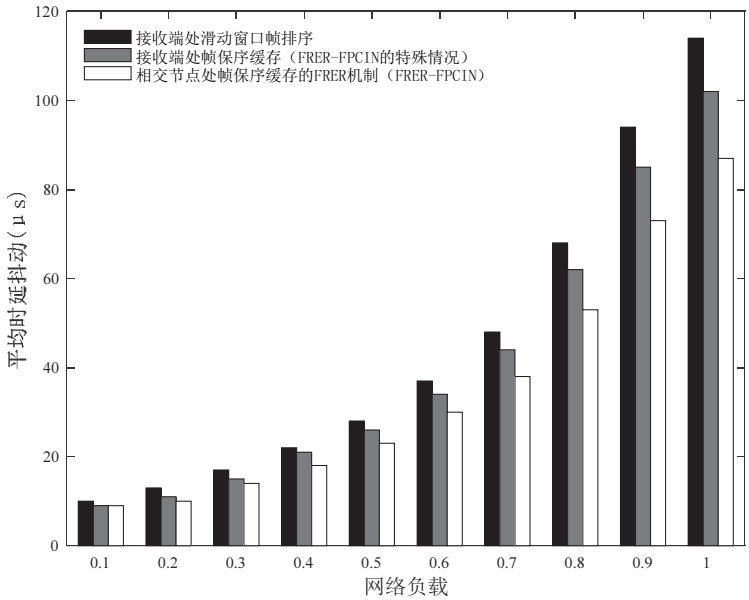


图 5　不同网络负载下的平均时延抖动

图 5 显示了接收端滑动窗口帧排序机制、接收端帧保序缓存和在相交节点处帧保序缓存的 FRER 机制（FRER-FPCIN）三种策略的平均时延抖动随网络负载变化的情况。三种策略的时延抖动均随着网络负载的增大而增大。其中接收端用滑动窗口帧排序时延抖动最大，因为乱序帧重排序时间偏移增加了缓存区排队时间和数量。使用保序缓存算法的策略减少了缓存区溢出，降低了时延抖动。相交节点处帧保序缓存策略提前处理帧顺序，减少了后续节点重排序时间偏移，降低了时延抖动与接收端滑动窗口帧排序和接收端保序缓存帧排序方案策略相比，FRER-FPCIN 平均时延抖动分别降低了 19.44%和 10.12%。

6　结束语

本文主要提出了一种基于相交节点处帧保序缓存的 FRER 机制，简称 FRER-FPCIN。FRER-FPCIN 通过在流传输路径对中的相交节点上设置保序缓存区提前进行重排序，以减少后续相交节点以及接收端处的帧重排序时间偏移。同时保序缓存区中帧的调度规则用保序缓存算法实现，分为帧到达事件触发与定时器超时事件触发。最后为了避免保序缓存区中因缓存区大小 B 或定时器 T 的设置过小导致的缓存区溢出，利用帧重排序时间偏移和帧重排序字节偏移推导出了这两个参数的范围。仿真结果表明，与在接收端处利用滑动窗口帧排序方法相比，提出的机制能明显降低帧丢失率，并且由于提前处理了帧的乱序问题，降低了后

续相交节点上帧的重排序时间偏移，避免了帧重排序时间偏移的扩增，在时延和时延抖动上也有更好的表现。

参考文献：

[1] YAN L L, GE J C, PAN Z X, et al. Time-sensitive network control and management system for heterogeneous networks convergence[C]. 2023 3rd International Conference on Intelligent Communications and Computing, Nanchang, China, IEEE, 2023: 60-69.

[2] XUE J L, SHOU G C, LIU Y Q, et al. Scheduling time-critical traffic with virtual queues in software-defined time-sensitive networking[J]. IEEE Transactions on Network and Service Management, 2024, 21(1): 967-978.

[3] IEEE standard for local and metropolitan area networks--audio video bridging (AVB) Systems[S]. IEEE Std 802.1BA-2021, 2021: 1-45.

[4] MIN J H, KIM W, PAEK J, et al. Effective routing and scheduling strategies for fault-tolerant time-sensitive networking[J]. IEEE Internet of Things Journal, 2024, 11(6): 11008-11020.

[5] SUN W J, ZOU Y, ZHANG X D, et al. Joint routing and scheduling optimization of in-vehicle time-sensitive networks based on improved grey wolf optimizer[J]. IEEE Internet of Things Journal, 2024, 11(4): 7093-7106.

[6] JOVER M, BARRANCO M, ÁLVAREZ I, et al. Migrating legacy ethernet-based traffic with spatial redundancy to TSN networks[C]. 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation, Stuttgart, Germany, IEEE, 2022: 1-8.

[7] KEHRER S, KLEINEBERG O, HEFFERNAN D. A comparison of fault-tolerance concepts for IEEE 802.1 Time Sensitive Networks (TSN)[C]. Proceedings of the 2014 IEEE Emerging Technology and Factory Automation, Barcelona, Spain, IEEE, 2014: 1-8.

[8] QIAN S, LUO F, XU J. An analysis of frame replication and elimination for time-sensitive networking[C]. In Proceedings of the 2017 VI International Conference on Network, Communication and Computing. New York, USA, ACM, 2017: 166-170.

[9] PRINZ F, SCHOEFFLER M, LECHLER A. End-to-end redundancy between real-time I4.0 components based on time-Sensitive networking[C]. 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation, Turin, Italy, IEEE, 2018: 1083-1086.

[10] HOFMANN R, NIKOLIĆ B, ERNST R. Challenges and limitations of IEEE 802.1CB-2017[J]. IEEE Embedded Systems Letters, 2020, 12(4): 105-108.

[11] THOMAS L, MIFDAOUI A, BOUDEC J-Y L. Worst-case delay bounds in time-sensitive networks with packet replication and elimination[J]. IEEE/ACM Transactions on Networking, 2022, 30(6): 2701-2715.

[12] MOHAMMADPOUR E, BOUDEC J-Y L. On packet reordering in time-sensitive networks[J]. IEEE/ACM Transactions on Networking, 2022, 30(3): 1045-1057.

[13] BENES T, UBIK S, HALAK J. Packet reordering correction for low-latency network applications[C]. 2022 11th Mediterranean Conference on Embedded Computing. Budva, Montenegro, IEEE, 2022: 1-5.

[14] TIAN Z, YANG F. FOS: A shaping mechanism for frame ordering in time sensitive networking[C]. 2022 IEEE 8th International Conference on Computer and Communications, Chengdu, China, IEEE, 2022: 401-405.

[15] WANG W, GUO W, HU W S. Dynamic wavelength and bandwidth allocation algorithms for mitigating frame reordering in NG-EPON[J]. IEEE/OSA Journal of Optical Communications & Networking, 2018, 10(3): 220-228.

[作者简介]

胡绍柳（1997_ ），男，重庆荣昌人，硕士生，重庆大学微电子与通信工程学院，主要研究方向为时间敏感网络。

蔡岳平（1980_ ），男，江苏丹阳人，博士，重庆大学副教授，主要研究方向为工业互联网、确定性网络、5G/6G 网络、数据中心网络、算力网络等。

韩笑（2001_ ），男，山西忻州人，硕士生，重庆大学微电子与通信工程学院，主要研究方向为时间敏感网络。

基于“微服务+中台”内核的航天离散协同制造工业互联网平台构建及其应用[1]

钟珂珂，郭具涛，刘骁佳，陈晓棠，刘晓，向美红，洪海波

（上海航天精密机械研究所，上海 201600）

摘要：新一代信息通信技术的发展加速推进企业信息系统架构的更新换代，微服务架构逐步从商业领域走向工业制造领域。针对航天离散制造技术状态多变、协作关系复杂、过程管控严格等特点，以及传统信息系统架构难以满足航天产品质与量、类型与形态、成本与周期要求同步提高的迫切需求，本文基于微服务理念和技术，对企业信息系统进行重构，设计了具有技术中台、业务中台和数据中台的航天离散协同制造工业互联网平台；通过平台应用实现科研生产和经营管理核心业务全在线、过程全透明、信息全追溯，构建了面向企业全局数据感知、分析和应用的新体系，有效赋能企业科研生产管理模式升级。

关键词：微服务架构；中台；航天离散协同制造；工业互联网；转型升级

Construction and Application of Aerospace Discrete Collaborative Manufacturing Industrial Internet Platform based on Micro-services Architecture and Middle Center

ZHONG Keke，GUO Jutao，LIU Xiaojia，CHEN Xiaotang， LIU Xiao, XIANG Meihong, HONG Haibo

Shanghai Spaceflight Precision Machinery Institute, Shanghai 201600

Abstract: The development of new generation information and communication technology accelerates the upgrading of enterprise information system architecture, and the Micro-services architecture gradually moves from the commercial field to the industrial manufacturing field. In view of the characteristics of aerospace discrete manufacturing technology, such as changeable state, complex collaboration relationship and strict process control, as well as the difficulty of traditional information system architecture to meet the increasingly complex collaborative rapid development needs of aerospace products, based on the concept and technology of micro-service, the enterprise information system was reconstructed, and the aerospace discrete collaborative manufacturing Industrial Internet platform with technology, business and data middle platforms was created; Through platform applications, the core business of scientific research production and business management is

基金项目：国家自然科学基金资助项目（92367301，92267201）

fully online, the process is fully transparent, and information is fully traceable. A new system for enterprise global data perception, analysis, and application has been constructed, effectively empowering the upgrading of enterprise scientific research production management mode.

Keywords: Micro-services architecture; Middle Center; Aerospace discrete collaborative manufacturing; Industrial Internet; Transformation

0　引言

当今，全球制造业随着新一代信息通信技术的快速融合发展孕育着制造技术体系、制造模式、产业形态和价值链的巨大变革，制造技术与数字技术、智能技术及新一代信息技术的融合已成为制造业发展的大趋势[1-3]。航天产品研制具有多品种、小批量的典型离散制造特点，在低成本快速研制，以及技术状态多变、协作关系复杂的研制模式下，存在资源快速重组和优化配置、质量过程精准控制、跨单位跨专业高效协作等业务需求[4]。而传统的企业信息系统存在架构孤立、标准不统一、技术难兼容、数据源不统一，进而造成业务集成扩展难度大等问题，难以支撑航天产品高质量、高效率、高效益研制需求，迫切需要构建面向企业全局数据感知、分析和应用新体系。工业互联网是新一代信息通信技术与现代工业技术深度融合的产物，可有效支撑对传统研制技术、研制手段和研制模式进行创新和变革，同时，工业互联网具有行业特性，只有与特定行业、特定应用场景结合，沉淀工艺知识和行业模型的工业互联网平台才具有生命力[5,6]。

本文针对航天产品研制对企业全局数据感知、分析和应用新体系的需求，开展行业特色工业互联网构建技术研究，设计了航天离散协同制造工业互联网平台架构，从技术中台、业务中台、数据中台三个方面阐述了工业互联网平台构建关键技术，并基于数字化工厂/车间“管、做、送、数据”的业务模型，设计了覆盖计划调度、质量管理、工艺管理、供应链管理、资源管理、制造执行管理六大功能的平台功能模块。本文研究成果已应用于某航天企业制造企业并取得良好效果，对加速企业科研生产管理模式转型升级具有重要现实作用，为航天乃至离散制造企业车间生产管理提供了可行的技术途径。

1　企业信息系统架构的演进

信息系统架构[7]（Information System Architecture，ISA）是一个体系结构，它反映了一个组织的信息系统的各个组成部分之间的关系，以及信息系统与相关业务，信息系统与相关技术之间的关系。总体上看，企业信息系统架构经历了四个大的阶段：单体架构、垂直架构、SOA 架构（Service-Oriented Architecture，面向服务架构）和微服务架构，如图 1 所示。

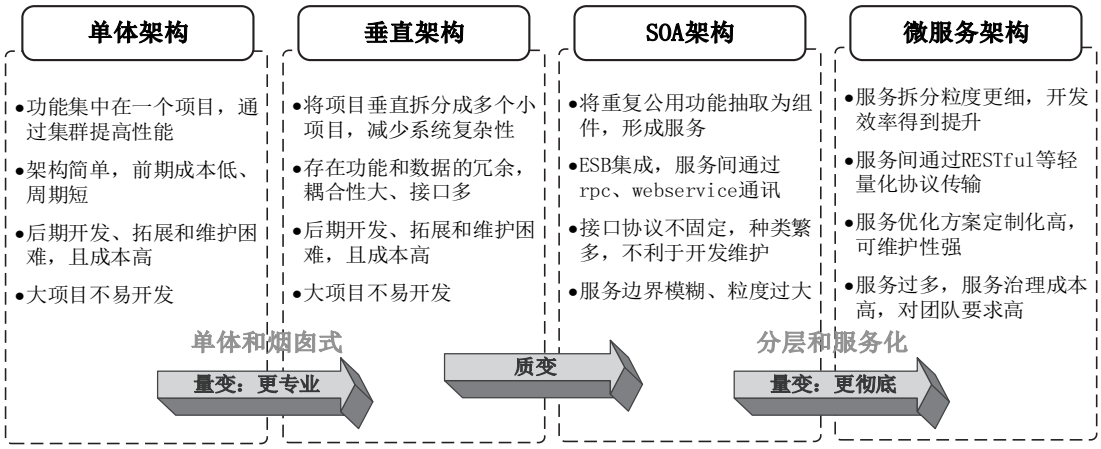


图1　企业信息架构发展四个阶段

伴随着信息技术的发展，企业信息系统架构从传统的“封闭式”功能定义的单体和垂直架构转变为以分层和服务化为基础的“开放式”的 SOA 和微服务架构是一种必然趋势[8]。利用微服务理念和技术重塑企业科研生产管理系统，打造符合技术发展趋势且具有行业特色的工业互联网平台，可有效应对离散制造企业多变的业务需求、复杂的协作关系和精细的管控要求等，具有重要的现实意义。

2　平台总体架构设计

航天产品研制模式、工艺流程、管控要求和组织管理方式具有自身的特点，通用的工业互联网平台存在功能定制开发量大、行业算法和模型库缺失、模块化组件化能力不足等问题，难以快速适应航天离散协同制造需求。参照工业互联网体系架构[9,10]，按照分层和服务化思想，基于“微服务+中台”的理念和技术，设计面向航天及离散制造行业的企业级特色工业互联网平台总体架构，如图 2 所示。

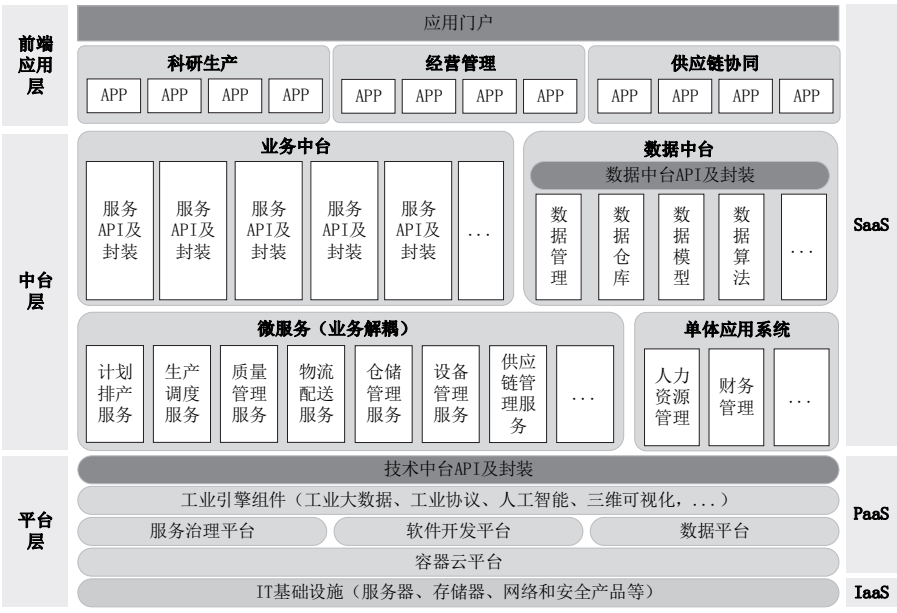


图2　面向航天及离散制造行业的特色工业互联网平台总体架构

（1）平台层。平台层又分为 IaaS（Infrastructure as a Service，基础设施即服务）和工业 PaaS（Platform as a Service，平台即服务），其中，IaaS 主要是支撑平台开发和运营的 IT 基础设施；工业 PaaS 是工业互联网平台的技术中台，既包括通用 PaaS 平台组件，又包括支撑制造企业工业应用场景开发的工业物联网、工业大数据、人工智能、三维可视化等工业引擎组件。

（2）中台层。制造中台层是核心资源能力平台，为前台生产提供关键资源和服务。制造中台分为业务中台和数据中台，业务中台包括计划排产、生产调度、质量管理、设备管理等业务微服务，实现业务互联和数字化协同；数据中台实现数据汇聚、处理、治理，以接口的形式为前端生产和业务过程处理提供服务，实现数据驱动的业务流。

（3）应用层。应用层是面向科研生产、经营管理和供应链协同具体业务功能的实现需求，开发面向用户的工业 APP。

3　平台构建关键技术

3.1 工业 PaaS 平台设计技术

工业 PaaS 的本质是在现有成熟的 IaaS 平台上构建一个可扩展的工业操作系统，为工业应用软件开发提供一个基础平台。工业 PaaS 平台是在平台化框架不断发展的过程中产生的，充分体现了平台和框架高聚合、低耦合，数据高可用、资源易集成的特点，是工业软件自主可控的基础。

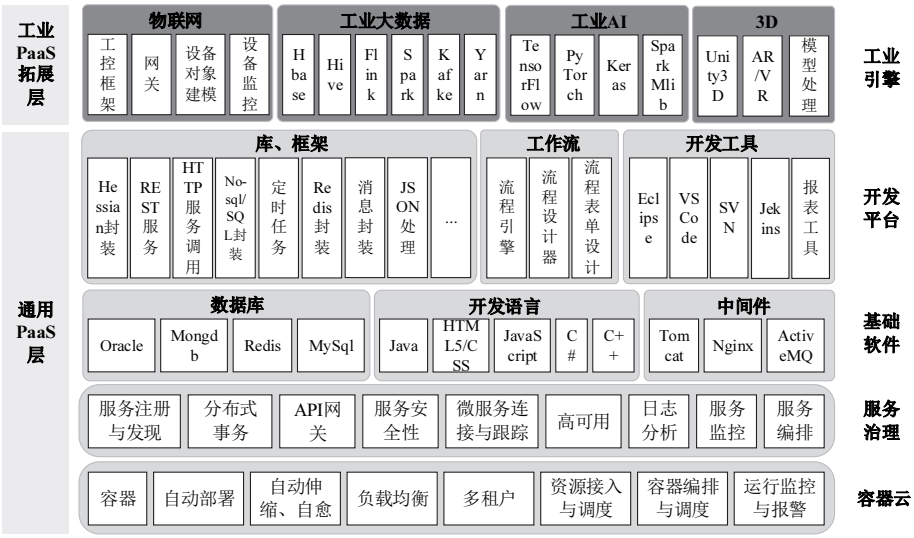


图3　工业PaaS平台组成结构

结合航天离散制造资源快速重组和优化配置、质量过程精准控制、跨单位跨专业高效协作对数据、模型的需求，在通用 PaaS 平台的基础上增加工业物联、工业大数据、工业 AI 和 3D 处理等工业引擎，搭建具有行业特征的工业 PaaS 平台，如图 3 所示。其中，通用 PaaS 层设计功能包括开发平台、基础软件、服

务治理和容器云，提供通用的软件开发、测试、部署、运行监控环境，支撑各微服务及 APP 的开发；工业 PaaS 扩展层设计功能包括设备联网与数据采集组件、工业大数据组件、工业 AI 组件、3D 可视化组件，满足制造企业设备物联与数据采集、工业大数据分析、基于数据孪生的虚拟监控与智能决策等数字化领域应用需求。

3.2 业务中台构建技术

业务中台[11,12]是阿里巴巴首先提出的企业 IT 架构的转型之道，其本质上是一个体系或系统，承载了企业核心的业务运行机制，通过把后台的资源沉淀出可以“被共享的能力”，并整合成前台应用需要的“中间件”，方便被随需调用，从而实现资源或能力的极度共享。航天离散制造具有业务范围广、涉及专业多、工艺流程长、协作关系复杂等特点，且业务数据相互关联，要从复杂的业务中抽取可复用强的能力，需要在对业务充分理解、抽象和建模的基础上，进行业务的解耦与服务的封装。

首先，将“数字化企业”视为一个系统自顶向下设计，把数字化工厂/车间抽象为业务、生产、物流和决策，分别解决生产对象的业务流程变化、状态变化、空间变化和决策方法变化问题。基于此，对数字化工厂/车间进行业务建模，分为“管、做、送、数据”四部分；然后，基于数字化工厂/车间“管、做、送、数据”的业务模型，从业务功能的视角对业务功能分层、业务功能解耦、同类功能合并与去重，将专业性的业务功能提取出来形成中台层，提供业务功能职能单一、边界清晰、接口关系简单的共享业务功能。如图 4 所示，结合微服务架构技术和理念，将数字化工厂/车间生产管控平台分解为六大部分组成：计划调度、质量管理、工艺管理、仓储物流管理、资源管理、制造执行管理。

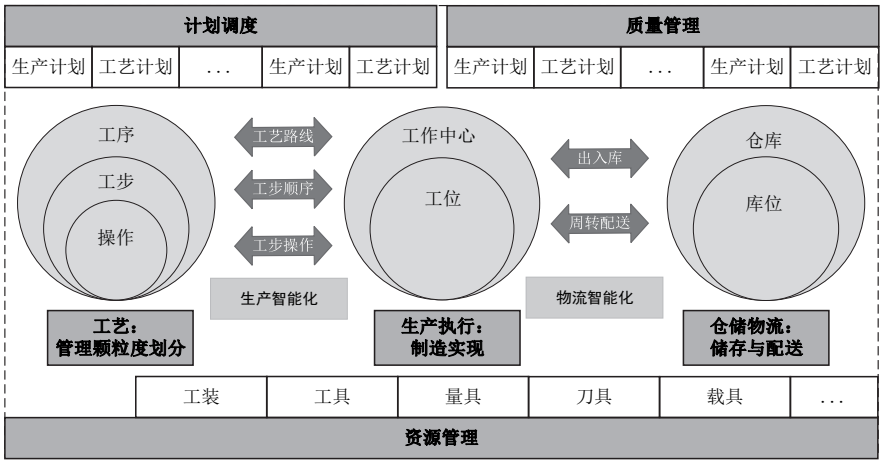


图 4 业务中台模型组成结构

3.3 数据中台构建技术

数据中台是一个技术连接大数据计算存储能力，用业务连接数据用于场景能力的平台，通过将生产过程中的多源异构数据梳理、分类、管理、整合成为有价值的数据资源，更好地应用于各类工业场景开发应

用[12,13]。航天离散制造具有生产要素种类繁多、制造过程高度离散、生产过程状态多变、生产管理策略复杂等特征，带来了生产过程数据的多源性、异构性、时空性和冗余性等特点。因此，要实现数据中台高效、便捷支撑工业场景开发，对多源异构数据的建模是基础。

航天制造车间是由工作中心（制造单元）组成的，每个工作中心又包含具体的加工设备、检验设备、在制品、辅助工艺装备、人员、线边库、物料等多种制造要素，基于数据时空模型建模方法，从时间、空间和属性三个维度对车间人机料法环等要素进行客观描述，将航天离散制造车间的数据按层级进行划分，分为车间级、工作中心级、单个制造要素级三个层次，三个层次从上向下为包含关系，在构建数据时空模型时从下而上逐级建立，面向航天离散制造车间的时空数据模型如图 5 所示，通过数据时空模型描述航天产品研制过程中各类制造要素在不同时间不同位置的状态。在此基础上，从业务需求出发，对数据中台功能体系结构进行设计，具备数据汇聚、数据治理、数据建模、数据加工、知识沉淀，以及数据集成、同步和交换等提供数据能力。

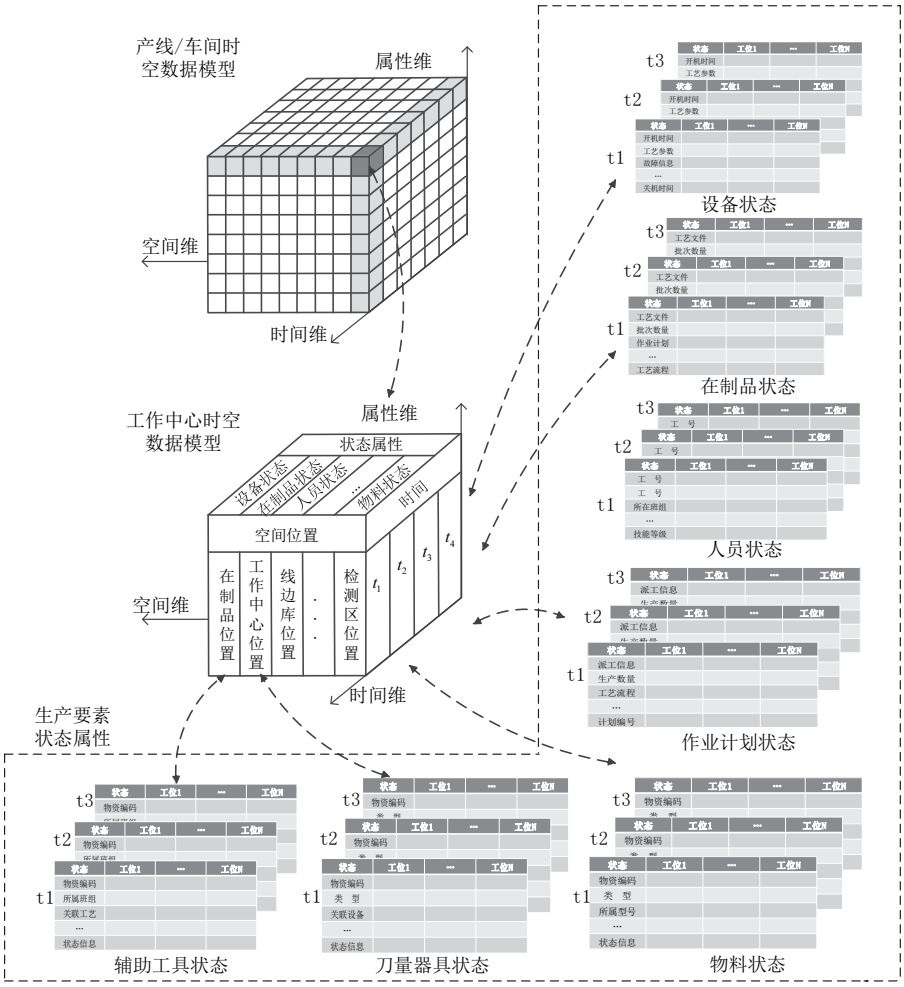


图 5　面向离散制造车间的时空数据模型

4 平台功能实现与应用验证

4.1 平台功能设计

在行业特色工业互联网平台总体架构下，结合数字化工厂/车间“管、做、送、数据”的业务模型和六大核心业务功能模型结构，按照“大平台、小前端”的思路，从工业互联网功能视角确定工业互联网平台的功能要素、相互关系、接口及交互方式[14]，将工业互联网平台功能规划为制造前台、制造中台两大层次六个业务领域，如图 6 所示。并基于制造前台和制造中台产生的数据构建基于场景的看板、基于角色的报表和基于业务的预警消息，支撑车间生产过程精准高效的决策。

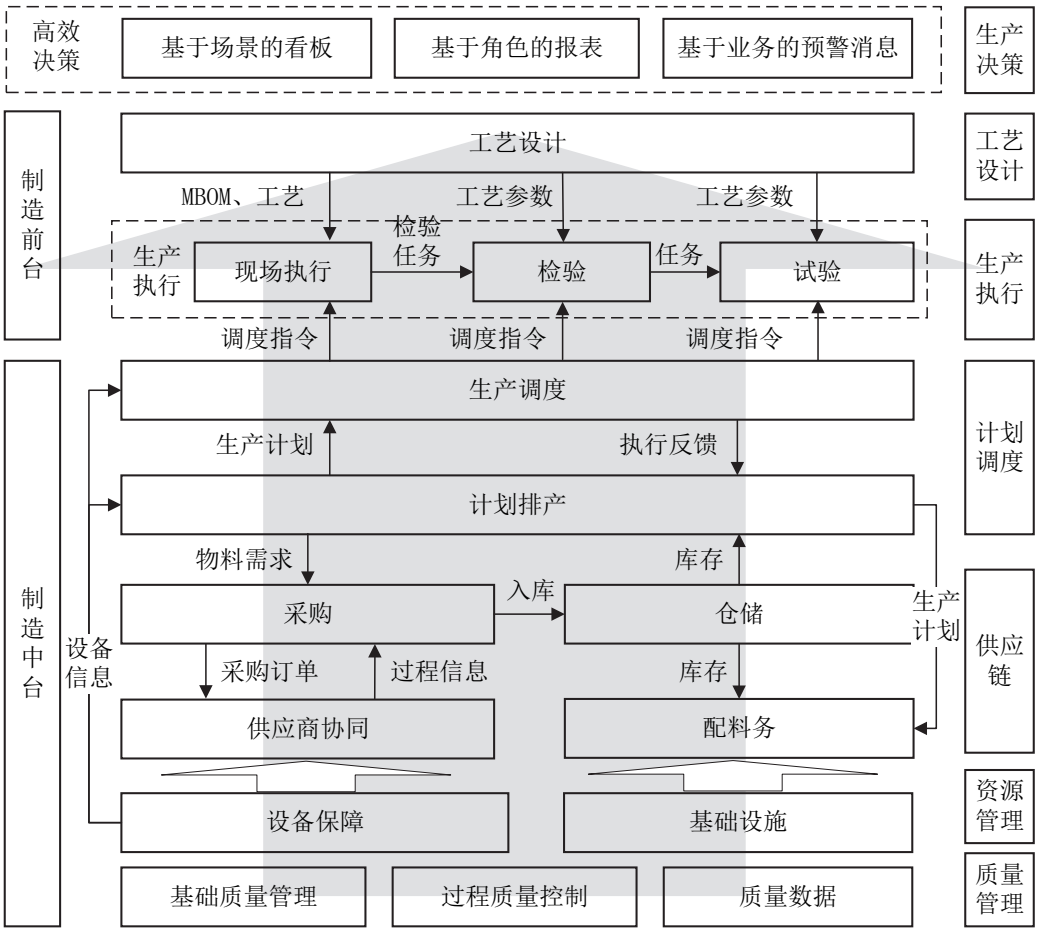


图 6 平台功能体系结构

制造前台即产品实现过程，聚集与产品对象直接相关的产品实现增值过程，包括工艺设计和生产执行两个业务领域，其中，工艺设计业务领域用于对零部件及产品的制造工艺进行设计，实现工艺计划、工艺规程、工艺参数、工序模型、工艺知识库、工时定额、工艺签审、工艺变更、工艺状态控制、工艺仿真等管理；生产执行业务领域用于车间制造现场执行管理，实现工艺可视化、生产作业、物料管理、操作记录、数控程序集成、看板等管理，支撑人机料法环生产要素的协同管理。

制造中台是为实现前端轻量化，灵活适应复杂多变的离散制造特点以及不均衡的生产需求，将计划、资源和支撑性过程放到中后台，包括计划调度、供应链、设备设施、质量管理四个业务领域。其中，计划调度业务领域实现对生产计划和资源的统筹安排和执行过程调度，包括计划排产和生产调度两个服务模块；供应链业务领域重点实现内部物流集成高效运转，保证生产物流与仓储物流紧密衔接，包括采购、供应商、仓储、配料四个服务模块；资源管理业务领域提供设备设施等资源的全生命周期管理，包括设备保障、基础设施保障两个服务模块；质量管理业务领域实现质量策划、控制、保证、改进的 PDCA 过程，支撑质量管理过程的数字化，包括基础质量管理、过程质量控制、质量数据分析三个服务模块。

4.2　平台应用验证

基于平台总体架构和功能体系结构，融合航天工艺知识和业务模型，对科研生产管理系统进行重构，形成具有统一技术平台、统一中台 API、统一用户界面的航天离散协同制造工业互联网平台，其主界面如图 7 所示。作为面向离散制造企业的新型网络基础设施，全面支撑企业数字化转型、智能工厂建设，基本实现了企业生产运营业务全在线、过程全透明、数据全追溯。

图 7　航天离散协同制造工业互联网平台主界面

（1）业务全在线：平台功能覆盖科研生产与经营管理核心业务，实现从工艺→资源→计划→调度→现场管理业务流程闭环控制；另外，通过对车间设备、产品、工艺、检测等生产信息的全面感知，实现工艺设计、计划调度、生产执行、质量检验、物料配送、资源管理等各类数据统一记录管理，以及车间“人-机-物”互联互通和无纸化生产。

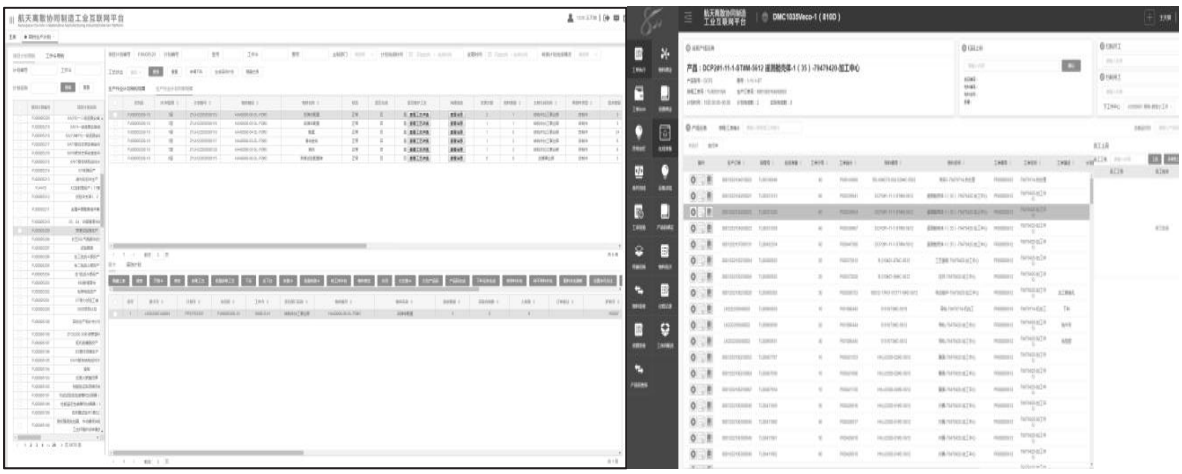


图 8　工业互联网平台业务功能界面

（2）过程全透明：针对航天制造车间两张网的情况，系统内网 IT（information technology，信息技术）层负责采集生产过程中的报工、完工、操作人员、检验、异常问题等生产过程数据；工控网 OT（Operational Technology，运营技术）层负责对生产过程中底层加工、生产、物流、检验等各类设备运行参数、实时状态信息进行采集。通过生产看板按领域、车间、工作中心多层次进行信息展示，实现生产过程透明化管理。

图 9　生产现场看板

（3）信息全追溯：通过对生产过程多源异构数据的全面采集，基于产品码按 BOM 层级结构“一键式”生成产品数据包。通过多源信息融合、识别、信息流的协同管理对全过程的质量进行跟踪和追溯，满足治理问题追溯需求，以及支撑跨单位数据包交付。

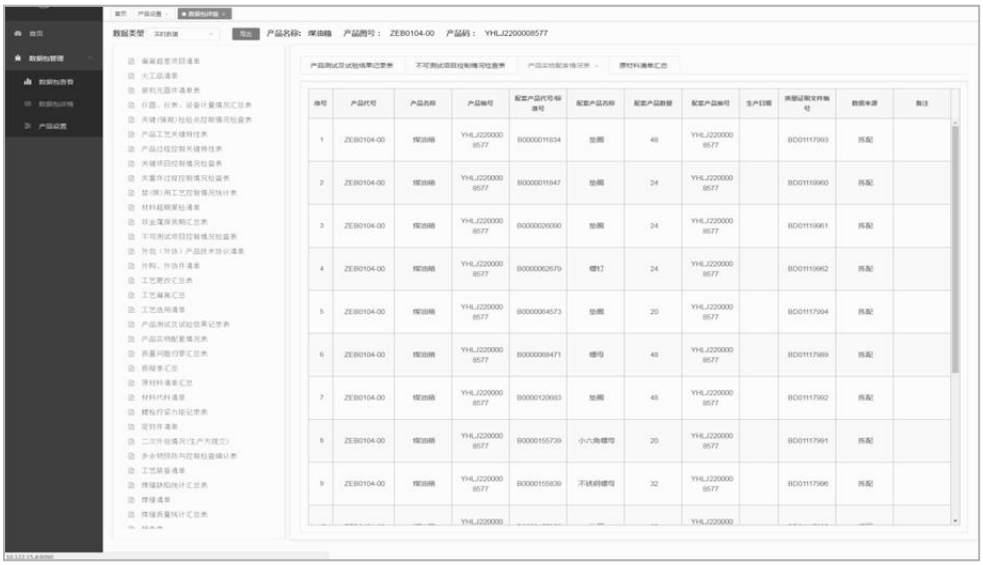


图 10　基于产品数据包的过程全追溯

5　结束语

本文针对航天离散制造资源快速重组和优化配置、质量过程精准控制、跨单位跨专业高效协作等业务需求，以及传统信息系统架构孤立、标准不统一、技术难兼容、数据源不统一等带来的业务集成扩展难度大、生产过程控制和生产决策滞后、上下游协同效率偏低等问题，结合“微服务+中台”的理念和技术，搭建了面向航天及离散制造企业的“技术、业务、数据三中台”的行业特色工业互联网平台架构，阐述了平台构建涉及的工业 PaaS 平台设计、业务中台构建、数据中台构建等关键技术，研发了具有全业务融合、柔性灵活、自主可控、敏捷复制特点的航天离散协同制造工业互联网平台，构建了面向企业全局数据感知、分析和应用的新体系和技术底座。本文研究成果已在某航天企业全面工程应用，初步实现了企业生产运营业务全在线、过程全透明、数据全追溯，为离散制造企业数字化转型和数字化工厂管理提供了可行、有效的平台级系统解决方案。

参考文献

[1]　周济．智能制造——“中国制造 2025 的主攻方向”[J]. 中国机械工程,2015,26(17):2273-2284.
ZHOU Ji. Intelligent Manufacturing——Main Direction of “Made in China 2025”[J]. China Mechanical Engineering,2015,26(17):2273-2284.

[2]　姚锡凡, 景轩, 张剑铭, 等.走向新工业革命的智能制造[J].计算机集成制造系统,2020,26(9):2299-2320.
YAO Xifan, JING Xuan, ZHANG Jianming, et al. Towards smart manufacturing for new industrial

revolution[J]. Computer Integrated Manufacturing System,2020,26(9):2299-2320.

[3] Ding H, Gao R X, Isaksson A J, et al. State of AI-based monitoring in smart manufacturing and introduction to focused section. IEEE/ASME Trans Mech,2020,25:2143-2154.

[4] 郭具涛，洪海波，钟珂珂，等．基于数字孪生的航天制造车间生产管控方法[J]. 中国机械工程,2020,31(7):808-814.

GUO Jutao, HONG Haibo, ZHONG Keke, et al. Production Management and Control Method of Aerospace Manufacturing Workshops Based on Digital Twin[J]. China Mechanical Engineering,2020,31(7):808-814.

[5] 蒋敏，郑力. 面向航空协同制造的工业互联网架构研究与应用.中国科学:技术科学,2022,52(1):3-13.

JIANG Min, ZHENG Li. Industrial internet architecture for collaborative manufacturing of aviation equipment[J]. SCIENTIA SINICA Technologica,2022,52(1):3-13.

[6] 王晨，宋亮，李少昆，等. 工业互联网平台：发展趋势与挑战[J].中国工程科学,2018,20(2):15-19.

WANG Chen, SONG Liang, LI Shaokun, et al. The Industrial Internet platform: trend and challenges[J]. Engineering Science,2018,20(2):15-19.

[7] 百度百科.信息系统架构[EB/OL][2023-07-10]. https:// baike.baidu.com/item/信息系统架构?fromModule=lemma_search-box.

Baidu Baike. Enterprise architecture [EB/OL] [July 10, 2023] .https://baike.so.com/doc/2534127-2677102.html.

[8] 褚健，谭彰，杨明明．基于工业操作系统的智能互联工厂建设探索[J].计算机集成制造系统,2019,25(12):3026-3031.

CHU Jian, TAN Zhang, YANG Mingming. Construction of intelligent Internet factory based on industrial operating system[J]. Computer Integrated Manufacturing System,2019,25(12):3026-3031.

[9] 中国信息通信研究院.云计算白皮书[R].2016.

China Academy of Information and Communication Technology. Cloud Computing White Paper [R]. 2016

[10] 余晓晖，刘默，蒋昕昊，等.工业互联网体系架构 2.0[J].计算机集成制造系统,2019,25(12):2983-2996.

Yu Xiaohui, Liu Mo, JIANG Xinhao, et al. Industrial Internet Architecture 2.0[J]. Computer Integrated Manufacturing System,2019,25(12):2983-2996.

[11] 百度百科．企业架构 [EB/OL][2023-07-04].https://baike.baidu.com/item/业务中台?fromModule=lemma_search-box.

Baidu Baike. Enterprise architecture [EB/OL] [July 4, 2023] https://baike.baidu.com/item/ Business center? From Module=lemma_Search box.

[12] 陈新宇, 罗家鹰, 邓通, 等. 中台战略:中台建设与数字商业[M]. 北京:机械工业出版社,2019.8.
CHEN Xinyu, LUO Jiaying, DENG Tong, et al. Middle-Platform Strategy: Middle-Platform Construction and Digital Commerce[M]. Beijing：China Machine Press，2019.8.

[13] Yuan Y, Tang X C, Zhou W, et al. Data driven discovery of cyber physical systems. Nature Commun,2019,10:1-9.

[14] 张卫, 石涌江, 唐任仲, 等. 基于工业互联网的制造与服务融合技术[J]. 中国科学:技术科学,2022,52(1):104-122.
ZHANG Wei, SHI Yongjiang, TANG Renzhong, et al. Research on manufacturing and service integration technology based on industrial internet. SCIENTIA SINICA Technologica,2022,52(1):104-122.

[作者简介]

钟珂珂（1987—），男，工学硕士，高级工程师，研究方向：航天先进制造技术、工业互联网技术研究。

郭具涛（1988—），男，工学博士，研究员，研究方向：数字化集成制造技术研究。

刘骁佳（1990—），男，工学博士，高级工程师，研究方向：工业大数据、人工智能技术研究。

陈晓棠（1982—），男，工学学士，高级工程师，研究方向：新型工业互联网平台开发技术研究。

刘晓（1987—），女，工学硕士，高级工程师，研究方向：新型工业互联网技术研究。

向美红（1975—），女，工学硕士，工程师，研究方向：工业互联网应用技术研究。

洪海波（1986—），男，工学博士，高级工程师，研究方向：智能制造、数字化检测技术研究。

面向工业互联网的推-抓协作式机械臂精细化自主抓取方法

何自明[1]，杨喆瑞[1]，王柯新[1]，史豪斌[1]，吉庆兵[2,3]

（1. 西北工业大学计算机学院，陕西 西安 710072）

（2. 中国电子科技集团公司第三十研究所，四川 成都 610041）

（3. 西北工业大学网络空间安全学院，陕西 西安 710072）

摘　要：机械臂精准作业是生产线智能化升级的重要功能性保障，而日渐扩增的工业应用场景对机械臂“控得精”提出了新的要求。现有机械臂抓取方法在面对不规则目标和物体间紧密排布缺乏抓取空间的场景成功率和效率显著下降。针对该问题，本文提出一种基于强化学习的推-抓协作式机械臂精准控制方法。该方法通过模仿人眼注意力机制提升不规则目标的抓取姿态识别模型的准确率；其次，建模杂乱场景下机械臂抓取任务的马尔科夫决策过程，设计基于语义分割和深度强化学习的推-抓协同策略；最终实现面向复杂环境的协作式机械臂端到端路径规划框架，精细化奖励塑形方案和最佳抓取点的可靠推荐使得本框架的效能进一步提升。所提方法在包括工业流水线分拣在内的 3 个任务，5 种不同场景中取得了比现有流行方法更高的抓取成功率和更少的动作总数，展示了其在工业互联网环境下的高效性和实用性。

关键词：工业互联网；深度强化学习；机械臂抓取；目标检测；注意力机制

Refined autonomous grasping method for push-grasp collaborative manipulator for Industrial Internet

HE Ziming[1], YANG Zherui[1], WANG Kexin[1], SHI Haobin[1], JI Qingbing[2,3]

（1. School of Computer Science, Northwestern Polytechnical University, Xi’an 710072, China）

（2. The 30th Research Institute of China Electronics Technology Group Corporation, Chengdu 610041, China）

（3. School of Cybersecurity, Northwestern Polytechnical University, Xi’an 710072, China）

Abstract: The accurate operation of manipulators is an important functional guarantee for the intelligent upgrading of production lines, and the increasing industrial application scenarios put forward new requirements for the "precision control" of manipulators. The success rate and efficiency of existing manipulator grasping methods are significantly reduced in the face of irregular targets and scenes with tight arrangement between objects and lack of grasping space. To solve this problem, this paper proposes a precise control method of push-grasp cooperative manipulator based on reinforcement learning. This method imitated the human eye attention mechanism to improve the accuracy of the grasping posture recognition model for irregular targets. Secondly, the Markov decision process of the grasping task of the manipulator in the cluttering scene is modeled, and the push-grasp collaborative strategy

通信作者：史豪斌，shihaobin@nwpu.edu.cn；吉庆兵，jqbdxy@163.com

基金项目：国家自然科学基金重大研究计划项目（No.92267110）；国家重点研发计划项目（No.2023YFF0905604）；国家自然科学基金面上项目（No.62076202）；陕西省重点研发计划项目（No.2023-YBGY-354）

Foundation Items: The Major Research Project of National Natural Science Foundation of China (No.92267110), The National Key R\&D Program of China (No.2023YFF0905604), The National Natural Science Foundation of China (No.62076202), The Shaanxi Province Key Research and Development Program of China (No.2023-YBGY-354)

based on semantic segmentation and deep reinforcement learning is designed. Finally, an end-to-end path planning framework for collaborative manipulators in complex environments is realized, and the efficiency of this framework is further improved by the refined reward shaping scheme and the reliable recommendation of the best grasp point. The proposed method achieves higher success rate and fewer total number of actions than the existing popular methods in three tasks and five different scenarios including industrial sorting, demonstrating its efficiency and practicability in the industrial internet environment.

Key words: industrial internet, deep reinforcement learning, manipulator grasping, object detection, attention mechanism

1 引言

工业互联网构建起覆盖全产业链、全价值链的全新制造和服务体系，成为我国制造业从“中国制造”向“中国智造”转型的关键支撑。机械臂精细化操作方法是智造升级的重要抓手，现有工作大多集中在无目标抓取的研究上，在工业制造领域的应用价值有限[1]。而目标导向的机械臂抓取方法面对堆叠抓取空间和不规则目标都不可避免的出现效果明显下降，因此亟待研究适用于以上复杂工业场景的机械臂精准作业方法，以扩展机械臂的实际应用范围[2]。

近年来，学术界和工业界均提出多种解决方案以尝试提升机械臂的抓取能力。Levine[3]等人提出了一种基于学习的手眼协调方法，使用卷积神经网络预测末端执行器的运动对抓握成功概率的影响，采用单目相机对机械臂进行伺服控制。Jeff Mahler [4]等人提出的 Dex-Net[5]框架，通过训练得到的 Grasp Quality 卷积神经网络（GQ-CNN）将深度图像作为输入，预测抬起、运输和摇晃物体时机械臂抓取的成功概率，实现了从模拟到真实环境的迁移。Lenz[6]等人提出了两步级联结构来剔除弱可能的抓取操作同时评估抓取策略。基于 Lenz 的研究，Redmon[7]等人提出了 SingleGrasp 算法，通过卷积神经网络对 RGB-D 图像中的对象进行分类，并预测抓取边界框。由此衍生的 MultiGrasp[8]方法能够预测每张图像的多个抓取姿势。

试错式学习方式的强化学习范式近年来成为机械臂路径规划任务领域的研究热点[9-11]。Lerrel 等人[12]提出了一种多阶段学习方法，对被遮挡的物体表现出良好的泛化能力。Dmitry [13]等人提出的 QT-OPT 方法使用约 60 万次的真实抓取操作数据来训练深度神经网络，该算法主要在现实场景中进行闭环抓取。为了减少深度强化学习算法的训练时间，Breyel[14]等人研究了奖励函数、预训练策略和课程学习对深度强化学习的影响。Clavera[15]通过将任务先验知识纳入状态空间和奖励函数来加速算法收敛，解决了深度强化学习易陷入局部最优解的问题。

现有的监督学习和强化学习方法在提升机械臂抓取能力方面取得了显著进展。但在面对环境的不确定性、目标的不规则性、目标物体的可夹取空间不足、奖励稀疏等问题时，效果仍不尽如人意。受人类作业方式和现有工作[16]的启发，本文设计并实现了一种基于深度强化学习的端到端推-抓协作式机械臂精细化控制框架，并通过三个阶段来训练。概括来说，本文的主要研究工作如下：

（1）为了提升不规则目标的抓取成功率和效率，将人类注意力机制应用于抓取姿态识别网络，通过预训练模型提前获取待抓取目标的推荐抓取点；

（2）为了求解堆叠结构复杂场景下的目标抓取问题，针对不同任务建模协作式马尔可夫决策过程，设计精细化奖励塑形方案克服奖励稀疏造成的学习效果欠佳的问题；

（3）为了提升排布紧密可抓取空间不足场景下抓取成功率，引入探索性推动、目标性推动和目标性抓取三种动作基元，设计基于强化学习的推-抓协作式网络，根据策略输出自主选择最佳的动作执行顺序；

（4）为了验证所提方法在工业互联网环境下的实效，开展了包括工业流水线分拣在内的 3 个任务，5 种不同场景中的实验调查与分析。结果表明本文所提方法对比现有流行方法在抓取成功率和动作总数指标上均具有明显优势。

2　问题建模

2.1　问题定义

本文以工业界广泛使用的 6 自由度 UR5（Universal Robots 5）机械臂为例定义抓取系统。UR5 机械臂的模型结构如图 1 所示，它包含由 7 个刚体连杆和 6 个关节。机械臂通过各个关节的旋转来实现末端执行器在三维空间内以任意姿态运动。抓取检测、规划和控制系统共同组成了机械臂的抓取系统，如图 2 所示，抓取检测系统的关键组件包括机械臂、末端执行器及相机等，要完成的任务主要是目标物体定位、物体姿态估计、抓取姿态估计以及运动规划，其中不规则目标的抓取姿态估计和杂乱环境下的抓取运动规划是本文研究重点，其对应的问题定义如下：

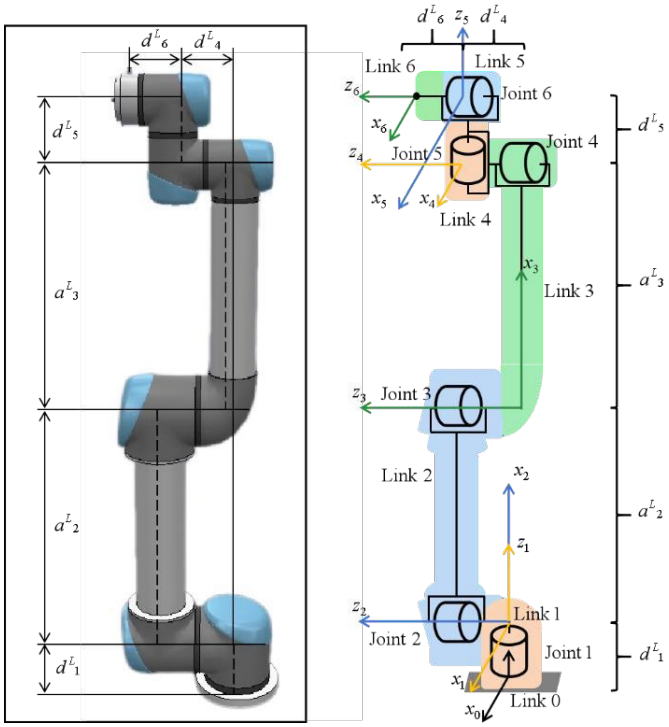


图1 UR5机械臂构型图

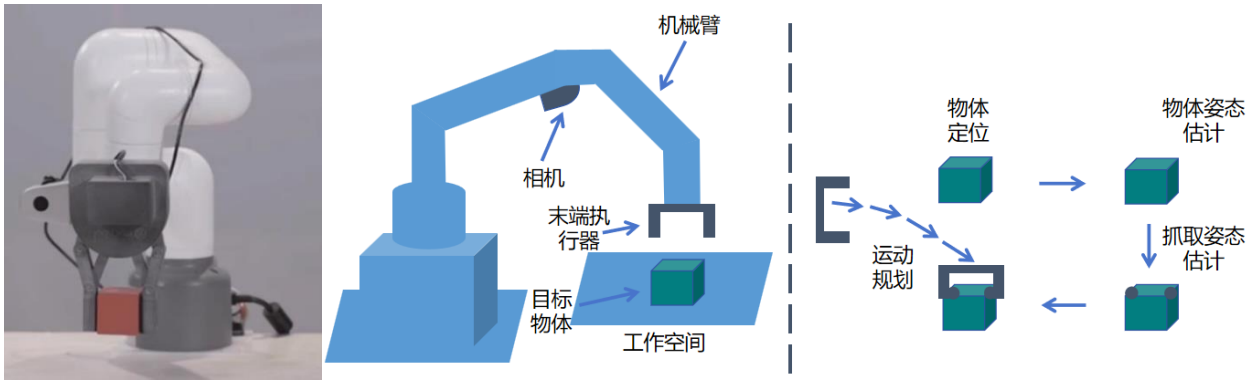


图2 左图：六轴机械臂实物抓取任务，右图：抓取检测系统示意图

不规则目标抓取姿态识别：给定机械臂上方拍摄的不规则待抓取目标的俯视图，以高识别准确度为约束条件输出末端执行器（夹爪）的推荐抓取位置和角度，即有效抓取框，同时重定向到高度图中。

杂乱环境下机械臂抓取规划：机械臂从一系列密集无序的物体中选取目标物体，通过有限的推抓动作，以最少的动作总数获取目标。杂乱场景中的对象可以具有不同的形状、大小、颜色、重量和其他物理属性。目标可以在密集杂乱场景中以任意姿态被遮挡放置在任意位置。

2.2 马尔可夫决策过程建模

强化学习通过与环境的交互来解决序列决策问题，在不断试错中提升自己的策略。通常以马尔科夫决策过程（Markov Decision Process, MDP）来描述强化学习的学习流程，如图 3 所示。MDP 由五元组$<\boldsymbol{S},\boldsymbol{A},P,\boldsymbol{R},\gamma>$组成，其中$\boldsymbol{S}$表示状态空间；$\boldsymbol{A}$表示动作空间；$P$为状态转移概率，表示从当前状态$s_t$到下一状态$s_{t+1}$的转移概率；$\boldsymbol{R}$为奖励函数，描述智能体在状态$s$采取动作$a$之后环境反馈的奖励；折扣因子$\gamma \in [0,1)$，$\gamma$越大表示智能体越关注长期收益。强化学习的目标是通过学习适当的策略π，使智能体在未来的决策序列中最大化期望回报G_t。

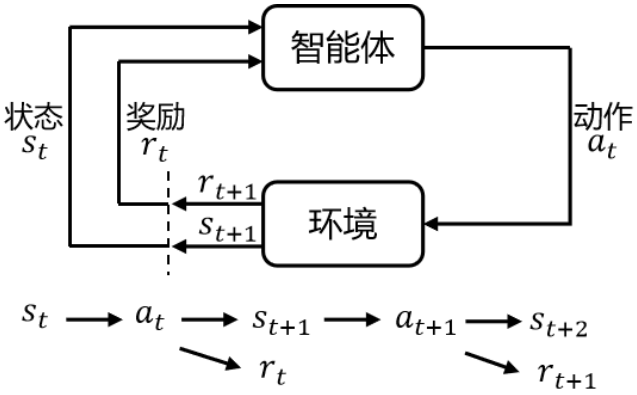


图 3 马尔科夫决策过程

状态空间：将相机倾斜固定在工作空间上方，通过将 RGB-D 数据投影到 3D 点云上，然后在重力方向上进行正交向上的投影以获得 RGB-D 通道的高度图。相机拍摄的彩色高度图c_t、深度高度图d_t以及目标的掩码m_t共同构成了t时刻状态s_t。

动作空间：末端执行器沿 X、Y、Z 轴的平移来改变(x,y,z)位置，通过绕自身的 X、Y、Z 轴旋转，改

变滚动(Roll)、俯仰(Pitch)、偏航(Yaw)角度。本文只进行自上而下的抓取，因此末端执行器的抓取姿态减少为 4 个自由度$(x, y, z, roll)$，当x和y确定后，可以根据 D 通道的高度图确定z。

奖励函数：常见的非目标性抓取任务的奖励一般设置为二值奖励，即抓取成功给予 1 奖励，抓取失败则为 0 奖励。目标性抓取任务涉及到是否抓取到正确目标，因此一般设置为三段式奖励，除了以上额外添加抓取错误目标成功的奖励$\alpha \in (0,1)$。

3　目标抓取姿态估计网络

本文将注意力机制和强化学习引入到可抓取点的识别流程中，提出一种适用于不规则目标的抓取姿态估计网络，网络架构示意图如图 4 所示。识别网络主要包括特征提取器、对象定位与行动、分类器 3 个模块。

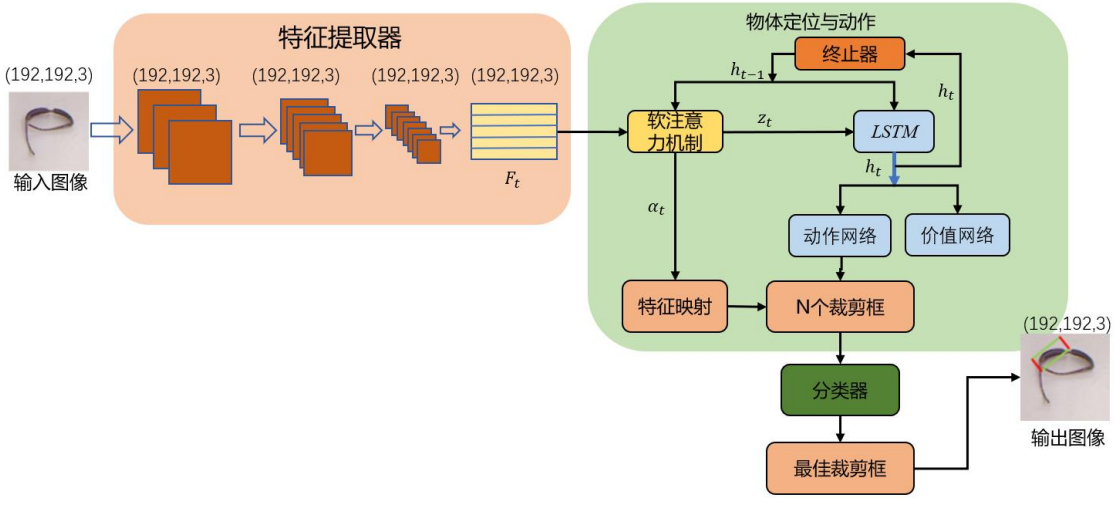


图 4　目标抓取姿态估计网络架构

3.1　对象定位与行动模块

对象定位与行动是抓取姿态架构的核心模块，通过软注意力机制(Soft Attention Mechanism，SAM)、长短期记忆网络(Long Short-Term Memory, LSTM)以及强化学习算法来实现智能体动作与可抓取位置的定位的关联。具体网络运作流程如图 5 所示，Soft Attention 对 CNN 神经网络输出的 Fully Connected Layer 做特征比较，给予每个特征区域不同的权重后送入 LSTM。在 LSTM 中，将每次的隐藏状态串联后输出新的隐藏状态，当作 REINFORCE 算法的环境状态，送入 Action Network 以及 Value Network 得到该次的动作和状态值。使用 Action network 得到的动作以及a_t过滤后的特征图位置，对图像执行动作，产生 Cropping box，送入辨别器辨识，回传奖励。

SAM 分别输入从 CNN 运算后的特征向量F_t，以及从前一个 LSTM 获得的输出隐藏状态h_{t-1}，将两者分别乘上权重W_F、权重$\mathrm{W_h}$，相加后以$relu$激励函数输出G_t，如式(1)。之后再将G_t乘上向量W_g并加上偏差b_g做线性运算输出s_t，如式(2)，再经过 softmax 激励函数得到α_t，即为关注程度权重如式(3)。将权重α_t与特征向量F_t相乘后把每个特征区域做相加即为综合向量z_t，如式(4)：

$$G_t = relu(\mathrm{W_h} h_{t-1} + W_F F_t) \tag{1}$$

$$s_t = W_g G_t + b_g \tag{2}$$

$$\alpha_t = softmax(s_t) \tag{3}$$

$$z_t = \sum_i \alpha_t^i v_t^i \tag{4}$$

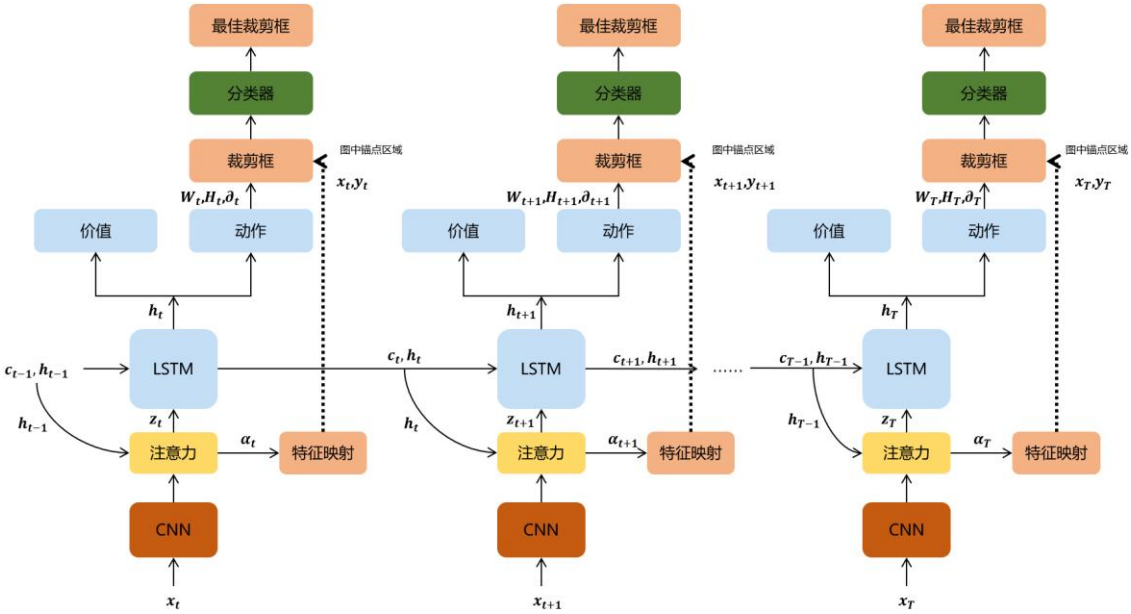


图 5 单回合网络运作流程示意图

3.2 辨别器设计

本文模仿人类视觉系统设计辨别器模型架构，共由 5 个神经网络与一个视网膜传感模块构成。当包含待抓取目标的图片进入视网膜传感模块会被截取为一个区域影像，我们称为一瞥c_t。l_t代表 glimpse(c_t)的中心点坐标，而g_t表示 Glimpse 影像特征与其中心坐标l_t的综合信息，g_t与前次的h_t进入 Core Network，通过 LSTM 循环神经路进行信息整合与运算，最后输出h_t，h_t作为 Location Network、Value Network 的输入，由 Location Network 输出l_t，由 Value Network 输出v_t，而在 LSTM 循环网络最后一次输出h_t时，才会进入 Action network 输出a_t，作为辨别器的输出项。辨别器模型内部流程如图 6 所示。

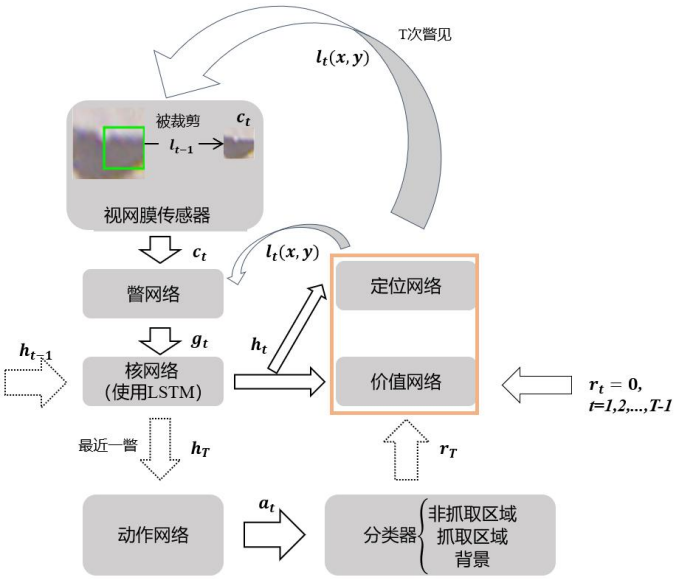


图 6 辨别器模型内部细节图

3.3　训练方式

此架构的损失函数总共有两个，动作损失函数L_A，状态损失函数L_V，形式化为：

$$L_A = \nabla J(\theta) \approx \frac{1}{N}\sum_{t=1}^{N}(R_t - v_t)\nabla \log p_\theta(a_t^n|s_t^n) \tag{5}$$

$$L_V = \sum_{t=1}^{N}\frac{(R_t - v_t)^2}{N} \tag{6}$$

以下列出完整的模型训练过程，T 为一回合最大步数，J_{max}为训练终止条件。

算法 1　目标抓取姿态识别网络训练算法伪代码

1）初始化：假设共享全局参数θ；Action Network 参数为θ_a、Value Network 参数为θ_v，Max loop M，Step counter $j \leftarrow 1$

2）**Repeat**

3）　初始化梯度$d\theta \leftarrow 0$，初始化梯度$d\theta_v \leftarrow 0$、$d\theta_a \leftarrow 0$，$t_{start} = t$，取得影像x_j

4）　**Repeat**

5）　　由 CNN 提取x_j特征，返回特征F_j

6）　　初始化 LSTM 状态c_0、h_0

7）　　**For** $t \in [1,2,\dots,T]$ **do**

8）　　根据F_j与h_{t-1}由注意力机制取得特征状态z_t

9）　　将z_t、c_{t-1}、h_{t-1}输入 LSTM

10）　　LSTM 返回隐藏状态h_t，　$s_t \leftarrow h_t$

11）　　根据策略$\pi(a_t|s_t;\theta')$采取动作a_t，返回奖励r_t

12）　　Value Network 根据s_t，返回v_t单值

13）　　$t \leftarrow t+1$

14）　　**End For**

15）　　**For** $t \in [t_{end}-1,\dots,t_{start}]$**do**

16）　　$R \leftarrow r_t + \gamma R$

17）　　计算梯度θ_v' ：$d\theta_v \leftarrow d\theta_v + \frac{\partial(R_t - v(s_t;\theta_v'))^2}{\partial\theta_v'}$

18）　　计算梯度θ_a ：$d\theta \leftarrow d\theta + \nabla_{\theta_a}\log\pi(a_t|s_t;\theta_a)\big(R_t - v(s_t;\theta_v')\big)$

19）　　**End for**

20）　　执行异部更新至全局参数，使用$d\theta$更新θ，使用$d\theta_a$更新θ_a；使用$d\theta_v$更新θ_v

21）**Until** $j > J_{max}$

4 机械臂推-抓协同作业框架

4.1 推-抓协同框架设计

为了应对杂乱场景下堆叠和紧密排列导致的目标不完全可见问题，首先利用探索式推动动作基元找出“看不见”的目标，通过探索任务找到待抓取目标并推开足够空间。一旦找到目标，进行协同任务决定执行目标性推动或目标性抓取动作。如果决定抓取，则根据上文预训练的目标抓取姿态识别网络找出合适的抓取角度和位置。整体框架如图 7 所示。

本文使用 RGB-D[17]相机捕获工作空间图像，通过预训练的语义分割模块预测目标掩模，并投影得到彩色、深度和目标掩模高度图。构建高度图后，将图像输入动作评判器，预测并输出推动和抓取 Q 值[18]图，策略综合 Q 值和先验知识协同完成抓取任务。对可见目标，使用全卷积编码器-解码器[19]网络输入高度图，通过残差网络[20]提取特征，再通过 DenseNet[21]生成特征，预测推动和抓取 Q 值图。对不可见目标，机械臂先执行推动动作进行探索，直到目标可见。推动动作的 Q 值图和杂乱状态预测图构成探索阶段的先验，先验概率分布图由两者相乘得到。为了减少无效推动，构建高斯分布[22]的无效推动预测图。最终策略通过矩阵哈达玛积[23]决策。

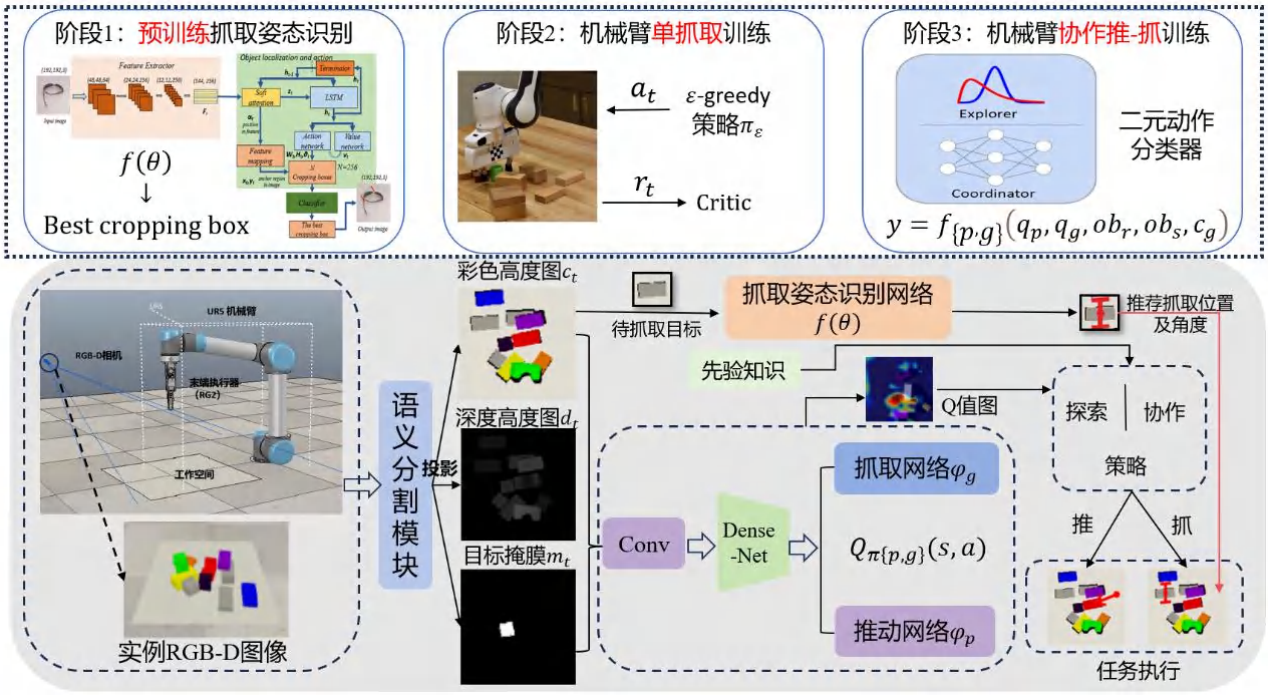


图 7 推-抓协作控制框架图

4.2 推-抓协作任务的 MDP 建模

有别于 2.2 节中建立的杂乱环境下机械臂抓取系统的通用 MDP，我们使用基于环境复杂度的奖励塑形方法和预训练姿态估计模型分别简化了动作空间、改进了奖励函数设置，状态空间保持不变，具体如下：

动作空间：推动动作的动作空间A_p为如下，其中n_{img}为原始图像像素大小。末端执行器以坐标(x_p, y_p)为起始位置，朝离散化的16个方向中的第k_p个执行推动动作，推动距离为待抓取物体最长边长的一半。

$$A_p = \{(x_p, y_p, k_p), 0 \le x_p, y_p \le n_{img}, 0 \le k_p < 16\} \tag{7}$$

策略网络输出的抓取动作对应的动作空间A_g为预训练目标抓取姿态模型的偏置量，即在推荐的抓取位置和角度进行微调：

$$A_g = \{(\Delta x_g, \Delta y_g, \Delta k_g), -\Delta n_{img} \le x_p, y_p \le \Delta n_{img}, -3 \le \Delta k_g \le 3\} \tag{8}$$

奖励函数：在推动动作奖励函数设计部分本文引入了环境复杂度变化τ这一概念，通过不同状态高度图之间差异的总值来判断环境复杂度的改变，形式化为：

$$\tau = \frac{1}{N}\sum_{i,j=1}^{N}(p_i - q_j)^2 \tag{9}$$

其中p_i和q_j分别为推动前后状态s_{t+1}和s_t中的归一化后的像素值大小。完整的奖励函数设置如下：

$$R = \begin{cases} 1 & \text{抓取成功，抓取} \\ 0 & \text{抓取失败，抓取} \\ 0.3 & 0.1 \le \tau < 0.24\text{，推动} \\ 0.5 & 0.24 \le \tau < 0.4\text{，推动} \\ 0.7 & 0.4 \le \tau \le \text{，推动} \\ -0.1 & \text{其它情况，推动} \end{cases} \tag{10}$$

4.3　训练方式

本文设计三阶段训练架构并给出推-抓协作控制算法流程，如算法 2 所示。在仿真环境训练过程中，本文通过最小化 TD 误差δ_t来训练推抓协同策略，利用 Huber 损失进行优化。δ_t的定义如式(11)所示，Huber 损失如式(12)所示。通过二值交叉熵损失训练二元动作分类器，分别如式(12)和式(13)所示。其中y表示动作判断器$f_{\{p,g\}}$的预测结果，$\bar{y}$表示真实值，目标物体被成功抓取时其值为 1，反之为 0。

$$\delta_t = Q(s_t, a_t|\theta_t) - (R_{a_t}(s_t, s_{t+1}) + \gamma \max_a Q(s_{t+1}, a|\theta_t^-)) \tag{11}$$

$$L_\delta = \begin{cases} \frac{1}{2}\delta_t^2 & |\delta_t| \le 1 \\ |\delta_t| - \frac{1}{2} & |\delta_t| > 1 \end{cases} \tag{12}$$

$$L_y = -(\bar{y}\log y + (1-\bar{y})\log(1-y)) \tag{13}$$

算法 2　推-抓协作控制算法伪代码

1）初始化：动作评判器 C 的经验缓冲池B_c，π_c的经验缓冲池B_π，训练次数i，$\varepsilon - greedy$策略π_ε，图像I，推动或抓取网络Φ，最大 Q 值q，先验知识$D = (r_b, n_b, c_g)$

2）**While** training **do**

3）　重置模拟环境并随机掉落物体

4）　随机设置一个目标 T

5）　**While** T 尚未被成功抓取 **do**

6）　　*i*++

7） 利用(I,T)进行语义分割得到目标掩膜M

8） 利用目标掩膜得到当前状态s_t，并输入至推动网络和抓取网络得到相应 Q 值

9） **If** $i < 1000$ **then**

10） 执行$\varepsilon - greedy$策略$\pi_\varepsilon(Q_p, Q_g) \rightarrow a_t$

11） **Else**

12） 执行策略$\pi_c(Q_p, Q_g, D) \rightarrow a_t$

13） 根据抓取结果标记$\bar{y}$，将(Q_p, Q_g, D)、$\bar{y}$保存到B_π中：$B_\pi \leftarrow B_\pi \cup \{\bar{y}, (Q_p, Q_g, D)\}$

14） 从B_π中采样一批来训练f_a

15） **End If**

16） 计算奖励R_t，将s_t, a_t, R_t保存至B_c

17） **If** 非目标物体被抓住 **then**

18） 将额外的掩模m'和奖励R，保存到B_c中

19） **End If**

20） 从B_c采样样本训练 C

21） **End While**

22） **End While**

5 实验分析

4.1 实验设置

本文使用 Cornell grasp dataset 验证目标抓取姿态识别模型的有效性，并利用 Bullet 和 CoppeliaSim 引擎搭建仿真实验平台来验证推-抓协作框架的效能。实验采用的部分数据集和仿真环境如图 8 所示。

(a) Cornell grasp dataset 部分数据可视化 (b)机械臂流水线分拣抓取任务可视化

图 8 实验数据集及任务场景

4.2 评价指标与基线

抓取姿态识别被视为一个监督学习任务，因此选用混淆矩阵对应的复合指标——准确率(Accuracy)、

预测不可夹取数据准确度(PRECISION NGR)、预测可夹取数据准确度(PRECISION GR)、预测背景数据准确度(PRECISION BG)作为评价指标，对应的计算方式如下：

$$PRECISION\ GR = \frac{TP}{TP + FN + FGB}$$
$$PRECISION\ NGR = \frac{TN}{FN + TN + FNB}$$
$$PRECISION\ BG = \frac{BN}{FGB + FBG + BN} \tag{14}$$
$$Accuracy = \frac{TP+TN+BN}{TP+FN+FGB+FN+TN+FNB+FGB+FBG+BN}$$

在实际应用中，我们希望机械臂能以更少的动作成功抓取到目标，因此评价指标被量化为式(15-17)。其中，ϕ_1表示抓取成功率，s_i表示第i次实验中机械臂抓取成功的次数，S_i表示第i次实验中机械臂抓取动作的总次数，N为实验总次数，ϕ_2表示任务完成率，M表示动作总数由推和抓动作共同组成。

$$\phi_1 = \frac{\sum_{i=0}^{N} \frac{s_i}{S_i}}{N} \times 100\% \tag{15}$$

$$\phi_2 = \frac{n}{N} \times 100\% \tag{16}$$

$$M = M_p + M_g \tag{17}$$

以下算法被选作为比较面向目标的机械臂抓取的基线算法：1）Clutter-Prior[26]（通过深度高度图构建与 Q 值图类似的推动动作的概率图）；2）GOPG[27]（经验池重新标记用于提高训练效率）；3）SP-Reward（不使用精细化奖励塑形）；4）RAND（不使用二元动作分类器）。

4.3　实验结果与分析

1）不规则目标可抓取点识别实验

本文将所提方法与常见目标识别骨架网络 LETNET5 和 VGG19 进行了性能对比，如图 9 所示。由实验结果可知加入注意力机制和强化学习方法的识别模型性能优于其他两个模型，究其原因为所提识别模型中每张图像都会有十次类似人眼的综合信息。训练后期，经注意力机制处理的十瞥综合信息大多注意在目标上，减少了背景信息的计算干扰，有效提高识别精度。

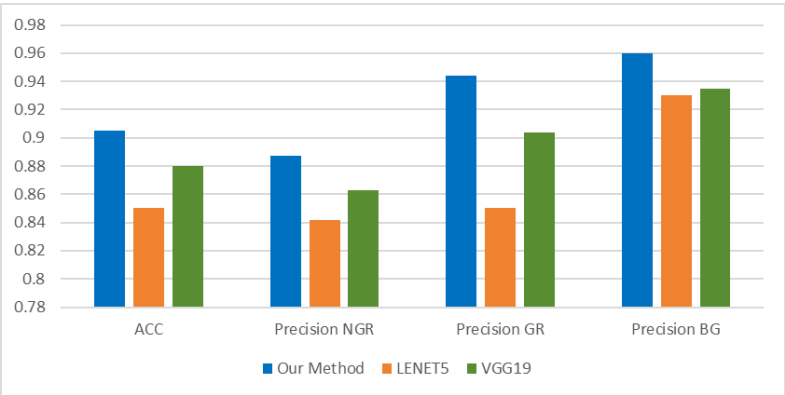


图 9　不同模型的识别效果比较

将预训练模型推荐的可抓取框进行了可视化，并对比了添加终止器模块与否对最终性能的影响。实验结果如图 10 所示，由于加入终止器可以有条件的停止动作，减少资源的计算，同时保证动作不会偏离好的奖励方向，因此推荐的可抓取框比固定瞥 10 眼更加准确。总的来说，本工作提出的抓取姿态识别预训练模型可以适用不规则目标，并为抓取系统推荐精准的可抓取姿态。

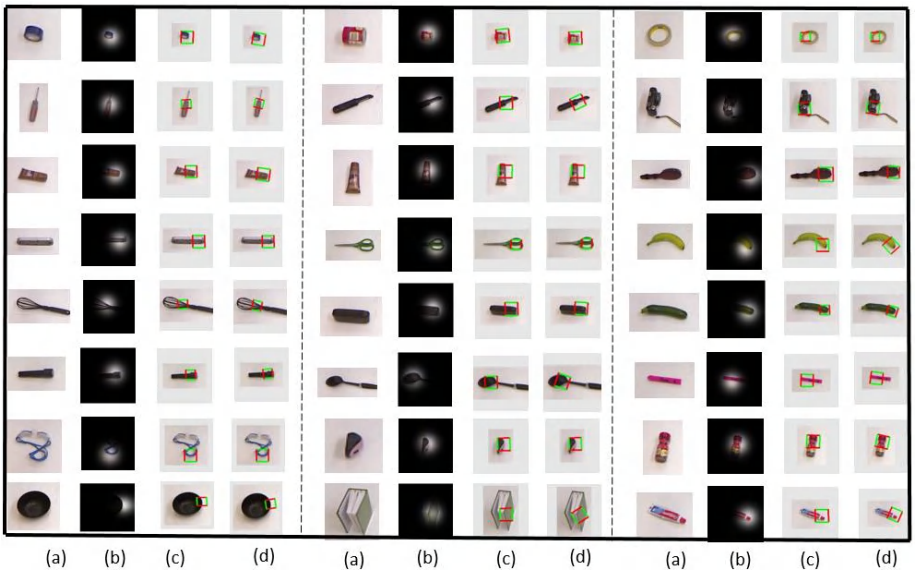
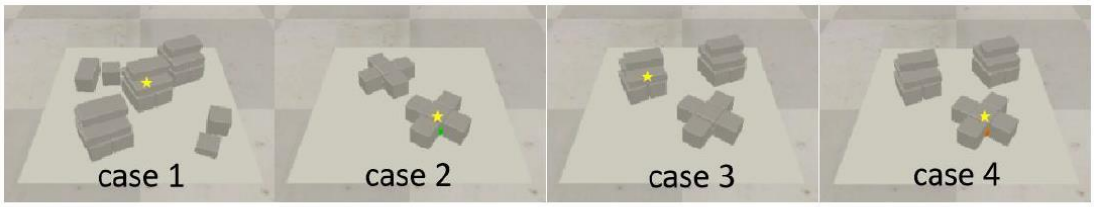


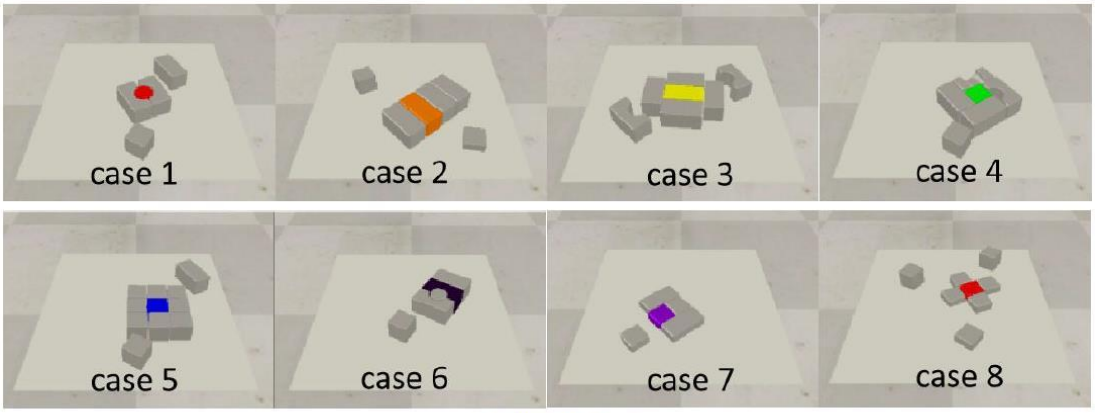
图 10 预测的抓取框可视化。(a)原始图像，(b)注意力机制聚焦位置，(c)预测的夹取框，(d)调整后的夹取框位置。

2）探索与协作任务实验

测试阶段设置 8 个任务，目标物体被其余物体紧密地包围，直接进行抓取操作难以成功完成任务，如图 11 所示。其中彩色物体为目标物体，在实验结果中，按照不同的任务，分别被记为$case_i$表示该任务下的第i个测试用例。测试阶段对每个测试用例均执行 50 次运行，记录每次运行结果并取均值作为每个方法在各个测试场景的任务成功率和动作总数。



(a)探索任务场景



(b)合作任务场景

图 11 探索与协作任务实验环境可视化

图 12 为基线方法 Clutter-Prior、SP-Reward、RAND 与本文所提方法在训练阶段的任务完成率对比，由实验结果可以看出本章节提出的单目标协同算法在训练阶段有着相较于其他基线方法更好的效果。基线算法和本文算法在各个测试用例的表现如图 13 所示，其中，图 13(a)展示了各算法在探索任务上的表现，图 13(b)展示了各算法在合作任务中的表现。平均性能如表 1 所示。

由图 13 和表 1 所示，本文方法在任务完成率和动作总数方面均优于其他方法。在更困难的合作任务场景所提方法取得了 88%的平均任务成功率和 3.8 的平均动作总数。相比之下，RAND 方法的任务成功率为仅为 20%，说明了本文算法中二元动作分类器的有效性。Clutter-Prior 取得 78%的成功率，但由于其最初设计用于目标可知的任务，因此在目标及周围物体动作推断方面存在一定不足，故性能也不如本文方法。

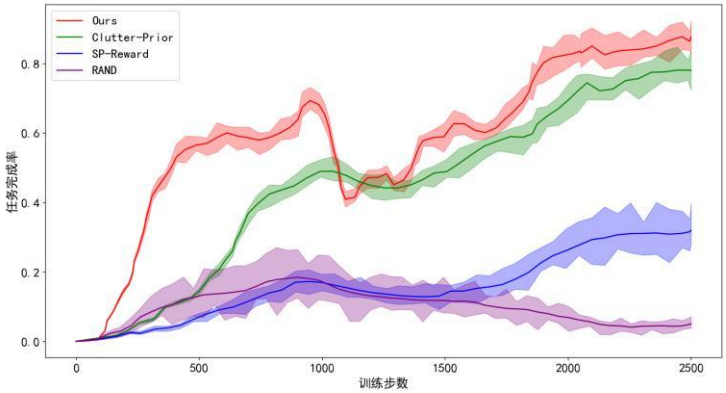
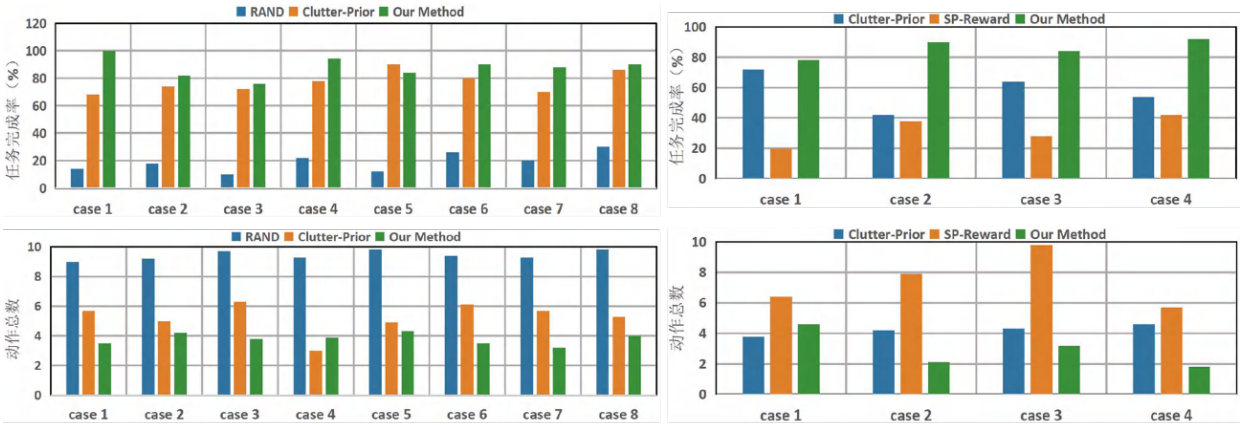


图 12 训练阶段不同算法任务完成率对比



(a) 探索任务　　(b) 合作任务

图 13 两种任务下完成率、动作总数对比

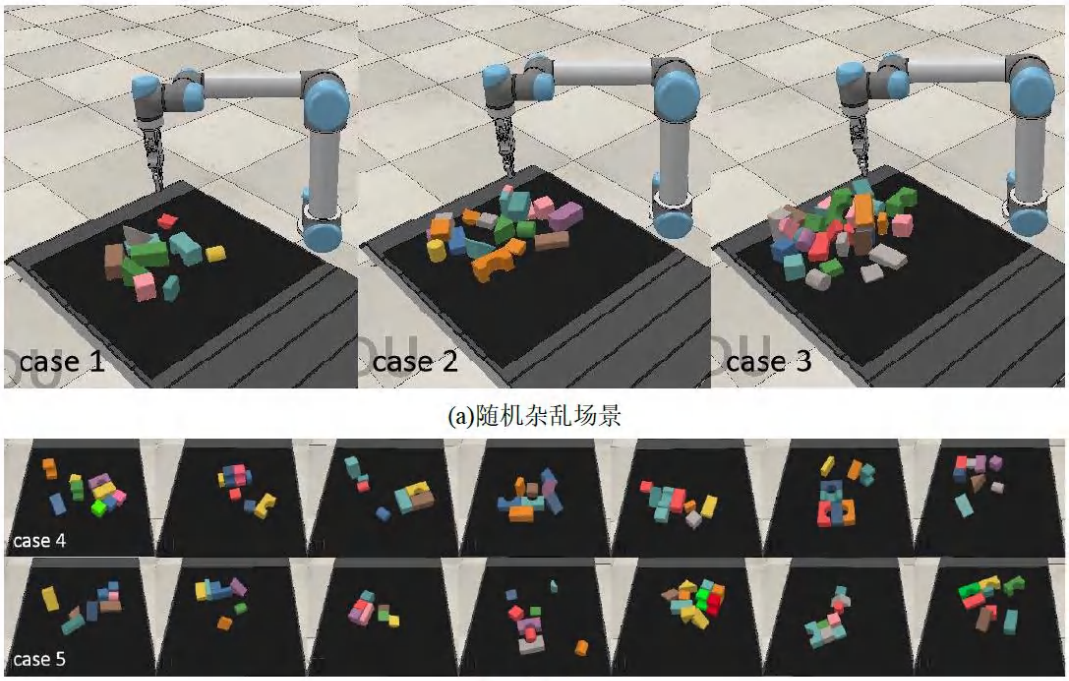
表 1 两种任务下完成率、动作总数平均值

任务类型	算法	任务完成率（%）	动作总数
探索任务	Clutter-Prior	58	4.3
	SP-Reward	32	8.6
	Our Method	**86**	**2.9**
合作任务	RAND	20	9.4
	Clutter-Prior	78	5.3
	Our Method	**88**	**3.8**

3）传送带分拣任务实验

图 14 是工业传送带分拣任务的仿真建模，包括不同程度的随机杂乱场景和不同分布的紧密排列场景。对于紧密排列的情况，如果目标物体被成功识别，机械臂更倾向于抓住目标，但由于周围没有足够的空间，接下来会转而执行推动动作。当目标对象被堆叠不可见时，机械臂倾向于执行推动动作来重新排列位置，一旦物体暴露在相机中并被成功检测到，将类似于紧密排列情况执行后续的动作。

基于上述观察，机械臂的动作序列完全符合预期。在随机杂乱测试场景中，随着杂乱程度的增加，协同算法的任务完成率略有下降，但最低值仍高达 86.7%，表明协同算法由传送带产生的随机杂乱场景中取得了较好的效果，并且算法表现出良好的鲁棒性。在紧密排列的 case4、case5 场景中，协同算法平均任务完成率约为 88%。如表 2 所示，本文所提算法在平均任务完成率、平均动作总数以及平均抓取成功率上的优秀表现，表明算法能够较好地完成工业随机杂乱场景和紧密排列场景的抓取任务。



(a)随机杂乱场景

(b)紧密排列场景

图14 传送带分拣仿真环境各任务可视化

表 2 完成率、动作总数平均值

任务类型	算法	任务完成率（%）	动作总数	抓取成功率（%）
Case 1-3	Clutter-Prior	75	5.6	73
	GOPG	79	9.2	63
	Our Method	**92**	**1.7**	**81**
Case 4-5	Clutter-Prior	60	6.8	72
	GOPG	71	9.5	61
	Our Method	**88**	**3.1**	**84**

6 结束语

本文聚焦于工业互联网智造升级的核心问题，面向流水作业中机械臂物品自主抓取任务，分解为不规则目标抓取姿态识别和遮挡场景下的协同抓取两个子问题分别求解，并提出基于注意力机制的不规则目标可抓取点识别网络和基于深度强化学习的推-抓协作式机械臂抓取框架。所提方法在包括工业流水线分拣在内的3个任务，5种不同场景中取得了比现有流行方法更高的抓取成功率和更少的动作总数，展示了其在工业互联网环境下的高效性和实用性，为实际场景下的机械臂复杂作业提供了新的思路和解决方案。本文所提方案未来可进一步扩展至杂乱场景下的多目标协同抓取问题，提升现有机械臂自主控制方法的应用范围。

参考文献：

[1] Huang S, Wang Z, Zhou J, et al. Planning irregular object packing via hierarchical reinforcement learning[J]. IEEE Robotics and Automation Letters, 2022, 8(1): 81-88.

[2] 宋明俊,严文,邓益昭,等.轻量化机器人抓取位姿实时检测算法[J].浙江大学学报(工学版),2024,58(03):599-610.

[3] Levine S, Pastor P, Krizhevsky A, et al. Learning hand-eye coordination for robotic grasping with deep learning and large-scale data collection[J]. The International journal of robotics research, 2018, 37(4-5): 421-436.

[4] Mahler J, Pokorny F T, Hou B, et al. Dex-net 1.0: A cloud-based network of 3d objects for robust grasp planning using a multi-armed bandit model with correlated rewards[C]//2016 IEEE international conference on robotics and automation (ICRA). IEEE, 2016: 1957-1964.

[5] Mahler J, Matl M, Satish V, et al. Learning ambidextrous robot grasping policies[J]. Science Robotics, 2019, 4(26): eaau4984.

[6] Lenz I, Lee H, Saxena A. Deep learning for detecting robotic grasps[J]. The International journal of robotics research, 2015, 34(4-5): 705-724.

[7] Redmon J, Angelova A. Real-time grasp detection using convolutional neural networks[C]. 2015 IEEE international conference on robotics and automation (ICRA), 2015: 1316-1322.

[8] Park D, Seo Y, Chun S Y. Real-time, highly accurate robotic grasp detection using fully convolutional neural network with rotation ensemble module[C]//2020 IEEE International Conference on Robotics and Automation (ICRA). IEEE, 2020: 9397-9403.

[9] 章坚武,芦泽韬,章谦骅,等.基于拟牛顿法的深度强化学习在车联网边缘计算中的研究[J].通信学报,2024,45(05):90-100.

[10] 李静晨,史豪斌,黄国胜.基于自注意力机制和策略映射重组的多智能体强化学习算法[J].计算机学报,2022,45(09):1842-1858.

[11] He Z, Li J, Wu F, et al. DeRL: Coupling Decomposition in Action Space for Reinforcement Learning Task[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2024, 8(1): 1030-1043.

[12] Pinto L, Gupta A. Supersizing self-supervision: Learning to grasp from 50k tries and 700 robot hours[C]. 2016 IEEE international conference on robotics and automation (ICRA), 2016: 3406-3413.

[13] Lee K H, Xiao T, Li A, et al. PI-QT-Opt: Predictive information improves multi-task robotic reinforcement learning at scale[C]//Conference on Robot Learning. PMLR, 2023: 1696-1707.

[14] Breyer M, Furrer F, Novkovic T, et al. Comparing task simplifications to learn closed-loop object picking using deep reinforcement learning[J]. IEEE Robotics and Automation Letters, 2019, 4(2): 1549-1556.

[15] Clavera I, Held D, Abbeel P. Policy transfer via modularity and reward guiding[C]. 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2017: 1537-1544.

[16] Yang Y, Liang H, Choi C. A deep learning approach to grasping the invisible[J]. IEEE Robotics and Automation Letters, 2020, 5(2): 2232-2239.

[17] Zhou T, Fan D P, Cheng M M, et al. RGB-D salient object detection: A survey[J]. Computational Visual Media, 2021, 7: 37-69.

[18] Watkins C J C H, Dayan P. Q-learning[J]. Machine learning, 1992, 8: 279-292.

[19] Badrinarayanan V, Kendall A, Cipolla R. Segnet: A deep convolutional encoder-decoder architecture for image segmentation[J]. IEEE transactions on pattern analysis and machine intelligence, 2017, 39(12): 2481-2495.

[20] Targ S, Almeida D, Lyman K. Resnet in resnet: Generalizing residual architectures[J]. arxiv preprint arxiv:1603.08029, 2016.

[21] Horn R A. The hadamard product[C]//Proc. Symp. Appl. Math. 1990, 40: 87-169.

[22] D’Agostino R B. Tests for the normal distribution[M]//Goodness-of-fit-techniques. Routledge, 2017: 367-420.

[23] Iandola F, Moskewicz M, Karayev S, et al. Densenet: Implementing efficient convnet descriptor pyramids[J]. arxiv preprint arxiv:1404.1869, 2014.

[24] Zhang J, Kim J, O'Donoghue B, et al. Sample efficient reinforcement learning with REINFORCE[C]//Proceedings of the AAAI conference on artificial intelligence. 2021, 35(12): 10887-10895.

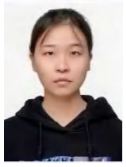
[25] Zeng A, Song S, Welker S, et al. Learning synergies between pushing and grasping with self-supervised deep reinforcement learning[C]. 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2018: 4238-4245.

[26] Xu K, Yu H, Lai Q, et al. Efficient learning of goal-oriented push-grasping synergy in clutter[J]. IEEE Robotics and Automation Letters, 2021, 6(4): 6337-6344.

[作者简介]

何自明（1996—），男，安徽马鞍山人，西北工业大学博士生，主要研究方向为强化学习、多智能体系统、智能机器人、智能控制与决策等。

杨喆瑞（2001—），男，吉林镇赉人，西北工业大学硕士生，主要研究方向为智能系统与智能决策、机械臂智能控制等。



王柯新（1999—），女，硕士，西北工业大学，主要研究方向为深度强化学习、目标检测、机械臂智能控制等。

史豪斌（1978—），男，浙江宁波人，博士，西北工业大学教授，博士生导师，主要研究方向为分布式人工智能、智能机器人、群机器人协同决策、智能控制与决策、机器人路径规划与导航、机器学习等。

吉庆兵（1976—），男，四川绵竹人，博士，中国电子科技集团公司第三十研究所正高级工程师，硕士生导师，主要研究方向为网络空间安全、加密流量分析、密码分析破译、人工智能等。

考虑工人移动性的人员排班和生产调度研究

毛照昉，宋满金，方侃，黄典+
（天津大学管理与经济学部，天津，300072）

摘要：本文针对考虑工人移动性的人员排班和生产调度进行研究。工人作为生产资源的重要组成部分，其可移动的特性在生产调度中起到了不可或缺的作用，可有效提高生产效率和平衡生产线间的工作负荷。同时，在本文所研究的假设中，对于给定工序，其加工时间与在其加工的工人数量有直接关系。本文以流水车间调度问题为研究对象，将工人的可移动性纳入考虑，建立了考虑工人移动性的流水车间调度数学模型，同时针对该问题设计了引入模拟退火机制的遗传算法。此外，为了得到高质量的调度方案，本文还提出了基于最早处理规则（EPR）的 4 种解码方法，确定了各操作间的优先级关系，据此提出相关管理启示，从而优化任务分配以及人员调度，实现生产效率的提升。

关键词：人员排班，流水车间调度，工人移动性，遗传算法，模拟退火，最早处理规则

0 引 言

在愈发激烈的全球化竞争以及加速变化市场环境中，传统的生产方式早已不能满足企业长期生存的要求。在以往的研究中，生产调度大多都只针对机器选择和工序排序进行决策，而对人员排班的研究则比较缺少。但实际上，人员作为生产资源的重要组成部分，其可移动的特性可以在生产调度中起到不可或缺的作用。

如图 1 所示，良好的人员排班可以大幅地降低基层工作人员的工作强度；合理地平衡生产线之间的工作负荷；有效地缩短产线整体的工作时间；极大程度上地提高生产效率，降低运营成本，提高产品质量。为寻找在生产调度当中合理的人员排班计划，许多国内外研究学者针对工人分配提出了很多思路和方法。

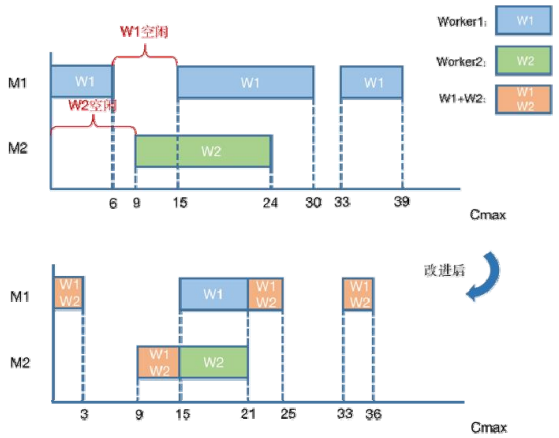


图 1 工人移动效果示意图

在装配线平衡领域，Liu 等[1] 研究了考虑多技能工人分配和并行团队调度的复杂产品装配线调度问题，以最小化最大完成时间和团队工作量不平衡程度为优化目标，提出了一个整数规划模型，并考虑了工人分配和任务顺序的混合编码方法。Liu 等[2] 研究了考虑最大完工时间和总流动时间同时最小化的混合流水车间双目标调度和工人分配问题。Hu [3] 研究了具有非抢占作业的相同并行机器模型中的总流动时间最小化问题，对工人分配子问题采用了最大边际贡献(LMC)方法。Chaudhry 等[4] 提出了一种通用的基于电子表格的遗传算法(GA)方法，用来寻找最优的工人分配方式以最小化并行机调度的总完成时间。Cappadonna 等[5] 研究了有限人力资源下不相关的并行机调度问题，在给出求解该问题的混合整数线性规划(MILP)模型的基础上提出了一种适用于更大规模问题的遗传算法。Costa 等[6] 以最大完成时间最小化为目标，研究了具有序列依赖设置时间和有限人力资源的不相关并行机调度问题，提出了基于排列编码的遗传算法(GA)、多编码遗传算法和混合遗传算法。在该研究中，工人由于拥有不同的技能水平被认为是一种关键资源，影响着完成时间。Ruiz-Torres 等[7] 认为订单完成情况和工人满意度是生产计划当中包含的两个重要目标，由此提出了一种同时考虑这两个标准的作业调度模型，并导出了生成非支配解的求解方法。Behnamian 等[8] 假设任何作业的处理时间取决于在特定阶段分配给该作业的工人数量，并且分配给该作业的工人越多，作业处理时间越短。以提前、延迟、完工时间和总用工成本最小为目标函数，提出了一种基于变邻域搜索算法的殖民竞争算法。

在双资源约束（Dual Resource Constrained）系统中，对工人的分配也经常作为约束资源之一。Xu 等[9] 将在规划和调度考虑人力资源的双资源约束系统中需要考虑的技术挑战分为工作释放机制、工

作分配、工人灵活性、工人分配和转移成本五个主要维度。Xiao 等[10] 采用鲁棒调度方法对双资源约束下具有随机加工时间的作业车间调度问题进行研究，建立了基于加工时间预期场景的 SJSSP 机器-工人双资源约束鲁棒调度模型(DR-SJSSP-EPS)。Li 等[11] 针对双资源约束作业车间调度问题，提出了一种分支种群遗传算法(BPGA)，通过信息素积累以传递亲本染色体的进化经验。ElMaraghy 等[12] 提出了一种基于遗传算法(GAs)的调度方法，用于解决同时受机器和工人约束的制造系统的调度问题。Araz 等[13] 为探究动态选择的作业调度、工人分配和作业路由规则之间的相互作用，提出了一种针对 DRC 系统的多标准实时调度方法，并采用人工神经网络作为元模型来降低计算复杂度。Dunke 等[14] 提出了一种结合数学优化、模拟和数据分析的方法管道，以随着时间的推移处理由于数据的不确定性和工人效率的变化所产生的问题。Renna 等[15] 利用博弈论提出了一种新的 DRC 作业车间工人分配规则，以避免在工作站数量过多的情况下，计算时间和复杂性较高的弊端。Delgoshaei 等[16] 提出了一种双资源约束环境下动态元胞制造系统的短期周期调度新方法, 可以在零件需求不确定且定期变化的情况下，通过对工人进行分配，找到内部制造的最佳生产策略。

在流水车间调度问题中，针对工人排班的研究也较为广泛。Han 等[17] 考虑了一种全新且实际的考虑工人约束的混合流水车间，构建了其混合整数线性规划模型。并提出了 7 种带启发式解码(HD)的多目标进化算法来求解该考虑工人约束的混合流水车间。Geng 等[18] 提出了一种改进的多目标模因算法(IMOMA)来求解考虑机器和工人双重柔性的混合流水车间调度问题。Gong 等[19] 提出了一种具有工人灵活性的节能柔性流水车间 (EFFSPW)，同时考虑了机器和工人的灵活性以及加工时间、能耗和工人成本等相关因素并提出了一种混合进化算法(HEA)。Alexander 等[20] 提出了异构流水车间调度问题 (Het-FSSP)，同时解决了两个问题:找到最佳的工人分配到工作站，并解决相应的调度问题。Pargar 等[21] 将学习效应作为一种资源利用技术，分析了工人学习对分配给机器的工作结构及其顺序的影响，提出了两种基于混合水流算法和非支配排序和排序概念的求解方法。Matheus 等[22] 研究了非置换流水车间调度问题的一个推广，并获得了最优的工人分配计划，以达到最小化最大完工时间的目的，在该研究中，机器上处理工作的时间取决于所分配给该机器的工人。Tasnim 等[23] 研究了具有工人灵活性的分布式置换流水车间调度问题，并提出了一种建设性的启发式算法。Alex 等[24] 研究了一个具有工人资源的两阶段混合流水作业问题，其中工人的平均效率决定了处理工作的时间。Santiago 等[25] 在手工密集型制造系统中分析了工人疲劳，研究了一个处理时间与位置相关的流水车间调度问题。

通过对以往研究的回顾不难发现，尽管部分学者考虑到了工人分配对处理时间及加工顺序的影响，但几乎没有学者在流水车间调度问题中对工人移动的时间、空间等规则进行研究。基于该情况，本文提出了一种考虑工人移动性的人员排班和生产调度方法。

在经典的调度问题中，无论涉及多少台机器，每台机器上的工人的数量都可能被忽略或假定为适当的，不纳入考虑范围。而在本文中的研究主体为包装线。与普通生产线不同，包装线上的工作大多是较为基础的包装工作，工作模式简单，工作压力较小，对工人的技术水平要求不高，包装线之间没有技术隔阂。因此工人可以在包装线间按照排班要求自由移动，给定工序的加工时间与加工的工人数量有直接关系，指派更多的工人从事相同的工作会减少工作完成时间。工作处理的时间不再是一个常数，而是与分配到工作的工人数量相关。

同时，本文不仅重点研究任务的调度以及人员的排班，还将人员的移动原则也纳入考虑，以优化任务分配以及人员调度，实现生产效率的提升。针对该类问题，本文首先以最小化最大完工时间为目标构建了考虑工人移动性的流水车间调度模型，并设计了一种引入模拟退火机制的遗传算法。其中为了保证得到解的可行性及质量，在解码过程中提出了基于最早处理规则（EPR）的 4 种解码方法，确定了各操作间的优先级关系。最后，通过大量算例实验，本文验证了文中所构造的模型和引入模拟退火机制的遗传算法的有效性，据此提出相关管理启示，从而优化任务分配以及人员调度，实现生产效率的提升。

1　问题与模型

1.1 问题描述

在本研究中，工人具有可移动的特性，即在满足可移动条件时（即当前所在机器的处理任务已结束），可以从所在机器移动到其他机器上并与该机器上的工人共同作业，以减少作业在机器上的处理

时间，进而缩短所有作业的总完成时间。注意工人不可以在中途插入到其他作业处理中，只能等待下一作业并从头开始处理。关于该问题，本文做出以下几点假设：

- 每个作业都需要按照 π 的顺序在每台机器上各处理一次。
- 每个作业在处理时，所选择机器上最少需要 1 名工人。
- 每个作业在处理时，所选择机器上可以有多名工人。
- 任何机器都不能同时处理多个作业
- 机器不会出现故障，在每个阶段都可用。
- 作业处理时间与作业序列无关。
- 机器设置时间忽略不计。
- 作业数量是固定的。
- 机器数量是固定的。
- n 个作业，m 个机器，ℓ 个工人在 0 时刻都是可用的。
- 有一组具有相同能力的工人 W_w，可被分配到不同机器上。
- 分配工人时受到资源限制，总工人数不能超过 ℓ。
- 工人具有可移动性，在某时刻当前所在机器完成作业处理时，可以移动到其他机器上，与该机器上的其他工人共同进行处理。
- 工人只有在处理完所负责机器上的当前作业后才可以进行移动。
- 工人不可以在中途插入到其他作业处理中，只能等待下一作业并从头开始处理。（每个工序的工人数固定）
- 当作业在给定的机器上开始处理时，该机器上的工人数量将保持不变，直到该工作完成。
- 工人的移动时间可忽略不计。
- 作业的处理时间取决于所选机器上的工人数量。
- 设 M 为最优计划的最大完工时间的上界。$M = \sum_i^m \sum_j^n P_{i,j,1}$

为了阐明上述问题描述，图 2 给出了一个简单的实例

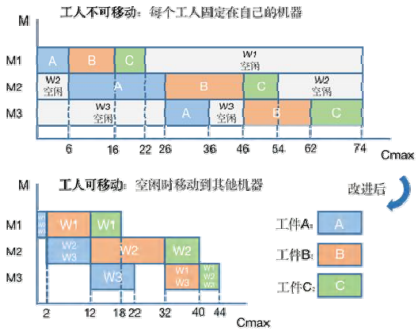


图 2 工人移动问题实例

1.2 参数符号

设定作业集合 $N = \{1, 2, \ldots, n\}$，这些作业要在一组工作站中按流水车间的原则进行顺序处理（每个工作站中要都要按照 π 的顺序进行），π 是所有作业的处理顺序，工作站集合 $M = \{1, 2, \ldots, m\}$。其中每个作业在不同机器上的处理时间取决于当时在该机器上的工人数量。如果机器 i 上有 s 个工人在处理作业 j 上，那么作业 j 的处理时间就等于 $P_{i,j,s}$。设定 $S_{i,j}$ 为作业 j 在机器 i 上的开始时间，$C_{i,j}$ 为作业 j 在机器 i 上的完成时间，研究目标为最小化最大完成时间 C_{max}。本文的符号定义具体如表 1 所示。

表 1 符号定义

Table 1 Symbol definitions

参数符号	含义
n	等待处理的作业总数
m	机器总数
ℓ	工人总数
$N_{j/k}$	作业的集合，$j/k = 1$，…，n
$M_{i/h}$	机器的集合，$i/h = 1$，…，m
W_s	工人数的集合，$s = 1$，…，ℓ
$P_{i,j,s}$	由 s 个人加工时，作业 j 在机器 i 上的处理时间
$S_{i,j}$	作业 j 在机器 i 上的开始时间
$C_{i,j}$	作业 j 在机器 i 上的完成时间
C_{max}	最大完工时间
$\theta_{j,k}$	若作业 j 在作业 k 之前加工则为 1；否则为 0
$x_{i,j,s}$	若有 s 个工人在机器 i 上处理作业 j 则为 1；否则为 0
$\alpha_{h,k,i,j}$	若机器 h 上作业 k 的开始时间小于机器 i 上作业 j 的开始时间（$S_{h,k} \le S_{i,j}$）则为 1；否则为 0

$\beta_{h,k,i,j}$	若机器 h 上作业 k 的完成时间大于机器 i 上作业 j 的完成时间（$C_{h,k} > S_{i,j}$）则为 1；否则为 0
$y_{h,k,i,j}$	若机器 i 上作业 j 的开始时间发生在机器 h 上处理作业k的过程中（$S_{h,k} \le S_{i,j} < C_{h,k}$）则为 1；否则为 0
$z_{h,k,s,i,j}$	若当作业 j 开始在机器 i 上处理时，作业 k 以 s 的人数在机器 h 上处理（$x_{h,k,s} = 1, y_{h,k,i,j} = 1$）则为 1；否则为 0

1.3 模型构建

在该模型的输入中，作业信息包括：作业数量、每个作业包含的工序数以及各工序在不同工人数量的条件下进行处理的加工时间；工人信息包括：工人数量（同质化工人）；机器信息包括：机器数量。模型的输出包括，作业排序调度情况以及工人移动调度情况（也就是各机器上工人数量的变化）；优化目标为，最大完工时间最小。

Formulation

$$min\ C_{max} \tag{1}$$

subject to

$$C_{max} \ge C_{m,j}\ \forall j \in N \tag{2}$$

$$C_{1,j} \ge \sum_{s=1}^{\ell} P_{1,j,s}\, x_{1,j,s}\ \forall j \in N \tag{3}$$

$$C_{i,j} \ge C_{i-1,j} + \sum_{s=1}^{\ell} P_{i,j,s}\, x_{i,j,s}$$

$$\forall i \in M \setminus \{1\}; j \in N \tag{4}$$

$$C_{i,j} \ge C_{i,k} + \sum_{s=1}^{\ell} P_{i,j,s}\, x_{i,j,s} - M\theta_{j,k}$$

$$\forall i \in M; j,k \in N; k > j \tag{5}$$

$$C_{i,k} \ge C_{i,j} + \sum_{s=1}^{\ell} P_{i,k,s}\, x_{i,k,s} - M\left(1 - \theta_{j,k}\right)$$

$$\forall i \in M; j,k \in N; k > j \tag{6}$$

$$C_{i,j} = S_{i,j} + \sum_{s=1}^{\ell} P_{i,j,s}\, x_{i,j,s}\ \forall i \in M; j \in N \tag{7}$$

$$S_{i,j} - S_{h,k} \le M\alpha_{h,k,i,j} - 1$$

$$\forall i,h \in M; j,k \in N \tag{8}$$

$$S_{h,k} - S_{i,j} \le M\left(1 - \alpha_{h,k,i,j}\right)$$

$$\forall i,h \in M; j,k \in N \tag{9}$$

$$C_{h,k} - S_{i,j} \le M\beta_{h,k,i,j}\ \forall i,h \in M; j,k \in N \tag{10}$$

$$S_{i,j} - C_{h,k} \le M\left(1 - \beta_{h,k,i,j}\right) - 1$$

$$\forall i,h \in M; j,k \in N \tag{11}$$

$$\alpha_{h,k,i,j} + \beta_{h,k,i,j} = 1 + y_{h,k,i,j}$$

$$\forall i,h \in M; j,k \in N \tag{12}$$

$$x_{h,k,s} + y_{h,k,i,j} \le 1 + z_{h,k,s,i,j}$$

$$\forall i,h \in M; j,k \in N; s \in W \tag{13}$$

$$\sum_{s=1}^{\ell} x_{i,j,s} = 1\ \forall i \in M; j \in N \tag{14}$$

$$\theta_{j,k} + \theta_{k,j} = 1\ \forall j,k \in N, j \ne k \tag{15}$$

$$\theta_{j,k} + \theta_{k,l} + \theta_{l,j} \le 2\ \forall j,k,l \in N, j \ne k \ne l \tag{16}$$

$$\sum_{s=1}^{\ell} s{\cdot}x_{i,j,s} + \sum_{h=1}^{m(h\ne i)} \sum_{k=1}^{n} \sum_{s=1}^{l} s{\cdot}z_{h,k,s,i,j} \le l$$

$$\forall i \in M; j \in N \tag{17}$$

$$x_{i,j,s}, \theta_{j,k}, \alpha_{h,k,i,j}, \beta_{h,k,i,j}, y_{h,k,i,j}, z_{h,k,s,i,j} \in \{0,1\}$$

$$\forall i,h \in M; j,k \in N; s \in W \tag{18}$$

目标函数 (1) 是最小化最大完工时间。

式 (2)-(3) 定义了最大完工时间，保证最大完工时间等于在机器 m 上处理的最后一个作业的完成时间。式 (4) 保证了同一作业在不同机器上有顺序约束，对于同一个作业来说，要保证其在上一台机器处理完成，才能在下一台机器上开始处理。式 (5)-(6) 保证了同一机器上的不同作业有顺序约束，对于同一台机器来说，要保证前一作业处理完成，后一作业才能开始处理。式 (7) 确定了完成时间与开始时间的关系，确保作业被非优先处理。式 (8)-(9) 确定了作业 j 在机器 i 上的开始时间与作业 k 在机器 h 上的开始时间的关系。式 (10)-(11) 确定了作业 j 在机器 i 上的开始时间与作业 k 在机器 h 上的完

成时间的关系。式 (12) 定义了决策变量 α、β、y 的关系。式 (13) 定义了决策变量 x、y、z 的关系。式 (14) 保证了每个作业可以在任何给定的机器上被一定数量的工人处理。式 (15)-(16) 保证了在每台机器上以相同的顺序处理作业。式 (17) 保证了在任何时候，各机器上的的总人数不超过 ℓ。式 (18) 明确了部分决策变量的取值范围。

1.4 模型验证

为验证所建立考虑工人移动性的流水车间模型的可行性，同时便于下文对编码方式进行介绍。本文使用 Gurobi 求解器对该混合整数规划模型进行求解，以 3 个作业、3 台机器和 3 位工人为例，每个作业在每台机器上的标准加工时间如表 2 所示，最终求解结果为 44，作业排序为[1, 3, 2]，工人分配为[3, 1, 1, 2, 2, 1, 2, 2, 3]，如图 4 所示，与图 3 中不考虑工人移动性的流水车间调度结果 72 形成对比。

表 2 各作业在各机器的标准处理时间

$P_{i,j,1}$ $/p_{\pi(j),i}$	i=1	i=2	i=3
j=1	6	18	12
j=2	12	24	18
j=3	24	12	6

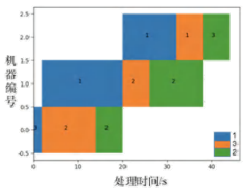


图 3 Gurobi 求解器求解结果

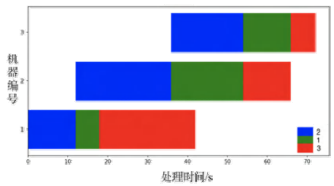


图 4 不考虑工人移动性的结果

2 引入模拟退火机制的遗传算法

2.1 算法流程

遗传算法作为常见的启发式算法之一，以其强大的全局搜索能力、适应性及并行计算能力等优势，被广大学者所青睐。在流水车间调度问题中有着相当广泛的应用。

但遗传算法的局部搜索能力较差，容易产生早熟现象或陷入局部最优。因此本文把遗传算法与局部搜索能力较强的模拟退火算法进行结合，以遗传算法运算流程作为主体，并把模拟退火的机制融入其中，以调整优化群体，进而实现遗传算法运行效率和求解质量的提高。

2.2 编码

针对考虑工人移动性的流水车车间调度模型，设计了一种作业排序与工人分配相结合的编码方式，解决方案包含作业排序和工人分配两个部分。

第一部分编码 $\pi = [\pi_1, \pi_2, \cdots, \pi_n]$ 表示作业处理顺序，编码长度为 n；第二部分编码 $S = [s_{1,1}, \cdots, s_{1,m}, \cdots, s_{j,i}, \cdots, s_{n,1}, \cdots, s_{n,m}]$ 表示工序处理人数，编码长度为作业数量 n 与机器数量 m 的乘积，其中 $s_{j,i}$ 代表作业 j 在机器 i 上处理时的处理人数。因此，一个解可以用 (S, π) 的编码组合来表示。

同样以 1.4 中所表示的 3 个作业、3 台机器和 3 位工人为例，单个工人的标准处理时间 $p_{\pi(j),i}$ 如表 3-1 所示。考虑一个已编码的解 (S, π)，其中 $\pi = [1, 3, 2]$，$S = [3, 1, 1, 2, 2, 1, 2, 2, 3]$。

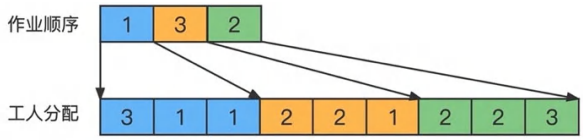


图 5 染色体编码示意图

由图 3、图 4 的结果可以得到，在考虑工人的可移动性之后，甘特图中的最大处理时间为 44，比不考虑工人可移动性的情况缩短了 28。同时根据甘特图，可以直观的看出各机器上处理各作业的工人数量在发生变化。

其中，在 t=1 的时间点，有 3 位工人正在机器 1 上处理作业 1，这时由于其他机器上没有处理任务，不需要额外工人，因此该情况满足工人约束；在 t=5 的时间点，有 2 位工人在机器 1 上处理作业 3，1 位工人在机器 2 上处理作业 1，机器 3 上没有处理任务，因此该情况同样满足工人约束；以此类推，如果在例子中出现了不满足工人约束，超过工人数量限制的情况，应采取相应的规则来进行处理，并结合解码方法共同获得可行的调度方案，具体规则详见下文。

2.3 最早处理规则

对于 2.1 解的编码方式，在将作业处理顺序解码为可行调度时，需要考虑工人约束。因此本文引入了最早处理规则 (The Earliest Processing Rule, EPR)，再满足工人约束的前提下，尽可能更早的处理各项任务。在最早处理规则中，需要记录每台机器上每项作业的开始时间、完成时间，以及各时间段内的工人使用数量。

设 T 为计划处理作业的所有开始时间和完成时间的的排序列表，$T[k]$ 为 T 的第 k 个分量。设 S 为所有时间区间对应的已使用工人数，其中 $S[k]$ 为时

间区间 $(T_k, T_{k+1}]$ 内的已使用工人数，在初始状态时 $T=\{0\}$，$S=\emptyset$。$x[k]$ 为时间区间$(T_k, T_{k+1}]$ 内的可用工人数，其中$x[k]=S_{max}-S[k]$。对于作业处理顺序 $\pi=[\pi(1),\pi(2),\ldots,\pi(n)]$，$\pi(j)$ 代表要处理的第 j 个作业，$O_{\pi(j),i}$ 代表 $\pi(j)$ 在机器 i 上进行处理，$ST_{\pi(j),i}$代表 $O_{\pi(j),i}$ 的开始时间，$CT_{\pi(j),i}$ 代表 $O_{\pi(j),i}$ 的完成时间，$p_{\pi(j),i}$ 代表 $O_{\pi(j),i}$ 的标准处理时间，$s_{\pi(j),i}$ 代表在编码中分配给 $O_{\pi(j),i}$的工人数量，$s'_{\pi(j),i}$ 代表处理 $O_{\pi(j),i}$的实际工人数量。

假设已经通过编码得到了作业处理顺序 π 以及各操作的处理人数 $s_{\pi(j),i}$，对于操作 $O_{\pi(j),i}$，最早处理规则的执行流程如下：

Step1: 找出 T 中的时间节点 $T[k]=max\{CT_{\pi(j-1),i}, CT_{\pi(j),i-1}\}$,设置新的时间列表 $T'=T$，新的工人列表 $S'=S$。

Step2:设置操作 $O_{\pi(j),i}$ 的开始时间为 $ST_{\pi(j),i}=T'[k]$。

Step3:通过在时间区间 $(T_k, T_{k+1}]$ 内的已用工人数 $S[k]$，判断可使用工人数$x[k]=S_{max}-S[k]$。如果$S[k]$、$x[k]$ 不存在，则表示所选择的开始时间 $T'[k]$ 为 T'中的最后一个元素，则无需考虑工人限制，用染色体编码中的工人数 $s_{\pi(j),i}$ 直接计算完成时间 $CT_{\pi(j),i}=ST_{\pi(j),i}+p_{\pi(j),i}/s_{\pi(j),i}$；如果 $x[k]>0$，则实际使用的工人数 $s'_{\pi(j),i}=min\{x[k], s_{\pi(j),i}\}$，$CT_{\pi(j),i}=ST_{\pi(j),i}+p_{\pi(j),i}/s'_{\pi(j),i}$；如果 $x[k]=0$，则令 $k=k+1$，重复 Step2。

Step4:在 T' 中搜索等于 $CT_{\pi(j),i}$ 的元素，如果存在，把该元素的所在位置定义为 c。无需对 S' 进行操作。

如果 $CT_{\pi(j),i}$ 没有指向 T'中的任意一个元素，则将 $CT_{\pi(j),i}$ 插入到 T'中的第 c 个位置，满足 $T'[c-1]<CT_{\pi(j),i}<T'[c+1]$。若 $T'[c]$ 为 T' 中的最后一个元素，将 0 插入到 S'中的第 $c-1$ 个位置；否则将 $S'[c-1]$ 复制到其前一个位置。

Step5:对于$h=k$到 $c-1$，更新$S'[h]=S'[h]+s'_{\pi(j),i}$。最后令 $T=T', S=S'$，操作 $O_{\pi(j),i}$ 的调度已完成。

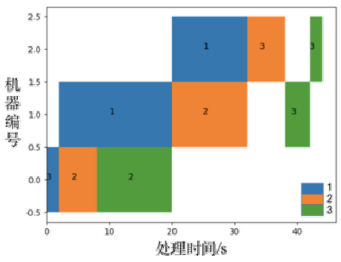


图 6 最早处理规则示意图

以图 6 中的调度结果为例，假如在解码前染色体中的作业处理顺序 $\pi=[1,2,3]$，工人数量分配 $s_{\pi(j),i}=[3,3,2,2,2,3,3,3,3]$。

在不考虑工人数量约束，只考虑流水车间工序约束的前提下，假设作业优先顺序为 $O_{1,1}\rightarrow O_{2,1}\rightarrow O_{1,2}\rightarrow O_{3,1}\rightarrow O_{2,2}\rightarrow O_{1,3}\rightarrow O_{2,3}\rightarrow O_{3,2}\rightarrow O_{3,3}$。因此，$O_{1,1}$优先调度，在初始状态时 $T=\{0\}$，$S=\emptyset$，设置开始时间为 $T[1]$，$k=1$，判断所需时间区间的已用工人数，发现$S[1]$、$x[1]$ 不存在，因此不用考虑工人约束。完成时间等于 $0+6/3=2$，将其插入 T'的第 2 个位置，$T'=\{0,2\}$。将 0 插入 S' 的第 1 个位置，$S'=\{0\}$，更新实际使用人数，最终得到 $T=\{0,2\}$，$S=\{3\}$，完成操作 $O_{1,1}$ 的调度；然后按照上述优先顺序继续调度 $O_{2,1}$，设置开始时间为 $T[2]$，$k=2$，判断所需时间区间的已用工人数，发现 $S[2]$、$x[2]$ 不存在，依然不用考虑工人约束。计算完成时间，并将其插入 T' 的第 3 个位置，$T'=\{0,2,8\}$。将 0 插入 S' 的第 2 个位置，$S'=\{3,0\}$，更新实际使用人数，最终得到 $T=\{0,2,8\}$，$S=\{3,2\}$，完成操作 $O_{2,1}$ 的调度；之后对 $O_{1,2}$ 进行调度，设置开始时间为 $T[2]$，$k=2$，判断已用工人数，发现 $S[2]=2$，$x[2]=1$，因此 $s'_{\pi(j),i}=1$，对应染色体中的工人数应该改为 1，按上述方式继续计算完成时间并插入T'的第 4 个位置，$T'=\{0,2,8,20\}$，将 0 插入 S' 的第 3 个位置，$S'=\{3,2,0\}$，更新使用人数，最终得到 $T=\{0,2,8,20\}$，$S=\{3,3,1\}$，完成操作$O_{1,2}$的调度。

同理调度 $O_{3,1}$ 至 $O_{2,3}$，得到 $T=\{0,2,8,20,32,38\}$，$S=\{3,3,3,3,3\}$;继续调度 $O_{3,2}$，首先设置开始时间为 $T[5]$，$k=5$，判断已用工人数，发现 $S[5]=3$，$x[5]=0$，因此需将 $k=5+1=6$，重新设置开始时间为 $T[6]$，$k=6$，判断已用工人数，发现 $S[6]$、$x[6]$ 不存在，因此不用考虑工人约束。计算完成时间并插入 T' 的第 7 个位置，$T'=\{0,2,8,20,32,38,42\}$，将 0 插入 S' 的第 6 个位置，$S'=\{3,3,3,3,3,0\}$，更新使用人数，最终得到 $T=\{0,2,8,20,32,38,42\}$，$S=\{3,3,3,3,3,3\}$，完成操作 $O_{3,2}$；最后同理调度 $O_{3,3}$。

当所有的处理都被以 EPR 的规则进行调度后，就得到了满足工人约束的调度方案。最终得到完成时间 $T=\{0,2,8,20,32,38,42,44\}$，各时间区间的工人数 $S=\{3,3,3,3,3,3,3\}$，以及实际工人数量分配 $s'_{\pi(j),i}=[3,1,1,2,2,3,2,3,3]$。

2.4 解码

根据编码中的作业顺序，在满足 EPR 规则的前提下，本文提出了作业优先解码、机器优先解码、

最大总剩余负载解码、最早完成时间解码四种方法。

2.4.1 作业优先解码

作业优先解码方法是将操作按照 $O_{\pi(1),1} \rightarrow O_{\pi(1),2} \rightarrow \ldots \rightarrow O_{\pi(1),m} \rightarrow O_{\pi(2),1} \rightarrow O_{\pi(2),2} \rightarrow \ldots \rightarrow O_{\pi(2),\mathrm{m}} \rightarrow \ldots \rightarrow O_{\pi(n),\mathrm{m}}$ 的顺序进行调度，同时使用 EPR 规则。即先在所有机器上完成第一个作业的操作，然后在所有机器上完成第二个作业的操作，以此类推直到完成所有操作。

解码 1 作业优先解码

输入：染色体编码中作业加工顺序 π，染色体编码中各作业在各机器使用的人数 $s_{\pi(j),i}$，各工件单个工人所需时间 $p_{\pi(j),i}$；

输出：各个工件的开始时间、结束时间、实际分配的工人数量，目标值为 max{makespan}

1: **For** 机器 *i* **in** [1,2,...,m]:
// 初始化每台机器工作的最大时间
2: makespan[i]=0
3: **End For**
4: **For** 作业 *j* **in** 作业顺序 π:
5: **For** 机器 *i* **in** [1,2,...,m]:
// 按照作业优先顺序逐个更新
6: 找到机器 *i* 空闲且满足作业顺序的最早时间 t_1
7: 使用**最早处理规则（EPR）**找到满足工人约束的最早时间 t_2
8: 找到满足工人约束的各工序实际使用工人数 $s'_{\pi(j),i}$
9: 工件 *j* 在机器 *i* 进行加工的开始时间为 $ST_{\pi(j),i}$=max{t_1, t_2}
10: 工件 *j* 在机器 *i* 进行加工的完成时间为 $CT_{\pi(j),i}= ST_{\pi(j),i}$ +ceil($p_{\pi(j),i}/s'_{\pi(j),i}$)
11: makespan[i] = $CT_{\pi(j),i}$
// 更新各机器加工时长
12: **End For**
13: **End For**

2.4.2 机器优先解码

作业优先解码方法是将操作按照 $O_{\pi(1),1} \rightarrow O_{\pi(2),1} \rightarrow \ldots \rightarrow O_{\pi(n),1} \rightarrow O_{\pi(1),2} \rightarrow O_{\pi(2),2} \rightarrow \ldots \rightarrow O_{\pi(n),2} \rightarrow \ldots \rightarrow O_{\pi(n),m}$ 的顺序进行调度，同时使用 EPR 规则。即先在第一台机器上完成所有作业的操作，然后在第二台机器上完成所有作业的操作，以此类推直到完成所有操作。

2.4.3 最大总剩余负载解码

最大总剩余负载解码方法是根据候选操作的总剩余负载确定其优先级，即在规定的候选操作集合中，选择总剩余负载最大的元素应用 EPR 规则进行处理。一旦操作 $O_{\pi(j),i}$ 完成调度，它的后工序 $O_{\pi(j+1),i}$ 和 $O_{\pi(j),i+1}$ 就会被加入到候选操作集合中，如果他们的紧前工序 $O_{\pi(j+1),i-1}$ 和 $O_{\pi(j-1),i+1}$ 已经被调度。

解码 2 机器优先解码

输入：染色体编码中作业加工顺序 π，染色体编码中各作业在各机器使用的人数 $s_{\pi(j),i}$，各工件单个工人所需时间 $p_{\pi(j),i}$；

输出：各个工件的开始时间、结束时间、实际分配的工人数量，目标值为 max{makespan}

1: **For** 机器 *i* **in** [1,2,...,m]:
// 初始化每台机器工作的最大时间
2: makespan[i]=0
3: **End For**
4: **For** 机器 *i* **in** [1,2,...,m]:
5: **For** 作业 *j* **in** 作业顺序 π:
// 按照机器优先顺序逐个更新
6: 使用 EPR 规则完成对 $O_{\pi(j),i}$ 的调度
// 具体参照解码 1
7: **End For**
8: **End For**

操作 $O_{\pi(j),i}$ 的总剩余负载将应用各工序被单个工人加工的处理时间进行计算：$\mathrm{TRL}_{\pi(j),i} = \sum_{i'=i}^{m}\sum_{j'=j}^{n} p_{\pi(j),i}$。

2.4.4 最早完成时间解码

最早完成时间解码方法是根据候选操作的完成时间确定其优先级，即在规定的候选操作集合中，选择完成时间最早的元素应用 EPR 规则进行处理。最早完成时间解码方法与最大总剩余负载解码方法过程类似，仅在候选操作集合中选择元素的标准不同。

2.5 初始化

初始化的作用是为了尽可能地覆盖搜索空间，提高算法的全局搜索能力。通过随机生成初始种群，可以使算法在搜索空间中广泛搜索，有效地避免算法陷入局部最优解，增加算法的收敛速度和准确性。

在作业排序部分，随机生成一个作业处理顺序 π；在工人分配部分，各作业在各机器上的加工人数分别在总共人数的范围内随机生成。

2.6 交叉操作

交叉操作作为主要的遗传操作，通过随机选择某些位点进行基因重组，产生全新的后代个体。其作用在于增加种群的多样性，提高种群的适应度。在这个过程中，需要尽量降低父代中优良信息被破坏的风险，将其保留到子代并且在子代中不产生过多无用信息。常见的交叉方式有单点交叉（SPX）、多点交叉（MPX）、均匀交叉（UX）、映射交叉（PMX）等。

解码 3 最大剩余负载解码

输入：染色体编码中作业加工顺序 π，染色体编码中各作业在各机器使用的人数 $s_{\pi(j),i}$，各工件单个工人所需时间 $p_{\pi(j),i}$，候选操作集合 CO，调度操作集合 SO；

输出：各个工件的开始时间、结束时间、实际分配的工人数量，目标值为 max{makespan}

1:将操作 $O_{\pi(1),1}$ 作为起始任务进行优先调度
2:令 j=1，i=1
3: **Repeat** until |SO| = $n \times m$
4:　　使用 EPR 规则完成对 $O_{\pi(j),i}$ 的调度
5:　　CO=CO\$\{O_{\pi(j),i}\}$
6:　　SO=SO+$\{O_{\pi(j),i}\}$
　　// 更新候选操作集合、调度操作集合
7:　　**If** i=1 ∨ $O_{\pi(j+1),i-1}$ ∈ SO
　　// 判断紧前工序加工情况
8:　　CO=CO+$\{O_{\pi(j+1),i}\}$
9:　　**End If**
10:　　**If** j=1 ∨ $O_{\pi(j-1),i+1}$ ∈ SO
11:　　CO=CO+$\{O_{\pi(j),i+1}\}$
12:　　**End If**
13:　　令 k=0
14:　　**While** k < |SO|
15:　　计算 CO 中 $O_{\pi(j),i}$ 的总剩余负载 $TRL_{\pi(j),i}$
16:　　使 k 的值增加
17:　　**End While**
18:　　找到 $\{i,j\} = \arg\{\max TRL_{j,i} | O_{\pi(j),i} \in \mathrm{CO}\}$
　　// 找到使剩余负载最大的 i 和 j
19: **End**

具体来说，交叉操作可以将两个不同的个体的染色体部分交换，这样就能够创造出新的个体，从而增加了种群的多样性。同时，交叉操作还可以加速优秀基因的传递和组合，使得优秀基因更容易被保留和发扬光大，从而提高种群的适应度和进化速度。

在本研究中所使用的交叉方法为两点交叉（TPX），在染色体中随机设置两个交叉点，然后再进行部分基因交换，两点交叉的具体操作过程为：

Step1:在相互配对的两个个体编码串中随机设置两个交叉点；

Step2:交换两个个体在所设定的两个交叉点之间的部分染色体。

在工人分配部分中，两点交叉在随机选择两个交叉点后，直接交换中间的工人数量即可，解的可行性由最早处理原则进行保证；而在作业排序部分中，两点交叉后所得解中的作业处理顺序可能会有重复，因此需要进一步约束。如果交换前的解 1 为 [1,2,3,4,5] ,解 2 为 [4,2,5,1,3]，要交换的部分为中间 3 个基因位 [2,3,4] 与 [2,5,1]，则交换后的解 3 为 [1,2,5,1,5]，解 4 为[4,2,3,4,3]，与实际情况不相符。为解决这种情况，我们重新对染色体的结构进行划分，将每条染色体的第一位基因与最后一位基因设置为“头”和“尾”。重新定义后，解 1 的“头”为 [1] ，被交换过来的部分为 [2,5,1] ，其中作业 1 产生重复，因此就将解 1 的“头”更改为在交换过去的部分中，与被交换过来的 1 属于同一位置的数，修正后解 3 的“头”为 [4] 。解 1 的“尾”为 [5] ，同样产生重复，则将解 1 的“尾”更改为在交换过去的部分中，与被交换过来的 5 属于同一位置的数，修正为 [3] 。解 2 的修正规则同理，最终可以得到解 3 为 [4,2,5,1,3] ，解 4 为 [1,2,3,4,5] 。

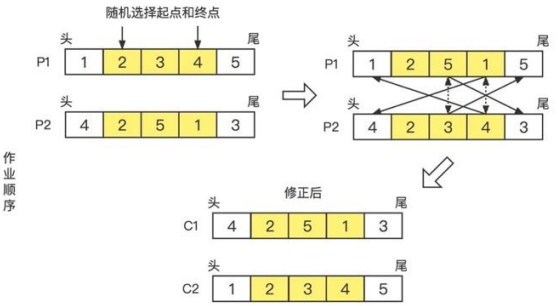


图 7 作业顺序交叉操作示意图

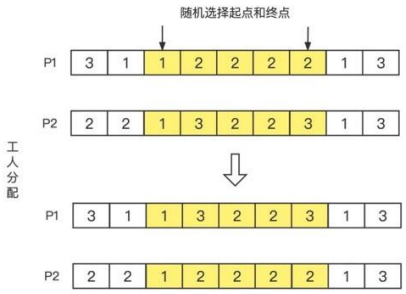


图 8 工人分配交叉示意图

2.7 变异操作

变异操作是一种通过随机改变某些基因信息，产生全新后代个体的操作。其作用在于使得种群保持多样性，避免出现过早收敛的情况。同时，变异操作还能够在搜索空间中探索新的方向和可能性，防止种群过早陷入局部最优解，从而提高全局搜索能力。

对于作业排序部分，随机选择两个基因位进行位置交换，交换后形成新的作业加工顺序；在工人分配部分，则随机选择一个基因位，重新生成一个在最大工人数限制内的随机人数，调整了某一作业在某台机器上进行处理的人数。

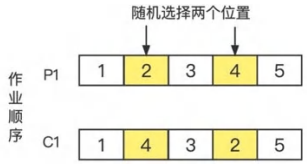


图 9 作业顺序变异操作示意图

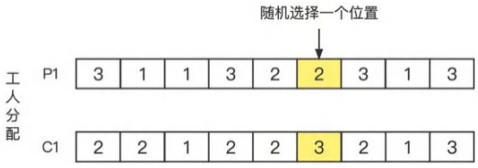


图 10 工人分配变异操作示意图

2.8 选择操作

选择操作的目的就是保留高适应度的个体和种群大小恒定，加快全局收敛和提高计算效率。常用的选择方法有轮盘赌（RWS）、排序选择（RBS）和锦标赛选择（TS）等。

本研究采用的是轮盘赌的方法进行选择，该方法的基本思想如下，各个个体被选中的概率与其适应度函数值的大小成正比。设种群大小为 N，个体 x_i 的适应度为 $f(x_i)$,则个体 x_i 被选择的概率为：

$$P(x_i) = \frac{f(x_i)}{\sum_{j=1}^{N} f(x_j)} \tag{19}$$

轮盘赌选择法的实现过程为：

Step1:在 [0,1] 区间内产生一个服从均匀分布的随机数 r。

Step2:若 $r \le q_1$，则染色体 x_1 被选中。

Step3:若 $q_{k-1} < r \le q_k (2 \le k \le N)$，则染色体 x_k 被选中。

其中 q_i 代表染色体 $x_i (i = 1,2,\dots,N)$ 的累积概率，其计算公式为：

$$q_i = \sum_{j=1}^{i} P(x_i) \tag{20}$$

3 实验设计与结果分析

本文所设计的算法采用 Python 3.9.5 进行编程实现，运行环境为：四核 英特尔(R) Core(TM) i5 2 GHz 的 CPU、16GB 内存、macOS Ventura 13.2 系统的计算机。所提出问题模型由 Gurobi 9.5.2 求解器使用默认设置运行求解。

3.1 实验设置

为验证所设计遗传算法的效果，本研究采用了小、中、大三种规模的算例进行试验，小规模算例为自行设计的算例“sma01”与“sma03”，中、大规模算例分别为由 J. Carlier 在 1978 年与 C.R. Reeves 在 1995 年所提供的经典算例“car01”、“car07”与“rec01”、“rec03”。其中小规模算例“sma01”与“sma03”是通过中规模算例“car01”、“car07”进行截取得到。

各算例的具体数值如表 3 至表 8 所示。其中算例“sma01”有 5 个作业、5 台机器和 5 位工人，算例“sma03”有 7 个作业、3 台机器和三位工人；其中算例“car01”有 11 个作业、5 台机器和 5 位工人，算例“car07”有 7 个作业、7 台机器和 7 位工人；算例“rec01”有 20 个作业、5 台机器和 5 位工人，算例“rec03”同样有 20 个作业、5 台机器和 5 位工人。

3.2 解码方式对比

各解码方式对算例的求解结果如表 9 所示，其中 JP 代表作业优先解码方法，MP 代表机器优先解码方法，LTRL 代表最大剩余负载解码方法，ECT 代表最早完成时间解码方法。通过对比可以看出最大剩余解码方法效果最优。

3.3 是否考虑工人移动性的对比

在确定最大剩余解码方法效果最优的前提下，为检验考虑工人移动性后的调度效果，将考虑与不考虑工人移动性的两种调度结果进行了对比。

与普通的流水车间调度结果进行对比，考虑工人移动性的流水车间调度结果在最大完成时间上有

着明显的缩短。如表 10 所示，在考虑工人可移动性的条件下，算例“sma01”、“sma03”、“car01”、“car07”、“rec01”、“rec03”的最大完成时间分别为[2140, 3294, 5259, 3627, 1166, 981],比不考虑工人移动性的调度结果[4578, 3964, 7038, 6590, 1343, 1208]分别减少了[2438, 670, 1779, 2963, 177, 227]，相当于原来总时间的 53%、17%、25%、45%、13%和 19%。

3.4 Gurobi **求解器与所提出算法的结果对比**

为了验证所提出遗传算法的求解效果，本文将其与 Gurobi 求解器在求解时间和求解结果两个维度进行了对比实验，分别使用 Gurobi 求解器与所提出遗传算法对小、中、大三种规模的算例进行求解。

通过表 11-13，通过对比实验，可以看出对于小规模算例，所提出遗传算法在求解时间和求解结果两个维度上都有着不错的效果；而对于中、大规模算例，所提出算法在求解时间上有着明显优势，尤其是针对大规模算例，而在求解结果上则容易由于陷入局部最优而搜索不到最优解。

3.5 结束语

本研究在搜集大量相关文章的基础上，提出了考虑工人移动性的流水车间调度模型，该模型是通过线性排序变量和成对的二分约束来构建的混合整数规划。此外，本研究在使用引入模拟退火机制的遗传算法求解考虑工人移动性的流水车间调度问题时，根据所提出的考虑各工序加工人数的编码方式，在解码过程中引入了最早处理规则，以保证解的可行性。在实验部分对“sma01”、“sma03”、“car01”、“car07”、“rec01”、“rec03”三种规模的算例进行了求解，验证工人可移动优势的同时，寻找了效果最优的解码方法。

参考文献:

[1] Liu Z W, Liu J H, Zhuang C B, et al. Multi-objective complex product assembly scheduling problem considering parallel team and worker skills[J]. Journal of Manufacturing Systems, 2022, 63: 454-470.

[2] Liu M, Yang X N. Bi-objective optimization for Scheduling and Multi-skilled Worker Assignments in the Hybrid Flow Shop[J]. IFAC-PapersOnLine, 2019, 52: 2128-2133.

[3] Hu P C. Further study of minimizing total flowtime for the worker assignment scheduling problem in the identical parallel-machine models[J]. International Journal of Advanced Manufacturing Technology, 2006, 29: 753-757.

[4] Chaudhry I A, Mahmood S, Ahmad R, et al. Minimizing Makespan for Machine Scheduling and Worker Assignment Problem in Identical Parallel Machine Models Using GA[C]. World Congress on Engineering (WCE 2010), 2010: 2464-2469.

[5] Cappadonna F A, Costa A, Fichera S. Makespan minimization of unrelated parallel machines with limited human resources[C]. 8th CIRP International Conference on Intelligent Computation in Manufacturing Engineering (CIRP ICME), 2012: 450-455.

[6] Costa A, Cappadonna F A, Fichera S. A hybrid genetic algorithm for job sequencing and worker allocation in parallel unrelated machines with sequence-dependent setup times[J]. International Journal of Advanced Manufacturing Technology, 2013, 69: 2799-2817.

[7] Ruiz-Torres A J, Alomoto N, Paletta G, et al. Scheduling to maximise worker satisfaction and on-time orders[J]. International Journal of Production Research, 2015, 53: 2836-2852.

[8] Behnamian J. Scheduling and worker assignment problems on hybrid flowshop with cost-related objective function[J]. International Journal of Advanced Manufacturing Technology, 2014, 74: 267-283.

[9] Xu J, Xu X, Xie S Q. Recent developments in Dual Resource Constrained (DRC) system research[J]. European Journal of Operational Research, 2011, 215: 309-318.

[10] Xiao Shichang, Wu Zigao, Yu Shaohua. A two-stage assignment strategy for the robust scheduling of dual-resource constrained stochastic job shop scheduling problems[C]. 9th IFAC/IFIP/IFORS/IISE/INFORMS Conference on Manufacturing Modelling, Management and Control (IFAC MIM), 2019, 52: 421-426.

[11] Li Jingyao, Huang Yuan, Niu Xinwei. A branch population genetic algorithm for dual-resource constrained job shop scheduling problem[J]. Computers & Industrial Engineering, 2016, 102: 113-131.

[12] ElMaraghy H, Patel V, Ben Abdallah I. Scheduling of manufacturing systems under dual-resource constraints using genetic algorithms[J]. Journal of Manufacturing Systems, 2000, 19: 186-201.

[13] Araz Oezlem Uzun, Salum Latif. A multi-criteria adaptive control scheme based on neural networks and fuzzy inference for

DRC manufacturing systems[J]. International Journal of Production Research, 2010, 48: 251-270.

[14] Dunke Fabian, Nickel Stefan. A multi-method approach to scheduling and efficiency analysis in dual-resource constrained job shops with processing time uncertainty[J]. Computers & Industrial Engineering, 2022, 168.

[15] Renna Paolo, Thurer Matthias, Stevenson Mark. A game theory model based on Gale-Shapley for dual-resource constrained (DRC) flexible job shop scheduling[J]. International Journal of Industrial Engineering Computations, 2020, 11: 173-184.

[16] Delgoshaei Aidin, Ariffin Mohd Khairol Anuar, Ali Ahad. A multi-period scheduling method for trading-off between skilled-workers allocation and outsource service usage in dynamic CMS[J]. International Journal of Production Research, 2017, 55: 997-1039.

[17] Han Wenwu, Deng Qianwang, Gong Guiliang, Zhang Like, Luo Qiang. Multi-objective evolutionary algorithms with heuristic decoding for hybrid flow shop scheduling problem with worker constraint[J]. Expert Systems with Applications,2021,168: 114282.

[18] Geng Kaifeng, Ye Chunming, Liu Li. Research on Multi-Objective Hybrid Flow Shop Scheduling Problem With Dual Resource Constraints Using Improved Memetic Algorithm[J]. IEEE Access,2020,8: 104527-104542.

[19] Gong Guiliang, Chiong, Raymond, Deng Qianwang, Han Wenwu, Zhang Like, Lin Wenhui, Li Kexin. Energy-efficient flexible flow shop scheduling with worker flexibility[J]. Expert Systems with Applications,2020,141: 112902.

[20] Benavides Alexander J, Ritt Marcus, Miralles Cristóbal. Flow shop scheduling with heterogeneous workers[J]. European Journal of Operational Research,2014, 237: 713-720.

[21] Pargar Farzad, Zandieh Mostafa, Kauppila Osmo, Kujala Jaakko. The Effect of Worker Learning on Scheduling Jobs in a Hybrid Flow Shop: A Bi-Objective Approach[J]. Journal of Systems Science and Systems Engineering,2018,27: 265-291.

[22] Freitas Araujo Matheus, Arroyo José Elias C, Tavares Ricardo G. An effective hybrid meta-heuristic for a heterogeneous flow shop scheduling problem[J]. Proceedings of the Genetic and Evolutionary Computation Conference,2018, 245-252.

[23] Mraihi Tasnim, Driss Olfa Belkahla, El-Haouzi Hind Bril. A New Variant of the Distributed Permutation Flow Shop Scheduling Problem with Worker Flexibility[J]. Advances in Computational Collective Intelligence,2022, 587-597.

[24] Ruiz-Torres Alex J, Paletta Giuseppe, Adenso-Díaz Belarmino. Hybrid two stage flowshop scheduling with secondary resources based on time buckets[J]. International Journal of Production Research,2021,60: 1954-1972.

[25] Sánchez-Herrera Santiago, Montoya-Torres Jairo R, Solano-Charris Elyn L. Flow shop scheduling problem with position-dependent processing times[J]. Computers & Operations Research,2019,111: 325-345.

The Vehicle Routing Problem with Drone Stations

Abstract: This paper studies personnel scheduling and production scheduling considering worker mobility. As an important part of production resources, workers' movable characteristics play an indispensable role in production scheduling, which can effectively improve production efficiency and balance the workload between production lines. At the same time, in the hypothesis studied in this paper, for a given process, its processing time is directly related to the number of workers working on it. This paper takes the flow shop scheduling problem as the research object, takes the mobility of workers into consideration, establishes a mathematical model of flow shop scheduling considering the mobility of workers, and designs a genetic algorithm with simulated annealing mechanism to solve this problem. In addition, in order to obtain a high-quality scheduling scheme, this paper also proposes four decoding methods based on the earliest processing rule (EPR), determines the priority relationship between each operation, and puts forward relevant management enlightenment, so as to optimize task allocation and personnel scheduling, and realize the improvement of production efficiency.

Key words: Personnel Scheduling, Flow Shop Scheduling, Worker Mobility, Genetic Algorithms, Simulated Annealing, Earliest Processing Rules

表 3 算例“sma01”中的各标准处理时间

$p_{\pi(j),i}$	i=1	i=2	i=3	i=4	i=5
j=1	375	12	142	245	412
j=2	632	452	758	278	398
j=3	12	876	124	534	765
j=4	460	542	523	120	499
j=5	528	101	789	124	999
S_{max}			5		

表 4 算例“sma03”中的各标准处理时间

$p_{\pi(j),i}$	i=1	i=2	i=3
j=1	692	310	832
j=2	581	582	14
j=3	475	475	785
j=4	23	196	696
j=5	158	325	530
j=6	796	874	214
j=7	542	205	578
S_{max}		3	

表 5 算例“car01”中的各标准处理时间

$p_{\pi(j),i}$	i=1	i=2	i=3	i=4	i=5
j=1	375	12	142	245	412
j=2	632	452	758	278	398
j=3	12	876	124	534	765
j=4	460	542	523	120	499
j=5	528	101	789	124	999
j=6	796	245	632	375	123

j=7	532	230	543	896	452
j=8	14	124	214	543	785
j=9	257	527	753	210	463
j=10	896	896	214	258	259
j=11	532	302	501	765	988
S_{max}			5		

表 6 算例“car07”中的各标准处理时间

$p_{\pi(j),i}$	**i=1**	**i=2**	**i=3**	**i=4**	**i=5**	**i=6**	**i=7**
j=1	692	310	832	630	258	147	255
j=2	581	582	14	214	147	753	806
j=3	475	475	785	578	852	2	699
j=4	23	196	696	214	586	356	877
j=5	158	325	530	785	325	565	412
j=6	796	874	214	236	896	898	302
j=7	542	205	578	963	325	800	120
S_{max}				7			

表 7 算例“rec01”中的各标准处理时间

$p_{\pi(j),i}$	**i=1**	**i=2**	**i=3**	**i=4**	**i=5**
j=1	5	76	74	99	26
j=2	74	21	83	52	90
j=3	67	48	6	66	38
j=4	97	36	71	68	81
j=5	87	86	64	11	31
j=6	1	42	20	90	23
j=7	69	32	99	26	57
j=8	69	12	54	80	16
j=9	11	63	24	16	89
j=10	87	52	43	10	26
j=11	25	59	88	87	40
j=12	50	42	72	77	29
j=13	58	76	71	82	94
j=14	79	48	20	63	97
j=15	35	57	78	99	80

j=16	70	76	53	2	19
j=17	79	22	77	74	95
j=18	34	99	49	3	61
j=19	37	24	32	35	4
j=20	50	88	46	63	76
S_{max}			5		

表 8 算例“rec03”中的各标准处理时间

$p_{\pi(j),i}$	**i=1**	**i=2**	**i=3**	**i=4**	**i=5**
j=1	34	6	63	85	60
j=2	11	65	4	1	73
j=3	63	67	3	73	100
j=4	22	46	88	1	66
j=5	76	4	34	9	76
j=6	20	22	7	3	28
j=7	44	30	55	68	92
j=8	29	89	12	96	71
j=9	54	12	21	74	2
j=10	62	96	61	79	53
j=11	50	13	48	40	37
j=12	89	69	57	1	70
j=13	50	56	8	67	46
j=14	32	24	23	87	62
j=15	12	88	64	14	13
j=16	59	78	95	59	48
j=17	41	20	83	65	20
j=18	94	48	26	93	3
j=19	28	59	10	81	20
j=20	66	33	34	8	5
S_{max}			5		

表 9 解码方法对比

算例名称	JP	MP	LTRL	ECT
sma01	2230	2345	2140	2275
sma03	3348	3456	3294	3322

car01	5378	5522	5259	5426
car07	3728	3844	3627	3780
rec01	1246	1326	1166	1272
rec03	1022	1248	981	1174

表 10 是否考虑工人移动性的结果对比

结果对比（单位 s）	**sma01**	**sma03**	**car01**	**car07**	**rec01**	**rec03**
不考虑工人移动性	4578	3964	7038	6590	1343	1208
考虑工人移动性	2140	3294	5259	3627	1166	981
目标值优化大小	2438	670	1779	2963	177	227
优化百分比	53%	17%	25%	45%	13%	19%

表 11 所提出算法与 Gurobi 的小规模算例结果对比

结果对比	**sma01**		**sma03**	
（单位 s）	时间	目标值	时间	目标值
Gurobi	213	2140	190	3294
遗传算法	32.559	2140	38.895	3294

表 12 所提出算法与 Gurobi 的中规模算例结果对比

结果对比	**car01**		**car07**	
（单位 s）	时间	目标值	时间	目标值
Gurobi	710	5167	469	3414
遗传算法	78.341	5259	62.437	3627

表 13 所提出算法与 Gurobi 的大规模算例结果对比

结果对比	**rec01**		**rec03**	
（单位 s）	时间	目标值	时间	目标值
Gurobi	12923	1089	4662	968
遗传算法	91.714	1166	92.432	981

减小系统控制成本的双阈值水印添加策略用于重放攻击检测

朱琦琳 [a,b]，丁宇龙 [a,b]，杨双华 [a,c]

[a] 深圳市未来工业互联网安全保障重点实验室，南方科技大学，深圳，518055，中国

[b] 计算机科学与工程系，南方科技大学，深圳，518055，中国

[c] 计算机科学系，雷丁大学，雷丁，RG6 6UR，英国

摘　要：信息物理系统（Cyber-Physical Systems, CPS）是一种集成计算、物理过程和网络通信的智能控制系统，广泛应用于航空航天、工业制造和建筑行业中。近年来，CPS 越来越多地成为恶意攻击的目标，对社会和环境造成了严重影响。为了保障 CPS 的安全性，异常检测成为了守护系统正常运行的关键手段。然而，现有的 CPS 异常检测方法往往存在局限性。很多方法只在网络层面进行异常检测，并未考虑 CPS 是网络和物理融合的特殊性，缺乏对系统物理组件的身份认证。物理水印利用系统底层的控制逻辑，能够检测到 CPS 中难以发现的重放攻击。然而，传统持续性的水印添加方法造成了系统巨大且不必要的控制成本的增加。本文提出了双阈值的简约水印添加方法，在不依赖于攻击模型的情况下尽可能满足在无攻击时避免水印的添加并在攻击存在的时候始终添加水印，有效减少了系统的控制成本。通过在 CPS 领域广泛使用的线性化后四容水箱系统上进行的仿真实验，本文方法在节约系统控制成本上的有效性得到了验证。

关键词：信息物理系统；异常检测；重放攻击；物理水印

Dual-Threshold Watermarking Method for Replay Attack Detection with Reduced System Control Costs

Qilin Zhu[a,b]，Yulong Ding[a,b]，Shuang-Hua Yang[a,c]

[a] Shenzhen Key Laboratory of Safety and Security for Next Generation of Industrial Internet, Southern University of Science and Technology, Shenzhen, 518055, China

[b] Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, 518055, China

[c] Department of Computer Science, University of Reading, Reading, RG6 6UR, the UK

Abstract: Cyber-Physical Systems (CPS) are intelligent control systems that integrate computation, physical processes, and network communications, and are widely used in the aerospace, industrial manufacturing, and construction industries. In recent years, CPS have increasingly become the target of malicious attacks, causing serious impacts on society and the environment. In order to safeguard the security of CPS, anomaly detection has become a key means to guard the normal operation of the system. However, existing CPS anomaly detection methods often have limitations. Many methods perform anomaly detection only at the network level and do not take into account the specificity of CPS as a combination of network and physical, and lack the authentication of the system's physical components. Physical watermarking utilizes the underlying control logic of the system, enabling the detection of hard-to-detect replay attacks of CPS. However, traditional persistent watermarking

adding methods cause huge and unnecessary control cost increases. In this paper, we propose a dual-threshold parsimonious watermark adding method, which effectively reduces the control performance loss of the system by avoiding watermarking when there is no attack and always adding watermarks when an attack exists, without relying on the attack model. The effectiveness of this paper's method in reducing the system's control costs is verified through simulation experiments on a linearised quadruple water tank system widely used in CPS.

Key words: Cyber-physical system, anomaly detection, replay attack, physical watermarking

1 引言

CPS 是集成传感、网络、计算和控制技术并应用于物理空间的综合系统，旨在提升物理空间的自主性、效率和可靠性[1-2]。随着低成本设备在传感、通信和计算能力方面的提升，CPS 在航空航天、交通运输、建筑环境、能源、医疗保健和制造业等领域得到了广泛应用[1]。然而，随着 CPS 的大规模部署，系统安全性问题也日益突出。攻击者可以对 CPS 实施各种攻击，这些攻击可能对社会经济造成巨大破坏，甚至危及生命安全[1]。为确保 CPS 系统的有效运行，必须实施适当的安全防御措施，其中最基本的是攻击检测[3-4]。

异常检测系统能够从数据日志或网络流量中监控活动，并有效地对潜在的或尝试进行的攻击发出警报。尽管在传统的信息技术（Information Technology，IT）系统中已经对该领域进行了广泛研究，但传统 IT 领域的异常检测技术不能完全适用于 CPS[5-7]。具体来说，CPS 中的身份验证不仅需要在网络层面上验证，还需要在物理层面上进行验证。例如，针对 IT 领域的加密、防火墙、用户身份验证等保护措施对于物理攻击的防范可能仍然不足[8]，因为它们没有充分利用系统自身的物理特性。历史数据表明，攻击者常常能够破坏这些安全机制。此外，这些工具对内部人员的物理攻击无效[9]。

CPS 攻击策略主要分为数据欺骗攻击和拒绝服务（DoS）攻击[10]。在数据欺骗攻击中，攻击者向系统提供虚假数据[2,9]，其中一种典型方式是重放攻击。在重放攻击中，攻击者劫持传感器节点，记录一段时间的观测数据，然后在未来的时间点重放这些数据。攻击者无需了解系统参数和控制逻辑，即可在重放攻击期间保持隐身[9]。例如，著名的 Stuxnet 蠕虫攻击[11]是一个典型的重放攻击例子，该攻击成功破坏了伊朗的铀浓缩设施，造成了重大破坏[9]。

一种广泛应用的重放攻击检测技术是物理水印技术，即将水印信号添加到控制信号中，然后使用传感器观测值和来自卡尔曼估计器的估计值进行统计测试[2,9,12]。通过物理水印技术，可以在系统的物理动态框架内验证组件的身份，从而确保控制系统的正确运行[9]。物理水印是在系统控制信号中注入的已知噪声。通过向系统注入噪声信号，系统的动态特性会在传感器输出中反映出这些噪声的影响。异常检测器通过在系统实际接收到的传感器测量值中检测水印信号的存在，以验证系统的真实状态和操作。如果攻击者不了解这一物理水印，他们将无法模拟出与实际输入相一致的输出，从而无法成功躲避异常检测系统的检测。这种方法利用 CPS 的动态特性和底层的控制逻辑，可以有效识别异常，从而提高异常检测的精度和系统的韧性[9,13]。

虽然水印的添加可以提高异常检测的概率，但也会增加控制成本[9,14]。因此，如何在减少系统控制成本的情况下最大化异常检测率，成为研究的一个重要方向。考虑到实际场景中攻击事件的频率较低，例如 Stuxnet 蠕虫攻击每月仅激活 50 分钟[15]，持续性添加水印会导致系统性能的不必要下降。一些研究人员设计了不连续的水印信号[16]，以在攻击不存在时减少水印的添加，从而减小对系统性能的影响。

尽管不连续水印方法减少了系统的控制成本，但仍存在一些挑战。首先，水印的强度可能不足。为了不影响系统性能，研究者设置的水印强度通常较小，因此难以保证异常检测算法的准确性。其次，对水印添加时机的研究不足，即不连续水印的添加周期可能与实际攻击周期不匹配，从而影响检测效果[15]。

本文提出了一种双阈值的简约水印添加方法，在对重放攻击不进行任何假设的前提下，尽可能仅在攻击发生时刻添加水印，并在其他时刻减少水印的添加，从而显著减少系统的控制成本。通过在 CPS 领域广泛使用的线性化后四容水箱系统上的仿真实验，验证了该方法在减少系统控制成本上的显著效果。

本文的其余部分组织如下。第二节介绍 CPS 异常检测算法的相关工作。第三节提供背景和符号定义。第四节详细描述本文提出的算法。第五节展示实验设置和实验结果。第六节进行讨论和展望。最后，第七节总结本文的结论。

2　相关工作

Mo 等[9,13]是最早研究物理水印方法以确保 CPS 安全的论文。具体来说，Mo 等[13]在 CPS 中第一次提出“动态水印”概念：通过向控制信号输入中添加独立同分布的高斯水印信号并使用基于真实传感器测量值和来自卡尔曼估计器的传感器估计值之间的剩余项来提高系统异常检测器对重放攻击的检测能力。Mo 等[9]研究了从隐马尔可夫模型（Hidden Markov Model，HMM）生成的平稳高斯分布水印信号，扩展了以前仅考虑独立同分布高斯水印信号的结果。Satchidanandan 等[2]首次提出针对任意攻击的基于水印的一般理论和技术。这些论文均表明了物理水印方法对检测攻击特别是重放攻击的有效性。

在控制信号输入中添加物理水印增加了异常检测的概率，但同时也增加了系统的控制成本[9,14]。部分工作将水印直接相加或相乘到传感器测量值中[17-21]。在这类方法中，接收端首先检查传感器测量值的真实性，然后在控制器使用测量结果之前过滤掉水印信号。由于水印信号被滤除，因此系统控制成本不会增加。然而，这些方法并未利用系统的控制动力学信息，无法对物理组件进行物理身份验证[8,10]。例如，攻击者劫持传感器节点并在添加水印之前提供虚假数据。

一般来说，通过向控制信号中注入动态水印然后利用基于传感器测量值和预估值的剩余项来进行卡方检测的方法更为普遍。由于攻击是一种不太频繁的事件，因此在正常操作期间长时间添加水印信号会显著增加总控制成本[15]。研究人员正在探索多种方法来减少由于添加水印而导致的控制成本的增加并同时保持令人满意的异常检测性能[10,15,21]。

Ma 等[15]着重解决瞬态隐蔽攻击（Transient Covert Attacks，TCAs）的威胁（具有特定频率和短暂持续时间的重放攻击）。由于 TCAs 的活跃周期明显短于它们的休眠周期，因此减少不必要的水印将有助于

减小系统的控制成本。作者通过采用“事件触发”策略，提出了基于递归水印的检测算法。依照攻击发生的概率来决定水印添加的概率，将水印的触发模式分为三种类型：强制型、高概率型和低概率型。但该方法对攻击模型做了太多假设，攻击防御面较窄。Zhu 等[21]将水印容器从数据点转移到段，类似于平均滤波，平滑每个块内的噪声的同时维持住了所有块之间的波动特征，降低了剩余项的波动幅度，可以用更低功率的水印信号实现同样的异常检测率，从而减少了系统的控制成本。同时，该方法通过求解具有实际约束条件的优化问题，确定了最小水印强度和滑动时间窗口大小。但由于该方法只保证传感器数据通道传输的完整性，它固有前文所述难以检测出恶意传感器的弊端。Goyal 等[22]在系统中同时合成最佳水印信号和鲁棒控制器，以最小化由添加水印信号导致的控制成本的增加，并最大化攻击的检测。该方法基于 H_2范数设计了一个通用的动态控制器，同时添加水印信号。Naha 等[10]研究了一种基于证据的最快攻击检测水印策略，来限制不存在攻击时的水印事件的平均数量，从而减少攻击前控制成本的增加。作者将系统建模为随机最优控制问题，应用动态规划来在固定误报率上界和平均水印事件数上界的前提下最小化平均检测延迟。作者将攻击起始点建模为一个遵循参数 ρ 的几何分布的随机变量，这里 ρ 反映了防御者对攻击发生频率的估计。基于攻击呈几何分布的先验假设和系统建模，作者利用似然函数推导出在各时刻下存在攻击的后验概率 p_k，并利用基于 p_k 的值迭代动态规划方法解决前述最优控制问题。相较于传统持久添加水印的方法，该方法大幅度减少了系统的控制成本。

前述方法在减少水印的添加时或采用周期性水印添加方法，或者十分依赖于对攻击的建模，例如假定重放攻击具有特定的发生频率和特定的最短持续时间。并未解决如何在对重放攻击不进行任何假设时减少水印的添加的问题。本文提出了一个简约的双阈值动态水印添加方法。该方法在未对重放攻击模型做假设的前提下，尽量保证只在攻击发生时刻添加水印，其余时刻减少水印的添加，进而大幅减少系统控制成本。

3 背景和符号

CPS 通常被设计成闭环反馈控制（Closed-loop Feedback Control）系统，包含传感器、执行器和控制器等基本组件，通过传感器和控制器的协同工作以最小化噪声的影响并确保系统稳定运行。本部分我们把问题定义在离散线性时不变（Linear Time Invariant，LTI）系统上，并通过介绍卡尔曼滤波器（Kalman Filter）、LQG 控制器（Linear Quadratic Gaussian Control）、卡方检测器（χ^2 Failure Detector）和重放攻击模型来构建问题框架。接下来介绍传统方法中持续性水印的添加过程并解释有效性。

3.1 基本概念和符号

考虑以下离散 LTI 系统，其控制动力学方程由下式给出：

$$x_{k+1} = Ax_k + Bu_k + w_k \tag{3-1}$$

其中 $x_k \in \mathbb{R}^n$ 是 k 时刻下的系统状态，$w_k \in \mathbb{R}^n$ 是 k 时刻下的过程噪声，$w_k \sim \mathcal{N}(0, Q)$，$u_k \in \mathbb{R}^p$ 是 k 时刻下的控制信号输入。

假设一个传感器网络正在监测式 3-1 所描述的系统。在每一个时间步长下，所有的传感器读数都被发

送到控制器端。观测方程可以被表示为：

$$y_k = Cx_k + v_k \tag{3-2}$$

其中 $y_k \in \mathbb{R}^m$ 是 k 时刻下的传感器测量值向量，$v_k \sim \mathcal{N}(0, R)$ 是与 w_k 相独立的测量噪声。

本论文假设该系统已经运行了很长时间并且正处于稳定状态。

3.1.1　卡尔曼滤波器

卡尔曼滤波器是基于历史传感器测量值 $y_0, \cdots, y_k$ 的最优状态估计器，在存在高斯分布的随机噪声的情况下，它提供了对状态 x_k 的最小方差无偏估计。卡尔曼滤波器呈现如下递归形式：

$$\begin{aligned}
\hat{x}_{0|-1} &= \bar{x}_0, P_{0|-1} = \Sigma \\
\hat{x}_{k+1|k} &= A\hat{x}_{k|k} + Bu_k, P_{k+1|k} = AP_{k|k}A^T + Q, \\
K_k &= P_{k|k-1}C^T(CP_{k|k-1}C^T + R)^{-1}, \\
\hat{x}_{k|k} &= \hat{x}_{k|k-1} + K_k(y_k - C\hat{x}_{k|k-1}), P_{k|k} = P_{k|k-1} - K_kCP_{k|k-1}
\end{aligned} \tag{3-3}$$

尽管卡尔曼滤波器使用了一个随时间变化的增益 K_k，但如果系统是可检测的，增益 K_k 将会迅速收敛，此时卡尔曼滤波器将是一个固定增益估计器：

$$\begin{aligned}
&K \triangleq PC^T[CPC^T + R]^{-1} \\
&P = APA^T + Q - APC^T[CPC^T + R]^{-1}CPA^T
\end{aligned} \tag{3-4}$$

此时，系统状态的迭代方程为：

$$\hat{x}_{0|-1} = \bar{x}_0, \hat{x}_{k+1|k} = A\hat{x}_{k|k} + Bu_k, \hat{x}_{k|k} = \hat{x}_{k|k-1} + K(y_k - C\hat{x}_{k|k-1}) \tag{3-5}$$

3.1.2　LQG 控制器

在给定状态估计 $\hat{x}_{k|k}$ 的情况下，LQG 控制器最小化以下目标函数（体现系统的控制成本）：

$$J = minlim_{T\to\infty} E\frac{1}{T}\left[\sum_{k=0}^{T-1}\left(x_k^T W x_k + u_k^T U u_k\right)\right] \tag{3-6}$$

其中 W，U 是半正定矩阵，而 u_k 对于 $y_0, \cdots, y_k$ 是可测的，即 u_k 是历史传感器测量值的函数。由于分离原理的成立，式 3-6 的最优解是卡尔曼滤波器和 LQG 控制器的组合。其中卡尔曼滤波器由式 3-4 和 3-5 定义，而 LQG 控制器是一个基于最优状态估计 x_k 的固定增益线性控制器，形式如下：

$$u_k^* = Lx_{k|k} \tag{3-7}$$

其中 u_k^* 是系统最优控制信号输入，L 是控制增益矩阵，定义如下：

$$L \triangleq -(B^TSB + U)^{-1}B^TSA \tag{3-8}$$

其中 S 满足以下 Riccati 方程：

$$S = A^TSA + W - A^TSB(B^TSB + U)^{-1}B^TSA \tag{3-9}$$

此时，最优状态估计器和控制器给出的目标函数如下：

$$J = trace\,(SQ) + trace\left[(A^T SA + W - S)(P - KCP)\right] \tag{3-10}$$

3.1.3 卡方检测器

卡方检测器[23]是控制系统中广泛使用的异常检测器。

对于在 3-1 中定义的 LTI 系统，使用卡尔曼滤波器和 LQG 控制器，卡尔曼滤波器的剩余项 $y_i - C\hat{x}_{i|i-1}$ 满足均值为 0，协方差为 $\mathcal{P}$ 的独立同分布高斯分布，其中 $\mathcal{P} = CPC^T + R$。详细证明过程请查阅论文[23]。

因此，定义残差为：

$$g_k = \sum_{i=k-\mathcal{T}+1}^{k} (y_i - C\hat{x}_{i|i-1})^T \mathcal{P}^{-1} (y_i - C\hat{x}_{i|i-1}) \tag{3-11}$$

当残差很高时，意味着系统的最优估计和真实情况存在着很大偏差，系统很可能已经发生了某种故障。为了检测异常和可能存在的攻击，定义 k 时刻下卡方检测器所满足的形式为：

$$g_k = \sum_{i=k-\mathcal{T}+1}^{k} (y_i - C\hat{x}_{i|i-1})^T \mathcal{P}^{-1} (y_i - C\hat{x}_{i|i-1}) \lessgtr threshold \tag{3-12}$$

其中 $\mathcal{T}$ 是检测窗口的大小。如果 g_k 大于某个设定的阈值，那么检测器将触发警报。

3.1.4 重放攻击

假设攻击者有以下能力：

1. 攻击者可以实时监测所有传感器读数，并可以随时对其进行任意修改。令攻击者修改后的传感器读数为 $y_k^{'}$。

2. 攻击者可以随时向系统中注入虚假控制信号输入 u_k^{a}。

在具备这些能力的前提下，攻击者将执行以下重放攻击，分为两个阶段：

1. 攻击者在不给系统注入任何输入的情况下记录足够长时间的传感器测量值 y_k。

2. 攻击者重放记录的历史传感器测量值 y_k，并同时注入一系列错误的控制信号输入。

3.2 重放攻击绕过卡方检测

本小节将分析不考虑物理水印时卡方检测器对检测重放攻击无效。论文[13]给出了详细证明，但为了行文完整性，这里也包含了此部分说明。对于重放攻击，由于攻击者重放的数据是真实系统的历史测量值，不妨认为攻击者虚拟运行了一个真实系统的时移版本。因此，将 $y_k^{'}$ 视为以下虚拟系统的输出（攻击者并未真实运行虚拟系统）：

$$\begin{aligned} x_{k+1}^{'} &= Ax_k^{'} + Bu_k^{'} + w_k^{'}, y_k^{'} = Cx_k^{'} + v_k^{'} \\ \hat{x}_{k+1|k}^{'} &= A\hat{x}_{k|k}^{'} + Bu_k^{'}, \hat{x}_{k+1|k+1}^{'} = \hat{x}_{k+1|k}^{'} + K\left(y_k^{'} - \hat{x}_{k+1|k}^{'}\right) \\ u_k^{'} &= L\hat{x}_{k|k}^{'} \end{aligned} \tag{3-13}$$

假设攻击者从时 t 时刻开始记录序列 y_k，那么 $x_k^{'} = x_{t+k}$，$\hat{x}_{k|k}^{'} = \hat{x}_{t+k|t+k}$。

现假设系统正受到重放攻击，而防御者正在使用卡方检测器进行入侵检测，则卡尔曼滤波器的估计值 $\hat{x}_{k|k-1}$ 能以递归方式重写如下：

$$\begin{aligned}\hat{x}_{k+1|k} &= A\hat{x}_{k|k} + Bu_k = (A+BL)\hat{x}_{k|k} \\ &= (A+BL)\left[\hat{x}_{k|k-1} + K\left(y_k^{'} - C\hat{x}_{k|k-1}\right)\right] \\ &= (A+BL)(I-KC)\hat{x}_{k|k-1} + (A+BL)Ky_k^{'}\end{aligned} \tag{3-14}$$

对于虚拟系统，同样的方程也适用于 $\hat{x}_{k|k-1}^{'}$：

$$\hat{x}_{k+1|k}^{'} = (A+BL)(I-KC)\hat{x}_{k|k-1}^{'} + (A+BL)Ky_k^{'} \tag{3-15}$$

定义 $\mathcal{A} \triangleq (A+BL)(I-KC)$，式 3-14 减去式 3-15，则：

$$\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^{'} = \mathcal{A}^k\left(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'}\right) \tag{3-16}$$

因此：

$$y_k^{'} - C\hat{x}_{k|k-1} = \left(y_k^{'} - C\hat{x}_{k|k-1}^{'}\right) + C\mathcal{A}^k\left(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'}\right) \tag{3-17}$$

残差 g_k 可以被改写为：

$$\begin{aligned}g_k &= \sum_{i=k-\mathcal{S}+1}^{k}\left[\left(y_i^{'} - C\hat{x}_{i|i-1}\right)^T\mathcal{P}^{-1}\left(y_i^{'} - C\hat{x}_{i|i-1}\right)\right]. \\ &= \sum_{i=k-\mathcal{S}+1}^{k}\left[\left(y_i^{'} - C\hat{x}_{i|i-1}^{'}\right)^T\mathcal{P}^{-1}\left(y_i^{'} - C\hat{x}_{i|i-1}^{'}\right)\right. \\ &\left.+2\left(y_i^{'} - C\hat{x}_{i|i-1}^{'}\right)^T\mathcal{P}^{-1}C\mathcal{A}^i\left(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'}\right) + \left(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'}\right)^T(\mathcal{A}^i)^TC^T\mathcal{P}^{-1}C\mathcal{A}^i\left(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'}\right)\right]\end{aligned} \tag{3-18}$$

由于假设系统稳定运行，且虚拟系统是真实系统的时移版本，因此 $y_k^{'} - C\hat{x}_{k|k-1}^{'}$ 的分布与 $y_k - C\hat{x}_{k|k-1}$ 完全相同。如果攻击者想尽量保持隐蔽，即 $\mathcal{A}$ 是稳定的，式 3-18 中的第二项和第三项将收敛到 0（本研究将始终假设矩阵 $\mathcal{A}$ 是稳定的）。因此，残差 g_k 将收敛到与系统正常运行时相同的分布。卡方检测器的异常检测率将收敛到系统正常运行状态下的误报率，这表明检测器提供的有效信息将趋于 0，即检测器变得无效。

3.3　添加持续性水印后的重放攻击检测

正如前一小节所述，控制系统不具备抵抗重放攻击的能力。本部分将介绍在如式 3-1 所定义的一般离散 LTI 系统上传统的持续性水印添加过程和给出该方法的有效性证明。

物理水印是针对重放攻击设计的检测方法。持续性水印方法会始终往最优控制信号中添加如下水印 Δu_k：

$$u_k = u_k^* + \Delta u_k \tag{3-19}$$

其中 u_k^* 是最优的 LQG 控制信号，Δu_k 从均值为零、协方差矩阵为 $\mathcal{Q}$ 的独立同分布的高斯分布中随机抽取，且 Δu_k 与 u_k^* 相互独立。

添加的水印 Δu_k 作为认证信号，以下证明展示了添加水印信号对提高系统对重放攻击的检测能力的有效性。

假设系统正遭到重放攻击，由式 3-14 和式 3-19 易知：

$$\begin{aligned}\hat{x}_{k+1|k} &= (A+BL)(I-KC)\hat{x}_{k|k-1} + (A+BL)Ky_k^{'} + B\Delta u_k \\ &= \mathcal{A}\hat{x}_{k|k-1} + (A+BL)Ky_k^{'} + B\Delta u_k\end{aligned} \tag{3-20}$$

同理，对于虚拟系统：

$$\hat{x}_{k+1|k}^{'} = \mathcal{A}\hat{x}_{k|k-1}^{'} + (A+BL)Ky_k^{'} + B\Delta u_k^{'} \tag{3-21}$$

因此，式 3-20 减去式 3-21，得到：

$$\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^{'} = \mathcal{A}^k\left(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'}\right) + \sum_{i=0}^{k-1}\mathcal{A}^{k-i-1}B\left(\Delta u_i - \Delta u_i^{'}\right) \tag{3-22}$$

继而：

$$\begin{aligned}y_k^{'} - C\hat{x}_{k|k-1} &= y_k^{'} - C\hat{x}_{k|k-1}^{'} + C\mathcal{A}^k\left(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'}\right) \\ &\quad + C\sum_{i=0}^{k-1}\mathcal{A}^{k-i-1}B\left(\Delta u_i - \Delta u_i^{'}\right)\end{aligned} \tag{3-23}$$

式 3-23 中项 $y_k^{'} - C\hat{x}_{k|k-1}^{'}$ 与 $y_k - C\hat{x}_{k|k-1}$ 具有完全相同的分布。当 $\mathcal{A}$ 稳定时，第二项 $C\mathcal{A}^k(\hat{x}_{0|-1} - \hat{x}_{0|-1}^{'})$ 将收敛为 0。又由于 Δu_i 独立于虚拟系统，且对于虚拟系统，$y_k^{'} - C\hat{x}_{k|k-1}^{'}$ 独立于 $\Delta u_i^{'}$。因此：

$$\begin{aligned}&lim_{k\to\infty}Cov\left(y_k^{'} - C\hat{x}_{k|k-1}\right) = lim_{k\to\infty}Cov\left(y_k^{'} - C\hat{x}_{k|k-1}^{'}\right) \\ &+ \sum_{i=0}^{\infty}Cov\left(C\mathcal{A}^iB\Delta u_i\right) + \sum_{i=0}^{\infty}Cov\left(C\mathcal{A}^iB\Delta u_i^{'}\right) \\ &= \mathcal{P} + \sum_{i=0}^{\infty}C\mathcal{A}^iBQB^T(\mathcal{A}^i)^TC^T + \sum_{i=0}^{\infty}C\mathcal{A}^iBQB^T(\mathcal{A}^i)^TC^T \\ &= \mathcal{P} + 2\sum_{i=0}^{\infty}C\mathcal{A}^iBQB^T(\mathcal{A}^i)^TC^T\end{aligned} \tag{3-24}$$

令 $\mathcal{U}$ 表示以下 Lyapunov 方程的解:

$$\mathcal{U} - BQB^T = \mathcal{A}\mathcal{U}\mathcal{A}^T \tag{3-25}$$

可得：

$$\mathcal{U} = \sum_{i=0}^{\infty}\mathcal{A}^iBQB^T(\mathcal{A}^i)^T \tag{3-26}$$

因此，$\lim_{k\to\infty}\mathrm{Cov}\left(y_k^{'} - C\hat{x}_{k|k-1}\right) = \mathcal{P} + 2C\mathcal{U}C^T$，且：

$$\begin{aligned}&lim_{k\to\infty}E\left[\left(y_k^{'} - C\hat{x}_{k|k-1}\right)^T\mathcal{P}^{-1}\left(y_k^{'} - C\hat{x}_{k|k-1}\right)\right] \\ &= trace\left[lim_{k\to\infty}Cov\left(y_k^{'} - C\hat{x}_{k|k-1}\right)\times\mathcal{P}^{-1}\right] \\ &= m + 2trace\left(C^T\mathcal{P}^{-1}C\mathcal{U}\right).\end{aligned} \tag{3-27}$$

综合式 3-11 式 3-27，在重放攻击下，残差的渐进期望为：

$$lim_{k\to\infty}E(g_k) = m\mathcal{T} + 2trace\left(C^T\mathcal{P}^{-1}C\mathcal{U}\right)\mathcal{T} \tag{3-28}$$

当系统正常运行时，若无重放攻击：

$$\begin{aligned}&lim_{k\to\infty}E\left[(y_k - C\hat{x}_{k|k-1})^T\mathcal{P}^{-1}(y_k - C\hat{x}_{k|k-1})\right] \\ &= trace\left[lim_{k\to\infty}Cov\left(y_k - C\hat{x}_{k|k-1}\right)\times\mathcal{P}^{-1}\right] \\ &= m\end{aligned} \tag{3-29}$$

综合式 3-11 和式 3-29，当系统正常运行时，残差 g_k 的渐进期望为：

$$E(g_k) = m\mathcal{T} \tag{3-30}$$

对比式 3-30 和式 3-28，残差 g_k 期望值的差异说明了算法对重放攻击的检测率不再会收敛到误报率，证明了水印方法的有效性。

4　算法框架

由于物理水印是往系统的最优控制信号上添加扰动，因此控制器在 LQG 意义上不再是最优。这意味着为了检测攻击，算法牺牲了系统的控制性能。式 4-1 描述了当水印 Δu_k 注入到控制信号后 LQG 的控制成本（由于证明过程复杂，本文将不再进行阐述，感兴趣的读者详见论文[13]：

$$J^{'} = J + trace\left[(U + B^T SB)Q\right] \tag{4-1}$$

持续性水印方法会造成系统大量且不必要的控制成本的增加，因为攻击者的攻击频率往往非常低，例如著名的震网攻击每个月只攻击 50 分钟并在剩余的时间保持沉默。受已有工作的启发[10,15]，在攻击不存在或者是小概率存在的情况下减少水印的添加能有效减少系统的控制成本。本研究提出双阈值的水印添加方法，在不依赖于攻击模型的情况下尽量满足在无攻击时避免水印的添加并在攻击存在的时候始终添加水印，极大减少了系统的控制成本。

4.1　双阈值的水印添加方法

由式 3-18 可知，虽然在无水印添加时，针对重放攻击，卡方检测器的异常检测率将迅速收敛到系统正常运行状态下的误报率，检测器变得无效。但是若能敏锐捕捉到攻击发生瞬间的异常并在此后攻击发生过程中稳住水印的添加，那么我们将能最大限度实现只在攻击发生的时刻持续添加水印。

本研究提出双阈值水印添加方法，设置阈值 Th_0 和 Th_1，其中 Th_0 用于决定是否添加水印，Th_1用于决定是否判定为攻击，$Th_0 < Th_1$。定义判断条件为：

$$\begin{cases} g_k > Th_0, k+1 \text{ 时刻加水印} \\ g_k < Th_0, k+1 \text{ 时刻无水印} \end{cases}$$
$$\begin{cases} g_k > Th_1, k \text{ 时刻有异常} \\ g_k < Th_1, k \text{ 时刻无异常} \end{cases} \tag{4-2}$$

当攻击发生的瞬间，卡尔曼滤波器对传感器测量值的估计会产生更大偏差；以及偶尔由于系统过程噪声和测量噪声的影响，残差 g_k 可能会超过阈值 Th_0。若 k 时刻下 g_k 超过了阈值 Th_0，算法将在 $k+1$ 时刻为系统增添水印。此时，若系统并未遭到重放攻击，水印误添加，则残差 g_k 会快速回到正常水平，水印的添加将会终止；而若系统正遭到重放攻击，由于水印的添加，由式 3-27 和式 3-29 知，每一时刻 $\lim_{k\to\infty} E\left[\left(y_k^{'} - C\hat{x}_{k|k-1}\right)^T \mathcal{P}^{-1}\left(y_k^{'} - C\hat{x}_{k|k-1}\right)\right]$相较于 $\lim_{k\to\infty} E\left[(y_k - C\hat{x}_{k|k-1})^T \mathcal{P}^{-1}(y_k - C\hat{x}_{k|k-1})\right]$的期望会多出一部分，进而在接下来的时刻 g_k 更有可能超过阈值 Th_0，以此实现在攻击发生过程中水印的持续添加。

双阈值的水印添加方法是一个简约直观的方法，后续的实验充分表明了该方法的有效性。该方法大幅

减少了在攻击不存在时水印的添加，并在攻击发生过程中持续添加水印，极大节约了系统的控制成本。

5 实验

实验使用 Windows 10 上的 Python 3.7.4 进行，配备 Intel(R) Core(TM) i7-8750H CPU，16GB。

5.1 实验设置

为了测试本研究所提方法的性能，考虑一个在工业控制领域广泛应用的典型四容水箱控制系统。本研究使用的系统模型通过将论文[24]中的四容水箱控制系统在操作点 $x=[10,10,10,10]^T$ 附近线性化，并以 2 秒为采样周期来离散化得到。

$$
\begin{gathered}
A=\begin{bmatrix}0.9394 & 0 & 0.0575 & 0\\ 0 & 0.9508 & 0 & 0.0496\\ 0 & 0 & 0.9406 & 0\\ 0 & 0 & 0 & 0.9491\end{bmatrix},\\
B=\begin{bmatrix}0.0177 & 0.0002 & 0 & 0.009\\ 0.0002 & 0.0187 & 0.0069 & 0\end{bmatrix},\\
C=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix},\\
W=\begin{bmatrix}20\cdot I_2 & 0\\ 0 & I_2\end{bmatrix},\\
U=10\cdot I_2, Q=0.25\cdot I_4, R=0.5\cdot I_2
\end{gathered}
\tag{5-1}
$$

矩阵 $\mathcal{A}=(A+BL)(I-KC)$ 是稳定的。设置持续性水印方法的误报率为 2%，并借此选定阈值 Th_1 为 89。阈值 Th_0 的设置取决于用户对检测率的追求情况以及对控制成本的接受度，Th_0 设置得越高，攻击检测的能力会越强，但同时平均控制成本也会上升。本实验中我们将阈值 Th_0 设定为 75，此时存在攻击时漏添加水印的比例不高于 10%，无攻击情况下误添加水印的比例约为 20%。残差 g_k 的窗口范围 $\mathcal{T}$ 设置为 32。通过求解具有控制代价约束的半定规划问题[25]，确定水印的标准协方差矩阵 Q 为 $Q=\begin{bmatrix}5001 & 98.5\\ 98.5 & 2\end{bmatrix}$。

为验证本文所提出的双阈值水印添加方法在节约系统控制成本方面的有效性，本实验的对比算法为典型的持续性水印添加方法，其他的依赖于对重放攻击进一步建模（利用到假定的攻击发生的频率和周期性和持续时长等先验）的非持续性水印方法不做对比。

设置水印的添加强度为α（$0\leqslant\alpha\leqslant1$），此时水印定义为从均值为 0，协方差矩阵为 α^2Q 的独立同分布多元高斯分布中采样。持续性水印方法测试 α 分别取值为 0.1, 0.2, ..., 1 时的情况，本文方法将 α 取为 1。

令检测到的异常信号为正（Positive），正常信号为负（Negative）。实验使用精确率（Precision）、召回率（Recall）、F1 分数（F1-Score）以及 MTTD（Mean Time To Detection，平均检测时间）四个度量来衡量算法性能。其中 MTTD 指攻击者从发起攻击到最终被网络或终端安全设备检测出来所持续的时间，在本实验中指重放攻击发生时刻与卡方检测器检测到异常的时刻之间的时间间隔。

5.2 实验结果

为了尽可能保持隐蔽，实际场景中攻击者发动重放攻击的频率往往非常低，且攻击的连续持续时间不会太长[15]。图 5-1、图 5-2，和图 5-3 分别展示了当重放攻击的持续时长分别为 1000，1500，以及 2000

个时间步长（采样时间间隔），且攻击占比分别为 5%，2%和 1%时持续性水印方法和本文提出的双阈值水印方法在召回率-控制成本，精确率-控制成本，F1 分数-控制成本上的性能对比。每组实验均被重复了 100 次，这里仅展示平均结果。

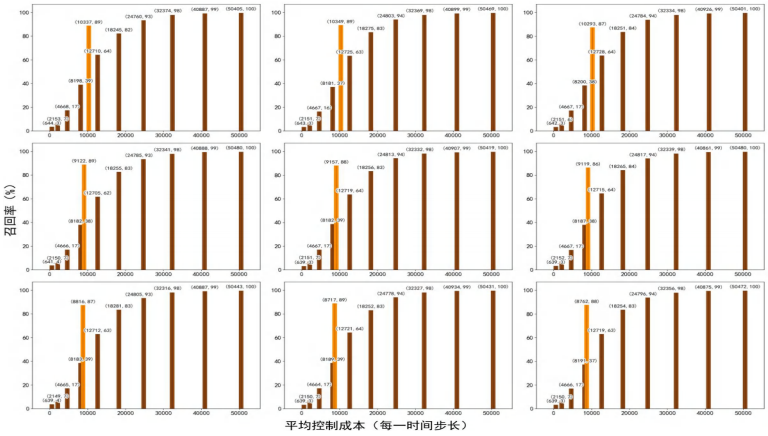


图 5-1 不同攻击持续时长和占比下持续性水印方法和本方法检测重放攻击的召回率-控制成本性能对比。上左：攻击持续时长 1000，攻击占比 5%；上中：攻击持续时长 1000，攻击占比 2%；上右：攻击持续时长 1000，攻击占比 1%；中左：攻击持续时长 1500，攻击占比 5%；中中：攻击持续时长 1500，攻击占比 2%；中右：攻击持续时长 1500，攻击占比 1%；下左：攻击持续时长 2000，攻击占比 5%；下中：攻击持续时长 2000，攻击占比 2%；下右：攻击持续时长 2000，攻击占比 1%

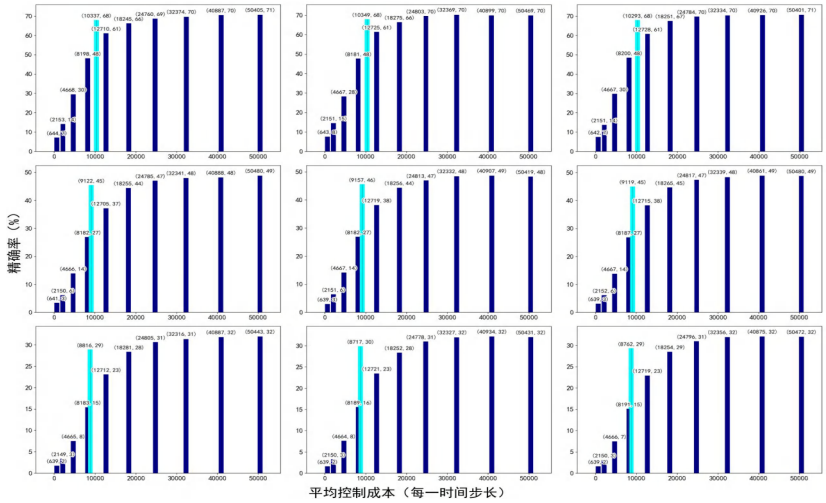


图 5-2 不同攻击持续时长和占比下持续性水印方法和本方法检测重放攻击的精确率-控制成本性能对比。上左：攻击持续时长 1000，攻击占比 5%；上中：攻击持续时长 1000，攻击占比 2%；上右：攻击持续时长 1000，攻击占比 1%；中左：攻击持续时长 1500，攻击占比 5%；中中：攻击持续时长 1500，攻击占比 2%；中右：攻击持续时长 1500，攻击占比 1%；下左：攻击持续时长 2000，攻击占比 5%；下中：攻击持续时长 2000，攻击占比 2%；下右：攻击持续时长 2000，攻击占比 1%

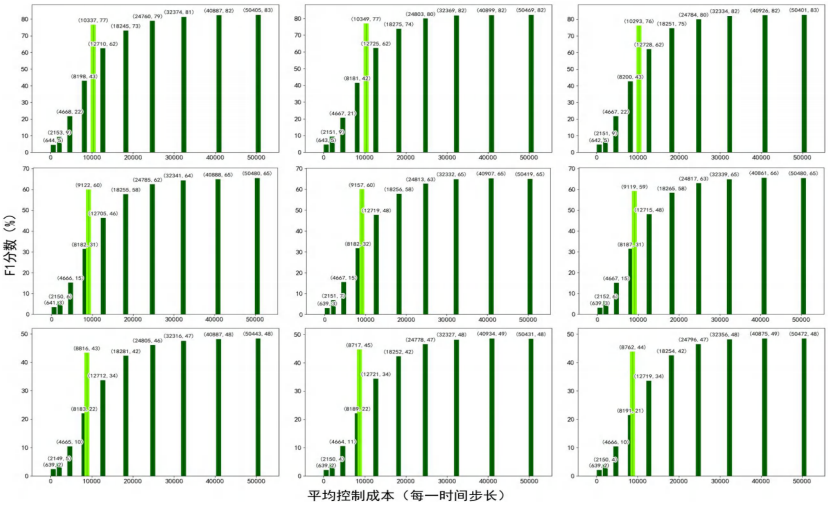


图 5-3 不同攻击持续时长和占比下持续性水印方法和本方法检测重放攻击的 F1 分数-控制成本性能对比。上左：攻击持续时长 1000，攻击占比 5%；上中：攻击持续时长 1000，攻击占比 2%；上右：攻击持续时长 1000，攻击占比 1%；中左：攻击持续时长 1500，攻击占比 5%；中中：攻击持续时长 1500，攻击占比 2%；中右：攻击持续时长 1500，攻击占比 1%；下左：攻击持续时长 2000，攻击占比 5%；下中：攻击持续时长 2000，攻击占比 2%；下右：攻击持续时长 2000，攻击占比 1%

可见，对于召回率指标，改变攻击持续时长和攻击占比对两方法的影响不大。本文方法的召回率指标性能上限相对于持续性水印方法略有降低。当水印强度为 1 时，持续性水印方法能达到几乎 100%的召回率。然而，本文方法在节约系统控制成本上效果始终显著，在同一控制成本下本文方法的召回率约为对比方法的 2 倍，在同一召回率下本文方法的控制成本约为对比方法的 50%。且当攻击占比降低时本文方法的优势越发明显。

当攻击占比降低，两方法精确率均有大幅下降，这是因为本文将误报率固定为了 2%，因此攻击占比会直接影响精确率。此外，当两方法的精确率相当时，本文方法的控制成本约为持续性水印方法的一半。对比持续性水印添加方法，本研究方法在攻击占比越低时优势越明显。虽然本文方法并不能达到对比方法的性能上限，但是差距不大，仅相差 2-4%。当攻击占比为 1%时，在几乎同样的控制成本下，本文方法精确率约为对比方法的 1.8 倍。

F1 分数是综合召回率和精确率的结果，因此更具代表性。在 F1 分数指标上，两方法在精确率和召回率指标上随着攻击持续时长和攻击占比的改变而改变的趋势特点也均有体现，这里不再赘述。需要强调的是，持续性水印方法在水印强度大于等于 0.7 倍以后得到的性能回报收益太低，这意味着需要用极大量的控制成本才能换来一点检测效果的提升，因此不太具有现实意义。

图 5-4 展示了当重放攻击的持续时长分别为 1000，1500，以及 2000 个时间步长（采样时间间隔），且攻击占比分别为 5%，2%和 1%时持续性水印方法和本文提出的双阈值水印方法在 MTTD-控制成本上的性能对比。同样，每组实验均被重复了 100 次，这里仅展示平均结果。

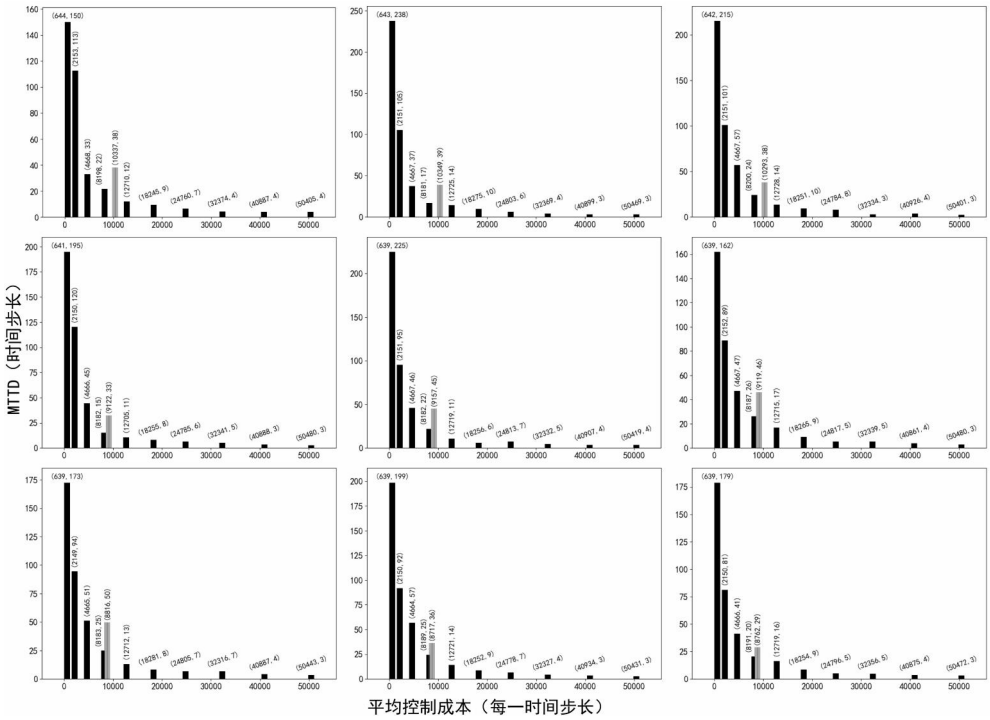


图 5-4 不同攻击持续时长和占比下持续性水印方法和本方法检测重放攻击的 MTTD-控制成本性能对比。上左：攻击持续时长 1000，攻击占比 5%；上中：攻击持续时长 1000，攻击占比 2%；上右：攻击持续时长 1000，攻击占比 1%；中左：攻击持续时长 1500，攻击占比 5%；中中：攻击持续时长 1500，攻击占比 2%；中右：攻击持续时长 1500，攻击占比 1%；下左：攻击持续时长 2000，攻击占比 5%；下中：攻击持续时长 2000，攻击占比 2%；下右：攻击持续时长 2000，攻击占比 1%

同一成本下本文方法的 MTTD 约为对比方法的两倍。因为所提出的双阈值水印添加方法并不能保证在攻击发生时刻一定添加水印，水印的添加可能存在延迟，因而对攻击的平均检测时间的延迟也会更长。尽管如此，本文方法的 MTTD 始终维持在 30-50 个时间步长（采样时间间隔）内，相较于攻击时长完全可以接受。

6　总结与展望

本方法充分利用了以下信息：在攻击发生的瞬间，卡尔曼滤波器对传感器测量值的估计会产生更大偏差；以及偶尔由于系统过程噪声和测量噪声的影响，残差 g_k 可能会增大，从而提出了双阈值的简约水印添加方法。水印添加后，一旦系统真实遭到了重放攻击，残差会进一步增长，进而更有可能在接下来的攻击过程中维持在超过阈值 Th_0 的水平。借此，本文方法实现了在无攻击时减少水印的添加并在攻击发生过程中持续添加水印的目的，相较于持续性水印方法减少了系统的控制成本。

本方法也存在以下不足。首先，本方法设定阈值 Th_0 为硬阈值，一旦设定后不会随着系统实时状态的改变而改变，且阈值 Th_0 的选取依赖于仿真实验测试。未来将考虑利用强化学习来动态调整这一阈值，以实现控制成本进一步的节约。此外，由于所提出方法并不能保证在攻击发生时一定添加水印，算法的检测性能相比于持续性水印方法在同样水印强度下的性能略低。

7　结论

基于物理水印的控制系统异常检测算法提高了系统对恶意攻击的检测能力，特别是对重放攻击的检测。本文在传统的持续性水印方法基础上提出简约的双阈值水印添加方法。在 CPS 领域广泛使用的线性化后四容水箱系统上的仿真实验表明了本方法在减少系统控制成本上的贡献。

总结本文方法的技术贡献点如下：

- 提出双阈值的简约水印添加方法，在不依赖于攻击模型的情况下能够尽可能在无攻击时避免水印的添加并在攻击存在的时候始终添加水印，极大减少了系统的控制成本。
- 提出的双阈值水印添加方法不依赖于对重放攻击的建模，水印的添加过程和攻击的检测均不需要预先假设攻击发生的频率和持续时间，具有更大的普适性。

参考文献

[1] Alguliyev R, Imamverdiyev Y, Sukhostat L. Cyber-physical systems and their security issues[J]. Computers in Industry, 2018, 100: 212-223.

[2] Satchidanandan B, Kumar P R. Dynamic watermarking: Active defense of networked cyber－physical systems[J]. Proceedings of the IEEE, 2016, 105(2): 219-240.

[3] Bai C Z, Gupta V, Pasqualetti F. On Kalman filtering with compromised sensors: Attack stealthiness and performance bounds[J]. IEEE Transactions on Automatic Control, 2017, 62(12): 6641-6648.

[4] Lucia W, Gheitasi K, Ghaderi M. Setpoint attack detection in cyber-physical systems[J]. IEEE Transactions

on Automatic Control, 2020, 66(5): 2332-2338.

[5] Ding K, Ren X, Quevedo D E, et al. Defensive deception against reactive jamming attacks in remote state estimation[J]. Automatica, 2020, 113: 108680.

[6] Liu G, Lai L. Action-manipulation attacks against stochastic bandits: Attacks and defense[J]. IEEE Transactions on Signal Processing, 2020, 68: 5152-5165.

[7] Zhou C, Huang S, Xiong N, et al. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2015, 45(10): 1345-1360.

[8] Naha A, Teixeira A, Ahlén A, et al. Sequential detection of replay attacks[J]. IEEE Transactions on Automatic Control, 2022, 68(3): 1941-1948.

[9] Mo Y, Weerakkody S, Sinopoli B. Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs[J]. IEEE Control Systems Magazine, 2015, 35(1): 93-109.

[10] Naha A, Teixeira A M H, Ahlén A, et al. Quickest detection of deception attacks on cyber－physical systems with a parsimonious watermarking policy[J]. Automatica, 2023, 155: 111147.

[11] Langner R. Stuxnet: Dissecting a cyberwarfare weapon[J]. IEEE security & privacy, 2011, 9(3): 49-51.

[12] Ding D, Han Q L, Xiang Y, et al. A survey on security control and attack detection for industrial cyber-physical systems[J]. Neurocomputing, 2018, 275: 1674-1683.

[13] Mo Y, Sinopoli B. Secure control against replay attacks[C]//2009 47th annual Allerton conference on communication, control, and computing (Allerton). IEEE, 2009: 911-918.

[14] Liu H, Mo Y, Yan J, et al. An online approach to physical watermark design[J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3895-3902.

[15] Ma L, Chu Z, Yang C, et al. Recursive watermarking-based transient covert attack detection for the industrial cps[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 1709-1719.

[16] Fang C, Qi Y, Cheng P, et al. Optimal periodic watermarking schedule for replay attack detection in cyber－physical systems[J]. Automatica, 2020, 112: 108698.

[17] Ferrari R M G, Teixeira A M H. Detection and isolation of replay attacks through sensor watermarking[J]. IFAC-PapersOnLine, 2017, 50(1): 7363-7368.

[18] Trapiello C, Rotondo D, Sanchez H, et al. Detection of replay attacks in CPSs using observer-based signature compensation[C]//2019 6th International Conference on Control, Decision and Information Technologies (CoDIT). IEEE, 2019: 1-6.

[19] Sánchez H S, Rotondo D, Escobet T, et al. Detection of replay attacks in cyber-physical systems using a frequency-based signature[J]. Journal of the Franklin Institute, 2019, 356(5): 2798-2824.

[20] Ye D, Zhang T Y, Guo G. Stochastic coding detection scheme in cyber-physical systems against replay attack[J]. Information Sciences, 2019, 481: 432-444.

[21] Zhu H, Liu M, Fang C, et al. Detection-performance tradeoff for watermarking in industrial control systems[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2780-2793.

[22] Goyal R, Somarakis C, Noorani E, et al. Co-design of watermarking and robust control for security in cyber-physical systems[C]//2022 IEEE 61st Conference on Decision and Control (CDC). IEEE, 2022: 4821-4826.

[23] Mehra R K, Peschon J. An innovations approach to fault detection and diagnosis in dynamic systems[J]. Automatica, 1971, 7(5): 637-640.

[24] Navarro A F. Security analysis of a wireless quadruple tank control system[J]. KTH Electrical Engineering, Master" s Degree Project, 2011.

[25] Mo Y, Chabukswar R, Sinopoli B. Detecting integrity attacks on SCADA systems[J]. IEEE Transactions on Control Systems Technology, 2013, 22(4): 1396-1407.

[作者简介]

朱琦琳（1999—），女，2018 年获得四川大学网络空间安全学院学士学位，目前正在深圳市南方科技大学计算机科学与工程系攻读硕士学位。研究兴趣包括信息物理系统安全等。

丁宇龙（1983—），男，分别于 2005 年和 2008 年在北京清华大学获得化学工程学士学位和硕士学位，并于 2012 年在加拿大不列颠哥伦比亚大学（温哥华）获得化学工程博士学位。目前担任深圳市南方科技大学计算机科学与工程系以及深圳市未来工业互联网安全保障重点实验室副研究员。研究兴趣包括工业物联网和低功耗广域网络等。

杨双华（1963—），男，1991 年在中国浙江大学获得博士学位，并于 2014 年因其在无线监控研究方面的贡献被拉夫堡大学授予 DSc 学位。目前担任雷丁大学计算机科学系主任兼南方科技大学深圳市未来工业互联网安全保障重点实验室主任。研究兴趣包括信息物理系统安全与保障、物联网等。他是 IET 和 InstMC 的会士，是 IET 期刊《Cyber-Physical Systems Theory and Applications》的副编辑。

基于多视野感知的多智能体协同策略融合方法

王彬锐，杜永萍，张博超，李方昱，韩红桂

北京工业大学，北京，100124

摘　要：在船舶部件制造的仓储调度优化中，使用多智能体系统在复杂动态环境中进行协作与决策的优化是关键问题。传统的单一视野策略在应对复杂环境时常常表现不足。本文提出了基于多视野感知的多智能体协同控制策略融合方法，结合全局视野、局部视野和混合视野的信息，通过智能体间的直接通信机制，实现高效的信息共享和动态决策。智能体通过定期广播其位置和目标位置，邻近智能体接收并更新其局部视野，从而进行路径重新规划，避免冲突。本文设计并构建了多智能体交互环境，支持自定义的观测类型和视野距离下的多方验证，实验结果表明，本文提出的方法在智能体数量增多和视野范围扩大的情况下，能够显著减少智能体间的冲突次数，并保持较高的任务完成效率，相比单一的局部视野、全局视野和混合视野策略，具有明显优势。

关键词：多智能体协同；策略优化；强化学习；多视野融合

Multi-view perception and collaborative strategy fusion method for Multi-agent Spatial arrangement

Binrui Wang, Yongping Du, Bochao Zhang, Fangyu Li, Honggui Han

Beijing University of Technology, Beijing, 100124

Abstract: In the optimization of warehouse scheduling for ship component manufacturing, enhancing collaboration and decision-making in multi-agent systems within complex dynamic environments is a critical issue. Traditional single-view strategies fall short in handling such complexity. This paper proposes a multi-agent cooperative control strategy fusion method based on multi-view perception. By integrating information from global, local, and hybrid views, and leveraging direct communication mechanisms between agents, efficient information sharing and dynamic decision-making are achieved. Agents periodically broadcast their positions and target locations, which neighboring agents receive to update their local views, enabling path replanning and collision avoidance. We designed and constructed a multi-agent interaction environment that supports customizable observation types and view distances for comprehensive validation. Experimental results demonstrate that the proposed method significantly reduces collision occurrences and maintains high task completion efficiency as the number of agents and view ranges increase.

Key words: multi-agent cooperation; strategy fusion; multi-agent reinforcement learning; multi-view fusion

1. 引言

在工业制造领域，生产效率和资源优化是实现经济效益和竞争力的关键因素，其部件生产流程涉及复杂的部件制造、组装、存储和运输过程，需要精确协同和优化。传统的生产策略往往依赖于预先设定的规则和经验，在面对生产进度变化和紧急情况时缺乏灵活性和适应性[1]。船舶制造的调度策略优化涉及多环节和多决策点，属于多智能体系统（Multi-Agent Systems, MAS）的领域，涉及到多智能体之间的协调与合作以实现高效的生产流程和空间利用，其研究目标在于通过强化学习算法来优化船舶制造过程中的生产策略和部件存放空间。

多智能体系统（Multi-Agent Systems, MAS）研究分布式自主智能体如何协作以解决复杂问题[2][3]。智能体可以是软件代理、机器人或其他能够执行任务并做出独立决策的实体。MAS 的核心特性包括智能体的自主性、去中心化的决策制定，以及基于局部信息的智能体交互。在多智能体系统中，智能体之间即存在协作也存在竞争关系，旨在实现个体和整体的优化目标。MAS 研究和应用的主要挑战包括智能体之间的有效通信、行为协调、资源共享、冲突解决，以及在动态和部分可观测环境中的学习与适应[4]。MAS 在工业自动化领域可用于优化生产流程、物料搬运、质量监控和设备维护[5]；在智能交通系统中，MAS 有助于优化交通流量和减少拥堵；在智能电网中，MAS 用于优化电力分配和消耗[6]。

在 MAS 中，强化学习（Reinforcement Learning, RL）应用广泛，用于训练智能体通过与环境的交互学习最优策略，以最大化累积奖励。然而，多智能体环境的动态性和部分可观测性带来了额外挑战。为了解决以上挑战，研究人员开发了多种针对多智能体环境的强化学习算法，如多智能体深度 Q 学习（MA-DQN）和多智能体深度确定性策略梯度（MADDPG），旨在促进智能体之间的有效协作和学习。虽然使用基于强化学习的方法，智能体能够在多智能体环境中实现整体优化并完成共同目标，但如何构建让智能体间进行有效的协作和竞争，提升效率仍是巨大挑战。针对船舶制造中部件运输存放环境复杂的问题，本文提出一种基于强化学习的多视野分布式合作策略融合方法，主要工作如下：

- 本文提出了一种基于多视野感知的多智能体协同控制策略融合方法（Multi-View Distributed Cooperation Fusion Strategy，MVDCF）。通过融合全局视野、局部视野和混合视野的信息，增强了智能体在动态环境中的适应能力和决策准确性。
- 本文设计了基于直接通信的分布式优化与协作方法，智能体能够定期广播其位置和目标位置，邻近的智能体接收广播信息并更新其局部视野。该机制有效提高了多智能体系统的协作效率和任务完成质量。
- 基于 OpenAI Gym 库构建了基于船舶制造部件规划仓储的多智能体环境，并支持不同观测类型和视野距离的多视野策略训练。实验结果验证了在不同环境设置下，本文方法在减少智能体间碰撞次数和提高任务完成效率方面表现出显著优势。

2. 相关工作

多智能体系统由多个具有独立决策能力的智能体组成。智能体通过与相邻的智能体或环境进行交互来学习新的知识和动作，通过相互作用、沟通和协调进行决策以完成分配的任务。多智能体系统因智能体固有的学习和自主决策能力而具有很高的灵活性，因而能够用于解决计算机网络、船舶、电气和交通等多个领域的问题。多智能体系统中的强化学习通过与环境进行交互以学习策略，其核心思想是通过智能体在执行动作、观察环境反馈的状态和奖励的过程中，学习到最优策略，从而实现长期累积奖励的最大化。目前多智能体强化学习方法主要分为基于价值函数[7][8]、基于策略[9]以及基于演员-评论家（Act or-Critic）[10]的方法。

在智能电网领域，多智能体系统在能源管理、能量营销、定价、能量调度、可靠性和网络安全等方面显示出了重要应用价值。Binyamin 和 Slama[11]对多智能体系统在智能电网中的应用进行了全面分析，讨论了其在资源分配和调度方面的优势。Shobole[12]提出了一种基于多智能体系统的自适应保护技术，通过改进电网保护的通信可靠性来提高智能电网的稳定性。Li 等人[13]提出一种基于多智能体系统的两级分散协调控制方案来保证微电网的安全性和稳定性。交通管理领域，Mushtaq 等[14]提出了一种基于多智能体强

等[15]结合物联网技术的多智能体系统，利用无线传感器网络实现智能交通管理。在社交网络和网络安全领域，Meng 等[16]讨论了网络系统中的安全性和信任问题，对于理解和应对现代网络环境中的安全威胁提供了重要参考。Nie 等[17]研究了智能工厂中基于社交网络属性的多机器人系统，通过实时任务分配优化制造流程，提升了生产效率。Nezamoddini 等[18]研究者通过分析自适应多智能体网在智能城市中的应用，提出了一种基于 MASs 的方法，利用分布式计算平台来处理和管理系统中收集的大量数据。Kim [19] 等人提出了基于多智能体强化学习的方法，解决堆场时间和空间约束下的堆场位置确定问题。Huang [20] 等提出了基于深度时空-通道注意力神经网络的多智能体强化学习方法（MARL-DSTAN)，用于大规模交通网络中的交通信号配时。Roesch[21] 等提出了基于 PPO 的算法用于控制工厂内的能量交换，通过全局奖励与局部奖励相结合，鼓励智能体之间的协调。Calvo[22] 等使用独立的深度 Q 网络（independent deep Q-network, IDQN）解决异构多路口城市的交通控制问题，通过优化奖励函数减少累计等待时间。成旺磊等[23]提出了一种用于无人机−无人车异构编队的多智能体预设时间最优容错控制算法，实现同步最优控制和交互纳什均衡以优化策略的有效性。多机协同空战领域，施伟[24]等提出“集中式训练－分布式执行”的多机协同空战决策框架，改进了 PPO 算法，增强复杂空战场景下的实时决策能力。

3. 任务定义

本项研究旨在研发基于多智能体强化学习的系统，以优化船舶制造过程中的生产策略和部件存放空间。

生产策略优化任务：在船舶制造的生产策略优化方面，包括生产进度的动态调整，生产部件的顺序规划以及存放地点的决策优化任务。通过数据分析车间当前的生产线状态，包括工人、机器设备的利用率，以及材料的可用性，根据订单要求的交付截止日期，动态调整生产计划，以优化资源分配和降低延误风险；随后确定生产部件的最优顺序，以减少生产周期并提高效率。根据部件的尺寸、重量及对特定工序的依赖性决定最佳存放位置，以减少物流成本和提高存储效率。

形式化定义：

状态空间S_1：表示车间的生产线状态，包括工人利用率u_w，机器设备利用率u_m，材料可用性a_m，以及订单交付截至日期d_d，则有$S_1 = \{u_w, u_m, a_m. d_d\}$。

动作空间A_1：表示生产计划的调整，包括生产顺序O_p和资源分配r_a。有$A_1 = \{O_p, r_a\}$。

转移函数$T_1(s, a)$：表示在状态$s \in S_1$下采取动作$a \in A_1$时，系统状态的转变。

奖励函数$R_1(s, a)$：表示在状态s下采取动作a所获取的奖励，目标是减少延误并优化资源分配。

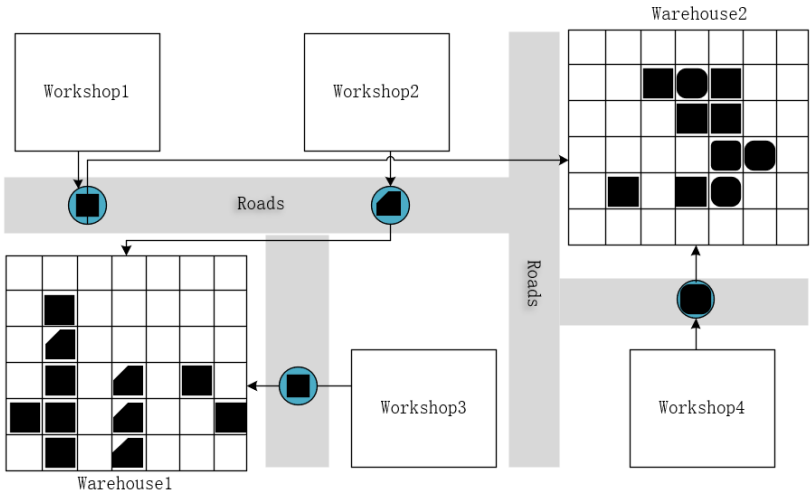


图 1. 船舶部件制造流程及仓储调度过程

部件仓储调度子优化任务：子优化任务关注于部件被生产后，到达指定存放位置的路径优化。首先设计多智能体协调机制，使多智能体之间（自动化搬运车辆，机器人）能够高效的合作，确保通信流畅，便于实时分享关键信息。随后，根据存储仓库的空间和工厂布局，以及生产状态计算船块部件的最优运输路径，避免交叉及拥堵，确保物流的顺畅和安全。最后，依据生产进度及车间生产的事实数据，动态调整部件的存放策略，优化存放位置来减少运输时间和提高存取效率。

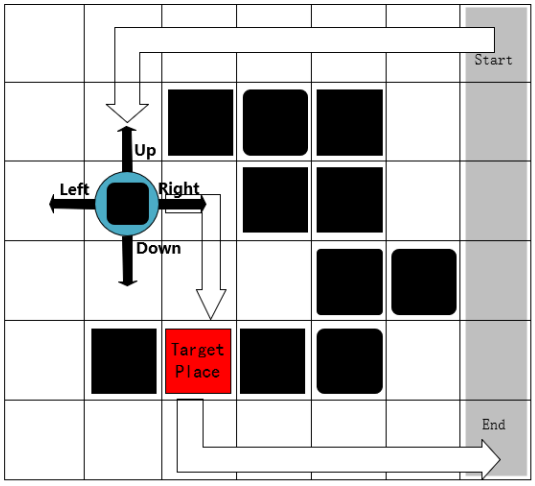


图 2 仓库智能体物流运输过程

形式化定义：

状态空间S_2：表示工厂的当前布局和生产状态，包括仓库布局l_w，车间布局l_f，和生产状态s_p。则有$S_2 = \{l_w, l_f, s_p\}$。

动作空间A_2^i：表示环境中单个智能体i的可以与环境交互的动作集合，有$A_2^i = \{a_1, a_2, \dots, a_n\}$。

转移函数$T_2(s, a)$：表示在状态$s \in S_2$下采取动作$a \in A_2$时，物流和存储状态的转变。

奖励函数$R_2(s, a)$：表示在状态s下采取动作a所获得的及时奖励值，其目标是优化运输路径和提高存储效率。

4. 多视野感知的多智能体协同策略融合方法

4.1 环境构建

本文基于 OpenAI gym 库构建强化学习模拟环境，实现了部件存储路径优化的智能体模拟环境。主要设计包括了智能体所处的交互环境，包括观察空间（observation space）及智能体的动作合集（action space），环境初始化条件以及环境的图形可视化展示。

4.2 算法优化

PPO 是一种基于策略梯度（on-policy）方法，旨在解决策略梯度优化中的两个主要问题：大幅度策略更新和样本效率低下。PPO 通过引入裁剪机制来限制策略更新的幅度，从而保持更新的稳定性。在策略梯度算法中，使用$\pi_\theta(a|s)$表示为参数化的策略函数，其中θ为策略参数，策略函数的目的是最大化智能体的期望奖励，表示为：

$$J(\theta) = \mathbb{E}_{\pi_\theta}\left[\sum_{i=1}^{n}\left[\sum_{t=0}^{\infty}\gamma^t R^i(s_t, a_t)\right]\right] \tag{1}$$

其中$R(s_t, a_t)$为状态s_t下，动作a_t所得到的第t步的奖励值，γ为折扣因子。PPO 引入了一种裁剪机制来

修改策略梯度的目标函数。该机制利用优势估计（Advantage estimate）的项$A^{\pi}(s,a)$以及裁剪参数ϵ。优势函数衡量执行特定动作相比于平均情况的优势，它的计算基于状态值函数$V(s)$和价值函数$Q(s,a)$，其定义为下：

$$A^{\pi}(s,a)=Q^{\pi}(s,a)-V^{\pi}(s) \tag{2}$$

$Q(s,a)$是执行动作a时的期望回报值，$V(s)$是在状态s下所有动作的期望回报的平均值，优势函数$A(s,a)$衡量了当前选择的执行动作相比于该状态下平均情况的期望奖励值。其中状态值函数在状态s和策略π下的计算可表示为：

$$V^{\pi}(s)=\mathbb{E}_{\pi}\left[\sum_{t=0}^{\infty}\gamma^{t}R^{i}(s_t,a_t,s_{t+1})|a_t\sim\pi(.|s_t),s_0=s\right] \tag{3}$$

在给定当前步执行动作a下，动作值函数$Q^{\pi}(s,a)$定义为：

$$Q^{\pi}(s,a)=\mathbb{E}_{\pi}\left[\sum_{t=0}^{\infty}\gamma^{t}R^{i}(s_t,a_t,s_{t+1})|a_t\sim\pi(.|s_t),s_0=s\,,a_0=a\right] \tag{4}$$

在给定的状态转换函数$T(s_{t+1}|s_t,a_t)$及奖励函数$R(s_t,a_t)$下，贝尔曼公式（Bellman equation）表明在任意时间步t时，状态值函数都满足：

$$V^{\pi}(s_t)=\sum_{a\in A(s_t)}\pi(a|s_t)\sum_{s'\in S}p(s'|s_t,a)[r(s_t,a)+\gamma V^{\pi}(s')] \tag{5}$$

通过对动作策略的奖励值最大化优化，最优化的状态值和最优策略可以从公式（6）得到：

$$V^{\pi^*}(s_t)=\max_{a}\sum_{s'\in S}p(s'|s_t,a)\left[r(s_t,a)+\gamma V^{\pi^*}(s')\right] \tag{6}$$

最优化动作值函数可以表示为：

$$Q^{\pi^*}(s_t,a_t)=\sum_{s'}p(s'|s_t,a)[r(s_t,a)+\gamma\max_{a'}Q^{\pi^*}(s',a')] \tag{7}$$

裁剪目标函数定义为：

$$L^{CLIP}(\theta)=E_{\pi\theta old}\left[min\left(r(\theta)A^{\pi_{\theta old}}(s,a),clip(r(\theta),1-\epsilon,1+\epsilon)A^{\pi_{\theta old}}(s,a)\right)\right] \tag{8}$$

其中：$r(\theta)=\frac{\pi_{\theta(a|s)}}{\pi_{\theta_{old}(a|s)}}$为新策略和旧策略之间的概率比。

PPO 的特点在于其能够在保持策略更新效率的同时，避免过大的策略变化，维持训练过程的稳定性。通过在目标函数中引入裁剪项，限制了策略更新的步幅，以防止由于过大的策略更新引起的训练不稳定性。

奖励函数设计：奖励函数设计对于多智能体在交互环境中的决策表现至关重要，合理的奖励函数设计不仅可以引导智能体高效的学习到最优解决策略，同时可以帮助智能体避免无效及有害的行为。本文设计奖励函数主要遵循一下原则：当智能体成功到达目标位置时，给予较高的正奖励；当智能体与其他智能体或障碍物发生冲突时，给予负奖励；当智能体保持不动或试图移动到不可到达的位置时，给予轻微的负奖励；每一步动作默认给予轻微的负奖励，以鼓励智能体尽快到达目标位置。设智能体i在第t步时，其动作a_t^i下的奖励函数表示为$R_t^i(Pos_t^i,a_t^i)$。

$$R_t^i(Pos_t^i,a_t^i)=\begin{cases}1000, & if\ Pos_t^i=Goal^i\\ -5, & if\ isBlock\left(Pos_t^i,obstacles\right)\\ -5, & if\ collision\left(Pos_t^i,Pos_t^j\right)(j\neq i)\\ -3, & if\ Pos_t^i=Pos_{t-1}^i\\ -1, & otherwise\end{cases} \tag{9}$$

其中，Pos_t^i表示智能体i在第t步时的位置，$Goal^i$表示第i个智能体的目标位置，

$isBlock\left(Pos_t^i, obstacles\right)$表示第$i$个智能体在位置$Pos_t^i$是否与障碍物发生冲突，$collision\left(Pos_t^i, Pos_t^j\right)(j \neq i)$表示第$i$个智能体在位置$Pos_t^i$是否与其他智能体发生冲突。

4.3 多视野策略融合优化方法

为提高多智能体协同效率和决策质量，结合中心决策的全局信息和分布式决策的局部信息，通过整合多个智能体视角，增强决策系统的动态适应性。定义全局决策层、局部决策层和综合决策层，针对不同需求和环境条件应用不同策略和信息流。

4.3.1 全局视野

全局决策层通过中心控制单元收集和分析数据，制定长期动作策略和优化目标，利用深度强化学习预测环境变化和调整策略，计算智能体的最优方案。全局视野的观测空间表示为 $\mathbf{O}_{\text{global}} \in R^{W\times H}$，全局视野表示为$\mathbf{O}_{\text{global}}$，则有：

$$\mathbf{O}_{\text{global}}[x,y] = \begin{cases} -1, & if(x,y) \in P_{block} \\ 2, & if(x,y) \in P_{target} \\ 1, & if(x,y) \in P_{block} \\ 0, & otherwise \end{cases} \tag{10}$$

4.3.2 局部视野

局部决策层由各智能体独立操作，处理视野范围内的局部信息，判断最优动作策略。智能体采取反应式进行避障和路径规划，根据实时反馈调整行为，应对动态变化的局部环境。观测空间为$\mathbf{O}_{\text{local}} \in R^{N\times(V\times V)}$，其中$V$为智能体的局部视野范围大小。局部观测表示为公式（11），其中$\boldsymbol{o}_{x,y}^i$的定义与$\mathbf{O}_{\text{global}}$相同。

$$\mathbf{O}_{\text{local}}^{\text{i}} = \left\{\boldsymbol{o}_{x,y}^i \middle| x \in \left[x_i - \frac{V}{2}, x_i + \frac{V}{2}\right], y \in \left[y_i - \frac{V}{2}, y_i + \frac{V}{2}\right]\right\} \tag{11}$$

4.3.3 混合视野

综合决策层作为全局和局部决策层的桥梁，协调整合信息和策略。中心处理单元与智能体共享关键信息，通过决策支持系统同步优化策略。综合决策层实现全局和局部视野的信息流动和策略快速迭代，支持全局智能体的整体目标。混合视野策略中智能体的观测空间为：$\mathbf{O}_{\text{combined}} \in R^{N\times(W\times H\times V\times V)}$，则混合观测视野表示为：

$$\mathbf{O}_{\text{combined}}^{\text{i}} = \mathbf{O}_{\text{global}} \cup \mathbf{O}_{\text{local}}^i \tag{12}$$

4.3.4 智能体间通信策略

基于直接通信的分布式优化与协作方法中，每个智能体定期广播其当前位置和目标位置，邻近智能体接收信息后更新局部视野以感知相互位置。这种信息交换机制为位置共享和目标共享策略。智能体在固定时间间隔内广播其坐标位置和目标位置，便于邻近智能体进行空间感知和决策，预判行动路径，实现高效路径规划和冲突避免。通信范围有限，以减少通信开销和提高系统可扩展性。智能体接收信息后按时间戳存储，确保基于最新环境感知进行决策，并映射邻近智能体位置和预判移动方向。更新后的局部视野帮助智能体进行冲突检测和路径重新规划，提高多智能体系统的协作效率和任务完成质量。

4.5 多视野策略融合

通过多视野观测空间下的多智能体进行训练，使用基于深度强化学习进行智能体路径规划的策略学习，并使用 PPO 算法进行优化。策略分别表示为：π_{global}，π_{local}及$\pi_{combined}$，分别表示全局视野、局部视野和混合视野下的策略，则有$\pi_{global}\left(a|\mathbf{O}_{\text{global}}\right)$，$\pi_{local}\left(a^i|\mathbf{O}_{\text{local}}^i\right)$，$\pi_{combined}\left(a^i|\mathbf{O}_{\text{combined}}^i\right)$。

策略融合阶段，通过使用加权平均方法将多策略模型的输出融合，融合策略表示为π_{fused}，其输出为

各策略的加权平均。设策略的数量为K，每个策略所对应的权重为γ，则融合策略由公式（13）表示，其中$\sum_{k=1}^{K}\gamma_k = 1$。

$$\pi_{fused}(a^i|O^i) = \sum_{k=1}^{K}\gamma_k\pi_k(a^i|O^i) \tag{13}$$

5. 实验结果

5.1 实验设置

本实验基于 OpenAI Gym 自定义的多智能体环境，采用 10x10 网格，包含随机生成的障碍物和 n 个智能体，初始位置和目标位置随机生成。使用 PPO 算法训练，余弦退火学习率函数，初始学习率 1e-3，裁剪范围 clip_range 为 0.2，优化器为 RMSprop，参数 eps 为 1e-4。

5.2 实验结果：

5.2.1 多视野模型训练

为验证多视野策略融合方法的有效性，我们在不同智能体数量及不同视野距离下分别进行多视野策略的训练，如图 3 为四智能体三视野距离下的平均奖励值和平均步长变化，实验结果表明该环境设置下，仅使用局部视野的多智能体优化比依靠全局视野和混合视野的模型效果更好，具有更高的平均奖励值和更低的平均步长，说明多智能体可以在较少的动作步数下，获得更高的奖励值，完成优化总目标。

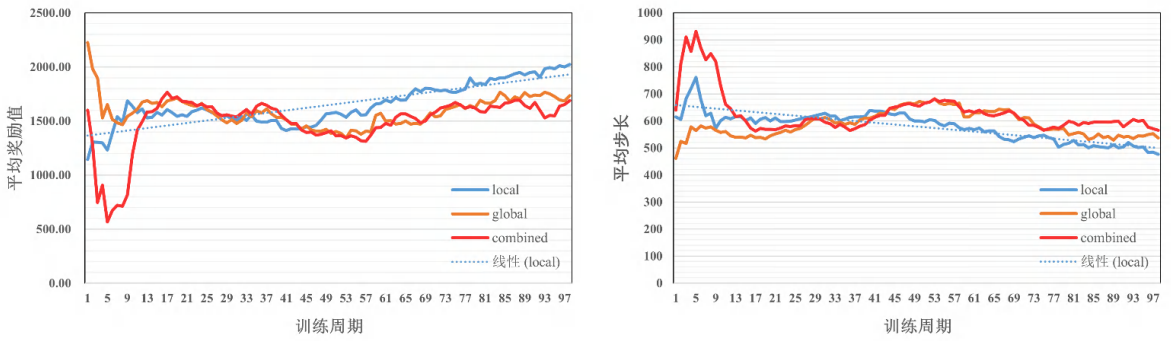


图 3 四智能体三视野距离下平均奖励及平均步长

如图 4 所示为四智能体在五视野范围内的平均奖励及步长变化曲线，实验结果表明在智能体视野范围增大后，仅依赖局部视野进行路径搜索的性能降低，伴随着平均奖励值的降低及步长的增加。局部视野的增加使得模型需要处理的局部信息增多，导致决策的效率下降。此外，可以观察到视野范围扩大的情况下，混合视野策略的性能优于仅使用局部视野及全局视野的策略。这是因为混合策略能够在局部视野的基础上结合全局信息，使智能体可以在复杂环境时具备更强的全局感知能力，从而提高决策的准确性和效率,同时混合视野策略的平均奖励值较高，步长较低，表明其在较短时间内能够获得更多的奖励。

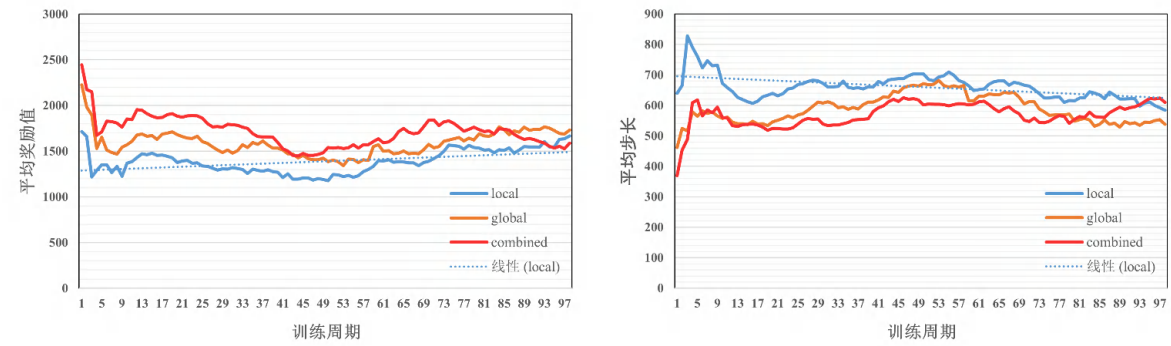


图 4 四智能体五视野距离下平均奖励及平均步长

如图 5 所示为三智能体三视野距离下的平均奖励值和平均步长变化，实验结果表明仅使用局部视野的多智能体优化在训练周期内表现出较高的平均奖励值和较低的平均步长，但基于全局视野的策略在第 85 个训练周期略高于局部策略和混合策略。随着训练步长的增加，全局视野策略能够捕捉到整个环境的全面信息以更好地适应环境变化。然而，局部视野策略由于其关注点集中在智能体周围的局部信息，在大多数情况下能够更快速地做出有效的决策，从而提高效率。

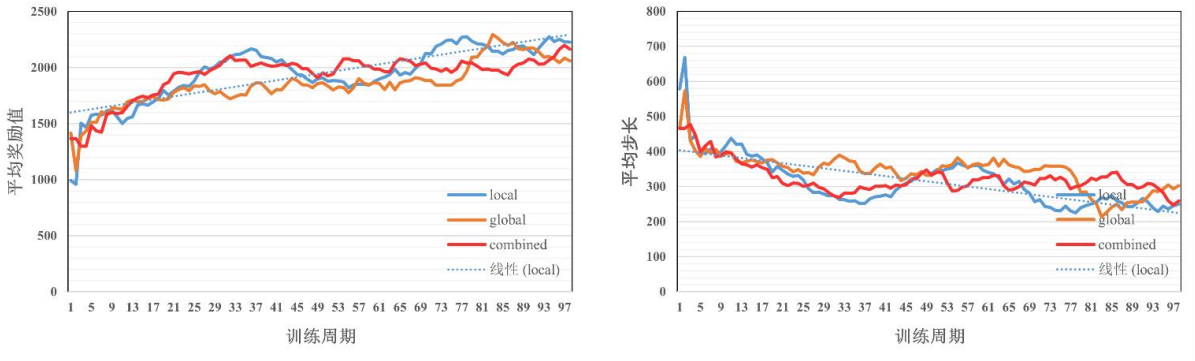


图 5 三智能体三视野距离下平均奖励及平均步长

如图 6 所示，随着智能体局部视野的增加，基于局部视野和混合策略的模型表现有所下降，此时全局视野策略可以更好的适应环境的变化。同时混合视野策略在结合全局和局部信息后，可以结合其优点在不同的环境设置下保持一定的稳定性，具有更强的鲁棒性。

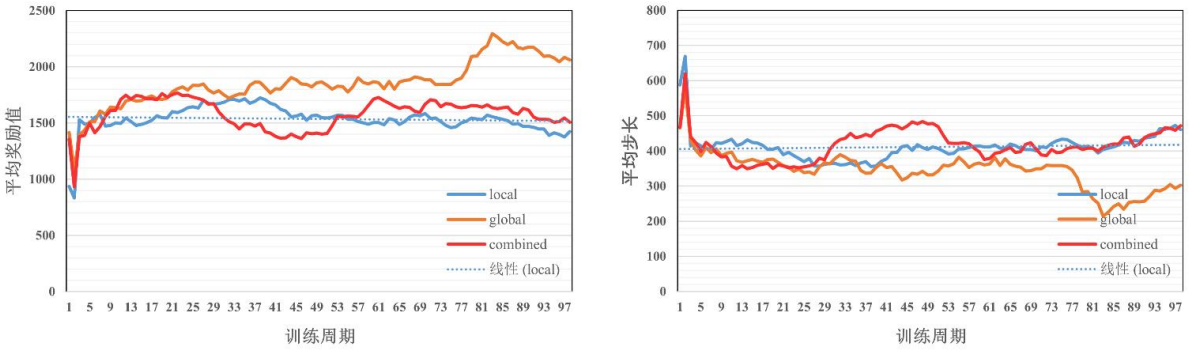


图 6 三智能体五视野距离下平均奖励及平均步长

5.2.2 冲突次数评估

为了评估多视野策略融合方法的有效性，通过对不同策略下的模型进行测试，使用在相同测试环境下的智能体平均冲突次数及成功完成目标的平均步长进行评估。如图 7 所示为不同测试环境下，多种策略模型中智能体平均冲突次数及 MVDCF 融合模型分别与局部，全局及混合策略的冲突差值。实验结果表明，在智能体数量为 4 的情况下，随着视野变大智能体的平均冲突逐渐增多。其中，仅依靠局部视野策略的冲突次数最多，MVDCF 策略下的智能体间发生冲突次数最少，相对于局部策略更具有优势。同时，在智能体数量为 3 的情况下，随着视野的增加，平均冲突次数在局部视野策略下有所减少。这是因为智能体减少降低了环境复杂度，更大的视野范围可以帮助智能体更好地判断其他智能体的位置，降低冲突概率。此环境下 MVDCF 策略的平均冲突次更少，表明多视野分布式协同融合策略下具有更好的性能，与全局视野策略相比，表现出显著优势。

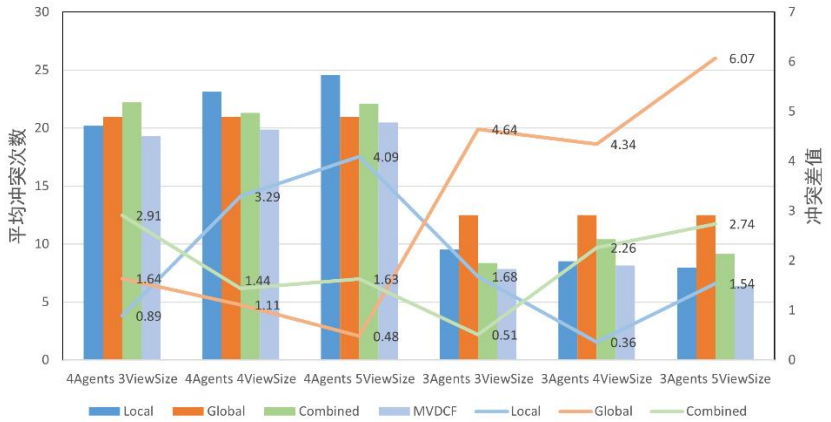


图 7 平均冲突测试及冲突差值结果

如图 8 为不同环境下不同策略的平均完成步长，步长越低说明智能体完成全部任务所需要的动作次数越少，策略更加高效。实验结果表明在不同环境下，不同策略的平均完成步长有显著差异。智能体数量和视野范围对策略效率影响明显。在 4 智能体环境下，随着视野增加，局部视野策略需要更多动作完成任务，混合视野策略的步长也有所增加。MVDCF 策略在增加视野范围时仍保持较高效率，步长变化较小。在 3 智能体环境中，MVDCF 策略在小视野范围内表现出高效性，随着视野范围增加，其步长增长幅度最小，显示出其在不同环境下的适应性和高效性。

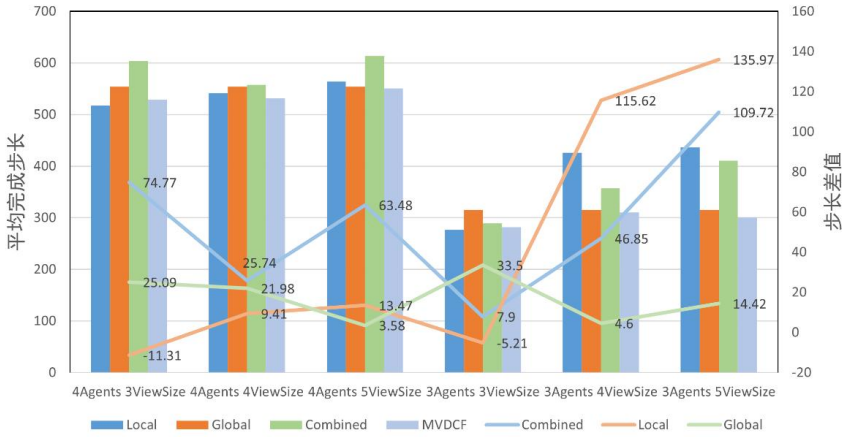


图 8 平均完成步长及差值结果

5. 结论

本文研究了基于多视野感知的多智能体协同控制策略融合方法，提出了一种结合全局视野、局部视野和混合视野的信息融合策略 MVDCF。通过智能体间直接通信实现高效信息共享和动态决策的方法，设计并实现了支持自定义观测类型和视野距离的多智能体交互环境进行验证。该策略在多视野融合中表现出显著的优势，尤其是在智能体数量增多和视野范围扩大的情况下，能够显著减少智能体间的冲突次数，并保持较高的任务完成效率。通过对比不同策略的冲突次数和平均完成步长，我们发现，尽管局部视野策略在特定情况下表现良好，但在复杂环境中，MVDCF 策略由于其综合了局部和全局视野的信息，能够在减少冲突次数和提高任务完成效率方面表现得更稳定。智能体间的直接通信机制通过位置共享和目标共享的策略，显著提高了多智能体系统的协作效率和任务完成质量。智能体通过广播其位置和目标位置，使得邻近智能体能够及时获取最新信息，动态更新其局部视野，从而进行路径重新规划，避免冲突。该机制在复杂

系统中具有一定的应用前景，能够提高系统的灵活性和适应性，提升生产效率和资源利用率。未来的研究将进一步优化通信协议和分布式算法，探索更加多样化的应用场景，同时实现多层级的策略优化方法，推动多智能体系统在船舶制造领域的广泛应用。

参考文献

[1] Esteso A, Peidro D, Mula J, et al. Reinforcement learning applied to production planning and control[J]. International Journal of Production Research, 2023, 61(16): 5772-5789.

[2] Yan Y, Chow A H F, Ho C P, et al. Reinforcement learning for logistics and supply chain management: Methodologies, state of the art, and future opportunities[J]. Transportation Research Part E: Logistics and Transportation Review, 2022, 162: 102712.

[3] Li C, Zheng P, Yin Y, et al. Deep reinforcement learning in smart manufacturing: A review and prospects[J]. CIRP Journal of Manufacturing Science and Technology, 2023, 40: 75-101.

[4] Kanishka K, Acherjee B. Revolutionizing manufacturing: A comprehensive overview of additive manufacturing processes, materials, developments, and challenges[J]. Journal of Manufacturing Processes, 2023, 107: 574-619.

[5] Zhang H, Wang W, Zhang S, et al. A novel method based on deep reinforcement learning for machining process route planning[J]. Robotics and Computer-Integrated Manufacturing, 2024, 86: 102688.

[6] Zhou Z, Liu G, Tang Y. Multi-agent reinforcement learning: Methods, applications, visionary prospects, and challenges[J]. arXiv preprint arXiv:2305.10091, 2023.

[7] KRÖSE B J A. Learning from delayed rewards[J]. Robotics and autonomous systems, 1995, 15(4): 233-235.

[8] Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., ... and Petersen, S. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529-533.

[9] Schulman, J., Wolski, F., Dhariwal, P., Radford, A., Klimov, O.: Proximal policy optimization algorithms. arXiv preprint arXiv:1707.06347 (2017)

[10] Lillicrap T P, Hunt J J, Pritzel A, et al. Continuous control with deep reinforcement learning[J]. arXiv preprint arXiv:1509.02971, 2015.

[11] Binyamin S S, Ben Slama S. Multi-agent Systems for Resource Allocation and Scheduling in a smart grid[J]. Sensors, 2022, 22(21): 8099.

[12] Shobole A A. Multi-agent systems based adaptive protection for smart distribution network[J]. Electric Power Components and Systems, 2022, 49(18-19): 1432-1444.

[13] Li Zhe, Yan Ting, Dou Chunxia. Stability control strategy of microgrid based on multi-agent system[J]. Science Technology and Engineering, 2024, 24(11): 4527-4538.

[14] Mushtaq A, Haq I U, Sarwar M A, et al. Multi-agent reinforcement learning for traffic flow management of autonomous vehicles[J]. Sensors, 2023, 23(5): 2373.

[15] Kumar G R, Latha S B, Shaker Reddy P C, et al. Multi-agent Iot-based System for Intelligent Vehicle Traffic Management Using Wireless Sensor Networks[J]. Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering), 2024, 17(5): 515-522.

[16] Meng W, Katsikas S K, Chen J, et al. Editorial for special issue on security and trust on networked systems[J]. International Journal of Network Management, 2023, 33(3).

[17] Nie Z, Chen K C, Alanezi Y. Socially Networked Multi-Robot System of Time-Sensitive Multi-Link Access in a Smart Factory[C]//ICC 2023-IEEE International Conference on Communications. IEEE, 2023: 4918-4923.

[18] Nezamoddini N, Gholami A. A survey of adaptive multi-agent networks and their applications in smart cities[J]. Smart Cities, 2022, 5(1): 318-347.

[19] Byeongseop Kim, Yongkuk Jeong & Jong Gye Shin (2020) , Spatial arrangement using deep reinforcement learning to minimise rearrangement in shipblock stockyards, International Journal of Production Research, 58:16, 5062-5076, DOI: 10.1080/00207543.2020.1748247.

[20] Huang H, Hu Z, Lu Z, et al. Network-scale traffic signal control via multiagent reinforcement learning with deep spatiotemporal attentive network. IEEE Transactions on Cybernetics, 2023, 53(1): 262-274.

[21] Roesch, M.; Linder, C.; Zimmermann, R.; Rudolf, A.; Hohmann, A.; Reinhart, G. Smart Grid for Industry Using Multi-Agent Reinforcement Learning. Appl. Sci. 2020, 10, 6900.

[22] Calvo, A.; Dusparic, I. Heterogeneous Multi-Agent Deep Reinforcement Learning for Traffic Lights Control. In Proceedings of the 26th Irish Conference on Artificial Intelligence and Cognitive Science, Dublin, Ireland, 6–7 December 2018.

[23] 成旺磊，张柯，姜斌. 基于层级结构的空−地协同预设时间最优容错控制. 自动化学报, 2024, 50(8): 1−12 doi: 10.16383/j.aas.c230699

[24] 施伟，冯旸赫，程光权，黄红蓝，黄金才，刘忠，贺威. 基于深度强化学习的多机协同空战方法研究. 自动化学报，2021，47(7): 1610−1623 doi: 10.16383/j.aas.c201059

[作者简介]

王彬锐（1997-），男，博士生，主要研究领域为强化学习与多智能体协同。

张博超（1999-），男，硕士生，主要研究领域为多智能体路径规划与智能信息处理。

韩红桂（1983-），男，博士，教授，博士生导师，研究领域为复杂系统智能优化控制研究。

杜永萍（1977-），女，博士，教授，博士生导师，主要研究领域为信息抽取和智能信息处理

李方昱（1985-），男，博士，教授，博士生导师，研究领域为智能感知与智能建模研究；

Relay Selection for Multi-Source Cooperation in Wireless Powered Industrial Sensor Networks

Min Li, Qinqin Xiong, Yong Ku, Heng Wang

***Abstract*—Wireless powered communication (WPC) with cooperative relaying is a promising strategy to improve reliability and energy efficiency in industrial wireless sensor networks (IWSNs), particularly the use of a combination of WPC with multi-relay technologies. This paper considers a multi-source wireless powered IWSN with beacon transfer in the downlink and cooperative information transmissions in the uplink, where the energy harvesting sources harvest energy and receive information simultaneously from the beacon power and volunteer to serve as relays whenever they have enough harvested energy for cooperation. In such multi-relay scenarios, conventional schemes select the relay with the "best" characteristics in energy or in channel quality as the only best relay in considered networks, which would be not valid when multiple sources are present, where the only best relay's energy highly likely to get drained in frequently cooperation. The key contribution of this paper is that a cooperation protocol with multiple best relays is proposed. It addresses the "energy drain" problem and is easy to implement in practical IWSNs. Besides, to reduce the possible conflicts in relay selection and further improve the achievable performance, two selection algorithms stand from separately source perspective and relay perspective are studied for the centralized scenarios, and a distributed competition algorithm is developed for the distributed scenarios. Simulation results demonstrate the performance of the provided schemes.**

***Index Terms*—Industrial wireless sensor networks, wireless powered communication, cooperative communication, relay selection.**

I. Introduction

Industrial Internet of Things (IIoT) has been widely investigated as the extension of IoT in industry [1], [2]. Industrial wireless sensor networks (IWSNs) are the infrastructure for the realization of IIoT, in which hundreds of sensor nodes collect different processing data and then transmit the data wirelessly to a sink node for analysis. However, two challenging problems are faced before implementing massive IWSNs deployment. One is the energy constraint of sensor nodes, which are typically powered by batteries with limited operation life, whereas replacing or recharging the batteries is often impractical or costly, particularly in hostile environments. Another is the communication reliability caused by signal fading in wireless transmission process. Therefore, designing reliable and energy-efficient communication strategy holds great importance for such networks.

The authors are with the Key Laboratory of Industrial Internet of Things and Networked Control, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: limin@cqupt.edu.cn; xiongqq7@qq.com; 1355447958@qq.com; wangheng@cqupt.edu.cn). (*Corresponding author: Heng Wang.*)

This work was supported by the National Natural Science Foundation of China under Grant 92267106 and Grant U23B2003.

Energy harvesting (EH) scavenging energy from surrounding environment has been recognized as a sustainable solution to prolong the lifetime of wireless nodes [3]. In particular, radio frequency energy harvesting (RFEH) technique is rather attractive since compared to conventional energy sources (*e.g.*, solar and wind), RF signals have the advantage of carrying information and energy at the same time, which enables wireless nodes to receive information as well as harvesting energy from RF signals broadcast in communication networks. This technique has opened a new research field, termed wireless-powered communication (WPC). Specifically, two hot research paradigms can be classified in WPC: simultaneous wireless information and power transfer (SWIPT) [4] and wireless powered communication networks (WPCNs) [5]–[7]. In SWIPT systems, the wireless nodes receive information and energy simultaneously from a RF signal. In WPCN systems, the wireless nodes first harvest energy from a dedicated RF transmitter (usually is a hybrid access point) and then transmit independent information using the harvested energy, which is referred to as "harvest-then-transmit" [7].

On the other hand, cooperative communication using relays promises significant improvements in transmission reliability. By assigning one or more relays to forward signals received from a source to the destination, spatial diversity is achieved [8]–[10]. Recently, the concept of WPC with cooperative relaying has gained much attention, which is demonstrated to be an effective strategy to achieve gains in both reliability and energy efficient in wireless networks [11]–[14]. This concept was initially proposed in [11] for simple three-node SWIPT systems consisting of one source-destination pair and one EH relay. The extensions to multi-user WPCNs, single-input-multiple-output (SIMO) systems and multiple-input multiple-output (MIMO) systems were investigated in [12] and [13], respectively. Also, the combination of this concept with multi-relay technologies were studied in plenty of recent works [14].

It has previously been established that multiple additional relays, if exist, can be used to provide further improvement in achievable reliability by exploiting more diversity gains. When multiple relays are present, single relay selection strategy which selects the "best" relay to perform information forwarding, is of practical interest because it avoids tight synchronization among separated relays compared to multi-relaying and reduces the network overhead [15]. Several relay selection schemes based on different "best" criteria were investigated in multi-relay WPC networks [16]–[19]. In [16], the popular opportunistic relaying (OR) and partial relay selection (PRS) schemes, based on the channel state information (CSI) comparisons, were applied in a WPCN with one source-destination pair. In OR scheme,

the best relay is the one with the highest instantaneous channel value to both source and destination. And in PRS scheme, the relay between sources and the destination having the maximum channel to one of the two hops becomes the best. An energy-based selection scheme, according to the harvested energy at relays, was developed in [17] for a SWIPT system. Inspired by the OR and energy-based ideas, a new selection rule takes into account both CSI and energy status have been studied in [18] and [19], in which the relays that harvested energy exceeding a certain threshold form a set firstly, and then the one with the highest end-to-end channel in the set is selected out as the best relay. This scheme was proved to improve outage performance compared to that of merely energy-based.

The CSI or energy threshold based relay selection schemes have been widely adopted in multi-relay WPC networks. However, the previously schemes were largely focused on the scenarios with single source, where all relays serve for it. When more sources join in the transmission, we find these schemes would not perform well. In single source scenarios, the "best" relay may use up all its harvested energy to forward the source information. In multi-source scenarios, with the task of serving all sources, some power (energy) allocation strategy should be made carefully at the "best" relay. Whatever strategy it made, an inevitable fact is that the more often the node is selected as the best relay, the sooner its harvested energy drains out. Once the harvested energy drains out, it can no longer participate in cooperative transmission, which will result in the termination of cooperation. This *energy drain* is particularly serious when the network with large size or the channels between sources and the destination are poor.

Inspired by the performance benefits of using multi-relay WPC, this paper considers the application of this strategy in IWSNs where multiple sources communicate with a common destination, and focuses on the challenging problem of energy drain. Note that although the "best" relay may be constrained by limited energy, the other relays in the system potentially remain a large amount of unused energy. Then, an interesting solution is raised: If the best relay candidates for each source can be extended from one single node to a group of nodes, more energy at relays could be utilized and the energy drain problem will be avoided accordingly. Fortunately, such multi-best-relay idea was proved to be achievable as reflected in [20], which combined the selection cooperation protocol with feedback mechanism adequately, not only achieves the optimal diversity-multiplexing tradeoff, but also enlarges the best relay candidates to a set of nodes. The key idea behind it is to select any relay that correctly decoded the information from the source and the feedback frame from the destination.

Motivated by this, in this paper, we apply selection cooperation to multi-source wireless powered IWSNs. The main contributions are summarized as follows:

1) A transmission protocol based on selection cooperation with effective utilization of feedbacks is developed. Compared to the existing schemes (*e.g.*, [16]–[19]), the proposed protocol has three important characteristics. Firstly, it avoids the energy drain problem in multi-source scenarios by providing several available candidates of the best relay for each source, and hence achieves significant improvement in transmission reliability. Secondly, the approach of source-based relaying without requiring introducing additional relays will reduce the network overhead while remaining the benefits of multi-relay. Thirdly, unlike the prior works in which wireless information transmission occurs merely in the uplink (UL), the downlink (DL) beacon (a message used in IWSNs to synchronize the network nodes and describe the structure of transmission superframes [21]) transfer is taken into consideration explicitly, which makes the protocol easy to implement in practical IWSNs.

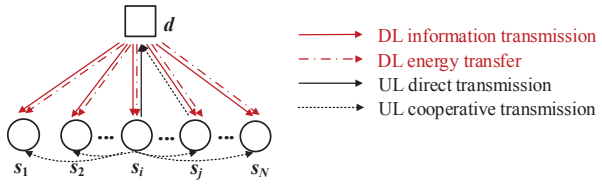


Fig. 1. A wireless powered IWSN model with energy and information transmissions in the DL and cooperative information transmissions in the UL.

2) To further reduce to the possible conflicts in relay selection among sources, three best relay selection algorithms are investigated. Specifically, for the centralized networks, we propose a source-based selection algorithm and a relay-based selection algorithm, where both exhibit reduced complexity compared to the exhaustive search method with factorial complexity. For the distributed networks, we present a distributed competition algorithm, which shows the lowest complexity, albeit at a price of a relatively worse conflict-avoid result.

3) The outage probability performance achieved by the proposed three relay selection algorithms are demonstrated by numerical simulations. The simulation results show that any of the proposed algorithm outperforms the OR scheme [16]. Also, the impacts of the system parameters including source number, source-source channel quality and source-destination distance, on the performance are extensively investigated.

This paper is structured as follows. Section II introduces the multi-source cooperative wireless powered IWSN model. In Section III, the selection cooperation protocol with WPC is investigated. In Section IV, the relay selection algorithms for centralized and distributed scenarios are studied. Simulation results are presented in Section V, and are followed by the conclusion in Section VI.

II. System Model

We consider a general IWSN with beacon transmission in the DL and cooperative information transmissions in the UL, as shown in Fig. 1. The network consists of N source nodes s_1, s_2, $\ldots$, s_N, and one destination node d, where all are equipped with one single antenna and operate in a half-duplex mode. Since no additional relay nodes exist in the system, we emphasize that each source acts as the potential relay for the other $N-1$ sources, *i.e.*, each source plays two equal roles, source and relay. Note that this is a stepping stone to the algorithms presented in Section IV. The destination is assumed to have stable energy supply, while sources operate with limited battery power. In order to prolong the battery life, in each

transmission superframe (also referred to transmission block), the energy constrained sources first decode information and harvest energy simultaneously from the beacon signal broadcast by the destination in the DL using power splitting (PS) strategy, which splits the received signal into two power streams for separate information receiving and energy receiving via a power manage circuit [11], and then use the harvested energy to transmit information in the UL. It is assumed that the power required for operating circuits is supplied by the energy stored in battery, instead of the harvested energy [22]. For the purpose of exploration, we follow most of current works on WPC (*e.g.* [7], [16]) and further assume that the energy harvested from the current transmission superframe cannot be accumulated for future use, so if there is any energy left after sources delivering their own information, they are willing to use up the remaining energy to help forwarding information overheard from others. It is noteworthy that considering energy storage would lead to a more practical framework [18], although this strategy is beyond the scope of this paper. As in most existing IWSNs, such as WirelessHART and ISA100.11a, the UL transmissions are performed in a Time Division Multiple Access (TDMA) fashion, which assigns each source the dedicated direct transmission slot and the possible retransmission slot. Moreover, we assume network-wide synchronization is maintained.

The distances between d and s_i, s_i and s_j are denoted by L_{d,s_i} and L_{s_i,s_j}, respectively. We use $h_{X,Y}$ to denote the channel from X to Y with $X, Y \in \{s_i, s_j, d\}$. As presented in [23], Rayleigh fading model has been widely used in practical industrial environment. We assume that the channels between each pair of nodes are modeled as independent Rayleigh fading with variance $1/\lambda_{X,Y}$. All channels are reciprocal and long-term static, *i.e.*, $h_{X,Y} = h_{Y,X}$, and the channel gain $\widetilde{h}_{X,Y} = |h_{X,Y}|^2$ remains constant during a superframe, which is in line with the prior research in this field [7], [12], [15].

The communications among sources and the destination are target at a rate R and corrupted by additive white Gaussian noise (AWGN) with variance σ^2. We use outage probability as the figure of merit to compare various relay selection algorithms. Specifically, we focus on the UL node outage, which counts the outage events in the UL transmissions node by node. The outage event is referred as the event that the mutual information I for a source-destination pair falls below the transmission rate R [24], [25]. When s_i distributes its own information to the destination in the assigned direct transmission slot, the mutual information between s_i and d is $I_{direct} = \log(1 + |h_{s_i,d}|^2 \frac{P_i}{\sigma^2}) = \log(1 + |h_{s_i,d}|^2 \rho_i)$, where P_i and ρ_i are s_i's transmission power and the non-faded signal-to-noise rate (SNR) at the destination, respectively. According to [20], if this direct transmission fails and s_j as relay forwards the information in s_i's retransmission slot under decode-and-forward mode with feedback, the mutual information between s_j and d is $I_c = \log(1 + |h_{s_j,d}|^2 \rho_j)$.

III. Protocol Description

In most existing WPC protocols with multi-relay, the relay with the “best” characteristics (in energy or channel quality) is usually selected as the unique best relay in considered networks. Our protocol differs from the conventional ones in that a set of available best relays will be formed for each source.

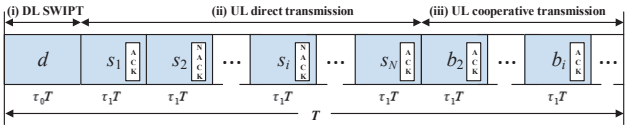


Fig. 2. The communication process of the protocol in a superframe.

We consider the communication in superframes of time duration T, where each superframe is composed of three phases, (i) DL SWIPT, (ii) UL direct transmission and (iii) UL cooperative transmission, as shown in Fig. 2. In phase i, the destination broadcasts a beacon signal in the DL for a time duration $\tau_0 T (0 < \tau_0 < 1)$, while all the sources decode information and harvest energy simultaneously from the signal. In phase ii, s_1, s_2, ..., s_N take turn to transmit information to the destination in the UL using the harvested energy, during the first N time slots where each slot accounts equally $\tau_1 T (0 < \tau_1 < 1)$ amount of time. At the end of each slot, the destination feeds back ACK/NACK frames indicating the decoding result of the current information. If decoding correctly, it returns an ACK frame and the transmission of current information finishes. Otherwise, a NACK frame it replies and cooperative retransmission is needed. In this case, a group of available best relays which is named active set $A(s)$ will be formed in the current slot for the source's information forwarding. The details for active set formation will be provided later. In phase iii, the sources who get a NACK frame from the destination sequentially select one best relay from their active sets to perform cooperative retransmission in the subsequent time slots. For the sake of presentation simplicity, the selected best relay is renamed as b, *i.e.*, if s_j is selected as the best relay of s_i, it is renamed as b_i. Specifically, for the source s_i, the activity in a superframe is as follows.

(1) In phase i, s_i decodes information and harvests energy simultaneously from the beacon signal using PS approach, as well as performing channel estimate based on the signal. Let γ_i denote the power splitting factor, *i.e.*, γ_i is the fraction of signal used for energy harvesting. The received information at s_i is given by

$$y_{s_i,d} = \frac{\sqrt{(1-\gamma_i)P} h_{d,s_i} x}{\sqrt{L_{d,s_i}}} + n \tag{1}$$

where P is the transmission power at the destination, x is the destination signal having normalized power, and n is the AWGN with unit variance. Because the beacon signal contains important information, such as synchronization and time slot allocation, it is assumed that the received beacon power will firstly be used to the information decoding circuit, and then to the energy harvesting circuit if there is any power left after successful decoding [22]. By setting the data rate supported by the i-th source-to-destination channel $R_{s_i,d} = R$, where $R_{s_i,d} = \log(1 + \frac{(1-\gamma_i)P}{L_{d,s_i}} |h_{d,s_i}|^2)$, we get the optimal γ_i is

$$\gamma_i^* = \max\{1 - \frac{\left(2^R - 1\right) L_{s_i,d}}{P|h_{d,s_i}|^2}, 0\} \tag{2}$$

$\gamma_i = 0$ denotes that all the received power is directed to the information decoding circuit and no power left for energy harvesting, due to the poor channel condition between s_i and the destination. With ignoring the energy harvested from the noise, we get the amount of energy obtained at s_i in phase i as

$$E_i = \frac{\eta|h_{d,s_i}|^2 P\gamma_i^*}{L_{s_i,d}}\tau_0 T \tag{3}$$

where $\eta \in (0,1)$ is the energy harvesting efficiency coefficient.

At the end of phase i, according to the obtained receiver side CSI, s_i computes the lowest energy required to transmit its information reliably in the UL, denoted as $E_{i,req}$:

$$E_{i,req} = \frac{\left(2^R - 1\right) L_{s_i,d}}{|h_{d,s_i}|^2}\tau_1 T \tag{4}$$

(2) In phase ii, s_i performs the following operations in the i-th time slot depending on the values of E_i and $E_{i,req}$. There are four cases as follows.

- When $E_i = 0$, s_i cannot transmit information. The system declares an outage event since no energy can transmit data.
- When $0 < E_i < E_{i,req}$, s_i broadcasts its information with energy E_i to strive for chances to be overheard. From the decoding set $D(s_i)$, which contains the sources that successfully decoded the information from s_i, the ones which also correctly decoded the NACK frame sent by the destination at the end of the i-th slot form another active set $A(s_i)$. Any member in $A(s_i)$ is eligible to be the best relay to perform cooperative retransmission. In other words, $A(s_i)$ is the set of the best relays available for s_i.
- When $E_{i,req} < E_i < 2E_{i,req}$, s_i delivers information using full energy E_i.
- When $E_i \geq 2E_{i,req}$, under the assumption that all packets are of the same size, the energy is sufficient to support at least twice reliable transmissions. In this case, s_i distributes its information with energy $E_{i,req}$. The remaining energy $E_i - E_{i,req}$ is reserved for forwarding information overheard from other sources in phase iii. We denote the maximum number of times that the remaining energy can support cooperation action as $m_i = \lfloor E_i/E_{i,req} \rfloor - 1$.

In the j-th $(0 < j \leq N, j \neq i)$ time slot of phase ii, if $E_i \geq 2E_{i,req}$, s_i volunteers to serve as a relay and overhears information from s_j. Once s_i decodes successfully, it becomes a member of s_j's best relays. At the end of phase ii, s_i counts the number of times acted as the best relay. We denote the times by $k_i (0 \leq k_i < N)$.

(3) In phase iii, if s_i's information has not been correctly decoded by the destination, the best relay b_i is selected from $A(s_i)$ to forward its information in the assigned retransmission time slot, where the details of best relay selection schemes will be discussed below in Section IV. Once $A(s_i)$ is empty, an outage event occurs.

Compared to the existing WPC protocols with multi-relay, the most important characteristic of the proposed protocol is that it provides several candidates of the best relay to sources. Hence, the competition for best relay among sources will be weakened, and the energy drain problem of the best relay will be avoided or mitigated, and, thus leads to significantly improvement in transmission reliability. Besides, the approach of source-based relaying reduces the network overhead because additional relays are no longer needed to deploy dedicately. Furthermore, by ultilizing the SWIPT technique in the DL, the DL beacon message transmission is considered explicitly and utilized adequately, which indicates that the protocol is easy to be implemented in practical IWSNs, such as IEEE 802.15.4 networks. Finally, with the consideration that any relay performs information forwarding at the lowest required energy rather than full harvested energy like [16], the protocol also improves the relay utilization efficiency because one relay is highly likely to assist several sources whenever it has sufficient energy.

IV. Best Relay Selection Algorithms

In this section, we focus on the design of best relay selection algorithms for centralized and distributed versions of the network. The centralized network is governed by a central unit (CU) with global CSI. The CU makes all best relay assignment decisions. When without a CU inside, the network is distributed and decisions are made by sources themselves, with local information regarding the network.

Before describing the algorithms, we first recall that all source nodes in the system play the dual role of source and relay. For presentation clearly, we in the following use the notation r_i for a relay to highlight the role, whereas in fact $s_i = r_i$. From a perspective of source, each source s_i $(0 < E_i < E_{i,req})$ that failed in direct transmission needs one best relay from $A(s_i)$ to perform cooperative retransmission. The number of available best relays, $|A(s_i)|$, determines the chances it can be assisted. From a perspective of relay, each relay r_i $(E_i \geq 2E_{i,req})$ with $k_i \geq 1$ is able to forward the information of the source for which it was chosen as a best relay. The parameters m_i and k_i stand for the maximum number of cooperative actions its remaining energy can support, and the total number of times it was chosen as the member of the best relays, respectively. In other word, m_i and k_i jointly determine the "cooperative ability" a relay with. The analysis above actually motivates the study of the following algorithms.

A. Centralized Selection Algorithm

In centralized networks, with knowledge of all network parameters, an intuition is that the CU could exhaustively search all possible best relay assignments and find a combination that minimizes the outage probability of the system, which, however, is too complex for practical implementation, particularly the complexity will increase in a factorial manner with the increase of the possible combinations. We thus propose two algorithms with reduced complexity.

1) *Relay-based selection algorithm*: The basic idea of this algorithm is that from the relay point of view, the CU sequentially assigns sources for each relay. In total sense, the relay with

Algorithm 1 Relay-based selection algorithm

Input: $\Re$: The set of relays with $k \geq 1$;
$R_{\min\{k,m\}}(r_u)$: The set of relays with the minimum $\min\{k,m\}$ in $\Re$;
$R_k(r_v)$: The set of relays with the minimum k in $R_{\min\{k,m\}}(r_u)$;
$S_{r_i}(s_p)$: The set containing sources whose information has been decoded correctly by r_i but not received by the destination;
$S_{|A(s)|}(s_q)$: The set of sources with the minimum $|A(s)|$ in $S_{r_i}(s_p)$;
$Sum_{s_i,\min\{k,m\}}$: The sum of $\min\{k,m\}$ of all relays in $A(s_i)$;
$H_{r_i}(s_t)$: The set of sources which will be assisted by r_i.

for $i = 1 \rightarrow |\Re|$ **do**
　$R_{\min\{k,m\}}(r_u) = \arg\min_{r_j \in \Re} \min\{k_j, m_j\}$;
　if $|R_{\min\{k,m\}}(r_u)| == 1$ **then**
　　$r_{i^*} \leftarrow r_u$;　　$//r_{i^*}$ is the relay with priority
　else
　　$R_k(r_v) = \arg\min_{r_u \in R_{\min\{k,m\}}(r_u)} k_u$;
　　if $|R_k(r_v)| == 1$ **then**
　　$r_{i^*} \leftarrow r_v$;
　　else
　　$r_{i^*} = \arg\min_{r_v \in R_k(r_v)} m_v$;
　　end if
　end if
　if $k_{i^*} \leq m_{i^*}$ **then**
　　$H_{r_{i^*}}(s_t) \leftarrow S_{r_{i^*}}(s_p)$;
　else
　　for $l = 1 \rightarrow m_{i^*}$ **do**
　　$S_{|A(s)|}(s_q) = \arg\min_{s_p \in S_{r_{i^*}}(s_p)} |A(s_p)|$;
　　if $|S_{|A(s)|}(s_q)| == 1$ **then**
　　$s_t \leftarrow s_q$;
　　else
　　$s_t = \arg\min_{s_q \in S_{|A(s)|}(s_q)} Sum_{s_q,\min\{k,m\}}$;
　　end if
　　s_t joins $H_{r_{i^*}}(s_t)$;
　　$S_{r_{i^*}}(s_p) \leftarrow S_{r_{i^*}}(s_p) - s_t$;
　　end for
　end if
　for *each* $r_j \in \Re$ **do**
　　for *each* $s_p \in S_{r_j}(s_p)$ **do**
　　if $s_p \in H_{r_{i^*}}(s_t)$ **then**
　　$S_{r_j}(s_p) \leftarrow S_{r_j}(s_p) - s_p$;
　　$k_j \leftarrow k_j - 1$;
　　if $k_j == 0$ **then**
　　$\Re \leftarrow \Re - r_j$;
　　end if
　　end if
　　end for
　end for
　$\Re \leftarrow \Re - r_{i^*}$;
end for

small m and the relay with small k both have weaker ability in performing cooperation, the CU could take $\min\{k,m\}$ as the metric to evaluate a relay's cooperative ability and prioritize the relay with smaller $\min\{k,m\}$ for the sake of giving more relays a chance to participate in cooperation. We note here is a potential case in which two relays have the same $\min\{k,m\}$. In this case, it might be a good choice to give priority to the one with smaller k because it has narrower space to choose. Specially, if they have identical k as well, the relay with smaller m should be picked for consideration. On the other hand, in single relay sense, if $k \leq m$, the relay is automatically assigned to serve all the k sources it supports. Otherwise, due to energy constraint, the CU needs to select m out of the k candidates. When selecting, it considers sources having smaller $|A(s)|$ for the reason that they have a lower probability to be assisted. The details of the algorithm is described in Algorithm 1.

The complexity of this algorithm is $O(N^4)$, which is much lower than that of factorial complexity.

Algorithm 2 Source-based selection algorithm

Input: S: The set of sources whose information has not been correctly decoded by the destination;
$S_{|A(s)|}(s_u)$: The set of sources with the minimum $|A(s)|$ in S;
$R_{s_i,\min\{k,m\}}(r_v)$: The set of relays with the minimum $\min\{k,m\}$ in $A(s_i)$;
$R_k(r_p)$: The set of relays with the minimum k in $R_{s_i,\min\{k,m\}}(r_v)$.

for $i = 1 \rightarrow |S|$ **do**
　$S_{|A(s)|}(s_u) = \arg\min_{s_i \in S} |A(s_i)|$;
　if $|S_{|A(s)|}(s_u)| == 1$ **then**
　　$s_{i^*} \leftarrow s_u$;　　$//s_{i^*}$ is the source with priority
　else
　　$s_{i^*} = \arg\min_{s_u \in S_{|A(s)|}(s_u)} Sum_{s_u,\min\{k,m\}}$;
　end if
　$R_{s_{i^*},\min\{k,m\}}(r_v) = \arg\min_{r_v \in A(s_{i^*})} \min\{k_v, m_v\}$;
　if $|R_{s_{i^*},\min\{k,m\}}(r_v)| == 1$ **then**
　　$b_{i^*} \leftarrow r_v$;　　$//b_{i^*}$ is the best relay of s_{i^*}
　else
　　$R_k(r_p) = \arg\min_{r_v \in R_{s_{i^*},\min\{k,m\}}(r_v)} k_v$;
　　if $|R_k(r_p)| == 1$ **then**
　　$b_{i^*} \leftarrow r_p$;
　　else
　　$b_{i^*} = \arg\min_{r_p \in R_k(r_p)} m_p$;
　　end if
　end if
　$k_{b_{i^*}} \leftarrow k_{b_{i^*}} - 1$;　　$//k_{b_{i^*}}$ is b_{i^*}'s paremeter k
　$m_{b_{i^*}} \leftarrow m_{b_{i^*}} - 1$;　　$//m_{b_{i^*}}$ is b_{i^*}'s paremeter m
　if $m_{b_{i^*}} == 0$ **then**
　　for *each* $s_j \in S$ **do**
　　if $b_{i^*} \in A(s_j)$ **then**
　　$|A(s_j)| \leftarrow |A(s_j)| - 1$;
　　end if
　　end for
　end if
　for *each* $r_j \in A(s_{i^*})$ **do**
　　$k_j \leftarrow k_j - 1$;
　end for
　$S \leftarrow S - s_{i^*}$;
end for

2) *Source-based selection algorithm*: In contrast to the relay-based approach, this algorithm exploits from the source perspective and the rationale is in the following. Because sources with small $|A(s)|$ have a higher probability of outage, the CU assigns the best relay for each source according to an ascending $|A(s)|$ order, *i.e.*, it begins with the source having the minimum $|A(s)|$ and then for the one with the next minimum $|A(s)|$, until either all sources have been assigned a best relay or no available relays left. There is a special case where two sources have the minimum $|A(s)|$ simultaneously, which motivates search for a further comparison. We note here intuitively the probability of being assisted for a source is determined by $|A(s)|$, it is related to the cooperative ability of every member in $A(s)$ from a more specific point of view. So suppose two sources with $|A(s_i)| = |A(s_j)| = |A(s)|_{\min}$, s_i should be considered first if the "sum cooperative ability" of relays in $A(s_i)$, demoted by

$Sum_{s_i,\min\{k,m\}} = \sum \min\{k_l, m_l\}$, $r_l \in A(s_i)$, is weaker. As for the specific relay assignment, the CU may follow a similar principle used in the relay-based selection algorithm and pick up from $A(s)$, the relay with the minimum $\min\{k, m\}$. The pseudocode of this algorithm is presented in Algorithm 2. This algorithm is of $O(N^3)$ complexity in the worst case.

Algorithm 3 Distributed competition algorithm

Input: $flag(i)$: The flag that indicates whether s_i successes in direct transmission; λ: Time constant.

```
for i = 1 → N do
  if flag(i) == 0 then
    for each r_j ∈ A(s_i) do
      T_j = λ(α min{k_j, m_j} + βk_j + m_j);
    end for
    b_i = arg min_{r_j ∈ A(s_i)} T_j;
    flag(i) ← 1;
    k_{b_i} ← k_{b_i} − 1;      //k_{b_i} is b_i's paremeter k
    m_{b_i} ← m_{b_i} − 1;      //m_{b_i} is b_i's paremeter m
    if m_{b_i} == 0 then
      for each s_k (b_i ∈ A(s_k)) do
        A(s_k) ← A(s_k) − b_i;
      end for
    end if
  end if
end for
```

B. Distributed Selection Algorithm

In distributed scenarios, the centralized algorithms are not suitable. This subsection proposes a distributed competition algorithm for the distributed networks. The algorithm works in a fully decentralized manner, where each relay in $A(s_i)$ competes the best relay by starting an own timer with an initial value. Someone expires first wins and be the best relay of s_i. The initial value is set inversely proportional to $\alpha \min\{k, m\} + \beta k + m$, where $\alpha = (k_{\max} + 1)(m_{\max} + 1)$, $\beta = (m_{\max} + 1)$, $k_{\max}$ and $m_{\max}$ are the upper bounds of parameters k and m, respectively. Such a setup ensures the relays with weaker cooperative ability have more chances to perform cooperation. The pseudocode of the algorithm is shown in Algorithm 3.

In the absence of a CU scheduling source/relay selection orders, this simple algorithm is of the lowest complexity $O(N^2)$.

V. Simulation Results

This section presents simulation results of outage performance achieved by the relay selection algorithms described in this paper. To capture the spatial randomness of node location, particularly we consider all sources are randomly deployed in a square with the destination at its center and a side length of r meters, whereas other shapes of distribution model, such as disc, can also be applied without effecting the results. For the reason that the length of a time duration T is uncertain depending on the number of retransmission time slots, which is in turn determined by the number of sources failed in direct transmission, we describe T by several time units of $t_s = 2$ ms. Unless otherwise stated, we set the DL transmission time $\tau_0 T = 3t_s$, each transmission slot accounts one time unit, *i.e.*, $\tau_1 T = t_s$, the rate $R = 1$ b/s/Hz, $r = 5$ meters and $\eta = 0.6$.

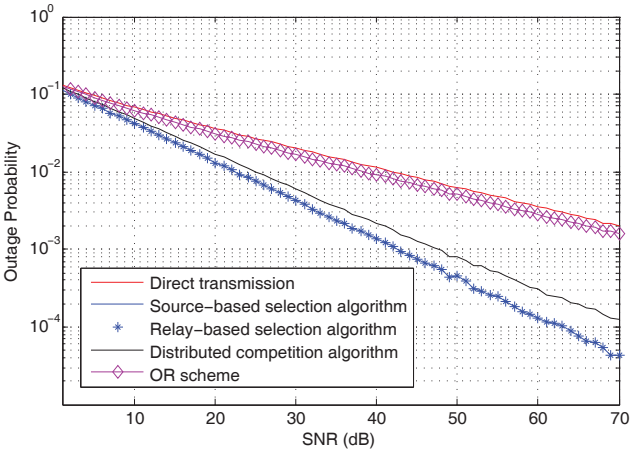


Fig. 3. Comparison of the outage probabilities among source-based, relay-based and distributed competition algorithms as well as direct transmission and OR scheme. $N = 5$, $\lambda_{s_i,d} = 0.1$, $\lambda_{s_i,s_j} = 0.2$.

Fig. 3 shows outage probabilities for the proposed relay selection algorithms as functions of DL SNR. Also shown are the direct transmission (non-cooperative) and the OR scheme in [16] for comparisons. Firstly, it can be seen from Fig. 3 that the outage probability decreases as DL SNR increases for each method considered. Such a phenomenon is because the DL SNR largely depends on the transmission power P at the destination when the receiver noise with unit variance. Hence, a larger DL SNR means a large P, leading to more power splitted to energy harvesting, which decreases the chance of an outage event. Besides, we also observe that the direct transmission achieves the worst performance, and the three proposed algorithms outperform OR scheme. Compared to the OR scheme where the node with the strongest end-to-end path is the unique best relay in the system, our protocol provides several available best relays for every source, which reduces competition among relays, and thus resulting in good performance. Moreover, as can be seen from the figure, the relay-based selection algorithm and the source-based selection algorithm enjoy significantly dominance over the distributed competition algorithm. The centralized algorithms give priority to sources with less chances to be assisted, so more source information is possible to be correctly received. Finally, we note that the source-based algorithm performs very close to the relay-based algorithm, which is the result of similar basic idea.

In Fig. 4, the influence of inter-source quality on outage performance for the proposed algorithms is provided ($\lambda_{s_i,s_j} = 0.1, 10$). It is clearly shown that as λ_{s_i,s_j} increases, the outage probability increases as well. This is because the protocol uses source-source channels to perform cooperation, weaker inter-source link means less cooperation possibility.

In Fig. 5, the outage probabilities of the proposed algorithms in the case of different source numbers are shown ($N = 3, 10$). When more sources join in the transmission, it is highly likely more potential relays available at each source since every source in the considered system is a source and is also a relay, which is the reason to observe the phenomenon in Fig.

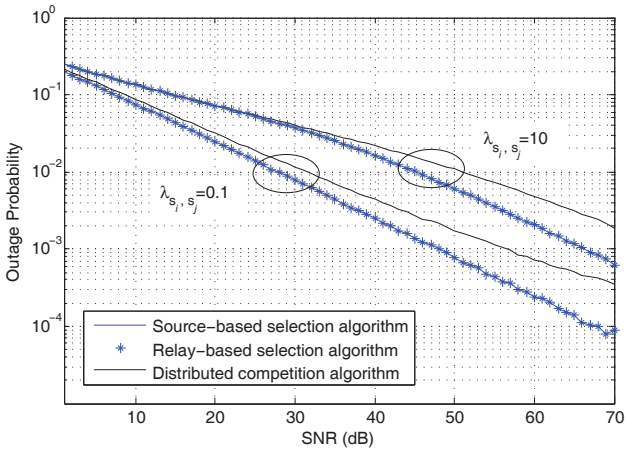


Fig. 4. Comparison of the outage probabilities with different inter-source channel quality. $\lambda_{s_i,d} = 0.2$, $N = 5$.

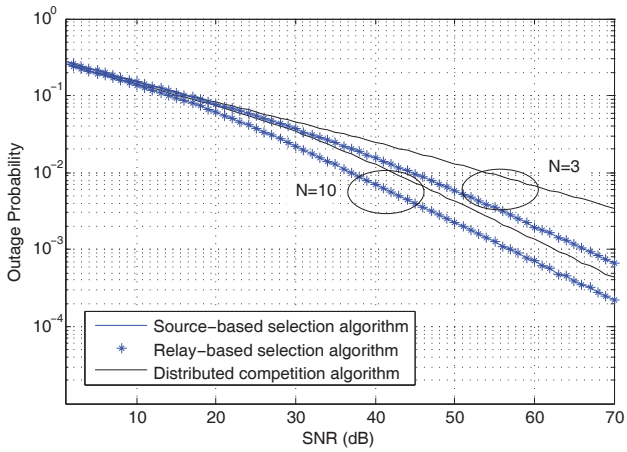


Fig. 5. Comparison of the outage probabilities with different source number. $\lambda_{s_i,s_j} = 5$, $\lambda_{s_i,d} = 0.2$.

5 that with a larger number of sources, the outage performance improves.

Finally in Fig. 6, the impact of node distances on the network outage performance is studied by considering different values of r ($r = 0.5, 10$). We can see from Fig. 6 that the performance degrades as r increases. Increasing r, the energy harvested in the DL at each source (E_i defined in (3)) decreases due to path loss. Consequently, less successful UL direct transmissions occur and less possibilities of cooperation.

VI. Conclusion

In this paper, we have studied a cooperation protocol with multiple available best relays for multi-source wireless powered IWSNs with beacon transfer in the DL and cooperative information transmissions in the UL. It addressed the “energy drain” problem in conventional schemes and had the advantage of easy to be implemented in practical IWSNs. In addition, the best relay selection algorithms were also studied to reduce the possible conflicts of relay selection among sources. Specifically, a source-based selection algorithm and a relay-based selection algorithm were proposed for centralized scenarios, and a distributed competition algorithm is investigated for distributed scenarios. Simulation results verified the performance of each algorithm developed. In this work, we did not consider the possible energy cooperative among sources, which might be a promising future direction to further improve system performance.

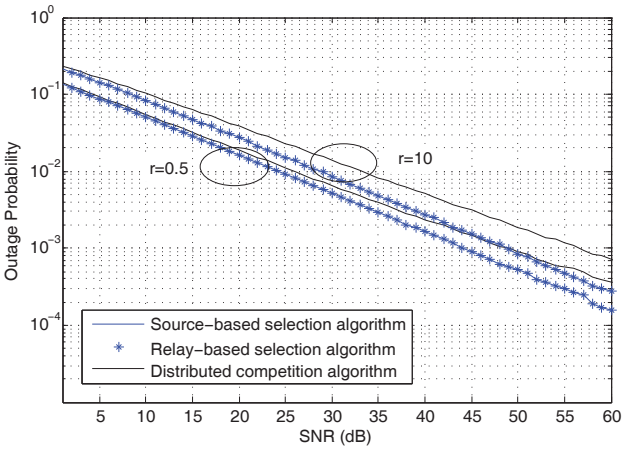


Fig. 6. Comparison of the outage probabilities with different source-destination distance. $\lambda_{s_i,s_j} = 0.2$, $\lambda_{s_i,d} = 0.1$, $N = 5$.

References

[1] B. Babayigit and M. Abubaker, “Industrial internet of things: A review of improvements over traditional scada systems for industrial automation,” *IEEE Systems Journal*, vol. 18, no. 1, pp. 120–133, 2024.

[2] X. Xie, H. Wang, and X. Liu, “Scheduling for minimizing the age of information in multisensor multiserver industrial internet of things systems,” *IEEE Transactions on Industrial Informatics*, vol. 20, no. 1, pp. 573–582, 2024.

[3] D. Van Leemput, A. Sabovic, K. Hammoud, J. Famaey, S. Pollin, and E. De Poorter, “Energy harvesting for wireless iot use cases: A generic feasibility model and tradeoff study,” *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15 025–15 043, 2023.

[4] X. Zhou, R. Zhang, and C. K. Ho, “Wireless information and power transfer: Architecture design and rate-energy tradeoff,” *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.

[5] M. Poposka, S. Pejoski, V. Rakovic, D. Denkovski, H. Gjoreski, and Z. Hadzi-Velkov, “Delay minimization of federated learning over wireless powered communication networks,” *IEEE Communications Letters*, vol. 28, no. 1, pp. 108–112, 2024.

[6] X. Jiang, K. Liang, X. Chu, C. Li, and G. K. Karagiannidis, “Multiplexing embb and urllc in wireless powered communication networks: A deep reinforcement learning-based approach,” *IEEE Wireless Communications Letters*, vol. 12, no. 10, pp. 1716–1720, 2023.

[7] H. Ju and R. Zhang, “Throughput maximization in wireless powered communication networks,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[8] L. Bai, Z. Huang, T. Feng, and X. Cheng, “A non-stationary channel model for 6g multi-uav cooperative communication,” *IEEE Transactions on Wireless Communications*, vol. 23, no. 2, pp. 949–961, 2024.

[9] K. G. Rallis, V. K. Papanikolaou, P. D. Diamantoulakis, S. A. Tegos, A. A. Dowhuszko, M.-A. Khalighi, and G. K. Karagiannidis, “Energy efficient cooperative communications in aggregated vlc/rf networks with noma,” *IEEE Transactions on Communications*, vol. 71, no. 9, pp. 5408–5419, 2023.

[10] Z. Zhang, Y. Wu, X. Lei, L. Lei, and Z. Wei, “Toward 6g multicell orthogonal time frequency space systems: Interference coordination and cooperative communications,” *IEEE Vehicular Technology Magazine*, vol. 19, no. 1, pp. 55–64, 2024.

[11] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.

[12] H. Ju and R. Zhang, "User cooperation in wireless powered communication networks," in *Proc. IEEE Globecom*, Austin, TX, USA, Dec. 2014, pp. 1430–1435.

[13] R. Zhang and C. K. Ho, "Mimo broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[14] Y. Gu, H. Chen, Y. Li, Y. C. Liang, and B. Vucetic, "Distributed multi-relay selection in accumulate-then-forward energy harvesting relay networks," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 74–86, Mar. 2018.

[15] H. Wang, Q. Xiong, and M. Li, "Selection cooperation using packet aggregation with equal rate feedback in industrial wireless sensor networks," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2531–2534, Dec. 2018.

[16] H. Chen, Y. Li, J. L. Rebelatto, B. F. Uchôa-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, no. 7, pp. 1700–1711, Apr. 2015.

[17] I. Krikidis, "Relay selection in wireless powered cooperative networks with energy storage," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2596–2610, Dec. 2015.

[18] K.-H. Liu, "Performance analysis of relay selection for cooperative relays based on wireless power transfer with finite energy storage," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5110–5121, Jul. 2016.

[19] B. Medepally and N. Mehta, "Voluntary energy harvesting relays and selection in cooperative wireless networks," *IEEE Trans Wireless Commun.*, vol. 9, no. 11, pp. 3543–3553, Nov. 2010.

[20] M. Li, M. Yu, Y. Zhang, and H. Wang, "A lightweight selection cooperation protocol with multiple available best relays," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1172–1175, Jun. 2013.

[21] L. Li, Y. Liu, I. You, and F. Song, "A smart retransmission mechanism for ultra-reliable applications in industrial wireless networks," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1988–1996, 2023.

[22] Z. Ding and H. V. Poor, "Multi-user swipt cooperative networks: Is the max–min criterion still diversity-optimal?" *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 553–567, Jan. 2016.

[23] M. Cheffena, "Propagation channel characteristics of industrial wireless sensor networks," *IEEE Antennas Propag Mag*, vol. 58, no. 1, pp. 66–73, Feb. 2016.

[24] M. Chitra, S. Yashaswini, and S. Dhanasekaran, "Performance analysis of cooperative underlay noma-assisted cognitive radio networks," *IEEE Wireless Communications Letters*, vol. 13, no. 1, pp. 203–207, 2024.

[25] Y. Geng, E. Liu, R. Wang, P. Sun, B. Lu, and J. Wang, "Reinforcement-learning-based policy design for outage minimization in df relaying networks," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15 359–15 374, 2024.

An empirical analysis of RIS phase quantization effect in an IIoT scenario

PAN Junjian[1], ZHANG Yuxiang[1], ZHANG Jianhua[1], GONG Huiwen[1], XIA Liang[2], LIU Guangyi[2]

***Abstract*—The Industrial Internet of Things (IIoT) leverages advanced communication technologies to enhance industrial manufacturing processes. Reconfigurable Intelligent Surface (RIS) is considered a key technology for optimizing wireless propagation environments in complex IIoT scenarios. This paper investigates the impact of RIS phase quantization on communication performance within IIoT settings. First, measurements of RIS-assisted communication channels under different quantization bits are conducted in an IIoT scenario. Next, this pa**

per analyzes the effect of phase quantization on the received signal level and the main lobe direction. The results indicate that RIS can provide regular performance improvements at different points in the plant with different quantization bits, which align with theoretical analysis.

***Keywords*—Reconfigurable Intelligent Surfaces, Industrial Internet of Things, wireless communication, RIS phase quantization**

This work was supported in part by the National Key R&D Program of China (2023YFB2904802), in part by the National Natural Science Foundation of China under Grant 92167202, Grant U22B2057 and Grant 62201087, in part by the National Science Foundation for Distinguished Young Scholars under Grant 61925102, in part by Guangdong Major Project of Basic and Applied Basic Research (2023B0303000001) and in part by the Beijing University of Posts and Telecommunications-China Mobile Research Institute Joint Innovation Center.

J. J. Pan, Y. X. Zhang, J. H. Zhang, H. W. Gong. School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: junjianpan@bupt.edu.cn; zhangyx@bupt.edu.cn; jhzhang@bupt.edu.cn; birdsplan@bupt.edu.cn).

L. Xia, G. Y. Liu. China Mobile Research Institute, Beijing 100053, China (e-mail: xialiang@chinamobile.com; liuguangyi@chinamobile.com).

I. INTRODUCTION

The Industrial Internet of Things (IIoT) represents a crucial arena in future communications, characterized by its high demands for connectivity and reliability[1]. In IIoT scenarios, the presence of numerous scatterers such as metal pipe networks, metal machinery and transport carts often leads to severe deep fading during signal propagation[2]. Reconfigurable Intelligent Surface (RIS) is a promising solution to these challenges. RIS can actively beam the incident signal in a specific direction to control the wireless propagation environment[3].

Nevertheless, practical deployment of RIS usually faces limitations in phase configuration, typically constrained by 1-bit/2-bit quantization, which introduces phase inaccuracies and associated errors. Consequently, extensive research is conducted to investi-

Figure 1 Photograph of measurement campaign.

Table I Parameters and Configurations of The Measurement Campaign

Label	No.1	No.2
Scenario	IIoT	
Central Frequency	3.45 GHz	
Bandwidth	200 MHz	
TX Antenna Type	Horn antenna	
RX Antenna Type	Omnidirectional antennas	
Power Amplifier Gain	22 dB	
Low-noise Amplifier	65 dB	
RIS Size	1.64 m*1.09 m	0.64 m*0.64 m
Amount of RIS units	48*32	32*32
RIS Quantization Number	1-bit/2-bit	1-bit
Measurement Route	Line 1	Line 1/2

gate the RIS phase quantization problem and its effect on communication systems. Some works study the impact of RIS phase quantization on beamforming capability, received signal levels, signal-to-noise ratio and channel estimation accuracy[4-6]. In [7], the authors explore the impact of continuous and discrete phase shifts on RIS-
aided systems in wideband communication channels. Authors in [8-9] explain the influence of RIS phase quantization on the data rates and secrecy outage probability. These papers theoretically provide insights into the impact of quantization bits of RIS on communication performance in various aspects. Additionally, some papers study the performance of RIS in practical communication scenarios. Some works [10-11] discuss the 1-bit/2-bit RIS on channel stationarity and beam effect in indoor scenarios. Paper [12] integrates modeling and measurement results of RIS reflection coefficients in an anechoic chamber to optimize RIS codebook configurations.

Previous research on RIS quantization bits primarily focuses on theoretical performance analysis, with limited experimental studies conducted in indoor or anechoic chamber settings. Thus, there is a significant gap in practical measurement and analysis under IIoT scenarios. It is crucial to investigate the effect of RIS phase quantization specifically in IIoT environments. This paper addresses this gap by conducting channel measurements in a typical IIoT scenario within an indoor factory setting. The study analyzes the channel characteristics across the entire scenario under different RIS quantization bits. It identifies systematic variations in received signals at different locations along the route and assesses the main lobe direction error.

The structure of this paper is arranged as follows: Section II details the experimental environment and methods, including system construction, parameter settings, and performance indicators. Section III presents and analyzes the experimental results, discussing RIS performance under different phase quantization bits. Finally, Section IV summarizes the paper.

II. EXPERIMENTAL MEASUREMENT AND VALIDATION FOR RIS PHASE QUANTIZATION ERROR

To study the propagation characteristics in IIoT scenario, we conduct a channel measurement campaign in an indoor manufacturing factory. The photograph of the measurement environment is shown in Fig. 1.

A. MEASUREMENT SYSTEM

This section details the setup and positioning of the

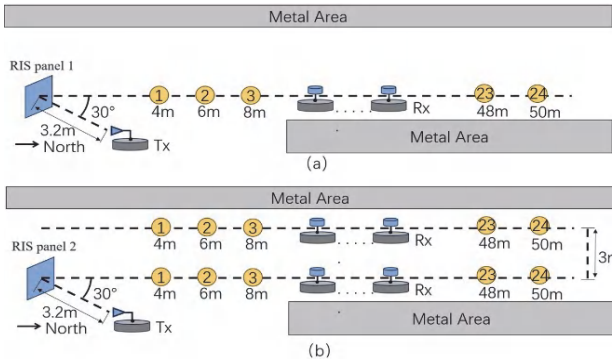


Figure 2 The schematic diagram of the measurement. (a)Route No.1; (b) Route No.2.

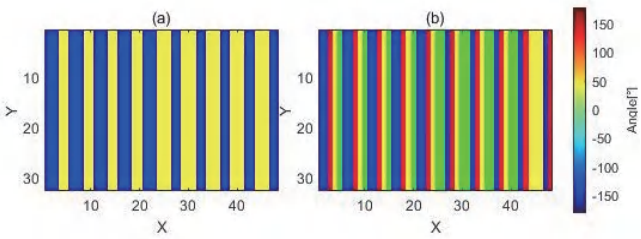


Figure 3 RIS Codebook. (a) 1-bit quantization; (b) 2-bit quantization.

experimental equipment, the operating mode of the RIS panels, and other detailed parameters. The experiment utilizes two RIS panels: RIS panel 1, a 1.64 m × 1.09 m panel with 1 or 2-bit quantization, and RIS panel 2, a 0.64 m × 0.64 m panel with 1-bit quantization for channel measurements. On the TX side, the vector signal generator generates continuous wave signals at 3.45GHz. On the RX side, the spectrum analyzer captures and records the received signals. The RIS is placed in the channel between the TX and RX, and the phase configuration is calculated based on the positions of the TX and RX.

To guarantee the effective dynamic range of the received signal, we employ a high-gain horn antenna at the TX to direct the signal at the RIS panel. At the RX, an omnidirectional antenna is used. The measurement system parameters are shown in the Table I.

B. MEASUREMENT SETTING

This factory represents a typical IIoT scenario. We conduct channel measurements in a factory with 150 m × 50 m and the height is 25m. To accurately represent the profusion of metal scatterers in the IIoT context, we choose a straight and unobstructed central path of metal pipe networks with mechanical devices on both sides. The regions on both sides are designated as metal zones. Measurements are conducted at night when the factory is not operational, ensuring a static channel environment is not influenced by moving machine parts and assembly equipment. For Route No. 1, the TX and RIS are fixed in the southern part of the factory, with the RX starting 4m from the RIS and measuring every 2 m up to 50 m. TX is positioned at a 30° angle to the RIS normal, 3.2 m from the RIS center. The measurement setup ensures that the TX-RX channel is a non-line-of-sight (NLOS) channel and RIS-RX channel is a line-of-sight (LOS) channel. In this configuration, the signals received by the RX are exclusively due to reflections from the RIS and scattering from other scatterers, with no direct signals being received from the TX. Three configuration methods are employed for RIS panel 1: 1-bit quantization, 2-bit quantization, and a RIS off state. For Route No. 2, a parallel line is introduced 3 m east of the existing line, maintaining identical point settings across both routes. The RIS board adopts only 1-bit phase quantization. The layout of the measurement scenario is shown in Fig. 2.

C. RIS CODEBOOK CONFIGURATION

All RIS codebooks are configurated based on the positions of the TX, RIS and RX. Specifically, for $(m,n)^{th}$RIS unit, the required phase shifts $\phi_{m,n}$ is

$$\phi_{m,n} = -2\pi\left(\frac{d_m \sin(\theta_i) + d_n \sin(\theta_o)}{\lambda}\right), \#(1)$$

where d_m and d_n are the distances of the unit from the center of the RIS panel in the m and n directions, respectively, θ_i is the incident angle, θ_o is the outgoing angle, and λ is the wavelength.

Next, we typically configure quantization phase

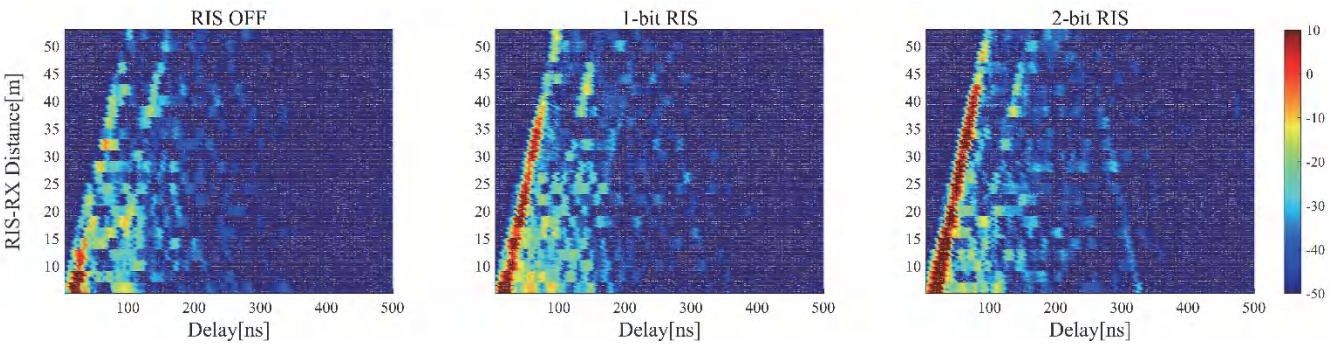


Figure 4 PDP evolution vs RIS-RX distance. (a.) RIS OFF; (b) 1-bit RIS; (c) 2-bit RIS.

shift for each RIS unit to take on a finite set of discrete values. The quantization process for i-bit quantization involves dividing the range into 2^i intervals and mapping the calculated phase shift to the nearest interval center value. The quantization formula is

$$\phi_{m,n}^{\text{quantized}} = \frac{2\pi k}{2^i}, \#(2)$$

where k is the integer that corresponds to the closest quantization level of the continuous phase shift.

Based on this, the quantization phase shift for each RIS unit is calculated and these phase shift values are stored in the codebook. Codebooks for the RIS panel under 1-bit and 2-bit quantization are calculated, as shown in the Fig. 3, where variable x represents the element number index in the horizontal direction, y represents the element number index in the vertical direction.

III. ANALYSIS OF RIS PHASE QUANTIZATION ERROR

A. POWER DELAY PROFILE

Power delay profile (PDP) can be utilized to analyze the impact of multipath effects on the performance of communication systems. To capture the overall multipath information of the scenario, PDP evolution vs RIS-RX distance under different RIS phase quantization bits is observed along the Route No. 1. Measurement results are shown in Fig. 4. For the case RIS is off, a clear main path can be observed within the range of 4 to 15 m. However, the power of the main path diminishes beyond 15 m, and rich multipath components (MPCs) are observed within a 200 ns window following the main path delay. This phenomenon occurs because the RIS reflects the incident signal symmetrically, since the RX is not at the specular reflection point, the received signals result entirely from surrounding rich scattering environment. For the 1-bit quantization, RIS moderately improves beam focusing capability, with a clear main path observed within the range of 4 to 35 m point, while still rich MPCs can be observed within a 200 ns window following the main path delay. For the 2-bit quantization, RIS significantly improves beam focusing capability with a clear main path observed at 45 m point and the power of the main path is improved by approximately 2.5 dB compared with 1-bit quantization case. Besides, the MPCs along the entire route are also significantly reduced. The measurement results indicate that the introduction of RIS can significantly enhance the main path power and mitigate the effects of multipath, making it suitable for deployment in IIoT scenarios.

B. SIGNAL LEVEL ERROR

The normalized signal level is the ratio of the received signal strength from the direct signal of the RIS under i-bit quantization to that under continuous quantization. According to [4], the authors provided the normalized signal level expressions for RIS under i-bit quantization, the formula is:

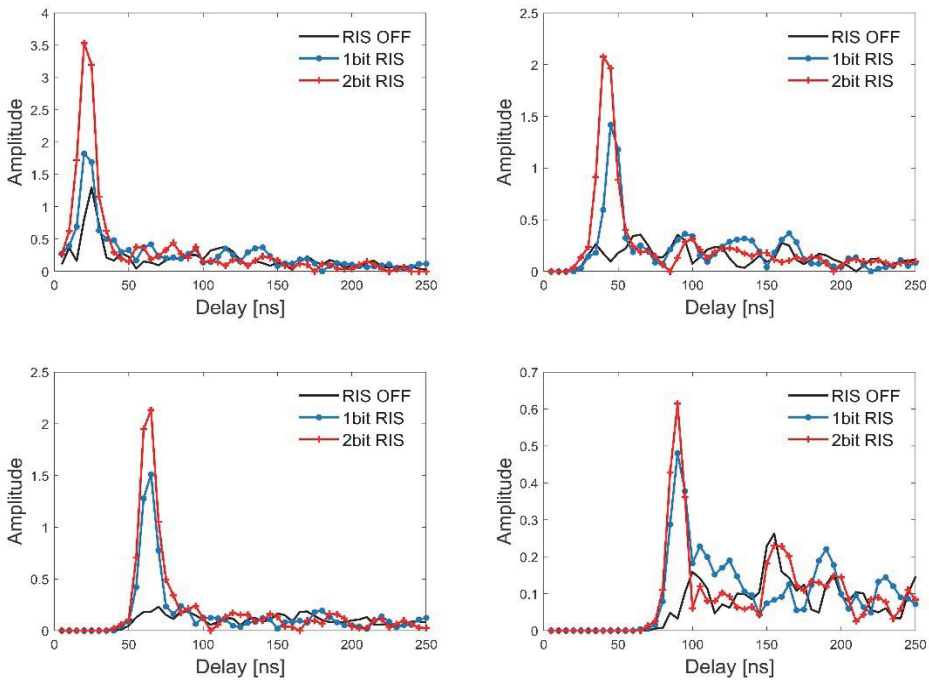


Figure 5 CIR at different receiving points with the RIS in different configurations. (a.) Point at 8 m; (b) Point at 22 m; (c) Point at 30 m; (d) Point at 6 m.

$$S_{\text{relative}} = \frac{E_{\psi_{m,n}}\left(s_{rx_q}\right)}{s_{rx_q}{}'} = \text{sinc}\left(\frac{\pi}{2^i}\right), \#(3)$$

where i is the number of quantization bits. The signal level error is used to measure the variation of received signal strength of the direct signal from the RIS between different RIS quantization bits, which can be calculated through the ratio of S_{relative} under different quantization bits.

In the empirical measurements, the channel impulse response (CIR) main path represents the direct signal from the RIS. The CIR and main path levels for Route No.1 with RIS panel 1 at different points are provided in Fig. 5. For 1-bit quantization with $i = 1$, the normalized signal level is $\frac{2}{\pi}$ (approximately 0.64). For 2-bit quantization with i =2, the normalized level is approximately $\frac{2\sqrt{2}}{\pi}$ (approximately 0.90). Thus, the signal level error of 1-bit RIS to 2-bit RIS on a single main path is 0.711. The signal level error between 1-bit and 2-bit quantization is small at nearby locations but becomes larger at farther locations. The CIR at the 22 m and 30 m points is shown in Fig. 5 (b) and (c). For the main path, the measured signal level error between 1-bit and 2-bit quantization at the 22 m point is 0.7, which is close to the theoretical analysis. At the 8 m and 46 m point in Fig. 5 (a) and (d), the measured signal level error between 1-bit and 2-bit quantization is 0.5 and 0.8 respectively. These values are lower or higher than the theoretical predictions. This discrepancy is due to the cumulative effect of multiple factors. At nearby locations, the higher signal strength makes the impact of quantization errors more pronounced, resulting in received main path signal strength being lower than theoretical predictions. While at farther distances, the signal strength experiences greater attenuation, making the influence of 1-bit quantization

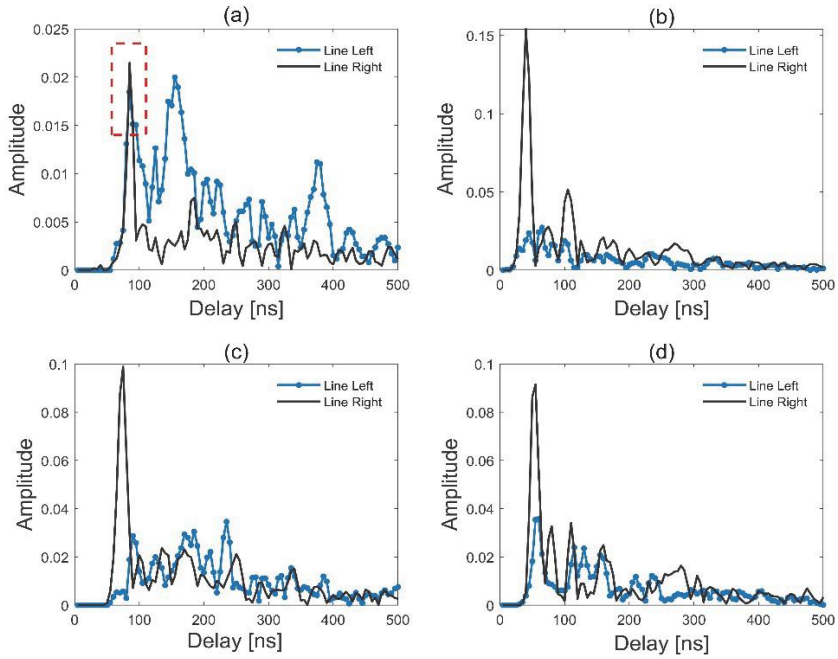


Figure 6 CIR at different receiving points with the RX in different lines. (a) Point 46m; (b) Point 22m; (c) Point 42m; (d) 4 Point 30m.

errors relatively smaller compared to multipath effects and other factors, leading to a higher normalized signal level. Overall, in IIoT scenarios, high-bit quantization configurations of RIS can increase the main path signal level compared to low-bit configurations. However, due to the influence of highly reflective scatterers in the environment, the ratio of the main path level of low-bit quantization to high-bit quantization will generally increase from near to far points.

C. MAIN LOBE DIRECTION ERROR

Due to the i-bit quantization of the RIS phase, there will be a deviation between the actual main lobe direction and the expected emission direction. The difference between the actual main lobe direction and the desired direction is defined as the main lobe direction error, formulated as follows.

$$\theta_{error} = \theta_{max} - \theta_{except}. \#(4)$$

We use RIS panel 2 to conduct channel measurements on Route 2 to analyze the main lobe direction error. Route 2 consists of two parallel lines spaced 3 meters apart. As the classic RIS radiation pattern main lobe is symmetrical, when the main signal levels of the left and right lines are equal, it can be considered that the actual maximum emission direction of the RIS is exactly pointing to the midpoint between the two lines. Combining this with the RIS-RX distance, the main lobe direction error of the RIS radiation pattern can be obtained. The main lobe direction error calculation method is given:

$$\theta'_{error} = arctan\frac{d_0}{d_{rx}}, \#(5)$$

where θ'_{error} represents the main lobe direction error obtained through measurements and d_0 is the midpoint between the two lines, which is 1.5 m.

As shown in the Fig. 6, the CIR curves at the left and right points of the RIS panel No.2 at the 46 m position are compared. It can be seen that the main path signal levels of the left and right lines are very close, as shown in the red box part in Fig. 6 (a). At points before 46 m, such as 22 m and 42 m positions, the main signal level of the left line is significantly higher than that of the right line. Conversely, at points beyond 46 m, such as the 48 m position, the main signal level of the right line is significantly higher

than that of the left line. According to (5), it can be concluded that there is an angle error of 1.87° for the 1-bit RIS compared to continuous phase quantization. This conclusion indicates that the actual deployment of RIS must consider potential angle errors to identify and mitigate any adverse impact on signal propagation.

IV. CONCLUSION

This paper investigates the effect of RIS phase quantization on wireless system in an IIoT scenario. The experimental results indicate that, in an IIoT scenario a 2-bit quantization significantly improves received signal level and emission accuracy compared to a 1-bit quantization, which is consistent with theoretical predictions. And as the distance increases, the performance differences of RIS under different quantization accuracies gradually become apparent due to the impact of metal scatters. These results provide valuable insights for the practical application and optimization of RIS in IIoT scenarios.

References

[1] DE ALWIS C, KALLA A, PHAM Q, et al. Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research[J]. IEEE Open Journal of the Communications Society, 2021, 2: 836-886.

[2] JIANG T, ZHANG J H, Tang P, et al. 3GPP Standardized 5G Channel Model for IIoT Scenarios: A Survey [J]. IEEE Inter-net of Things Journal, 2nd ed., 2021, 8(11): 8799-8815.

[3]ZHANG J H, ZHANG J W, ZHANG Y X, et al. Advancements in RIS Channel Measurement and Modeling for 6G[J]. Radio Communications Technology, 2024, 50(2): 227-237.

[4] HASKOU A, KHALEGHI H. On the Effect of RIS Phase Quantization on Communications System Performances [C]. International Wireless Communications and Mobile Compu-ting (IWCMC). USA: IEEE, 2023: 1406-1411.

[5] RENZO M D, MOHAMED A, ZAPPONE A, et al. Effects of realistic reradiation models in digital reconfigurable intelligent surfaces [J]. Journal of Information and Intelligence, 2023, 1(3): 238-252.

[6] GONG H W, Zhang J H, Zhang Y X, et al. How to Extend 3D GBSM Model to RIS Cascade Channel with Non-ideal Phase Modulation? [J]. IEEE Wireless Communications Letters, 2024, 13(2): 555-559.

[7] SOUZA P, KHAZAEE M, MENDES L. Continuous and Discrete Phase-shifts for RIS-aided Systems in Wideband Communication Channels [C]//XLI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT2023). 2023: 1406-1411.

[8] ZHANG H L, DI B Y, SONG L Y, et al. Reconfigurable Intelligent Surfaces Assisted Communications With Limited Phase Shifts: How Many Phase Shifts Are Enough? [J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4498-4502.

[9] WEI S, XU J D, XU W, et al. Secure Outage Analysis of RIS-Assisted Communications With Discrete Phase Control [J]. IEEE Transactions on Vehicular Technology, 2023, 72(4): 5435-5440.

[10] LIU G Y, WANG J Z, ZHANG Y, et al. Field trial measurement and channel modeling for reconfigurable intelligent surface[C]. Proceedings of the International Conference on Communications (ICC). 2022: 1-6.

[11] ZHANG S, SUN H R, YU R Z, et al. Two-Bit RIS-Aided Communications at 3.5GHz: Some Insights from the Measurement Results Under Multiple Practical Scenes [C] // International Conference on Communications in China (ICCC). 2022: 1-6.

[12] CAO L, YIN H F, TAN L, et al. RIS with Insufficient Phase Shifting Capability: Modeling, Beamforming, and Experimental Validations [J]. IEEE Transactions on Communications, 2024: 1-1.

About the authors

PAN Junjian received B.S. degree in electronic information engineering from Hefei University of Technology in 2022. He is now pursuing the Master's degree in Beijing University of Posts and Telecommunications. His current research interest includes channel modeling and Reconfigurable Intelligent Surface technology. (Email: junjianpan@bupt.edu.cn)

ZHANG Yuxiang received B.S. degree in electronic information engineering from Dalian University of Technology in 2014 and Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT) in 2020. He is now a associate research fellow in BUPT. His current research interests include channel modeling, massive MIMO, beamforming, OTA testing and etc. (Email: zhangyx@bupt.edu.cn)

ZHANG Jianhua received the B.S. degree from the North China University of Technology, in 1994 and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2003. She is currently the Professor with the Information and Engineering College, BUPT. (Email: jhzhang@bupt.edu.cn)

GONG Huiwen received the B.S. degree from the Beijing University of Posts and Tele-communications, Beijing, China, in 2021, where he is pursuing the M.S. degree. His research interest contains RIS channel mod-eling. (Email: birdsplan@bupt.edu.cn)

XIA Liang received the B.S. degree in Electronic and Information Engineering in 2005 and the M.S. degree in Information and Communication Engineering in 2008 from Tsinghua University, Beijing, China. He was a researcher at LTE physical layer in Huawei from 2008 to 2014 and was a researcher at 5G physical layer in China Mobile from 2015 to 2019. His current research interests include millimetre-wave, THz, and visible light communication.(Email: xialiang@chinamobile.com)

Liu Guangyi received the Ph.D. degree from the Beijing University of Posts and Telecommunications. He is currently the CTO of the Wireless Department, China Mobile Research Institute, where he is in charge of the wireless technology research and development, including LTE/LTE-Advanced and 5G. (Email: liuguangyi@chinamobile.com)

Industrial process monitoring based on multi-block graph convolutional network[1]

Chen Xufei[1], Li Shijin [1], Yu Jianbo

***Abstract*—The complex characteristics of multi-unit and strong corrections among different units in modern industrial processes have imposed great challenges to process modeling and monitoring. To solve these issues, a new multi-block graph convolutional network monitoring model based on Pearson correlation coefficient is proposed (MBGCN) for multi-block process monitoring in this study. Firstly, graph data is constructed to describe the intricate correlations of the high-dimensional process data. The adjacency matrix of the graph structure is initiated via K-Nearest Neighbor, and a graph autoencoder is utilized to automatically learn the interactions between samples. Secondly, the Pearson correlation coefficient is employed to divide the process into sub-blocks. Graph convolutional neural network is applied to learn effective feature representations for constructing monitoring statistics. Finally, the monitoring results of each sub-block are fused through Bayesian inference. The experimental results in Tennessee Eastman Process illustrate the effectiveness and superiority of MBGCN in multi-block process fault detection.**

***Keywords*—Complex industrial processes, graph convolutional neural network, multi-block process monitoring, Bayesian inference**

I. INTRODUCTION

As the industries advance, processes become more integrated and intricate. It is essential to monitor and control industrial processes effectively to maintain the integrity and reliability of complex systems with fast-evolving industrial landscapes[1]. In the past decades, multivariate statistical process monitoring methods have been proposed for fault detection and diagnosis. The representative methods mainly include principal component analysis (PCA)[2], independent component analysis (ICA)[3], canonical variate analysis (CVA)[4] and their extensions. Each of these methods have been extensively studied and has demonstrated significant success in industrial process monitoring and fault diagnosis.

However, modern industrial processes are evolving towards the trend of multiple different parts and operation units, which are usually featured with complex correlations among process variables. In this scenario, constructing a global model for the entire process is inappropriate as it overlooks local behaviors, and the monitoring results are usually difficult to interpret. The multi-block process monitoring methods are typically developed to reduce process complexity and provide closer insight into each sub-part of the industrial processes. Zhang et al.[5] proposed a multiblock kernel partial least squares model for decentralized fault diagnosis in complex industrial process. Zhu et al.[6] developed a distributed parallel PCA model for multi-block process monitoring, which designed a fusion rule for integrating local block statistics. The above works performed well in reducing the complexity and capturing the local information. Nevertheless, the variables division is conducted based on prior knowledge, and the decomposition result relies on the cognition or experience of operators. To overcome this issue, Zeng et al.[7] designed a mutual information-based sparse multiblock dissimilarity method for fault detection and diagnosis, which utilized mutual information for multiblock division.

Xufei Chen, Li Shijin and Jianbo Yu are with School of Mechanical Engineering, Tongji University, Shanghai, China, Jianbo Yu is also with State Key Laboratory of Large Electric Drive System and Equipment Technology Gansu, China

This work was supported by the National Natural Science Foundation of China (No.92167107).

Jiang et al.[8] proposed a multiblock PCA model based on mutual information and adopted a support vector data description technique to combine the monitoring results of each block.

In parallel with the process division issue, constructing local models for different sub-blocks also has a significant impact on monitoring performance. PCA and its variations are the commonly used techniques. Jiang et al.[9] adopted kernel PCA for modeling the sub-blocks divided via mutual information-spectral clustering. Tian et al.[10] proposed a weighted copula-correlation based multiblock PCA method for process monitoring, which employs PCA for feature learning and adopts Bayesian inference for information fusion of different sub-blocks. However, with the expansion of industrial production scale, PCA and its extensions fail to learn effective feature representations for the increasingly complex process data. Yao et al.[11] employed variational autoencoder to learn feature embeddings of each sub-block for effective distributed process monitoring. He et al.[12] used a temporal one-dimensional convolutional neural network to learn the temporal-correlated features of each block and fused the local features to construct a global feature representation. Zhu et al.[13] utilized an improved convolutional neural network to learn the features of each block and a decoupling layer as a feature regularizer.

However, the above methods often struggle to express the intricate connections among process data, which leads to suboptimal performance in detecting faults. Graph neural networks (GNN)[14][15], on the other hand, can leverage the structure information inherent in the data, enabling more accurate and robust identification of anomalies. In recent years, GNN has been widely applied to process monitoring to model spatial relationship. Ren et al.[16] a novel spatial-temporal associations representant model for process monitoring, which adopted graph convolutional neural network (GCN) for feature learning. Li et al.[17] designed a spatial-temporal graph autoencoder model for process fault diagnosis, which employs GCN, long short-term memory network and attention mechanism to learn comprehensive features. Although the above methods have obtained good performance, the application of GNN in multi-block process monitoring still remains under-explored. Zhang et al.[18] proposed a distributed dynamic graph embedding model for multiblock process monitoring, which considered both temporal and neighborhood information via constructing graph structure from process data.

In consideration of the above-mentioned limitations, a new multi-block graph convolutional network monitoring model based on Pearson correlation coefficient is proposed (MBGCN) for multi-block process monitoring in complex large-scale industrial processes. The main contributions are as follows: (1) A multi-block graph convolutional network is proposed for process monitoring, which can provide an interpretable fault detection result concerning the exact sub-block of the detected fault; (2) A novel graph construction algorithm based on K-Nearest Neighbor and Graph Auto-Encoder (GAE) is proposed. KNN is used to obtain the initial adjacency matrix, and then the GAE model is used to obtain the correlation between samples automatically; (3) Pearson correlation coefficient is utilized to segment the process variables into sub-blocks by measuring the correlations between variables. GCN is employed to extract effective features from each block, which not only considers the correlation between samples but also captures the correlation between variables. Finally, the Bayesian fusion is used to fuse the monitor results of each subblock for global process monitoring.

The rest of this paper is structured as follows: Section II discusses the MBGCN methodology. Section III presents the results of the experimental verification. Finally, the conclusion and future work are drawn in Section IV.

II. METHODOLOGY

In this section, the framework structure of MBGCN is presented in Fig. 1. MBGCN consists of four parts: graph construction algorithm, sub-block division, sub-block GCN network modeling and sub-block performance Bayesian fusion.

A. KNN and GAE based GRAPH CONSTRUCTION

Industrial process data signals are generally one-dimensional data, which need to be transformed into graph structured data using graph construction algorithms. GNN can be used to extract features from graph data. Defining a graph as $G = (X,\ A)$, where $X \in R^{N*M}$ is the node feature data, and $X \in R^{N*N}$ is the adjacency matrix, *N* is the number of samples and *M* is the number of variables.

Let $v_i \in V$ denote the node and $e_{(i,j)} \in E$ denote the edge between v_i and v_j. It should be emphasized that the graph data in this study are undirected graphs. Then the adjacency matrix $a_{(i,j)} \in A$ can be obtained via Eq. (1)

$$a_{(i,j)} = \begin{cases} 1, & if\ e_{(i,j)} \in E \\ 0, & if e_{(i,j)} \notin E \end{cases} \#(1)$$

where $a_{(i,j)}$ indicates whether v_j is a neighbor of v_j or not. As shown in Eq. (1), $a_{(i,j)} = 1$ if $e_{(i,j)} \in E$, which means that there is an edge between v_i and v_j. Contrarily, if $e_{(i,j)} \notin E$, which means that v_j is not a neighboring node of v_j, then $a_{(i,j)} = 0$.

There are two common approaches for graph construction, one is unsupervised combination by measuring joint feature statistics, the other is supervised combination by using initial network as a proxy for the estimation[19]. The k-nearest neighbors graph is an unsupervised synthetic method based on sample statistics. It can restrict the number of nearest neighbor to a limited number and the construction process is simple and efficient. The k-nearest neighbors graph is constructed by using all samples as nodes in a nearest neighbors graph. The connectivity between the samples is measured by the distance between the samples, which can efficiently extract the correlation between the samples. Assuming that $x_i \in X$ is the *i*th sample in the set of samples, the Mahalanobis distance between $x_i$and x_j is computed as follows:

$$dist(x_i, x_j) = \sqrt[2]{(x_i - x_j)^T S^{-1}(x_i - x_j)} \#(2)$$

where *S* is the covariance of the process data.

An edge exists between $x_i$and x_j if the sample x_j is one of the k nearest neighbors of x_i, which means $a_{(i,j)} = 1$. Finally, the adjacency matrix *A* is obtained. There is no fixed rule for the selection of the nearest neighbor parameter *k*. In this study, *k* is set to 2.

Compared with the Euclidean distance, the Mahalanobis distance can exclude the interference of correlation between variables, which is often correlated in industrial process data. The Mahalanobis distance can obtain sample connectivity based on sample similarity, but the hidden connectivity between samples cannot be obtained. Thus, it is meaningful to reconstruct the adjacency matrix A via graph autoencoder (GAE) model[20]. GAE extends the concept of AE to graph-structured data and is primarily used for link prediction problems on graphs. In this study, GAE is used to extract the connectivity relationships between nodes automatically. The encoding layer of GAE employs graph convolution to aggregate the neighboring node features for updating the node's hidden-layer presentation as follows:

$$H^{(i)} = \sigma\left(\widetilde{D}^{-\frac{1}{2}}\tilde{A}\widetilde{D}^{-\frac{1}{2}}H^{(i-1)}W^{(i)}\right) \#(3)$$

where $H^{(i)}$ is the feature matrix of the *i*th layer when *i*=1, the input feature $H^{(i-1)} = X$ is the sample feature data. $\tilde{A} = A + A_n$ means self-connecting (i.e., unit matrix A_n) is added to the adjacency matrix A, $\widetilde{D}$ is the degree matrix of $\tilde{A}$, in which $\widetilde{D}_{ij} = \sum_j \tilde{A}_{ij}$, $W^{(i)}$ is the trainable parameter, and $\sigma(\cdot)$ denotes the LeakyRelu activation function. In this study, GAE encoding layer consists of 2 graph convolution layers, which can be defined as follows:

$$Z = f(X, A) = \widetilde{D}^{-\frac{1}{2}}\tilde{A}\widetilde{D}^{-\frac{1}{2}}LeakyRelu\left(\widetilde{D}^{-\frac{1}{2}}\tilde{A}\widetilde{D}^{-\frac{1}{2}}XW^{(1)}\right)W^{(2)} \#(4)$$

where *Z* denotes the output representation of the GAE encoding layer.

After the encoding process, the adjacency matrix *A* is reconstructed as follows:

$$\hat{A} = \varphi(ZZ^T) \#(5)$$

where $\hat{A}$ is the reconstructed adjacency matrix, *Z* is the output of the encoding layer, and *φ* is the sigmoid activation function. In this way, industrial fault data is transformed into graph-structured data $G = (X,\ \hat{A})$.

B. SUB-BLOCK PARTITIONING by PEARSON'S CORRELATION COEFFICIENT

Pearson's correlation coefficient measures the

correlation between two variables. Variables with high correlation coefficients are grouped together to form a sub-block. Variables within the sub-block share similar information and exhibit more localized characteristics. Let the $x_{,i}$ denote the *i*th variable of the sample data, then the correlation coefficient between the $x_{,i}$ and $x_{,j}$ can be expressed as:

$$r(x_{,i}, x_{,j}) = \frac{\sum_{p=1}^{n}(x_{p,i} - \bar{X}_{,i})\sum_{q=1}^{n}(x_{q,j} - \bar{X}_{,j})}{\sqrt{\sum_{p=1}^{n}(x_{p,i} - \bar{X}_{,i})^2 \sum_{q=1}^{n}(x_{q,j} - \bar{X}_{,j})^2}} \quad \#(6)$$

where $x_{p,i}$ is the value of the *i*th variable in the *p*th sample and $\bar{X}_{,i} = \frac{1}{n}\sum x_{p,i}$ is the mean value of $x_{,i}$. The value of $abs(r(x_{,i}, x_{,j}))$ is greater when the correlation between $x_{,i}$ and $x_{,j}$ is greater. On the contrary, the lower correlation between the two variables, the value of $abs(r(x_{,i}, x_{,j}))$ is closer to 0. The threshold is set to 0.8. $x_{,i}$ and $x_{,j}$ are divided into the same sub-block when $abs\left(r(x_{,i}, x_{,j})\right) > 0.8$.

Finally, the sample data are divided into *B* sub-blocks, which can be denoted as $X = [X_1, X_2, \cdots, X_B]$, where B is the number of sub-blocks, $X_b \in R^{n*m_b}$ has n samples, and m_b variables. In this study, the normal dataset is used to divide sub-blocks to ensure that all fault data can be categorized into the same sub-blocks.

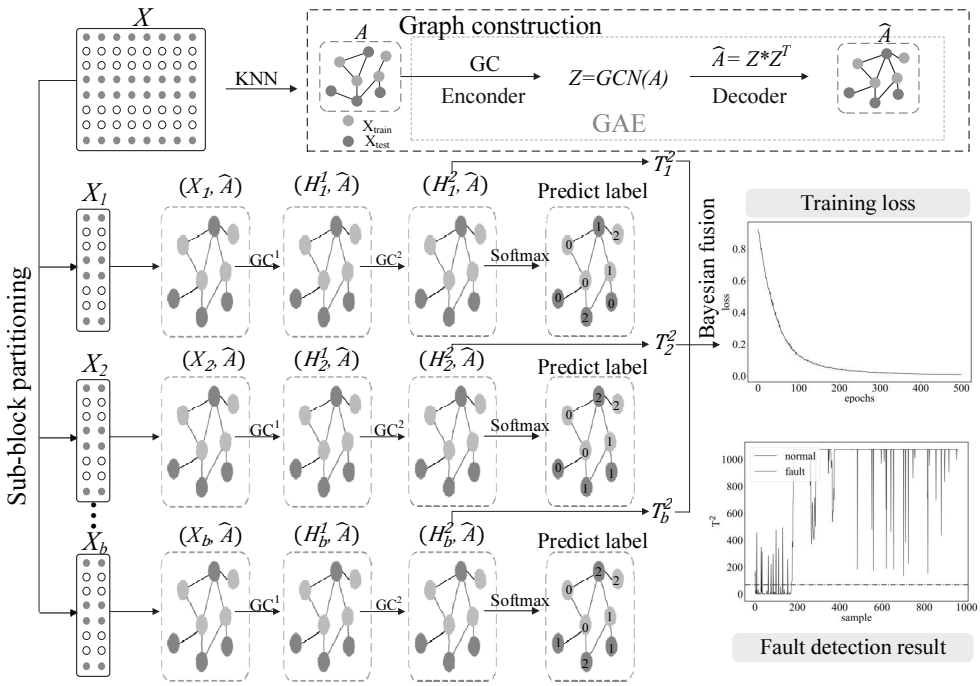


Figure 1 The network structure of MBGCN

C. SUB-BLOCK GCN MODELING

By sub-block partitioning, the sub-block graph structure data $G_b = (X_b, \hat{A})$ is generated. As shown in Fig. 1, the sub-block graph data is input into the GCN[21] model. The graph convolutional layers aggregate the fault features using the following equation:

$$H_b^{(2)} = f(X_b, \hat{A}) = \widehat{D}^{-\frac{1}{2}}\hat{A}\widehat{D}^{-\frac{1}{2}} LeakyRelu\left(\widehat{D}^{-\frac{1}{2}}\hat{A}\widehat{D}^{-\frac{1}{2}} X_b W^{(1)}\right) W^{(2)} \quad \#(7)$$

As shown in Eq. (7), the GCN model in this paper consists of two layers, with Z_b representing the output of the second graph convolutional layer. Then the sigmoid classifier is used to discriminate the labels of the nodes.

In this study, the input sample data consists of only one class of faulty and normal samples, so unlabeled nodes will ultimately be classified as either normal or faulty. In order to train the parameters $W^{(i)}$ of graph convolution, the cross entropy loss function is used as the objective function. The weight parameters of the GCN are updated by backpropagation. The cross-entropy is expressed as:

$$Loss = -\sum_{i \in V_{label}} \sum_{j=1}^{c} Y_{ij} \ln(Y'_{ij}) \quad \#(8)$$

where Y_{ij} is the real label of the *i*th labelled sample, Y'_{ij} is the predicted label of the *i*th unlabeled samples, and V_{label} is the set of labeled samples. In fault detection, labeled samples is the training data, which only conclude normal samples.

Only normal process data are used to construct GCN model for process fault detection by obtaining the extracted features $H_b^{(2)}$ of the graph convolutional network via Eq. (7). The Hotelling squared (T^2) statistic can be defined as follows:

$$T_b^2 = \left(H_b^{(2)} - \overline{H_b^{(2)}}\right)^T \Sigma^{-1} \left(H_b^{(2)} - \overline{H_b^{(2)}}\right) \#(9)$$

where $H_b^{(2)}$ is the extracted features of the *b*th sub-block, and $\overline{H_b^{(2)}}$ and Σ are denoted as the mean and covariance of $H_b^{(2)}$.

The control limits are calculated by kernel density estimation (KDE)[22] with a confidence level of α. The KDE with Gaussian kernel function for T_b^2 can be written as:

$$K(T_b^2) = \frac{1}{\sqrt{2\pi}n\omega} \sum_{i=1}^{n} \frac{\left(T_b^2 - T_{b,i}^2\right)^2}{2\omega^2} \#(10)$$

where ω is bandwidth, $T_{b,i}^2$ is the *i*th value of T_b^2.

Then, the threshold of block *b* $T_{b,thr}^2$ can be obtained when the T^2 presents a 95% confidence level. Fault Detection Rate (*FDR*) and False Alarm Rate (*FAR*) are commonly used metrics for evaluating the monitoring performance of a model. *FDR* and *FAR* are defined as follows:

$$FDR = \frac{number\ of\ detected\ faulty\ samples}{number\ of\ total\ faulty\ samples} \#(11)$$

$$FAR = \frac{number\ of\ normal\ samples\ detected\ as\ faults}{number\ of\ total\ normal\ samples} \#(12)$$

Typically, a larger *FDR* and a smaller *FAR* indicate better performance of the monitoring model.

D. BATYESIAN FUSION

After obtaining T_b^2 and $T_{b,thr}^2$ for each sub-block, the next step is to decide if there are faulty samples in the process data. Every sample is monitored differently in different sub-blocks so as to get a fused result. Bayesian fusion is a commonly used fusing method based on probabilistics. Assuming that the test sample $x_{test} \in X_{test}$, the conditional failure probability of this sample in the *i*th sub-block $P_{T_i^2}\left(F \middle| x_{test,i}\right)$ can be obtained based on the T_i^2 and $T_{b,thr}^2$ of the *i*th sub-block as follows:

$$P_{T_i^2}\left(F \middle| x_{test,i}\right) = \frac{P_{T_i^2}\left(x_{test,i} \middle| F\right) P_{T_i^2}(F)}{P_{T_i^2}\left(x_{test,i} \middle| N\right) P_{T_i^2}(N) + P_{T_i^2}\left(x_{test,i} \middle| F\right) P_{T_i^2}(F)} \#(13)$$

$x_{test,i}$ denotes the test sample in the *i*th sub-block, and $P_{T_i^2}(N)$ and $P_{T_i^2}(F)$ are the prior probabilities of the normal and faulty samples, with confidence levels α and $1-\alpha$ respectively. $P_{T_i^2}\left(x_{test,i} \middle| N\right)$ and $P_{T_i^2}\left(x_{test,i} \middle| F\right)$ are defined as follows:

$$P_{T_i^2}\left(x_{test,i} \middle| N\right) = e^{-\frac{T_{i,new}^2}{T_{i,thr}^2}} \#(14)$$

$$P_{T_i^2}\left(x_{test,i} \middle| F\right) = e^{-\frac{T_{i,thr}^2}{T_{i,new}^2}} \#(15)$$

where $T_{i,new}^2$ denotes the T^2 statistic of the new sample in the *i*th sub-block and $T_{i,thr}^2$ is the control limit of the *i*th sub-block.

Finally, the conditional probability $P_{T_i^2}\left(x_{test,i} \middle| N\right)$ and $P_{T_i^2}\left(x_{test,i} \middle| F\right)$ are used as the weights to calculate the probability of the test sample x_{test} being faulty sample in the fusion model. BIC_{T^2} is the probability that the test sample x_{test} is faulty, which can be calculated by Eq. (16):

$$BIC_{T^2} = \sum_{i=1}^{B} \left\{ \frac{P_{T_i^2}\left(x_{test,i} \middle| F\right) P_{T_i^2}\left(F \middle| x_{test,i}\right)}{\sum_{j=1}^{B} P_{T_j^2}\left(x_{test,j} \middle| F\right)} \right\} \#(16)$$

After getting the final fusion statistic BIC_{T^2}, KDE is used to estimate the control limit $BIC_{T^2,\mathrm{thr}}$ of the fusion model. When $BIC_{T^2} > BIC_{T^2,\mathrm{thr}}$, then the test sample is judged as a faulty sample, otherwise it is a normal sample.

E. APPLICATION PROCEDURES of MBGCN

The application procedures in process fault detection and diagnosis of MBGCN is presented in Fig. 2. The offline modeling procedure is listed as follows:

Step 1: The training dataset X_{train} is obtained and

normalized;

Step 2: Using the dataset X_{train}, calculate the Mahalanobis distance between each pair of samples use eq. (2). Then get the graph-construction data $G = (X, A)$. Input A into GAE model to obtain the reconstructed $\hat{A}$;

Step 3: Calculate the Pearson correlation coefficient between each pair of variables to perform process division.

Step 4: Input $X_{train,\ b}$ and $\hat{A}$ into trained sub-block GCN model. First, obtain the extracted features $H^{(2)}_{train,b}$ then calculate $T^2_{train,b}$ statistic by eq. (9) and the threshold $T^2_{thr,b}$ for each sub-block is determined using KDE.

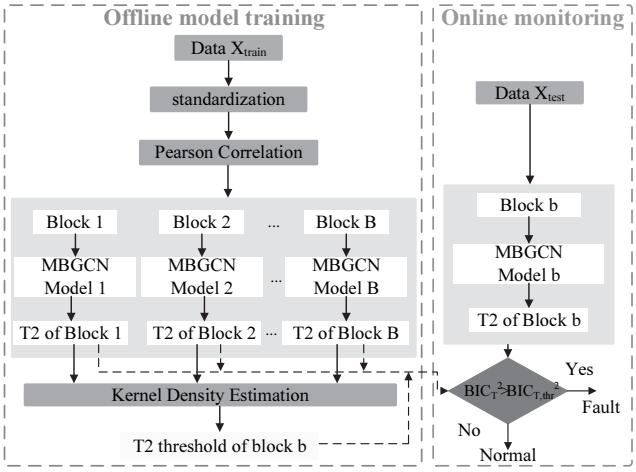


Figure 2 Application procedures of MBGCN.

The online modeling procedure is listed below:

Step 1: The online test dataset X_{test} is obtained and divide the variables into blocks based on the outcomes of offline modeling step 3;

Step 2: Input $X_{test,\ b}$ and into trained sub-block GCN model. Calculate $T^2_{test,b}$ through the extracted features $H^{(2)}_{test,b}$ by eq. (9).

Step 3: Define the significance level α and combine the outcomes of all sub-blocks through Bayesian fusion to obtain the composite index BIC_{T^2} and $BIC_{T^2,\mathrm{thr}}$;

Step 4: If $BIC_{T^2} > BIC_{T^2,\mathrm{thr}}$, the test sample is judged as a faulty sample, otherwise it is a normal sample. Calculate the FDR and FAR through eq. (11) and eq. (12)

III. CASE STUDY AND EXPERIMENTAL

In this section, the Tennessee Eastman process (TEP)[23] is considered to verify the effectiveness of MBGCN in process fault diagnosis and detection. TEP is a simulation system based on actual chemical processes, which is a commonly used benchmark in process monitoring. As show in figure 3, TEP contains five working units: a reactor, a product condenser, a vapor-liquid separator, a recycle compressor, and a product stripper. In this section, all 21 faults and 52 variables are used to validate the performance of MBGCN for process fault diagnosis and detection. Additional details of the TE process can be found in the reference[24] and reference [25].

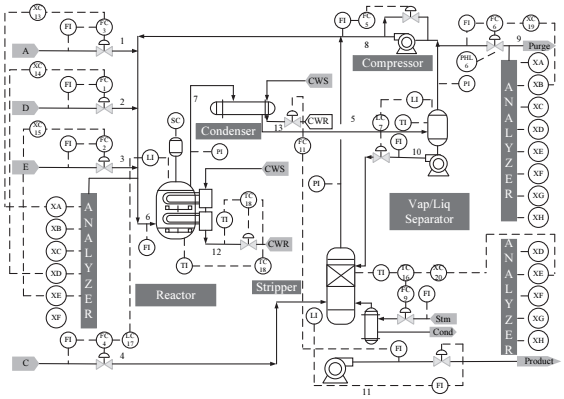


Figure 3 The schematic of TE process.

To build the multiblock model, the Pearson correlation coefficient between every pair of variables is calculated. The entire set of process variables is divided into nine sub-blocks: eight typical blocks and one unknown block. The variables in each sub-block are listed in Table 1.

Table 1 Blocks division results of the TE process.

Block no.	Variable no.	Block no.	Variable no.
1	1, 44	6	17, 52
2	7, 13, 16	7	18, 19, 50
3	10, 47	8	20, 46
4	12, 48	9	The rest of variables
5	15, 49		

A. FAULT DIAGNOSIS PERFORMANCE

Firstly, verify the multi-fault classification results of the MBGCN model. The classification results of 9 sub-blocks are shown in Table 1. From Table 1, it can be seen that sub-block 9 has the best fault diagnosis result, which is due to the fact that the more variables, the more information that data contains about all fault characteristics. The fault diagnosis result of the first 8 sub-blocks after sub-block division is poor, but different sub-blocks are sensitive to different fault

types. For example, in sub-block 1, faults 1 and 6 are well categorized, which indicates that faults 1 and 6 are mainly influenced by the variables in sub-block 1. The variables in sub-block 1 are A feed (Stream 1) and A feed flow (Stream 1). Fault 1 is mainly induced by a change in the ratio of A and C feed, and the material A feed flow in sub-block 1 is an operating variable. This indicates that the change in the A feed flow leads to the change in the ratio of A and C feed, which ultimately leads to the appearance of fault 1. The results align with the actual situation, which suggests that sub-block partitioning can help isolate specific variables that are sensitive to specific fault.

Table 2 9 Sub-blocks Classification accuracy (%).

Category	Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7	Block 8	Block 9	MAX
Fault 1	99.47	0	68.35	0	0	0	93.38	2.89	**100**	100
Fault 2	72.00	0	**99.12**	59.25	0	92.43	95.51	0	98.55	99.12
Fault 3	0	0	0	**49.41**	0	0	0	0	21.66	49.41
Fault 4	21.75	5.76	16.65	0	50.34	67.14	20.13	0	**91.21**	91.21
Fault 5	0	0	21.19	42.10	7.98	**57.93**	0	0	11.04	57.93
Fault 6	99.46	98.21	86.18	0	91.57	87.35	96.99	95.00	**100**	100
Fault 7	0	0	0	0	0	18.49	0	0	**100**	100
Fault 8	12.28	0	51.24	0	0	62.67	0	0	**88.28**	88.28
Fault 9	0	**100**	34.68	0	0	0	0	0	36.71	100
Fault 10	0	0	0	0	0	20.67	8.49	0	**32.11**	32.11
Fault 11	0	0	0	0	0	46.13	0	0	**50.69**	50.69
Fault 12	0	4.16	0	60.00	0	38.13	3.13	0	**97.85**	97.85
Fault 13	0	30.99	13.62	0	0	0	39.87	55.61	**100**	100
Fault 14	0	0	0	0	0	0	0	0	**100**	100
Fault 15	65.20	0	0	48.00	0	0	**70.93**	0	27.22	70.93
Fault 16	0	3.12	0	0	0	**61.02**	0	0	0	61.02
Fault 17	0	0	0	0	0	59.35	0	0	**80.25**	80.25
Fault 18	82.19	82.76	75.85	0	0	28.24	78.46	75.68	**87.84**	87.84
Fault 19	0	0	0	0	0	45.97	0	0	**90.76**	90.76
Fault 20	0	43.93	0	0	47.82	0	0	**50.91**	0	50.91
Fault 21	0	**82.35**	0	0	0	39.66	0	0	9.22	82.35
Avg.	21.54	21.49	22.23	12.32	9.41	34.53	24.14	13.34	63.02	80.51

In this section, the fault diagnosis performance of MBGCN is compared with PCA[26], Typical LSTM[27], Optimized LSTM[28], Autoencoder[29], BPN[30], and SVM[31] models, and the results are shown in Table 3. Among the diagnosis results of 21 faults, the MBGCN obtained the highest correct rate of 80.51%. Although MBGCN achieved the highest correct rate in only 8 faults, the best diagnostic results were achieved in the more faults 9 and 15, which are difficult to diagnosis, and the diagnostic rate for fault 9 was up to 100%. This also illustrates that sub-block partitioning can separate variables that are sensitive to specific faults. With MBGCN, it is possible to extract fault information for diagnosis using a small number of variables.

Table 3 Comparison between the proposed method with other FDD methods

Category	PCA	Typical LSTM	Optimized LSTM	Autoencoder	BPN	SVM	MBGCN(BEST)
Fault 1	**100.00**	9.00	68.00	98.00	97.27	**100**	**100**
Fault 2	79.00	12.00	74.00	85.00	**100**	**100**	99.12
Fault 3	18.33	3.00	45.00	**91.00**	11.30	9.57	49.41
Fault 4	**96.88**	4.00	75.00	89.00	5.47	78.91	91.21
Fault 5	**96.88**	20.00	89.00	93.00	67.20	90.40	57.93
Fault 6	99.48	34.00	1.00	85.00	**100**	**100**	**100**
Fault 7	99.27	19.00	89.00	80.00	**100**	**100**	**100**
Fault 8	94.90	22.00	71.00	73.00	91.97	**100**	88.28
Fault 9	20.21	1.00	67.00	76.00	17.46	4.76	**100**
Fault 10	**87.81**	28.00	77.00	79.00	41.96	23.21	32.11
Fault 11	77.81	12.00	83.00	**93.00**	26.14	38.64	50.69
Fault 12	97.81	31.00	56.00	91.00	94.40	100	**97.85**
Fault 13	79.17	22.00	89.00	78.00	95.69	99.14	**100**
Fault 14	98.23	41.00	99.00	1.00	47.37	100	**100**
Fault 15	23.02	1.00	0	33.00	0	5.98	**70.93**
Fault 16	69.48	12.00	0	**89.00**	27.56	44.09	61.02
Fault 17	74.47	24.00	20.00	89.00	0	**95.16**	80.25
Fault 18	59.90	31.00	88.00	95.00	76.38	**96.06**	87.84
Fault 19	84.06	17.00	**91.00**	64.00	0	86.92	90.76
Fault 20	77.50	28.00	64.00	83.00	0	**92.65**	50.91
Fault 21	**85.00**	-	-	-	63.03	33.61	82.35
Avg.	77.11	18.55	62.30	78.25	50.63	72.26	**80.51**

B. FAULT DETECTION PERFORMANCE

From the results of fault diagnosis, it can be seen that the sub-blocks of MBGCN are more sensitive to single faults. Then, validating the fault detection performance of the model. The training process of MBGCN is exhibited in Fig 4. It can be observed that

MBGCN has strong enforceability as it converges after several rounds of training.

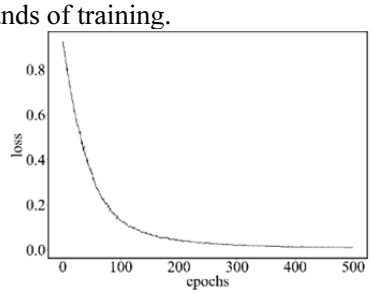


Figure 4 Training process of MBGCN

The fault detection results of block 1 of fault 1 is presented in Fig. 5. In this figure, the blue dots represent the normal samples and the red dots represent the fault samples. Dashed lines indicate control limit. It can be seen that the fault is detected at the 170st point. This indicates that there is a lag in the detection effect of MBGCN, this is the reason FDR is hard to 100%.

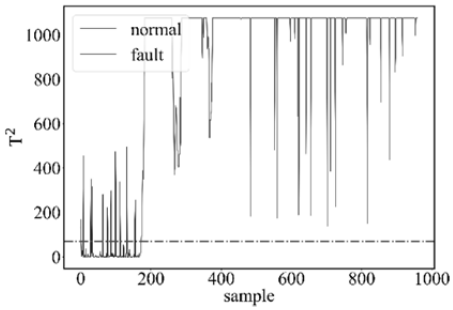


Figure 5 Fault detection result of block 1 of fault 1.

The fault detection results of fusion model of fault 1 is presented in Fig. 6. After Bayesian fusion, the fault is detected at the 164st point, it means Bayesian fusion can effectively mitigate the lag in model detection.

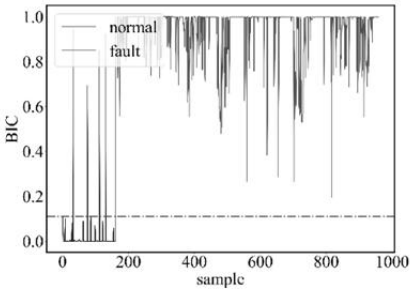


Figure 6 Fault detection result of BIC of fault 1.

Next, the detection effectiveness of 21 faults is tested and the results are listed in Table 4. In the MBGCN, the FDR of BIC reaches 82.8% while the FAR is only 2%, and BIC achieves more than 95% fault detection rate in six faults. Notably, sub-block 6 possesses the best detection results in fault 5, fault 7, fault 8, fault 10, fault 12, fault 13, fault 16, fault 17 and fault 19. The sub-block 6 is also the best-classification sub-block except for the largest sub-block 9 in fault 5, fault 7, fault 8, fault 10, fault 16, fault 17, and fault 19 in the fault diagnosis results. This also shows that the sub-block partitioning in this study can extract the variables that are sensitive to the specific faults.

Table 4 FDR/FAR of MBGCN (%).

Category	Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7	Block 8	Block 9	BIC
Fault 1	98.6/1.9	43.3/0	34.2/0	0/0	0/0	93/0	22.8/0	51.8/0	2.9/0	**99.1/2.7**
Fault 2	12.6/0	74.4/0	96.5/0.1	0.3/0	0/0	86.5/0.1	54.2/0	66.6/0	2.7/0	**97.4/0**
Fault 4	0/0	12.4/0	0.3/0	0/0	8.3/1.8	47.9/0	0.1/0	9.5/0	90.3/0	**95.2/3.8**
Fault 5	4/0	20.5/0	8.9/0	0.1/0	0.8/0	72/0.9	36.2/2.7	25.1/0.9	5.8/0	**81.3/0.6**
Fault 6	94/0	91.4/0	89.1/0	0/0	0/0	8.1/0	93.9/0	93.7/0	22/0	**99.6/0**
Fault 7	30.9/0	41.1/0.1	10.9/0	0/0	0/0	84.5/0.1	40.6/0	23.1/0	74.3/3.6	**90/6.8**
Fault 8	43.2/0	78.4/0	73.4/0	1.3/0	2.2/0	79.9/0	74.1/0	34/0	8.1/0	**96.8/3.1**
Fault 10	10.8/0	8/0	0.2/0	0.1/0	0.1/0	**81.8/1.8**	61.2/0.1	34.3/2.7	4.6/0	79.1/3.6
Fault 11	2.9/0	0.2/0	0/0	0.3/0	0.7/0	49.1/0	55.2/2.7	13.1/0	2.1/0	**56.6/2.3**
Fault 12	31.2/0	34.1/0	22.6/0	2.2/0	2/0	**94.5/1.8**	51.4/0	34.7/0	20.5/0	93.3/1.7
Fault 13	30.6/0	80.9/1.8	48.2/0	2.2/0	0.1/0	**95.8/0.9**	88.8/1.2	33.2/1.8	45.9/0.9	92.3/2.1
Fault 14	5.1/0	1.8/0	1.4/0	0.7/0	0/0	38.1/0.9	10.6/0	3.6/0	92/0.2	**95.8/2.1**
Fault 16	3.5/0	20.9/0	13.2/0	0.1/0	0/0	88.6/0	7.5/0	12.4/0.9	3.6/0	**90.6/1.4**
Fault 17	0.2/0	9.8/0	0.5/0	0.9/0	0.5/0	**44.6/0**	32/0	28.4/0	25.1/0.9	37.9/0.6
Fault 18	80.5/0	79.9/2.7	77.2/7.2	0.1/0	0.1/1.8	86.4/2.7	91.6/11.8	81.1/0.7	0/0	**89.1/2.1**
Fault 19	5.8/0	6.8/0	0.4/0	0.1/0	0/0	52/1.8	28.6/0	0/0	0.9/0	**52.3/1.1**
Fault 20	17.1/0	46.7/0	4.5/0	0.4/0	0/0	43.5/0	**79.1/0.9**	54.4/0.9	2.9/0.9	78.6/1.3
Fault 21	0.7/0	29.6/0	0.2/0	0.8/0	0/0	55.5/0	**70.6/6.3**	26.9/0	12.8/0	66/1.2
Avg.										82.8/2.0

Table 5 shows MBGCN compared with PCA, CAE, GDAE, DBN, GAN, MBPCA, and MBCAE models. MBPCA and MBCAE are the BIC statistics after using the sub-block partitioning of this study. It is worth noting that fault 3, 9 and15 are not considered as they are extremely difficult to detect. For the remaining 18 faults, MBGCN get the highest FDR and lowest FAR only in 5 faults, but get the best overall performance in terms of average FDR and FAR. Among the three sub-block models, MBGCN has the best detection results, which indicates that using GNN can extract the correlation between the samples and thus enhance the

detection effect of the model. Meanwhile, both MBPCA and MBCAE have better detection results than PCA and CAE, which means that the sub-block partitioning in this study can enhance the fault detection rate of the model.

Table 5 FDR/FAR of MBGCN and other fault detect models (%).

Category	PCA (T^2)	CAE (T^2)	GDAE (T^2)	DBN(T^2)	GAN(T^2)	MBPCA(BIC)	MBCAE(BIC)	MBGCN(BIC)
Fault 1	99.3/0.6	99.5/3.1	99.8	99/1	100/3	99.4/3.8	99.6/18.1	99.1/2.7
Fault 2	98.5/0.6	98.5/1.9	98.6/5.6	98/2	99	98.5/2.5	98.8/13.8	97.4/0
Fault 4	27.8/0.6	44.2/0.6	100/0.6	9/1	56/6	100/4.1	26/13.8	95.2/3.8
Fault 5	23.8/0.6	26.7/0.6	40.9/0.6	22/1	32/6	27/3.1	46.1/13.8	**81.3/0.6**
Fault 6	98.8	99	100	99/2	100	88.1/0	100/7.5	99.6/0
Fault 7	100	100	100/4.4	100/3	100	100/0	56.8/8.1	90/6.8
Fault 8	97.3	97.5/1.9	98.4/1.9	94/1	98	97.4/1.9	98.2/13.1	96.8/3.1
Fault 10	23.4	35.7/0.6	60.1	18/3	51	23.5/2.5	62.3/10	**79.1/3.6**
Fault 11	45	50.4/1.3	73/0.6	35/1	58/6	78.6/0.6	60.1/21.9	56.6/2.3
Fault 12	98.4	99/1.9	100/18.1	92/2	99/13	98.8/4.4	99.6/23.8	93.3/1.7
Fault 13	94.5/1.3	94.25/0.6	95.6/2.5	88/2	95/2	68.6/0	96.2/10	92.3/2.1
Fault 14	98.9	99.62/0.6	100/1.3	93/2	100/2	92.8/0	89.1/14.4	95.8/2.1
Fault 16	11/3.1	17.9/5.0	44.1/35.0	4/2	34/20	55.3/16.9	50.6/53.1	**90.6/1.4**
Fault 17	75.9	79.9/1.9	94.25	64/1	91/2	47.1/0	75.9/14.4	37.9/0.6
Fault 18	89/0.6	89/3.8	91	88/3	90/2	91/2.5	93.4/15.6	89.1/2.1
Fault 19	6.3	8.2/0	5.3/8.8	16/2	12/1	63/2.5	41.4/16.9	52.3/1.1
Fault 20	27.9	35.9/0	68.4	43/1	58/0	70.3/0	55/10.6	**78.6/1.3**
Fault 21	39.5	38.4/1.3	48.3/3.8	37/1	50/6	62.6/1.3	53.8/26.2	**66/1.2**
Avg.	64.2/0.4	67.4/1.4	78.8/4.6	78.6/1.7	73.5/3.1	75.7/3.1	72.4/16.9	**82.8/2.0**

IV. CONCLUSION AND FUTURE WORK

This paper proposed a multi-block graph convolutional neural network for distributed process monitoring in complex industrial processes. This approach involves constructing a graph structure to depict the complex relationships among process data. Moreover, the process is separated into sub-blocks using the Pearson correlation coefficient. Graph convolutional neural network is utilized to learn informative feature embeddings for developing monitoring statistics. Finally, the monitoring result of each sub-block is fused via Bayesian inference to achieve global process monitoring. The experimental results on TE process have verified the effectiveness of MBGCN. MBGCN obtains better process monitoring results compared with the state-of-art methods. Future work would focus on exploring the evolving mechanism among different sub-blocks to further enhance the interpretability of the model.

References

[1] YIN S, DING S X, XIE X C, et al. A review on basic data-driven approaches for industrial process monitoring[J]. IEEE Transactions on Industrial Electronics, 2014, 61(11): 6418-6428.

[2] CHEN J H, LIAO C M. Dynamic process fault monitoring based on neural network and PCA[J]. Journal Process Control, 2002, 12: 277–289.

[3] LI Z C, YAN X F. Fault-relevant optimal ensemble ICA Model for Non-Gaussian Process Monitoring[J]. IEEE Transactions on Control Systems Technology, 2020, 28(6): 2581-2590.

[4] Cao Y P, Hu Y P, Deng X G, et al. Quality-relevant batch process fault detection using a multiway multi-subspace CVA Method[J]. IEEE Access, 2017, 5: 23256-23265.

[5] ZHANG Y W, ZHOU H, QIN S J, et al. Decentralized fault diagnosis of large-scale processes using multiblock kernel partial least squares[J]. IEEE Transactions on Industrial Informatics, 2010, 6(1): 3-10.

[6] ZHU J L, GE Z Q, SONG Z H, et al. Distributed parallel PCA for modeling and monitoring of large-scale plant-wide processes with big data[J]. IEEE Transactions on Industrial Informatics, 2017, 13(4): 1877-1885.

[7] ZENG J, HUANG W P, WANG Z Y, et al. Mutual information-based sparse multiblock dissimilarity method for incipient fault detection and diagnosis in plant-wide process[J]. Journal of Process Control, 2019, 83: 63-76.

[8] JIANG Q, YAN X, Plant-wide process monitoring based on mutual information–multiblock principal component analysis[J]. ISA Transactions, 2014, 53(5): 1516-1527.

[9] JIANG Q C, YAN X F, Nonlinear plant-wide process monitoring using MI-spectral clustering and Bayesian inference-based multiblock KPCA[J]. Journal of Process Control, 2015, 32: 38-50.

[10] TIAN Y, YAO H, LI Z, Plant-wide process monitoring by using weighted copula–correlation based multiblock principal component analysis approach and online-horizon Bayesian method[J]. ISA Transactions, 2020, 96: 24-36.

[11] YAO Z Y, JIANG Q C, GU X S, Distributed process monitoring based on kantorovich distance-multiblock variational autoencoder and Bayesian inference, Chinese Journal of Chemical Engineering, 2024.

[12] HE Y M, SHI H B, TAN S, et al. Multiblock temporal convolution network-based temporal-correlated feature learning for fault diagnosis of multivariate processes[J]. Journal of the Taiwan Institute of Chemical Engineers, 2021, 122: 78-84.

[13] ZHU J Z, SHI H B, SONG B, et al. Convolutional neural network based feature learning for large-scale quality-related process monitoring[J]. IEEE Transactions on Industrial Informatics, 2022, 18(7): 4555-4565.

[14] M. Defferrard, X. Bresson, and P. Vandergheynst, Convolutional neural networks on graphs with fast localized spectral filtering[C]. Proc. Adv. Neural Inf. Process. Syst., 2016, 29: 3837–3845.

[15] Zhang Y, YU J, Pruning graph convolutional network-based feature learning for fault diagnosis of industrial processes[J]. Journal of Process Control, 2022, 113: 101-113.

[16] REN H, LIANG X J, YANG C H, et al. Spatial-temporal associations representation and application for process monitoring using graph convolution neural network[J]. Process Safety and Environmental Protection, 2023, 180: 35-47.
[17] LI S Z, MENG W C, HE S B, et al. STAGED: A spatial-temporal aware graph encoder–decoder for fault Diagnosis in industrial processes[J]. IEEE Transactions on Industrial Informatics, 2024, 20(2): 1742-1752.
[18] ZHANG W, GAO Y P, WANG J Z, et al. Distributed dynamic graph embedding for quality-related monitoring in the flotation process[J]. IEEE Transactions on Instrumentation and Measurement, 2024, 73: 1-11.
[19] Mikael H, Joan B, Yann L. Deep convolutional networks on graph-structured data [J]. arxiv preprint arxiv:1506.05163, 2015.
[20] Kipf T N, Welling M. Variational graph auto-encoders[J]. arxiv preprint arxiv:1611.07308, 2016.
[21] Kipf T N, Welling M. Semi-supervised classification with graph convolutional networks[J]. arxiv preprint arxiv:1609.02907, 2016.
[22] Frosst N, Hinton G. Distilling a neural network into a soft decision tree[J]. arxiv preprint arxiv:1711.09784, 2017.
[23] Onel M, Kieslich C A, Guzman Y A, et al. Simultaneous fault detection and identification in continuous processes via nonlinear support vector machine based feature selection[M]//Computer Aided Chemical Engineering. Elsevier, 2018, 44: 2077-2082.
[24] Downs J J, Vogel E F. A plant-wide industrial process control problem[J]. Computers & chemical engineering, 1993, 17(3): 245-255.
[25] Lyman P R, Georgakis C. Plant-wide control of the Tennessee Eastman problem[J]. Computers & chemical engineering, 1995, 19(3): 321-331.
[26] Li W, Yue H H, Valle-Cervantes S, et al. Recursive PCA for adaptive process monitoring[J]. Journal of process control, 2000, 10(5): 471-486.
[27] Tax N, Verenich I, La Rosa M, et al. Predictive business process monitoring with LSTM neural networks[C]. Advanced Information Systems Engineering: 29th International Conference, CAiSE 2017, Essen, Germany, June 12-16, 2017, Proceedings 29. Springer International Publishing, 2017: 477-492.
[28] Kaselimi M, Doulamis N, Doulamis A, et al. Bayesian-optimized bidirectional LSTM regression model for non-intrusive load monitoring[C]. ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2019: 2747-2751.
[29] Lee S, Kwak M, Tsui K L, et al. Process monitoring using variational autoencoder for high-dimensional nonlinear processes[J]. Engineering Applications of Artificial Intelligence, 2019, 83: 13-27.
[30] Hecht-Nielsen R. Theory of the backpropagation neural network[M]. Neural networks for perception. Academic Press, 1992: 65-93.
[31] Yin Z, Hou J. Recent advances on SVM based fault diagnosis and process monitoring in complicated industrial processes[J]. Neurocomputing, 2016, 174: 643-650.

About the authors

Xufei.Chen, received the B.Eng. degree from the school of Mechanical Engineering, Tongji University, Shanghai, China, in 2022. He is currently a M.D. degree candidate in the department of Industrial Engineering, at Tongji University, Shanghai, China. His current research interests include process fault diagnosis and machine learning. (Email: 2232708@tongji.edu.cn)

Shijin Li, received the B.Eng. degree from the school of Mining Engineering, China University of Mining and Technology, Jiangsu, China, in 2021. She is currently a Ph.D. degree candidate in the department of Industrial Engineering, at Tongji University, shanghai, China. Her current research interests include process fault diagnosis and machine learning. (Email: 2111049@tongji.edu.cn)

Jianbo Yu, received the B.Eng. degree from the Department of Industrial Engineering, Zhejiang University of Technology, Zhejiang, China, in 2002, the M.Eng. degree from the Department of Mechanical Automation Engineering, Shanghai University, Shanghai, China, 2005, and the Ph.D. degree from the Department of Industrial Engineering, Shanghai Jiaotong University, Shanghai, China, 2009. From 2009-2013, he was associate professor at Shanghai University, Shanghai, China. Since 2016, he worked as professor at School of Mechanical Engineering, Tongji University, Shanghai, China. His research interests focus on machine maintenance and machine learning. He is Associate Editor of IEEE Transactions on Instrumentation Measurement (Email: jbyu@tongji.edu.cn)

知识图谱驱动的船舶管件加工车间制造资源推荐方法

田思思 [1,2], 张子俊 [1,2], 李瑞芳 [1,2], 徐文君 [1,2]

1.武汉理工大学 信息工程学院，湖北 武汉 430070；

2. 宽带无线通信与传感器网络湖北省重点实验室，湖北 武汉 430070

摘　要：随着船舶管件制造企业向着数字化、智能化转型，船舶管件加工车间积累的大量知识与经验迫切需要得到充分利用。为了快速有效利用车间知识为用户推荐制造资源，提出了一种知识图谱驱动的船舶管件加工车间制造资源推荐方法。在分析车间中的加工管件信息、制造设备信息、加工工艺信息和加工订单信息和数据基础上，构建了船舶管件加工车间制造资源知识图谱，融合度中心性的采样改进策略，提出了基于改进型知识图卷积神经网络的船舶管件加工车间制造资源推荐方法，实验结果证明了所提方法的有效性且在车间生产过程中进行制造资源推荐时具有更高的准确率。

关键词：船舶管件加工车间；知识图谱；制造资源推荐；知识图卷积神经网络

Knowledge graph-driven manufacturing resource recommendation for ship pipe production workshop

Sisi Tian[1,2], Zijun Zhang[1,2], Ruifang Li[1,2], Wenjun Xu[1,2]

[1]School of Information Engineering, Wuhan University of Technology, Wuhan 430070, China

[2]Hubei Key Laboratory of Broadband Wireless Communication and Sensor Networks, Wuhan University of Technology, Wuhan 430070, China

Abstract: With the transformation of the ship pipe production workshop towards digitalization and intelligence, there is an urgent need to make full use of the large amount of knowledge and experience accumulated in the workshop. In order to quickly and effectively utilize workshop knowledge and recommend manufacturing resources to users, a knowledge graph-driven manufacturing resource recommendation method for ship pipe production workshop is proposed. Based on analyzing manufacturing equipment, ship pipe, process, and manufacturing order in the workshop, the knowledge graph of manufacturing resources for ship pipe production workshop is constructed, and with an improved sampling strategy that integrates degree centrality, an improved knowledge graph convolutional neural network-based recommendation method is then introduced. Experimental results demonstrate the effectiveness of the proposed method, which achieves higher accuracy when recommending manufacturing resources during workshop production process.

Key words: ship pipe production workshop, knowledge graph, manufacturing resources recommendation,

基金项目：国家自然科学基金资助项目(项目编号 92367108)；国防基础科研计划资助项目(项目编号 JCKY2023206B022)；湖北省重点研发计划项目(项目编号 2023BAB012)。

Knowledge Graph Convolutional Neural Network

1 引言

《“十四五”智能制造发展规划》对我国智能制造发展做出了全面的布局，智能制造成为了全球工业界关注的重点和学术界研究的热点[1]。船舶制造业是推动海洋强国战略的基础和重要支撑，智能制造技术的引入，推动了船舶制造业向数字化、智能化方向的快速发展。船舶管件加工车间是典型的多品种、小批量、离散性制造，车间内累积了大量的数据（加工管件类、制造设备类、加工工艺类、加工订单类等），但由于数据利用率低和缺乏知识管理能力，难以满足当前船舶管件加工车间生产的智能化需求。针对车间制造知识难以积累以及制造资源选择过渡依赖人工决策问题，亟需探究知识驱动的船舶管件加工车间制造资源推荐问题，充分理解数据并提供制造智能决策支持，实现制造资源的优化配置，提升船舶建造效率，推进船舶工业智能化转型升级。

知识图谱（Knowledge Graph，KG）作为知识工程的前沿技术，能够对知识进行有效组织和利用，通过知识推理、知识推荐等技术重用知识与经验，并指导生产决策，提高制造企业的信息化、智能化水平。文献[2]探索了知识图谱在智能领域的应用情景，探讨了知识图谱应用和实施的相关关键技术。文献[3]采用自顶向下与自底向上相结合的方法，利用知识图谱构建了车间关系网络，为车间智能协同生产提供决策。文献[4]提出一种基于知识图谱的认知制造数据表示方法，并将其应用于信息物理生产系统场景。文献[5]整合了多源异构数据，通过结合传统的自然语言处理和深度学习方法，从大型非结构化文本中自动提取三元组，构建了汽车领域的工业知识图谱。文献[6]提出了一种知识图谱驱动的生产资源分配方法，在资源加工信息和设备评估策略的前提下，对给定的订单插入任务进行快速的资源分配决策。文献[7]基于金属切削过程知识图谱，并采用个性化的 PageRank 算法实现了用于工艺流程的切削工具的推荐。文献[8]利用知识图谱对制造服务能力的功能信息、关联信息和非功能信息进行描述，实现了工业云机器人的制造能力服务的最优选择。文献[9]通过构建拆卸知识图谱对人机拆卸过程中的知识进行整理和管理，并提出知识推荐程序为操作人员推荐拆卸知识，从而提高了人机协同拆卸效率。文献[10]开发了一种新型卷积神经网络模型，利用领域知识来指导模型训练，从而提高了质量预测的准确性和模型可解释性。文献[11]利用知识图卷积神经网络实现了制造资源的推荐。

综上所述，以船舶管件加工车间为对象，将知识图谱应用于船舶管件加工车间，实现船舶管件车间制造资源的有效组织和管理，在此基础上，提出基于改进型知识图卷积神经网络的制造资源推荐方法，以知识驱动制造资源推荐，提高车间生产过程制造资源推荐效果，提升制造资源利用率和生产效率。

2　基于知识图谱的船舶管件加工车间制造资源推荐框架

基于知识图谱的船舶管件加工车间资源推荐框架如图 1 所示。主要包含面向船舶管件加工的制造资源知识图谱构建和基于改进型知识图卷积神经网络的制造资源推荐方法两个模块。

首先，面向船舶管件加工车间管件生产过程，分析船舶管件加工车间制造设备、加工工艺、加工订单、加工管件所涉及的相关概念，利用 OWL 本体建模语言构建船舶管件加工车间制造资源知识图谱模式层。分析船舶管件加工车间制造资源数据来源与结构，基于 D2RQ 进行知识抽取，构建船舶管件加工车间制造资源数据层，并利用 Neo4j 完成船舶管件加工车间制造资源知识图谱存储。在此基础上，将船舶管件加工订单融入船舶管件加工车间制造资源知识图谱，结合知识图卷积神经网络算法进行制造资源推荐，精准的制造设备推荐可以降低操作人员的经验水平要求，提高制造设备选择的准确性和效率。

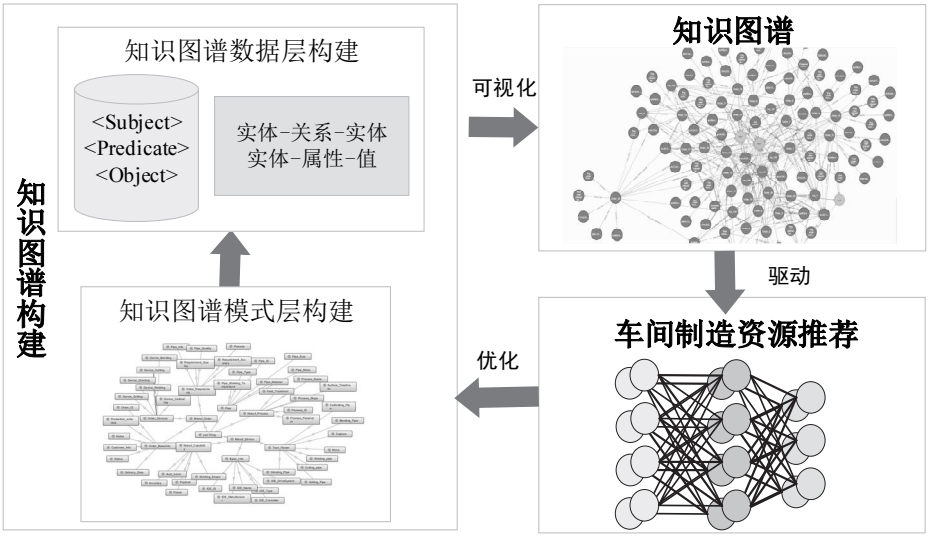


图1 基于知识图谱的船舶管件加工车间制造资源推荐框架

3　船舶管件加工车间制造资源知识图谱构建

船舶管件加工车间制造资源知识图谱属于一种领域知识图谱，对知识的准确性和专业性有更高的要求，因此采用自上而下方法构建船舶管件加工车间制造资源知识图谱，包括基于本体的知识图谱模式层的构建、基于 D2RQ 的知识图谱数据层的构建和基于 Neo4j 的知识图谱存储和可视化。

3.1　船舶管件加工车间制造资源知识图谱模式层构建

面向船舶管件加工任务，通过分析船舶管件加工整个流程，梳理其中所涉及的制造资源知识，包括制造设备类知识、加工管件类知识、加工工艺类知识、加工订单类知识，并基于 OWL 本体描述语言和改进的 IDEF5 本体构建方法构船舶管件加工车间制造资源(Ship Pipe Production Workshop Manufacturing Resources, SPPWMR)知识本体，采用 Protégé5.5.0 本体编辑软件对制造资源各子本体进行描述建模，如图

2 所示，包括制造设备本体模型，加工管件本体模型，加工工艺本体模型和加工订单本体模型。

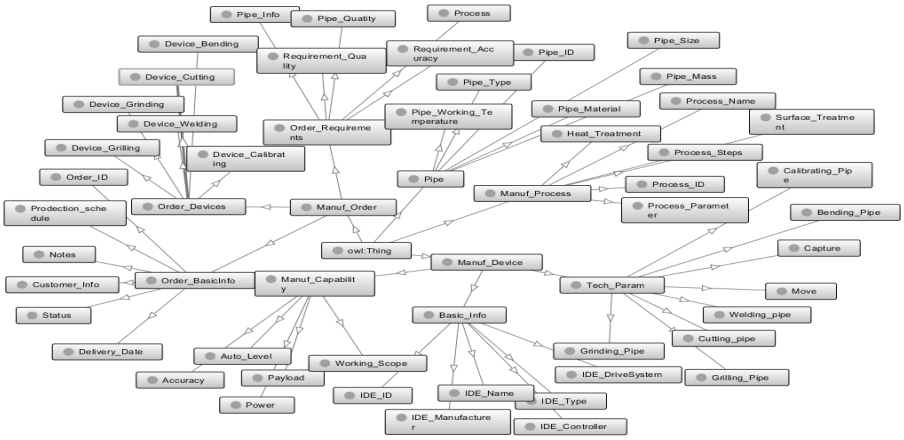


图2 船舶管件加工车间制造资源本体模型

（1）制造设备本体模型对 SPPWMR 中的制造设备进行了描述，包括三个子本体模型：设备基础信息、性能指标和制造能力本体。其中设备基础信息本体描述了制造设备的各种基础属性，主要包括设备 ID、名称、设备制造商信息、设备类型等静态信息，以及设备的控制装置、驱动系统等组件信息；性能指标本体描述了制造设备所具备的性能指标，包括各种运行参数，如工作功率、工作负载、工作范围、加工精度、自动化程度等，反应了制造设备的加工能力，是决定设备能否胜任加工订单的重要因素；制造能力本体描述了制造设备所拥有的制造能力，包括抓取、移动等基础能力，对应工艺流程中的工序所需要的能力，如切割、弯管、焊接等，反映了制造设备完成特定制造任务的能力。

（2）加工管件本体模型描述了 SPPWMR 中的管件资源，包括管件 ID、管件类型、管件尺寸、质量、材料、工作温度等属性信息。

（3）加工工艺本体模型对 SPPWMR 中的加工工艺进行了描述，包括工艺 ID、工艺方法、工艺流程、工艺参数、热处理、表面处理等。

（4）加工订单本体模型主要描述 SPPWMR 中的加工订单，包括订单基础信息、订单要求信息和订单设备选择三个子本体。其中，加工订单基础信息本体主要包括订单编号、客户信息、交付日期、价格和费用、生产计划、状态、备注等订单基础属性信息；订单要求信息本体描述了加工订单的指标要求信息，包括管件信息、管件数量、加工工艺要求、质量要求、精度要求等，决定了所加工管件的规格、工艺和精度；订单设备选择本体记录了订单完成加工管件这一任务所选择的制造设备，包括完成工艺流程的所有设备，如切割机、焊接机、弯管机等。

3.2　船舶管件加工车间制造资源知识图谱数据层构建与存储

制造资源知识抽取是指对船舶管件加工车间生产制造过程中存在的海量制造数据进行收集并按照知识本体模型定义的格式进行知识转化的过程，是构建 SPPWMR 知识图谱的关键一步。由于车间内的制造资源知识主要以半结构数据和结构化数据为主，首先对半结构化数据进行数据化转化存储于关系型数据库，然后采用 D2RQ 工具实现从关系型数据库中进行知识抽取，如图 3 所示，包括关系数据库到 RDF 格式的映射规则的构建和基于 D2RQ 的自动抽取，从而完成 SPPWMR 知识图谱数据层的构建。

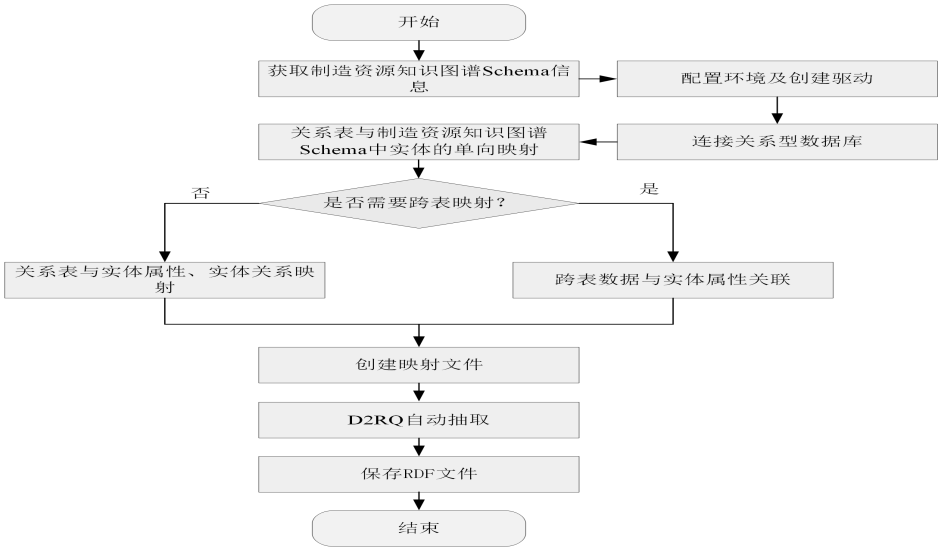


图3　基于D2RQ知识抽取流程图

Neo4j 图数据库在可视化、数据导入、内置算法、查询语言、知识图谱可视化等方面优势明显，基于 Neo4j 实现对 SPPWMR 知识图谱的存储，如图 4 所示。

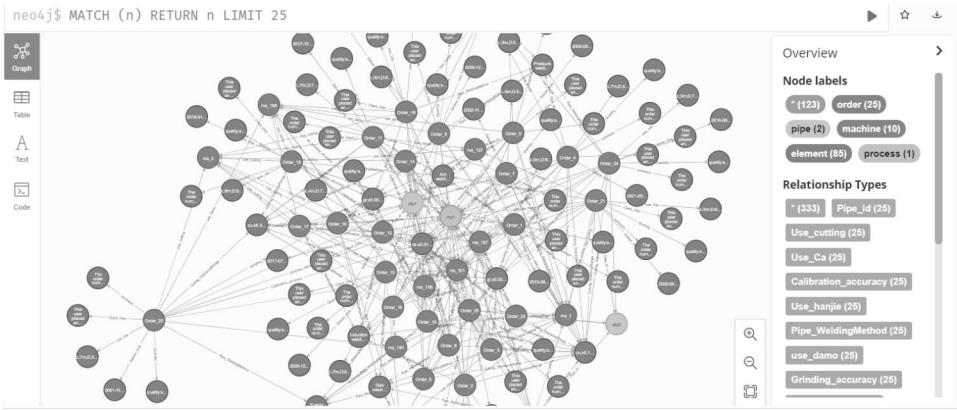


图4　船舶管件加工车间制造资源知识图谱

4　基于改进型知识图卷积神经网络的船舶管件加工车间制造资源推荐方法

以知识图卷积神经网络模型为基础，面向 SPPWMR 推荐场景，针对基于知识图卷积神经网络推荐算法存在采样不足的问题，提出了基于度中心性的采样改进策略的知识图卷积神经网络（Knowledge Graph

Convolutional Networks Based On Degree-Centrality, KGCN-DC）的船舶管件加工车间制造资源推荐方法。

船舶管件加工车间制造资源推荐根据船舶管件加工订单的加工要求推荐对应工序的制造设备，精准的制造设备推荐可以降低操作人员的经验水平要求，提高制造设备选择的准确性和效率。其中制造设备集合被定义为$u=\{u_1,u_2,u_3,...,u_m\}$，加工订单集合被定义为是$v=\{v_1,v_2,v_3,...,v_n\}$，而制造设备与加工订单的交互序列为$Y\in R^{M\times N}$，$y_{uv}=1$表示为制造设备和加工订单存在交互，相应的$y_{uv}=0$表示不存在交互。船舶管件加工车间的制造资源推荐模型是由已知的制造设备与加工订单的交互矩阵 Y 和辅助信息加工订单知识子图 G，向加工订单推荐对应工艺流程的制造设备，也可理解为向制造设备分配订单，推测制造设备与加工订单之间潜在的兴趣程度，即推荐程度。

4.1 知识图卷积神经网络算法

知识图卷积网络算法能够挖掘知识图谱中项目的相关联属性，发现项目之间的关联并捕获用户的偏好，主要步骤可分为节点采样、邻域聚合和预测生成。节点采样是从实体的邻居中抽取样本作为接受域。邻域聚合是对实体其邻域节点进行聚合，并和结合实体自身计算实体表示。概率预测是将得到的广泛信息的向量与制造设备向量进行计算得到预测值。

对于单层实体感受野，聚合实体 v 邻域信息的过程主要分为三步，具体描述如下。

第一步：计算用户对每个邻居关系的权重。对于每个邻居，用户的偏好程度都各不相同。这种偏好与邻居关系 r 相关，用户偏好评分如公式(1)所示。

$$\pi_r^u=g(u,r) \tag{1}$$

其中，$u\in R^d$ 和 $r\in R^d$ 分别表示用户向量和用户视角下的关系向量，d 表示向量维度，g 为内积函数，π_r^u 是用户对关系的偏好程度。例如，制造资源知识图谱中加工订单的加工精度关系对于制造设备选择来说更为重要，意味着制造设备能否处理该船舶管件加工订单。在此基础上，需要用户偏好评分进行归一化处理，如公式(2)所示，归一化后的用户关系偏好评分作为用户对每个邻居关系的权重。

$$\tilde{\pi}_{r_{v,e}}^u=\frac{\exp(\pi_{r_{v,e}}^u)}{\sum_{e\in N(v)}\exp(\pi_{r_{v,e}}^u)} \tag{2}$$

其中，$r_{v,e}$ 表示实体 v 与其邻居节点 e 的关系向量，$\tilde{\pi}_{r_{v,e}}^u$ 表示归一化后的用户对关系的偏好评分，即用户对邻居关系的权重。

第二步：进行邻居聚合，将求得的归一化后的邻居关系权重 $\tilde{\pi}^{u}_{r_{v,e}}$ 与各自对应的邻居向量相乘，如公式(3)所示。

$$V^{u}_{S(v)} = \sum_{e \in S(v)} \tilde{\pi}^{u}_{r_{v,e}} e \tag{3}$$

$$S(v) \triangleq \{e \mid e \sim N(v)\}, |S(v)| = K \tag{4}$$

其中，$V^{u}_{S(v)}$ 即为实体 v 的邻域表示，$S(v)$ 为实体 v 的单层感受野。当进行邻居聚合时，并不对将实体的所有邻居纳入计算，而是对每个实体都采用固定数量的邻居集合，如公式(4)所示，$S(v)$ 表示采样的邻居集合，其大小受一个超参数 K 控制，采用固定随机采样方式。

第三步：进行最后一次消息聚合，将实体自身表示与邻域表示进行聚合，采用求和聚合的方式进行最后一次消息聚合，如公式(5)所示。

$$agg_{sum} = \sigma(W \bullet (v + v^{u}_{S(v)}) + b) \tag{5}$$

其中，v 表示实体自身表示，$v^{u}_{S(v)}$ 表示实体邻域聚合表示，W 是权重参数，b 是偏置参数，σ 是非线性函数，agg_{sum} 是经过求和聚合后的结果。

经过知识图卷积层聚合后实体 v 的向量具有丰富的邻域信息，且可将接受域拓展到多层，从而发现知识图谱中实体的高阶结构和语义信息，进而发现用户的潜在兴趣。经过邻域聚合操作后，实体的最终表示包含丰富的上下文信息，与其自身表示及其相邻节点的信息相关。将聚合后的向量表示输入预测函数，生成用户 u 对项目 v 的 CTR 点击概率，即对应制造设备对订单的偏好程度，如公式(6)所示。

$$\hat{y}_{uv} = f(u, v^{u}) \tag{6}$$

其中，u 为制造设备向量，v^{u} 为聚合后的加工订单向量，$\hat{y}_{uv}$ 为最后生成的预测概率，得到的预测概率即制造设备与加工订单的匹配概率。

4.2　基于度中心性邻居采样的知识图卷积神经网络算法优化

为节省推荐模型的性能开销，知识图卷积神经网络算法并不将所有的邻居节点纳入邻域聚合的计算过程，而是采样固定随机采样，这种采样方法会导致一些重要的节点被遗漏，对应的邻域信息没有被采集到，影响了推荐系统的推荐效果。因此，在邻居节点采样过程中考虑到了实体节点的重要性，提出了一种基于度中心性的采样改进策略[12]。

通过计算知识图谱中节点的邻居节点的度中心性，按照其值大小来选取邻居采样节点，其计算过程如

公式(7)所示。

$$C_D(N_i)=\sum_{j=1}^{g}x_{ij}(i\neq j) \tag{7}$$

其中 $C_D(N_i)$ 表示节点 N_i 的度中心性，x_{ij} 表示在含有 g 个节点的知识图谱中，节点 N_i 和节点 N_j 是否存在直接联系，是则值为 1，否则值为 0，即理解为节点 N_i 的邻居个数。网络规模越大，度中心性的最大可能值越大，因此，需要进行标准化处理，如公式(8)所示，以消除网络规模大小的变化对度中心性的影响。其中，$g-1$表示知识图谱中节点最大可能的连接数，$C_D{}'$是标准化后的结果。

$$C_D{}'=\frac{C_D(N_i)}{g-1} \tag{8}$$

5 实验结果与分析

5.1 数据集与评价指标

实验所用数据集为所构建的 SPPWMR 知识图谱数据集 KGMR 和公共数据集 MovieLens-20M。KGMR 包含加工订单知识子图、加工订单-制造设备交互数据，作为推荐模型的输入。实验数据集如表 1 所示，数据集按照 6：2：2 的比例划分为训练集、评估集和验证集。为验证所提出的改进型 KGCN-DC 算法的有效性，与 RippleNet[13]、KGNN-LS[14]和 KGCN[15]算法进行了 CTR 点击率预测对比实验，并对推荐模型的超参数进行分析，选择 ACC、AUC 和 F1 三个指标进行评估。KGCN-DC 算法在两个数据集上的参数设置如表 2 所示。

表1 实验数据集

数据集	KGMR	MovieLens-20M
制造设备（用户）数量	206	138159
加工订单（项目）数量	6000	16954
交互数	57180	13501622
实体数	37030	102569
三元组数	77056	499474
关系种类	24	32

表2 KGCN-DC在两个数据集上参数设置

	KGMR	MovieLens-20M
学习率 lr	1e-3	2e-3
优化函数 Optimizer	Adam	Adam

嵌入维度 d	16	32
感受野深度 h	1	1
正则化权重 l2_weight	1e-7	1e-7
采样邻居大小 K	6	4
batch_size	1024	65536

KGCN-DC算法涉及了一些超参数，这些参数的设置一定程度上影响着模型的推荐效果，参数的选取参考前期研究工作[11]，在邻居采样节点数量K、感受野深度H和实体嵌入维度d三个超参数方向做了相关实验，实验数据集为KGMR，实验结果如图5-7所示，采样节点数K取6、感受野深度H取1、嵌入维度d等于16时，推荐性能最好。

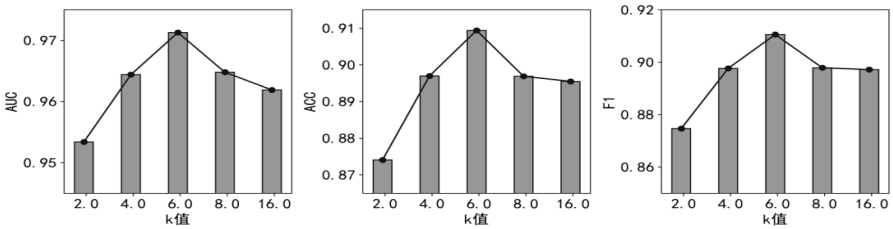


图5 邻居采样节点数量K对结果影响

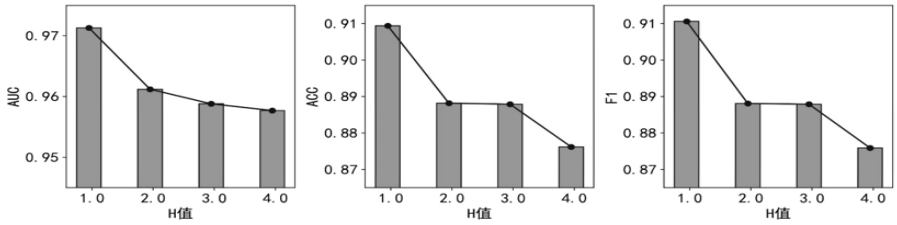


图6 感受野深度H对结果的影响

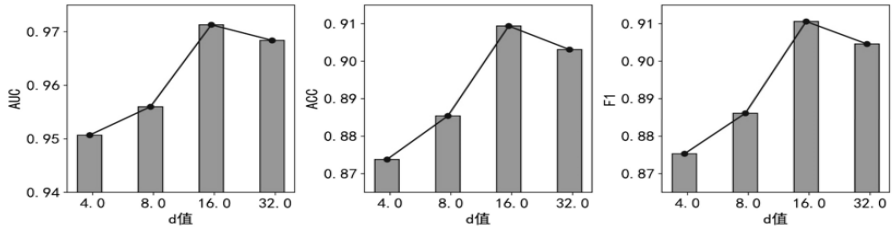


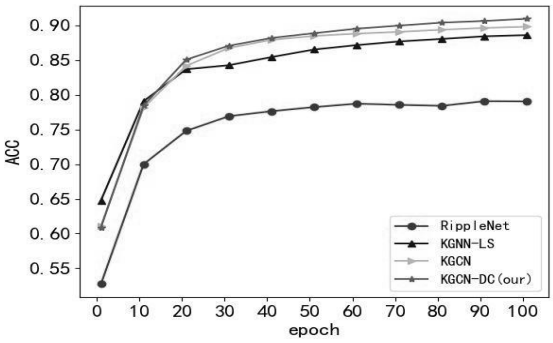
图7 实体嵌入维度d对结果的影响

5.2 实验结果分析

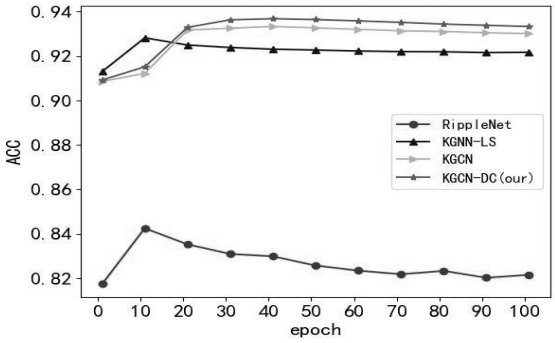
CTR 点击率预测对比实验结果如表 3 和图 8 所示，改进型 KGCN-DC 在 AUC 和 F1 这两个指标均优于其他对比算法。相较于 RippleNet 算法、KGNN-LS 算法、KGCN 算法，改进型 KGCN-DC 算法效果更好，在所构建的数据集中能够更有效地聚合邻域信息，捕捉用户的兴趣偏好。

表3 CTR点击预测实验结果

	KGMR		MovieLens-20M	
	AUC	F1	AUC	F1
RippleNet	0.8447	0.7865	0.8921	0.8217
KGNN-LS	0.9594	0.8873	0.9716	0.9222
KGCN	0.9663	0.8989	0.9768	0.9333
KGCN-DC	0.9713	0.9106	0.9772	0.9341



（a）KGMR 数据集



（b）MovieLens-20M 数据集

图8 准确率ACC变化曲线

6 结束语

为了解决船舶管件加工车间中制造资源知识的组织、利用不足的问题，从船舶管件加工车间中知识概念和生产过程出发，构建了船舶管件加工车间制造资源知识图谱；为了解决船舶管件加工车间中制造设备的选择严重依赖操作人员的经验导致生产效率及生产质量受限的问题，提出了基于知识图谱的船舶管件加工车间资源推荐方法，基于构建的船舶管件加工车间制造资源知识图谱，结合图卷积网络算法，捕捉制造资源与加工订单之间的关联性，实现了制造资源的准确推荐，提高加工任务速度，使得船舶管加加工更加高速准确，提升了船舶管件加工车间智能化水平。

对于实际船舶管件加工车间中的生产线和更复杂的生产流程，还需更深入的分析和挖掘，完善船舶管件加工车间制造资源知识图谱，未来研究中可以将制造服务组合优选方法与推荐算法相结合，进一步提高知识推荐的有效性。

参考文献

[1] 刘强. 智能制造理论体系架构研究[J]. 中国机械工程, 2020, 31(01): 24-36.

Liu Q. Study on Architecture of Intelligent Manufacturing Theory[J]. China Mechanical Engineering, 2020, 31(01): 24-36.

[2] 张栋豪, 刘振宇, 郑维强, 等. 知识图谱在智能制造领域的研究现状及其应用前景综述[J]. 机械工程学报, 2021, 57(05): 90-113.

Zhang D H, Liu Z Y, Jia W Q, et al. A Review on Knowledge Graph and Its Application Prospects to Intelligent Manufacturing[J]. Journal of Mechanical Engineering, 2021, 57(05): 90-113.

[3] 曹雨燕, 徐湛, 田志刚, 等. 面向制造车间数字孪生知识图谱研究[J/OL]. 机械科学与技术, 1-7[2024-07-04].

Cao Y Y, Xu Z, Tian Z G, et al. Research on digital twin knowledge graph for manufacturing workshops[J/OL]. Mechanical Science and Technology for Aerospace Engineering, 1-7[2024-07-04].

[4] Liu M, Li X, Li J, et al. A knowledge graph-based data representation approach for IIoT-enabled cognitive manufacturing[J]. Advanced Engineering Informatics, 2022, 51: 101515.

[5] Zhao M, Wang H, Guo J, et al. Construction of an industrial knowledge graph for unstructured chinese text learning[J]. Applied Sciences, 2019, 9(13): 2720.

[6] Zhou B, Bao J, Li J, et al. A novel knowledge graph-based optimization approach for resource allocation in discrete manufacturing workshops[J]. Robotics and Computer-Integrated Manufacturing, 2021, 71: 102160.

[7] Duan Y, Hou L, Leng S. A novel cutting tool selection approach based on a metal cutting process knowledge graph[J]. The International Journal of Advanced Manufacturing Technology, 2021, 112: 3201-3214.

[8] Ma Y, Xu W, Tian S, et al. Knowledge graph-based manufacturing capability service optimal selection for industrial cloud robotics[C]. International Manufacturing Science and Engineering Conference. American Society of Mechanical Engineers, 2020, 84263: V002T07A022.

[9] Hu Y, Ding Y, Xu F, et al. Knowledge recommendation system for human-robot collaborative disassembly using knowledge graph[C]. International Manufacturing Science and Engineering Conference. American Society of Mechanical Engineers, 2021, 85079: V002T07A022.

[10] Guo S, Wang D, Feng Z, et al. Di-CNN: Domain-Knowledge-Informed Convolutional Neural Network for Manufacturing Quality Prediction[J]. Sensors, 2023, 23(11): 5313.

[11] Zhang Z J, Tian S S, Peng L, et al. Knowledge Graph-Driven Manufacturing Resources Recommendation Method for Ship Pipe Manufacturing Workshop[C]. In: International Workshop on Autonomous Remanufacturing (IWAR 2023), 2024: 251-264.

[12] 赵构恒, 贾鹏, 周安民. 有向加权网络中的改进度中心性[J]. 计算机应用, 2020, 40(S1): 141-145.

Zhao G H, Jia P, Zhou A M. lmproved degree centrality for directed-weighted network[J]. Journal of Computer Applications, 2020, 40(S1): 141-145.

[13] Wang H, Zhang F, Wang J, et al. Exploring high-order user preference on the knowledge graph for recommender systems[J]. ACM Transactions on Information Systems (TOIS), 2019, 37(3): 1-26.

[14] Wang, Hongwei, et al. Knowledge-aware graph neural networks with label smoothness regularization for recommender systems[C]. Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining. 2019.

[15] Jiang X, Fu Y, Dong C. Recommendation method for fusion of knowledge graph convolutional network[J]. EURASIP Journal on Advances in Signal Processing, 2022, 2022(1): 27.

[作者简介]

田思思（1989-），女，博士研究生，研究方向：数字孪生技术、工业云机器人、智能优化。

张子俊（1999-），男，硕士研究生，研究方向：工业机器人与可持续制造。

李瑞芳（1978-），女，副教授，博士，硕士生导师，研究方向：无线通信，无线网络，车联网等。

徐文君（1983-），男，教授，博士，博士生导师，研究方向：智能协同制造、数字孪生、工业智能、人机协作、工业互联网等。

作者图片

田思思

张子俊

李瑞芳

徐文君

基于数据驱动的转炉能耗建模与工艺参数节能优化

敬培锋[1]，李聪波[1]，史春燕[2]，吴畏[1]，李博[1]

（1. 重庆大学高端装备机械传动全国重点实验室，重庆，400044；

2. 中冶赛迪信息技术（重庆）有限公司，重庆，400041）

摘　要：转炉作为钢铁冶金能源高消耗、高回收的主要设备，开展基于数据的转炉节能优化研究对推动钢铁冶金行业网络化、绿色化转型具有重要意义。因此，本文提出一种基于数据驱动的转炉能耗建模与工艺参数节能优化方法。首先，分析转炉物质流与能量流特性，利用支持向量机回归方法构建转炉能耗模型；基于此，以转炉吨钢能耗为目标，以废钢比、吹氧强度、铁水入炉温度为优化变量，建立转炉工艺参数节能优化模型，并采用徒步优化算法进行优化求解。最后，结合炼钢实际生产数据，验证所提方法的有效性。

关键词：转炉；节能优化；能耗建模；工艺参数；数据驱动

Energy consumption modelling and process parameter energy-saving optimization of converter based on data-driven approach

JING Peifeng[1]，LI Congbo[1]，SHI Chunyan[2]，WU Wei[1]，LI Bo[1]

（1. State Key Laboratory of Mechanical Transmission for Advanced Equipment, Chongqing, University, Chongqing 400044, China;

2. CISDI-INFO Co., Ltd., Chongqing 400041, China）

Abstract: Converter is the main equipment of iron and steel metallurgy with high energy consumption and high recovery. It is of great significance to conduct data-based converter energy-saving optimization research to promote the networked and green transformation of iron and steel metallurgy industry. Accordingly, this study proposes a method based on data-driven energy consumption modelling and process parameter energy-saving optimization for converter. Firstly, the material flow and energy flow characteristics of converter are analyzed, and a converter energy consumption model is constructed by using support vector regression approach. Then, a process parameter optimization model for minimizing converter energy consumption per ton steel is established with scrap ratio, oxygen blowing intensity and iron temperature as optimization variables, and a hiking optimization algorithm is adopted to solve the optimization model. Finally, the effectiveness of the proposed method is verified based on actual steelmaking production data.

Key words: converter, energy saving optimization, energy consumption modeling, process parameter, data drive

---

通信作者：李聪波，congboli@cqu.edu.cn

基金项目：国家自然科学基金(No. 92367107)

1 引言

炼钢工序是影响钢铁冶金总能耗的关键工序，其冶炼过程消耗氧气、氮气等多种能源介质，并产生大量的转炉煤气和蒸汽，是钢铁冶金能源消耗和二次能源回收的最主要工序之一[1-2]。转炉是炼钢工序能源产耗最大的核心设备，其炼钢工艺参数的选择对能源产耗影响很大[3]。因此，如何构建转炉能耗模型及工艺参数节能优化模型，以实现降低转炉能源消耗、提升转炉二次能源回收量，是目前亟需解决的问题。

转炉能耗建模是工艺参数节能优化的基础，部分学者对转炉能耗建模开展了深入研究。例如，Shao等[4]构建了基于氧气平衡机制和深度神经网络的转炉吹氧时间预测模型，并结合吹氧强度得到转炉的耗氧量预测模型，其预测精度可达96.67%。Wang等[5]建立了一种结合转炉氧气平衡与多元线性回归的机理与数据混合耗氧量预测模型。阳青锋等[6]针对转炉冶炼工况多、钢种数据维度不统一等问题，提出了一种基于粒度聚类的转炉氧气消耗量预测方法。Shi等[7]提出一种基于改进鲸群优化算法和随机配置网络的建模方法，分别建立了转炉炼耗氧量模型、转炉煤气回收模型和蒸汽回收模型。

近年来，钢铁冶金工艺参数节能优化研究已受到关注。例如，Wang等[8]建立了以钢铁冶金各原料配比、废钢比等工艺参数为调控变量的能耗优化模型，降低了能耗6.3%。Na等[9]通过选取高炉煤比、铁水温度等工艺参数，显著提升了钢铁冶金能效，降低了能耗与碳排放。Yang等[10]分析了焦比、废钢比等工艺参数对钢铁冶金能耗的影响，并构建了钢铁冶金全流程能耗工艺参数优化模型。Zhang等[11]提出了一种炼焦、烧结、炼铁、炼钢和热轧工艺的组合优化模型，通过优化高炉热风温度、转炉废钢比等参数，有效降低了钢铁冶金能耗。

综上所述，转炉能耗建模研究已见报道，但其主要针对氧气、转炉煤气、蒸汽等单一能源产耗，考虑多种能源产耗的转炉综合能耗模型研究较少。在钢铁冶金工艺参数节能优化方面，现有研究主要面向钢铁冶金全流程。然而，钢铁冶金工序复杂繁多，涉及的工艺参数数量巨大，仅选取少量关键工艺参数优化，在一定程度上可以实现钢铁冶金全流程节能，但对于单个设备的节能潜力挖掘不足。

鉴于此，本文以转炉为研究对象，开展基于数据驱动的转炉能耗建模与工艺参数节能优化方法研究。首先，系统分析转炉炼钢过程物质流与能源流特性；在此基础上，结合转炉炼钢过程能耗与相关参数的历史数据，构建基于数据驱动的转炉能耗模型；然后，以转炉吨钢能耗为目标，以废钢比、吹氧强度、铁水入炉温度为决策变量，建立转炉工艺参数节能优化模型；最后，结合转炉实际生产数据，对本文所提方法的准确性和有效性进行验证。

2 问题描述

转炉炼钢包括兑铁、通氧吹炼、出钢、溅渣护炉、倒渣等过程，如图1所示。然而，转炉炼钢工序繁多，其冶炼过程存在氧气、氮气等多种能源消耗，且会产生大量转炉煤气、蒸汽等二次能源，具有能源

产耗种类多、量大的复杂特性。转炉工艺参数的选择不仅决定着炼钢过程各能源介质的消耗，同时也对二次能源的产量有着重要影响。实际生产中通过经验选择参数易出现能源输入冗余，增加能源消耗，或输入能源不足，影响钢水生产质量。本文将基于转炉废钢比、吹氧强度、铁水温度等历史数据构建转炉能耗模型，研究转炉工艺参数节能优化方法，从而降低转炉生产过程的能源消耗。

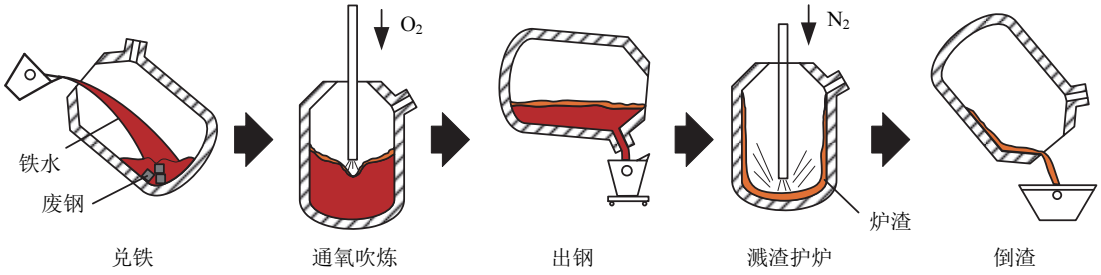


图1 转炉炼钢流程

3 基于数据驱动的转炉能耗模型

3.1 转炉炼钢物质流与能量流分析

转炉炼钢涉及多种物质输入输出与能源介质的消耗产生。首先，向转炉中按一定比例兑入废钢和铁水；其次，通入氧气进行吹炼，期间加入石灰石、白云石等造渣剂，钒氮合金等脱氧剂，以及其他辅助原料，同时为提升炉内反应效率，通入氮气、氩气进行搅拌，达到除去铁水杂质、调节钢水成分的目的；完成炼钢、倒出钢水，并加入镁球等调渣剂调整终渣成分；最后，再次通入氮气进行溅渣护炉，倒出余下的炉渣，进行下一次兑铁。此外，吹炼过程会发生一系列物理化学反应，产生CO、H_2、CO_2等气体形成高温烟气，经除尘、余热回收处理产生炉尘、转炉煤气、蒸汽等。综上分析，可得到转炉物质与能量流动模型如图2所示。

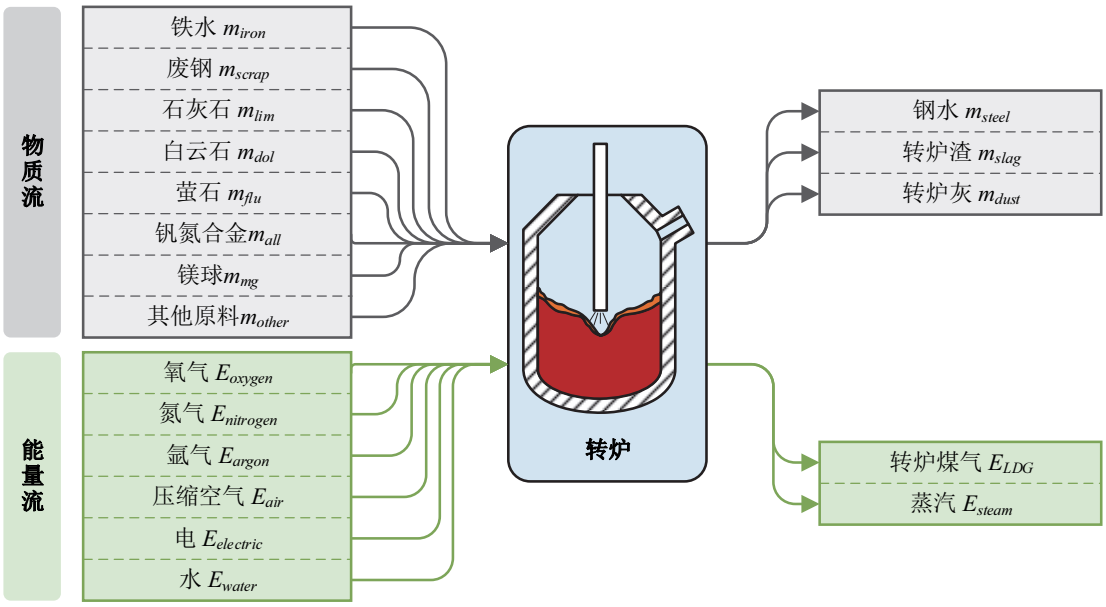


图2 转炉物质流与能量流模型

3.2 转炉能耗模型

转炉能耗通常以各能源介质的消耗量与二次能源产生量的综合能耗表示。具体计算为各种能源介质产耗转化的标准煤量，并以单位产品能耗作为衡量转炉能耗的指标。

3.2.1 转炉能耗分析

基于转炉炼钢过程的能量流分析，转炉能源消耗包括氧气、氮气、氩气、压缩空气、电、水等，产生的能源介质主要包括转炉煤气和蒸汽，其中

（1）转炉能源消耗分析

1）氧气消耗E_{oxygen}。转炉通入氧气主要用于氧化去除铁水中的杂质元素，并为冶炼过程提供热量，是消耗最多的一种能源。

2）氮气消耗$E_{nitrogen}$。氮气消耗包括两个阶段，吹炼前中期吹入氮气用于除去钢液中杂质，钢水冶炼完成后用于溅渣护炉。因此，氮气总消耗需考虑不同应用场景和压力下的消耗量。

3）氩气消耗E_{argon}。氩气不会参与冶金反应，在炼钢后期用于搅动钢水，促使钢水中的N_2、H_2等气体杂质排出，起到“气洗”作用。

4）压缩空气消耗E_{air}。压缩空气主要用于驱动气动调节阀门，控制气体介质的输送。

5）电能消耗$E_{electric}$。转炉工序涉及的耗电设备复杂多样，包括起重机、转炉、除尘风机等，但由于转炉本身电能消耗极少，故本文不考虑。

6）水消耗E_{water}。水在转炉工序中主要用于冷却转炉、氧枪等，这部分水通常属于工厂冷却水循环系统，在炼钢过程循环使用，故本文不考虑水耗。

（2）转炉能源回收分析

1）转炉煤气回收E_{LDG}。吹炼过程产生的高温烟气经除尘会形成转炉煤气，当转炉煤气CO含量大于25%，O_2含量小于1%时，进行转炉煤气回收，否则通入烟囱点火放散[12]。

2）蒸汽回收E_{steam}。转炉产生的高温烟气通过与冷却烟道和冷却水进行热交换，从而产生蒸汽。

转炉能耗为各能源介质总消耗量与二次能源回收量之差，基于上述能源产耗分析，转炉能耗可由下式表示：

$$E_{\mathrm{BOF}} = \left(E_{oxygen} + E_{nitrogen} + E_{\mathrm{argon}} + E_{air} + E_{electric} + E_{water} - E_{LDG} - E_{steam}\right) / m_{steel} \qquad (1)$$

3.2.2 基于数据驱动的转炉能耗模型构建

转炉能耗受铁水中的C、Si、P、S等含量、废钢比、铁水温度、吹氧强度等因素的影响。铁水中的C、Si、P、S等含量，经氧气氧化而得以降低，在此过程中产生CO、CO_2等气体，与转炉煤气的生产量密切相关。但实际生产过程中，很难直接调整铁水中各元素，来减少能耗，并且在同一批次中，铁水中各元

素成分变化不大，故在本文中不考虑。废钢比增加会降低转炉内C、P等杂质含量，从而减少氧气、氮气、氩气的吹入时间和转炉煤气、蒸汽的回收量，但废钢量过大会影响转炉热平衡，需要增加燃料，导致钢水杂质含量上升，影响钢水质量；铁水温度过低需要加入燃料提供热量，使冶炼时间变长，增加氧气等能源消耗，温度过高会导致炉内压力不稳定，氧化还原反应不平衡，影响氧气利用率；提升吹氧强度可加快氧气与铁水的反应速度、缩短冶炼时间，降低能耗，但吹氧强度过大会导致炉内温度过高、氧气使用效率下降，造成能源浪费。此外，各能源介质的消耗过程伴随着复杂多变的物理化学反应，使转炉的能源产耗量难以通过机理分析获取。因此，本文将以废钢比、铁水温度、吹氧强度作为输入变量，以转炉能耗作为输出变量，采用数据驱动的方式构建转炉能耗模型。

本文选用支持向量机回归(Support Vector Regression, SVR)、BP神经网络(Back Propagation，BP)、人工神经网络（Artificial Neural Network，ANN）和随机森林（Random Forest, RF）4种方法来构建转炉能耗模型，然后根据所建模型精度选取建模方法。

（1）SVR

SVR算法是利用非线性映射原始的输入变量从低维空间映射至高维空间，构造出拟合数据的最优线性平面[13]。SVR的建模流程可以表示为：

1）定义目标函数。寻找函数$f(x)=\omega x+b$使得大多数数据点落在距离该函数ε以内，其目标函数可写成：

$$\min_{\omega,b,\xi,\xi^*}\frac{1}{2}\|\omega\|^2+C\sum_{i=1}^{n=1}\left(\xi_i+\xi_i^*\right) \tag{2}$$

其中，ζ和ζ^*是松弛变量，表示允许的误差，C是惩罚参数，用于平衡模型复杂度和误差。

2）约束条件。约束条件确保所有数据点偏离回归函数的误差在ε以内，即：

$$y_i-\omega x_i-b\le\varepsilon+\xi_i \tag{3}$$

$$\omega x_i+b-y_i\le\varepsilon+\xi_i^* \tag{4}$$

3）训练模型。使用优化算法（如拉格朗日乘子法）求解目标函数，得到最优的权重向量ω和偏置b。

4）预测。使用训练好的模型对新数据进行预测，预测函数即：$f(x)=\omega x+b$。

（2）BP

BP神经网络是一种多层前馈神经网络，包括输入层、隐含层及输出层。通过计算网络输出与期望输出的误差来逐层反向传播误差，并不断调整网络权重与阈值[14]，从而优化网络性能以达到最小化误差的目的。

（3）ANN

ANN算法是基于生物神经网络运作原理开发，能够处理复杂的模式识别、分类、回归和其他任务[15]。主要训练过程为：通过网络逐层传递输入数据，计算每个神经元的输出，并生成最终输出。衡量预测输

出与实际输出的差距，计算损失函数相对于每个权重的梯度，从输出层向输入层反向传播，不断调整权重以最小化损失函数，逐步趋近最优解。

（4）SF

SF算法包括数据采样、构建决策树和集成结果三个步骤[16]。从训练数据集中不断抽取多个子数据集，将每个子数据集构建一棵决策树，在每个节点分裂时，从所有特征中随机选择一个子集，选取能最大化信息程度或最小化均方误差的特征进行分裂。最后选择所有决策树预测结果中占比高的结果作为最终预测。

4 基于徒步优化算法的转炉工艺参数节能优化方法

4.1 转炉工艺参数节能优化模型

4.1.1 目标函数

本文通过优化转炉工艺参数来实现转炉炼钢过程的节能，因此转炉能耗为优化目标，即公式（1）。

4.1.2 决策变量及约束条件

根据转炉炼钢能耗分析，本文选择废钢比、吹氧强度、铁水入炉温度等可调工艺参数作为决策变量。

转炉炼钢过程应遵循物质约束、能量约束和工艺约束。其中，物质约束指物质质量守恒，主要考虑Fe、C、Si、P、Mn等成分的质量守恒，计算方法如下：

$$\begin{aligned} & m_{iron}\times\omega_{i,iron}+m_{scrap}\times\omega_{i,srap}+m_{\lim}\times\omega_{i,\lim}+m_{dol}\times\omega_{i,dol}+m_{flu}\times\omega_{i,flu} \\ & +m_{all}\times\omega_{i,all}+m_{mg}\times\omega_{i,mg}+m_{other}\times\omega_{i,other}+m_{oxygen}\times\omega_{i,oxygen} \\ & +m_{nitrogen}\times\omega_{i,nitrogen}+m_{\arg on}\times\omega_{i,\arg on}+m_{air}\times\omega_{i,air} \\ = & m_{steel}\times\omega_{i,steel}+m_{slag}\times\omega_{i,slag}+m_{dust}\times\omega_{i,dust}+m_{LDG}\times\omega_{i,LDG}+m_{steam}\times\omega_{i,steam} \end{aligned} \tag{5}$$

式中，m_j表示物质或能源j的质量，t，j为铁水、石灰石、氧气等；$\omega_{i,j}$表示物质或能源j中元素或化合物i的含量，i为Fe、C、Si等。

能量约束基于能量守恒定律，即转炉的输入能量应与输出能量相等。输入能量包括铁水物理热、氧化放热等，输出能量包括产品和副产物的物理热、化学反应吸热、物料熔化吸收热及生产中的热损失，其能量平衡具体表达如式（6）所示：

$$Q_{iron}+Q_{ele\text{-}oxi}+Q_{dus\text{-}oxi}=Q_{dec}+Q_{raw}+Q_{steel}+Q_{slag}+Q_{dust}+Q_{LDG}+Q_{loss} \tag{6}$$

式中，Q_{iron}为铁水热量，kJ；$Q_{ele\text{-}oxi}$为原料中元素氧化反应放热，kJ；$Q_{dus\text{-}oxi}$为烟尘氧化放热，kJ；Q_{dec}为分解反应吸热，kJ；Q_{raw}为原料熔化吸热，kJ；Q_{steel}为钢水热量，kJ；Q_{slag}为转炉渣热量，kJ；Q_{dust}为炉尘热量，kJ；Q_{LDG}为转炉煤气热量，kJ；Q_{loss}为其他热量损失，kJ。

工艺约束为结合实际生产能力与经验的决策变量控制范围约束，本文主要考虑废钢比、铁水温度、吹氧强度、转炉渣碱度等工艺要求。此外，能耗优化应该在确保钢水质量的前提下，主要考虑钢水中Fe、

C、Si、P、Mn等元素含量和温度在要求的范围之内。

4.2 基于徒步优化算法的转炉工艺参数节能优化模型求解

徒步优化算法（Hiking Optimization Algorithm，HOA）是基于人类徒步旅行开发的元启发式算法[17]。HOA的灵感来源于徒步者攀登山峰过程中随机遇到各种地形，如优化问题在寻找全局最优值时，会随机遇到各种情况，而徒步者则会考虑地形，选择性避开陡峭的地形和小径，以保持前进的速度。

HOA以Tobler徒步函数（Tobler’s Hiking Function，THF）为前提，建立数学模型[18]。在考虑地形的情况下确定徒步者的徒步速度：

$$w_{\mathrm{i,t}} = 6e^{-3.5\left|S_{\mathrm{i,t}}+0.05\right|} \tag{7}$$

$$S_{\mathrm{i,t}} = \frac{\mathrm{d}h}{\mathrm{d}x} = \tan\theta_{\mathrm{i,t}} \tag{8}$$

其中，$W_{i,t}$是在迭代过程中徒步者i在迭代点或时间点t的速度；$S_{i,t}$是所走地形的坡度，坡度$S_{i,t}$计算如公式（8）所示；d 表示海拔高度的差异，dx为徒步者所行走的距离；$\theta_{i,t}$为所走地形的倾角[0，50°]。

徒步者更新速度是初始速度、领队者位置、徒步者实际位置和扫描因子的函数，公式如下：

$$w_{\mathrm{i,t}} = w_{\mathrm{i,t\text{-}1}} + \gamma_{\mathrm{i,t}}\left(\beta_{\mathrm{best}} - \alpha_{\mathrm{i,t}}\beta_{\mathrm{i,t}}\right) \tag{9}$$

其中，$\gamma_{i,t}$是[0，1]范围内的均匀分布数；$W_{i,t}$和$W_{i,t\text{-}1}$分别表示徒步者i当前和初始的速度。β_{best}为领队的位置，$\alpha_{i,t}$为徒步者i的扫描因子（SF），范围为[1，3]。SF保证了徒步者不会离领队太远，可以接收到领队的信号。

通过考虑徒步者的速度，给出徒步者i的更新位置$\beta_{i,t+1}$：

$$\beta_{\mathrm{i,t+1}} = \beta_{\mathrm{i,t}} + w_{\mathrm{i,t}} \tag{10}$$

结合HOA算法开展工艺参数节能优化，流程如图3所示，主要步骤包括：

Step1: 随机生成多组初始的废钢比、铁水入炉温度、吹氧强度参数组合，并计算对应的能耗值。

Step2：选取最小转炉能耗所对应的工艺参数组合作为“领队”。

Step3：随机生成的地形倾斜角度，在不同方向上探索新的工艺参数组合。

Step4：计算地形坡度和参数初始的迭代速度，并不断更新迭代速度。

Step5：根据迭代速度更新工艺参数组合，并计算对应的能耗值。重复Step2，直到达到停止条件。输出最优参数组合及最小能耗值。

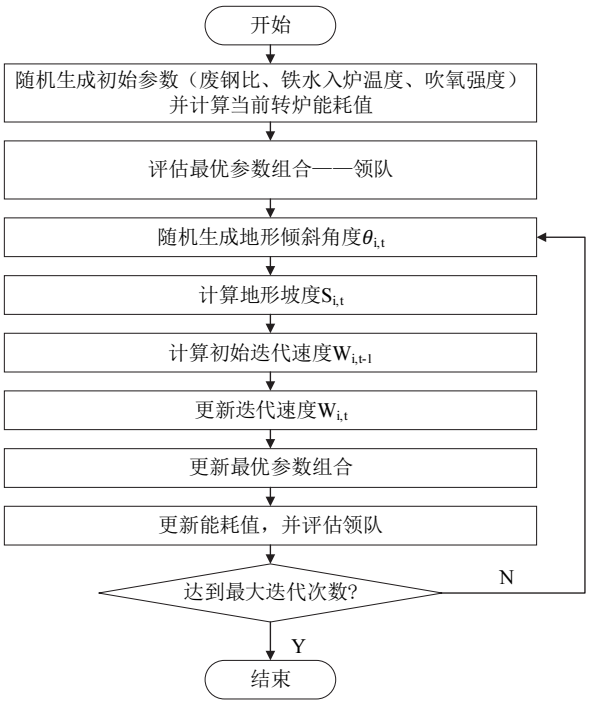


图3 HOA算法流程

5 案例分析

5.1 案例背景

本文以转炉为对象，在国内某炼钢厂采集了248炉次转炉炼钢数据，具体包括每炉铁水量、废钢量、氧气等的消耗量，铁水入炉温度、吹氧强度、转炉煤气和蒸汽回收量、钢水产量等数据。数据采集过程可能发生传感器故障等情况，造成某些数据缺失，如图4所示。本文将存在缺失的炉次数据进行剔除，最终选取231组数据，部分数据如表1所示。

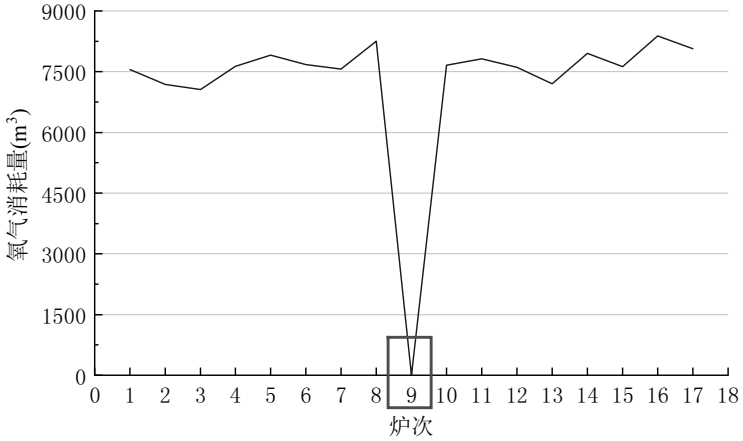


图 4 部分炉次氧气消耗数据曲线

表 1 转炉参数及能耗数据

序号	数据名称	炉次 1	炉次 2	炉次 3	…	炉次 230	炉次 231
1	铁水量（t）	115.87	117.01	110.93	…	112.86	116.52
2	废钢量（t）	50.30	51.42	50.92	…	51.17	48.23
3	铁水入炉温度（℃）	1363.00	1372.00	1393.00	…	1413.00	1311.00
4	氧气消耗（m³）	7802.00	7823.00	7561.00	…	7647.00	7468.00
5	吹氧强度（$m^3 \cdot min^{-1} \cdot t^{-1}$）	4.126	4.054	4.092	…	3.820	4.068
6	氮气消耗（m^3）	4243.34	4357.38	4134.80	…	4221.44	4159.63
7	氩气消耗（m^3）	9.12	9.34	8.82	…	9.17	8.96
8	压缩空气消耗（m^3）	1828.97	1871.66	1767.33	…	1835.74	1795.68
9	转炉煤气回收（m^3）	27868.70	25372.21	23782.80	…	24594.76	23552.63
10	蒸汽回收（kg）	15408.12	15767.82	14888.87	…	15465.17	15127.71
11	钢水产量（t）	159.35	163.07	153.98	…	159.94	156.45
12	吨钢能耗（$kgce \cdot t^{-1}$）	-35.727	-35.713	-35.399	…	-35.379	-34.745

本文将结合炼钢实际生产历史数据，验证所提建模和优化方法的可靠性与有效性。其中，目标函数即转炉能耗模型由数据集训练所得，约束条件则根据该钢厂转炉炼钢的实际情况进行设定，具体约束条件如表2所示。

表2 转炉工艺约束条件[9]

序号	名称	约束条件	序号	名称	约束条件
1	铁水温度(℃)	1320~1420	7	钢水Mn含量(%)	0.20~0.65
2	废钢比(%)	20~35	8	钢水P含量(%)	0~0.045
3	吹氧强度($m^3 \cdot min^{-1} \cdot t^{-1}$)	3.5~4.5	9	钢水S含量(%)	0~0.04
4	钢水Fe含量(%)	99~100	10	钢水温度(℃)	1600~1660
5	钢水C含量(%)	0.05~0.12	11	转炉渣碱度	1~3
6	钢水Si含量(%)	0.12~0.30			

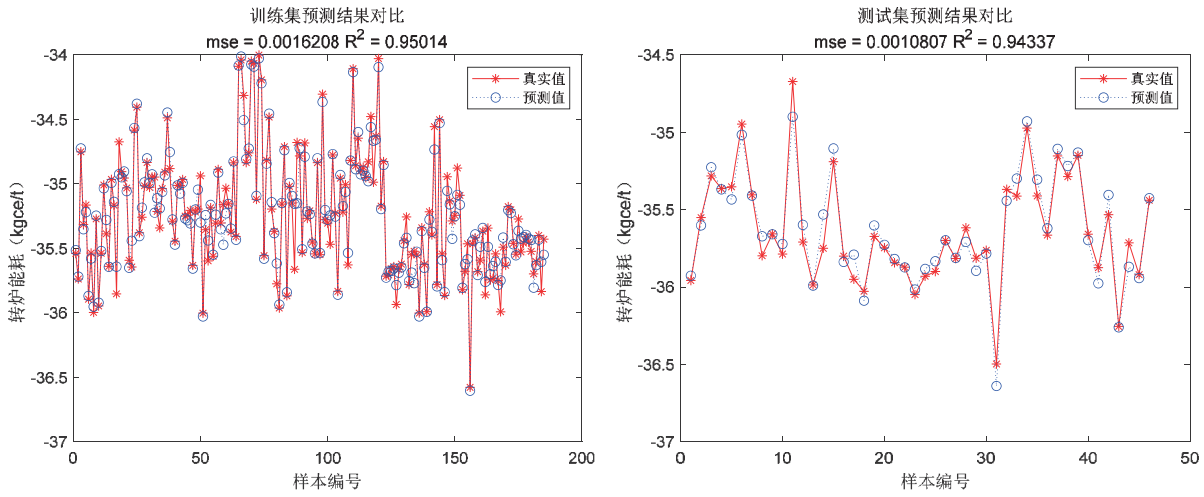
5.2 转炉能耗模型验证

本文将采集数据按8:2进行划分为训练集和测试集，其中训练集185组，测试集46组。分别采用BP、SVR、ANN和RF算法建立转炉能耗的数据模型，并利用平均绝对误差(MAE)、均方根误差(RMSE)和可决定系数（R^2）作为评价指标对各模型的进行评估，从中挑选精度最高的模型，用于转炉能耗优化。

为确保4种算法所建模型的精度与模型对比结果的可靠性，将每种算法运行10次，然后取各评价指标均值。不同算法训练集与测试集结果如表3所示，4种算法所建数据模型精度均比较高，在训练集中RF算法的MAE优于其他算法，但对于其他指标，SVR算法更具有优势。与BP、ANN、RF算法相比，SVR在RSME指标上分别降低了13.04%、4.76%、27.27%，在R^2上分别提升了3.03%、3.94%、2.93%。同时，在测试集中SVR算法各项指标皆优于其他算法，仅在MAE上稍大于ANN算法。综上分析，SVR算法更适用于本文的模型构建，SVR训练集与测试集预测结果对比如图5所示。因此，本文选用SVR算法构建转炉数据模型，作为优化部分的目标函数。

表3 模型性能指标对比

方法	训练集指标			测试集指标		
	MAE	RMSE	R^2	MAE	RMSE	R^2
SVR	0.065	0.040	0.950	0.064	0.033	0.943
BP	0.071	0.046	0.922	0.068	0.045	0.902
ANN	0.073	0.042	0.914	0.063	0.048	0.917
RF	0.063	0.055	0.923	0.071	0.051	0.919



(a) 训练集 (b) 测试集

图 5 SVR 训练集与测试集预测结果对比

5.3 优化结果与分析

根据转炉能耗模型以及约束条件，建立工艺参数节能优化模型。采用HOA优化算法进行优化模型求解，得到最优吨钢能耗下的废钢比、铁水入炉温度、吹氧强度的工艺参数组合。并与遗传算法（Genetic Algorithm，GA）、模拟退火算法（Simulated Annealing，SA）和粒子群优化算法（Particle Swarm Optimization, PSO）进行对比。为确保4种算法对比结果的可靠性，将迭代次数、种群数目等设置为相同值，进行迭代优化，结果如图6所示。4种算法迭代收敛情况以HOA算法最优，收敛速度最快，且最终得到的最小目标函数值也优于其他三种算法，证明了本文采用HOA算法优化求解的可靠性与优越性。

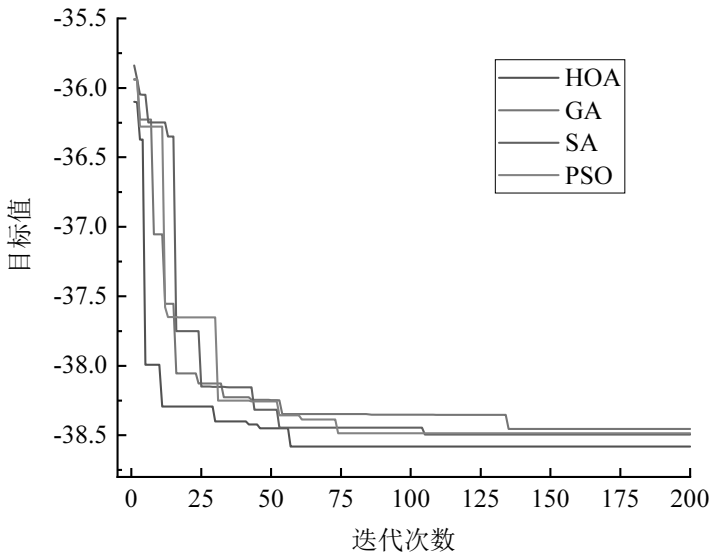


图6 4种算法的收敛对比

本文将采用数值模拟方法对优化结果进行对比分析，将转炉废钢比、铁水入炉温度、吹氧强度的优化值和经验值产生的转炉能耗进行对比。为确保方法的可靠性，选取了3组经验数据进行对比，优化结果

对比如表4所示。经优化后的废钢比为29.8%，铁水入炉温度为1323.86℃，吹氧强度为3.843 $m^3/(min·t)$，吨钢能耗为-38.581kgce/t。优化参数组的能耗均小于3组经验值产生的能耗，且转炉吨钢能耗相比3组经验值分别降低了9.08%、11.14%和8.20%，证明了本文所提转炉工艺参数节能优化方法的有效性。

表4 优化结果对比

	废钢比（%）	铁水入炉温度（℃）	吹氧强度（$m^3·min^{-1}·t^{-1}$）	吨钢能耗（kgce/t）
优化值	29.8	1323.86	3.843	-38.581
经验值1	30.2	1345.00	4.027	-35.368
经验值2	30.5	1372.00	4.277	-34.713
经验值3	30.8	1334.00	3.924	-35.657

6 结束语

（1）系统地揭示了转炉的物质流与能量流特性，并以转炉炼钢能耗与工艺参数历史数据为基础，构建了基于支持向量机回归方法的转炉能耗模型。

（2）构建了以吨钢能耗为目标，以废钢比、吹氧强度、铁水入炉温度为优化变量的转炉工艺参数节能优化模型，并采用徒步优化算法进行优化求解，经实际生产数据验证，可降低转炉能耗8.20%以上。

（3）在钢铁实际生产中，碳排放和成本也是钢铁企业关注的重点，因此，下一步工作将研究同时考虑钢铁冶金设备能耗、碳排放及成本的多目标优化方法。

参考文献

[1] 袁喻兴, 闫天一, 那洪明, 等. 炼铁系统能耗和成本的集成优化及分析[J]. 中国冶金, 2022, 32(01): 97-103. YUAN Y, YAN T, NA H, et al. Integrated optimization and analysis of energy consumption and cost in ironmaking system[J]. China Metallurgy, 2022, 32(01): 97-103.

[2] QIU Z, SUN J, DU T, et al. Impact of hydrogen metallurgy on the current iron and steel industry: A comprehensive material-exergy-emission flow analysis[J]. Applied Energy, 2024: 122452.

[3] YANG Y, ZHANG L, YUAN Y, et al. Muti-objective optimization on energy consumption, CO2 emission and production cost for iron and steel industry[J]. Journal of Environmental Management, 2023: 119102.

[4] SHAO X, LIU Q, XIN Z, et al. Hybrid model for BOF oxygen blowing time prediction based on oxygen balance mechanism and deep neural network[J]. International Journal of Minerals, Metallurgy and Materials, 2024, 31(1): 106-117.

[5] WANG D, BAO Y, GAO F, et al. Hybrid model for predicting oxygen consumption in BOF steelmaking process based on cluster analysis[J]. steel research international, 2023, 94(1): 2200595.

[6] 阳青锋, 赖旭芝, 杜胜, 等. 基于粒度聚类的转炉炼钢氧气消耗量预测[J]. 自动化学报, 2024, 50(1): 132-142.

YANG Q, LAI X, DU S, et al. Converter Steelmaking Oxygen Consumption Prediction Based on Granularity Clustering[J]. Acta Automatica Sinica, 2024, 50(1): 132-142.

[7] SHI C, WANG B, GUO S, et al. Energy consumption prediction of steelmaking process based on improved whale optimization algorithm and stochastic configuration network[J]. JOM, 2023, 75(10): 4320-4331.

[8] WANG Y, WEN Z, YAO J, et al. Multi-objective optimization of synergic energy conservation and CO_2 emission reduction in China's iron and steel industry under uncertainty[J]. Renewable and Sustainable Energy Reviews, 2020: 110128.

[9] NA H, SUN J, QIU Z, et al. Optimization of energy efficiency, energy consumption and CO_2 emission in typical iron and steel manufacturing process[J]. Energy, 2022, 257: 124822.

[10] YANG Y, ZHANG L, YUAN Y, et al. Muti-objective optimization on energy consumption, CO_2 emission and production cost for iron and steel industry[J]. Journal of Environmental Management, 2023, 347: 119102.

[11] ZHANG Q, WEI Z, MA J, et al. Optimization of energy use with CO_2 emission reducing in an integrated iron and steel plant[J]. Applied Thermal Engineering, 2019, 157: 113635.

[12] 陈光, 胡鹏, 包向军, 等. 基于柜位预测的转炉煤气热值优化模型[J]. 钢铁, 2024, 59(3): 197-206.
CHEN G, HU P, BAO X, et al. Optimization model of converter gas calorific value based on cabinet location prediction[J]. Iron & Steel, 2024, 59(3): 197-206.

[13] BALOGUN A L, REZAIE F, PHAM Q B, et al. Spatial prediction of landslide susceptibility in western Serbia using hybrid support vector regression (SVR) with GWO, BAT and COA algorithms[J]. Geoscience Frontiers, 2021, 12(3): 101104.

[14] LIU K, LIN T, ZHONG T, et al. New methods based on a genetic algorithm back propagation (GABP) neural network and general regression neural network (GRNN) for predicting the occurrence of trihalomethanes in tap water[J]. Science of the Total Environment, 2023, 870: 161976.

[15] IKRAM R M A, EWEES A A, PARMAR K S, et al. The viability of extended marine predators algorithm-based artificial neural networks for streamflow prediction[J]. Applied Soft Computing, 2022, 131: 109739.

[16] FAN G F, ZHANG L Z, YU M, et al. Applications of random forest in multivariable response surface for short-term load forecasting[J]. International Journal of Electrical Power & Energy Systems, 2022, 139: 108073.

[17] OLADEJO S O, EKWE S O, MIRJALILI S. The Hiking Optimization Algorithm: A novel human-based metaheuristic approach[J]. Knowledge-Based Systems, 2024, 296: 111880.

[18] GOODCHILD M F. Beyond Tobler’s hiking function[J]. Geographical Analysis, 2020, 52(4): 558-569.

[作者简介]

敬培锋（2000 年—），男，重庆大学硕士研究生，主要研究方向为智能制造、绿色制造。

李聪波（1981 年—），男，博士，重庆大学教授，主要研究方向为绿色制造、智能制造系统、制造系统工程。

史春燕（1987 年—），女，硕士，高级工程师，主要研究方向为钢铁企业智慧能源管控体系及系统研究。

吴畏（1995 年—），男，博士，重庆大学助理研究员，主要研究方向为智能工厂，智能制造系统，智能算法，工业室内定位。

李博（1996 年—），男，重庆大学博士研究生，主要研究方向为智能制造、绿色制造。

3DGLS: A Location Scheme based on 3D Geo-Magnetic Sensors for Multi-Workshop and Multi-Production Line Optimization

Yu Tang[1], Xiaolong Xu[2, *] and Honghao Gao[3, 4, *]

[1] Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, Nanjing University of Posts and Telecommunications, China

[2] School of Computer Science, Nanjing University of Posts and Telecommunications, China

[3] School of Computer Engineering and Science, Shanghai University, China

[4] College of Future Industry, Gachon University, Korea

Abstract: In the optimization of production processes across multi-workshop and multi-line environments, location-based services (LBS) play a crucial role. By enabling the positioning and monitoring of workers, LBS facilitate optimized management of production flows, enhancing both efficiency and safety. Among the various indoor positioning technologies, geomagnetic fields have garnered extensive attention from the commercial and academic sectors due to their advantages of passivity, low cost, and lack of radiation. Despite the rich information content of geomagnetic fields, current indoor positioning solutions can only utilize the total intensity of the geomagnetic field as an auxiliary matching condition due to sensor precision limitations. To address these issues, this paper conducts an in-depth study of geomagnetic field information in indoor environments and proposes an indoor positioning mechanism utilizing geomagnetic fields. This mechanism first employs a geomagnetic information solution algorithm to resolve the geomagnetic field information into three-dimensional geomagnetic feature information. Then, the three-dimensional geomagnetic information is used to construct a geomagnetic fingerprint map, which is employed for positioning and updating the geomagnetic fingerprint map within indoor environments. Finally, the performance of the proposed indoor positioning mechanism based on geomagnetic fields is validated through experiments.

Keywords: indoor positioning; 3D; geomagnetic filed; fingerprint map; sensor error; attitude angle

1. INTRODUCTION

In optimizing production processes across multi-workshop and multi-line environments, positioning technology plays a crucial role by accurately obtaining the location information of production units along assembly lines through various sensors (such as GPS, inertial navigation, etc.) or base station signal strength. This information provides a solid foundation for subsequent management decisions. Consequently, location-based services (LBS) in indoor environments have garnered increasing attention, bringing significant convenience and commercial value to industrial production processes [1-2].

Ongoing research in indoor positioning technology within both academic and industrial sectors has led to significant advancements. Positioning technologies using electrical signal sources, such as Wi-Fi, in indoor environments have reached a high level of maturity [3].

These positioning algorithms primarily use signals to measure distance and calculate the location of the sub-

This work was supported by the National Natural Science Foundation of China under grant No. 92367103. (Corresponding authors: Xiaolong Xu and Honghao Gao)

E-mail addresses: 2022040516@njupt.edu.cn(Y. Tang), xuxl@njupt.edu.cn(X. Xu), gaohonghao@shu.edu.cn(H. Gao)

ject according to geometric principles. However, in indoor environments, various complexities such as complex structures and high foot traffic can impact the accuracy of these algorithms. Additionally, some positioning technologies are affected by the multipath effect and Doppler effect of signals. To address these challenges and achieve reliable indoor positioning, several optimized positioning mechanisms have been developed. These include the Active Bat positioning mechanism [4], Easy Living positioning system [5], Smart Floor positioning system [6], Spot On positioning mechanism [7], Pin Point 3D-ID positioning mechanism [8], Radar positioning system [9], Hiball Tracker positioning system [10], and Aero Scout positioning system [11]. These systems often integrate multiple positioning mechanisms to mitigate the shortcomings of individual approaches.

Due to the influence of signal attenuation and the multipath effect of electrical signals, non-electrical signal sources have gradually attracted the attention of experts and scholars. Consequently, researchers are increasingly interested in using the geomagnetic field as a source of indoor positioning signals [12]. As is well known, the geomagnetic field is a fundamental property of the Earth, composed of several different magnetic fields, and characterized by full coverage and rich information. The geomagnetic field contains abundant position-related information, such as the three-component characteristic data quantified by the magnetic field in the sensor coordinate system. Compared with conventional radio signal sources, the geomagnetic field signal source offers stability and requires no power maintenance, which provides significant advantages in terms of energy consumption and ensures stable signals in blackout situations.

Therefore, the geomagnetic field becomes an excellent signal source for indoor positioning technology. However, due to sensor errors and other factors, the geomagnetic field can only be used as an auxiliary reference in indoor positioning technology. If we use the intensity of the magnetic induction tangent of the geomagnetic field as the reference information, we overlook the directional information of the geomagnetic field. Therefore, we first calculated the directional information based on the characteristics of the geomagnetic field. Then, in the indoor environment, we designed a fingerprint map construction method based on the particularities of the geomagnetic field.

The geomagnetic field information is acquired by sensors, but the limitations in technology and cost of micro-electro-mechanical systems (MEMS) [13] make these sensors less accessible. Due to the particularities of magnetometers, the magnetic values read by sensors can vary significantly. In our experiments, we found that the magnetic values read by two smartphones of the same model at the same position were significantly different. Therefore, sensor error is also a key problem to be addressed. While the geomagnetic field often seems unstable, data monitored by the China Geological Bureau shows that the geomagnetic field on the Earth's surface is quite stable. Over a month, the indoor geomagnetic field is uniquely distributed and stable. However, with the Earth's revolution and other factors, the geomagnetic field changes over longer periods. Moreover, the geomagnetic field is highly dependent on the environment, especially the presence of electrical equipment, which significantly impacts the surrounding geomagnetic field. This is a problem that needs to be resolved. Therefore, to use the geomagnetic field for indoor positioning, we must address these key challenges.

In summary, the main contributions of this paper are as follows:

(1) We conducted in-depth research and analysis on the inherent attributes of the geomagnetic field and designed a feasible geomagnetic fingerprint map construction scheme based on the unique

characteristics of the geomagnetic field. This algorithm utilizes the irregular distribution of the geomagnetic field in indoor environments for constructing the geomagnetic fingerprint map, taking into account the particularities of non-electrical signal sources.

(2) We considered both the characteristics of the geomagnetic field and the impact of sensor errors on the geomagnetic data. For instance, magnetic sensor reading errors can be caused by different hardware configurations, the electric current of the smartphone itself, and the electric current of external powered devices.

(3) Upon completing the construction of the geomagnetic fingerprint map, we addressed the challenge of updating the map when significant changes occur in the indoor environment layout, which can alter the magnetic field distribution.

II. RELATED WORK

The existence of geomagnetic field is not affected by space, which makes the geomagnetic field has the natural advantage of becoming the location signal source. In the indoor scene, due to the influence of reinforced concrete in the building on the geomagnetic field, the influence will be transformed into another a stable and special magnetic field distribution. In recent years, business and academic circles have conducted a series of research on it. IndoorAtlas in Finland is the first commercial company to apply the geomagnetic field to positioning. Not only the business community has obtained considerable results, but also the academic community has a lot of research results. The magnetic field technology is used to realize the positioning of the micro-capsule lens [14], which generates a magnetic field according to the requirements, and then carries out the positioning and operation of the micro-capsule lens. The authors in [15] study the matching of fingerprint map in the offline situation, especially how to achieve the matching of fingerprint map in different complex indoor scenes. The authors in [16] propose a sequence matching method similar to geomagnetic field under the premise of Wi-Fi fingerprint map, which can effectively improve the efficiency of matching and constructing fingerprint map. An indoor positioning system, BASMAG, is proposed in [17], which completely uses the geomagnetic field as the fingerprint map combined with the pedestrian reckonings algorithm to achieve indoor positioning requirements.

III. Method

A. The architecture of 3DGLS

The whole structure of 3DGLS is composed of two modules: fingerprint map construction module and fusion positioning module. They are working in construction stage of the geomagnetic fingerprint map and the navigation and positioning stage. The whole system architecture is shown in Figure 1.

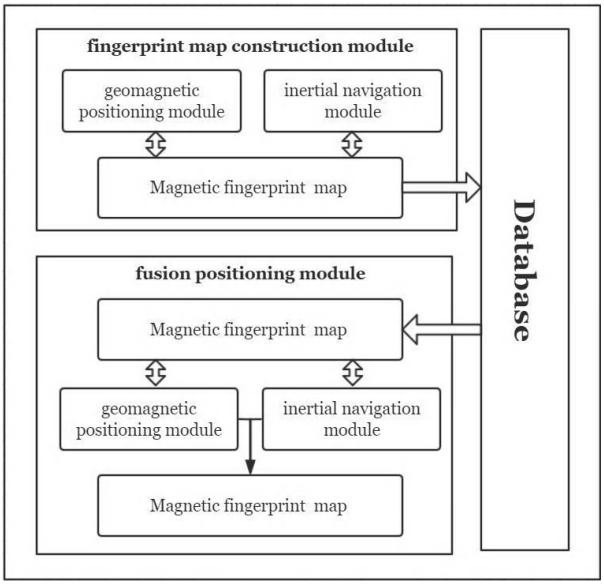


Figure 1. Geomagnetic indoor positioning system of 3DGLS architecture diagram.

In the first stage, the geomagnetic positioning module obtains the original data by calling the three sensors of the geomagnetic sensor, accelerometer and gyroscope in the smart phone. Then the geomagnetic positioning module calculates the geomagnetic data to get the geomagnetic characteristic information, and the inertial

navigation module processes the accelerometer and gyroscope data to get the step number, step size and attitude angle information. The path coordinates of pedestrians can be calculated by calculating the information of attitude angle, step number and step length. The fingerprint map can be constructed with the coordinate information and geomagnetic field characteristic information.

In the second stage, the fusion positioning module also obtains the geomagnetic information, acceleration information and gyroscope information at this time through magnetometer, accelerometer and gyroscope. The same method is used to calculate the feature information of geomagnetic information, and then the feature information is compared with the fingerprint map in the database, and the corresponding plane coordinate information can be returned when the matching results are suitable. The location service is completed when the coordinate position is displayed.

B. Fingerprint map

1) Geomagnetic North Pole and geographical North Pole.

Geomagnetic field is a three-dimensional space field. Mathematical functions are used to describe the upper geomagnetic field of the earth in the study of geomagnetic field. At present, the mainstream function describing the distribution of the main magnetic field is usually expressed by spherical harmonic series [17], which divides the geomagnetic field into the sum of equal components of dipole and quaternary. The position r and time t of the geomagnetic field B can be expressed by the following formula.

$$B(r,t)=B_m(r,t)+B_c(r,t)+B_d(r,t) \quad (1)$$

where B_m is the home field of the geomagnetic field, B_c is the magnetic field on the earth's surface, and B_d is the magnetic field produced by the high atmosphere and solar particles. We mainly use the two magnetic fields B_m and B_c for positioning and navigation. The geomagnetic field exists at any point on the surface of the earth. Let us assume that one of these points is the origin O. From this origin we generate a three-dimensional coordinate system whose three axes are perpendicular to each other. The vertical horizontal downward axis is denoted as the Z axis, and the X axis and Y axis form the horizontal plane, which is parallel to the ground plane. We do not specify the X and Y directions of that coordinate system at this time. In a coordinate system such as Figure 2, the tangent line of the geomagnetic field at point O is the space vector $\overrightarrow{OM}$, and the starting point is at point O, and the ending point is at M.

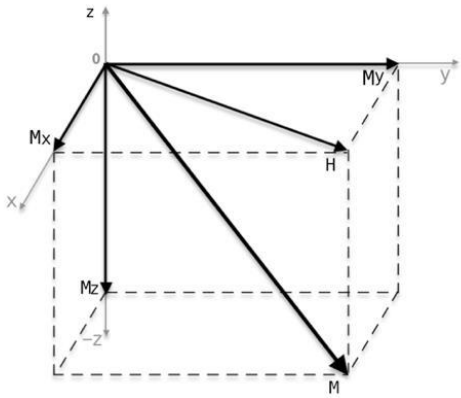


Figure 2. Tangent line of magnetic induction line at a point.

Since the geomagnetic field is an actual physical property, but it cannot be seen or touched, we describe it in the form of magnetic induction lines. Assuming that the tangent line of the geomagnetic field at the origin O is a vector $\overrightarrow{OM}$, then the total magnetic field intensity at this point is following formula.

$$\left|\overrightarrow{OM}\right|=\sqrt{M_x^2+M_y^2+M_z^2} \quad (2)$$

where $\left|\overrightarrow{OM}\right|$ is the total strength of the geomagnetic field, M_x, M_y and M_z are the components of the coordinate system along the X, Y and Z axes. In a spatial rectangular coordinate system, we can express the angles between vectors in terms of the proportions of the components of each coordinate system. Firstly, the vector $\left|\overrightarrow{OM}\right|$ is projected onto the horizontal plane, and H represents the projection of the tangent line of the magnetic induction line on the horizontal plane.

$$H=\sqrt{M_x^2+M_y^2} \quad (3)$$

where M_x and M_y are the components of the tangent line of the magnetic induction line on the X and Y

axes. At this point, we set the Angle between the horizontal component and the Y axis as the deviation Angle of the tangent line of the magnetic induction line at this point, which is denoted as D. Then the deflection Angle can be expressed by the following formula.

$$D = \arctan \frac{M_x}{M_y} \tag{4}$$

The Angle between the total magnetic field intensity at this point and the horizontal plane is denoted as the inclination Angle of the tangent line of the magnetic induction line at this point, denoted as I. Then the inclination can be expressed by the following formula.

$$I = \arctan \frac{M_z}{H} \tag{5}$$

where M_z is the component of the tangent of the magnetic induction line in the Z axis, and H is the composite quantity of the tangent of the magnetic induction line in the horizontal plane. In this way, the geomagnetic field can be numerically represented in terms of its properties. It should be noted here that the reference coordinate system for the inclination angles D and I specified here is the coordinate system itself, which should be distinguished from the magnetic declamation Angle and magnetic inclination Angle.

The geomagnetic field exists at any point on the surface of the earth. We assume that one of these points is the origin O, and generate a three-dimensional coordinate system. The vertical horizontal downward axis is Z axis, the X axis and Y axis form the horizontal plane, which is parallel to the ground plane. We do not specify the X and Y directions of that coordinate system at this time. In the coordinate system shown as Figure 2, the tangent line of the geomagnetic field at point O is the space vector $\overrightarrow{OM}$.

As shown in Figure 3, the Y axis coincides with the geographic North Pole, and the X axis coincides with the geographic east. The horizontal projection direction H of this point is geomagnetic north, while the geographic North Pole is in the direction of the Y axis. In this case, the Angle between the geomagnetic North Pole and the geographic North Pole is called magnetic declination. The direction read by the smart phone sensor is the geomagnetic North Pole direction of the position, while the geographic North Pole needs to be corrected by the geomagnetic North Pole and the magnetic declination.

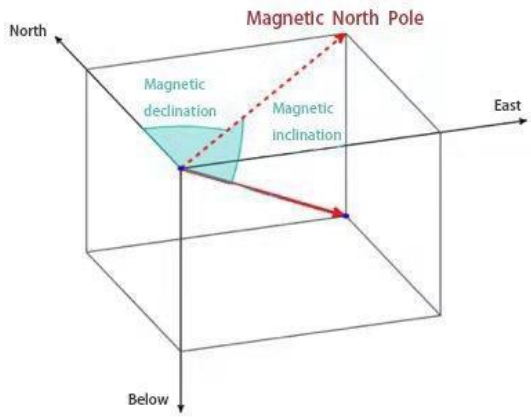


Figure 3. Magnetic North Pole and Geographic North Pole Schematic Map.

2) Sensor error and attitude angle calculation

In the experiment, we found it will bring great errors to the data collection because of the technology and cost control of the sensor and the smart phone itself [18]. This influence is mainly divided into two aspects: the error of attitude Angle and magnetometer data acquisition.

In order to solve fluctuation during sampling, we increase sampling frequency of the sensor, and smooth the sampled data by mean filter. We found in the experiment that when constructing the fingerprint map, different sensors had the same change rule for the same path. Therefore, this problem needs to be solved during the overall maintenance and update of the fingerprint map.

The error of attitude angle mainly comes from the heading angle Yaw. 3DGLS mainly use gyroscope, magnetometer and accelerometer to obtain the attitude angle of mobile phones. The roll angle $Roll$ and pitch angle $Pitch$ in the attitude angle can be realized by the complementary filtering algorithm of gyroscope and accelerometer, and the heading angle Yaw is the most important problem to be solved. In the experiment, we realized the idea of using the extended Kalman filter to obtain a stable attitude angle.

The basic Kalman filter algorithm uses a linear random difference equation to estimate the current state.When the state estimation relation and measurement relation are nonlinear in practice, the extended Kalman filter algorithm is proposed to solve the nonlinear problem.

In the process of constructing the geomagnetic fingerprint map, we used the attitude angle acquisition method integrated by the Android system, but there are obvious errors and fluctuations in actual use [19]. Therefore, we design a set of stable attitude angle algorithm for smart phone attitude angle from the sensor level, and it is found in the experiment that the attitude angle provided by this algorithm has a great performance improvement. We use the interface of the Android system to directly obtain the original data of the sensor, and use the algorithm flow as shown in Figure 4 to calculate the attitude angle.

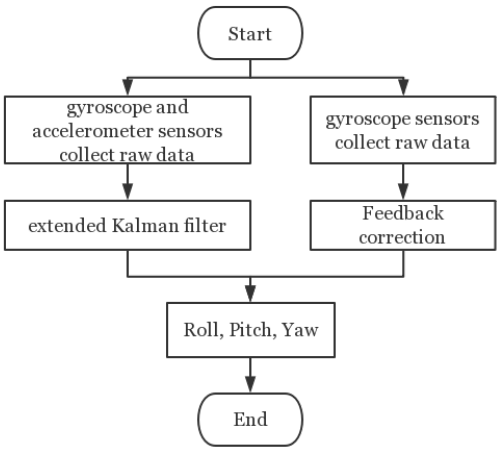


Figure 4. Workflow of Attitude Angle calculation.

Step 1: Use the interface provided by Android platform to obtain the original data of the accelerometer and gyroscope.

Step 2: Steps 2 and 3 are the main process for extending Kalman. In Step 2, the original data obtained by the accelerometer was sent into the extended Kalman matrix [20] to calculate the state transition matrix $R_k^{\square}$ and observation matrix H. In the application of the extended Kalman filter, we take the horizontal state obtained by the accelerometer as the state quantity x_k in the Kalman filter, where k is the time series. We take the change of gyroscope on the X and Y axes as the observation variable z_k. Since the model is a nonlinear model, we need to convert the state quantity and observation quantity into the form of nonlinear random difference equation as Equation (6).

$$x_k = f\left(x_{k\square 1}, u_{k\square 1}, w_{k\square 1}\right) \quad (6)$$

The observed variable is in Equation (7).

$$z_k = h\left(x_k, v_k\right) \quad (7)$$

In the above equations, u_{k-1} and $w_{k\square 1}$ are the observation noise and excitation noise at the last moment. x_{k-1} is the state quantity at time $k-1$, the nonlinear function f in the difference equation maps the state $k\square 1$ at the previous time to the state at the current time k. v_k is the measurement noise of the observation function. The nonlinear function h reflects the relationship between the state variables x_k and z_k. When inputting the acceleration parameter, we will set $v_{k\square 1}$ and $w_{k\square 1}$ default to 0, and then calculate the Jacobian A of the partial derivative of f with respect to x.

$$A_{[i,j]} = \frac{\square f_{[i]}}{\square x_{[j]}}(x_{k\square 1}, u_{k\square 1}, 0) \quad (8)$$

The Jacobian W of the partial derivative of f with respect to w is

$$W_{[i,j]} = \frac{\square f_{[i]}}{\square w_{[j]}}(x_{k\square 1}, u_{k\square 1}, 0) \quad (9)$$

The Jacobian H of the partial derivative of h with respect to x is

$$H_{[i,j]} = \frac{\square h_{[i]}}{\square x_{[j]}}(x_k, 0) \quad (10)$$

The Jacobian V of the partial derivative of h with respect to v is

$$V_{[i,j]} = \frac{\square h_{[i]}}{\square v_{[j]}}(x_k, 0) \quad (11)$$

We need to use the state quantity to calculate the state

variable and error covariance P_k of the prediction stage with

$$P_k^{\square} = A_k P_{k-1} A_k^T + W_k Q_{k-1} W_k^T \quad (12)$$

Q_k is the covariance matrix of process excitation noise at the moment k.

the prediction stage of the extended Kalman filter has so far been completed. In this step, we use the original three-axis data of the accelerometer to calculate the state variable at time k and the error covariance P_k of the state variable.

Step 3: We take the change of gyroscope on the X axis and Y axis as the observation quantity of the extended Kalman filter, but in this step, we update the extended Kalman filter, and we use the relevant results calculated in Step 2 to carry out relevant calculations.

First we need the error covariance P_k in step 2 to calculate the Kalman gain K_k with

$$K_k = P_k^- H_k^T \left(H_k P_k^- + V_k R_k^- V_k^T \right)^{-1} \quad (13)$$

where R_k is the covariance matrix of the observed noise at the moment k.

In the next step, we will update the state quantity x_k according to the observed quantity z_k, and update the error covariance P_k, then return the updated state quantity and error covariance to the prediction stage in Step 2.

$$\hat{x}_k = \hat{x}_k^{\square} + K_k (z_k \square h(\hat{x}_k^{\square}, 0)) \quad (14)$$

$$P_k = (I \square K_k H_k) P_k^{\square} \quad (15)$$

At this point, the extended Kalman filter has completed a prediction and update work. In step 3 , we can constantly calculate the latest attitude angle $Roll$, $Pitch$ and Yaw through the Kalman filter. As shown in Figure 5, the accelerometer and gyroscope of a smart phone can form an overlapping plane on the horizontal plane, where $Pitch$ and $Roll$ angles share the same state and observation values on the two sensors [21]. However, only the gyroscope can detect the change of Yaw. As mentioned above, we cannot calculate the geomagnetic north of the magnetometer as a state quantity or observation quantity, so we need to calculate the Yaw angle. Then, we need to correct it in Step 4.

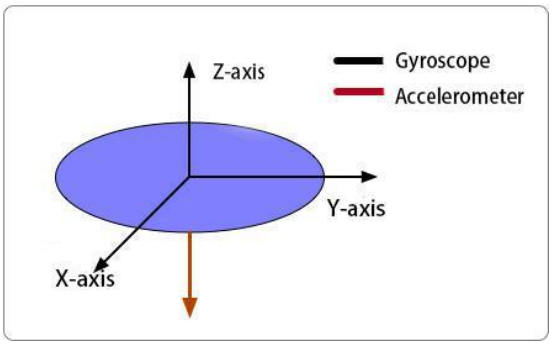


Figure 5. Accelerometer and gyroscope to solve the attitude Angle diagram.

Step 4: Through Step 3, We can get real-time attitude angle. However, due to the particularity of Yaw angle and the problem of zero-degree drift of gyroscope, we need to design a feedback adjustment system in Step 4. To be specific, we will design a timer tool to count the drift degree of the gyroscope within a period of time. This degree and time will fed back to the Yaw angle output in Step 3. Finally, we can use the accelerometer and gyroscope of the smart phone to get the relative attitude angle of the phone.

3) Calculation of geomagnetic information

In this section we will go through the details of implementing the 3DGLS. The geomagnetic fingerprint map designed has three geomagnetic characteristic information: the total intensity of the tangent of the magnetic induction line, the deviation and the inclination difference. As shown in Figure 6, The input of the geomagnetic information solution algorithm is the original geomagnetic data of the three axes and the attitude angle data, and the output is the three characteristic information of the geomagnetic field.

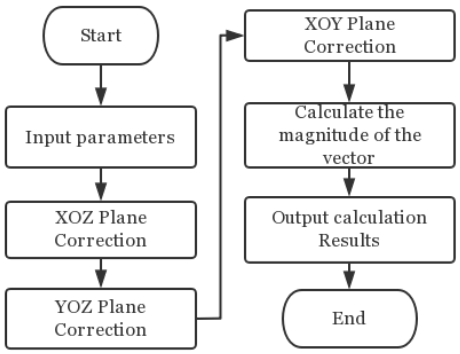


Figure 6. Workflow of geomagnetic information calculation algorithm.

The workflow of the algorithm includes the following steps:

Step 1: When the initial information is entered, the Yaw angle is 0°. The input parameter should be used to calculate the first location of the geomagnetic characteristics.

Step 2: Since the data measured by the three-axis sensor is related to the position of the coordinate axis, we should keep the direction and intensity of resultant field component unchanged during the conversion on the XOZ plane. As shown in Figure 7, the Y axis is vertical to the plane. First, the M_x and M_z components are synthesized into T on the horizontal plane XOZ, and then the XOZ plane is modified into a horizontal attitude according to the angle θ of the attitude angle $Roll$.

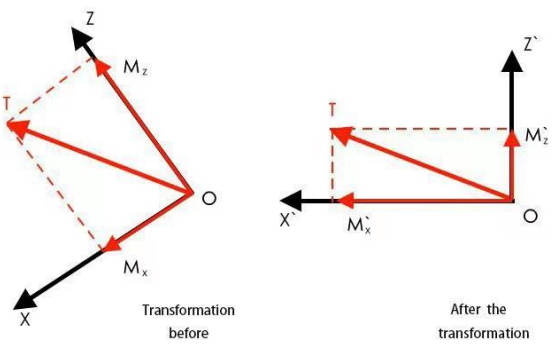


Figure 7. Angle conversion of XOZ plane magnetic field components.

Use the formula (16) to correct M_x and M_z.

$$\begin{aligned} M_x^{'} &= T \cdot \tan(\theta - \phi) \\ M_z^{'} &= T \cdot \cot(\theta - \phi) \end{aligned} \qquad (16)$$

The composition of the plane is $T = \sqrt{M_x^2 + M_z^2}$, the angle between the composition component and the X axis is $\phi = \arctan\frac{M_z}{M_x}$. The XOZ plane can be modified according to the above method, and then the impact of $Roll$ angle can be eliminated.

Step 3: Update the modified M_x and M_z components in Step 2 to the input of the geomagnetic field, and use the method similar to that in Step 2 to modify the YOZ plane to obtain the modified M_y and M_z components.

Step 4: The M_y and M_z components in Step 3 are updated to the input of the geomagnetic field. The method similar to Step 2 is used to modify the XOY plane to obtain the final M_x and M_y components. At this point, the angle conversion process is finished. The M_x, M_y, and M_z components are in the coordinate system when the sensor is initialized, and the declination angle D and inclination angle I of the tangent line of the magnetic induction line at that position are calculated.

Step 5: Calculate the length of the tangent line of the magnetic induction line as the information of the total magnetic field strength at this position.

Step 6: Output the deflection angle D, inclination angle I and total intensity T of the tangent line of the magnetic induction line obtained in Step 4 and 5.

At this point, the calculation of magnetic field angle information has been completed. After inputting the attitude angle information and the original triaxial magnetic force data, three geomagnetic characteristic information of this position were obtained through a series of solutions.

4) Fingerprint map construction

The tangent line of each coordinate of the geomagnetic field is inherent and stable in space, so we can construct the fingerprint map by combining the change of path with the change of angle information. As shown in Figure 8, we assume that positions A, B, C and D are four different positions, and the direction of the arrow is the projection of the magnetic induction tangent line of

the corresponding positions on the horizontal plane. We can see the effect as shown in the figure from the top down. We recorded the position of the mobile phone in coordinate system at position A, and the angle between the tangent line of magnetic induction line and the Y axis. When the position moves, we collect the new magnetic induction line information at position B by recording the angle between it and the coordinate axis Y axis, and mark it as θ_1. Then we move to position C, repeat the methods, marks the angle as θ_2. Using the same method, mark the angle as θ_3. These angle information and the corresponding position information are saved to construct the fingerprint map. When matching, using the same method, we can effectively solve the problem of reference frame.

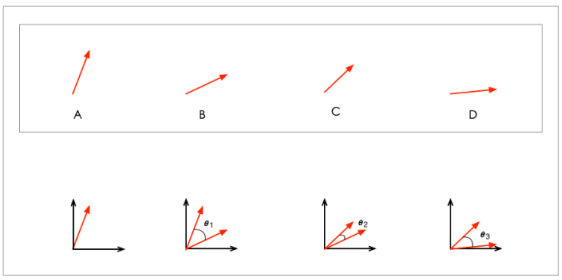


Figure 8. Geomagnetic fingerprint map construction.

Similarly, the inclination I is collected using the same principle. Through our research, a set of fingerprint map construction scheme suitable for geomagnetic field is designed as shown in Figure 9.

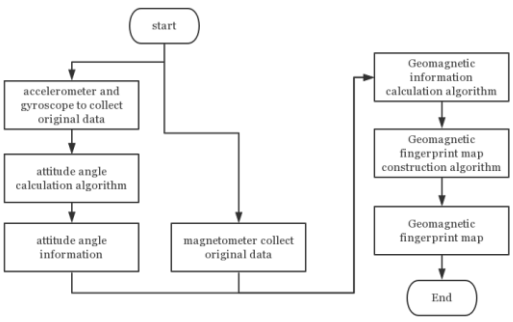


Figure 9. Workflow of geomagnetic fingerprint map construction.

The specific process is as follows.

Step 1: Use accelerometer, magnetometer and gyroscope to collect data in real time.

Step 2: We input the acceleration and angle data, and use attitude angle solution algorithm to get stable and accurate angle information.

Step 3: Use attitude information in Step 2 and the original geomagnetic data collected in Step 1 to calculate the information such as the total intensity of the tangent line of the magnetic induction line, the deflection angle and the inclination angle.

Step 4: The geomagnetic feature information obtained in Step 3 was stored in the database together with the position information obtained from the inertial navigation, to complete the construction of the geomagnetic fingerprint map.

C. Indoor location matching

1) Fingerprint map update and maintenance

No matter the positioning mode of electrical signal source or non-electrical signal source, we need to construct fingerprint map before use [22]. In the process of using the fingerprint map, we need to update it according to the changes of the environment. Therefore, we designed a set of geomagnetic fingerprint map construction mode based on swarm intelligence.

At the beginning of the construction, we can let users build their own fingerprint map. We integrate the data collected from the same building in the cloud and eliminate the differences in numerical values between the data collected by different smart phones. We integrate the data through dynamic time consolidation algorithm, so that multiple users can construct the same fingerprint map for the same building floor. The system will keep collecting the magnetic information of the location when positioning. We will update new data in the geomagnetic fingerprint map by making use of the information above. In this way, we can effectively solve the problem of magnetic field change.

2) Geomagnetic matching algorithm

We will introduce an algorithm similar to dynamic time warping [23] to solve the problem of inconsistent readings in the matching and construction of fingerprint maps.

The positioning stage is divided into two stages. In the first stage, we use geomagnetic data to obtain the initial position. In the second stage, we use Particle filter algorithm to correct the location in real time. When matching, we need to use Dynamic Time Warping(DTW) algorithm to match fingerprint map [24], so as to solve

the problem of non-uniform density of horizontal axis caused by the speed problem during the acquisition of fingerprint map.

The flowchart for obtaining the initial position is shown in Figure 10. The specific process of first stage is as follows.

Step 1: Register the accelerometer, gyroscope, and magnetometer, and calibrate the sensor using the word "8" around and place the smart phone on a horizontal plane.

Step 2: Pedestrians take the first step.

Step 3: Accelerometer, magnetometer, and gyroscope to obtain the initial data. The algorithm introduced in the 3.2.3 is used to solve the original geomagnetic data and obtain the matching feature information.

Step 4: Match the three feature information with the geomagnetic fingerprint database, and save the coordinate points within the threshold value range into the set.

Step 5: Pedestrians take the second step.

Step 6: We use the same algorithm as step 3, and match the characteristic values obtained by the processing with the next point of all coordinate points in the set obtained in Step 4. Update the matching results to the collection.

Step 7: Repeat Step 5 and Step 6 to update the coordinate points in the set until there is only one coordinate point in the set. At this time, return the coordinate point to get the initial position of the pedestrian.

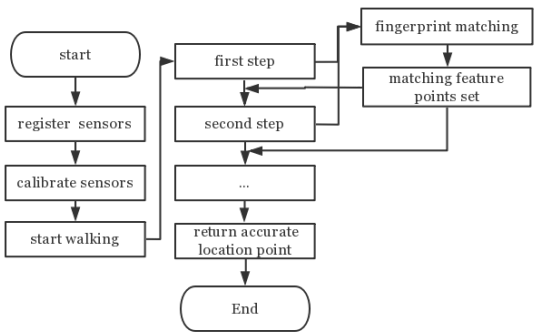


Figure 10. Workflow of geomagnetic matching to obtain the initial position.

After getting the initial location, the localization work moves into the second phase. We need to use the idea of particle filtering [24] to realize the process of constantly updating and revising the user's position. We divided the subsequent continuous update work into three parts: the prediction phase, the update phase and the resampling phase, which is shown in Figure 11. The specific process includes the following steps:

Step 1: After getting the initial position of the pedestrian, we use the accelerometer, gyroscope and magnetometer to obtain the next coordinate position by using the attitude angle solution algorithm and gait detection algorithm.

Step 2: At the same time, the original geomagnetic data collected on the path were processed by using the algorithm introduced in the matching module to obtain three geomagnetic characteristic values. The eigenvalue is matched with the geomagnetic fingerprint database to obtain the next matching rate of the suspicious set from the initial position, and then the best matching coordinate point is returned from the suspicious set according to the matching degree.

Step 3: By comparing the coordinate points of inertial navigation in the prediction stage and each suspicious coordinate point in matching, the coordinate of this position can be obtained.

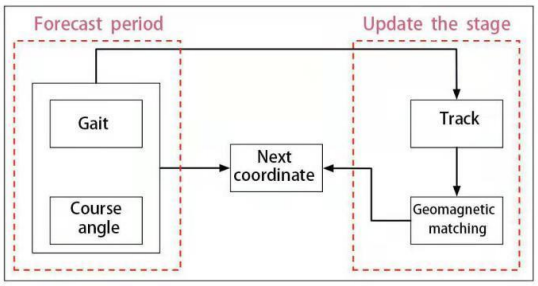


Figure 11. Schematic diagram of the second stage matching method.

After the two stages, we can obtain the indoor position in real time by using the geomagnetic field. At the same time, the geomagnetic information collected will be fed back to the geomagnetic fingerprint map for updating and revising.

IV. Results

A. Performance indicators

When evaluating the positioning accuracy of a positioning algorithm, the straight-line distance between the

positioning coordinate and the actual position coordinate is usually the most common standard.

$$d_{error} = \sqrt{(x_l - x_r)^2 + (y_l - y_r)^2} \quad (17)$$

where d_{error} is the distance between the actual position and the positioning coordinate, x_l and y_l are the position obtained during positioning, and x_r and y_r are the actual coordinates.

Most location algorithms based on geomagnetic field only use the total intensity of the tangent line for matching, while two angle information are used in 3DGLS, so we will not compare these two kinds of methods.

Because the matching effect of the fingerprint map is related to the database, the matching effect and error of different fingerprint data are analyzed in this paper.

B. Experimental environment and process

The experimental environment of this paper is the corridor of the subject building of the School of Computer Science. There are continuous path, corner and other special positions, which is more in line with the requirements of verification of positioning effect. As shown in Figure 12, we used the Android platform to display the floor plan on the screen. At this point, each pixel of the plane graph has an (x,y) coordinate. We will add a series of sampling points to the plane graph, and we need to start at one of the points and go through the sampling points.

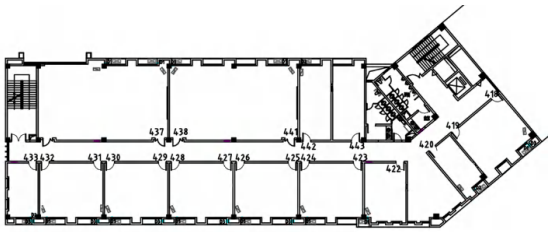


Figure 12. Experiment Scene Diagram.

Through the inertial navigation module, we can generate the path of the positioning stage based on the actual number of steps, step size and attitude angle. The walking track is shown in Figure 13.

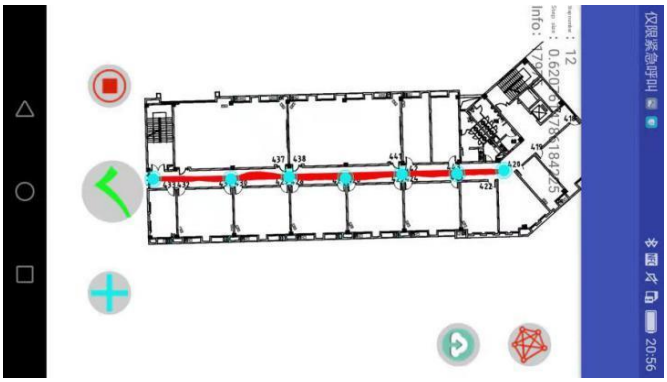


Figure 13. Map of geomagnetic data collected in the experiment.

We can obtain the geomagnetic field characteristic information on the path by using the algorithm introduced in the Section 3 and generate the fingerprint map by one-to-one correspondence with the above coordinate information. In the positioning stage, we choose the path as shown in Figure 13 for testing on the floor where fingerprints were collected.

C. Experimental verification and analysis

In this section, we conduct experiments and analyses from two aspects. According to the geomagnetic information solution algorithm, we first calculate the magnetic information collected on the same path, and compare the similarity of the three-feature information, and then test the positioning effect. Since 3DGLS is based on the geomagnetic field information, the positioning effect of the eigenvalue calculated by using only the total magnetic field strength and the geomagnetic information proposed in this paper will be compared in the test.

1) Comparison experiment of geomagnetic information eigenvalues

In the above experimental environment, the experimenter held Honor8 and Redmi Note 3 smart phones in both hands and kept the distance between at more than 50cm. From one side of the corridor in the experimental environment to the other side at a constant speed. The smart phones are used to collect and process the magnetic information along the path simultaneously. After the collection is completed, we use MATLAB software to read out the data stored in the database, and draw the characteristic information of the two smart phones in the figure.

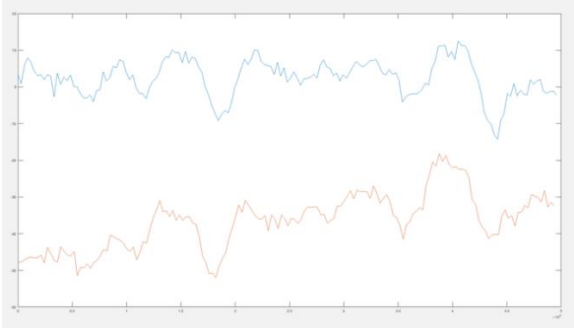


Figure 14. geomagnetic inclination eigenvalue matching map

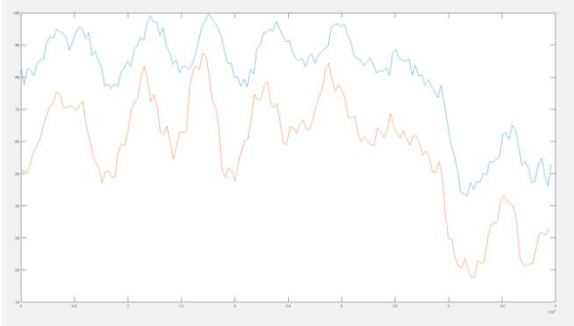


Figure 15. magnetic declination eigenvalue matching map

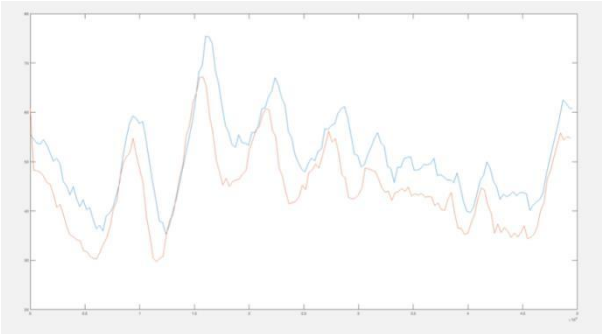


Figure 16. geomagnetic total intensity eigenvalue matching map

As the figures shown, when two smart phones move along the same path, the collected value of the total strength of the geomagnetic field has some errors, but the change rules are similar. The feature information of geomagnetic declination angle and geomagnetic inclination angle we proposed also have a high similarity. Compared with the total intensity of geomagnetic field, the characteristic information proposed in this paper can achieve the effect of data matching. The experimental results show that different types of smart phones will produce certain differences in the numerical values, while the construction of geomagnetic fingerprint map solution introduced in this chapter can solve this problem. Therefore, the three feature information based on geomagnetic field in 3DGLS are effective.

2) Comparison test of positioning error

We test the performance of the two stages: initial position matching stage and positioning stage. Similar to the calculation time of the initial position signal of Wi-Fi and other wireless signals, the geomagnetic field requires users to walk on the path to obtain geomagnetic information so as to match the initial position. Therefore, this part of the test is still compared vertically with the popular geomagnetic positioning method, to verify the applicability of the 3DGLS. The second stage is the matching error stage. In this stage, the most conventional positioning error model is used to measure the positioning accuracy. According to the different capacity of the geomagnetic fingerprint database, the locating error is tested.

we carried out experimental verification and analysis based on geomagnetic information. First, we choose a segment of the scene constructed by fingerprint map as the standard path of location test. As shown in Figure 17, the tester starts from point A and carries out the test on the premise that the mobile phone posture is stable. The position of point B is the result of the first stage of positioning, namely the coordinate position of the initial matching. It is used to update the matching results in the second stage.

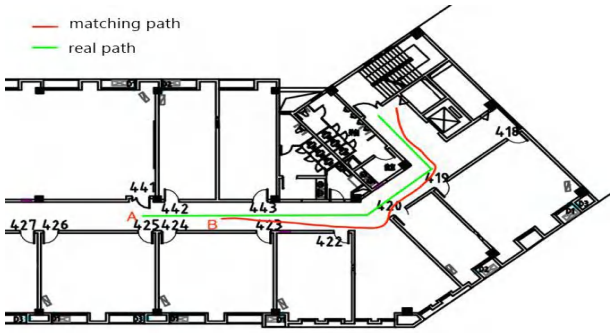


Figure 17. Positioning test path diagram.

The capacity of the geomagnetic fingerprint map will affect the matching efficiency, so we carried out a comparative experiment on the number of steps needed to walk in the initial position at different capacities. The experimental results are shown in Figure 18.

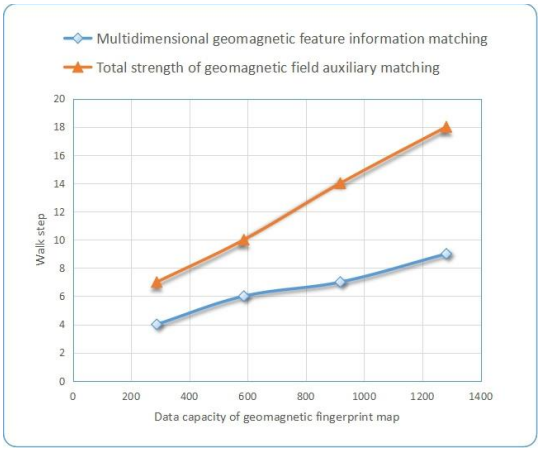


Figure 18. Comparison diagram of first stage matching performance of different geomagnetic feature information.

In the first stage experiment as shown in Figure 18, the horizontal axis is the number of fingerprint map capacity, and the vertical axis is the number of steps. For example, in the capacity of 288 fingerprint map, 4 steps are needed to match the initial position, while 7 steps are needed to use the total strength of geomagnetic field. Therefore, it shows that in the first stage of matching, the capacity of the geomagnetic fingerprint map has a certain influence on the matching efficiency. Therefore, the efficiency of geomagnetic matching can be effectively improved by using the 3DGLS proposed in this paper.

In the second stage positioning error experiment, the capacity of geomagnetic fingerprint map has little influence on the error. Therefore, we conduct an experimental analysis on the positioning error of 1282 fingerprint maps with the capacity here. The Euclidean distance between the real position and the location position is used as the error standard, and the corresponding CDF chart is drawn according to the location error.

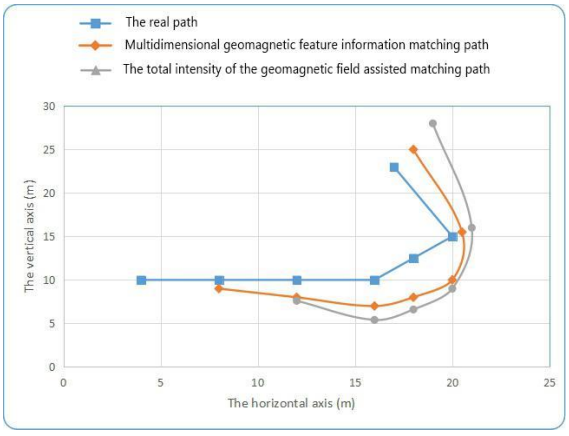


Figure 19. Schematic diagram of test path.

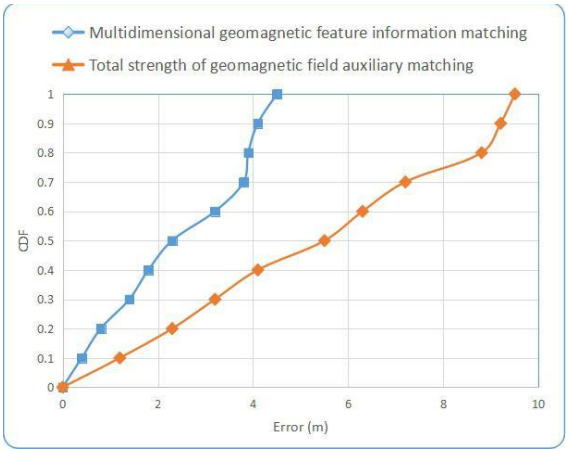


Figure 20. Schematic diagram of test path.

Figure 19 shows the comparison of the real path matching results between the calculated eigenvalues using the total geomagnetic field strength and the geomagnetic information in this paper. According to the errors in the above experiments, the CDF diagram is drawn as shown in Figure 20.

V. Conclusions

This paper mainly focuses on the research of geomagnetic field in indoor positioning technology. The geomagnetic field, as a passive, non-radiation, and stable existence, has received great attention. Due to a variety of technical limitations, the application of geomagnetic field in indoor positioning only uses the total intensity as a reference for positioning matching. In this way, a lot of information of the geomagnetic field is ignored. Therefore, this paper proposes 3DGLS according to the above problems. It firstly solves the problem of inconsistent readings of the geomagnetic field given by sensor error, and then calculates the geomagnetic information into three characteristic information for constructing the geomagnetic fingerprint map. Finally, the positioning requirements are realized in indoor environments by using the idea of dynamic time warping and particle filtering. Experimental results show that 3DGLS can effectively reduce the errors and improve the matching efficiency of indoor positioning technology.

Through the in-depth study of the geomagnetic field, although the scheme proposed in this paper can effectively improve the error and matching efficiency of geomagnetic field in indoor positioning technology, due to

the need to collect data from different sensors during the construction of the geomagnetic fingerprint map, geomagnetic field information will change slightly as time goes by. Therefore, more efficient training and integration of the geomagnetic fingerprint map has become the focus of future research. It is also hoped that through in-depth research and excavation of geomagnetic field positioning technology, efficient and high-precision positioning requirements can be realized in the indoor environment. Furthermore, the application of 3DGLS in multi-workshop and multi-production line optimization can significantly enhance the efficiency and accuracy of tracking and managing resources across different workshops and production lines, ultimately leading to optimized production processes and improved operational efficiency.

References

[1] Weihao, L; Sheng, D; Jiajie, M. Spatio-temporal aware privacy-preserving scheme in LBS. Journal on Communications, 2018; Volume 39, pp.138-146.

[2] Pavel; Davidson; Robert; Piche. A survey of selected indoor positioning methods for smartphones. IEEE Communications Surveys & Tutorials , 2017; Volume 19, pp. 1347-1370.

[3] Simin, L; Chenglin, C; Yana, W. A Fusion Method for PDR and Magnetic Fingerprinting Based Indoor Localization on Smartphone. Chinese Journal of Sensors and Actuators, 2018, 31, 1; pp. 36-42.

[4] Vella, F; Infantino, I; Scardino, G. Person identification through entropy oriented mean shift clustering of human gaze patterns. Multimedia Tools and Applications, 2017, 76, 2; pp. 2289-2313.

[5] Kuang, J; Niu, X; Chen, X. Robust Pedestrian Dead Reckoning Based on MEMS-IMU for Smartphones. Sensors, 2018, 18, 5; pp.1391.

[6] Feng, G; Yang, Y; Guo, X. A smart fiber floor for indoor target localization. IEEE Pervasive Computing, 14, 2; pp. 52-59..

[7] Luo, J; Zhan,X. Characterization of Smart Phone Received Signal Strength Indication for WLAN Indoor Positioning Accuracy Improvement. Journal of Networks, 2014, 9, 3; pp.1061-1065.

[8] Huang, R; Xie, W; Alison, J N. VP-Nets: Efficient automatic localization of key brain structures in 3D fetal neurosonography. Medical Image Analysis, 2018, 47; pp.127-139.

[9] Kumari, P; Choi, J; Gonzá lez-Prelcic,N. IEEE 802.11ad-Based Radar: An Approach to Joint Vehicular Communication-Radar System. IEEE Transactions on Vehicular Technology, 2018, 67, 4; pp.3012-3027.

[10] Mossel,A. Robust 3D position estimation in wide and unconstrained indoor environments. Sensors, 2015, 15, 12; pp.31482-31524.

[11] Pham,D D ; Suh ,Y S . Pedestrian Navigation Using Foot-Mounted Inertial Sensor and LIDAR. Sensors, 2016, 16, 1; pp.120.

[12] Xie, H; Gu, T; Tao, X. A Reliability-Augmented Particle Filter for Magnetic Fingerprinting Based Indoor Localization on Smartphone. IEEE Transactions on Mobile Computing, 2016, 15, 9; pp.1877-1892.

[13] Yongle, L ; Yongwei, C; Ke ,D. High-precision step-length estimation method based on MEMS inertial sensor. Journal of Chinese Inertial Technology, 2018, 26, 2; pp.167-172.

[14] Turan, M; Shabbir, J; Araujo, H. A deep learning based fusion of RGB camera information and magnetic localization information for endoscopic capsule robots. International Journal of Intelligent Robotics & Applications, 2017, 1, 4; pp.442-450.

[15] Safaa, B; Alfonso, B; Díez, L. Conditional Random Field-Based Offline Map Matching for Indoor Environments. Sensors, 2016, 16, 8; pp. 1302-1305.

[16] Li, W; Wei, D; Lai, Q. Geomagnetism-Aided Indoor Wi-Fi Radio-Map Construction via Smartphone Crowdsourcing. Sensors, 2018, 18, 5; pp.1462.

[17] Ma,Y , Dou Z , Jiang Q. Basmag: An Optimized HMM-Based Localization System Using Backward Sequences Matching Algorithm Exploiting Geomagnetic Information. IEEE Sensors Journal, 2016, 16, 20; pp.7472-7482.

[18] Xiaofeng, L; Xueyuan, G; Wensheng, L. Error correction model of geomagnetic sensor based on least square method. Electronic Measurement Technology, 2018, 3; pp.46-49.

[19] Xirui, C, Jie, L, Minglang, C. A Research on Method of MEMS Gyroscope Drift Error Inhibition.

Chinese Journal of Electron Devices, 2018, 41, 2; pp. 356-360.
[20] Jie, L; Yanyu, Y; Kaiqiang, F. High-precision attitude measurement algorithm based on complementary filtering and Kalman filtering. Journal of Chinese Inertial Technology, 2018, 26, 1. pp.51-55.
[21] Zhuqing, H; Hua, Y. Multiple Sensors Based Algorithm for Pedestrian Heading Estimation. Computer Measurement & Control, 2018, 26, 5; pp. 191-193.
[22] Jun, J; He, L; Gu, Y; Jiang, W; Kushwaha, G; Vipin, A; Cheng, L; Liu, C; Zhu, T. Low-overhead WiFi fingerprinting. IEEE Transactions on Mobile Computing, 2018, 17, 3; pp. 590-603.
[25] Zhongsen, S; Qu, W; Haiyong, L. Online magnetic fingerprints based personal dead reckoning calibration algorithm. Electronic Measurement Technology, 2017, 40, 3. pp.147-152.
[26]Simin, L; Chenglin, C; Yana, W; Yunxiang, Q; Yanhu, H. A Fusion Method for PDR and Magnetic Fingerprinting Based Indoor Localization on Smartphone. Chinese Journal of Sensors and Actuators, 2018, 31, 1. pp. 36-42.

About the authors

Yu Tang is currently working as a researcher for the Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, Nanjing, China. Moreover, he is currently pursuing his doctoral degree in information networks at Nanjing University of Posts & Telecommunications, Nanjing, China. His primary research focus is on artificial intelligence security, with an emphasis on the security of network models in the audio domain.

Xiaolong Xu is currently a professor at the School of Computer Science, Nanjing University of Posts & Telecommunications, Nanjing, China. He is also working for the Jiangsu Key Laboratory of Big Data Security & Intelligent Processing. He received a B.E. in computer and its applications, and M.E. in computer software and theories and a Ph.D. degree in communications and information systems in 1999, 2002 and 2008, respectively. He is a senior member of the China Computer Federation. He teaches graduate courses and conducts research in areas of Cloud Computing, Big Data, Information Security and Novel Network Computing Technologies. As the leader of project teams, he has successfully completed a number of high-level research projects, including projects sponsored by the National Science Fund of China. He has published more than 100 journal and conference papers as the first or corresponding author and 5 books. He is authorized to have 52 patents by the State Intellectual Property Office of China as the first inventor. He was rated as an excellent young professor of Jiangsu Province in 2014, selected as the high-level creative talent of Jiangsu province in 2015, and won the title of outstanding expert in the area of computer science and technology.

Honghao Gao is currently with the School of Computer Engineering and Science, Shanghai University, China. He is also a Professor at the College of Future Industry, Gachon University, Korea. Prior to that, he was a Research Fellow with the Software Engineering Information Technology Institute at Central Michigan University, USA, and was an Adjunct Professor at Hangzhou Dianzi Uni-

versity, China. His research interests include Software Intelligence, Cloud/Edge Computing, and AI4Healthcare. He was the 2022 recipient of Highly Cited Chinese Researchers by Elsevier, and the 2021 recipient of IEEE Outstanding Paper Award for the IEEE Transactions on Industrial Informatics.

Edge Intelligence-based Collaborative Device Authentication and Localization for Industry 5.0

Li Xu[1], He Fang[1], Jia Zhu[2], Yulong Zou[2]

***Abstract*-While Industry 5.0 provides resource-efficient and user-preferred manufacturing solutions, the growing complexity of Industry Internet systems (IISs) and dramatically increased use of intelligent machines and devices within industry processes have brought many security vulnerabilities. To defense against the identity spoofing and location faking attacks, this paper proposes an edge intelligence-based collaborative device authentication and localization scheme. Firstly, multiple cooperative nodes are selected to help the access points to collaboratively authenticate their users by utilizing multiple device/location-related features based on the feedback mechanism. Then, a federated learning-based multi-dimensional information fusion and collaborative device authentication model is designed for reliable identification of different edge devices. Based on the feature estimation and authentication results, the proposed scheme can localize the identified attackers directly. The simulation results verify the feasibility and security enhancement of the proposed scheme.**

***Keywords*-IIS, device security, distributed learning, multi-dimensional information fusion, collaborative authentication, attacker localization**

1. L. Xu and H. Fang are with the College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350007, China (e-mails: xuli@fjnu.edu.cn, fanghe@fjnu.edu.cn). *Corresponding author: He Fang*.

2. J. Zhu and Y. Zou are with the School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mails: jiazhu@njupt.edu.cn, yulong.zou@njupt.edu.cn).

I. INTRODUCTION

Industry 5.0 integrates the swerving strengths of cyber-physical production systems and human intelligence to create synergetic factories [1][2]. As shown in Figure 1, the advancements in wireless communications and artificial intelligence (AI), have provided significant vitality to the Industrial Internet-of-Things (IIoT) [3][4]. Moreover, human-cyber-physical systems have been proposed for Industry 5.0, which could be applied in supply chain management, cloud manufacturing, manufacturing/production, smart education, intelligent healthcare, and so on [5]. The evolution of Industry 5.0 with human-cyber-physical system not only can help the enterprises realize automation and reduce production errors caused by human factors, but also can monitor the equipment running status, reduce equipment downtime, and improve production efficiency [5]. More importantly, the collaboration between humans and machines aims to increase production at a rapid pace by assigning repetitive and monotonous tasks to the robots/machines, where the tasks need critical thinking to the humans.

As shown in Figure 2, several enabling technological trends such as AI, Internet-of-Everything (IoE), data analytics, cobots, sixth-generation (6G)-and beyond, and blockchain are integrated with cognitive skills and innovation that can help industries increase production, deliver customized products more quickly, facilitate human capabilities more productive [6]. Due to the extremely tight interactions of the system and the physical environment, the security or privacy

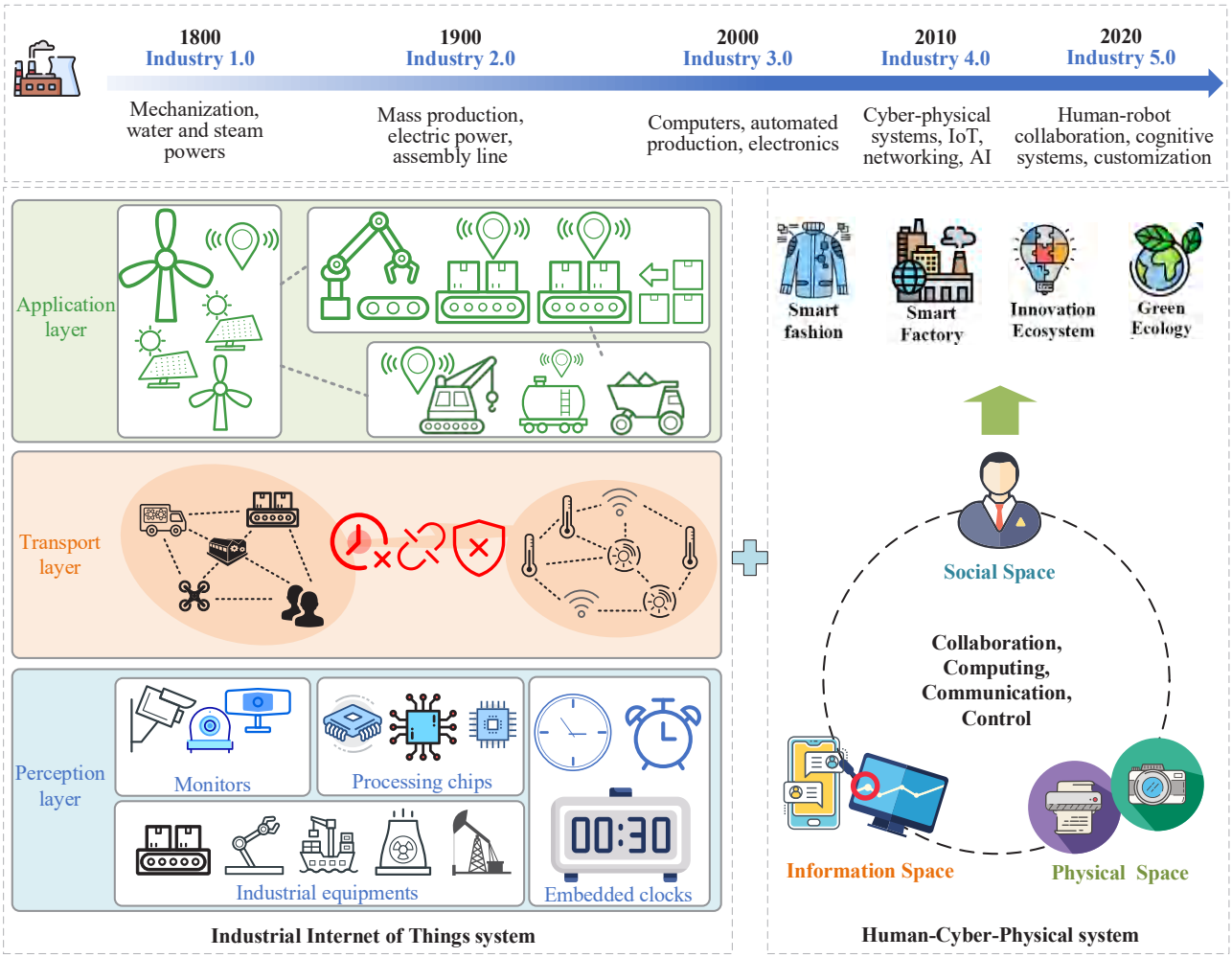


Figure 1 Framework of Industry 5.0 with human-cyber-physical systems.

vulnerabilities will cause reputation and financial loss, as well as the loss of life or serious environmental damages [7][8]. Security and privacy technologies are required for Industry 5.0 to protect devices, manufacturing/production, network, application, and data. The authentication of massive number of different stakeholders such as Internet-of-Things (IoT) nodes, machines, vehicles, fog nodes, communication nodes, and collaborative partner nodes is critical requirement to establish the mutual trust in the ecosystem [9][10]. To defend against the spoofing attacks and forgery attacks for guaranteeing the mutual trust in the ecosystem, this paper focuses both the device authentication and localization for Industry 5.0.

The conventional password/key/credential-based methods may suffer from the high computation overhead and latency in providing verifications for massive number of devices and are unavailable for the low-power devices [11]. In the era of quantum computing, they are also facing challenges because the complex operations to be carried out by classical computers may be readily cracked by quantum computers. Hence, it is extremely important to explore the inherent properties of the communication and devices, as well as to design new device authentication scheme through intelligently utilizing and fusing the heterogeneous multi-dimensional information.

Physical layer authentication provides an efficient method to identify different devices by exploiting the attributes of communication links and devices to protect

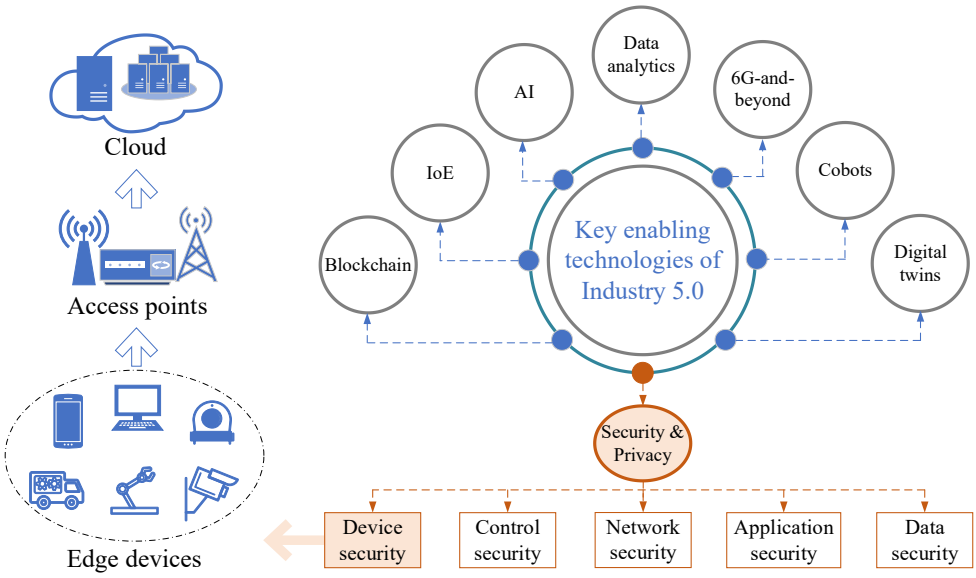


Figure 2 Key enabling technologies of Industry 5.0 with security management.

legitimate communications from the spoofing attacks, e.g., channel impulse response (CIR), carrier frequency offset (CFO), received signal strength indicator (RSSI), just to name a few [12]-[15]. However, the performance of physical layer authentication strongly relies on the time-invariant attributes, which may be difficult to estimate accurately in Industry 5.0 due to the increases of manufacturing accuracy and device number used.

To further increase the device authentication accuracy and to provide the localization services, this paper explores more attributes including the device position-related attributes for authentication, such as the time of arrival (TOA), time difference of arrival (TDOA), the trajectory of devices collected by lidar or camera [9]. In the ISSs, the abundance of environmental sensing information may be beneficially harnessed for facilitating the device authentication. Many intelligent machines and devices are equipped with many cameras and sensors, including radar, light detection and ranging (LiDAR) sensors, sonar, and global navigation satellite systems [16]. However, the performance of authentication relying on only one node suffers from the inaccurate estimation of wireless communications/device/position-related features.

The edge intelligence (EI) provides an efficient method to collect more authentication information at the network edge through allowing the machine learning (ML) models to be trained based on the collaboration among multiple edge servers and edge devices [17]-[21]. Through this process, the time and bandwidth required for training and authentication model can be also reduced. However, the designs of distributed learning algorithm and collaboration among edge nodes for accurate and efficient device authentication and localization are open issues to protect the IISs.

In this paper, we propose an edge intelligence-based collaborative device authentication and localization scheme. The contributions of this paper can be summarized as:

1) The proposed scheme utilizes multiple authentication features collected by multiple edge nodes for collaborative device authentication to improve the authentication accuracy. Multi-dimensional information from different sources is fused based on the federated learning for achieving consensus of collaborative device authentication among multiple edge nodes.

2) The proposed scheme provides the attacker localization services with the help of collaborative nodes

to further protect the entire industrial chain of IISs. By moving the security provision from the center to the edge of the network, the efficiency and flexibility of collaborative device authentication and attacker localization can be improved.

3) The results verify the security performance of the proposed scheme. Moreover, the attacker localization can be achieved based on the estimated features and authentication results. The results also demonstrate that the device authentication accuracy can be increased by cooperating more edge nodes.

The rest of this paper is organized as follows. In Section II, the system model and problem formulation of this paper are presented. In Section III, we propose the distributed learning-based collaborative device authentication and localization scheme. The simulations results are shown in Section IV. Finally, Section V concludes this paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

To protect the IIS, this paper focuses on the device authentication and localization method to provide the first line of defense to guarantee the legitimate accesses of all devices and the track services of attackers. This section presents the system model of collaborative device authentication and localization, and the problem formulation of this paper.

A. SYSTEM MODEL

Attack Model: As shown in Figure 3, the attacker tries to imitate the legitimate edge devices of the IIS to access the network, leading to privacy leakage, data injection, control system tamper, destruction of smart applications and intelligent transportation, just to name a few. The access point identifies all the edge devices with the help of multiple collaborative nodes, and locates the edge device once it is identified as an attacker.

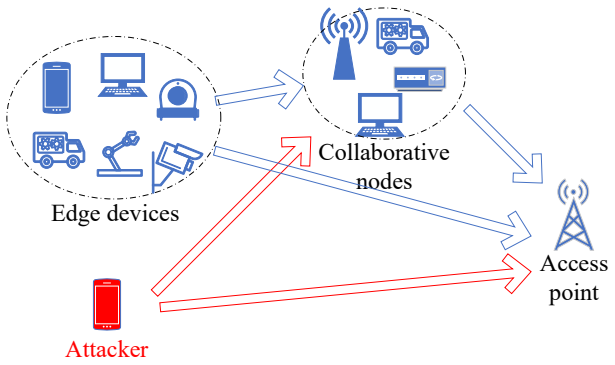


Figure 3 Collaborative device authentication and localization model.

Collaborative Authentication Model: As shown in Figure 3, multiple edge devices termed as collaborative nodes help the access point to authenticate its users by collecting their authentication information. Denoting the number of collaborative nodes as N and the number of authentication features as M, the collaborative device authentication is formulated as

$$\begin{cases} F\left(\boldsymbol{H}_{N\times M}\right) \le \theta, & \Phi_0 \\ F\left(\boldsymbol{H}_{N\times M}\right) > \theta, & \Phi_1 \end{cases} \tag{1}$$

$\boldsymbol{H}_{N\times M} = \left(h_{nm}\right)_{N\times M}, n = 1,2,\ldots,N, m = 1,2,\ldots,M,$ represents the authentication information matrix of the device to be authenticated collected by N collaborative nodes, and h_{nm} is the m-th feature estimated by the n-th collaborative node. θ is the collaborative authentication threshold. Φ_0 and Φ_1 denote the case that the authenticating edge device is legitimate and that is an attacker, respectively.

Authentication Features: As we discussed in the Introduction, the communication and device-related information can be utilized for security provision to achieve efficient device authentication in interconnected heterogeneous IIS. Typical wireless communication process information includes the radio frequency fingerprint (RFF), such as CFO, in-phase/quadrature (I/Q) imbalance, and the nonlinear characteristics of the

digital-to-analog converter and power amplifier. Moreover, the channel, location, and physical environment-related features can also be harnessed for collaborative authentication, including the CIR/channel frequency response (CFR), and the RSSI. In IIS systems, the location and moving direction of edge devices can also be utilized to assist the device authentication.

B. PROBLEM FORMULATION

This paper focuses on proposing an efficient collaborative authentication and localization scheme to identify and localize the attacker to protect the IIS. According to (1), the following steps are required:

1) selections of collaborative nodes and authentication features;

2) design of the collaborative device authentication model $F(\bullet)$;

3) design of collaborative authentication threshold θ;

4) localization of a node once it is identified as attacker.

To evaluate the proposed scheme, two criteria are considered, i.e., collaborative device authentication accuracy and localization accuracy. They are formulated, respectively, as

$$A_{\mathrm{CA}} = a_1 \Pr\left(F(\boldsymbol{H}_{N\times M}) \le \theta | \Phi_1\right) + a_2 \Pr\left(F(\boldsymbol{H}_{N\times M}) > \theta | \Phi_0\right) \tag{2}$$

and

$$A_{\mathrm{L}} = \left\| \boldsymbol{P}_{\mathrm{CE}} - \boldsymbol{P}_{\mathrm{Real}} \right\|. \tag{3}$$

a_1 and a_2 are two parameters satisfying $a_1 + a_2 = 1$. A_{L} represents the distance between the position of the edge device to be authenticated, i.e., $\boldsymbol{P}_{\mathrm{CE}}$, estimated by collaborative nodes and its real position $\boldsymbol{P}_{\mathrm{Real}}$. Hence, the designs of 1)-4) should maximize both the collaborative device authentication accuracy and localization accuracy.

III. THE PROPOSED SCHEME

In this section, we present the proposed edge intelligence-based collaborative device authentication and localization scheme. Firstly, the collaborative nodes and authentication features are selected based the feedback mechanism. Then, the collaborative authentication model is designed based on the federated learning relying on the collected authentication information from multiple collaborative nodes. Finally, the localization model of an identified attacker is designed.

A. FEEDBACK MECHANISM-BASED COLLABORATIVE NODE AND FEATURE SELECTION STRATEGY

The selection of a collaborative node depends on the distance between itself and the edge device to be authenticated. The reason is that the edge nodes located near to the device to be authenticated can seek more accurate information of its channel/device/location-related features. Hence, the N collaborative node located near to the authenticating edge device will be selected one by one for collaborative device authentication.

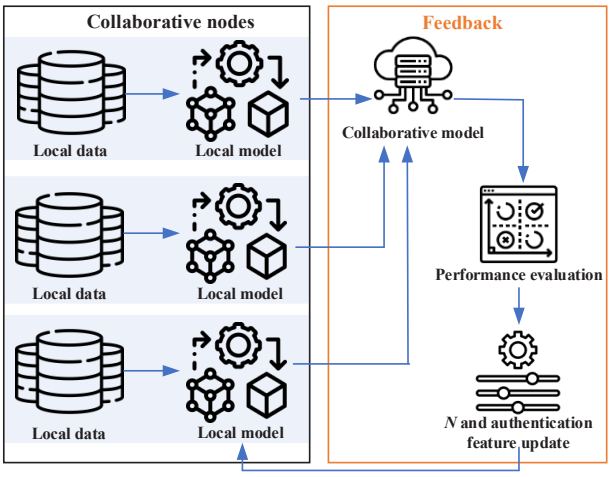


Figure 4 Collaborative node and authentication feature selection strategy.

Given the widely studied authentication features, i.e.,

RFF and channel/device/location-related features, the selection of authentication features depends on the collaborative nodes selected and the communication environment. To meet the requirement on authentication accuracy, we design a feedback mechanism-based collaborative node and feature selection strategy.

As shown in Fig. 4, given the collaborative authentication model and the authentication accuracy requirement, the authentication features are selected based on the feedback of performance evaluation of the collocative device authentication. To be more specific, the number of authentication features M and authentication features are selected iteratively. If $A_{\mathrm{CA}} < \delta$, the authentication features will be updated in the feature set Ω until the best features are selected, where δ is the minimum authentication accuracy required in the IIS. Then, the designed strategy evaluates the authentication accuracy based on the updated features. If $A_{\mathrm{CA}} < \delta$ still happens, the number of authentication features M is added. The above steps will be repeated until $A_{\mathrm{CA}} \geq \delta$ meets.

B. FEDERATED LEARNING-BASED COLLABORATIVE DEVICE AUTHENTICATION MODEL

To intelligently utilize multi-dimensional heterogeneous information gleaned from different nodes in the IIS, edge intelligence can be harnessed for information fusion and dynamic update. By moving the security provision from the center to the edge of the network, its efficiency and flexibility can be improved based on the edge AI algorithms. However, research on edge AI-based device authentication for IIS is still in its infancy. Moreover, the heterogeneous multi-dimensional information used in security provision is indeed beneficial, but also imposes new challenges on device authentication design.

To achieve efficient collaborative device authentication relying on multiple cooperators, a consensus is required, which contains the information sharing and fusion. This paper applies the federated learning algorithm for the collaborative authentication. The collaborative nodes firstly send requests to the access point to obtain the current model parameters. Then, they train their local models according to the local data and send the training results to the access point. Finally, the access point updates the global model parameters based on the received training results.

The objective function for federated learning-based collaborative device authentication is formulated as

$$f(\boldsymbol{x}_1,...,\boldsymbol{x}_N) = \frac{1}{N}\sum_{n=1}^{N} f_n(\boldsymbol{x}_n) \tag{4}$$

where $\boldsymbol{x}_n = \left(x_{n1}, x_{n2}, x_{n3}\right)^{\dagger}$ are the weights of model as viewed by node n, and $f_n(\boldsymbol{x}_n)$ is node n's local objective function, which describes how model weights $\boldsymbol{x}_n$ conforms to node n's local dataset, i.e., the estimations of selected authentication features $\boldsymbol{H}_{N\times M}$.

The node n's local objective function is designed as

$$f_n(\boldsymbol{x}_n) = \boldsymbol{X}_n\left(\boldsymbol{H}_n, \boldsymbol{P}_n\right) = \left(x_{n1}, x_{n2}, x_{n3}\right)^{\dagger} \tag{5}$$

where $\boldsymbol{H}_n = \left(h_{n1}, h_{n2}, \ldots, h_{nM}\right)^{\dagger}$ is the feature estimation collected by node n, and $(\bullet)^{\dagger}$ represents the transpose symbol. $\boldsymbol{X}_n(\bullet)$ is the node n's position estimation function of the device to be authenticated based on the feature estimations and the position of node n, i.e., $\boldsymbol{P}_n$.

Then, the collaborative device authentication model of (1) is designed as

$$\begin{cases} \left\| f(\boldsymbol{x}_1,...,\boldsymbol{x}_N) - \boldsymbol{P}_{\mathrm{Real}} \right\|_2 \leq \theta, & \Phi_0 \\ \left\| f(\boldsymbol{x}_1,...,\boldsymbol{x}_N) - \boldsymbol{P}_{\mathrm{Real}} \right\|_2 > \theta, & \Phi_1 \end{cases} \tag{6}$$

$\|\cdot\|_2$ is the 2-norm symbol. It can be seen from (6) that the device authentication result depends on the collaborative localization by the N cooperators based on the estimations of authentication features $\boldsymbol{H}_{N\times M}$. If the collaboratively estimated position of the authenticating edge device is not the same with its reported position, it will be identified as an attacker. Hence, both the location faking attacks and spoofing attacks can be identified.

Given the authentication accuracy requirement, i.e., $A_{\mathrm{CA}} < \delta$, the collaborative authentication threshold θ can be decided directly by solving

$$\begin{aligned} A_{\mathrm{CA}} &= a_1 \Pr\left(\|f(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N)-\boldsymbol{P}_{\mathrm{Real}}\|\le\theta|\Phi_1\right) \\ &\quad + a_2 \Pr\left(\|f(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N)-\boldsymbol{P}_{\mathrm{Real}}\|>\theta|\Phi_0\right) = \delta \end{aligned} \tag{7}$$

C. ATTACKER LOCALIZATION

According to the collaborative authentication model of (6), once a device to be authenticated is identified as an attacker, it is easy to obtain its position as

$$\boldsymbol{P}_{\mathrm{CE}} = f(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N) \tag{8}$$

It can be seen from both the collaborative device authentication model and the attacker localization process, the proposed scheme not only can protect the IIS from the spoofing attacks and location faking attacks, but also can identify the position of the attacker.

D. APPLICATION EXAMPLES

The proposed scheme can be applied in a broad range of Industry 5.0 applications, resulting in the improvement of existing businesses and creating new business opportunities.

Application example 1: In industry 5.0, customers can track purchased products and identify location fraud based on the proposed scheme and the identification resolution system.

Application example 2: In factory workshop environment, all the edge devices can be authenticated and localized by their access points based on the proposed scheme, and can be protected from the spoofing attackers.

Application example 3: In the Internet-of-Vehicle (IoV) system, the proposed scheme can provide quick authentication and seamless authentication handover between access points for the moving vehicles with the help from roadside units and edge computing servers.

IV. RESULTS

To quantify the performance of the proposed scheme, we simulate an IIS. The target user is an edge device and 5 edge nodes act as cooperators, e.g., access points, edge computation server, intelligent machines. The wireless communication and environmental sensing information collected for authentication in this simulation are the received signal strength (RSS) of the target user's radio frequency signal and the mobility trajectory (TRA) of the target user collected by laser radars, respectively. In this simulation, the RSS data collected by different edge devices are shared among them locally.

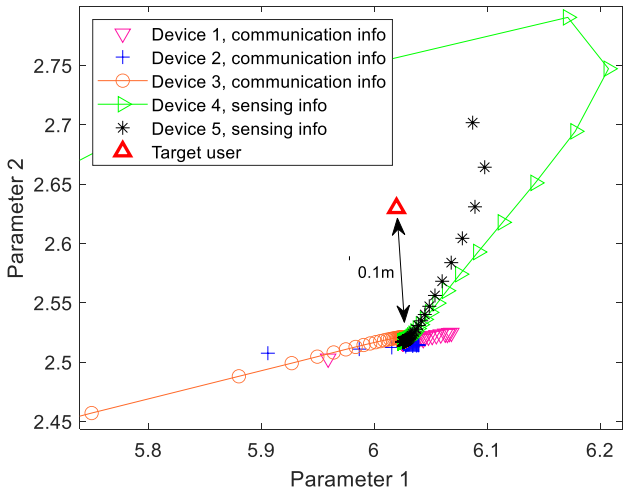


Figure 5 Learning results at cooperators for device authentication in the case that the device to be authenticated (i.e., target user) is a legitimate device.

Figure 5 characterizes the learning processes at the collaborative nodes, i.e., cooperators, relying on the wireless communication and environmental sensing information collected. One can be observed that the learning processes at all cooperators convergence to [6,2.5] m, which is the predicted location of the target user based on the collected RSS and TRA information. Given the real location of the user target at [6,2.6] m, the prediction error of the proposed scheme is 0.1 m. The authentication result is that the authenticating device is a legitimate user.

Furthermore, we simulate the case that an attacker tries to fake its localization. Figure 6 characterizes the learning processes at the cooperators. One can be observed that the learning processes at all cooperators convergence to [30.54,-6.35] m, which is the predicted location of the attacker based on the collected RSS and TRA information. Given the faked position of the attacker at [30.1,13.15] m, the distance between the estimated position and the faked position is 19.5088 m. Hence, it is easy to know that the device to be authenticated is an attacker, and its real position is [30.54,-6.35] m.

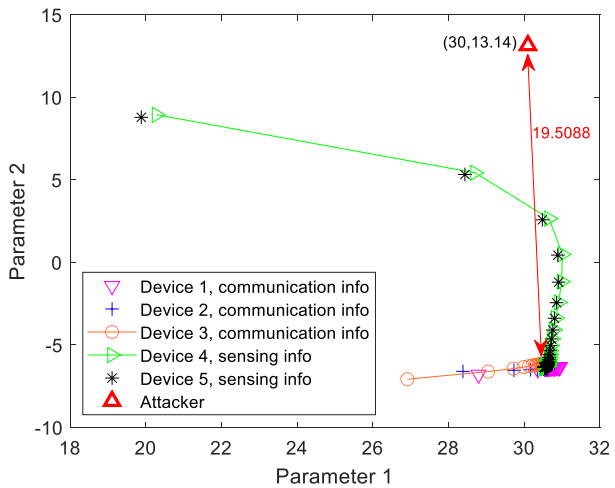


Figure 6 Learning results at cooperators for device authentication and localization in the case that the target user is an attacker.

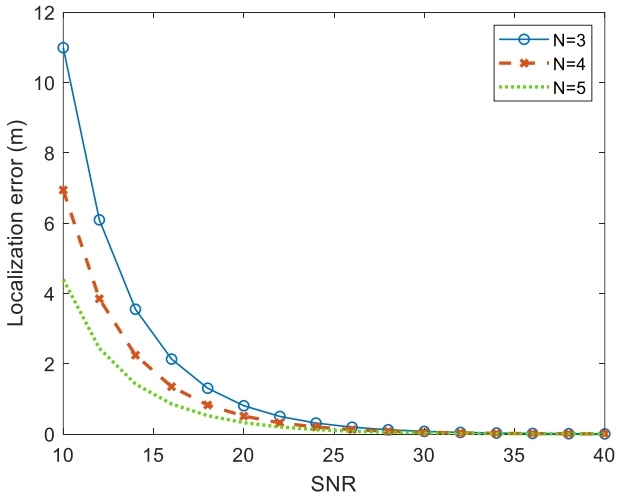


Figure 7 Localization error vs. Signal-to-Noise Ratio (SNR) in the cases that the proposed scheme utilizes 3, 4, and 5 cooperators.

Figure 7 characterizes the localization error of the proposed scheme in the cases that 3, 4, and 5 cooperators are used. It can be observed from the figure that with the increase of SNR, the localization error values of all cases decrease dramatically. Moreover, utilizing more collaborative nodes decreases the localization error, i.e., increases the performance of the proposed scheme.

VI. CONCLUSION AND FUTURE WORK

We introduced the concept of Industry 5.0 with the human-cyber-physical systems. With the assistance of edge AI algorithm, a collaborative device authentication and attacker localization scheme was proposed, which provides both identity verification and attacker localization services to protect the whole industry supply chain for Industry 5.0. The proposed scheme applies federated learning algorithm to fuse the collected multi-dimensional information from wireless communication and device/location-related features. Hence, the proposed scheme harnesses the inherent communication and device properties for enhancing security in IISs. Simulation results demonstrated the validity of the proposed scheme.

In the future work, we will focus on the improvement of the proposed scheme to reduce its time latency and communication overhead. The situation awareness will be also designed for the device authentication by identifying different application situations and time-varying communication environment of Industry 5.0. Moreover, we will focus more on the zero-trust security models and their integration with IISs. We will also consider the secure multi-party computation protocol to cope with the work of multi-public node signature and verification for different Industry 5.0 scenarios.

References

[1] XIANG W, YU K, HAN F L, FANG L, HE D H, HAN Q L, Advanced manufacturing in Industry 5.0: A survey of key enabling technologies and future trends [J]. IEEE Transactions on Industrial Informatics, 2024, 20(2): 1055-1068.

[2] LONGO F, PADOVANO A, UMBRELLO S, Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future [J]. Applied Sciences, 2020, 10(12): 4182.

[3] ZHOU H, SHE C, DENG Y, DOHLER M, NALLANATHAN A, Machine learning for massive Industrial Internet of Things [J]. IEEE Wireless Communications, 2021, 28(4): 81-87.

[4] RAHMAN M A, HOSSAIN M S, SHOWAIL A J, ALRAJEH N A, GHONEIM A, AI-enabled IIoT for live smart city event monitoring [J]. IEEE Internet Things Journal, 2023, 10(4): 2872-2880.

[5] WANG H, FU T, DU Y, GAO W, HUANG K et al., Scientific discovery in the age of artificial intelligence [J]. Nature, 2023, 620(7972): 47-60.

[6] KHARCHENKO V, ILLIASHENKO O, MOROZOVA O, SOKOLOV S, Combination of digital twin and artificial intelligence in manufacturing using Industrial IoT [C]//2020 IEEE 11th international conference on dependable systems, services and technologies (DESSERT), c2020: 196-201.

[7] BANAIE F, HASHEMZADEH M, AI-enabled threat detection and security analysis for Industrial IoT: Complementing IIoT services through AI: Feasibility and suitability [M]. Springer, 2021: 7-9.

[8] TANGE K, DONNO M, FAFOUTIS X, DRAGONI N. A systematic survey of Industrial Internet of Things security: Requirements and fog computing opportunities [J]. IEEE Communications Surveys & Tutorials, 2020, 22(4): 2489-2520.

[9] FANG H, ZHU Y, ZHANG Y, WANG X. Decentralized edge collaboration for seamless handover authentication in zero-trust IoV [J]. IEEE Transactions on Wireless Communications, doi: 10.1109/TWC.2024.3354064, 2024.

[10] BANSAL G, SIKDAR B. Beyond traditional message authentication codes: Future solutions for efficient authentication of message streams in IoT networks [J]. IEEE Internet of Things Magazine, 2022, 5(2): 102-106.

[11] FAROOQ S M, HUSSAIN S S, USTUN T S. A survey of authentication techniques in vehicular ad-hoc networks [J]. IEEE Intelligent Transportation Systems Magazine, 2020, 13(2): 39-52.

[12] ZOU Y, ZHU J, WANG X, HANZO L. A survey on wireless security: Technical challenges, recent advances, and future trends [J]. Proceedings of IEEE, 2016, 104(9): 1727-1765.

[13] FANG H, WANG X, XU L. Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach [J]. IEEE Transactions on Wireless Communications, 2020, 19(8): 5420-5432.

[14] XIAO L, LU X, XU T, ZHUANG W, DAI H. Reinforcement learning-based physical-layer authentication for controller area networks [J]. IEEE Transactions on Information Forensics Security, 2021, 16: 2535-2547.

[15] SHEN G, ZHANG J, MARSHALL A, VALKAMA M, CAVALLARO J R. Toward length-versatile and noise-robust radio frequency fingerprint identification [J]. IEEE Transactions on Information Forensics Security, 2023, 18: 2355-2367.

[16] ZHANG J, LETAIEF K B. Mobile edge intelligence and computing for the Internet of Vehicles [J]. Proceedings of IEEE, 2020, 108(2): 246-261.

[17] CANESE L, CARDARILLI G C, NUNZIO L D, FAZZOLARI R, GIARDINO D. Multi-agent reinforcement learning: A review of challenges and applications [J]. Applied Sciences, 2021, 11(11).

[18] CHANG T H. A proximal dual consensus ADMM method for multi-agent constrained optimization [J]. IEEE Transactions on Signal Processing, 2016, 64(14): 3719-3734.

[19] NGUYEN D C, DING M, PATHIRANA P N, SENEVIRATNE A, LI J. Federated learning for Industrial Internet of Things in future industries [J]. IEEE Wireless Communications, 2021, 28(6): 192-199.

[20] MAKKAR A, KIM T W, SINGH A K, KANG J, PARK J H. Secure IIoT environment: federated learning empowered approach for securing IIoT from data breach [J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6406-6414.

[21] LIU Y, HAO X, REN W, XIONG R, ZHU T, RAYMOND CHOO K K, MIN G. A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust Internet-of-Things [J]. IEEE Transactions on Computers, 2023, 72(2): 501-512.

About the authors

Li Xu received the Ph.D. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2004. He is currently a Professor with the College of Computer and Cyber Security, Fujian Normal University, Fuzhou. He is also the Dean of the College of Computer and Cyber Security and the Director of the Fujian Key Laboratory of Network Security and Cryptography. His research interests include network and information security, wireless networks and communication, big data, and intelligent information in complex networks. He has authored or coauthored more than 180 papers in international journals and conferences, including IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON COMPUTER, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.

He Fang received her Ph.D. degree in Electrical and Computer Engineering from Western University, Canada, in 2020, and Ph.D. degree in Applied Mathematics from Fujian Normal University, China, in 2018. She is currently a Full Professor with Fujian Normal University, China. Her research interests include intelligent security provision, trust management, machine learning, distributed optimization and collaboration techniques. She serves as an Associate Editor of China Communications, and a Guest Editor for several journals. She was involved in many IEEE conferences including IEEE GLOBECOM, VTC, and ICCC, in different roles such as Lead Track Chair, Session Chair, and TPC member. She also served as the Vice-Chair of Communication/Broadcasting Chapter, IEEE London Section, Canada, from Sep. 2019 to Aug. 2021. She has received several awards, including the Best Paper Award from IEEE GLOBECOM 2023.

Jia Zhu is a Professor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. She received the B.Eng. degree in Computer Science and Technology from the Hohai University, Nanjing, China, in July 2005, and the Ph.D. degree in Signal and Information Processing from the Nanjing University of Posts and Telecommunications, Nanjing, China, in April 2010. From June 2010 to June 2012, she was a Postdoctoral Research Fellow at the Stevens Institute of Technology, New Jersey, the United States. Since November 2012, she has been a full-time faculty member with the Telecommunication and Information School of NUPT, Nanjing, China. Her general research interests include the cognitive radio, physical-layer security and communications theory.

Yulong Zou is a Full Professor and Doctoral Supervisor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. He received the B.Eng. degree in information engineering from NUPT, Nanjing, China, in July 2006, the first Ph.D. degree in electrical engineering from the Stevens Institute of Technology, New Jersey, USA, in May 2012, and the second Ph.D. degree in signal and information processing from NUPT, Nanjing, China, in July 2012.

Dr. Zou was awarded the 9th IEEE Communications Society Asia-Pacific Best Young Researcher in 2014. He has served as an editor for the IEEE Communications Surveys & Tutorials, IEEE Communications Letters, EURASIP Journal on Advances in Signal Processing, IET Communications, and China Communications. In addition, he has acted as TPC members for various IEEE sponsored conferences, e.g., IEEE ICC/GLOBECOM/WCNC/VTC/ICCC, etc.

Application of Embedded Soft-PLC in Residential Photovoltaic System

Zhiwu Tang
College of Electrical Engineering,Zhejiang University
Hangzhou, China
22210097@zju.edu.cn

Xiaopeng Song
Zhejiang Institute of Communications Co. Ltd.
Hangzhou, China
songxiaopeng208@163.com

Zhen Fan
College of Electrical Engineering,Zhejiang University
Hangzhou, China
fanzhen@zju.edu.cn

Jie Yu
Zhejiang Institute of Communications Co. Ltd.
Hangzhou, China
1148990819@qq.com

***Abstract*—Photovoltaic energy storage system(PVESS) is a very promising form of energy system, which can integrate multiple forms of energy and is an important means to accommodate renewable energy. Through the reasonable control strategy, the utilization rate of photovoltaic power generation can be improved while reducing the power fluctuation in the process of system operation, and the operation quality of the actual power supply system can be improved. However, most of the existing control schemes complete the system control through specially developed controllers, and the control program runs on the controller in the form of firmware, which is difficult to migrate between different controllers. In this paper, based on IEC61499 standard, a soft-PLC system is proposed to realize the control of photovoltaic energy storage system. The simulation results show that the control program can be transferred on different hardware, and effectively improve the development efficiency of distributed control system.**

Keywords*—— *IEC61499,Photovoltaic Energy Storage System,Distributed Control

I. Introduction

With the implementation of China's ”peak carbon emissions and carbon neutrality” goals [1], the development of distributed generation, primarily driven by renewable energy sources such as photovoltaics and wind power, has rapidly advanced. As the installed capacity of renewable energy increases, optimizing the energy flow between generation, storage, and consumption in comprehensive energy systems becomes crucial to enhance energy absorption rates and economic benefits, ultimately realizing the ”dual-carbon” objectives.

Considering a typical application of a comprehensive energy system, namely, residential photovoltaic energy storage system which involves photovoltaic generation, battery storage, and user load consumption. Photovoltaic generation primarily serves the load demand, with surplus energy either stored in battery storage units or fed into the grid. This approach aims to reduce user consumption, minimize the economic costs associated with grid electricity purchases, and achieve energy conservation and emission reduction goals. Two main challenges arise from this process: enhancing the on-site absorption rate of photovoltaic generation and mitigating the impact of peak loads during photovoltaic grid integration.Battery storage units play a crucial role in improving the on-site absorption of photovoltaic energy by storing excess energy. Simultaneously, limiting the power fed into the grid during peak photovoltaic generation periods helps avoid grid peak loads. Against this backdrop, effective control strategies are needed to coordinate the energy flow among photovoltaics, batteries, and the grid.

Many scholars have studied the energy scheduling control strategy of residential photovoltaic energy storage system. For example, literature [2] proposed an operation strategy of residential photovoltaic energy storage system based on independent prediction, which can realize the economic operation of the optical storage system and ensure the stable operation of the power grid. Literature [3] studied the continuous prediction management strategy based on photovoltaic and load, and developed a proportional-integral controller to reduce the uncertainty of prediction, so as to maximize the self-sufficiency of the optical storage system. Literature [4] proposed a simple control strategy for residential photovoltaic energy storage system, which could maximize photovoltaic consumption and reduce power limiting loss. Literature [5] designed an optimal control strategy for residential optical storage system by considering the information of time-of-use electricity price and taking the user's economic benefit and battery loss cost as the objective function. As for the practical application of photovoltaic energy storage system, literature [6] designed a household light-storage integrated control device, which connected the household photovoltaic array, power converter and hybrid energy storage battery into the control device, so as to realize the coordinated and orderly operation of photovoltaic energy storage. The embedded user-side energy storage optimization controller designed in literature [5] can process and store the collected data in real time, and realize the power scheduling of the optical storage system by connecting

This research is supported by the Key Research and Development Program of Zhejiang Province No. 2023C01246

with the optical storage integrated machine. Literature [7] designed a user-side optical load storage coordination controller based on MPC, which was used to collect real-time operation data of each part of the user side and control the energy storage system in real time.

The above system applications all adopt a centralized control mode, through the specially developed centralized controller to complete the system control, the control program runs in the form of firmware on the controller, without considering the program configurability, migration scheduling and other issues. The international electrotechnical commission has proposed an Industrial Process Measurement and Control System (IPMCS) standard IEC61499, which pays more attention to the distributed deployment capability of applications [8]. It provides a solution for developing distributed and reconfigurable control system applications. IEC 61499 standard has the advantages of functional block-based component design, event-driven execution and distributed model architecture, which can meet the requirements of building modular, reusability and adaptive distributed automation systems proposed by Industry 4.0 [9] . The goal of this paper is to use a software platform conforming to IEC61499 standard to build an embedded soft PLC system to achieve energy optimization scheduling in residential photovoltaic energy storage system.

The rest of this paper is organized as follows. Section II introduces the model of PVESS. The mathematical formulation of the proposed energy management strategy is given in Section III. Several simulation cases are presented in Section IV to illustrate the effectiveness of the proposed strategy. Finally, the conclusion is drawn in the Section V.

II. System Model

A. Software Platform Complianted to IEC 61499

The IEC 61499 standard defines a set of distributed, modular, reusable distributed control system general model and design ideas independent of the specific implementation, and formulates rules for the use of reusable software module - Function Block (FB) [8]. It defines the use of an integrated development environment (IDE) to build applications and the use of a runtime environment to run applications. Each functional block (FB) represents an independent software unit, with its own variables and algorithms, connected to other FBS via its external interfaces (inputs and outputs) to form a complete application. Each FB can run on different hardware devices, so that an application can be distributed across multiple devices.

According to the IEC61499 standard, the Eclipse company released two open source software, 4diac IDE and Forte, in the early 2000s [9].The 4diac FORTE is a small portable implementation of an IEC 61499 runtime environment targeting small embedded control devices (16/32 Bit), implemented in C++. It supports online-reconfiguration of its applications and the real-time capable execution of all function block types provided by the IEC 61499 standard. The 4diac IDE is an extensible, IEC 61499 compliant engineering environment for distributed control applications, where applications can be downloaded to distributed field devices according the means defined by the IEC 61499 standard. Fig. 1 shows the distributed control system model based on IEC61499.

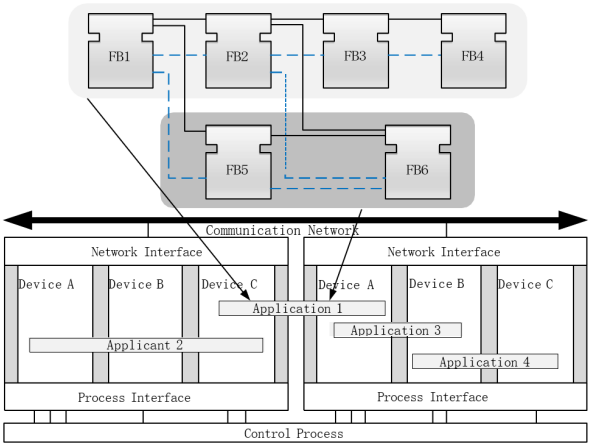


Fig. 1. Distributed control system model Based on IEC61499

B. Mathematical description of performance indicators

In this part, the control strategy and performance indicators of the photovoltaic energy storage system are proposed. The energy flow of PVESS is shown in the Fig. 2, we can obtain some indicators for the evaluation of the control strategy of photovoltaic energy storage system.

The variable e self-consumption rate is used to indicate the proportion of photovoltaic power generation used for load absorption and battery charging:

$$e = \frac{E_d u + E_b c}{E_p v} \tag{1}$$

The variable self-sufficient rate a is used to represent the proportion of photovoltaic power generation and battery discharge in the total load electricity consumption. The higher the self-sufficiency rates, the more sufficient the local absorption of photovoltaic will be:

$$a = \frac{E_{du} + E_{bd}}{E_{load}} \tag{2}$$

The abandonment rate c represents the percentage of the PV power lost to the total power due to exceeding the power feedback limitation:

$$c = \frac{E_{ct}}{E_{pv}} \tag{3}$$

III. Energy control Strategy for PVESS

The goal is to plan the battery charging and discharging behavior in advance, give full play to the battery energy storage system's ability to absorb photovoltaic power generation through the photovoltaic forecasting and load forecasting. The battery charging and discharging process is concentrated as far as possible in the time period of the highest photovoltaic output, to avoid a large amount of discarded light because

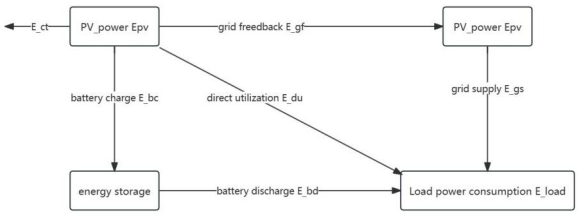


Fig. 2. Structure of the PVESS with energy flow directions.

of the upper limitation of battery absorption and constraints to feed into the grid. The energy saved in this way can be used for electricity consumption or fed into the grid to obtain greater economic benefits. At the same time, the peak period of photovoltaic power generation feedback is avoided to ensure the stable operation of the grid.

A. Mathematical description of control strategy

Building on previous research, the energy scheduling control strategy of residential photovoltaic energy storage system is studied in order to promote the local consumption of photovoltaic power generation and avoid the photovoltaic power generation from being fed into the grid during peak hours.

Considering that the power value obtained by real-time measurement is discrete power P and Δt is one step, the relationship between energy and discrete power can be written as

$$E = P\Delta t = \int_{t}^{t+\Delta t} Pdt \tag{4}$$

The reality measured power of photovoltaic power generation is denoted P_{pv}, the load power consumed by the user is denoted P_{load}, and the difference between the two is denoted as the remaining power P_{rest}:

$$P_{rest} = P_{pv} - P_{load} \tag{5}$$

As to the distribution of remaining power, if P_{rest} >0, then the photovoltaic power generation can cover the electricity consumption of the household user, and the remaining energy P_{bc} is first used for charging the battery. If there is any remaining energy, the remaining energy P_{gf} is fed into the grid within the maximum feed limit, and the part that exceeds the maximum feed limit is regarded as the discarded light part and recorded as P_{ct}:

$$P_{rest} = P_{bc} + P_{gf} + P_{ct}(P_{rest} \geq 0) \tag{6}$$

When P_{rest} <0, it means that the electricity consumption of the household user exceeds the photovoltaic power generation, and needs to use battery discharge P_{bd} to provide electricity, if it still can not meet the electricity consumption, power P_{gs} provided by the grid is needed:

$$P_{gs} = P_{bd} + P_{res}t(P_{rest}<0) \tag{7}$$

Lithium-ion battery mathematical model is used to describe the battery charging and discharging process in this paper. And the charge and discharge power of the battery Wh should be limited to the nominal discharge power range due to the constraints of battery inverters. Furthermore, battery energy storage will produce a certain amount of energy loss, one is the inverter loss 1- $\eta_{b,we}$, it's assumed 6%;the second is the battery conversion loss, i.e. the energy loss caused by a charge and discharge process. η_{Wh} describes the ratio of charge to discharge, it's assumed 95%:

$$\eta_{Wh} = \frac{E_{bd}}{E_{bc}} \tag{8}$$

Bidirectional inverter losses are considered during both charge and discharge, and battery conversion characterizes a complete cycle so only once is considered:

$$\eta_{bd} = \eta_{b,wr} \tag{9}$$

$$\eta_{bc} = \eta_{b,wr}\eta_{Wh} \tag{10}$$

So the energy balance formula of the simplified battery model is(regardless of temperature and pressure related characteristics):

$$\eta_{bc}P_{bc} + \frac{P_{bd}}{\eta_{bd}} + \frac{E_b(t) - E_b(t+1)}{\Delta t} = 0 \tag{11}$$

E_b is energy stored in the battery. So the battery capacity of the current time step can be calculated from the battery capacity of the previous time step. In order to ensure battery life, the charge and discharge state of the battery is usually limited during 20% to 80%. The dimensionless charge state SOC is used to represent the charging and discharging state of the battery

$$SOC(t) = \frac{E_b(t)}{C_{bn}} \tag{12}$$

where $E_b(t)$ is the energy stored in battery, C_{bn} is the normal capacity of battery. Charge process is expressed as:

$$E_b(t) = min(SOC_{max}C_{bn}, E_b(t) + P_{bc}\eta_{Wh}\eta_{b,wr}\Delta t) \tag{13}$$

Discharge process is expressed as:

$$E_b(t) = max(SOC_{max}C_{bn}, E_b(t) - P_{bc}\frac{\Delta t}{\eta_{b,wr}}) \tag{14}$$

B. Photovoltaic/Load Forecasting Based on Historical Data

Inspired by the calculation of empty irradiance, clearness index K_{Tf} is used to predict the power generation at a certain point in the future.Assuming the start time of calculation is t_0, the power at time W should be predicted using time interval t_0 to $t - 1min$. Variable K_{Tf} means the ratio of total photovoltaic power generation to total maximum power photovoltaic power generation during the time interval.

$$K_{Tf}(t) = \frac{\int_{t_0}^{t-1min} P_{pv}dt|P_{pv}>0}{\int_{t_0}^{t-1min} P_{pv,max}dt|P_{pv,max}>0} \tag{15}$$

where P_{pv} represents the photovoltaic power and $P_{pv,max}$ represents the maximum photovoltaic power in the past period of time.

In this paper, time interval is set to 15 minutes and predictions are made every 15 minutes. Then, $\overline{K_{Tf,15}}$ and $\overline{P_{pv,max15}(t)}$ the average value of result are used as new scaling factor.

$$\overline{K_{Tf,15}} = \frac{\int_{t-15min}^{t} K_{Tf}(t)dt}{15min} \tag{16}$$

$$\overline{P_{pv,max15}(t)} = \frac{\int_{t-15min}^{t} P_{pv,max}(t)dt}{15min} \tag{17}$$

Finally, the forecast photovoltaic power is obtained as:

$$P_{pv,f}(t) = \overline{K_{Tf,15}}\overline{P_{pv,max15}(t)} \tag{18}$$

Considering the regularity and continuity of the load, the forecast load is obtained using the weighted load i.e.$P_{load,fp}(t)$ used at the same time the previous day and the average load power of the previous 15 minutes i.e.$\overline{P_{load,15}(t)}$. The exponential weighting function $w(t)$ is used to weight $P_{load,fp}(t)$ and $\overline{P_{load,15}(t)}$:

$$\overline{P_{load,15}(t)} = \frac{\int_{t-15min}^{t} P_{load}(t)dt}{15min} \tag{19}$$

$$w_{lfp}(t) = exp(0.1)exp(-0.1\frac{t-15}{1min}) \tag{20}$$

$$w_{lc}(t) = 1 - w_{lfp}(t) \tag{21}$$

As a result, the load forecast is obtained:

$$P_{load,f}(t) = w_{lfp}(t)P_{load,fp}(t) + w_{lc}\overline{P_{load,15}(t)} \tag{22}$$

C. Deep Learning-Based Photovoltaic/Load Forecasting

A precise prediction of photovoltaic and load is desired to promote economic security in the integrated energy systems. When facing to high randomness, fluctuation and uncertainty load data,preciser result will be obtain through deep learning method due to its complex network structure and stronger learning ability compared to traditional method based on history data. In this part, the Darts toolbox is adopted for deep learning prediction to simplify the application process. Temporal fusion Transformers(TFT) model is used for photovoltaic generation forecast and Long Short-term Memory(LSTM) is employed to predict the load consumption. The battery charging behavior planning is based on the forecast result to plan.

Assuming that $p_{gf,max}$ is the maximum PV feedback limit and the virtual feed amount is set in increments of p_{gfvir}, the part of the remaining power P_{rest} fed into the grid is determined, and the remaining part $P_{rest,f+}$is used for battery charging as much as in one day. No need to consider the battery discharge process, because the discharge is only carried out when PV power generation cannot meet the load consumption. Considering the predicted power $P_{rest,f}$ >0, time interval[t, t+15h]:

$$P_{rest,f} = P_{pv,f} - P_{load,f} \tag{23}$$

$$P_{rest,f+} = max(0, P_{rest,f}) \tag{24}$$

$$P_{charge,f} = max(0, P_{rest,f+} - p_{gfvir}P_{vir}) \tag{25}$$

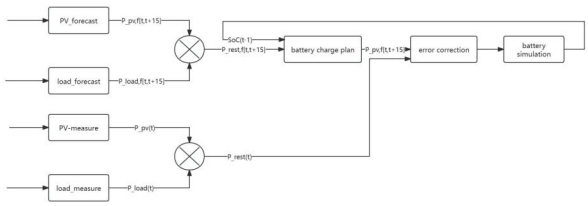


Fig. 3. Structure of the control strategy based on forecast.

The current actual charge of the battery can be obtained by charging power $P_{charge,f}$. The more energy feed back to the grid, the less battery stores. When the calculated charge of the battery is exactly the amount of battery used, the virtual feedback energy can be seen as the reality $p_{gf,f}$. So the battery charge power can be obtained as:

$$P_{b,f} = \begin{cases} P_{rest,f}P_{gf,g} = 0 or P_{rest,f} \leq 0 \\ max(0, P_{rest,f+} - p_{gfvir}P_{vir}) \quad P_{gf,f} > 0 \end{cases} \tag{26}$$

In order to offset the impact caused by the forecast error, an error control unit is needed to correct the battery charge and discharge power.

$$P_{rest}(t) = P_{pv}(t) - P_{load}(t) \tag{27}$$

$P_{rest}(t)P_{pv}(t)$ and $P_{load}(t)$ are the actual measured value. When $P_{rest}(t)$ >0, the charge power should be correct if one of the following conditions is satisfied: a.$P_{b,f}$ is not 0 at the moment b.$P_{rest}(t)$ overpass the feedback limitation at the moment c.$P_{rest,f}(t)$ overpass the predicted feedback limitation at the moment

$$P_{bc} = max(0, P_{b,f} + (P_{pv} - P_{load}) - (P_{pv,f} - P_{load,f})) \tag{28}$$

When $P_{rest}(t)$ <0, the battery need to discharge according to the actual consumption and the discharge power should be limited under the normal power:

$$P_{bc} = max(-P_{bwr}, P_{pv}(t) - P_{load}(t)) \tag{29}$$

The whole flow chart of the control strategy for the PVESSM is shown in fig. 3

IV. Simulation and Analysis

In this part, the proposed control strategy is implemented in embedded controllers which is based on the soft PLC platform conforming to IEC61499 standard.

A. Encapsulate algorithmic function blocks

The standard function block libraries based on IEC61499 is not able to implement the complex algorithm described above. Several FBs are created as shown below to the build photovoltaic energy storage control system application. Then, the control application of the PVESS can be constructed.

The simple forecast FB is a local prediction that can be completed on the embedded controller, and the historical data storage and query are involved in the calculation process. So,

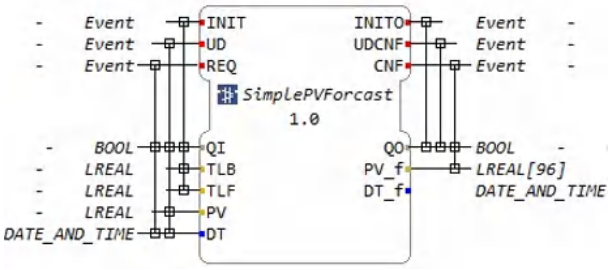


Fig. 4. Structure of the control strategy based on forecast.

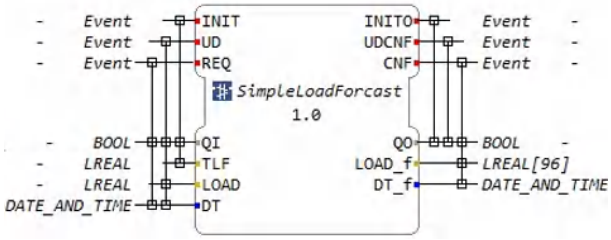


Fig. 5. Structure of the control strategy based on forecast.

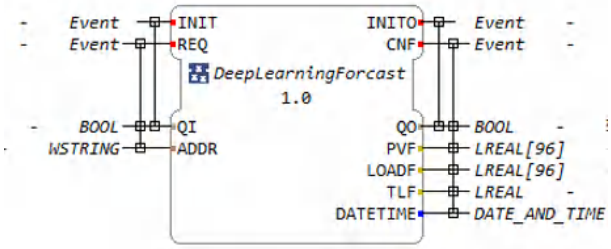


Fig. 6. Structure of the control strategy based on forecast.

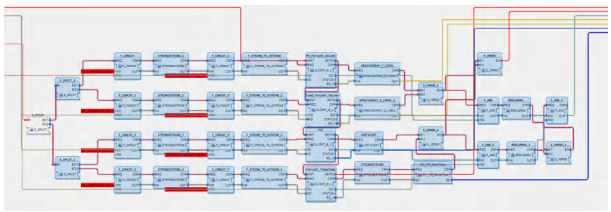


Fig. 7. Structure of the control strategy based on forecast.

it is encapsulated as service function block as shown in fig. 4 and fig. 5. The deep learning FB is normally run in the server because the huge amount of computation will consume too much resources, which embedded controls can not afford.

In a simulation, the embedded controller A is connected to the photovoltaic inverter device through a digital input port to read the generated power, and is connected to the battery management system through a digital output port to specify the battery charge and discharge power. The other embedded controller B is connected to the user's electricity meter through

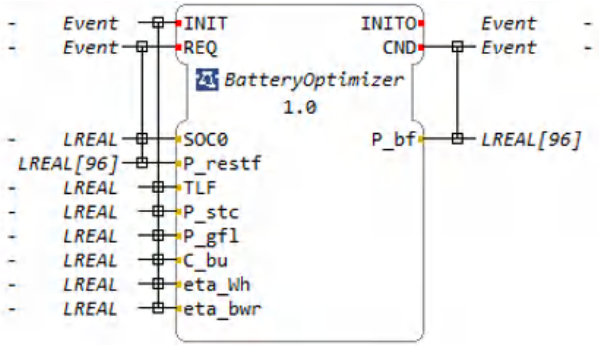


Fig. 8. Structure of the control strategy based on forecast.

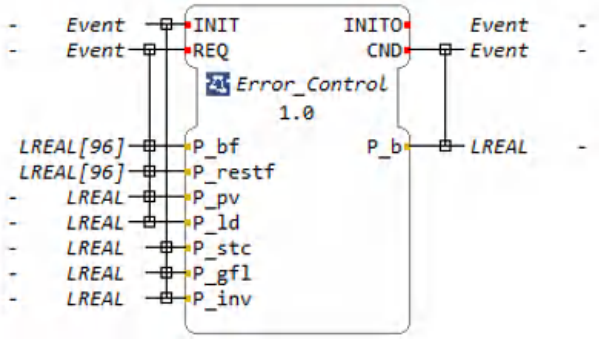


Fig. 9. Structure of the control strategy based on forecast.

the RS485 bus to obtain the electricity consumption data. According to the photovoltaic and load power and the battery charging and discharging state, Raspberry PI sends control commands to the inverter of the interconnection point to control the feeding and power supply behavior of the residential power system.

In this paper, open source data sets are used to simulate signal inputs in real scenarios, where the PV data is from the Australian DKASC data set and the load data is from the EULPs project in the United States [10]. As shown in fig. 10, ESP32-controllers and Raspberry Pi A are in the same local network, running IEC61499 runtime. Raspberry Pi B is used to generate PV data and connected to the digital input of ESP32-controller-A, and ESP32-controller-B is connected to a PC through a USB to RS485 converter to obtain electricity data. Meanwhile, an OPCUA server is built on the PC using open62541 protocol stack, and the prediction results of deep learning are published on the OPCUA server in the form of information model. The embedded controller Raspberry Pi A can directly access the OPCUA server through Ethernet communication, and obtain the prediction data results in real time in the execution control strategy application.

Building the complete test application and map the corresponding functions to the corresponding devices, and get the complete view in fig. 11. For ESP32-controller-A (yellow part), it mainly runs photovoltaic data acquisition and control strategy

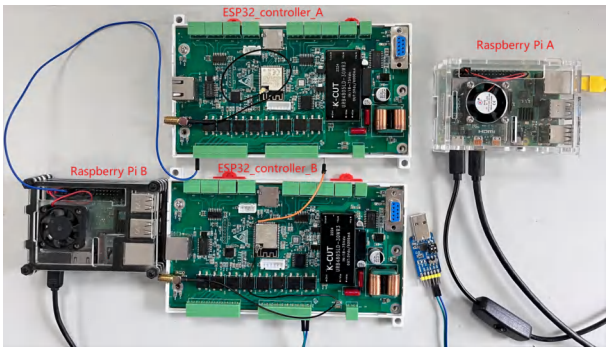


Fig. 10. Structure of the control strategy based on forecast.

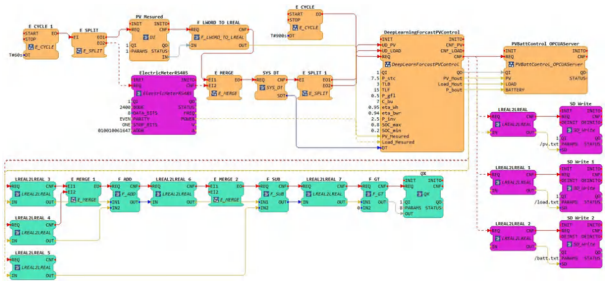


Fig. 11. Structure of the control strategy based on forecast.

algorithm based on deep learning, and publishes the algorithm output in the form of OPCUA server. For ESP32-controller-B (purple part), it can be divided into two resources, which can run different tasks on different resources at the same time, such as mapping the function of watt-hour meter data acquisition on EPS32-controller-B resources, writing the output results into SD card part of the function mapping on ESP32-B-SD resources, distributed on different resources mainly to provide an isolated environment for the two application processes to be executed in parallel. For raspberry Pi A (green part), it is mainly based on the sum of the measured photovoltaic value and the battery charge and discharge power value, minus the load power value, if the result is greater than 0, it can be fed to the power grid, if the result is less than 0, the power supply is needed, and finally the result is output through the general GPIO port.

B. Simulation results for the PVESS

According to the above application deployment process, the PV energy storage system applications under the three different control strategies proposed in the previous section are deployed on the experimental equipment for testing.In the test, the data acquisition was carried out at the frequency of 10ms, and the control calculation was carried out at the frequency of 150ms to obtain the application data results of 5 days. The results of PV and load forecast based on deep learning and the data stored on SD card of ESP-32-A were processed by MATLAB, and the PV and load forecast curves based on deep learning were

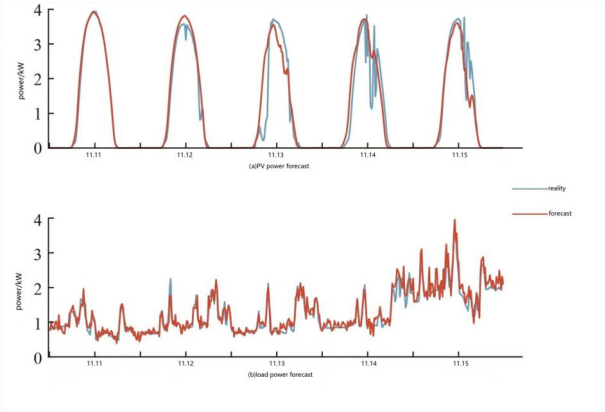


Fig. 12. PV and load forecast curves based on deep learning

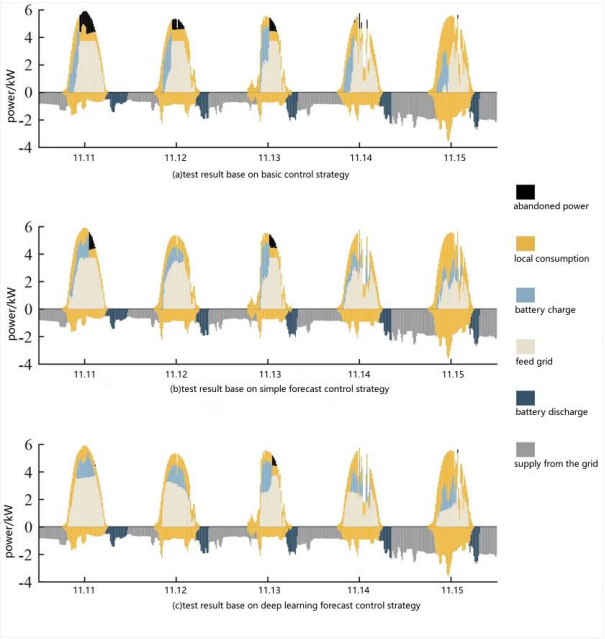


Fig. 13. Test results of different control strategies

obtained as shown in Figure 2. The evaluation indicators of PV and load forecast based on deep learning and simple forecast were shown in Figure 2. The power flow under three control strategies was shown in Figure 3. The system test performance indicators are shown in Table IV.

Comparing the power flow under three different control strategies, it can be intuitively seen that compared with the basic control strategy without prediction, the control strategy based on prediction can reduce the amount of photovoltaic light abandoned. The reason is that the control strategy based on prediction can plan the charging time of the battery in advance, so that it can be charged at the peak of the photovoltaic power at noon as much as possible, which greatly reduces the amount of photovoltaic light abandoned. From the performance index

TABLE I
COMPARISON OF OPERATION COSTS IN THREE CASES

Cases	e	a	c
basic control strategy	47.06%	56.02%	4.33%
simple forecast	47.05%	56.00%	1.36%
deep learning forecast	47.03%	55.59%	0.37%

results, the amount of abandoned light is reduced from 4.33% of the basic strategy to below 1.36%. Compared with the simple prediction, the method based on deep learning prediction can better plan the charging and discharging of the battery due to the higher prediction accuracy, which is reflected in the fact that the battery charging is more concentrated in the noon period, which further reduces the light drop rate (from 1.36% to 0.37%), and makes the power distribution of the feeding grid part smoother.

V. CONCLUSION

In this paper, the embedded PLC system based on IEC61499 standard is applied to the distributed residential photovoltaic energy storage system, and the control strategy of energy optimization scheduling of photovoltaic energy storage system is studied. Then, the algorithms of each part of the control strategy are encapsulated as function blocks, and the energy optimization scheduling programs under three air control strategies are constructed. Finally, the three applications were deployed on the embedded controller connected by the network to complete the running test. The experimental results show that the constructed control system realizes energy optimal scheduling, and reflects the advantages of IEC61499 standard in modeling and application of distributed control system.

REFERENCES

[1] 习近平. 在第七十五届联合国大会一般性辩论上的讲话. 中华人民共和国国务院公报, 28(3), 2020.
[2] Joseph Bergner, Johannes Weniger, Tjarko Tjaden, and Volker Quaschning. Feed-in power limitation of grid-connected pv battery systems with autonomous forecast-based operation strategies. In *29th European Photovoltaic Solar Energy Conference and Exhibition*, pages 2363–2370, 2014.
[3] Janina Moshövel, Kai-Philipp Kairies, Dirk Magnor, Matthias Leuthold, Mark Bost, Swantje Gährs, Eva Szczechowicz, Moritz Cramer, and Dirk Uwe Sauer. Analysis of the maximal possible grid relief from pv-peak-power impacts by using storage systems for increased self-consumption. *Applied Energy*, 137:567–575, 2015.
[4] Yannick Riesen, Christophe Ballif, and Nicolas Wyrsch. Control algorithm for a residential photovoltaic system with storage. *Applied Energy*, 202:78–87, 2017.
[5] 李天伦. 基于嵌入式的用户侧储能优化控制器研究与设计. Master's thesis, 常州大学, 2021.
[6] 李双双. 户用型光储一体化装置及其控制策略研究. Master's thesis, 陕西科技大学, 2020.
[7] 朱彦. 基于MPC的用户侧光储荷协调控制器设计. Master's thesis, 厦门理工学院, 2022.
[8] International Electrotechnical Commission, International Electrotechnical Commission, et al. Iec 61499-1: Function blocks-part 1 architecture. *Int. Stand. First Ed. Geneva*, 1, 2005.
[9] Alois Zoitl, Robert Lewis, et al. Modelling control systems using iec 61499. Technical report, IET, 2014.
[10] Georges Hebrail and Alice Berard. Individual Household Electric Power Consumption. UCI Machine Learning Repository, 2012. DOI: https://doi.org/10.24432/C58K54.

UEMA: An Symmetric-key AKA Scheme for Industrial Internet Multi-Cloud Applications in Untrusted Edge Environments Based on ECDH

Guiliang Chen[1,2],Jie Huang*[1,2]
1. 5G+ Industrial Internet Institute, Fuzhou University, Fuzhou 350108, China
2. College of Electrical Engineering and Automation, Fuzhou University, Fuzhou 350108, China
E-mail: chenguiliang_arm@163.com, jie.huang@fzu.edu.cn

***Abstract*:** The Industrial Internet of Things (IIoT) has transformed industrial processes, but the integration of edge computing introduces new security challenges, particularly in authentication and key agreement between resource-constrained edge gateways and multiple cloud application servers. In this article, we propose an Untrusted Edge Multi-cloud Authentication (UEMA) scheme for Industrial IoT, which relies on both symmetric encryption and elliptic curve Diffie-Hellman key exchange to enable efficient mutual authentication and secure communication channel establishment between edge gateways and multiple cloud-based applications in untrusted edge computing environments. Our approach addresses the unique security requirements of industrial environments while considering the limited computational and energy resources of edge devices. We implement a key evolution mechanism that enhances the protocol's security and robustness.The security of our protocol is formally verified using ProVerif, demonstrating its resilience against known attacks in IIoT scenarios. Performance evaluations show that UEMA offers efficiency in terms of computation and communication overhead, as well as scalability.

***Keywords*:** industrial internet of things, mutual authentication, key evolution, key synchronization, elliptic curve Diffie-Hellman

I. INTRODUCTION

The Industrial Internet of Things (IIoT) has emerged as a transformative paradigm, revolutionizing diverse industrial sectors through the integration of advanced information and communication technologies. By leveraging sensor networks, data analytics, and cloud computing, IIoT initiatives optimize industrial processes, enhance resource management, and improve operational efficiency [1, 2]. Within this context, edge computing has become a prevalent paradigm in IIoT, bringing computation and data storage closer to the point of need [3, 7]. This decentralized architecture significantly reduces latency and bandwidth usage while enhancing real-time performance and data privacy.

In factory settings, leveraging existing legacy infrastructure as edge gateways has become a common strategy to maximize resource utilization and minimize digital transformation costs. This approach is particularly advantageous for resource-constrained industrial environments, where devices may have limited processing power, memory, or energy capacity due to harsh operating conditions or outdated equipment [4]. In typical IIoT deployments, these edge gateways serve as crucial intermediaries between sensor networks and cloud application servers, collecting data from smart sensors and securely transmitting it to multiple cloud-based applications.

However, traditional security protocols often prove too resource-intensive for constrained industrial edge devices and are typically designed for single-application cloud environments [5, 6]. This limitation is particularly significant in real-world IIoT scenarios where multiple cloud application servers coexist and require simultaneous secure communication channels with edge gateways. The need for efficient mutual authentication and session key negotiation between resource-limited gateways and multiple cloud application servers introduces unique challenges that existing authentication protocols fail to address adequately [8–10].

To address these challenges, our research focuses on developing a secure and lightweight multi-application authentication scheme with key agreement specifically designed for resource-constrained edge gateways in IIoT environments. This approach aims to balance the critical requirements of security, efficiency, and scalability in industrial edge computing. The main contributions of this paper are as follows:

1) A novel multi-party authentication and key agreement scheme tailored for resource-constrained IIoT edge gateways communicating with multiple cloud application servers.
2) An innovative key evolution and synchronization mechanism that ensures authentication protocol security, strong consistency, and robustness while maintaining efficiency in multi-server IIoT environments.
3) A formal security analysis of the proposed scheme using ProVerif, demonstrating its resistance to known attacks in IIoT environments.

II. SYSTEM MODEL AND SECURITY FRAMEWORK

This section presents a comprehensive system model and security framework tailored for Industrial Internet of Things (IIoT) environments, addressing the unique challenges posed by Industry 4.0 initiatives. Our model considers the integration of legacy assets, reflects real-world industrial conditions, and optimizes for multi-cloud application deployment, all while operating under the constraints of potentially unreliable edge gateways and limited gateway resources.

A. SYSTEM MODEL

Our authentication framework comprises three principal components:

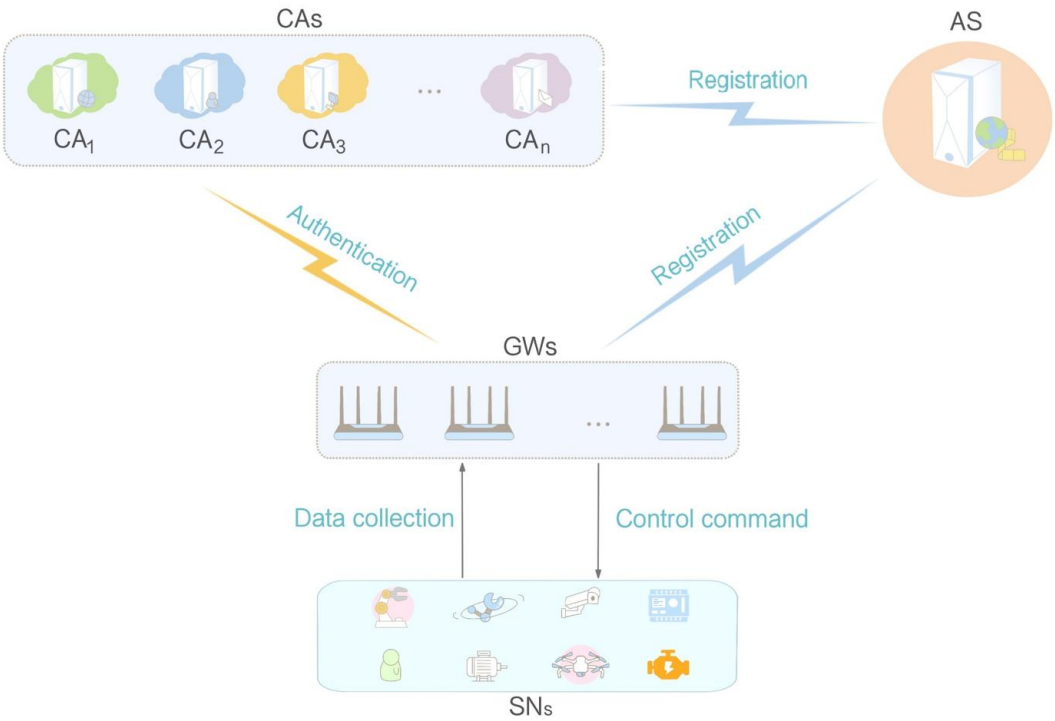


Fig. 1: System framework for IIoT authentication and key agreement

Table 1: Notations and Descriptions

Notation	Description
AS	Authentication Server
GW_i	IIoT Gateway i
CA_j	Cloud Application Server j
ID_E	Unique identifier for entity E
s	Master secret key of AS
$\mathcal{E}$	Elliptic curve over finite field $\mathbb{F}_p$
P	Base point on $\mathcal{E}$ of prime order n
$H(\cdot)$	Cryptographic hash function
$HMAC(\cdot)$	Hash-based Message Authentication Code
$E_K(\cdot)$	Symmetric encryption function with key K
$D_K(\cdot)$	Symmetric decryption function with key K
$F(\cdot)$	Key derivation function
$G(\cdot)$	Key evolution function
T	Key evolution interval
K^c_{AS-E}	Shared key between AS and entity E at counter c
c_E	Key evolution counter for entity E
c^{AS}_E	AS's stored counter for entity E
R_x	Random nonce generated by entity X
a, b	Ephemeral private ECDH keys
Q_a, Q_b	Ephemeral public ECDH keys
K_{shared}	ECDH shared secret between GW_i and CA_j
$K_{GW_i-CA_j}$	Session key between GW_i and CA_j
M_i	i-th protocol message, where $i \in \{1, 2, 3, 4\}$

- **Resource-Constrained IIoT Gateway (GW_i):** An edge device aggregating data from sensors and machinery, operating under moderate computational, memory, and energy limitations. It initiates connections and participates in mutual authentication with the Authentication Server and Cloud Application Servers.
- **Cloud Application Ecosystem ($\mathcal{CA} = \{CA_1, CA_2, ..., CA_n\}$):** Specialized cloud-based platforms processing data streams from IIoT gateways. Each $CA_j \in \mathcal{CA}$ requires secure authentication and communication with IIoT gateways.
- **Authentication Server (AS):** A trusted third-party facilitating initial authentication and key agreement between IIoT gateways and cloud application servers.

The model leverages Elliptic Curve Cryptography (ECC) for efficient key exchange in resource-constrained environments.

B. Security Framework

Our security framework is based on key assumptions and potential adversarial capabilities. We consider the Authentication Server (AS) as a trusted entity, immune to compromise, with long-term secret keys securely stored. However, communication channels are assumed susceptible to various attacks, including eavesdropping and manipulation. Adversaries may attempt Man-in-the-Middle (MITM), replay, and impersonation attacks. The potential compromise of individual cloud applications is also considered in our threat model. Additionally, we acknowledge that the key evolution process

may face interference from malicious actors. These considerations form the foundation of our robust security design, ensuring comprehensive protection against a wide range of potential threats in IIoT environments.

UEMA aims to achieve:

- **Mutual Authentication:** High-assurance identity verification.
- **Efficient Key Agreement:** Using ECC with minimal overhead.
- **Perfect Forward Secrecy:** Protect past sessions.
- **Key Independence:** Isolate compromised session keys.
- **Scalability:** Support dynamic addition/removal of entities.
- **Resource Efficiency:** Minimize requirements on IIoT gateways.
- **Multi-party Support:** Enable concurrent secure channels.
- **Resistance to Attacks:** Robust security against various threats.
- **Key Evolution and Synchronization:** Ensure reliable key management.

This framework addresses IIoT challenges including resource constraints, scalability requirements, potential untrustworthiness of edge gateways, and the need for efficient, secure communication across heterogeneous networks.

III. THE PROPOSED METHOD

UEMA comprises five main components: the initialization phase, entity registration phase, key evolution function, key synchronization function, and mutual authentication & key agreement phase. This section details each component of the protocol.

A. INITIALIZATION PHASE

Before system deployment, AS performs the following initialization steps:

1) Selects and publishes the parameters for the Elliptic Curve Diffie-Hellman (ECDH) key exchange:
   - An elliptic curve $\mathcal{E}$ over a finite field $\mathbb{F}_p$
   - A base point P on $\mathcal{E}$ of prime order n
   - The order p of the finite field
2) Chooses a secure hash function $H(\cdot)$
3) Chooses a secure symmetric encryption algorithm $E(\cdot)$ and a corresponding symmetric decryption algorithm $D(\cdot)$
4) Generates its master secret key s and keeps it secure
5) Selects a secure one-way hash function $G(\cdot)$ for key evolution
6) Decides on a key evolution interval T (e.g., number of authentications or time period)
7) Initializes a database to store entity information, including their identifiers and key evolution counters
8) Publishes the public parameters

$$\{\mathcal{E}, P, p, n, H(\cdot), E(\cdot), D(\cdot), G(\cdot), T\}$$

B. ENTITY REGISTRATION PHASE

The entity registration phase enables both gateways and application servers to become authorized participants in the system, as shown in Figure 2. This phase is crucial for establishing initial trust and secure communication channels.

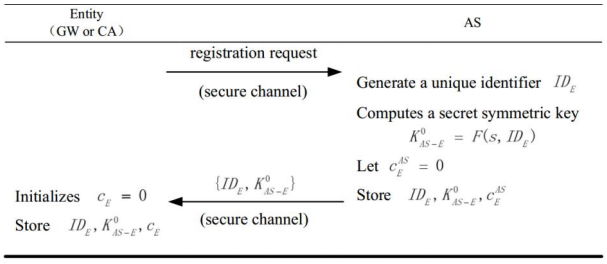


Fig. 2: Registration of Entity

Let E represent the registering entity, which can be either a gateway GW_i or an application server CA_j. The registration phase comprises the following steps:

1) The entity E initiates the registration process by transmitting a secure registration request to the AS through a pre-established secure channel.
2) Upon receiving the registration request, the AS:
   - Generates a unique identifier ID_E for entity E using a cryptographically secure pseudo-random number generator.
   - Computes an initial secret symmetric key K^0_{AS-E} for E:
   $$K^0_{AS-E} = F(s, ID_E) \tag{1}$$
   where F is a secure key derivation function and s is the AS's master secret key.
   - Initializes the key evolution counter $c^{AS}_E = 0$ for entity E in its database.
3) The AS constructs and securely transmits the following registration response to E:
   $$\{ID_E, K^0_{AS-E}\}$$
4) Upon receipt of the response, E:
   - Verifies the authenticity and integrity of the received data.
   - Securely stores the received values in its tamper-resistant storage module.
   - Initializes its local counter $c_E = 0$.

C. MUTUAL AUTHENTICATION & KEY AGREEMENT PHASE

As shown in Figure 3, this phase establishes a secure communication channel between GW_i and CA_j. The process is as follows:

1) GW_i initiates the process by generating an ECDH key pair $(a, Q_a = aP)$, selecting a unique random number R_1. It then sends message M_1 to the AS:
$$\begin{aligned} M_1 = \{&ID_{GW_i}, c_{GW_i}, \\ &E_{K^{c_{GW_i}}_{AS-GW_i}}(ID_{CA_j} \| R_1 \| Q_a), \\ &HMAC(K^{c_{GW_i}}_{AS-GW_i}, ID_{GW_i} \| c_{GW_i} \| \\ &H(E_{K^{c_{GW_i}}_{AS-GW_i}}(ID_{CA_j} \| R_1 \| Q_a)))\} \end{aligned}$$
2) Upon receipt of M_1, AS performs the following:

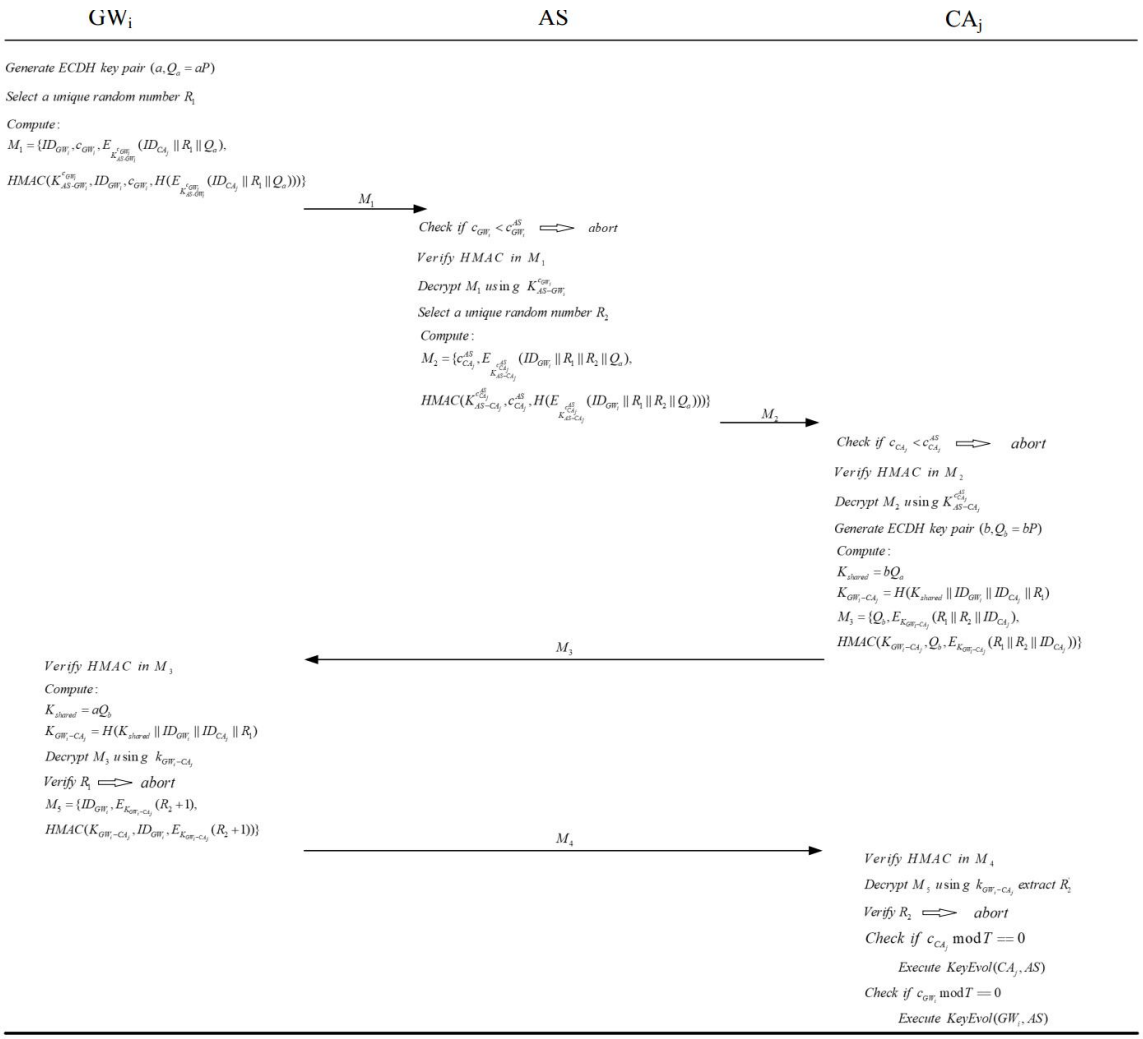


Fig. 3: Mutual authentication

- Checks if $c_{GW_i} < c^{AS}_{GW_i}$. If true, aborts.
- Verifies HMAC in M_1.
- Decrypts M_1 using $K^{c_{GW_i}}_{AS-GW_i}$.
- Selects a unique random number R_2.
- Constructs and sends message M_2 to CA_j:

$$M_2 = \{c^{AS}_{CA_j}, E_{K^{c^{AS}_{CA_j}}_{AS-CA_j}}(ID_{GW_i}\|R_1\|R_2\|Q_a),$$
$$HMAC(K^{c^{AS}_{CA_j}}_{AS-CA_j}, c^{AS}_{CA_j}\|$$
$$H(E_{K^{c^{AS}_{CA_j}}_{AS-CA_j}}(ID_{GW_i}\|R_1\|R_2\|Q_a)))\}$$

3) CA_j processes M_2 as follows:
   - Checks if $c_{CA_j} < c^{AS}_{CA_j}$. If true, aborts.
   - Verifies HMAC in M_2.
   - Decrypts M_2 using $K^{c^{AS}_{CA_j}}_{AS-CA_j}$.
   - Generates its own ECDH key pair $(b, Q_b = bP)$.
   - Computes the shared secret $K_{shared} = bQ_a$.
   - Derives the session key $K_{GW_i-CA_j} = H(K_{shared}\|ID_{GW_i}\|ID_{CA_j}\|R_1)$.
   - Constructs and sends message M_3 to GW_i:

$$M_3 = \{Q_b, E_{K_{GW_i-CA_j}}(R_1\|R_2\|ID_{CA_j}),$$
$$HMAC(K_{GW_i-CA_j}, Q_b\|$$
$$E_{K_{GW_i-CA_j}}(R_1\|R_2\|ID_{CA_j}))\}$$

4) Upon receiving M_3, GW_i:
   - Verifies HMAC in M_3.
   - Computes $K_{shared} = aQ_b$.
   - Derives $K_{GW_i-CA_j} = H(K_{shared}\|ID_{GW_i}\|ID_{CA_j}\|R_1)$.
   - Decrypts M_3 using $K_{GW_i-CA_j}$.
   - Verifies R_1.
   - Constructs and sends message M_4 to CA_j:

$$M_4 = \{ID_{GW_i}, E_{K_{GW_i-CA_j}}(R_2+1),$$
$$HMAC(K_{GW_i-CA_j}, ID_{GW_i}\|$$
$$E_{K_{GW_i-CA_j}}(R_2+1))\}$$

5) CA_j finalizes the process:
   - Verifies HMAC in M_4.
   - Decrypts M_4 using $K_{GW_i-CA_j}$ and verifies R_2+1.

- If $c_{CA_j} \bmod T == 0$, executes $KeyEvol(CA_j, AS)$.

6) GW_i completes the process:
   - If $c_{GW_i} \bmod T == 0$, executes $KeyEvol(GW_i, AS)$.

This mutual authentication and key agreement phase ensures secure communication between entities while maintaining key synchronization through the use of the $KeySync$ and $KeyEvol$ functions when necessary.

D. KEY EVOLUTION FUNCTION

We define a key evolution function $KeyEvol(E, AS)$ that takes an entity E and the Authentication Server AS as input. This function is used to evolve the shared keys between E and AS. The function is defined as follows:

Algorithm 1 KeyEvol(E, AS)

$c_E \leftarrow c_E + 1$
$K_{AS-E}^{c_E} \leftarrow G(K_{AS-E}^{c_E-1} \| ID_E \| c_E)$
E securely stores the new key $K_{AS-E}^{c_E}$ and updated counter c_E
AS updates $c_E^{AS} \leftarrow c_E^{AS} + 1$ in its database
AS computes and stores $K_{AS-E}^{c_E^{AS}} \leftarrow G(K_{AS-E}^{c_E^{AS}-1} \| ID_E \| c_E^{AS})$
return SUCCESS

The key evolution occurs every T authentications or time period, where T is a system parameter defined during the initialization phase.

E. KEY SYNCHRONIZATION FUNCTION

The KeySync(E, AS) function maintains system integrity by addressing counter inconsistencies between entity E and Authentication Server (AS). It serves as:

1) An error recovery mechanism for counter mismatches.
2) A security enhancement tool for proactive synchronization.
3) A system resilience feature, avoiding complete re-registration.
4) A long-term maintenance safeguard for extended operational periods.

The function securely re-establishes correct key states, enhancing overall system robustness. It operates only in exceptional cases, as normal communication interruptions do not directly cause desynchronization. This approach ensures consistent keys and counters under typical circumstances while providing a crucial safeguard for rare discrepancies.

The KeySync(E, AS) function is defined as follows:

Algorithm 2 KeySync(E, AS)

E generates a random nonce N_{sync}
E sends $\{ID_E, c_E, E_{K_{AS-E}^{c_E}}(N_{sync})\}$ to AS
AS retrieves c_E^{AS} from its database
AS verifies the authenticity of the request
$c_{correct} \leftarrow \max(c_E, c_E^{AS})$
AS computes $K_{AS-E}^{c_{correct}}$
AS sends $E_{K_{AS-E}^{c_E}}(c_{correct} \| N_{sync})$ to E
E decrypts the message and verifies N_{sync}
E sets $c_E \leftarrow c_{correct}$
E computes $K_{AS-E}^{c_{correct}} = G(K_{AS-E}^{c_{correct}-1} \| ID_E \| c_{correct})$
AS updates $c_E^{AS} \leftarrow c_{correct}$ in its database
if synchronization is successful **then**
  return SUCCESS
else
  return FAILURE
end if

IV. SECURITY ANALYSIS

A. FORMAL SECURITY VERIFICATION (AUTOMATED) USING PROVERIF TOOL

To rigorously validate the security properties of UEMA, we conduct a formal security verification using the ProVerif tool. ProVerif is an automatic cryptographic protocol verifier widely used in analyzing security protocols [11]. It can verify various security properties such as secrecy, authentication, and forward secrecy.

We model our protocol in the ProVerif language, defining the cryptographic primitives, functions, and processes for each participant. The full ProVerif code is available in the appendix. Here, we present the key aspects of our model and the verification results.

To verify the security properties of UEMA, we define queries to check whether an attacker can obtain the session key and verify the mutual authentication between the Gateway and the Cloud Application server, as well as the correct sequence of protocol events.

After running the ProVerif tool on our model, we obtain the following results:

```
RESULT not attacker(K_GW_CA[]) is true.
RESULT inj-event(CAStarted(x,y,n,q)) ==>
inj-event(GWStarted(x,y,n,q)) is true.
RESULT inj-event(GWFinished(x,y,k)) ==>
inj-event(CAStarted(x,y,n,q)) is true.
RESULT inj-event(CAFinished(x,y,k)) ==>
inj-event(GWFinished(x,y,k)) is true.
```

These results indicate that UEMA successfully preserves the secrecy of the session key and achieves mutual authentication, even with the addition of key evolution and synchronization mechanisms. Specifically:

1) The attacker cannot obtain the session key (K_{GW_CA}), ensuring the confidentiality of the communications between the Gateway and the Cloud Application server.
2) The correspondence assertions hold, confirming that UEMA achieves mutual authentication between the Gateway and the Cloud Application server, and that the protocol events occur in the correct sequence.
3) The key evolution and synchronization functions do not introduce vulnerabilities that could be exploited by an attacker.

In conclusion, the formal security verification using the ProVerif tool corroborates our theoretical security analysis, demonstrating that UEMA achieves its intended security goals, including secrecy of session keys and mutual authentication, while maintaining these properties through key evolution and synchronization processes. This verification adds another layer of confidence to the security of our protocol, complementing the other analytical methods used in this paper.

Table 2: Security Features of the Proposed Protocol

Security Feature	Supported
Explicit Mutual Authentication	✓
Key Agreement and Session Key Security	✓
Perfect Forward Secrecy (PFS)	✓
Weak Backward Security	✓
Session Key Independence	✓
End-to-end Security	✓
Data Integrity	✓
Data Confidentiality	✓
Resistance to MITM Attacks	✓
Resistance to Replay Attacks	✓
Resistance to Impersonation Attacks	✓
Scalability	✓
No Clock Synchronization	✓
Formal Security Proof	✓
Soundness	✓
Key Evolution	✓

B. ANALYSIS OF OTHER SECURITY REQUIREMENTS

Our proposed authentication and key agreement protocol for IIoT environments addresses a comprehensive set of security requirements. Table 2 presents an overview of the security features incorporated in UEMA.

The protocol achieves explicit mutual authentication through a multi-step process involving the Gateway (GW_i), Cloud Application (CA_j), and Authentication Server (AS). This ensures that all parties can verify each other's identities, mitigating the risk of impersonation attacks.

Key agreement and session key security are realized using Elliptic Curve Diffie-Hellman (ECDH) key exchange, providing a robust mechanism for secure key establishment. The use of ephemeral ECDH key pairs for each session guarantees Perfect Forward Secrecy (PFS), ensuring that compromise of current session keys does not affect the security of past sessions.

Weak Backward Security is implemented through a key evolution mechanism, enhancing the protocol's resilience against long-term key compromises. Session key independence is maintained by incorporating unique parameters for each session, preventing cross-session attacks.

The protocol supports end-to-end security by facilitating direct key agreement between GW_i and CA_j, reducing the risk of intermediary compromises. Data integrity and confidentiality are ensured through the use of cryptographic primitives such as HMAC and symmetric encryption.

UEMA demonstrates resistance to various attacks, including Man-in-the-Middle (MITM), replay, and impersonation attacks, through careful design of message flows and cryptographic operations. It also supports scalability, crucial for expanding IIoT deployments, and does not require clock synchronization, enhancing its practicality in diverse network conditions.

The incorporation of a key evolution mechanism further enhances the protocol's long-term security, allowing for periodic updates of long-term keys without requiring a complete re-registration process.

In summary, our proposed protocol offers a comprehensive security solution tailored to the unique challenges of IIoT environments, balancing robust security features with practical considerations for resource-constrained devices and scalable deployments.

Table 3: Computational Overhead for Registration and Authentication Phases

Phase	Entity	Computation
Registration	AS	$T_{prng} + T_h$
	E (GW or CA)	–
Authentication	GW	$2T_{ecdh} + 2T_{enc} + T_{dec} + 2T_h + 2T_{prng} + 2T_{hmac}$
	AS	$T_{dec} + T_{enc} + T_{prng} + 2T_h + 2T_{hmac}$
	CA	$2T_{ecdh} + T_{enc} + 2T_{dec} + 2T_h + T_{prng} + 2T_{hmac}$

V. PERFORMANCE EVALUATION

To evaluate the efficiency and practicality of UEMA, we conducted a comprehensive performance analysis. This section presents the results of our evaluation in terms of computational overhead, communication cost, and storage overhead.

A. COMPUTATIONAL OVERHEAD

To evaluate the computational efficiency of UEMA, we analyze the cryptographic operations performed by each entity (GW$_i$, AS, and CA$_j$) during various phases of the protocol. We employ the following notation to represent the computational cost of different operations:

- T_h: Time for one hash function operation
- T_{enc}: Time for one symmetric encryption operation
- T_{dec}: Time for one symmetric decryption operation
- T_{ecdh}: Time for one ECDH key pair generation or point multiplication
- T_{prng}: Time for one pseudo-random number generation
- T_{hmac}: Time for one HMAC operation

Table 3 summarizes the computational overhead for each entity in the registration and authentication phases of our protocol.

As evident from Table 3, the registration phase imposes minimal computational burden on the entities, with only the AS performing lightweight operations. This design choice facilitates efficient system scalability and easy integration of new devices.

In the authentication phase, the computational load is distributed among the entities, with the GW and CA bearing slightly higher costs due to the ECDH operations. However, these operations are crucial for establishing secure session keys. The AS, serving as a trusted intermediary, performs fewer computationally intensive operations, which is advantageous for centralized management in large-scale IIoT deployments.

The balanced distribution of computational overhead across entities reflects our protocol's design consideration for the heterogeneous nature of IIoT environments. By optimizing the computational requirements for resource-constrained devices while maintaining robust security measures, UEMA achieves a practical balance between security and efficiency in IIoT scenarios.

Table 4: Communication Cost by Entity

Entity	Sent (bits)	Received (bits)
GW	1920	1312
AS	1344	1120
CA	1312	2144

Table 5: Long-term Storage Requirements for Each Entity

Symbol	GW	CA	AS
ID_{GW_i}, ID_{CA_j}	✓	✓	✓
K_{AS-GW_i}, K_{AS-CA_j}	✓	✓	✓
c_{GW_i}, c_{CA_j}	✓	✓	✓
s	×	×	✓
$K_{GW_i-CA_j}$	✓	✓	×
Total (bits)	576	576	320n+320m+256

B. COMMUNICATION COST

To quantify the communication cost, we define the bit length of each parameter used in our protocol. Identifiers (ID_{GW_i} and ID_{CA_j}) and counters (c) are allocated 32 bits each, aligning with standard practices in network protocols. Random numbers (R) and ECDH public keys (Q) are assigned 256 bits, with the latter assuming the use of the NIST P-256 elliptic curve, which provides a balanced trade-off between security and efficiency. Encrypted blocks utilize AES-256 in CBC mode with padding, resulting in a length equal to the plaintext plus 256 bits. HMAC values are set to 256 bits, ensuring robust message integrity.

Based on these parameters, we calculate the size of each message exchanged in our protocol. Table 4 presents a breakdown of the communication cost by entity.

The total communication cost for one complete authentication and key agreement process amounts to 3200 bits (400 bytes). This relatively low overhead is particularly advantageous for bandwidth-constrained IIoT networks, where minimizing data transmission is crucial for overall system efficiency. The balanced distribution of communication load among entities reflects our protocol's design consideration for the heterogeneous nature of IIoT environments, ensuring that no single component bears a disproportionate burden.

C. STORAGE OVERHEAD

We analyze the long-term storage requirements for each entity in our protocol based on parameter sizes. Table 5 presents a comprehensive overview of these requirements. The Gateway (GW) and Cloud Application (CA) each require 576 bits of storage, which includes identifiers, shared keys with the Authentication Server (AS), counters, and session keys. The AS, serving as the central authority, needs more storage: 320n+320m+256 bits, where n and m represent the number of GWs and CAs in the system, respectively. This scalable storage requirement for AS accommodates the growing number of devices in IIoT environments. Notably, only AS stores the master secret key s, enhancing overall system security. This efficient storage allocation demonstrates our protocol's suitability for resource-constrained IIoT devices while maintaining robust security measures.

VI. CONCLUSION AND FUTURE WORK

This paper presented an authentication and key agreement scheme for IIoT environments, offering enhanced security with comprehensive features, improved efficiency for resource-constrained devices, key evolution and synchronization mechanisms, formal security verification using ProVerif, and thorough performance evaluation. Future research directions include integration with blockchain technology to further enhance data integrity and traceability in IIoT systems.

ACKNOWLEDGMENTS

This project was supported by the National Natural Science Foundation of China (NSFC) on "Basic Theory and Key Technologies of the Future Industrial Internet" Major Research Program under grant No.92367109.

REFERENCES

[1] Q. Fan, J. Chen, M. Shojafar, et al., "SAKE*: A Symmetric Authenticated Key Exchange Protocol With Perfect Forward Secrecy for Industrial Internet of Things," IEEE Trans. Ind. Inf., vol. 18, no. 9, pp. 6424–6434, 2022.

[2] Y. Zhang, D. He, P. Vijayakumar, et al., "SAPFS: An Efficient Symmetric-Key Authentication Key Agreement Scheme With Perfect Forward Secrecy for Industrial Internet of Things," IEEE Internet Things J., vol. 10, no. 11, pp. 9716–9726, 2023.

[3] F. Wu, L. Xu, S. Kumari, et al., "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," Journal of Network and Computer Applications, vol. 89, pp. 72–85, 2017.

[4] C. Patel and N. Doshi, "Secure Lightweight Key Exchange Using ECC for User-Gateway Paradigm," IEEE Trans. Comput., vol. 70, no. 11, pp. 1789–1803, 2021.

[5] Z. Yang, J. He, Y. Tian, et al., "Faster Authenticated Key Agreement With Perfect Forward Secrecy for Industrial Internet-of-Things," IEEE Trans. Ind. Inf., vol. 16, no. 10, pp. 6584–6596, 2020.

[6] Z. Zhang, W. Huang, Y. Huang, et al., "A Domain Isolated Tripartite Authenticated Key Agreement Protocol With Dynamic Revocation and Online Public Identity Updating for IIoT," IEEE Internet Things J., vol. 11, no. 9, pp. 15616–15632, 2024.

[7] J. Wang, L. Wu, H. Wang, et al., "A Secure and Efficient Multiserver Authentication and Key Agreement Protocol for Internet of Vehicles," IEEE Internet Things J., vol. 9, no. 23, pp. 24398–24416, 2022.

[8] M. K. Hasan, Z. Weichen, N. Safie, et al., "A Survey on Key Agreement and Authentication Protocol for Internet of Things Application," IEEE Access, vol. 12, pp. 61642–61666, 2024.

[9] I. U. Haq, J. Wang, Y. Zhu, et al., "A survey of authenticated key agreement protocols for multi-server architecture," Journal of Information Security and Applications, vol. 55, p. 102639, 2020.

[10] A. Kumar, R. Saha, M. Conti, et al., "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," Journal of Network and Computer Applications, vol. 204, p. 103414, 2022.

[11] P. M. Rao and B. D. Deebak, "A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions," Ad Hoc Networks, vol. 146, p. 103159, 2023.

Guiliang CHEN was born in 1993. He received the B.E. degree from Fuzhou University. He is now a Ph.D. candidate of Electronic Information at the College of Electrical Engineering and Automation, Fuzhou University. His research interests include industrial internet of things authentication, edge computing security, and multi-cloud application protocols. (Email: chenguiliang_arm@163.com)

Jie HUANG was born in 1983. He is now a professor and doctoral supervisor at the School of Electrical Engineering and Automation, Fuzhou University, and the dean of the 5G+ Industrial Internet Research Institute of Fuzhou University. His research interests include industrial internet, autonomous robots, complex network dynamics, and multi-agent systems. (Email: jie.huang@fzu.edu.cn)

面向 Eclipse 工业互联网开源软件的安全漏洞分析

李增扬 [a)]，黄彬彬 [a)]，刘慧 [b)*]，吕金虎 [c)]，吴晓群 [d)]

a) 华中师范大学 计算机学院，武汉 430079

b) 华中科技大学 人工智能与自动化学院，武汉 430074

c) 北京航空航天大学 自动化科学与电气工程学院，北京 100191

d) 深圳大学 计算机与软件学院，深圳 518060

摘　要：本文针对当前缺乏工业互联网软件安全态势评估这一现实问题，研究了 Eclipse 基金会旗下的三个工业互联网开源软件项目（即 Ditto、Hono 和 Kura）的软件安全漏洞分布和安全漏洞随软件版本迭代的演化情况。采用 CodeQL 对这每个项目的 8 个正式发布版本进行官方提供的 63 类软件安全漏洞检测，通过分析实验结果发现：（1）每个软件项目中均只检测出少部分类型的安全漏洞，不同项目中检测出的安全漏洞在具体安全漏洞类型上的聚集程度存在明显差异，但 CWE-798 类型（使用硬编码的凭证）的软件安全漏洞在三个软件项目中都频繁发生；（2）三个软件项目的漏洞总数随软件版本迭代更新呈稳定状态或上升趋势，而漏洞密度的演化趋势各不相同；（3）三个软件项目的高危漏洞数占漏洞总数的比例当前都维持在高位，均超过 65%。上述发现表明，工业互联网开源软件存在不同程度安全风险，其中的高危安全漏洞亟需得到软件开发团队的重视和及时修复，以有效降低工业互联网软件安全风险。

关键词：工业互联网；软件安全；安全漏洞；CodeQL

Analysis of Security Vulnerabilities of Eclipse Open-Source Software in Industrial Internet of Things

Zengyang Li [a)], Binbin Huang [a)], Hui Liu [b)], Jinhu Lü [c)], Xiaoqun Wu [d)]

a) School of Computer Science, Central China Normal University, Wuhan 430079, China

b) School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan 430074, China

c) School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China

d) College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China

Abstract: This paper addresses the current issue of the lack of security situation assessments for software in industrial internet of things (IIoT), by studying the distribution of software security vulnerabilities and the evolution of these vulnerabilities with software version iterations in three open-source software projects (i.e., Ditto, Hono, and Kura) supported by the Eclipse Foundation in the IIoT domain. Based on the experimental

*通讯作者

results of 63 officially recommended categories of software security vulnerability detection using CodeQL in eight releases of each project, it was found that: (1) Only a small portion of categories of security vulnerabilities were detected in each project, and there were significant differences in the concentration of specific categories of detected security vulnerabilities among different projects, with CWE-798 as the frequently commonly occurring security vulnerability in all the three projects; (2) The number of vulnerabilities in the three projects showed a stable state or an upward trend with the iteration and updates of software releases, and the vulnerability density evolves differently in the three projects; (3) The proportion of high-risk vulnerabilities in the total number of vulnerabilities for the three selected IIoT open-source software projects all remained high, each exceeding 65%. These findings indicate that IIoT open-source software projects have varying degrees of security risks, and the high-risk security vulnerabilities within such projects urgently require attention and timely remediation by the software development teams to effectively reduce the security risks of IIoT software.

Key words: Industrial Internet of Things, Software Security, Security Vulnerability, CodeQL

1　引言

在数字化浪潮席卷全球的今天，工业互联网（Industrial Internet of Things，IIoT）以其独特的魅力和巨大的潜力，正逐渐改变着传统制造业的面貌，成为推动全球经济数字化转型的重要力量。通用电气在 2012 年提出了工业设备和信息技术融合的概念，并在 2013 年 6 月提出了工业互联网革命的概念。 2016 年，中国成立了工业互联网产业联盟，重新定义了工业互联网为由互联网和新信息技术深度整合形成的工业和应用生态体系，并随后发布了“中国制造 2025”等相关战略[1]。

工业互联网通过深度融合先进的信息通信技术与现代工业技术，实现了工业生产的智能化、网络化和自动化，它通过连接各种设备和生产线，实现了数据的实时流通和资源的优化配置，极大地提高了生产效率和质量。而工业互联网的安全问题也日益凸显，其中软件安全漏洞成为威胁工业互联网安全的重要因素之一。

软件安全漏洞是指在软件的规范、开发或配置中出现错误，并导致软件执行违反一定安全策略的情况[2]，已有大量的研究表明，安全漏洞一旦被利用，可能导致生产设备的故障和停机，还可能引发数据泄露、系统被恶意控制等严重后果，造成巨大的经济损失[14-16]。因此，研究工业互联网的软件安全漏洞具有重要的现实意义。

工业互联网软件中开源软件也占据一定比重，开源软件具有开放、共享、协作等特性，使得开发者可以更加高效地进行软件开发和迭代。然而，由于开源软件的源代码是公开的，这也为恶意攻击者提供了可乘之机。攻击者可以通过分析源代码来发现潜在的安全漏洞，进而利用这些漏洞发起针对性的攻击。如何有效地识别、评估和应对工业互联网开源软件中的安全漏洞，成为了当前需要重视的安全问题。

本文以 Eclipse 基金会旗下的工业互联网开源软件为研究对象，并选取了其不同功能下规模较大的三个项目。在工业互联网领域，Eclipse 基金会通过提供一系列的开源项目和工具如 Eclipse Kura 等，与工业互联网领域建立了紧密的联系，其项目涵盖了数字孪生、云服务、Web 框架、API 等 IIoT 关键技术，促进了工业自动化和物联网技术的发展。Eclipse 基金会还推动了开放工业自动化工作组（Open Industrial Automation Working Group），旨在将工业级的开源软件引入车间，通过提供可靠的开源技术，满足工业和中小型企业向数字工厂发展的需求。通过对 Eclipse 基金会旗下的工业互联网开源软件进行软件安全漏洞检测，探究安全漏洞的分布、安全漏洞演化趋势，尤其是高危安全漏洞的演化趋势，从而实现对相关工业互联网开源软件的安全态势有一个清晰的认知。

传统软件安全漏洞检测方法主要包括静态分析和动态分析两种。静态分析是在不运行程序的情况下，通过对源代码或二进制代码进行分析来发现潜在的漏洞；这种方法能够全面地扫描代码，但对于大型复杂的软件系统，其效率和准确性往往受到限制。动态分析则是在程序运行时监控其行为，寻找异常情况，从而发现漏洞；这种方法能够更精确地定位漏洞，但需要构造大量的测试用例，且无法覆盖所有的执行路径[17]。

近年来，一些新兴的软件漏洞分析方法也相继出现。CodeQL 就是一种新兴的代码分析工具，具有独特的查询语言和强大的分析能力[1]。它能够处理大规模的代码库，并且能够自动发现潜在的安全隐患。CodeQL 的设计理念是让开发者能够像操作数据库一样操作代码，使用类似 SQL 的查询语言来寻找代码中的特定模式，这种抽象层面上的创新大大提高了代码分析的效率和精确度。通过使用 CodeQL，开发者可以更快地定位问题，发现那些常规测试可能遗漏的安全漏洞。

本文的主要贡献包括：（1）采用软件安全检测工具 CodeQL 对工业互联网开源软件进行了 63 类安全漏洞的安全风险评估，发现了 Eclipse 工业互联网开源软件中高频发生的安全漏洞类别；（2）发现工业互联网开源软件中的高危安全漏洞比例目前保持在超过 65%的高位。

本文剩余部分的结构如下：第 2 节对相关工作进行梳理，第 3 节阐述实验目标和实验流程，第 4 节报告实验结果及其分析，第 5 节总结全文并提供未来需进一步研究的方向。

2 相关工作

在工业互联网安全领域有不少学者进行了相关研究。邢晨对工业互联网的数据安全做出了研究，指出面临的挑战并给出应对策略[3]。马娟等人从网络安全管理和防护角度，梳理了工业互联网的发展现状和面临的问题，论证了安全管理与防护的具体路径[4]。王鹏等人从数据加密和入侵检测两方面研究，完成了基于改进卷积神经网络的异常流量检测模型，并做出了基于云存储的全同态数据加密方案[5]。李杺恬等人分

[1] https://securitylab.github.com/tools/codeql

析了不同场景下的不同安全风险，从四个方面进行了网络安全风险分析，并提出了工业互联网中区块链的网络安全管控策略[6]。马佳利等人基于数字孪生的想法，通过收集现场数据并使用孪生模型安全认知，研究了数字空间中的异常检测和响应方法[10]。李欣等人以智能制造和智慧城市发展为例，分析了相关应用面临的主要网络安全风险和挑战，并尝试给出了数字孪生技术的网络安全保障方案[11]。Selvarajan 等人研究通过实现基于人工智能的轻量级区块链安全模型，来确保工业物联网系统的隐私和安全性[18]。Zhou 等人构建了一种自主且可靠的联邦极端梯度提升学习算法，以破解数据隔离问题，提供隐私保护和可验证性[19]。Singh 等人则提出了使用混沌映射和 DNA 加密的图像安全框架[9]。但上述研究均为对工业互联网软件安全漏洞进行分析或对某一模块进行独立研究，而本文则聚焦于工业互联网领域开源软件的安全漏洞检测和安全风险评估。

CodeQL 在软件漏洞分析领域也存在一些研究。Majdinasab 等人[7]再现了 Pearce 等人[8]关于 AI 助力的代码生成工具存在的安全问题的研究，其结果表明，随着 Copilot 较新版本的改进，脆弱代码建议的百分比从 36.54% 降至 27.25%。Szabó等人探讨了增量化是否有助于加速生产 CodeQL 分析，为 GitHub 上的拉取请求提供自动反馈[13]。Hamer 等人利用 CodeQL 检测了来自 ChatGPT 和 StackOverflow 中 108 个项目的漏洞，并发现了其中 274 个独特的漏洞和 25 种 CWE（Common Weakness Enumeration）类型[11]。本文实验中进行的软件安全漏洞分析也采用 CodeQL 这一先进的安全漏洞分析工具，并使用 CodeQL 官方提供的用于 Java 代码的 63 类代表性安全漏洞检测查询。以期能够广泛地评估工业互联网软件的安全漏洞情况，对工业互联网软件安全态势有更全面和深刻理解。

3　实验设计

本实验主要研究目标是探索典型工业互联网软件中的软件安全漏洞分布和软件安全漏洞（尤其是高危漏洞）随软件版本的演化趋势，从而对工业互联网软件安全态势有一个整体性的理解。本节首先阐述研究问题，接下来详细描述本实验的主要流程包括五个步骤，即选择实验项目、编译 CodeQL 数据库、选择查询语句、执行查询语句和分析查询结果。

3.1　研究问题

基于本实验的研究目标，提出了以下三个研究问题（Research Question，RQ）。

RQ1：所选 Eclipse IIoT 开源软件项目中的安全漏洞是如何分布的？本实验将考察不同版本下软件安全漏洞在不同类型上的分布。此研究问题的答案可以让我们对所选 Eclipse IIoT 开源软件项目中的安全漏洞有一个基本的认识，比如有哪些类型安全漏洞频繁出现，从而有助于制定合理的策略来降低 Eclipse IIoT 开源软件项目中的安全漏洞可能带来的潜在风险。

RQ2：所选 Eclipse IIoT 开源软件项目中的安全漏洞随软件版本是如何演化的？本实验将从安全漏洞数量和密度的角度去考察所选 Eclipse IIoT 开源软件项目中的安全漏洞随软件版本的演化趋势。此研究问题的答案有助于理解所选 Eclipse IIoT 开源软件项目的安全质量是如何变化的，以及安全漏洞被重视的程度。

RQ3: 所选 Eclipse IIoT 开源软件项目中的高危安全漏洞随软件版本是如何演化的？本实验将从高危安全漏洞数量和高危安全漏洞占比的角度去考察高危安全漏洞随软件版本迭代的演化趋势。本文所指的高危漏洞特指位列 2023 年度 CWE 最危险的安全漏洞前 25 名的漏洞。此研究问题的答案有助于更深入理解所选 Eclipse IIoT 开源软件项目的安全态势变化情况，从而提升开发团队和用户提供有效的警示，提升他们的工业互联网软件安全意识。

3.2 选择实验项目

Eclipse 基金会旗下的 IIoT 开源软件生态为工业互联网提供了一系列重要的开源软件，因此，我们从这个开源软件生态中按一定的标准选择合适项目作为实验项目：（1）项目规模在 10 万行代码以上，保证软件项目规模较大；（2）项目仍在活跃，近三个月内仍在进行代码更新和缺陷修复；（3）项目具有 8 个以上正式发布版本，从而可以直观地观察安全漏洞的演变过程；（4）使用 Java 语言开发；（5）具有重要功能的 IIoT 项目功能，如网关连接，数字孪生模式等，这类软件在 IIoT 占据着重要的地位，其安全漏洞的出现，会对 Eclipse IIoT 开源生态造成更大地影响。选择 Eclipse IIoT 开源项目 Ditto[2]，Hono[3]和 Kura[4]作为研究对象，均为使用 Java 语言开发的项目。从 GitHub 上下载源码，Ditto、Hono 和 Kura 项目各下载 8 个正式发布版本的源代码。所选项目基本信息如表 1 所示。

表 1 实验项目基本信息

项目名	描述	规模	版本
Eclipse Ditto	Eclipse Ditto 是一个开源软件，为物联网应用程序提供数字孪生模式，从而实现工业系统中不同设备和服务的交互。它支持多种通信协议，使来自不同的设备可以在一个统一的平台上交流。Ditto 抽象了底层的通信细节，减少了对复杂的通信协议的处理问题。Ditto 的设计强调了模块化和可扩展性，可以轻松地与其他系统集成，以支持使用标准的或自定义设备协议的通信。这种集成能力使得 Ditto 能够在各种工业环境中发挥作用。并且提供了丰富的 API，为开发者提供便利。	41 万行代码	2.3.0、2.4.0、3.0.0、3.1.0、3.2.0、3.3.0、3.4.0、3.5.4
Eclipse Hono	Eclipse Hono 是一个开源的物联网设备连接和消息路由平台，支持多种协议，可以集成各种不同的设备。它提供统一的、高性能的接口，可以在大规模工业互联网场景中处理设备到云端的通信。Hono 用一种标准化的方式来管理大量设备的数据流，使开发人员不必关心复杂的物联网基础设施，可以集中精力构建业务逻辑。Hono 的微服务架构允许横向扩展，以适应增长的设备数量。安全性强，提供了基于 OAuth 2.0 的身份验证和授权机制，保证了数据传输过程中的安全性。	11 万行代码	1.5.0、1.7.0、1.9.0、1.11.0、2.1.0、2.3.0、2.4.0、2.5.0

[2] https://github.com/eclipse-ditto/ditto

[3] https://github.com/eclipse-hono/hono

[4] https://github.com/eclipse/kura

Eclipse Kura	Eclipse Kura 是一款开源的物联网网关软件，具备强大的连接能力，支持多种协议和多种网络连接方式。提供了丰富的 API，可以轻松访问多种底层硬件。除了连接功能，它还提供了防火墙配置、网络延时等功能，全面满足各种应用需求。还提供了 OSGI 捆绑包，简化了网络配置的管理、与服务器的通信和远程网关管理。	30 万行代码	2.0.0、4.0.0、4.1.2、5.0.0、5.1.0、5.2.0、5.3.0、5.4.0

3.3　编译 CodeQL 数据库

分别对每个项目每个版本的源代码进行数据库的编译。使用 CodeQL 命令行工具将源码编译成能够识别的 CodeQL 数据库，用作后续步骤的查询分析。在本文的实验中，数据库的生成是第一难点，三个项目的编译环境的配置各有差别。实验选取了每个项目的多个版本，不同版本的迭代更新也加大了数据库编译的难度，需要使用不同的方法来解决因为历史版本的变化导致的问题。

3.4　选择查询语句

本实验使用 CodeQL 官方文档里用于 Java 语言的所有标准安全漏洞查询文件[5]来作为 CodeQL 查询语句，一共有 63 类安全漏洞的查询，如表 2 所示。这些官方提供的安全漏洞查询文件是经过了大量实验检验的，具有较高的可信度。为了区分高危安全漏洞，在表 2 的最后一列给出了对应安全漏洞类型对应在 2023 年度 CWE 最危险的 25 类安全漏洞列表[6]中的名次。

表 2　查询文件表

漏洞编号	漏洞描述	在 2023 CWE TOP 25 最危险漏洞列表中的排名
CWE-020	输入验证不恰当	6
CWE-022	对路径名的限制不恰当（路径遍历）	8
CWE-023	路径遍历	
CWE-074	输出中的特殊元素转义处理不恰当（注入）	
CWE-078	OS 命令中使用的特殊元素转义处理不恰当（OS 命令注入）	5
CWE-079	在 Web 页面生成时对输入的转义处理不恰当（跨站脚本）	2
CWE-089	SQL 命令中使用的特殊元素转义处理不恰当（SQL 注入）	3
CWE-090	LDAP 注入漏洞	
CWE-094	对生成代码的控制不恰当（代码注入）	23
CWE-113	HTTP 响应拆分漏洞	
CWE-117	日志伪造	
CWE-129	数组索引验证不当	
CWE-134	格式化字符串漏洞	
CWE-190	整数溢出或超界折返	14
CWE-200	敏感信息暴露	
CWE-209	通过错误消息导致的信息暴露	
CWE-266	不正确的特权分配	

[5] https://github.com/github/codeql/tree/main/java/ql/src/Security/CWE
[6] https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

CWE-273	未能正确检查丢失的特权	
CWE-287	认证机制不恰当	13
CWE-295	证书验证不当	
CWE-297	与主机不匹配的证书验证不当	
CWE-312	敏感信息清晰文本存储	
CWE-319	敏感信息的明文传输	
CWE-326	加密强度不足	
CWE-327	使用已损坏或危险的加密算法	
CWE-330	使用随机值不足	
CWE-335	伪随机数发生器（PRNG）中种子使用不正确	
CWE-338	使用加密弱伪随机数发生器（PRNG）	
CWE-347	加密签名验证不当	
CWE-352	跨站请求伪造（CSRF）	9
CWE-367	时间戳检查与使用时的竞争条件	
CWE-421	在访问备用渠道时的竞争	
CWE-441	意外代理或中介	

续表 2 查询文件表

漏洞编号	漏洞描述	在 2023 CWE TOP 25 最危险漏洞列表中的排名
CWE-470	使用外部控制的输入来选择类或代码（不安全反射）	
CWE-489	Active Debug Code	
CWE-501	信托边界违规	
CWE-502	不可信数据的反序列化	15
CWE-522	保护不足的凭据	
CWE-524	使用包含敏感信息的缓存	
CWE-532	日志文件包含敏感信息	
CWE-601	网址重定向到不受信任的网站（打开重定向）	
CWE-611	对 XML 外部实体引用的不当限制	
CWE-614	HTTPS 会话里的敏感 Cookie 没有 "安全" 属性	
CWE-643	在 X 路径表达式中对数据的不当中和（XPath 注射）	
CWE-676	潜在危险功能	
CWE-681	数字类型的不正确转换	
CWE-730	重放攻击	
CWE-732	关键资源的权限分配不正确	
CWE-749	暴露的危险函数	
CWE-780	使用没有 OAEP 的 RSA 算法	
CWE-798	使用硬编码的凭证	18
CWE-807	在安全决策中依赖不信任的输入	
CWE-829	包含来自不受信任控制领域的功能	
CWE-833	死锁	
CWE-835	循环退出条件不可达	

CWE-917	表达语言陈述中使用的特殊元素的不当中和（表达语言注入）	
CWE-918	服务端请求伪造（SSRF）	
CWE-925	广播接收器意图验证不当	19
CWE-926	Android 应用程序组件的导出不当	
CWE-927	隐式意图在敏感通信中的使用	
CWE-940	通信通道来源的不当验证	
CWE-1104	使用未维护的第三方组件	
CWE-1204	生成弱的初始化向量（IV）	

3.5　执行查询语句

先使用 VS Code 的 CodeQL 插件导入要查询的已经编译完成的数据库，再依次运行表 2 所示的 63 项查询文件对数据库执行查询，并记录查询结果。分别对本实验所选择的三个 Eclipse IIoT 开源软件项目的各个版本共计 24 个 CodeQL 数据库执行查询。

3.6　分析查询结果

对查询的结果进行数据统计分析。针对 3.1 节中提出的三个研究问题，分析各个项目的软件安全漏洞检出情况，研究安全漏洞在具体类型和软件版本上的分布、安全漏洞随软件版本迭代的演化趋势特别是高危安全漏洞的演化趋势。

4　实验结果与分析

4.1　软件安全漏洞分布（RQ1）

Ditto 项目中的软件安全漏洞分布如表 3 所示。在所选的 8 个正式发布版本中，共检测出 8 类安全漏洞，即 CWE-20、CWE-190、CWE-273、CWE-295、CWE-319、CWE-330、CWE-730 和 CWE-798。 前三个版本中检测出除 CWE-330 之外的 7 类安全漏洞，而后 5 个版本中均检测出上述 8 类安全漏洞。除 CWE-190、CWE-319 和 CWE-798 在每个版本中存在 20 个以上实例外，其它 5 类安全漏洞在每个版本中只有 1-2 个实例。

表 3　Ditto 项目中的软件安全漏洞分布

版本	发布日期	CWE-20	CWE-190	CWE-273	CWE-295	CWE-319	CWE-330	CWE-730	CWE-798	**总数**	**类型数**
v2.3.0	2022-01-21	2	32	2	1	25	0	1	23	86	7
v2.4.0	2022-04-14	2	32	2	1	25	0	1	23	86	7

v3.0.0	2022-09-28	2	35	2	1	25	0	1	24	90	7
v3.1.0	2022-12-16	2	33	2	1	25	1	1	24	89	8
v3.2.0	2023-03-08	2	33	2	1	25	1	1	25	90	8
v3.3.0	2023-06-23	2	33	2	1	25	1	1	25	90	8
v3.4.0	2023-10-17	2	33	2	1	25	1	1	25	90	8
v3.5.4	2024-04-08	2	33	2	1	25	1	1	25	90	8

Hono 项目中的软件安全漏洞分布如表 4 所示。在项目的早期检出的安全漏洞总数和类型都较少，如在版本 v1.5.0 中仅检测出 CWE-020、CWE-129、CWE-347 和 CWE-798 等 4 类安全漏洞；在项目中后期，检测出的安全漏洞总数和类型均有增长，从版本 v1.9.0 及以后版本，均检测出 CWE-020、CWE-117、CWE-129、CWE-326、CWE-327、CWE-532 和 CWE-798 等 7 类安全漏洞。另外，CWE-347 仅存在于版本 v1.5.0 中，后续版本中均未检测出该安全漏洞。最后，整体来看，检测出的安全漏洞在不同漏洞类型上分布不均衡，存在明显聚集于特定安全漏洞类型（即 CWE-798）的情况。

表 4　Hono 项目中的软件安全漏洞分布

版本	发布日期	CWE-020	CWE-117	CWE-129	CWE-326	CWE-327	CWE-347	CWE-532	CWE-798	**漏洞总数**	**类型数**
v1.5.0	2020-12-17	8	0	7	0	0	1	0	99	**115**	**4**
v1.7.0	2021-04-07	10	3	7	1	1	0	0	102	**124**	**6**
v1.9.0	2021-07-13	10	3	7	1	1	0	6	107	**135**	**7**
v1.11.0	2022-01-24	10	3	7	1	1	0	6	129	**157**	**7**
v2.1.0	2022-08-30	21	6	7	1	1	0	6	138	**180**	**7**
v2.3.0	2022-11-29	24	6	7	1	1	0	6	142	**187**	**7**
v2.4.0	2023-08-17	26	6	8	1	1	0	6	143	**191**	**7**
v2.5.0	2024-01-18	26	6	8	1	1	0	6	143	**191**	**7**

Kura 项目中的软件安全漏洞分布如表 5 所示。此项目中检测出的安全漏洞的总数和类型数较 Ditto 和 Hono 项目有较大增加，每个版本检测出的安全漏洞实例总数均达到 100 个以上，安全漏洞类型除 v2.0.0 版本外均达到 13 类以上。最后，检测出的安全漏洞在 CWE-020、CWE-117、CWE-532 和 CWE-798 上聚集较为明显。

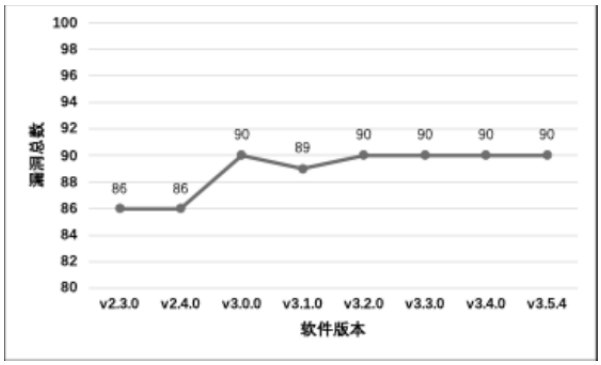
表 5　Kura 项目中的软件安全漏洞分布

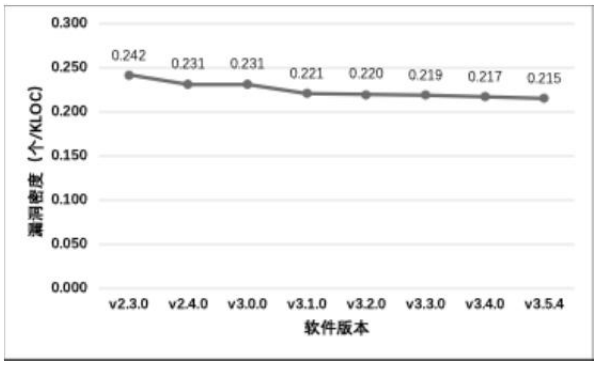
版本	发布日期	CWE-20	CWE-22	CWE-23	CWE-78	CWE-79	CWE-113	CWE-117	CWE-129	CWE-190	CWE-200	CWE-295	CWE-297	CWE-319	CWE-327	CWE-501	CWE-532	CWE-601	CWE-611	CWE-614	CWE-730	CWE-798	CWE-829	CWE-918	CWE-1104	**漏洞总数**	**类型数**
v2.0.0	2016-07-26	0	0	2	0	0	0	0	8	0	5	0	0	2	2	0	79	0	0	0	0	10	0	0	0	**108**	**7**
v4.0.0	2018-10-19	47	3	3	0	1	2	19	12	0	6	0	0	10	1	1	67	0	2	0	0	24	10	0	2	**210**	**16**
v4.1.2	2020-10-30	47	0	3	0	0	2	19	12	0	6	0	0	10	1	1	62	0	0	0	0	23	4	0	2	**192**	**13**
v5.0.0	2021-10-22	78	0	4	1	0	1	16	12	0	6	1	2	12	1	0	74	1	0	1	0	29	4	1	2	**246**	**18**
v5.1.0	2022-03-25	158	0	4	1	0	2	50	12	0	6	1	2	13	1	0	74	1	0	2	0	26	4	1	2	**360**	**18**
v5.2.0	2022-09-13	162	6	4	1	0	2	53	12	0	6	1	2	13	1	0	68	1	0	2	0	27	2	1	2	**366**	**19**
v5.3.0	2023-05-31	179	0	3	1	0	2	55	12	1	6	1	2	11	2	0	69	1	0	2	0	31	0	1	0	**379**	**17**
V5.4.0	2023-11-30	252	2	4	3	0	2	66	12	1	7	1	2	11	2	1	70	1	1	3	1	119	0	1	0	**562**	**21**

综上，尽管在实验中检测了 63 类软件安全漏洞，但每个软件项目中均只检测出少部分类型的安全漏洞；不同项目中检测出的安全漏洞在具体安全漏洞类型上的聚集程度存在明显差异，但 CWE-798 类型的安全漏洞在三个项目中都是高频发生的。

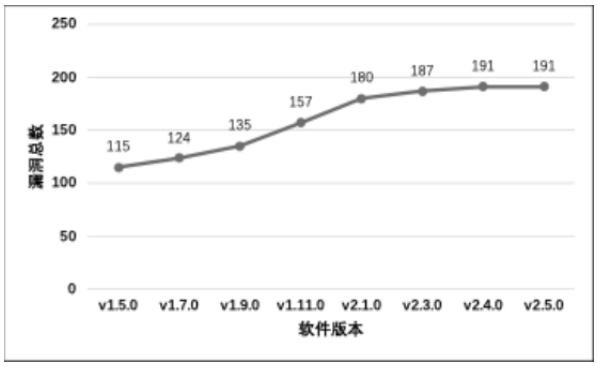
4.2　软件安全漏洞演化趋势（RQ2）

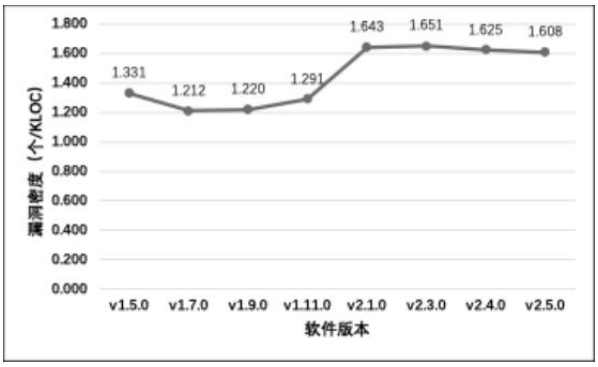
图 1 展示了三个软件项目中被检测出的安全漏洞总数和安全漏洞密度（即平均每千行代码中存在的安全漏洞数）随软件版本迭代更新的演化趋势。从图 1（a）可看出，从 Ditto 项目不同版本中检测出的安全漏洞总数相对稳定，也意味着一方面早期版本中的安全漏洞并没有被妥善的修复，另一方面后续版本也未引入新的安全漏洞。同时，Ditto 的安全漏洞密度在随软件版本迭代而减小，但变化幅度较小（由 0.242 下降到 0.215）。从图 1（b）可观察到从 Hono 不同版本中检测出的安全漏洞数量随版本迭代总体上呈增长趋势，但增长幅度在项目后期放缓，而该项目的安全漏洞密度随软件版本迭代先升后降。从图 1（c）可观察到从 Kura 不同版本中检测出的安全漏洞数量随版本迭代总体上也呈增长趋势，并且绝对数量增长显著；而安全漏洞密度总体上也呈增长趋势，需引起特别的重视。



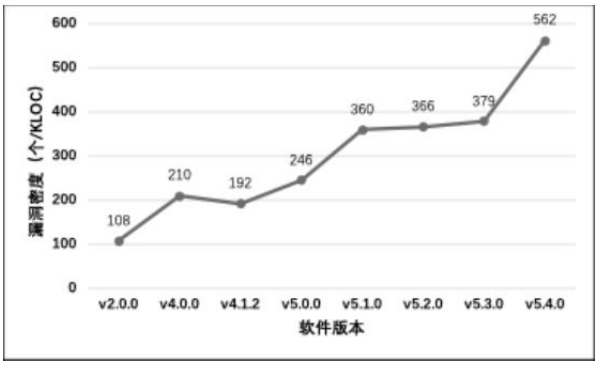


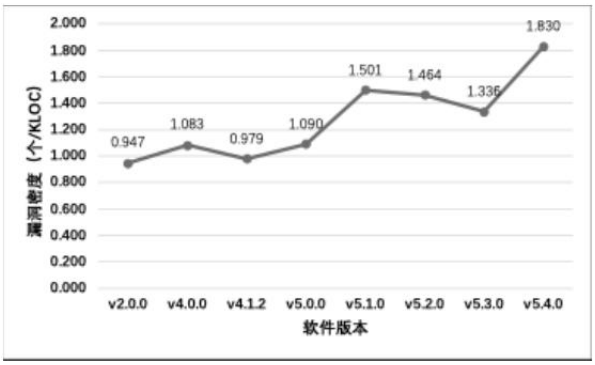
（a）Ditto





（b）Hono





（c）Kura

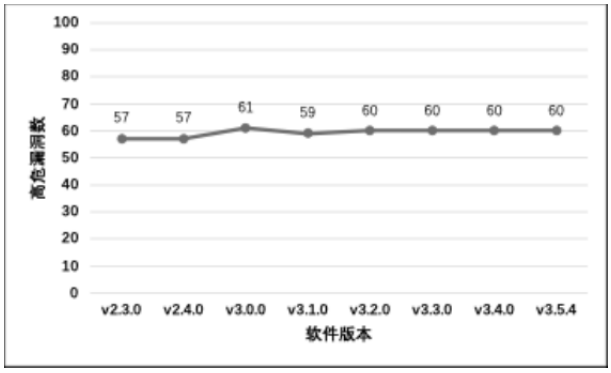
图 1　Ditto、Hono 和 Kura 项目的漏洞总数和漏洞密度演化趋势

综上所述，所选的三个 Eclipse IIoT 开源软件项目的漏洞总数随软件版本迭代更新呈稳定状态或上升趋势，而漏洞密度的变化趋势各不相同，其中 Kura 项目的漏洞密度随版本迭代总体呈显著增长趋势。

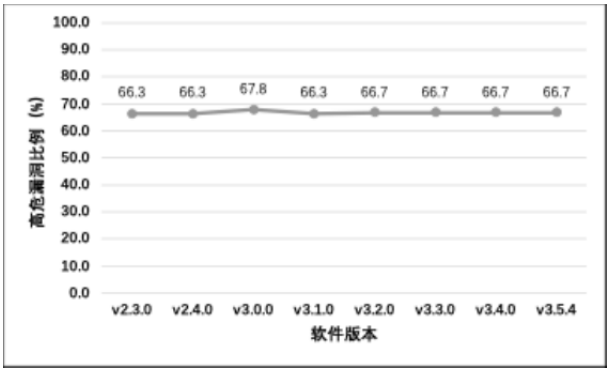
4.3　高危安全漏洞演化趋势（RQ3）

本节特别关注高危漏洞的演化趋势。本文所说的高危漏洞特指位列 2023 年度 CWE 最危险的安全漏洞前 25 名的漏洞，在本文实验中，如表 1 所示，所使用的 63 种漏洞查询包含安全漏洞 CWE-79（第 2）、CWE-89（第 3）、CWE-78（第 5）、CWE-20（第 6）、CWE-22（第 8）、CWE-352（第 9）、CWE-287（第 13）、CWE-190（第 14）、CWE-502（第 15）、CWE-798（第 18）、CWE-918（第 19）和 CWE-94（第 23）共 12 种高危安全漏洞。

图 2 展示了 Ditto 项目中高危安全漏洞数及其在漏洞总数中占比随软件版本迭代更新的演化趋势。从图 2 可知，高危漏洞数呈稳定演化趋势，但高危漏洞占比持续维持在 66%以上的较高水平，需要引起开发团队和用户的重视。



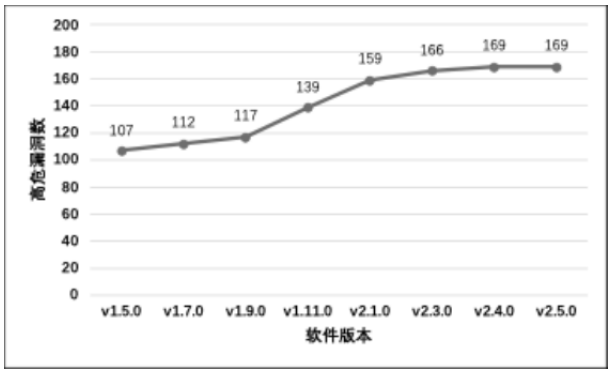
（a）高危漏洞数演化趋势



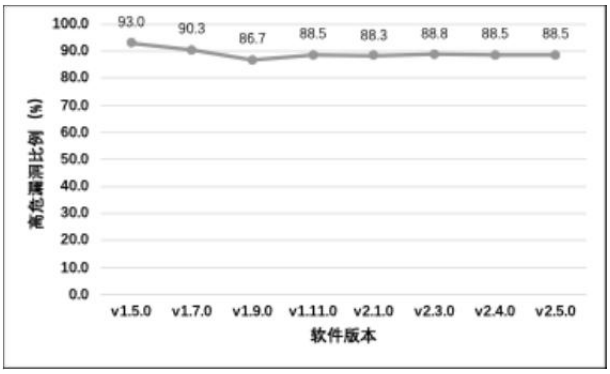
（b）高危漏洞数占比随软件版本演化趋势

图 2　Ditto 项目中高危漏洞数和占比随软件版本演化趋势

图 3 展示了 Hono 项目中高危安全漏洞数及其在漏洞总数中占比随软件版本迭代更新的演化趋势。从图 3 可知，高危漏洞数总体呈上升演化趋势，早期增长较慢，中期增长加快，后期增长缓慢至稳定状态。但高危漏洞比例从项目早期的 93.0%下降至中期的 86.7%，此后回升至 88.5%左右并一直维持在此水平，全程均处于 86%以上的高位。此项目如此高的高危漏洞比例，需要得到项目开发团队足够的重视和投入，以消除高危安全漏洞带来的隐患，同时，用户也要关注到此项目所面临的安全风险。



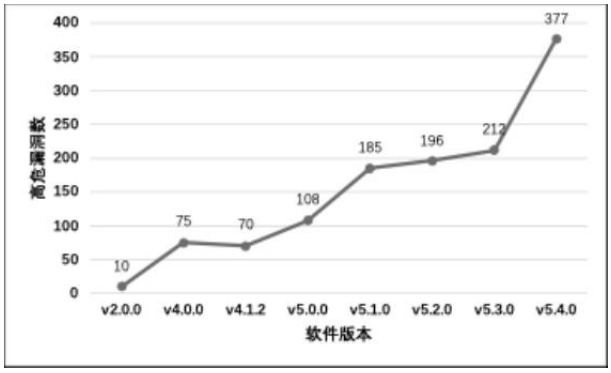
（a）高危漏洞数演化趋势



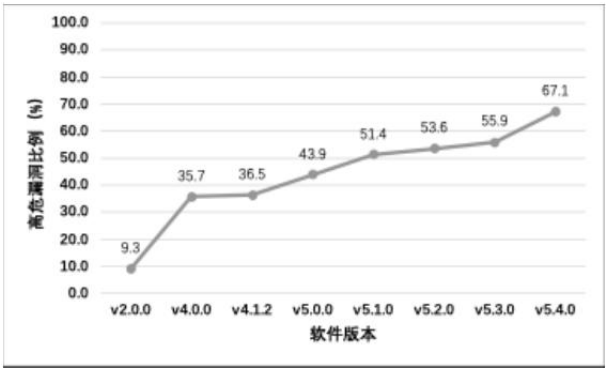
（b）高危漏洞数占比随软件版本演化趋势

图 3　Hono 项目中高危漏洞数和占比随软件版本演化趋势

图 4 展示了 Kura 项目中高危安全漏洞数及其在漏洞总数中占比随软件版本迭代更新的演化趋势。从图 4 可知，高危漏洞数和高危漏洞比例呈明显上升演化趋势，且高危漏洞数量较前两个项目明显偏大，高危漏洞占比从项目早期的 9.3%持续增长至最新版本的 67.1%，可以预见，随着此项目的高危漏洞数量和高危漏洞比例的进一步增长，该项目面临的安全风险将会进一步加剧，迫切需要得到项目开发团队的妥善处理。



（a）高危漏洞数演化趋势



（b）高危漏洞数占比随软件版本演化趋势

图 4　Kura 项目中高危漏洞数和占比随软件版本演化趋势

综上所述，所选的三个 Eclipse IIoT 开源软件的高危漏洞数占漏洞总数的比例都维持在高位，均超过 65%，迫切需要得到开发团队的解决和用户的关注，尽早将软件安全风险降低到合理的范围。

5　结束语

本文研究了 Eclipse 基金会旗下的 Ditto、Hono 和 Kura 三个具有代表性的 IIoT 开源软件项目的软件安全漏洞分布和安全漏洞随软件版本迭代更新的演化情况。基于 CodeQL 的 63 类软件安全漏洞检测实验结果，发现：（1）每个软件项目中均只检测出 63 类软件安全漏洞中的少部分安全漏洞类型，不同项目中检测出的安全漏洞在具体安全漏洞类型上的聚集程度存在明显差异；（2）所选的三个 IIoT 开源软件的漏洞总数随软件版本迭代更新呈稳定状态或上升趋势，漏洞密度演化趋势各有不同；（3）所选的三个 IIoT 开源软件的高危漏洞数占漏洞总数的比例都维持在高位，其中 Ditto 和 Hono 项目高危漏洞占比始终维持在同一水平，而 Kura 项目的高危漏洞占比随版本迭代持续增长。上述发现表明，Eclipse IIoT 开源软件存在不同程度安全风险，其中的高危安全漏洞亟需得到软件开发团队的重视和及时修复，以有效降低 IIoT 开源软件安全风险。

在未来的研究工作中，我们计划评估完整的 Eclipse IIoT 开源软件生态的软件安全风险，以感知整个 Eclipse IIoT 开源软件生态的安全态势，更好地服务于工业互联网产业。此外，我们还将与工业伙伴合作，从更多的维度来对工业伙伴的内部闭源工业互联网软件进行更全面的安全风险评估。

参考文献：

[1] Qin, Weite, et al. Recent advances in Industrial Internet: insights and challenges[J]. Digital Communications and Networks, 2020, 6: 1-13.

[2] Liu Bingchang, et al. Software vulnerability discovery techniques: A survey. In: Proceedings of the 4th International Conference on Multimedia Information Networking and Security. IEEE, 2012: 152-156.

[3] 邢晨.工业数据安全的挑战与应对策略[J].工业控制计机, 2024, 37(04):114-115..

[4] 马娟,于广琛,柯皓仁,等.工业互联网设备的网络安全管理与防护研究[J].中国工程科学,2021,23(02):81-87.

[5] 王鹏,韩俊飞,刘阳.工业控制系统的网络安全高等级环境数据平台[J].信息技术,2021,(05):28-33.

[6] 李杪恬,郭翔宇,宁黄江,等.区块链技术在工业互联网中的应用及网络安全风险分析[J].工业技术创新,2021,08(02):37-42.

[7] Majdinasab, Vahid, et al. Assessing the Security of GitHub Copilot's Generated Code - A Targeted Replication Study[C]//2024 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). 2023: 435-444.

[8] Pearce, Hammond A., et al. Asleep at the Keyboard? Assessing the Security of GitHub Copilot’s Code Contributions[C]//2022 IEEE Symposium on Security and Privacy (SP). 2021: 754-768.

[9] Singh, Anish Kumar, et al. An Image Security Model Based on Chaos and DNA Cryptography for IIoT Images[J]. IEEE Transactions on Industrial Informatics, 2023, 19(3): 1957-1964.

[10] 马佳利, 郭渊博, 方晨, 等. 基于数字孪生的工业互联网安全检测与响应研究[J]. 通信学报, 2024, 45(6): 87-100.

[11] 李欣, 刘秀, 万欣欣. 数字孪生应用及安全发展综述[J]. 系统仿真学报, 2019, 31(3): 385.

[12] Hamer, Sivana, et al. Just another copy and paste? Comparing the security vulnerabilities of ChatGPT generated code and StackOverflow answers[C]//2024 IEEE Security and Privacy Workshops (SPW). 2024: 87-94.

[13] Szabó, Tamás. Incrementalizing Production CodeQL Analyses[C]//Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2023: 1716-1726.

[14] Lazarine, Ben, et al. Exploring the Propagation of Vulnerabilities from GitHub Repositories Hosted by Major Technology Organizations[C]//Proceedings of the 15th Workshop on Cyber Security Experimentation and Test. 2022: 145-150.

[15] Lin, Guanjun, et al. Software Vulnerability Detection Using Deep Neural Networks: A Survey[J]. Proceedings of the IEEE, 2020, 108(10): 1825-1848.

[16] Chen, Sen, et al. AUSERA: Automated Security Vulnerability Detection for Android Apps[C]//Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering. 2022: Article 154.

[17] Grieco, Gustavo, et al. Toward Large-Scale Vulnerability Discovery Using Machine Learning[C] //Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. 2016: 85-96.

[18] Selvarajan, Shitharth, et al. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems[J]. Journal of Cloud Computing, 2023, 12: Article 38.

[19] Zhou, Zhou, et al. Blockchain-Enabled Secure and Trusted Federated Data Sharing in IIoT[J]. IEEE Transactions on Industrial Informatics, 2023, 19(6): 6669-6681.

[作者简介]

李增扬，（1982 年—），男，博士，副教授，主要研究方向为软件工程和软件安全。

黄彬彬，（2001 年—），男，学士，硕士在读，主要研究方向为软件安全。

刘　慧，（1983 年—），女，博士，副教授，主要研究方向为复杂网络优化与控制、网络安全。

吕金虎，（1974 年—），男，博士，教授，主要研究方向为工业互联网、网络控制。

吴晓群，（1978 年—），女，博士，教授，主要研究方向为复杂网络控制、工业互联网。

适应工业互联网的低延迟分组密码研究综述*

杨金玲，齐连硕，谢勇，李澄清

湘潭大学计算机学院，湖南 湘潭 411105
通讯作者: 李澄清，E-mail: chengqing@xtu.edu.cn

摘 要: 随着工业互联网的快速发展，确保数据安全和实时性成为了关键需求。传统的加密技术虽然能够提供高安全性，但往往以牺牲性能和响应时间为代价。因此，适应工业互联网需求的低延迟分组密码技术应运而生。本文分析了工业互联网对加密技术的特殊要求，包括低延迟、轻量化、高安全性和良好的硬件兼容性，探讨几种典型的低延迟分组密码算法如何实现数据的即时加密和快速解密。它们在设计上都考虑了在计算效率和资源消耗方面适用于资源受限的工业环境。然而，实际应用中还需考虑低延迟分组密码安全性存在的问题。本文重点聚焦于低延迟分组密码及组件的设计与分析，深入探讨其在资源受限、安全性等多方面的挑战，并对近年来关于低延迟分组密码及应用的相关工作进行了系统梳理。在此基础上，本文总结了将低延迟分组密码技术应用于工业互联网中的技术挑战，如算法的安全性验证、跨平台兼容性和标准化进程，并对未来的研究方向提出了展望，包括算法优化、硬件实现上的改进以及与工业应用更深层次的融合。

关键词: 工业互联网；低延迟分组密码；数据安全；实时性；轻量化

Review of the low-latency block ciphers research for industrial Internet

Yang Jin-Ling, Qi Lian-Shuo, Li Chengqing, Xie Yong

School of Computer Science, Xiangtan University, Xiangtan 411105, Hunan, China

Abstract: With the rapid development of the industrial Internet, data security and real-time performance have become key requirements. Although the traditional encryption technology can provide high security, it often comes at the expense of performance and response time. Therefore, low-latency block ciphers that meet the needs of the industrial Internet come into being. This paper analyzes the special requirements of industrial Internet encryption technology, including low latency, lightweight, high security and good hardware compatibility, and explores how to implement real-time encryption and fast decryption of data with several typical low-latency block ciphers, which are designed with computing efficiency and resource consumption in mind, and are suitable for resource-constrained industrial environments. However, in practical applications, the security issues of low-latency block ciphers still need to be considered. This paper focuses on the design and analysis of low-latency block ciphers and components, deeply explores the challenges in resource constraints and security, and systematically sorts out the low-latency block ciphers and their applications proposed by international scholars in recent years. This paper summarizes the existing challenges in the application of low-latency block ciphers in the industrial Internet, such as algorithm security verification, cross-platform compatibility and standardization process. Moreover, it provides an outlook of the research topics that deserve further investigation, including algorithm optimization, improvement in hardware implementation, and deeper integration with industrial applications.

Key words: Industrial Internet; Low-latency block cipher; Data security; Real-time; Lightweight.

* 基金项目: NSFC (no. 92267102); Hunan Provincial Natural Science Foundation of China (2024JJ7542).

引言

随着云计算、物联网等新技术的广泛应用，黑客对供应链、工业互联网平台、工业控制系统等的攻击持续不断，工业互联网的安全保障将面临全新挑战。工业互联网涉及大量生产设备之间数据传输，其数据具有来源广泛、种类多样、产生速率快、数据量大、更具价值属性和产权属性等特点，且安全级联效应明显。若发生数据泄露，除影响正常的生产运营外，极有可能损害国家安全、国计民生和人民生命健康。数据加密技术需考虑工业互联网场景下数据实时性、稳定性、可靠性等特殊要求，轻量级对称密码受到广泛的关注。大多数轻量级密码被优化的主要度量是芯片面积，通常用等效门(Equivalent Gate, GE)测量，即密码面积归一化到给定标准单元库中2输入NAND门的面积。这是一个有效的优化目标，特别是对有非常严格的功率或成本限制的设备。密码除了具有轻量级特性，根据应用程序的不同，还需满足其他实现参数。对称密码能够即时加密给定的明文，即整个加密和解密应该在可能最短的延迟内进行。然而，传统密码的软件实现需要数百或数千个时钟周期，不适合针对低延迟加密的设计者。工业互联网中一些重要的应用程序非常需要低延迟的加密和即时响应时间，例如即时身份验证或对内存设备基于分组的读/写访问。也有一些嵌入式应用程序，其中多时钟架构中当前分组密码可以足够快，但系统不支持所需的高时钟速率。例如，在许多现场可编程门阵列(Field Programmable Gate Array, FPGA)设计中，超过200 MHz的时钟速率往往难以实现。在硬件中实现流密码时，初始化阶段需要大量时钟周期，特别是当需要定期更改密钥时。此外，如果想加密随机选择的分组，那么流密码就不适合了。因此，低延迟分组密码成为近年来密码学界研究的热点方向。

传统的分组密码国际标准AES[1]、国内标准SM4算法实现规模相对较大。就AES而言，基于轮的架构使得低延迟实现成为一项具有挑战的任务。AES-128的一个基于轮的硬件架构需要10个时钟来输出一个密文，对于某些应用程序来说仍然太长了。若将这十轮循环展开，即实现单轮重复十次的电路，密码在一个时钟周期内返回一个密文，则代价是一条很长的关键路径，产生了非常缓慢的绝对响应时间和时钟频率。此外，展开的架构具有数万GE，意味着高功耗和高成本。这两个特性都是不可取的，特别是当考虑到许多瞬时密码的应用程序都位于嵌入式领域时。目前，国内外提出不少轻量级分组密码算法，这些密码算法大都基于SPN结构和Feistel结构两种主要应用结构。SPN结构是使用比较广泛的轻量级分组密码结构，充分体现了Shannon[2]提出的设计密码体制的两种基本方法:扩散(diffusion)和混淆(confusion)。在迭代轮函数运算过程中，SPN结构的扩散和混淆使得整个明文空间得到充分变换，低延迟分组密码大都采用该结构。一些基于SPN结构的密码，采用类AES密码结构，即类似AES密码的组件或者运算过程。AES密码算法自被提出以来，经过不断的考验仍然是安全的，可见AES算法的结构及轮函数是非常优秀的。龚征等人[3]在RFID SEC 2011会议上提出了KLEIN轻量级分组密码，采用AES密码的列混淆矩阵，将经过S盒变换的输出数据进行充分扩散。郭建等人[4]在CHES 2011会议上提出了LED轻量级分组密码，采用AES密码的轮函数运算流程:轮密钥加、S盒替换、行移位及列混淆。另一些基于SPN结构的密码在结构与组件上与AES不同。例如，Bogdanov等人[5]在CHES 2007会议上提出PRESENT，该密码收录在ISO-29192标准。其S盒具有良好的密码特性，线性扩散组件只有一个P置换。 PriPresen[6]、LED、QTL[7]及PHOTON[8]多个算法采用该S盒。Subhadeep等人[9]在CHES 2017会议上提出GIFT加密算法，改进了PRESENT密码P置换存在线性扩散不均的问题。Albrecht等人[10]在EUROCRYPT 2015会议上提出LowMC加密算法，使用3-bit S盒，仅涉及深度为1的3个AND逻辑门，可应用于安全多方计算和同态加密。

Feistel结构也是用于轻量级分组密码中一种重要的对称结构。Feistel结构优点是加解密运算过程一致，对于任何轮函数都是可逆的，解密时逆序使用轮密钥即可，减少了几乎一半成本。但存在

一轮只能混淆扩散一半明文状态的局限性，通常需要迭代更多的轮数。因此，Feistel结构并不适合用于低延迟的实现。为了保留加解密的一致性，同时又改善Feistel结构的局限性，研究者们陆续提出Feistel结构变体，广义Feistel结构(Generalized Feistel Networks, GFN)就是Feistel结构的一种推广。Feistel密码结构根据分支2N(N≥1)进行简单归类：当N=1时，它为一般Feistel结构；当N>1且N为整数时，它为GFN结构。即将明文状态划分为N个子块，从而降低轮函数的规模。吴文玲与张蕾[11]在ACNS 2011会议上提出了LBlock加密算法，该算法设计为类DES[12]密码结构，在每一轮中只有一半数据通过轮函数F，另一半应用一个简单的移位操作。美国国家标准技术研究所(National Institute of Standards and Technology, NIST)分别提出面向硬件平台实现的SIMON和面向软件平台实现的SPECK密码算法[13]。这类密码组合使用模加(Addition)、循环移位(Rotation)、异或(XOR)等操作来实现分组密码的混淆和扩散，因此也被称之为ARX型密码。首次将ARX操作与轻量级分组密码结合是Hong等人[14]在CHES 2006会议上提出的HIGHT密码。GFN结构形式多样，包括I-型GFN、II-型GFN等，如Suzaki等人[15]在EUROCRYPT 2011会议上提出的TWINE加密算法就是使用的一种II-型GFN结构，该算法中N=8，分为16个分支，每个分支是4-bit。索尼公司Shirai等[16]在FSE 2007会议上提出CLEFIA加密算法，也被收录在ISO-29192标准。该算法中N=2，分为4个分支，每个分支为32-bit。Shibutani等人[17]在CHES 2011会议上提出Piccolo加密算法，该算法中N=2，分为4个分支，每个分支是16-bit。II-型GFN结构每轮只有一个F函数，而II-型GFN结构每轮使用N/2个F函数，相比之下改善了扩散效果，但也不可避免的增加了硬件开销。进一步，Berger等人[18]提出一种具有良好全扩散延迟和低成本的扩展GFN (Extended Generalized Feistel Networks, EGFN) 结构作为GFN结构一种可能的推广，并介绍了基于II-型EGFN结构的LILLIPUT轻量级分组密码。随后， Cheng等人[19]提出基于I-型EGFN结构的ALLPC轻量级分组密码。

低延迟分组密码满足分组密码基本特性，并根据不同应用场景对延迟进行优化而设计。由于缺乏对工业互联网平台具体的应用环境进行分类研究，对于贴合实际工艺和用户实际安全需求方面仍相对薄弱。因此，需要对资源受限的工业互联网设备进行更多深入而明确的研究，给出不同设备对应的低延迟分组密码设计方案。然而，已有的分组密码综述也各有侧重。文献[20] [21] [22] [23]对适用于资源受限环境的轻量级分组密码进行了综合性的总结，但缺乏对低延迟分组密码研究的深入探讨。本文系统梳理了低延迟分组密码的研究进展，包括结构、性能等的全面总结。图1展示了低延迟分组密码在工业互联网场景下的应用。

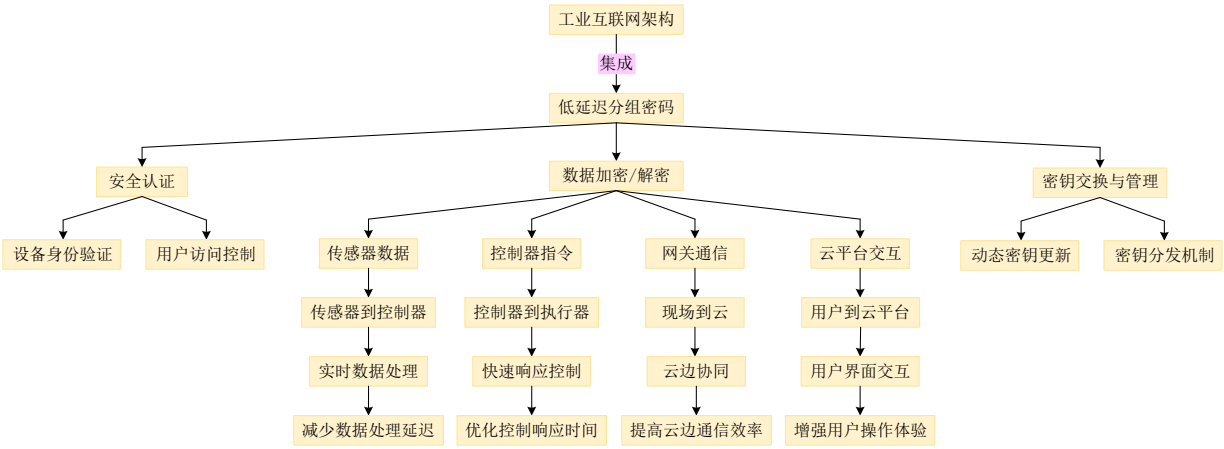


图 1 工业互联网场景下的低延迟分组密码应用

本文其他章节的内容安排如下，第二章对目前已有的低延迟分组密码进行了详细阐述与分析，包括基本原理、应用场景等。第三章介绍 S 盒、矩阵等低延迟密码部件。第四章为密码的硬件性能分析。第五章对全文进行总结，并对前沿技术进行展望。

低延迟分组密码概述

在响应工业互联网环境对数据处理的需求时，特别是在轻量级密码学中，低延迟特性变得越来越重要。近年来，针对实时安全性的需要，低延迟分组密码被相继提出。研究者们根据延迟对密码进行优化，使得整个加密和解密在最短的延迟内完成。在这一领域的第一个工作是Knežević等人[39]比较了多个（轻量级）分组密码的延迟特性。紧接着，Borghoff等人[24]在AsiaCrypt2012会议上提出第一个低延迟分组密码PRINCE，其分组长度为64-bit，密钥长度为128-bit，总体设计基于FX结构[25][26]。核心部分PRINCEcore包含12轮加密过程，轮函数基本遵循AES结构，主要区别是围绕中间的一个对合线性层对称。这种特殊的构造加上精心选择的轮常数使PRINCEcore满足α反射属性，意味着使用密钥K解密对应于使用密钥K⊕α进行加密，其中α是一个固定常数。使得在硬件实现中，解密的开销相对于加密可以忽略不计。这是低延迟设计的主要特性，并且对于完全展开实现至关重要，在电路开始时只需要多路复用器一次，允许在单个时钟周期内完成数据的加密。这种设计减少了所需的芯片面积，同时保持了与传统解决方案相比更有竞争力的性能，但其S盒的选择和实现可能依赖于特定的技术环境。也存在一些安全问题，如易遭受利用中间轮存在的固定点构造全轮PRINCEcore的反射攻击[27]。作为第一个低延迟加密方案，PRINCE已经部署在许多产品中，包括NXP半导体的LPC55。PRINCE在数据读取或写入闪存时操作，而无需先将数据存储在RAM中，再加密或解密到另一个内存空间。此功能对于资产保护非常有用，例如加密应用程序代码、加密数据和启用安全闪存更新。

密码的延迟与轮数直接相关，找到一个轮函数与可调(Tweak)算法的设计以确保最少轮数的安全性是至关重要的。受PRINCE设计的启发， Beierle等人[28]提出一种低延迟可调分组密码MANTIS，是专门为低延迟实现而设计的SKINNY变体，适用于内存加密。其分组长度为64-bit，密钥长度为128-bit，Tweak长度为64-bit。该密码基本上采用了相同的PRINCE结构，简单地用Midori[29]的轮函数替换PRINCE轮函数，同时使整个设计在中间对称，以保持α反射特性。在硬件实现方面，MANTIS的面积和延迟与PRINCE相当，但提供了额外的可调性。并在相关可调模型下，通过混合整数线性规划(Mixed Integer Linear Programming, MILP)方法证明了抵抗差分攻击和线性攻击的能力，也指出了在相关密钥模型下可能存在的安全风险。安全性存在的问题包括利用多条差分特征提高差分概率构造全轮$MANTIS_5$的差分攻击[30]。

2017年，高通公司提出低延迟可调分组密码QARMA[31]，主要是为了部署在完全展开或流水线的硬件实现中针对内存加密、生成短标签以防止软件漏洞利用等应用。其分组长度为64-bit和128-bit两个版本，密钥长度是分组长度的两倍，Tweak长度与分组长度相等。与FX结构不同，QARMA采用3轮Even-Mansour方案提供近似反射性质。第一和第三个置换在功能上互为倒数，中心置换被设计成容易通过简单的密钥转换来倒置，其轮函数为SP型结构，并提出了使用通用散列函数扩展Tweak长度的技术。QARMA用于ARMv8.3产品中部署的指针身份验证。ARMv8.3是ARM架构的一个扩展，旨在提供硬件级的指针认证和内存加密功能，以防御控制流完整性(Control Flow Integrity, CFI)攻击，如返回导向编程(Return Oriented Programming，ROP)和跳转导向编程(Jump Oriented Programming，JOP)等漏洞利用技术。QARMA用于生成认证标签。这些标签被嵌入到指针的未使用位中。当指针被使用，如函数返回地址，硬件会验证该标签以确保指针的合法性。

2020年，Bozilov等人[32]改进了PRINCE的设计，并提出PRINCEv2的版本，旨在提供更高的安全性而不显著增加计算复杂性。主要的区别是改变密钥编排算法和在中间轮增加了一个XOR操作。缺点是α反射特性略有减弱，意味着解密不再是简单的使用修改后的密钥进行加密，而是需要更多的计算。 PRINCEv2在不显著增加延迟、面积、功耗或能量消耗的情况下，提高安全性，符合NIST

要求的更高安全级别。由于设计与PRINCE高度相似， PRINCEv2可以轻易地部署在已经使用PRINCE的系统中，提供向后兼容性。尤其适合对实时操作和低延迟执行有高要求的场合。尽管PRINCEv2对通用攻击的抵抗力更强，但在某些特定攻击下，如相关密钥攻击，其安全性可能会降低。

Orshros是由Banik等人[33]在FSE 2021会议上提出的一个低延迟伪随机函数(Pseudorandom Function， PRF)，专为完全展开电路的延迟而设计，旨在为需要快速响应的应用提供加密服务，例如内存总线加密、存储系统、工业控制网络等。其分组长度为64-bit，密钥长度为128-bit，整体结构由两个基于SPN的分支组成。其设计考虑到了非可逆PRF的需求。由于它不支持解密，不需要使用对合的组件。因此不适用于需要解密功能的应用场景，如CBC和XTS。而适用于不需要解密例程的多种加密模式，如CTR、CMAC和GCM。

Leander等人[34]在CHES 2021会议上提出SPEEDY密码族，以单周期加密速度实现超低延迟，而解密效率较低。为了使之适应硬件中的最大执行速度，设计者首先分析了哪种类型的逻辑门和电路拓扑结构特别适合于超低延迟加密，考虑足够的电路拓扑来最小化组合电路的延迟。将工程专业知识混合到密码设计过程的每一步中，以便在CMOS硬件中创建一个具有极低延迟的安全加密算法。逻辑门的物理实例需要通过更新其输出信号来响应其输入信号变化的时间称为延迟。考虑到CMOS硬件，逻辑单元的物理实例的延迟取决于许多因素。除了温度和电源电压等环境的影响外，输入信号的转换时间和在其输出时需要驱动的电容也起着重要的作用。当所有外部因素都相等时，可以比较静态CMOS门的基本延迟。 SPEEDY主要针对嵌入在高端CPU中的安全架构，如安全缓存、专用硬件扩展、内存加密、指针身份验证等。高端CPU对面积和能量没有限制，高性能是首要考虑，设计者选择忽略硬件开销的增加。在后续的工作中该算法被认为存在差分类攻击的安全性问题，如Boura等人[35]对SPEEDY-7-192的全轮密钥恢复攻击，基于5。5 轮差分特征设计精巧复杂的密钥恢复步骤。

上述低延迟分组密码基本都采用类似的结构，而低延迟分组密码的轮数应尽可能少，以减少延迟。这在安全方面带来了更多的风险。 Zhang等人[36]在Inscrypt 2022会议上提出低延迟轻量级分组密码LLLWBC，它不再使用其他低延迟密码通常使用的SP型结构，而是采用EGFN结构。其分组长度为64-bit，密钥长度为128-bit，将明文状态划分为8个分支，使用基于字节的轮函数和基于半字节的轮置换，共经过21轮迭代。并通过精心选择轮置换和密钥编排以保留重要的α反射特性，使得在硬件上有效地完全展开实现，而解密开销可以忽略不计。论文中明确指出没有在相关密钥、已知密钥和选择密钥模型下提出安全声明，这可能限制了其在某些高安全需求场景下的应用。

随着针对CPU微架构的攻击增多，特别是基于缓存的侧信道攻击，随机化缓存架构被提出以增加攻击复杂性。低延迟是高速缓存随机化函数的一个关键要求，缓存用于各种CPU，从小型嵌入式设备到高端服务器集群。通过随机化地址到缓存索引的映射，攻击者无法轻易构造最小的逐出集合，这对于基于竞争的缓存攻击至关重要。Canale等人[37]在Inscrypt 2022会议上提出SCARF密码，是为安全缓存随机化设计的专用低延迟分组密码。该密码采用一种结合了SPN和Feistel结构优点的改进的MISTY结构。设计了一个低延迟的G函数，它不需要是双射的，主要目的是导致较高的密钥依赖性，即以最小的延迟吸收许多子密钥。 SCARF的设计为可逆的。随机化还依赖于密钥，这样攻击者就不知道映射，因此设计者将SCARF设计为一个可调分组密码。其分组长度为10-bit，密钥长度为240-bit， Tweak长度为48-bit。 240-bit密钥是在引导时间使用大多数CPU上存在的TRNG随机生成的。 SCARF的延迟时间还不到PRINCE、MANTIS和QARMA的一半，在硬件实现和系统性能方面展现出显著的优势，但主要针对特定的应用场景和攻击模型。

最近，名为加密能力计算(Cryptographic Capability Computing, C^3)的内存安全概念被提出。C^3是第一个不需要额外的元数据存储的内存安全机制，依赖于超低延迟的加密算法，且要求小尺寸分组。Belkheyar等人[38]在CHES 2023会议上提出低延迟可调分组密码BipBip以解决持久的内存安全问题。其分组长度为24-bit，密钥长度为256-bit， Tweak长度为40-bit。对于当前的64位计算机系统，C^3对其中一部分进行加密，并使用所有其他部分进行加密。更具体地说，它对64-bit指针中的24-bit进行加密，其余40-bit被用作Tweak。与SCARF的设计目标相反，BipBip专注于解密延迟，以适应C^3的环境要求。BipBip在专用集成电路(Application Specific Integrated Circuit, ASIC)上的实现表明BipBip在硬件上具有高效率和低功耗。并针对差分攻击、线性攻击、不可能差分攻击、积分攻击和中间相遇攻击等多种攻击进行了安全性分析，显示出对多种攻击的抵抗力。但可能需要更多的研究来探索其在更广泛场景下的应用潜力。表1总结了低延迟分组密码基本情况，包括是否关注统一的加解密电路中的硬件开销。

表 1 低延迟分组密码对照表

密码	结构	分组长度 (bits)	密钥长度 (bits)	Tweak长度 (bits)	关注模式	关注硬件开销	年份
PRINCE[24]	SPN	64	128	–	加密+解密	√	2012
MANTIS[28]	SPN	64	128	64	加密+解密	√	2016
QARMA[31]	SPN	64/128	128/256	64/128	加密+解密	√	2017
Orshros[33]	SPN	128	128	–	加密	√	2021
SPEEDY[34]	SPN	192	192	–	加密	×	2021
LLLWBC[36]	EGFN	64	128	–	加密+解密	√	2022
SCARF[37]	MISTY	10	240	48	加密	√	2022
BipBip[38]	SPN	24	256	40	解密	√	2023

*注：符号“—”代表不涉及 tweak 算法，“√”代表“关注”，“×”代表“不关注”

低延迟密码组件研究

低延迟与能耗密切相关，这是许多应用中的另一个关键标准[39][40]。在能耗方面进行优化的密码具有广泛的应用，特别是在紧张的功率/能量预算下运行的受限环境中。 Subhadeep等人在ASIACRYPT 2015会议上提出低能耗轻量级分组密码Midori，根据加密或解密操作中每bit电路所消耗的能量进行优化。功率(Power)和能量(energy)是相关的参数，能量本质上是功率的时间积分，功率等于单位时间内所消耗的能量。因此，能耗是电压源在执行过程中所做的总工作的度量。在许多方面，能耗可能是衡量设计效率的一个更相关的参数。密码的串行架构比基于轮的架构具有更小的功耗占用，但串行实现通常具有很高的延迟。也就是说，其加密需要更长的时间，可能会消耗更多的能量。因此，并不能保证低功耗架构必然会导致低能耗架构，反之亦然。 Midori有两种分组长度，分别为64-bit和128-bit，密钥长度均为128-bit。该加密算法也是一个典型的类AES密码，有着AES密码轮函数运算流程以及基于半字节的行移位，轮函数由专门为小面积和低电路深度优化的对合S盒组成，以改进延迟和安全性。 SFN[41]算法也采用该S盒。设计者观察到路径延迟与计算的依赖性高度相关，并引入一个度量深度来估计S盒的路径延迟——深度定义为基本运算AND、OR、NAND、NOR和NOT的顺序路径延迟之和。为了找到Midori S盒，按照增加深度的顺序进行检查，这种方法可能速度慢， QARMA设计者采用稍微不那么精确的启发式方法搜索低延迟S盒。

低延迟分组密码大都使用低延迟S盒、矩阵等组件。如4-bit S盒比8-bit S盒延迟低，几乎MDS矩

阵比MDS矩阵延迟低。 SPEEDY密码中提出极致低延迟6-bit S盒，并给出与其他低延迟S盒的比较。 BipBip同样采用低延迟6-bit S盒，在延迟和安全性之间提供了很好的权衡。还有一些工作只关注某些特定组件函数的延迟。在硬件实现中，布尔函数的延迟是一个重要的考量因素。尤其是当输入数量较大时，找到具有最小延迟的布尔函数实现是一个挑战。有关确定函数电路复杂性的工作，Stoffelen等人[42]提出一种基于SAT求解器的技术，根据不同的标准优化一些S盒的实现。虽然这种技术为实现小S盒提供了一种解决方案，但当S盒的输入大于5时无法找到复杂性。 Bilgin等人[43]提出构建具有低延迟掩码变体S盒的技术，应用于侧信道对策，要求低深度和门复杂度。然而，这通常与低延迟对称密码的开发没有直接关系。因为需求不同，有时甚至是相反的。在常规的密码S盒中，非线性门比线性门更有利于面积和延迟，而在掩码S盒中，线性操作是最优的，非线性门是主要的成本因素。随后， Rasoolzadeh[44]在FSE 2021会议上提出一种构建具有低延迟复杂度的双射S盒的算法，寻找所有具有低延迟复杂度的布尔函数，确定布尔函数的延迟复杂度，以及为给定布尔函数找到具有最小延迟复杂度的电路。并提出了一个新的度量标准——延迟复杂度，用于衡量布尔函数的延迟，研究在{NAND， NOR， INV}基础上向量布尔函数的门延迟复杂度。还讨论了布尔函数的线性等价、仿射等价以及扩展的比特置换等价性[45][46][47]。 IoVCipher[48]密码中也构造了两个低延迟的S盒，一个对合另一个非对合。并考虑到解密延迟，设计了一种低延迟的子密钥生成方法。LTLBC[49]密码通过门级自底向上电路搜索构建一个轻量级低延迟的4×4 S盒。

为实现低成本低延迟的MDS矩阵， Li等人[50]在基于SLP启发式算法中引入了电路深度感知能力，同时通过搜索大量矩阵，构建了分支数为5的32×32对合MDS矩阵。在FSE 2020会议上， Li等人[51]在理论上确定了轻量级迭代MDS矩阵，并且在延迟方面也达到了下界。 在文献[52]中，提出了一个对给定的低延迟实现进行局部重新优化的框架。随后，Shi等人[53]讨论了寻找线性层的低延迟实现，提出两种改进的BP算法，通过最小化新距离向量的欧几里得范数来改进搜索启发式方法。并提出一个新的框架，结合前向搜索和后向搜索，扩展了实现的搜索空间。

在硬件中，布尔掩码的有效实现以保护密码算法免受侧信道攻击(Side Channel Analysis, SCA)也很重要。文献[54]提出了一种基于PRINCE的低延迟阈值实现(Threshold Implementation, TI)架构。文献[55]讨论了低延迟密码学实现的挑战，特别是将掩码方案集成到设计中。还有一些工作是对二阶掩码实现的讨论[56] [57]。

硬件性能评估

低延迟分组密码主要关注完全展开的硬件实现性能，即包括所有的函数以及密钥编排数据路径是一个包含寄存器的单独组合电路，只存储明文 P、初始密钥 K、可调参数 T 和加密结果（即密文）C。这些寄存器用于定义逻辑合成中的时间约束和评估关键路径延迟/最大操作频率。实验使用 Xilinx ISE 14。7 进行仿真，并使用 Synopsys Design Compiler (DC)逻辑综合工具进行合成。表 2 为低延迟分组密码在 Nangate 45 nm 工艺库下的硬件资源比较，包括不同密码完全展开实现仅加密电路的最小延迟、合成最小延迟时加密电路的面积消耗以及在 100 KHz 和最大频率下的吞吐量。由于门的计数和延迟参数严重依赖于工艺库技术，对密码的性能进行比较是困难的。表 3 列出了在加密和解密电路中低延迟密码的性能结果。

表 2 低延迟分组密码完全展开实现的硬件资源比较

密码	延迟(ns)	面积(GEs)	吞吐量 @100KHz(KBit/s)	吞吐量 @最大值(MBit/s)	文献
Gimli E-M	4.54	52039	38400.00	84582	[34]
$MANTIS_6$	4.48	12661	6400.00	14286	[34]
$MANTIS_7$	5.07	14226	6400.00	12623	[34]
$MANTIS_8$	5.74	15663	6400.00	11150	[34]
Midori	4.93	10675	6400.00	12956	[34]
Orthros	3.77	31317	12800.00	33863	[34]
PRINCE	4.06	9873	6400.00	15764	[34]
PRINCEv2	4.08	10332	6400.00	15687	[34]
$QARMA_5$-64-σ_0	4.01	11825	6400.00	15921	[34]
$QARMA_6$-64-σ_0	4.55	14166	6400.00	14066	[34]
$QARMA_7$-64-σ_0	5.34	15769	6400.00	11985	[34]
$QARMA_8$-64-σ_0	5.97	17908	6400.00	10720	[34]
$QARMA_5$-64-σ_1	4.37	12350	6400.00	14646	[34]
$QARMA_6$-64-σ_1	4.94	15066	6400.00	12955	[34]
$QARMA_7$-64-σ_1	5.80	16641	6400.00	11034	[34]
$QARMA_8$-64-σ_1	6.50	18964	6400.00	9846	[34]
SPEEDY-5-192	3.19	27903	–	–	[34]
SPEEDY-6-192	3.85	34085	–	–	[34]
SPEEDY-7-192	4.52	39853	–	–	[34]
SPEEDY-5-192*	2.82	29839	–	–	[34]
SPEEDY-6-192*	3.38	36523	–	–	[34]
SPEEDY-7-192*	4.00	42813	–	–	[34]
SCARF	2.26	7，335	1000.00	4425	[37]
LLLWBC	8.20	17093	6400.00	7805	[48]
IoVCipher	4.07	8868	6400.00	15725	[48]

*: 表示使用直接实例化库单元的优化 HDL 代码

表 3 低延迟分组密码完全展开实现的性能结果比较

密码	延迟(ns)	面积(GEs)	工艺库	文献
LLLWBC	11.76	8227	NanGate 45 nm Generic	[36]
PRINCE	-	8263	NanGate 45 nm Generic	[24]
$MANTIS_5$	15.95	8544	UMC L180 0.18 μm 1P6M	[28]
$MANTIS_6$	17.60	9861	UMC L180 0.18 μm 1P6M	[28]
$MANTIS_7$	20.50	11209	UMC L180 0.18 μm 1P6M	[28]
$MANTIS_8$	21.34	12533	UMC L180 0.18 μm 1P6M	[28]
$QARMA_5$-64-σ_0	4.52	13395	FinFet 7 nm	[31]
$QARMA_6$-64-σ_0	5.28	14984	FinFet 7 nm	[31]
$QARMA_7$-64-σ_0	6.04	17109	FinFet 7 nm	[31]
$QARMA_8$-64-σ_0	6.59	18942	FinFet 7 nm	[31]
$QARMA_5$-64-σ_1	5.07	13751	FinFet 7 nm	[31]
$QARMA_6$-64-σ_1	5.80	16126	FinFet 7 nm	[31]
$QARMA_7$-64-σ_1	6.23	18362	FinFet 7 nm	[31]
$QARMA_8$-64-σ_1	6.63	20575	FinFet 7 nm	[31]
$QARMA_5$-64-σ_2	4.96	14472	FinFet 7 nm	[31]
$QARMA_6$-64-σ_2	5.69	16795	FinFet 7 nm	[31]
$QARMA_7$-64-σ_2	6.17	19055	FinFet 7 nm	[31]
$QARMA_8$-64-σ_2	6.61	21075	FinFet 7 nm	[31]

总结与展望

当前低延迟分组密码及组件的设计与分析是密码学研究的热点方向。其核心目标在于研究更加灵活、广泛适用的算法，以满足不同场景和应用需求的多样性。随着工业互联网的快速发展，对于安全可靠的低延迟分组密码算法的需求将会持续增长，未来的研究重心将放在提高安全性、资源效率和标准化推广等方面。面对现有综述在这一领域存在的空白，本文对现有算法进行深入分析和总结，同时介绍了低延迟研究的相关进展。接下来，本文将对适应工业互联网的低延迟分组密码研究进行详细总结。同时，基于工业环境的不断发展和变化，本文提出了一系列可能的研究方向和问题，对该领域的未来工作进行展望。这不仅包括理论层面的问题，也包括实际应用中的挑战，为研究者提供了一个系统全面的参考。

总结

低延迟密码算法在工业互联网的终端设备中发挥着重要的作用，为工业互联网的发展和应用提供了重要的安全基础。在实际应用中，需要综合考虑设备资源、安全性要求和性能等因素来选择适合的密码算法和方案。轻量级分组密码通常用于各种传感器、控制器、执行器等终端设备，根据其采集的数据量和实时性要求可将其分成“低数据量、高实时性”、“中等数据量、中等实时性”、“高数据量、高实时性”等。例如，工业传感器需要快速响应并传输采集到的数据，这种情况下可以选择具有适当强度和较高运算效率的轻量级分组密码算法来确保数据的安全性，同时满足实时性要求;工业控制系统的高速数据采集设备，需要以高速传输数据并进行实时处理和决策，这种情况对数据的实时性有非常高的要求，同时要考虑终端设备的计算和能源资源限制，为低延迟分组密码带来一些挑战。

展望

通过国内外研究现状分析，当前研究存在以下工作需要研究与探索：

1) 在算法优化方面，尽管已有一些低延迟密码算法，但仍需研究和开发更多算法，以适应不同工业应用场景的特殊需求。由于Feistel结构不适合用于低延迟的实现，现有大部分低延迟分组密码采用SPN类型的结构。因此，可以探索新型结构以达到更好性能，研究S盒等关键密码部件延迟和安全性的合理平衡。工业互联网设备往往对能耗有严格要求，研究如何设计或优化低延迟密码算法以降低能耗。此外，现有算法大都设定为某个具体场景，随着工业互联网的发展，能否突破该约束，设计自适应场景的算法，即通过自动检测环境的变化从而自适应实时更新重组，增强密码应用部署灵活性，实现多元化、多场景应用。
2) 在安全声明和分析评估方面，对现有低延迟密码算法进行深入的安全性分析， 包括抵抗量子计算机攻击的能力，以及在不同使用场景下的安全性评估。提高安全性分析的方法，完善面向工业互联网的低延迟分组密码的安全设计准则。提升安全性自动化分析评估手段，如差分自动分析的辅助搜索技术。在设计低延迟密码算法时，探索如何自然地融入抵抗侧信道攻击的特性，如通过算法的位切片实现。将传统密码分析领域知识与深度学习相结合，对安全性分析进行量化评估从而确定算法的实际可用性。
3) 在软硬件实现方面，研究如何在硬件上高效实现低延迟密码算法，包括FPGA、ASIC和其他嵌入式系统，以及如何优化以满足工业环境的特定要求。证明低延迟分组密码硬件架构是否符合工业互联网设备安全需求，需要对其进行硬件性能评估。在密码算法设计阶段，密码结构与组件参数设计可能需要根据硬件评估结果进行调整。开发高效的软件实现方法，以便在各种操作系统和平台上实现低延迟密码算法，同时保持跨平台兼容性。

4) 随着新的应用场景不断出现，结合工业自动化、网络通信、信息安全等领域的知识，探索密码算法在工业互联网中的综合应用。探索如何将低延迟密码算法与其他认证机制（如生物识别技术）结合，提供更全面的安全保护。在数据传输和处理过程中，如何实现对错误的容忍以及保障数据的完整性。

参考文献

[1] Rijmen V, Daemen J. Advanced encryption standard[J]. Proceedings of federal information processing standards publications, national institute of standards and technology, 2001, 19: 22.

[2] Shannon C E. Communication theory of secrecy systems[J]. The Bell system technical journal, 1949, 28(4): 656-715.

[3] Gong Z, Nikova S, Law Y W. KLEIN: a new family of lightweight block ciphers[C]. International workshop on radio frequency identification: security and privacy issues. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 1-18.

[4] Guo J, Peyrin T, Poschmann A, et al. The LED block cipher[C]. Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13. Springer Berlin Heidelberg, 2011: 326-341.

[5] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An ultra-lightweight block cipher[C]. Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. Springer Berlin Heidelberg, 2007: 450-466.

[6] Girija M, Manickam P, Ramaswami M. PriPresent: an embedded prime LightWeight block cipher for smart devices[J]. Peer-to-Peer Networking and Applications, 2021, 14(4): 2462-2472.

[7] Li L, Liu B, Wang H. QTL: A new ultra-lightweight block cipher[J]. Microprocessors and Microsystems, 2016, 45: 45-55.

[8] Guo J, Peyrin T, Poschmann A. The PHOTON family of lightweight hash functions[C]. Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31. Springer Berlin Heidelberg, 2011: 222-239.

[9] Longo J, De Mulder E, Page D, et al. SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip[C]. Cryptographic Hardware and Embedded Systems-CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17. Springer Berlin Heidelberg, 2015: 620-640.

[10] Albrecht M R, Rechberger C, Schneider T, et al. Ciphers for MPC and FHE[C]. Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I 34. Springer Berlin Heidelberg, 2015: 430-454.

[11] Wu W, Zhang L. LBlock: a lightweight block cipher[C]. Applied Cryptography and Network Security: 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings 9. Springer Berlin Heidelberg, 2011: 327-344.

[12] Standard D E. Data encryption standard[J]. Federal Information Processing Standards Publication, 1999, 112: 3.

[13] Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK lightweight block ciphers[C]. Proceedings of the 52nd annual design automation conference. 2015: 1-6.

[14] Hong D, Sung J, Hong S, et al. HIGHT: A new block cipher suitable for low-resource device[C]. Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8. Springer Berlin Heidelberg, 2006: 46-59.

[15] Suzaki T, Minematsu K, Morioka S, et al. TWINE: a lightweight block cipher for multiple platforms[C]. International Conference on Selected Areas in Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 339-354.

[16] Shirai T, Shibutani K, Akishita T, et al. The 128-bit blockcipher CLEFIA[C]. Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14. Springer Berlin Heidelberg, 2007: 181-195.

[17] Shibutani K, Isobe T, Hiwatari H, et al. Piccolo: an ultra-lightweight blockcipher[C]. Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13. Springer Berlin Heidelberg, 2011: 342-357.

[18] Berger T P, Francq J, Minier M, et al. Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput[J]. IEEE Transactions on Computers, 2015, 65(7): 2074-2089.

[19] Cheng J, Guo S, He J. An extended type-1 generalized feistel networks: Lightweight block cipher for iot[J]. IEEE Internet of Things Journal, 2021, 9(13): 11408-11421.

[20] Zhong Y, Gu J. Lightweight block ciphers for resource-constrained environments: A comprehensive survey[J]. Future Generation Computer Systems, 2024.

[21] Dar A B, Lone M J, Hussain N. Revisiting lightweight block ciphers: review, taxonomy and future directions[J]. Computer Science Review, Forthcoming, 2021.

[22] Shah A, Engineer M. A survey of lightweight cryptographic algorithms for iot-based applications[C]. Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS-2018. Springer Singapore, 2019: 283-293.

[23] Hatzivasilis G, Fysarakis K, Papaefstathiou I, et al. A review of lightweight block ciphers[J]. Journal of cryptographic Engineering, 2018, 8: 141-184.

[24] Borghoff J, Canteaut A, Güneysu T, et al. PRINCE–a low-latency block cipher for pervasive computing applications[C]. Advances in Cryptology–ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18. Springer Berlin Heidelberg, 2012: 208-225.

[25] Biryukov A. DES-X (or DESX)[J]. Encyclopedia of Cryptography and Security, 2011: 331.

[26] Kilian J, Rogaway P. How to protect DES against exhaustive key search[C]. Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16. Springer Berlin Heidelberg, 1996: 252-267.

[27] Soleimany H, Blondeau C, Yu X, et al. Reflection cryptanalysis of PRINCE-like ciphers[J]. Journal of Cryptology, 2015, 28: 718-744.

[28] Beierle C, Jean J, Kölbl S, et al. The SKINNY family of block ciphers and its low-latency variant MANTIS[C]. Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36. Springer Berlin Heidelberg, 2016: 123-153.

[29] Banik S, Bogdanov A, Isobe T, et al. Midori: A block cipher for low energy[C]. Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29--December 3, 2015, Proceedings, Part II 21. Springer Berlin Heidelberg, 2015: 411-436.

[30] Dobraunig C, Eichlseder M, Kales D, et al. Practical key-recovery attack on MANTIS5[J]. IACR Transactions on Symmetric Cryptology, 2016: 248-260.

[31] Avanzi R. The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes[J]. IACR Transactions on Symmetric Cryptology, 2017: 4-44.

[32] Božilov D, Eichlseder M, Knežević M, et al. PRINCEv2: more security for (almost) no overhead[C]. Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers 27. Springer International Publishing, 2021: 483-511.

[33] Banik S, Isobe T, Liu F, et al. Orthros: a low-latency PRF[J]. IACR Transactions on Symmetric Cryptology, 2021: 37-77.

[34] Leander G, Moos T, Moradi A, et al. The speedy family of block ciphers-engineering an ultra low-latency cipher from gate level for secure processor architectures[J]. IACR transactions on cryptographic hardware and embedded systems, 2021, 2021(4): 510-545.

[35] Boura C, David N, Heim Boissier R, et al. Better steady than speedy: full break of SPEEDY-7-192[C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2023: 36-66.

[36] Zhang L, Wu R, Zhang Y, et al. LLLWBC: A new low-latency light-weight block cipher[C]. International Conference on Information Security and Cryptology. Cham: Springer Nature Switzerland, 2022: 23-42.

[37] Canale F, Güneysu T, Leander G, et al. {SCARF}–A {Low-Latency} Block Cipher for Secure {Cache-Randomization}[C]. 32nd USENIX Security Symposium (USENIX Security 23). 2023: 1937-1954.

[38] Belkheyar Y, Daemen J, Dobraunig C, et al. Bipbip: A low-latency tweakable block cipher with small dimensions[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023: 326-368.

[39] Knežević M, Nikov V, Rombouts P. Low-latency encryption–is “lightweight= light+ wait”?[C]. Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14. Springer Berlin Heidelberg, 2012: 426-446.

[40] Kerckhof S, Durvaux F, Hocquet C, et al. Towards green cryptography: a comparison of lightweight ciphers from the energy viewpoint[C]. Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14. Springer Berlin Heidelberg, 2012: 390-407.

[41] Li L, Liu B, Zhou Y, et al. SFN: A new lightweight block cipher[J]. Microprocessors and Microsystems, 2018, 60: 138-150.

[42] Stoffelen K. Optimizing S-box implementations for several criteria using SAT solvers[C]. International Conference on Fast Software Encryption. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 140-160.

[43] Bilgin B, De Meyer L, Duval S, et al. Low AND depth and efficient inverses: a guide on s-boxes for low-latency masking[J]. IACR Transactions on Symmetric Cryptology, 2020, 2020(1): 144-184.

[44] Rasoolzadeh S. Low-latency Boolean functions and bijective S-boxes[J]. IACR Transactions on Symmetric Cryptology, 2022, 2022(3): 403-447.

[45] Leander G, Poschmann A. On the classification of 4 bit S-boxes[C]. Arithmetic of Finite Fields: First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007. Proceedings 1. Springer Berlin Heidelberg, 2007: 159-176.

[46] Biryukov A, De Canniere C, Braeken A, et al. A toolbox for cryptanalysis: Linear and affine equivalence algorithms[C]. Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22. Springer Berlin Heidelberg, 2003: 33-50.

[47] De Meyer L, Bilgin B. Classification of balanced quadratic functions[J]. IACR Transactions on Symmetric Cryptology, 2019, 2019(2): 169-192.

[48] Huang X, Li L, Zhang H, et al. IoVCipher: A low-latency lightweight block cipher for internet of vehicles[J]. Ad Hoc Networks, 2024, 160: 103524.

[49] Sun W, Li L, Huang X. LTLBC: a low-latency lightweight block cipher for internet of things[J]. Cluster Computing, 2024: 1-12.

[50] Li S, Sun S, Li C, et al. Constructing low-latency involutory MDS matrices with lightweight circuits[J]. IACR Transactions on Symmetric Cryptology, 2019: 84-117.

[51] Li S, Sun S, Shi D, et al. Lightweight iterative MDS matrices: how small can we go?[J]. Cryptology ePrint Archive, 2019.

[52] Liu Q, Zhao Z, Wang M. Improved Heuristics for Low-Latency Implementations of Linear Layers[C]. Cryptographers' Track at the RSA Conference. Cham: Springer International Publishing, 2023: 524-550.

[53] Shi H, Feng X, Xu S. A Framework with Improved Heuristics to Optimize Low-Latency Implementations of Linear Layers[J]. IACR Transactions on Symmetric Cryptology, 2023, 2023(4): 489-510.

[54] Müller N, Moos T, Moradi A. Low-latency hardware masking of PRINCE[C]. International Workshop on Constructive Side-Channel Analysis and Secure Design. Cham: Springer International Publishing, 2021: 148-167.

[55] Moradi A, Schneider T. Side-Channel Analysis Protection and Low-Latency in Action: –Case Study of PRINCE and Midori–[C]. Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22. Springer Berlin Heidelberg, 2016: 517-547.

[56] Beyne T, Dhooghe S, Moradi A, et al. Cryptanalysis of efficient masked ciphers: applications to low latency[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022: 679-721.

[57] Shahmirzadi A, Dhooghe S, Moradi A. Low-latency and low-randomness second-order masked cubic functions[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023, 2023(1): 113-152

Research paper

Empowering Industrial Fault Detection via Self-Supervised Learning Techniques

Qianwen Meng, Yonghui Xu, Lizhen Cui

***Abstract*—Industrial fault detection is crucial in the production process, enabling the timely identification of equipment failures and providing early warnings. The limited availability of labeled industrial data constrains the use of supervised learning techniques for fault detection. Self-supervised learning (SSL) has gained popularity in recent years due to its ability to leverage large amounts of unlabeled data. However, using SSL for industrial fault detection presents several challenges. Firstly, faults are typically rare events, leading to imbalanced datasets where fault instances are much less frequent than normal instances. Secondly, contrastive learning is an effective way to enrich the rare events, but selecting suitable augmentations that impose priors to select viable positive samples remains a challenge. To address these challenges, we propose a novel approach that balances the fault and normal data and enriches the labeled data through efficient data augmentation. We empirically evaluate our approach on three public industrial time series datasets. The results demonstrate its superiority over the state-of-the-art approaches in empowering industrial fault detection tasks.**

This work was supported by the National Key R&D Program of China [No.2021YFF0900800]; NSFC [No.62202279, No.92367202]; Shandong Provincial Key Research and Development Program [No.2021CXGC010108]; and Shandong Provincial Natural Science Foundation [No.ZR2022QF018].

Q. Meng, Y. Xu, L. Cui. School of Software, Joint SDU-NTU Centre for Artificial Intelligence Research, Shandong University, Jinan, China (e-mail: mqw_sdu@mail.sdu.edu.cn; xuyonghui@sdu.edu.cn; clz@sdu.edu.cn).

***Keywords*—industrial fault detection, classification, time series, self-supervised learning, contrastive learning.**

I. INTRODUCTION

Industrial data, typically time series data collected from sensors or devices, are characterized by their time-specific nature and originate from production and related processes[1]. As the industrial Internet evolves rapidly, the use of time series data in the industrial sector has surged. Time series refer to data recorded in chronological order, with each data point linked to a specific timestamp[2]. They are typically collected from various sensors measuring power, temperature, pressure, flow, and more. These sensors, distributed across different devices and complex systems, capture critical information about the performance and functionality of industrial machinery. Industrial time series data are essential for monitoring the operational status of individual devices, the real-time condition of production lines, and the performance of the entire industrial systems[3].

In the field of Industrial Internet of Things (IIoT) modeling and analyzing industrial time series data can significantly enhance production efficiency, reduce energy consumption, and prevent failures, leading to more sustainable and efficient industrial production[4,5]. By analyzing the collected time series data, companies can monitor their production and operation processes, enabling timely detection of equipment failures and providing early warnings. This improves the reliability and stability of equipment operation. Additionally, analyzing the periodicity and trends within time series

data allows for predictive maintenance, helping companies determine optimal times for equipment upkeep and replacement. This enables more informed and strategic decision-making. Furthermore, real-time collection and storage of equipment operation data and production line status facilitate the optimization and control of production processes, thereby improving both efficiency and quality.

With the advent of sophisticated technologies and the rise of automation, swiftly identifying and categorizing faults in industrial processes has become paramount[24]. This capability is essential for ensuring seamless operations, minimizing downtime, and optimizing overall productivity. Efficient fault detection systems leverage advanced techniques to promptly detect and address issues, thereby maintaining the continuous and efficient functioning of industrial processes[8]. Due to the continuous and voluminous nature of industrial data, tasks such as trend analysis and fault detection typically require querying data over extended time periods across multiple collection points. This enables trend analysis and anomaly detection, crucial for identifying system faults[12]. As artificial intelligence technology advances, integrating time series data with machine learning, deep learning, and similar technologies enhances intelligent data analysis and management. This fusion presents both significant opportunities and challenges for the advancement of the industrial sector.

Self-supervised learning, as an emerging technique for its ability to process limited labeled data, gained popularity in such data without the need of artificial expensive labeling[17]. However, self-supervised learning relies on large amounts of unlabeled data, but the quality of this data is crucial. Industrial datasets often have limited labeled data and may contain noise or inaccuracies[19]. In addition, faults are typically rare events, leading to imbalanced datasets where fault instances are much less frequent than normal instances. In recent years, contrastive learning, which uses distance discrimination as the pretext task to distinguish between different instances, helps mitigate the issue of insufficient labeled data[21]. Data augmentation techniques can generate diverse samples from the same data, helping the model learn robust features despite potential noise and inaccuracies in the datasets. Contrastive learning focuses on learning representations that are invariant to different transformations, which helps in capturing complex fault patterns. By training on augmented data that includes subtle variations, the model becomes more sensitive to detecting subtle faults. However, poorly chosen augmentation transformations can significantly impede the construction of positive pairs, leading to detrimental effects in the contrastive learning process[22,23].

In this paper, we propose a novel contrastive learning approach which balances the fault and normal data and enriches the labeled data by efficient data augmentation. We design an efficient pretext task to select beneficial augmentations based on nearest neighbors and form positive pairs, while concurrently reducing extra costs associated with constructing negative pairs. Such beneficial augmentations help the model learn robust and invariant features. Enforcing the consistency within neighborhoods can help in learning feature representations that are more coherent and contextually relevant. Rich feature representations can be used in downstream tasks for more precise fault diagnosis, aiding in distinguishing between different fault types.

The rest of this paper is organized as follows: In Section II, we conduct a review of relevant literature in the domains of industrial fault detection and self-supervised learning. In Section III, we provide the preliminary and an overview of our proposed model, including the implementation details. Then, we introduce experimental settings, dataset descriptions, and evaluation metrics in Section IV. Results are presented and discussed in Section V. Finally, we briefly

conclude our work and discuss the future research directions in Section VI.

II. RELATED WORK

A. INDUSTRIAL FAULT DETECTION

Due to the presence of abnormalities such as product quality defects, equipment failures, performance degradation, and changes in the external environment within manufacturing systems, tasks such as abnormal condition detection, fault monitoring, and equipment health status analysis are crucial for achieving lean production and intelligent manufacturing. These tasks are also key research areas in industrial big data analysis. Time series anomaly detection is a technique for identifying and labeling unusual points or events in time series data that deviate from expected patterns, trends, or behaviors. Methods used for fault detection can be classified into data-driven, model-based, and knowledge-based approaches[31,35]. To be specific, data-driven approaches are widely used in the field of industry due to their simplicity and effectiveness. They rely on historical data to detect patterns and anomalies, using techniques such as machine learning algorithms, statistical methods, etc. Model-based approaches utilize the strength of different backbones to learn effective representations and detect deviations indicating faults. The knowledge-based approaches use rule-based systems where knowledge from domain experts is encoded in the form of if-then rules to detect faults. They can also employ structured representations of knowledge about the complex system to infer faults through logical reasoning, such as expert systems, fuzzy logic, case-based reasoning, and ontologies.

B. SELF-SUPERVISED LEARNING

Self-supervised learning takes advantage of the inherent structure and relationships within data by transforming them into pretext tasks, such as cross-view prediction[30], context prediction[11], masked reconstruction[15], multi-task prediction[26], missing data imputation[18], etc. These pretext tasks help eliminate the need of reconstructing the full input and allow for the discovery of contextualized underlying factors of variations[25]. While some pretext tasks yield promising results, they rely on heuristics that can potentially limit the generalizability of the learned representations[13]. Instead, contrastive learning, as a distinct type of self-supervised learning that revolves around the pretext task of instance discrimination, has demonstrated remarkable benefits across various applications. Contrastive learning methods commonly employ various augmentation transformations to generate augmented views from original data and then proceed to learn representations by contrasting positive samples against negative ones[34]. Previous studies have demonstrated the substantial performance enhancements through the adoption of larger batch sizes[7,9], the utilization of robust augmentations[32,33], and the incorporation of supplementary storage space to accommodate additional negative candidates[16,20]. Recently, there are also studies[10,14] that eliminate the need of negative sampling, thereby obviating the necessity for large batch sizes or extensive storage space. They explore to incorporate an extra learnable predictor and employ the stop-gradient operation to prevent mode collapse[27]. Since these methods exclusively utilize positive samples for contrastive learning, the significance of choosing beneficial augmentation transformations becomes paramount. Poorly chosen augmentation transformations can significantly impede the construction of positive pairs, leading to detrimental effects in the contrastive learning process.

III. METHODOLOGY

A. PRELIMINARY

Given a dataset X consisting of N samples, $\mathbf{x}$ denotes a sample with the dimensionality of $S \times V$, where S denotes the sequence length (i.e., the number of

timestamps), and V denotes the number of features. $\mathbf{y}$ is the feature representation learned by the encoder $f_\theta(\cdot)$, $\mathbf{z}$ is the projection vector obtained by the nonlinear projection head $g_\theta(\cdot)$, and $\mathbf{h}$ is the prediction vector generated by the predictor $q_\theta(\cdot)$. The objective of our model is to learn an improved feature representation $\mathbf{y}$ for sample $\mathbf{x}$ to feed into a linear classifier, thereby enhancing the downstream industrial fault detection task. Tab.1 lists all the mathematical notations used throughout this paper.

Table 1 List of mathematical notations.

Notation	Description
$\mathbf{x}$	original sample
$\mathbf{y}$	feature representation
$\mathbf{z}$	projection vector
$\mathbf{h}$	prediction vector
N	number of samples
S	sequence length
V	number of features
$\mathcal{T}(\cdot)$	transformation function
$f_\theta(\cdot)$	encoder
$g_\theta(\cdot)$	nonlinear projection head
$q_\theta(\cdot)$	predictor
θ_1	parameters of the online network
θ_2	parameters of the target network

B. OVERVIEW

As presented in Fig.1, our proposed model consists of two main modules: a neighbor-driven transformation selection module and a contrastive representation learning module.

In the neighbor-driven transformation selection module, various augmentation transformation functions with different parameters are applied to original samples to generate multiple augmented samples. Then, the nearest neighbor search is performed to find the optimal augmented sample for each original sample. These augmented samples are then sorted in descending order to identify the top two optimal transformations, which will be used globally for data augmentation to construct neighbor-driven positive samples for contrastive learning.

In the contrastive representation learning module, a trainable online network and a fixed target network are designed. Both networks share identical architectures but possess different parameters. Parameters θ_1 of the online network are updated using stochastic gradient descent with back-propagation, while parameters θ_2 of the target network are updated via a momentum-based moving exponential average of the online network to maintain the consistency. The five key components in this module are as follows.

(1) Augmentation Transformation: two correlated augmented views $\mathbf{x^1}$ and $\mathbf{x^2}$ are generated by transformation functions $\mathcal{T}_1(\cdot)$ and $\mathcal{T}_2(\cdot)$ from the original sample $\mathbf{x}$, respectively.

(2) Encoder: $f_{\theta_1}(\cdot)$ and $f_{\theta_2}(\cdot)$ encode the feature representations $\mathbf{y^1}$ and $\mathbf{y^2}$ for the augmented views $\mathbf{x^1}$ and $\mathbf{x^2}$, respectively.

(3) Nonlinear Projection Head: $g_{\theta_1}(\cdot)$ and $g_{\theta_2}(\cdot)$ remaps the feature representations $\mathbf{y^1}$ and $\mathbf{y^2}$ of the augmented views to projection vectors $\mathbf{z^1}$ and $\mathbf{z^2}$ in a new latent space, respectively.

(4) Predictor: $q_{\theta_1}(\cdot)$ generates the prediction vector $\mathbf{h^1}$ based on the latent projection vector $\mathbf{z^1}$.

(5) Loss Function: The model learns parameters θ_1 and θ_2 of the online and the target network by minimizing the total contrastive learning loss $\mathcal{L}_{total}$.

After training, the learned feature representation $\mathbf{y}$ generated by the encoder $f_\theta(\cdot)$ will be frozen and then fed into a linear classifier to perform the downstream industrial fault detection task. The linear classifier is a logistic regression classifier, comprising a fully-connected layer followed by a softmax activation function.

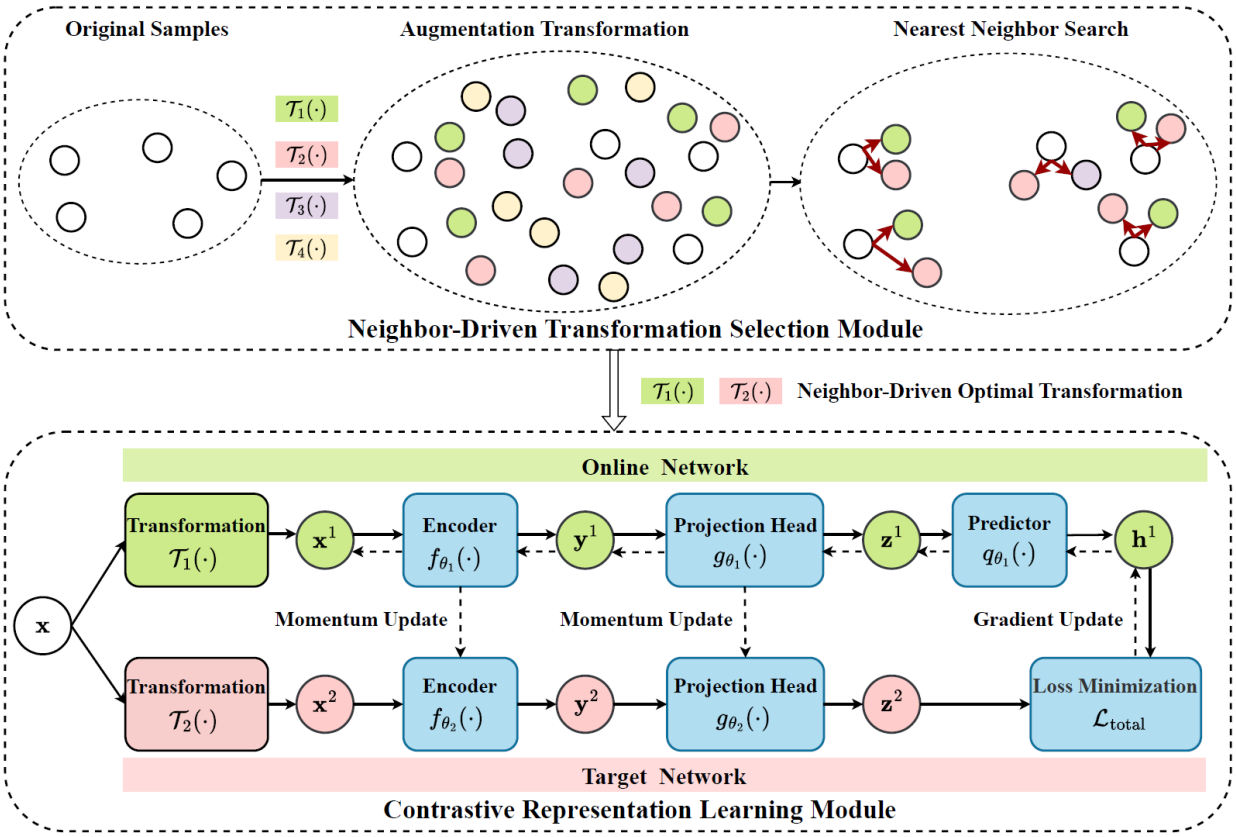


Figure 1 The proposed self-supervised learning framework for industrial fault detection.

C. NEIGHBOR-DRIVEN POSITIVE SAMPLES SELECTION

Data augmentation plays a crucial role in contrastive learning as it facilitates the generation of synthetic data that spans unexplored regions in the input space while retaining correct labels. Diverse augmentation transformations aid in the learning of more robust and generalizable representations. The widely-used augmentation transformations for time series data include rotation, scaling, jittering, permutation, window slicing, magnitude warping, and time warping. These transformations are characterized by diverse parameters with different ranges such as magnitude, which govern the effects on the original data. Tab.2 lists the detailed information of these augmentation transformations. Distinct transformation functions with varying magnitudes induce different degrees of alterations to the original data. Given that not all augmentations yield beneficial contributions to contrastive learning owing to variations in magnitudes or other factors relative to the original data, selecting the appropriate augmentation transformation with suitable parameters for improved contrastive learning becomes challenging.

In this study, we propose to leverage neighbor-driven positive samples to incorporate information from neighboring augmentations. To be specific, we first discretize the range of magnitudes with continuous values into ten values by uniform spacing. Then, each sample undergoes a single augmentation with varying parameter values within the range. We aggregate them together to construct a comprehensive set of diverse augmentations, each with varying parameters, within the same latent space as the original samples. This unified space facilitates the identification of neighbors for each sample using the Nearest Neighbor Search approach.

Once all augmented samples are generated, we calculate the nearest neighbor proportion for each type of augmentation transformation and sort them in descending order. Finally, the top two augmentation transformations are selected as the global augmentations for the selection of neighbor-driven positive samples, which are used in subsequent

contrastive learning.

Table 2 Detailed information of augmentation transformations.

Augmentation	Parameters	Range
rotation	axis, angle	[-1,1], [$-\pi$,π]
scaling	σ	[0.1, 2.0]
jittering	σ	[0.01, 0.8]
permutation	max_segments	{3, 4, 5, 6}
window slicing	reduce_ratio	[0.6, 0.95]
magnitude warping	σ, knot	[0.1, 2.0], {3, 4, 5}
time warping	σ, knot	[0.01, 0.5], {3, 4, 5}

D. NEIGHBOR-DRIVEN CONTRASTIVE LEARNING LOSS

We extend the contrastive loss in BYOL[14] to include neighbor-driven positive pairs, which achieved by selecting positive pairs from neighboring augmentations. This encourages the model to learn representations that are consistent with the local temporal context.

The contrastive learning loss function $\mathcal{L}_c$ is the mean squared error to measure the difference between the L2-normalized predictions of the online network and the projections of the target network. To achieve symmetrization, the two augmented views $\mathbf{x^1}$ and $\mathbf{x^2}$ generated from the original sample $\mathbf{x}$, are interchanged through both networks twice, thereby maximizing the utilization of all available data. The loss function is defined as follows,

$$\mathcal{L}_c = -\frac{\left\langle q_{\theta_1}\left(g_{\theta_1}\left(f_{\theta_1}(\mathbf{x^1})\right)\right), g_{\theta_2}\left(f_{\theta_2}(\mathbf{x^2})\right)\right\rangle}{|q_{\theta_1}\left(g_{\theta_1}\left(f_{\theta_1}(\mathbf{x^1})\right)\right)|_2 \cdot |g_{\theta_2}\left(f_{\theta_2}(\mathbf{x^2})\right)|_2} - \frac{\left\langle q_{\theta_1}\left(g_{\theta_1}\left(f_{\theta_1}(\mathbf{x^2})\right)\right), g_{\theta_2}\left(f_{\theta_2}(\mathbf{x^1})\right)\right\rangle}{|q_{\theta_1}\left(g_{\theta_1}\left(f_{\theta_1}(\mathbf{x^2})\right)\right)|_2 \cdot |g_{\theta_2}\left(f_{\theta_2}(\mathbf{x^1})\right)|_2} .$$

where $\langle \cdot,\cdot \rangle$ denotes the inner product.

In addition, we apply regularization techniques that enforce smoothness in the learned representations. To be specific, we add a regularization term $\mathcal{L}_s$ to the loss function that penalizes large differences between the embeddings of neighboring augmentations.

$$\mathcal{L}_s = |q_{\theta_1}\left(g_{\theta_1}\left(f_{\theta_1}(\mathbf{x^1})\right)\right) - g_{\theta_2}\left(f_{\theta_2}(\mathbf{x^2})\right)|_2^2 + |q_{\theta_1}\left(g_{\theta_1}\left(f_{\theta_1}(\mathbf{x^2})\right)\right) - g_{\theta_2}\left(f_{\theta_2}(\mathbf{x^1})\right)|_2^2 .$$

The total loss function with smoothness regularization is defined as follows:

$$\mathcal{L}_{total} = \mathcal{L}_c + \lambda \mathcal{L}_s ,$$

where λ is the regularization parameter that controls the strength of the temporal smoothness penalty.

During training, the total loss function is minimized with respect to θ_1 exclusively, while θ_2 are updated through the slowly moving exponential average of θ_1 as follows,

$$\theta_2 \leftarrow m\theta_2 + (1-m)\theta_1,$$

where $m \in [0,1]$ denotes the momentum coefficient.

IV. EXPERIMENTAL EVALUATION

A. EXPERIMENTAL SETTINGS

Our model is implemented under the PyTorch framework. The experiments are carried out on the computational platform equipped with an NVIDIA GeForce RTX 3090 GPU. We evaluate the performance of the learned feature representations on industrial fault detection downstream tasks using the standard linear evaluation method, as employed in previous works[9,13,30]. The batch size is set to 128 and the model is trained for 200 epochs using Stochastic Gradient Descent (SGD) as the optimizer.

B. DATASET DESCRIPTIONS

In order to investigate the effectiveness of our proposed model, we select three public industrial time series datasets for evaluation, including Wafer, ACSF1 and FaultDetectionA. More statistical information of these datasets is listed in Tab.3.

Table 3 Statistical information of datasets. N denotes the number of samples and V denotes the number of features. Classes refer to the number of classes in each dataset and S refers to the sequence length.

Dataset	N	V	Classes	S
Wafer	1194	6	2	198
ACSF1	200	1	10	1460
FaultDetectionA	13640	1	3	5120

C. EVALUATION METRICS

Given that industrial fault detection can be treated as a time series classification task, we employ two widely-used metrics to assess the classification performance, including Accuracy (ACC) and Macro-averaged F1-score (MF1). To be specific, ACC is the ratio of the

number of correctly classified samples to the total number of samples, i.e., $\mathrm{ACC} = \frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}}$, where TP, TN, FP, FN are true positive, true negative, false positive and false negative, respectively. MF1 is calculated as the arithmetic mean of individual classes' F1-score, i.e., $\mathrm{MF1} = \frac{2\times\mathrm{PR}}{\mathrm{P+R}}$, where Precision $\mathrm{P} = \frac{\mathrm{TP}}{\mathrm{TP+FP}}$ is the ratio of the number of correctly predicted positive samples to the total number of predicted positive samples, and Recall $\mathrm{R} = \frac{\mathrm{TP}}{\mathrm{TP+FN}}$ is the ratio of the number of correctly predicted positive samples to the total number of samples in actual classes.

Table 4 Comparison between our model against baselines on three datasets.

Dataset	Metric	SimCLR	BYOL	SwAV	CPC	TS-TCC	Ours
Wafer	ACC	0.912	0.920	0.891	0.905	0.917	**0.934**
	MF1	0.886	0.897	0.869	0.883	0.894	**0.915**
ACSF1	ACC	0.825	0.834	0.816	0.811	0.833	**0.850**
	MF1	0.794	0.815	0.760	0.754	0.807	**0.826**
FaultDetectionA	ACC	0.693	0.705	0.636	0.672	0.697	**0.719**
	MF1	0.655	0.670	0.604	0.629	0. 664	**0.681**

V. RESULTS AND ANALYSIS

To investigate the superiority of our proposed model, we compare it with the following baselines.

(1) SimCLR[9] is the most widely used contrastive learning model that highlights the significance of larger batch sizes, more training steps, and compositions of augmentations to improve the quality of the learned representations.

(2) BYOL[14] firstly removes the need of using negative samples for contrastive learning, instead employing the predictor and the stop-gradient strategy to learn the mappings while preventing the mode collapse problem.

(3) SwAV[6] incorporates cluster-level contrast and performs a swapped prediction task, simultaneously engaging in scalable online clustering while enforcing the consistency between cluster assignments produced for augmentations.

(4) CPC[30] integrates predictive coding and noise-contrastive estimation, creating a latent space that encodes predictions for future observations to capture information that is maximally beneficial for prediction.

(5) TS-TCC[13] constructs simple yet efficient time-series-specific augmented views to perform temporal and contextual contrasting, and designs a tough cross-view prediction task to learn robust and discriminative representations.

Tab.4 provides the comparison between our proposed model against five baselines on three public industrial time series datasets. Overall, our proposed model consistently outperforms all contrastive learning models across all three datasets. Notably, both BYOL[14] and our proposed model exhibit significant advantages over SimCLR[9], SwAV[6], CPC[30], and TS-TCC[13], which typically choose 2 positive samples and $2(N-1)$ negative samples for contrasting. The incorporation of an additional learnable predictor and the utilization of a stop-gradient operation in our model helps prevent collapsing, contributing to its superior performance. In addition, our proposed model, which employs a neighbor-driven augmentation selection strategy, surpasses BYOL[14] that eliminates negative sampling without augmentation filtering, underscoring the significance of performing beneficial augmentation selection to enhance the quality of the selected positive samples.

VI. CONCLUSION AND FUTURE WORK

In this paper, we propose a novel contrastive learning approach that balances fault and normal data while enriching labeled data through effective data augmentation. We design an effective pretext task that selects beneficial augmentations based on nearest neighbors to form positive pairs, simultaneously reducing the extra costs associated with constructing negative pairs. These beneficial augmentations facilitate the model in learning robust and invariant features. By enforcing consistency within neighborhoods, our approach aids in learning feature representations that are more coherent and contextually relevant. These rich feature representations can subsequently be utilized in downstream tasks for more precise fault diagnosis, thereby aiding in distinguishing between different fault types. Our approach performs contrastive learning without incurring additional costs for negative sampling, instead enhancing the quality of positive samples through the use of neighbor-driven information for augmentation selection. Furthermore, our proposed regularization strategy with smoothness enforces temporal smoothness in the learned representations of augmented and original samples. The experimental results demonstrate that our model outperforms state-of-the-art methods.

Although our proposed approach has some limitations in real-time processing, it has the potential to unlock new opportunities and applications in industrial domains. In future work, we will explore real-time implementations of the proposed approach to ensure immediate fault detection and response in industrial settings. This will further enhance the effectiveness and applicability of our approach in industrial fault detection, driving advancements in intelligent manufacturing and predictive maintenance.

References

[1] Suschnigg, J., Mutlu, B., Fuchs, A. K., Sabol, V., Thalmann, S., & Schreck, T. (2020). Exploration of Anomalies in Cyclic Multivariate Industrial Time Series Data for Condition Monitoring. In EDBT/ICDT Workshops (pp. 1-8).

[2] Meng, Q., Qian, H., Liu, Y., Xu, Y., Shen, Z., & Cui, L. (2023). Unsupervised representation learning for time series: A review. arXiv preprint arXiv:2308.01578.

[3] Pell, D., Mytton, O., Penney, T. L., Briggs, A., Cummins, S., Penn-Jones, C., ... & Adams, J. (2021). RETRACTED: Changes in soft drinks purchased by British households associated with the UK soft drinks industry levy: controlled interrupted time series analysis. bmj, 372.

[4] Tuli, S., Casale, G., & Jennings, N. R. (2022). Tranad: Deep transformer networks for anomaly detection in multivariate time series data. arXiv preprint arXiv:2201.07284.

[5] Liu, Y., Garg, S., Nie, J., Zhang, Y., Xiong, Z., Kang, J., & Hossain, M. S. (2020). Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. IEEE Internet of Things Journal, 8(8), 6348-6358.

[6] Caron, M., Misra, I., Mairal, J., Goyal, P., Bojanowski, P., & Joulin, A. (2020). Unsupervised learning of visual features by contrasting cluster assignments. Advances in neural information processing systems, 33, 9912-9924.

[7] Chen, C., Zhang, J., Xu, Y., Chen, L., Duan, J., Chen, Y., ... & Chilimbi, T. (2022). Why do we need large batchsizes in contrastive learning? a gradient-bias perspective. Advances in Neural Information Processing Systems, 35, 33860-33875.

[8] Park, Y. J., Fan, S. K. S., & Hsu, C. Y. (2020). A review on fault detection and process diagnostics in industrial processes. Processes, 8(9), 1123.

[9] Chen, T., Kornblith, S., Norouzi, M., & Hinton, G. (2020, November). A simple framework for contrastive learning of visual representations. In International conference on machine learning (pp. 1597-1607). PMLR.

[10] Chen, X., & He, K. (2021). Exploring simple siamese representation learning. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 15750-15758).

[11] Chen, Y., Zhou, X., Xing, Z., Liu, Z., & Xu, M. (2022, April). Cass: A channel-aware self-supervised representation learning framework for multivariate time series classification. In International Conference on Database Systems for Advanced Applications (pp. 375-390). Cham: Springer International

Publishing.

[12] Qian, J., Song, Z., Yao, Y., Zhu, Z., & Zhang, X. (2022). A review on autoencoder based representation learning for fault detection and diagnosis in industrial processes. Chemometrics and Intelligent Laboratory Systems, 231, 104711.

[13] Eldele, E., Ragab, M., Chen, Z., Wu, M., Kwoh, C. K., Li, X., & Guan, C. (2021). Time-series representation learning via temporal and contextual contrasting. arXiv preprint arXiv:2106.14112.

[14] Grill, J. B., Strub, F., Altché, F., Tallec, C., Richemond, P., Buchatskaya, E., ... & Valko, M. (2020). Bootstrap your own latent-a new approach to self-supervised learning. Advances in neural information processing systems, 33, 21271-21284.

[15] Haresamudram, H., Beedu, A., Agrawal, V., Grady, P. L., Essa, I., Hoffman, J., & Plötz, T. (2020, September). Masked reconstruction based self-supervision for human activity recognition. In Proceedings of the 2020 ACM International Symposium on Wearable Computers (pp. 45-49).

[16] He, K., Fan, H., Wu, Y., Xie, S., & Girshick, R. (2020). Momentum contrast for unsupervised visual representation learning. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 9729-9738).

[17] Gui, J., Chen, T., Zhang, J., Cao, Q., Sun, Z., Luo, H., & Tao, D. (2024). A Survey on Self-supervised Learning: Algorithms, Applications, and Future Trends. IEEE Transactions on Pattern Analysis and Machine Intelligence.

[18] Khayati, M., Lerner, A., Tymchenko, Z., & Cudré-Mauroux, P. (2020). Mind the gap. Proceedings of the VLDB Endowment, 13, 768-782.

[19] Fredriksson, T., Mattos, D. I., Bosch, J., & Olsson, H. H. (2020, November). Data labeling: An empirical investigation into industrial challenges and mitigation strategies. In International Conference on Product-Focused Software Process Improvement (pp. 202-216). Cham: Springer International Publishing.

[20] Li, J., Zhou, P., Xiong, C., & Hoi, S. C. (2020). Prototypical contrastive learning of unsupervised representations. arXiv preprint arXiv:2005.04966.

[21] Jaiswal, A., Babu, A. R., Zadeh, M. Z., Banerjee, D., & Makedon, F. (2020). A survey on contrastive self-supervised learning. Technologies, 9(1), 2.

[22] Meng, Q., Qian, H., Xu, Y., & Cui, L. (2024). Augmentation blending with clustering-aware outlier factor: An outlier-driven perspective for enhanced contrastive learning. Knowledge-Based Systems, 112014.

[23] Lin, S., Zhang, Z., Li, X., & Chen, Z. (2023, June). Selectaugment: Hierarchical deterministic sample selection for data augmentation. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 37, No. 2, pp. 1604-1612).

[24] Angelopoulos, A., Michailidis, E. T., Nomikos, N., Trakadas, P., Hatziefremidis, A., Voliotis, S., & Zahariadis, T. (2019). Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. Sensors, 20(1), 109.

[25] Mohamed, A., Lee, H. Y., Borgholt, L., Havtorn, J. D., Edin, J., Igel, C., ... & Watanabe, S. (2022). Self-supervised speech representation learning: A review. IEEE Journal of Selected Topics in Signal Processing, 16(6), 1179-1210.

[26] Sarkar, P., & Etemad, A. (2020). Self-supervised ECG representation learning for emotion recognition. IEEE Transactions on Affective Computing, 13(3), 1541-1554.

[27] Tian, Y., Chen, X., & Ganguli, S. (2021, July). Understanding self-supervised learning dynamics without contrastive pairs. In International Conference on Machine Learning (pp. 10268-10278). PMLR.

[28] Tonekaboni, S., Eytan, D., & Goldenberg, A. (2021). Unsupervised representation learning for time series with temporal neighborhood coding. arXiv preprint arXiv:2106.00750.

[29] Torres, J. F., Hadjout, D., Sebaa, A., Martínez-Álvarez, F., & Troncoso, A. (2021). Deep learning for time series forecasting: a survey. Big Data, 9(1), 3-21.

[30] Oord, A. V. D., Li, Y., & Vinyals, O. (2018). Representation learning with contrastive predictive coding. arXiv preprint arXiv:1807.03748.

[31] Taqvi, S. A. A., Zabiri, H., Tufa, L. D., Uddin, F., Fatima, S. A., & Maulud, A. S. (2021). A review on data‐driven learning approaches for fault detection and diagnosis in chemical processes. ChemBioEng Reviews, 8(3), 239-259.

[32] Wang, X., & Qi, G. J. (2022). Contrastive learning with stronger augmentations. IEEE transactions on pattern analysis and machine intelligence, 45(5), 5549-5560.

[33] Zhao, X., Du, T., Wang, Y., Yao, J., & Huang, W. (2023). ArCL: enhancing contrastive learning with augmentation-robust representations. arXiv preprint arXiv:2303.01092.

[34] Zhu, Y., Xu, Y., Liu, Q., & Wu, S. (2021). An empirical study of graph contrastive learning. arXiv preprint arXiv:2109.01116.

[35] Li, W., Li, H., Gu, S., & Chen, T. (2020). Process fault diagnosis with model-and knowledge-based approaches: Advances and opportunities. Control Engineering Practice, 105, 104637.

About the authors

Qianwen Meng is currently a Ph.D student in School of Software, Shandong University, China, and Joint SDU-NTU Centre for Artificial Intelligence Research, Shandong University, China. She received the Master's degree in School of Software, Shandong University, China in 2020, and the Bachelor's degree in School of Computer Science and Technology, Shandong University, China in 2017. Her research interests mainly lie in representation learning, unsupervised learning, time series modeling, and disease risk prediction. (Email: mqw_sdu@mail.sdu.edu.cn)

Lizhen Cui [corresponding author] (IET Fellow, IEEE Senior Member) is a professor and doctoral supervisor at School of Software, Shandong University. He is the Co-Director of Joint SDU-NTU Centre for Artificial Intelligence Research (C-FAIR) and Research Center of Software and Data Engineering, Shandong University. He received his B.Sc., M.Sc., and Ph.D. degrees from Shandong University, Jinan, China, in 1999, 2002 and 2005, respectively. He has published over 200 high-level academic articles in TKDE, TPAMI, TPDS, TSC, TCC, TNNLS, AAAI, SIGIR, CIKM, BIBM, ICDCS, DASFAA, ICWS, ICSOC, AAMAS, and MICCAI. He regularly serves as PC for prestigious conferences (i.e., KDD, IJCAI, and CIKM) and reviewers for IEEE/ACM Transactions Journals. His research interests include big data analysis, data mining, and crowd science. (Email: clz@sdu.edu.cn)

Yonghui Xu is a professor at Joint SDU-NTU Centre for Artificial Intelligence Research (C-FAIR), Shandong University. Before that, he was a research fellow in the Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY), Nanyang Technological University, Singapore. He received his Ph.D. from the School of Computer Science and Engineering at South China University of Technology in 2017 and BS from the Department of Mathematics and Information Science Engineering at Henan University of China in 2011. His research areas include various topics in Trustworthy AI, knowledge graphs, expert systems and their applications in e-commerce and healthcare. (Email: xuyonghui@sdu.edu.cn)

Recursive residual convolutional neural network with attention mechanism based on U-Net (Attention R2U-Net) for surface minor defect detection

Yongwen Zhang[1], Jun Zhou[2], Dongbin Ji[3],Xin Wen[4]

***Abstract*—Surface defect detection is a critical task in industrial production, involving the identification of defects in material surface images through advanced algorithms. While existing segmentation-based approaches struggle with issues such as weak anti-interference, susceptibility to noise, and poor performance in detecting minor defects, this paper introduces an enhanced approach using the R2U-Net framework combined with an attention mechanism. Our model integrates recurrent convolutional layers, residual connections, and attention gates within the U-Net framework to improve feature extraction, gradient flow, and focus on relevant regions. These enhancements allow for more accurate detection of small defects by iteratively refining features, improving network depth, and dynamically suppressing background noise. Compared to existing models, our approach demonstrates superior accuracy and precision in detecting small surface defects, making it a valuable contribution to industrial computer vision applications.**

***Keywords* — surface inspection, machine learning, attention mechanism**

Manuscript received XX. XX, 2024; accepted XX. XX, 2024.

Hengyuan Intelligent Manufacturing Industrial Park, No.2 Minjiang Road, China Pilot Free Trade Zone Area, Fushan District, Yantai City, Shandong Province, 264000, China.

This work is supported by Shandong Provincial Department of Industry and Information Technology Announcement on the "Work Empowers Hundred Scenarios" Digital Transformation Unveiling Pilot Projects，Key Projects for High-Quality Development of Software Industry in Shandong Province by Shandong Provincial Department of Industry and Information Technology.

I. INTRODUCTION

As industry and manufacturing continue to grow and evolve, the importance of detecting small defects on the surface of materials is becoming increasingly important[1,2]. In high-precision industries such as aerospace, automotive, electronics and medical devices, even the smallest defects can affect the structural integrity, functionality and safety of a product. Early detection of these defects can help prevent costly recalls, reduce waste and improve overall product quality. Additionally, as manufacturing processes become more complex and materials are pushed to their limits, the ability to identify and address defects at the micro level ensures that products meet stringent performance standards and regulatory requirements. This proactive approach not only improves product reliability and durability, but also enhances consumer trust and satisfaction, driving innovation and competitiveness in the global marketplace.

Currently, research on the detection of small defects on material surfaces is increasingly favoring the integration of machine learning (ML) techniques[3,4] that are transforming the field by providing more accurate, efficient and automated solutions. Machine learning algorithms, particularly deep learning models, are being trained on large datasets of material images to recognize patterns and identify defects that may not be detectable by the human eye or traditional inspection methods. Techniques such as convolutional neural networks (CNNs)[5] are proving particularly effective in analyzing high-resolution images and detecting microscopic anomalies. In addition, ML methods are augmenting non-destructive inspection (NDE)[6] methods with improved signal processing and interpretation to increase the reliability of defect detection for a wide range of materials. Researchers are also working to develop robust ML models that can be adapted to the characteristics of different types of materials and defects to ensure a wide range of applications in a variety of industries. Despite these advances, challenges such as the need for large labeled datasets, the complexity of model training, and the integration of ML systems into existing industrial workflows remain areas of active research and development.

First of all DCNN (Dynamic Convolution Neural Network)[7] has achieved great success in the field of computer vision, where different variants of the method have been applied to detect different surface defects. For example, DCNN has been applied to the tasks of recognizing defects in railroad tracks and classifying images of steel surfaces. RFCNs (Region-based Fully Convolutional Networks)[8], an approach based on Target Detection Networks (TDNs)[20], also performs well in the task of tiny surface defect detection.RFCNs combine the principles of Region Proposal Networks (RPNs)[21] and Fully Convolutional Networks (FCNs)[22] to create a powerful framework for the detection of small and complex defects on the surface of a material by generating Region Proposals, highlighting potentially defective regions. This is then processed by a series of convolutional layers to extract a detailed feature map. In addition, pixel segmentation network-based approaches also have good performance, e.g., U-Net[9,23], originally developed for biomedical image segmentation, has proven to be very effective for tiny surface defect detection due to its unique architecture and robust performance.The U-Net architecture consists of a contraction path for capturing context and a symmetric expansion path for pinpointing, which is essential for identifying material surface The U-Net architecture[24,25] includes a contraction path for capturing context and a symmetric expansion path for precise localization, which is critical for identifying small defects on material surfaces.

R2U-Net[10,11] was proposed by Alom et al. This framework utilizes the power of U-Net, residual networks and RCNN. Residual units help train deep architectures and feature accumulation through recursive residual convolutional layers ensures better feature representation for segmentation tasks. R2U-Net has better performance and results relative to U-Net in the task of saliency target detection in the field of image segmentation. In addition, the attention mechanism plays a crucial role in the detection of small defects on material surfaces by enhancing the model's ability to focus on the most relevant parts of the image, thereby improving the detection accuracy. In defect detection, the attention mechanism dynamically highlights regions of interest in the image, ensuring that the model pays more attention to potentially defective regions while ignoring extraneous background noise. This is particularly important for the detection of small, subtle defects, which are easily overlooked by conventional methods. Attention mechanisms such as self-attention and spatial attention

allow the model to learn and prioritize features that are critical to identifying defects, resulting in more accurate and reliable results. By incorporating attention mechanisms into convolutional neural networks (CNNs) or other deep learning models, researchers can improve the sensitivity and specificity of defect detection systems.

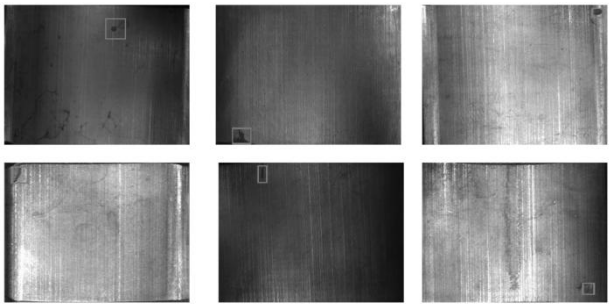


Figure 1 Small defects on the surface of the material

Tiny defects on the surface of the material are shown in Figure 1. Detecting tiny defects on the surface of a material[12,13,14] is a major challenge that is often difficult for traditional machine learning algorithms to cope with. One of the main difficulties is the subtle and small-scale nature of these defects, which can be easily masked by noise or variations in surface texture. Traditional machine learning algorithms typically rely on hand-crafted features and have limited ability to capture the complex patterns and details required to recognize such tiny anomalies. In addition, conventional methods typically require extensive preprocessing and feature extraction steps, which are not only time-consuming, but may also fail to highlight subtle differences between defective and non-defective areas. The variability of defect appearance, influenced by factors such as lighting conditions and surface reflectivity, further complicates the inspection process. Conventional algorithms lack the adaptability to work with different types of materials and defect manifestations, resulting in a high rate of false alarms and missed alarms.

In this paper, based on the R2U-Net framework and the attention mechanism, an Attention R2U-Net-based algorithm for detecting tiny defects on material surfaces is proposed. The attentional mechanism[15] selectively focuses on parts of the image that may contain defects while reducing the effect of extraneous background noise, ensuring that the network retains both critical local details and broader background information, which is crucial for recognizing small defects that may have been overlooked. Multi-scale information also allows the backbone network to analyze images at different levels of detail, thus improving its ability to detect defects of different sizes and shapes. This advancement is especially important for industries where high accuracy and early defect detection are critical, such as semiconductor manufacturing, aerospace and automotive.

This paper is structured as follows. In Section 2, we give an introduction to related work, including the basic principles of the U-Net model and the R2U-Net model and the mechanism of the attention gate. In Section 3, we present the AttR2U-Net model for detecting tiny defects on material surfaces. In Section 4, we analyze the results of the experiments and evaluate the performance of the model. Finally, Section 5 gives the conclusion.

II. RELATED WORK

A.BASIC THEORY OF U-NET AND R2U-NET (RECURRENT RESIDUAL CONBOLUTIONAL NEURAL NETWORK BASED ON U-NET)

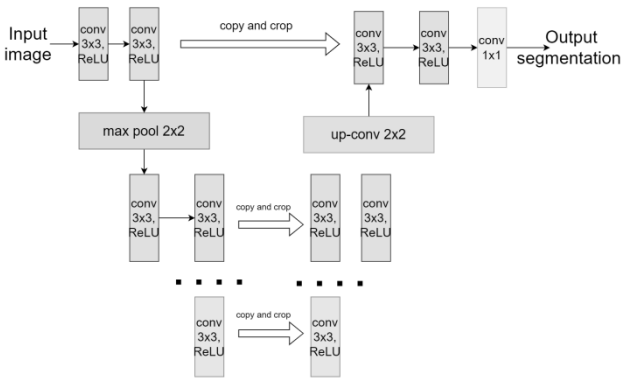


Figure 2 U-net architecture

The U-Net[16] network structure is shown in Figure 2. It has a contraction path on the left and an expansion path on the right. The contraction path follows the typical architecture of convolutional networks. It consists of repeated applications of two 3×3 convolutions. These convolutions are unfilled (i.e., "effective" convolutions), ensuring that the spatial dimensionality of the output is reduced. Each convolution is followed by a rectified linear unit (ReLU) activation function, which introduces nonlinearity into the model. A 2×2 maximum pooling operation with a step size of 2 is then applied for downsampling to halve the spatial dimensionality of

the feature map. This operation helps to capture the spatial hierarchy of the features and reduces the computational complexity. Each step in the expansion path up-samples the feature map and then performs a 2×2 convolution (called "up-convolution" or "transpose-convolution"). This operation increases the spatial dimension of the feature map while halving the number of feature channels, effectively reversing the downsampling process in the shrink path. The upsampled feature maps are then spliced with the correspondingly cropped feature maps in the contraction path. This step ensures that the network retains the high-resolution features of the previous layers, thus providing detailed contextual information. After concatenation, two 3×3 convolutions and ReLU activation are applied. This step refines the merged feature maps and enhances the network's ability to accurately localize and segment objects. In the final layer, a 1×1 convolution is used to map the feature vector to the desired number of output categories (e.g., defect or no defect). This layer effectively reduces the depth of the feature map to the number of target classes.

The U-Net architecture excels in tasks requiring precise localization and segmentation, making it particularly suitable for detecting tiny defects on material surfaces. The combination of downsampling (contracting path) and upsampling (expanding path)

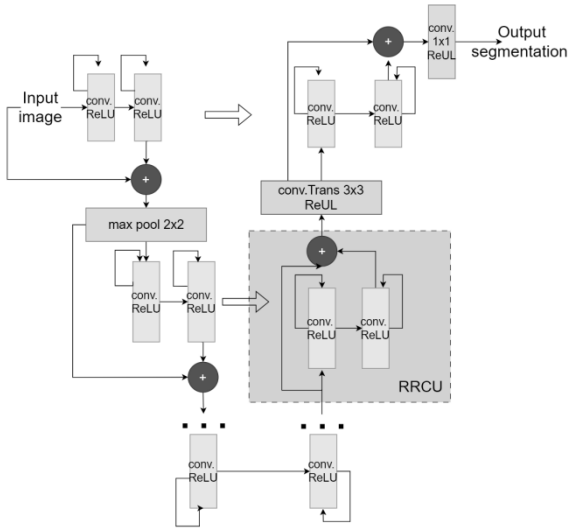


Figure 3 U-net architecture

allows the network to capture both global context and fine details, while the skip connections ensure that spatial information is preserved throughout the network.

The R2U-Net network structure[17] is shown in Figure 3, which builds upon the traditional U-Net model by integrating recurrent convolutional layers and residual connections, resulting in enhanced performance and feature representation. Its core components mainly include Recurrent Convolutional Layers (RCLs), Residual Connections, U-Net Framework. RCLs repeatedly apply convolutional operations over time steps, allowing the network to accumulate features and refine its understanding of the input data. This recurrent nature helps in capturing temporal dependencies and improving the model's ability to recognize intricate patterns within the image. Inspired by the ResNet architecture, R2U-Net incorporates residual units which help in training deeper networks by mitigating the vanishing gradient problem. These connections add the input of a layer to its output, ensuring that the essential features are retained and propagated through the network. RCL and

residual connections together form the Residual Recurrent Convolutional Unit (RRCU). In each RRCU, the input passes through a series of recurrent convolutions, and the resultant feature map is added back to the input, facilitating better feature retention and gradient flow during training. The foundational structure of R2U-Net is based on U-Net, which consists of a contracting path (encoder) and an expansive path (decoder). The contracting path captures context through convolution and max-pooling operations, while the expansive path restores spatial resolution via upsampling and concatenation with corresponding feature maps from the encoder.

Similar to U-Net, the encoding path in R2U-Net down-samples the input image, applying convolutional operations followed by ReLU activations and max-pooling layers. Here, recurrent convolutional layers replace standard convolutions, allowing the model to iteratively refine its feature representations. The decoding path up-samples the feature maps and applies up-convolutions. Recurrent convolutions in this path enhance the spatial resolution and context understanding. Skip connections from the encoding path are concatenated with the upsampled features to preserve high-resolution information.

B. ATTENTION GATES

Attention mechanisms have become integral components in various deep learning architectures, such as medical imaging. Attention gates enhance the model's ability to focus on relevant regions while suppressing irrelevant or noisy information. This capability is particularly crucial for tasks like detecting tiny defects on material surfaces, where the defects are subtle and can be easily missed. The attention gate receives feature maps from an intermediate layer of the neural network. It calculates attention coefficients for each spatial location in the feature maps. These coefficients indicate the relevance of each location with respect to the task at hand. The attention coefficients are passed through a sigmoid activation function to normalize them to a range between 0 and 1. The normalized attention coefficients are then multiplied element-wise with the input feature maps. This step amplifies the relevant features and suppresses the irrelevant ones. The resulting feature maps, now refined to highlight important regions, are passed to subsequent layers of the network for further processing.

The types of attention mechanisms mainly include self-attention, spatial attention and channel attention. Self-attention mechanisms compute the attention coefficients based on the input feature maps themselves, allowing the network to focus on different parts of the input dynamically. Spatial attention mechanisms focus on 'where' the important features are in the spatial dimensions, highlighting regions in the input image that are crucial for the task. Channel attention mechanisms focus on 'which' feature channels are important, adjusting the weights of different channels to prioritize significant features.

III. ATTENTION R2U-NET FOR SURFACE MINOR DEFECT DETECTION

Inspired by the deep residual model, U-Net and attention mechanisms, we propose recursive residual convolutional neural network with attention mechanism based on U-Net for surface minor defect detection. The Attention R2U-Net presents significant possibilities and advantages for the detection of minor surface defects, combining the strengths of recurrent convolutional layers, residual connections, and attention mechanisms. By leveraging the recurrent layers, the network can iteratively refine its feature representations, capturing intricate patterns and details essential for identifying subtle defects. The residual connections facilitate the training of deeper networks by ensuring better gradient flow, thus enhancing the

model's ability to learn complex features. Integrating attention gates into this framework further enhances its capabilities by allowing the network to focus on the

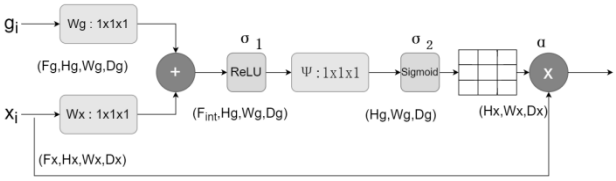


Figure 4 Attention gates architecture

most relevant regions of the input, dynamically emphasizing tiny defects while suppressing background noise. This selective attention not only improves the accuracy and reliability of defect detection but also enables the model to handle varying defect sizes and complex surface textures effectively.

A. ATTENTION GATES STRUCTURE

In the standard CNN architecture, the feature map grid is gradually downsampled to capture semantic context information. In this way, the relationship between the location and organization of features at the coarse spatial grid level model. However, it is still difficult to reduce false positive predictions for small objects with high variability. Attention gates (AGS) compute attention coefficients[18] that determine the importance of each spatial location in the feature maps. These coefficients are derived by analyzing both the features extracted from the image and contextual information from a coarser scale. By integrating AGS into a standard CNN model, not only does it not require a large number of additional model parameters, but AGS also gradually suppresses the feature responses of irrelevant background areas, so there is no need to crop ROIs between networks.

The output of AGS is the element-wise multiplication of the input feature map and the attention coefficient, which can be expressed as

$$\bar{x}_{l(i)} = x_{l(i)} \cdot \alpha_{l(i)}, \tag{1}$$

where attention coefficients $\alpha_l \in [0,1]$ identifies salient image regions and prunes feature responses, preserving task-specific activations. Each pixel vector corresponds to a single scalar attention value $x_{l(i)} \in R_{F_l}$ in which F_l corresponds to the number of feature maps in layer l. In addition, gating vector $g_i \in R_{F_g}$ is used to determine the area of focus by each pixel i. Compared with multiplicative attention, additive attention has higher accuracy, which is given by

$$q_l^{att} = \psi^T(\sigma_1(W_x^T x_{l(i)} + W_g^T g_i + b_g)) + b_\psi, \tag{2}$$

$$\alpha_{l(i)} = \sigma_2(q_l^{att}(x_{l(i)}, g_i; \Theta^{att})), \tag{3}$$

where AGS is characterised by a set of parameters Θ^{att}: linear transformations W_x^T, W_g^T and bias terms b_ψ. $\sigma_2(x)$ is the sigmoid activation function and it can be expressed as

$$\sigma_2(x) = \frac{1}{1+exp(-x)}. \tag{4}$$

Before the concatenation operation, information extracted from coarse scales is used for gating, which can merge relevant activations and eliminate irrelevant and noisy responses in skip connections. In addition, during the backward pass of AGS, gradients from background regions are down-weighted. The update rule for convolution parameters can be expressed as

$$\frac{\partial(\bar{x}_{l(i)})}{\partial(\Phi_{l-1})} = \frac{\partial(\alpha_{l(i)} f(x_{l-1(i)}; \Phi_{l-1}))}{\partial(\Phi_{l-1})}$$
$$= \alpha_{l(i)} \frac{\partial(f(x_{l-1(i)}; \Phi_{l-1}))}{\partial(\Phi_{l-1})} + \frac{\partial(\alpha_{l(i)})}{\partial(\Phi_{l-1})} x_{l(i)}. \tag{5}$$

In case of multi-dimensional AGS, $\alpha_{l(i)}$ is a vector at each grid scale. $\alpha_{l(i)}$ scales the first gradient term, ensuring that updates are more focused on relevant regions. Each sub-AG extracts and fuses complementary information to define the output of the skip connection. This approach reduces the number of trainable parameters and computational complexity. Linear Transformations are performed without any spatial support ($1 \times 1 \times 1$ convolutions) and input feature maps are downsampled to the resolution of the gating signal. To ensure that intermediate feature maps are semantically discriminative at each scale, deep supervision is applied. This approach forces attention units at different scales to influence the responses to a wide range of image foreground content. The linear transformations decouple the feature maps and map

them to a lower-dimensional space, reducing the computational complexity of AGS. AGS improve model sensitivity and accuracy for dense label predictions by suppressing feature activations in irrelevant regions. The necessity of using external

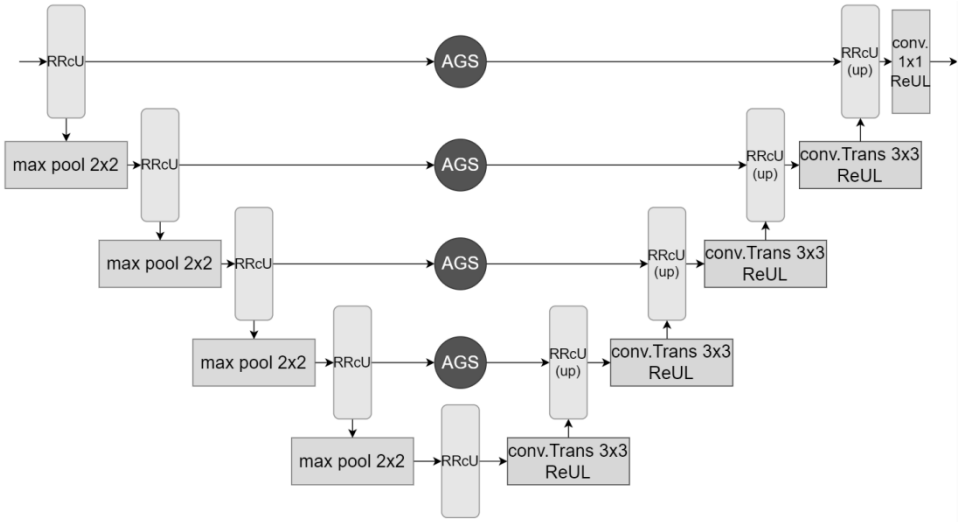


Figure 5 AttR2U-Net architecture

localization models is eliminated, simplifying the architecture while maintaining high prediction accuracy.

B. *ATTR2U-NET STRUCTURE*

The AttR2U-Net architecture, which is shown in Figure 5, combines the strengths of R2U-Net (which integrates Recurrent Convolutional Layers and Residual connections) with Attention Gates to create a powerful model for image segmentation. This combination enhances the model's ability to detect and segment small defects on material surfaces by focusing on the most relevant regions of the input image while ignoring background noise.

Recurrent Convolutional Layers (RCLs) are designed to iteratively refine feature representations through recurrent operations. They help the network capture intricate patterns by processing the input multiple times within the same layer, which is beneficial for recognizing subtle defects. Residual Connections connections allow the network to retain essential features and improve gradient flow during training, enabling deeper network architectures without the vanishing gradient problem. Integrated into the network, AGS focus the model’s attention on relevant regions of the input image, enhancing the segmentation performance by dynamically adjusting the importance of different parts of the image. The fundamental structure of U-Net, with its encoder-decoder design, is maintained. The encoder path captures context through downsampling, and the decoder path restores spatial resolution through upsampling. Skip connections between corresponding layers in the encoder and decoder paths ensure that high-resolution features are preserved.

Each block in the encoder path consists of recurrent convolutional layers followed by ReLU activations. These layers process the input image to extract features. Downsampling is performed using max-pooling layers, which reduce the spatial dimensions of the feature maps while preserving important information. Each block in the decoder path begins with upsampling the feature maps to restore the spatial resolution. Recurrent Up-Convolutional Layers refine the features after upsampling. Features from the encoder path are concatenated with the upsampled features from the decoder path. Attention gates are applied to the skip connections to filter out irrelevant information and highlight important features. A final 1×1 convolution is used to map the features to the desired number of output classes, producing the segmentation map. In addition, attention gates take input features from the encoder path and a gating signal from a coarser scale. They calculate attention coefficients, which determine the relevance of each spatial location

in the feature maps and the coefficients are normalized using a sigmoid function to produce values between 0 and 1, which are multiplied with the input features, enhancing relevant features and suppressing irrelevant ones.

In model training, the binary cross entropy loss function is used, which can be expressed as

$$L_{bce} = -\frac{1}{N}\sum_{i=1}^{N}\left[y_i \log\left(\hat{y}_i\right) + (1-y_i)\log\left(1-\hat{y}_i\right)\right], \tag{6}$$

where N is the number of samples, where each sample corresponds to a pixel. y_i is the true label of the i-th sample (pixel), with a value of 0 or 1, 0 means no defect, and 1 means defect. $\hat{y}_i$ is the probability that the i-th sample (pixel) predicted by the model is defective, and its value is between 0 and 1.

IV. EXPERIMENTS AND RESULTS

A. DATASET AND EXPERIMENTAL ENVIRONMENT

In order to verify the effectiveness of the algorithm in this paper, the magnetic tile defect dataset provided and annotated by Huang Y et al[19]. is used. This dataset contains images of common magnetic tile defects and performs semantic segmentation and annotation. The experimental environment is PyTorch 2.0.0, Python 3.8 (ubuntu20.04) and Cuda 11.8.

B. EVALUATION INDICATORS

In this paper, accuracy (AC), sensitivity (SE, also known as recall), and specificity (SP) are used to evaluate the performance of the model, and their formulas are given

$$\mathrm{AC} = \frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}}, \tag{7}$$

$$\mathrm{SE} = \frac{\mathrm{TP}}{\mathrm{TP+FN}}, \tag{8}$$

$$\mathrm{SP} = \frac{\mathrm{TN}}{\mathrm{TN+FP}}, \tag{9}$$

where TP (True Positive) is the number of samples correctly predicted as positive, TN (True Negative) is the number of samples correctly predicted as negative, FP (False Positive) is the number of samples incorrectly predicted as positive and FN (False Negative) is the number of samples incorrectly predicted as negative. Ac is the ratio of the number of correctly classified samples to the total number of samples. It indicates how accurate the model is overall. SE, also known as recall, is the ratio of the number of samples correctly predicted as positive to the number of samples actually positive. It indicates the model's ability to identify positive samples. High sensitivity means that the model can identify most positive samples, which is suitable for scenarios where you want to identify as many positive samples as possible. SP is the ratio of the number of samples correctly predicted as negative to the number of samples actually negative. It indicates the model's ability to identify negative samples.

AC is a good evaluation indicator when the positive and negative samples are balanced, but when the samples are unbalanced, the accuracy may mask the true performance of the model. SE is suitable for scenarios where you want to identify as many positive samples as possible, such as in medical diagnosis, you want to identify as many sick patients as possible. SP is suitable for scenarios where you want to misjudge negative samples as little as possible as possible, such as in security inspections, you want to misjudge normal objects as little as possible as dangerous objects. By using these indicators in combination, the performance of the model can be comprehensively evaluated, especially in different application scenarios, and the parameters of the model can be adjusted according to needs to achieve the best effect.

C. PARAMETER SETTINGS

Using images from the magnetic tile defect dataset, the training set, validation set, and test set account for 60%, 20%, and 20%, respectively.In the data augmentation stage, the images in the training set are augmented by Gaussian filtering, sharpening, and contrast adjustment.

D. COMPARATIVE ANALYSIS OF

EXPERIMENTAL RESULTS

Figure 6 is the training loss over epochs for four different models: U-Net, R2U-Net, AttU-Net, and AttR2U-Net, applied to the problem of detection of blowhole on the surface of magnetic tiles. We will analyze the four models in turn. The blue line represents the U-Net model, which starts with a relatively high loss and shows significant fluctuations during the initial epochs. Over time, the loss decreases but remains higher compared to the other models, indicating that U-Net has more difficulty stabilizing and achieving low loss in defect detection. The orange

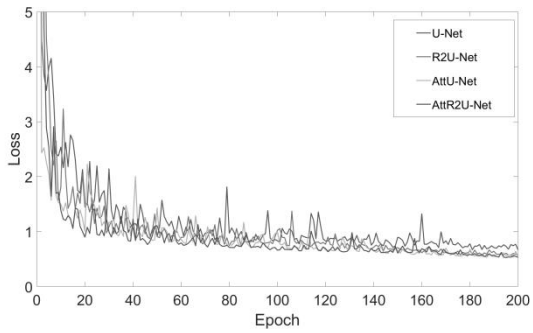


Figure 6 The training loss over epochs for four different models: U-Net, R2U-Net, AttU-Net, and AttR2U-Net.

line represents the R2U-Net model, which incorporates recurrent convolutional layers and residual connections. The initial loss is high, similar to U-Net, but it stabilizes faster and achieves lower loss values as training progresses, demonstrating better feature extraction and refinement capabilities. The yellow line represents the AttU-Net model, which integrates attention gates into the U-Net architecture. The model starts with high initial loss but shows a more rapid decrease compared to U-Net and R2U-Net, with fewer fluctuations, indicating the positive impact of attention mechanisms in focusing on relevant regions and reducing noise. The purple line represents the AttR2U-Net model, which combines the strengths of R2U-Net with attention gates. This model starts with a high loss but quickly stabilizes and achieves the lowest loss among all models, with minimal fluctuations throughout the training process.

The AttR2U-Net model stabilizes faster than U-Net and R2U-Net, indicating its ability to efficiently learn relevant features and ignore irrelevant ones from the early stages of training. AttR2U-Net achieves the lowest final loss, demonstrating superior performance in accurately detecting small defects. This highlights its effectiveness in handling complex defect patterns and subtle variations. The loss curve for AttR2U-Net shows fewer fluctuations compared to U-Net and R2U-Net, indicating more stable learning and better generalization capabilities. The combination of recurrent convolutional layers, residual connections, and attention gates in AttR2U-Net allows for iterative feature refinement, efficient gradient flow, and focused attention on defect regions. This results in enhanced feature extraction and noise suppression.

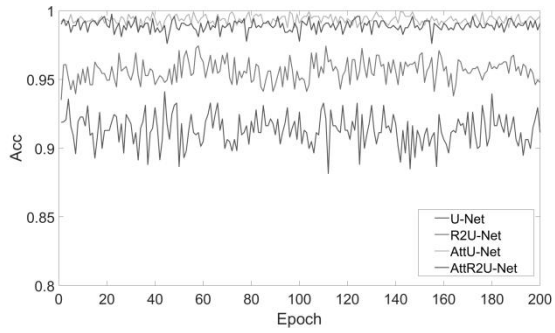


Figure 7 ACC over epochs for four different models: U-Net, R2U-Net, AttU-Net, and AttR2U-Net.

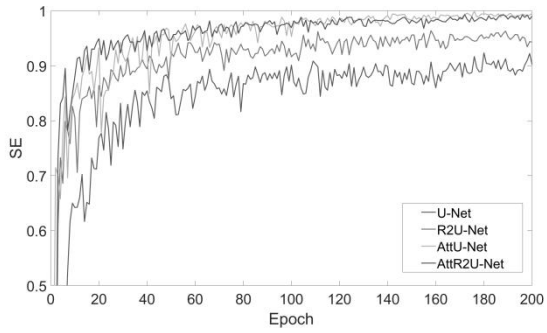


Figure 8 SE over epochs for four different models: U-Net, R2U-Net, AttU-Net, and AttR2U-Net.

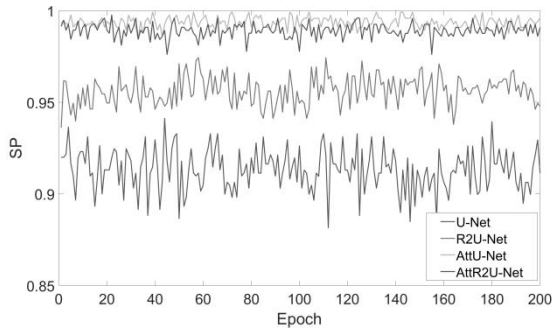


Figure 9 SP over epochs for four different models: U-Net, R2U-Net, AttU-Net, and AttR2U-Net.

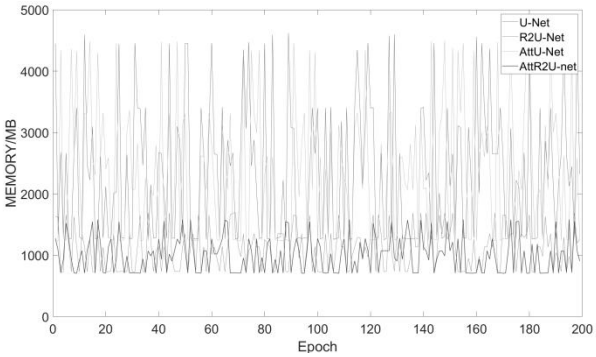


Figure 10 Computational resource loss of for four different models: U-Net, R2U-Net, AttU-Net, and AttR2U-Net.

Figure 7, Figure 8 and Figure 9 show the relationship between the number of training rounds and accuracy (AC), sensitivity (SE) and specificity (SP) of U-Net, R2U-Net, AttU-Net and AttR2U-Net when solving the problem of detecting small defects on the surface of materials. According Figure 7, U-Net has larger fluctuations compared to other models but stabilizes at a lower level of accuracy. R2U-Net stabilizes at a higher accuracy than U-Net but has larger fluctuations. AttU-Net achieves higher accuracy with less fluctuations, indicating better performance due to the attention mechanism. AttR2U-Net consistently achieves the highest accuracy with the least fluctuations, showing superior performance in accurately detecting small defects.

By analyzing Fig.8, U-Net starts with low sensitivity and gradually increases, but maintains a lower sensitivity than other models with greater fluctuations. R2U-Net has better sensitivity than U-Net and stabilizes at a higher level. AttU-Net quickly reaches higher sensitivity and maintains stable performance with less fluctuations. AttR2U-Net exhibits the highest sensitivity, indicating its excellent ability to detect true positives and consistently capture the smallest defects.

From Figure9, U-Net exhibits considerable variability, stabilizing at a lower level of specificity. R2U-Net achieves better specificity than U-Net with less fluctuation. AttU-Net achieves high specificity, maintains stability and demonstrates its ability to minimize false positives. AttR2U-Net achieves the highest specificity, demonstrating its strong performance in correctly identifying defect-free regions and reducing false positives.

Figure 10 shows the memory usage of the four models, U-Net, R2U-Net, AttU-Net, and AttR2U-Net, over the course of 200 training sessions.The U-Net model shows the highest and most volatile memory usage, often exceeding 4000 MB.R2U-Net and AttU-Net also show considerable fluctuations, but the memory usage is is usually lower than that of U-Net. In contrast, the AttR2U-Net model consistently shows the lowest memory consumption throughout the training process, with minimal fluctuations, well below 2000 MB. this suggests that the AttR2U-Net model is not only more efficient in memory usage, but also more stable during the training process, and is therefore suitable for environments where resources are limited and computational efficiency is required.Finally, we summarize the performance of different models in material surface defect detection, as shown as in Table 1. By integrating recurrent convolutional layers, residual connections, and attention gates, AttR2U-Net leverages advanced techniques to achieve the best performance in detecting tiny defects on material surfaces. This makes it an invaluable tool for applications requiring high precision and reliability in defect detection.

Table 1 Performance comparison of each model

	U-NET	R2U-NET	AttU-Net	**AttR2U-Net(our)**
ACC	0.9114	0.9478	0.9759	**0.9809**
SE	0.9023	0.9430	0.9752	**0.9803**
SP	0.9114	0.9478	0.9759	**0.9809**

V Practical application

Based on the above research results, we carry out validation application at the Long March rocket model inspection station of the pulsation production line of Shandong Hengyuan Intelligent Technology Co. Aerospace Intelligent Manufacturing Laboratory, focusing on the inspection object of the rocket model pallet base and using the Attention R2U-Net model to improve the defect identification ability, and then improve the product quality.

A. Data set construction

Considering the complexity of the production environment, a total of 5000 high-resolution images of the model rocket tray base were collected under different lighting, background noise, and material reflection conditions, which covered examples such as cracks, porosity, inclusions, and corrosion, and a variety of minor defects, and a dataset containing 5000 high-resolution images was constructed.

B. Parameter Settings

All images are adjusted to a uniform resolution of 1024 × 1024 pixels to adapt to the input size requirements of the model, and the images are labeled to distinguish between defective and defect-free regions. After that, to enhance the generalization ability and robustness of the model, the images were randomly rotated from 0 to 30 degrees to simulate defects in different directions, scaled to 80% to 120% of the original size to simulate defects of various sizes, Gaussian noise was added to the images to simulate the background noise that may be encountered in a natural production environment and the brightness, contrast, and saturation of the images were adjusted to simulate different lighting conditions. To reduce the computational complexity and focus on the shape and texture of the defects, some of the images are converted to grayscale, and histogram equalization is performed to enhance the contrast of the images to make the defects more obvious. At the same time, all images are normalized to the range of [0,1] to converge the model faster and improve the training process's stability.

C. Model Training

The detection model adopts the Attention R2U-Net model architecture based on U-Net, which significantly improves the accuracy of feature extraction through the combination of recursive convolutional layer, residual connection, and attention mechanism. A binary cross-entropy loss function is used in the model training strategy to quantify the difference between the predicted and actual labels, and the Adam optimizer is used for parameter updating. The Adam optimizer can adaptively adjust the learning rate, which effectively accelerates the convergence process of the model.

To systematically evaluate the model performance, the dataset is divided into a training set (60%), a validation set (20%) and a test set (20%). The training process is carried out in batches of 16 images, and the learning rate is reduced by 10% every 20 epochs. The training is stopped if the performance is not improved within 5 consecutive epochs to prevent the occurrence of overfitting. The hyper-parameters of the model, such as learning rate, batch size, number and size of filters in the convolutional layer, and depth of the recursive layer, were carefully adjusted by techniques such as grid search or random search; after each training epoch, the model performance was evaluated using a validation set and the key indexes, such as accuracy, sensitivity, specificity, were recorded. The possible bias or error in the model prediction was further identified by confusion matrix analysis: bias or error. During the testing process, the model was thoroughly evaluated using an independent test set to ensure that the model demonstrates high accuracy and good robustness even on unseen data.

D. Application Results

After full training and validation, the AttR2U-Net model performed excellently on the test set. In the defect detection task of the rocket model, the model achieved 98.09% accuracy, 98.03% sensitivity (recall), and 98.09% specificity. The actual verification and application results show that the AttR2U-Net model can effectively distinguish between defective and non-defective Long March rocket model tray bases, and even tiny defects can be accurately recognized.

After practical verification, the automated production line inspection process based on the AttR2U-Net model not only improves the inspection rate but also reduces human error, ensures the stability of product quality, and demonstrates the powerful potential of the model in improving the efficiency and accuracy of defect detection. At the same time, the instant feedback function of the model enables more timely adjustments in production, further reducing the defective rate and improving production efficiency. In the future, we plan to optimize the model further to suit a more comprehensive range of inspection needs and environments and explore its possible applications in

other manufacturing areas.

VI. CONCLUSION

In this paper, we introduced the AttR2U-Net model for detecting tiny defects on material surfaces, leveraging the strengths of recurrent convolutional layers, residual connections, and attention gates within the U-Net framework. Our approach enhances defect detection accuracy and reliability by iteratively refining features, improving gradient flow, and dynamically focusing on relevant regions to suppress background noise. Experimental results show that AttR2U-Net outperforms traditional U-Net, R2U-Net, and AttU-Net models, demonstrating rapid stabilization, lower final loss, and superior precision. These attributes make it particularly suitable for industrial applications where high precision in defect detection is critical. By integrating advanced deep learning techniques, AttR2U-Net provides an efficient solution for early detection of tiny defects, offering significant benefits for quality control and cost reduction in manufacturing processes. This work contributes valuable insights into the field of tiny defect detection on material surfaces.

References

[1] Chen Y, Ding Y, Zhao F, et al. Surface defect detection methods for industrial products: A review[J]. Applied Sciences, 2021, 11(16): 7657.

[2]Bhatt P M, Malhan R K, Rajendran P, et al. Image-based surface defect detection using deep learning: A review[J]. Journal of Computing and Information Science in Engineering, 2021, 21(4): 040801.

[3]Tabernik D, Šela S, Skvarč J, et al. Segmentation-based deep-learning approach for surface-defect detection[J]. Journal of Intelligent Manufacturing, 2020, 31(3): 759-776.

[4]Cumbajin E, Rodrigues N, Costa P, et al. A systematic review on deep learning with CNNs applied to surface defect detection[J]. Journal of Imaging, 2023, 9(10): 193.

[5]Chen X, Chen J, Han X, et al. A light-weighted CNN model for wafer structural defect detection[J]. IEEE access, 2020, 8: 24006-24018.

[6]Nooralishahi P, Ibarra-Castanedo C, Deane S, et al. Drone-based non-destructive inspection of industrial sites: A review and case studies[J]. Drones, 2021, 5(4): 106.

[7]Zhang Y, Zhang J, Wang Q, et al. Dynet: Dynamic convolution for accelerating convolutional neural networks[J]. arXiv preprint arXiv:2004.10694, 2020.

[8]Zhang D, Li F, Ding X, et al. Small Object Detection via Precise Region-Based Fully Convolutional Networks[J]. Computers, Materials & Continua, 2021, 69(2).

[9]Siddique N, Paheding S, Elkin C P, et al. U-net and its variants for medical image segmentation: A review of theory and applications[J]. IEEE access, 2021, 9: 82031-82057.

[10]Ma S, Tang J, Guo F. Multi-task deep supervision on attention R2U-net for brain tumor segmentation[J]. Frontiers in Oncology, 2021, 11: 704850.

[11]Alom M Z, Hasan M, Yakopcic C, et al. Recurrent residual convolutional neural network based on u-net (r2u-net) for medical image segmentation[J]. arXiv preprint arXiv:1802.06955, 2018.

[12]Li D, Li Y, Xie Q, et al. Tiny defect detection in high-resolution aero-engine blade images via a coarse-to-fine framework[J]. IEEE Transactions on Instrumentation and Measurement, 2021, 70: 1-12.

[13]Zhang X, Cheng L, Liu Y, et al. A review of non-destructive methods for the detection tiny defects within organic insulating materials[J]. Frontiers in Materials, 2022, 9: 995516.

[14]Ding R, Dai L, Li G, et al. TDD‐net: a tiny defect detection network for printed circuit boards[J]. CAAI Transactions on Intelligence Technology, 2019, 4(2): 110-116.

[15]Zhao Q, Liu J, Li Y, et al. Semantic segmentation with attention mechanism for remote sensing images[J]. IEEE Transactions on Geoscience and Remote Sensing, 2021, 60: 1-13.

[16] Du G, Cao X, Liang J, et al. Medical Image Segmentation based on U-Net: A Review[J]. Journal of Imaging Science & Technology, 2020, 64(2).

[17]Khankeshizadeh E, Mohammadzadeh A, Moghimi A, et al. FCD-R2U-net: Forest change detection in bi-temporal satellite images using the recurrent residual-based U-net[J]. Earth Science Informatics, 2022, 15(4): 2335-2347.

[18]Valvano G, Leo A, Tsaftaris S A. Learning to segment from scribbles using multi-scale adversarial attention gates[J]. IEEE Transactions on Medical Imaging, 2021, 40(8): 1990-2001.

[19]Huang Y, Qiu C, Yuan K. Surface defect saliency of magnetic tile[J]. The Visual Computer, 2020, 36(1): 85-96.

[20]Hou Q, Wang Z, Tan F, et al. RISTDnet: Robust infrared small target detection network[J]. IEEE Geoscience and Remote Sensing Letters, 2021, 19: 1-5.

[21]Song Y, Gao L, Li X, et al. A novel robotic grasp detection method based on region proposal networks[J]. Robotics and Computer-Integrated Manufacturing, 2020, 65: 101963.

[22]Sun W, Wang R. Fully convolutional networks for semantic segmentation of very high resolution remotely sensed images combined with DSM[J]. IEEE Geoscience and Remote Sensing Letters, 2018, 15(3): 474-478.

[23]Zunair H, Hamza A B. Sharp U-Net: Depthwise convolutional network for biomedical image segmentation[J]. Computers in biology and medicine, 2021, 136: 104699.

[24]Zhang Z, Wu C, Coleman S, et al. DENSE-INception U-net for medical image segmentation[J]. Computer methods and programs in biomedicine, 2020, 192: 105395.

[25]Futrega M, Milesi A, Marcinkiewicz M, et al. Optimized U-Net for brain tumor segmentation[C]//International MICCAI brainlesion workshop. Cham: Springer International Publishing, 2021: 15-29.

About the authors

Yongwen Zhang was born in 1983. He received t he master's degree from Guangxi University. No w he is studying for a Ph.D. degree in Mechanica l Engineering at Xi'an Jiaotong University. His re search interests include the application of artifici al intelligence engineering, the research and prac tice of industrial internet, and the research of key technologies for intelligent control and manage ment of production lines. (Email:yongwen.zhang @ytever.com)

Dongbin Ji, born in 1988, is a master's degree student of Industrial Engineering at Tsinghua University. His main research interests include the application of artificial intelligence technology in industrial scenarios, especially in industrial field image recognition scenarios, model-based system engineering standards and practices, process optimization and manufacturing efficiency improvement based on manufacturing data. (Email: dongbin.ji@ytever.com)

Jun Zhou, born in 1971, M.S., Fudan University, his research interests include research on key technologies of industrial internet platform, application of 5G and other new generation information technologies in industry, research and practice of model-driven digital twin and digital mainline methodology. (Email: jun.zhou@ytever.com)

Xin Wen, born in 1995, has a bachelor's degree from Shenyang Ligong University. His research interests include the design and optimization of lean production systems, the implementation of quality improvement strategies, and the data analysis and decision support of production processes. (Email:xin.wen@ytever.com)

基于过程挖掘的多维度过程分析方法

汤珺雅*，于青云，李莉

摘　要：过程分析通过对过程模型特征进行分析来识别过程中的偏差、瓶颈等问题，是揭示过程中存在的问题、确定优化空间、提高关键环节效率的关键。然而，当前的过程分析方法集中在操作流程层级，忽视了其他系统层级的影响，且多从孤立视角出发，缺乏系统性。针对上述问题，本文提出了一种基于过程挖掘的多维度过程分析方法。首先，设计了一个多维度过程分析框架，涵盖任务、人员和时间三个独立维度及其交叉维度，以系统化方式展现过程信息及其交互。其次，在一个交通控制系统设计过程上进行了案例研究，展示了本框架在任务、时间、人员维度上的分析能力，为决策提供可解释性支持。研究证实，该方法能有效识别过程中的瓶颈、资源分配状况，以及人员参与度等，从而为过程优化和管理提供依据。

关键词：过程挖掘；知识提取；过程分析

A Multi-dimensional Process Analysis Method Based on Process Mining

Junya Tang*, Qingyun Yu, Li Li

Abstract: Process analysis identifies deviations, bottlenecks, and other problems by analysing the characteristics of the process model. It is the key to revealing existing issues in the process, determining optimisation space, and improving the efficiency of critical links. However, current process analysis methods are too focused on the operational process level, ignore the impact of resource levels, and mostly start from an isolated perspective and lack systematicity. In response to the above problems, this paper proposes a multi-dimensional process analysis method based on process mining. First, a dimensional process analysis framework is designed, covering the three independent dimensions of task, people and time and their intersecting dimensions to systematically present process information and their interactions. Secondly, a case study was conducted on the design process of a traffic control system, demonstrating the analytical capabilities of this framework in the task, time, and personnel dimensions and providing interpretable support for decision-making. Research has confirmed that this method can effectively identify bottlenecks, resource allocation status, and personnel participation, providing a basis for process optimisation and management.

Key words: process mining, knowledge extraction, process analysis

1　引言

随着互联网技术的发展，各行业都希望通过信息化提升竞争力，然而传统的生产及经营管理方式依旧限制了企业的自我提升[1]。通过对业务过程进行挖掘、诊断、分析来提升和巩固自身的竞争力，以此面对来自产品质量、成本、服务满意度等方面的市场压力成为核心途径之一[2]。过程挖掘是在此背景下发展起

来的一门融合管理科学和数据科学的交叉学科。过程挖掘以传统的管理科学中的生产管理理论和工作流管理技术为基础，引入数据挖掘、机器学习和过程建模等数据科学技术，通过对历史数据的分析，实现对过程的管理和优化[3]。

经典的过程挖掘技术是从事件日志中挖掘有效信息来发现、改进、预测实际过程。随着企业对过程挖掘的重视，对于过程挖掘结果的分析得到了关注。过程分析在过程挖掘基础上对过程模型特征进行分析，并识别出过程中的偏差、瓶颈及其他问题，是揭示过程中存在的问题、确定优化空间、提高关键环节效率的关键[4]。

尽管过程挖掘理论研究不断成熟，应用也逐步增多，但在过程分析方面仍有待加强，目前对于过程分析的研究中存在两个局限：（1）对过程的分析主要集中于操作流程层级，忽视了其他系统层级的影响（例如资源层级）。（2）多以孤立视角对过程进行分析，鲜少关注不同视角的过程分析之间的联系，缺乏综合不同视角的系统分析。

针对上述局限，本文面向非结构化过程文档，提出一种基于过程挖掘的多维度过程分析方法，主要贡献为：（1）基于过程模型，设计一种多维度的过程分析框架，系统地呈现过程各维度信息及相互之间的交互。（2）以交通控制系统设计过程为案例，基于提出的分析框架，对任务、时间、人员维度进行分析，为可解释性决策提供支持。

本文后续章节安排如下：第 2 章介绍过程挖掘与过程分析的相关工作；第 3 章介绍了所提出的多维度过程分析方法；第 4 章进行了案例研究并对结果进行分析；第 5 章对全文进行总结。

2 相关工作

2.1 过程挖掘方法

过程挖掘一般指从过程数据中建立过程模型并对其进行分析的技术。过程建模是过程挖掘的主要任务，也是当前过程管理的重点。传统的过程挖掘的方法视角局限于平面图形模式下的路径，通常是Workflow Nets（WFN），不适合具有灵活工作流的过程，比如工业生产和产品研发[5]。随着事件日志流的出现，一些在线检测方法被提出[6]。Burattin等[7]提出了一种在线过程模型发现方法，以提供关于概念漂移的有价值信息。R G de Sousa等[8]提出了一种基于在线设置的轨迹聚类综合方法。Zaman R等[9]提出了一种在线过程挖掘框架，以处理大量事件日志交互时的GDPR违规问题。Ferilli S等[10]描述了WoMan（工作流管理）框架的增量过程挖掘方法，用于适应和微调现有模型。Schuster D等[11]提出了一种增量发现和扩展算法，以获得更好的过程模型。Armas Cervantes A等[12]提出了一种交互式和增量过程模型修复方法，允许用户根据视觉指导修复模型。这些方法试图通过过程挖掘技术来适应、微调或修复现有模型，而不是专注于发现正在进行的过程。这些增量过程挖掘方法在一些特定问题上表现良好，但多面向结构化数据。Junya等

[13-15]面向非结构化数据，提出了基于知识挖掘的增量过程挖掘方法，本研究在该工作的基础上进一步深入。

2.2　基于过程挖掘的过程分析

传统的过程分析通常关注操作流程层面，图模型是常用的方法之一。Wil M.P. van der Aalst 等[16]将图模型和数学模型相结合，利用 Petri Net 模型和过程仿真来分析复杂业务过程。Phalp 等[17]利用图模型度量过程中的行为和交互的相关性分析业务过程。与传统的过程分析方法有所不同，基于过程挖掘的过程分析关注更多视角，例如过程性能。Park 等[18,19]从工作负荷和工作延误情况对过程性能进行分析，并进一步针对制造过程中的瓶颈问题，提出评估分析方法。Knoll 等[20]从控制流和性能视角出发，将传统价值流图分析与过程挖掘相结合，为过程改进提供决策支持。Rebge 等[21]从异常角度出发，通过系统分析识别过程的常规行为和异常行为。上述过程分析方法在不同行业中得到了应用，但其存在系统性不足的问题，多数方法从单一系统层级出发，忽略了其他系统层级的影响，难以将各孤立视角的过程挖掘结果进行关联分析。

3　多维度过程分析方法

基于过程挖掘的多维度过程信息分析框架如图 1 所示。

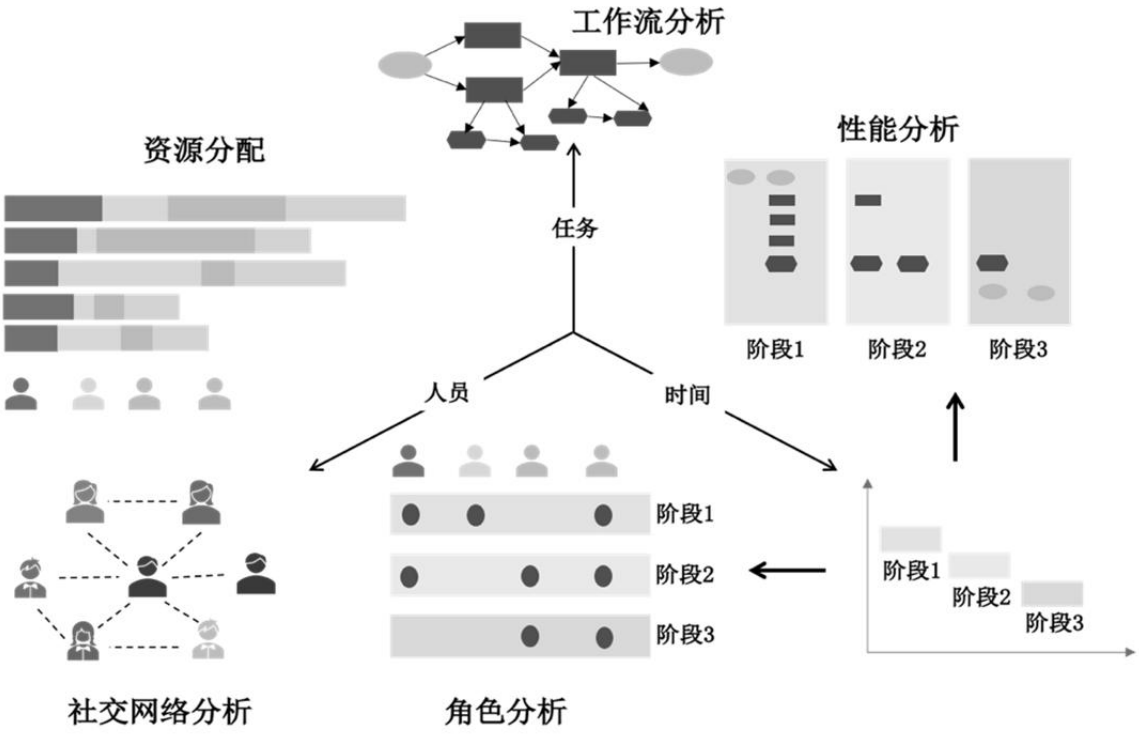


图1　多维度过程分析框架

根据图 1，基于过程挖掘的多维度分析框架包括三个独立维度：任务维度从工作流层面对过程进行分析；人员维度：从社交层网络层面对过程进行分析；时间维度：从阶段层面对过程进行分析。

上述三个维度相互交叉，形成三个交叉维度：任务与时间维度交叉，可以挖掘任务的持续时间、任务的等待时间等；人员与时间维度交叉，可以挖掘人员参与过程的时间、承担的工作量等；任务与人员维度交叉，可以挖掘过程中的资源分配情况等。

3.1 任务维度

任务维度通过挖掘任务之间的关联性、任务的时间频率和任务持续的相对周期，可以发现任务设置、任务分配的合理性以及任务执行中的不足之处，为过程改进和提升提供支持。

3.1.1 任务关联性分析

有关联的任务通常会在相同或相近的文档中被提及，因此可以通过计算过程文档中两个任务共同出现的频率来估计任务之间的关联程度。在以往工作中研究了面向非机构化过程文本的知识提取方法，通过适应性主题模型对文档进行粗粒度的知识提取[13-15]，在该方法的基础上计算任务关联性。

假设t_i和t_j是过程中的两个任务，h_i和h_j是与两个任务相关的主题。文档$d \in D$，文档d中的单词分布为V_d，t_i和t_j在文档d中出现的频率通过其相关主题h_i和h_j在文档d中出现的概率来估计。主题h_i和h_j在文档d中出现的概率为$P(h_i|V_d)$和$P(h_j|V_d)$可以通过已有工作中提出的适应性主题模型计算得到。t_i和t_j的关联程度为其在整个文档集D中的共现频率，其中文档集D的大小为N，计算方法如公式（1）所示：

$$RS(t_i, t_j) = \frac{\sum_{d=1}^{d=N} P(h_i|V_d)P(h_j|V_d)}{N} \tag{1}$$

3.1.2 任务时间频率和相对周期分析

任务和时间维度交叉，可以分析任务的执行频率在时间上的分布，以及各任务在整个过程中的相对周期。将整个过程周期划分为若干个时间段，令t_i为过程中的一个任务，h_{t_i}为任务相关的一个主题，文档$d \in D$，文档d中的单词分布为V_d，h_{t_i}在文档d中出现的可能频率为$p(\mathrm{h}_{t_i}|V_d)$。相应的时间段记为T，$|T|$表示时间段的长度。定义函数$f(d,T)$，若文档d的时间戳在时间段T内，则$f = 1$，否则$f = -1$。任务h_{t_i}在时间段T内的时间频率如公式（6.2）所示：

$$TF(h_{t_i}, T) = \frac{\sum_{d \in D} p(h_{t_i}|V_d) f(d,T)}{|T|} \tag{6.2}$$

任务与时间维度交叉也可计算任务在整个过程中的相对周期，为任务持续时间与整个过程持续时间的比值。相对周期的计算较为简单，但其充分反映了各任务消耗的时间在整个过程中的占比。

3.2 人员维度

人员维度关注社交网络、角色担任和人力资源分配，辅助对人员的合理分配。

3.2.1 社交网络分析

社交网络反映过程中参与人员之间的关系、交互程度，以此为依据可以对参与者组织结构进行推断。两个参与者的交互程度通过同时参与执行某项活动、彼此之间的交流次数等指标进行度量。基于过程中执

行者之间的交互，通过对网络图的聚类，可以进一步将相近的人员归为统一类别，即发现人员的组织结构。

3.2.2　角色分析

角色分析是基于参与人员的交互情况来分析参与者担任的角色。在过程中，认为执行相同或相似活动的人员在技能上具有相似性，可以认为担任同一类型角色。通常考虑三个层次的角色：

（1）一级领导者（First_leader）：对内负责指导整个内部成员的工作，对外负责与外部人员的联络和沟通。

（2）二级领导者（Second_leader）：对内负责监督一级领导者的决策的执行。

（3）执行者（Conductor）：负责具体的各项活动的执行。

根据上述三个角色设定，给出如下定义：

P：所有包括在社交网络中的过程参与人员的合集；

$nei(p)$:社会网络中与参与者p直接相连的参与者集合；

$coor(p)$:和参与者p具有相同角色的参与者集合；

$w(p,p')$:任意两个参与者之间的交互强度；

$fr(\,)$:计算一组参与者中的具有功能的角色数量；

不同角色在社交网络中的交互也会呈现出相应的特点。一级领导者与组织内和组织外均有较强的交互，根据该特性，一个参与者是一级管理者的概率估计如公式（2）：

$$First(p)=\frac{fr(nei(p)-coop(p))}{fr(P)}*\sum_{p'\in nei(p)-coor(p)} w(p,p') \tag{2}$$

二级领导者与一级领导者和组织内其它人员有较强的交互，而执行者与一级领导者呈现弱交互，与二级领导者呈现较强的交互，与组内其它执行者的交互情况视任务而定，根据该特性，一个参与者是二级管理者的概率估计如公式（3）：

$$Second(p)=\sum_{p'\in nei(p)\cap coor(p)} w(p,p') \tag{3}$$

其中社交网络中具有最高$Second(p)$值的参与者为二级领导者，如公式（4）：

$$Second_leader=\max_{p\in C} Second(p) \tag{4}$$

3.2.3　资源分配分析

人员和任务维度的交叉可以分析不同参与人员在任务中的参与度。合理的人力资源分配可以有效提高工作效率，降低人力成本。一种人力资源分配方案是将参与人员分配到与其职位或专业相匹配的任务中，但该方案并没有考虑到参与者在过往过程执行中的表现。因此，另一种分配方案从过往相似过程中分析其人力资源的分布情况，并以此作为新任务人力资源分配的依据。

3.3　时间维度

时间维度关注过程中被执行任务和其参与人员的时间行为，其中包括被执行任务的持续时间、等待时

间和中断时间；任务参与人员的时间频率等。时间维度分析用于挖掘在过程执行中的不规则任务执行、参与人员在不同时间的参与度等。

4 案例研究

4.1 案例背景

本研究在一个交通控制系统设计过程上进行案例研究。该设计过程的任务是设计一种交通控制系统来缓解高速公路上的交通堵塞，并且将该设计成果整理出论文进行发表。在整个设计过程中，参与者使用电子邮件作为主要的沟通方式，所有活动的执行均在邮件中进行说明。实验数据集是从该交通波项目中收集到的一组电子邮件。在整个设计过程中，所有参与者均向一个特定的公共地址发送邮件副本，记录过程的执行情况，最终有 569 封电子邮件保存在 Outlook 中，每封电子邮件都包含了设计任务的信息。本研究将根据所提出的框架对该案例进行过程挖掘和分析。

4.2 数据预处理

设计过程的数据保存于公共地址的邮箱中，从 Outlook 中导出 XML 格式的数据，在本文中，考虑的非结构化数据为文本数据。本文的案例研究主要针对的是跨度为 23 个月的设计过程数据，数据由参与者之间的邮件组成，包括时间、标题、收发人和邮件内容，邮件内容由设计过程中的每个任务的执行组成，包括执行时间、执行人、执行地点等，具备开展过程挖掘研究的可能性。经过对无效邮件的过滤，本文最终保留 357 封邮件作为研究对象。

经过初步过滤后保留的邮件数据需要进行进一步的预处理，为后续过程知识的提取进行数据准备，需要完成对邮件数据的标记和分句。邮件数据的标记如下：

Subject id：邮件主题编号，在本研究中，按照邮件主题进行实例（case）的划分，将同一个 subject id 下的邮件中所提取的事件归于同一个实例；

Subject description：邮件主题描述；

Email id：邮件编号；

Timestamp：邮件时间戳；

People id：人员编号。在本研究中，用编号代替人员的姓名；

People type：人员类型，分为发件人、收件人和抄送人；

Body：邮件主体内容；

Sentence：句子；

对于邮件主题部分，按照标点符号对其进行分句。进行标记和分句后的邮件数据如图所示：

```
▼<Process description="Ants transportation system tagged">
 ▼<Subject description="(To Prof. Lim, Dr. Liaw, Prof. Lu, Dr. Liu) DCC FTS Group 5 Progress Information" id="0">
  ▼<Email id="0">
     <Class>0</Class>
     <Topics>topic</Topics>
     <Timestamp>2011:03:10 10:05:34</Timestamp>
    ▼<Originator>
       <People id="0" type="sender">Zhou Quan-周全</People>
       <People id="1" type="to">Liu Ying</People>
       <People id="0" type="to">Zhou Quan-周全</People>
       <People id="2" type="to">squall_boo1989@hotmail.com</People>
       <People id="3" type="to">blueshero_u@hotmail.com</People>
       <People id="4" type="to">koh weiru</People>
       <People id="5" type="to">zhaoyufeng925@hotmail.com</People>
       <People id="6" type="to">mz_sjz@hotmail.com</People>
       <People id="7" type="to">Koh Wei Ru</People>
       <People id="8" type="to">Boo Jun Loong</People>
       <People id="9" type="to">Cheong Yit Fung Frederick</People>
       <People id="10" type="to">Wang Chao</People>
       <People id="11" type="to">Ma Zheng</People>
       <People id="12" type="to">Zhao Yufeng</People>
       <People id="13" type="to">Faizan Abid</People>
       <People id="14" type="to">faizan.abid@gmail.com</People>
       <People id="15" type="to">lukewangchao@gmail.com</People>
       <People id="16" type="to">zhouquan2003@hotmail.com</People>
       <People id="17" type="to">Lim Seh Chun (Deputy Dean, Engineering)</People>
       <People id="18" type="to">Liaw Hwee Choo</People>
       <People id="19" type="to">Lu Wen Feng</People>
       <People id="20" type="cc">Lim E C, Eunice</People>
       <People id="21" type="cc">Pang Sze Dai</People>
    </Originator>
     <Importance>0</Importance>
     <Body> This is Zhou Quan from DCC FTS Group 5. Koh Wei Ru and me are currently the leaders of this group. I am writing to you on Prof. Lim's request to report the progress of our
     group. Our group currently has 8 members, making it the largest group in DCC FTS. Among the 8 members, there are 5 ME and 3 EE Yr 2 undergraduates. The following is the complete
     contact list of all the current group members: For better communications between you and us, I have copied all the group members' email addresses in the receiver list of this
     email. Our group was initially formed in the last semester by the 5 ME students based on our common passion and interest on aeronautical engineering. Therefore, when we first
     tried to shape the project, we targeted on aeronautical aspect, specifically, flapping-wing aircrafts and wing-in-ground aircrafts. I have attached with this email a summary of
     our meeting on 07/03/2011, this Monday. This detailed summary will be able to give you a clear picture about our latest progress after deciding to redefine our problem. The issue
     now is that among group members there are different ideas. For our next meeting this Friday, we would like to discuss, persuade and must reach a common problem to work with. Once
     we agree with a common problem and the idea of individual transportation system is adopted, the concept paper should be able to be generated very soon. </Body>
    ▼<TaggedBody>
       <Sentence>This DT is VBZ Zhou NNP Quan NNP from IN DCC NNP FTS NNP Group NNP 5 CD . . Koh NNP Wei NNP Ru NNP and CC me PRP are VBP currently RB the DT leaders NNS of IN this DT
       group NN . . </Sentence>
       <Sentence>I PRP am VBP writing VBG to TO you PRP on IN Prof. NNP Lim NNP 's POS request NN to TO report VB the DT progress NN of IN our PRP$ group NN . . </Sentence>
       <Sentence>Our PRP$ group NN currently RB has VBZ 8 CD members NNS , , making VBG it PRP the DT largest JJS group NN in IN DCC NNP FTS. . </Sentence>
       <Sentence>Among IN the DT 8 CD members NNS , , there EX are VBP 5 CD ME NNP and CC 3 CD EE NN Yr NN 2 CD undergraduates NNS . . </Sentence>
       <Sentence>The DT following VBG is VBZ the DT complete JJ contact NN list NN of IN all DT the DT current JJ group NN members NNS : : For IN better JJR communications NNS between
       IN you PRP and CC us PRP , , I PRP have VBP copied VBN all PDT the DT group NN members NNS ' POS email NN addresses NNS in IN the DT receiver NN list NN of IN this DT email NN
       . . </Sentence>
       <Sentence>Our PRP$ group NN was VBD initially RB formed VBN in IN the DT last JJ semester NN by IN the DT 5 CD ME NNP students NNS based VBN on IN our PRP$ common JJ passion NN
       and CC interest NN on IN aeronautical JJ engineering NN . . </Sentence>
```


图 2 标记和分句后的邮件数据

4.3 多维度案例过程分析结果

4.3.1 任务维度分析结果

（1）任务关联性分析结果

在已有的研究基础上，本案例构建的过程模型包含七个顶层任务：“概念论文与团队确定”、“项目提案”、“交通运输系统设计”、“系统仿真”、“论文提交与展示”、“车辆确认与视频展示”以及“整体程序优化”。图 3 直观展现了这些任务间的关联强度，其中“项目提案”（任务 2）与其他任务关联最为密切，而“概念论文与团队确定”（任务 1）的关联度最低。此结果反映了任务 2 作为项目任务的核心地位，而任务 1 在项目初始阶段完成团队组建后，其后续影响减弱，与实际项目管理逻辑相符。此外，任务 3、4 和 6（“交通系统设计”、“系统仿真”、“车辆确认与视频展示”）显示了紧密的关联性，这三大任务分别对应设计、模拟与实施的不同阶段，按序推进，相互依存，其内在联系在图 3 中清晰可见，完全契合项目实施的真实流程。

（2）任务时间频率与相对周期分析

顶层任务的时间频率分析如图 4 所示。任务 1（概念论文与团队确定）与任务 2（项目提案）同步启动，并在前两个月内完成，奠定了项目的基础。随后，自第三个月起，进入执行阶段，核心任务如交通运输系统设计（任务 3）、系统仿真（任务 4）、车辆确认与视频展示（任务 6）、以及整体程序优化（任务 7）依次展开。其中，任务 3 和任务 4 分别跨越 8 和 10 个周期，任务 6 执行时间长达 16 个周期，但经历了一次 15 天的中断。任务 7 在第 38 个时间点启动，持续至第 45 个时间点。特别地，论文提交与展示（任务 5）贯穿项目始终，与主线任务并行。任务 6 的执行状态出现偏差，需深入分析其原因，以优化时间和资源管

理。这一精炼概述突出了项目管理的关键节点和异常情况，为后续改进提供了方向。

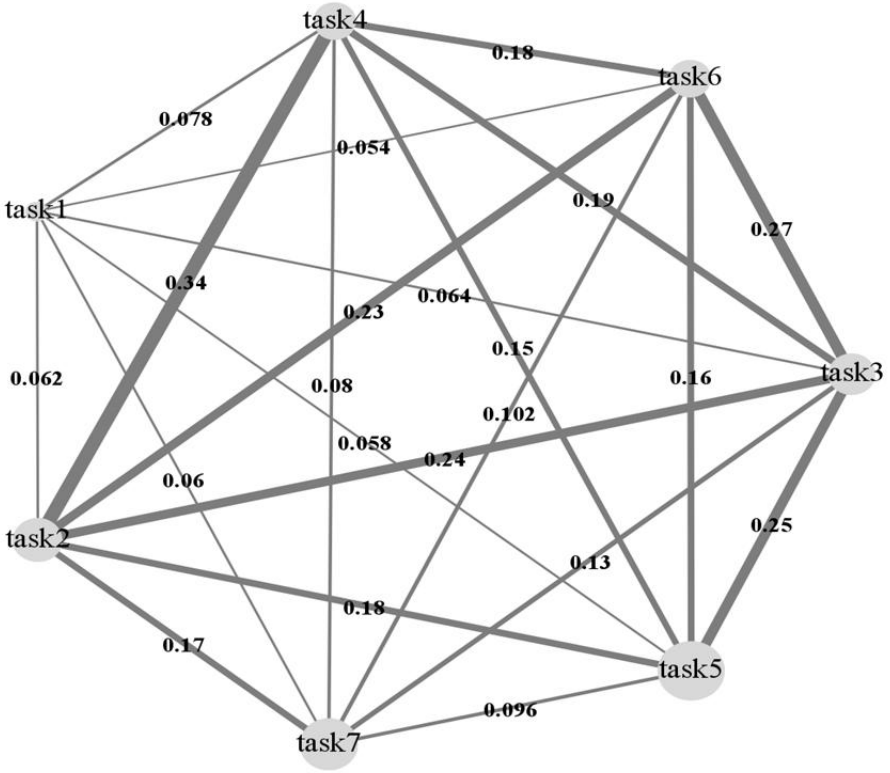


图 3 任务之间的关联性分析

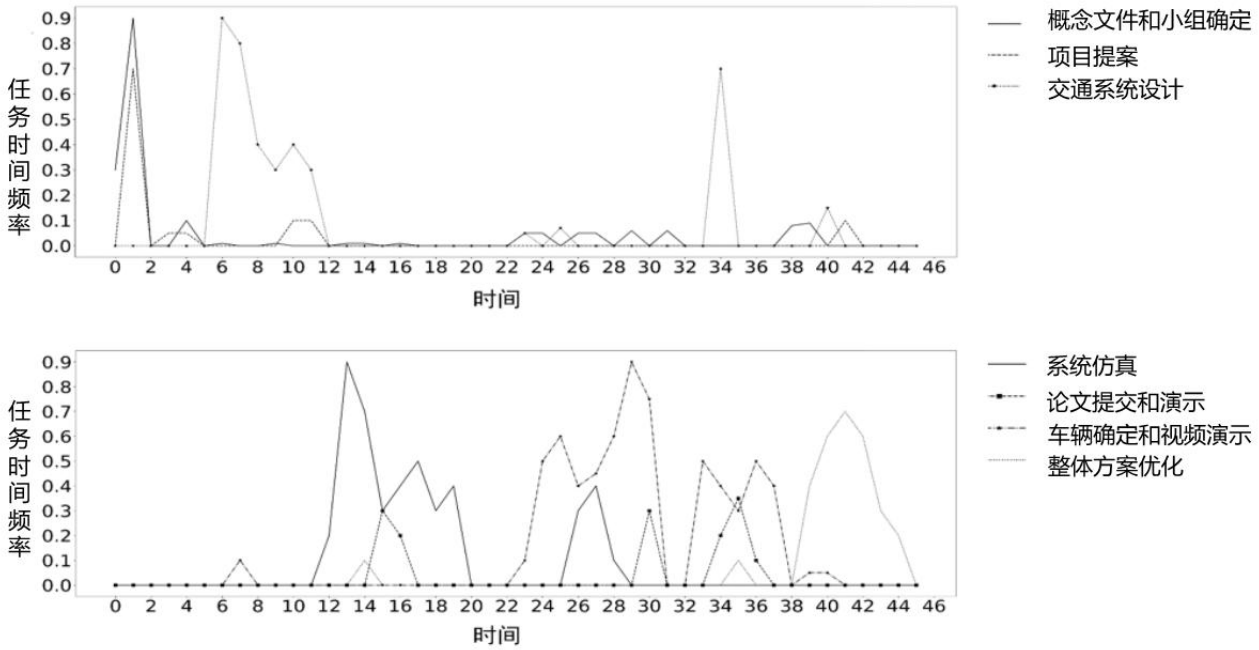


图 4 任务时间频率分析

顶层任务的相对周期分析如图 5 所示。任务 6（车辆确认与视频展示）与任务 4（系统仿真）分别占据项目周期的约三分之一和四分之一，揭示了这两项任务的复杂性和关键性。它们可能是项目的关键路径，

任何延迟都将严重影响整体进度。深入分析这两任务，关注资源分配、人员技能、技术难题及外部因素，对于识别并解决瓶颈至关重要。决策聚焦于此，不仅优化当前项目，也为未来项目管理积累宝贵经验，避免重复错误，提升整体效率和成功率。

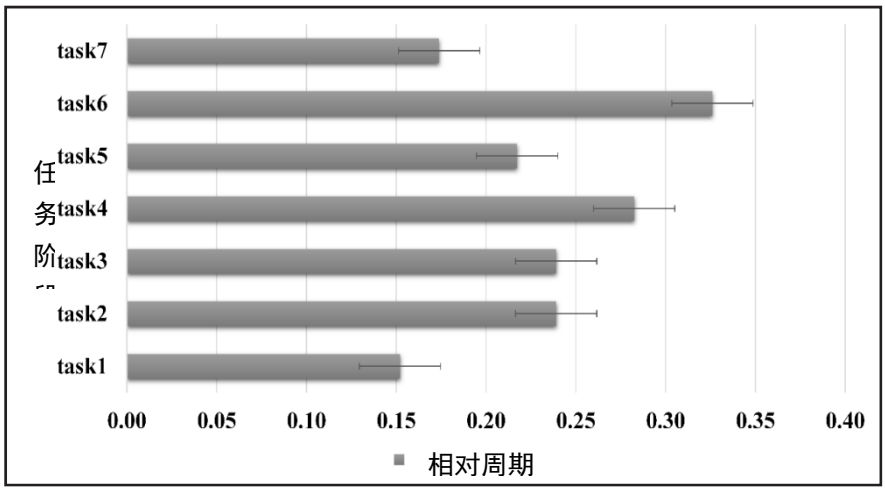
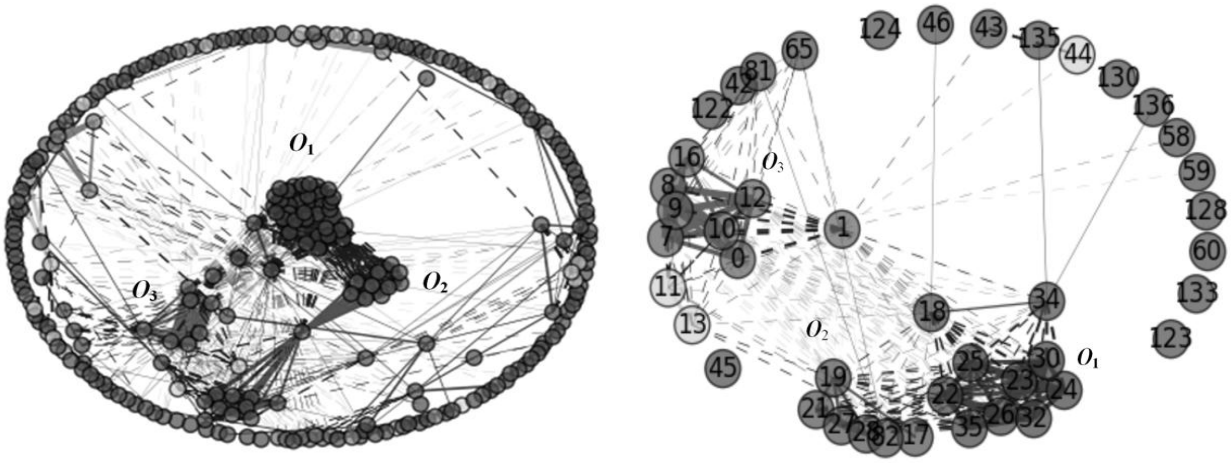


图 5 任务相对周期分析

4.3.2　人员维度分析结果

（1）社交网络分析

以交通波设计项目为案例，根据同时参与执行共同事件和进行互动为指标，对该设计过程的所有参与人员的社交网络进行分析。图 6 描述了该过程参与者的社交网络，该项目总共的涉及人员有 200 多个，包括项目主持团队的核心人员和在该项目执行过程中参与的外部人员。图 6 显示了参与者之间的互动，参与者表示为社交网络中的节点，参与者之间的交互表示为节点之间的边，交互的强度通过边的权重来反映。通过聚类方法将社区图中的所有参与者分为不同组织，相同的派中的参与者用相同的颜色标记，红色节点代表独立的参与者。



（a）　　（b）

图 6 社交网络分析

根据图 6 可以看出，在该设计过程中的参与者主要来自三个组织，分别标记为O_1、O_2和O_3，其中O_1中的人数最多，O_3中的人数最少。通过对参与者进行筛选，去除一些参与度低的人员，O_1和O_2中的人数显著减少，O_3中的人数基本稳定。这三个组织的类型解释了该现象，O_3为主持该设计过程的核心人员，对该过程的参与度高，而O_1和O_2中为外部人员，部分外部人员对过程的参与度低。这与实际情况具有高度的一致性。

（2）角色分析

角色分析的结果如图 7 所示，其中较大的节点表示一级和二级领导者。其中有四个参与者被归类于一级领导者，分别为 P_1、P_18、P_19 和 P_34，三个参与者被归类于二级领导者，P_23、P_21 和 P_0 分别为Q_1、Q_2和Q_3的二级领导者。从图中可以看出四个一级领导者在三个组织之间的交互起到了关键作用，根据参与者的信息记录，P_1、P_18、P_19 和 P_34 是负责不同子项目的教授，P_1 是负责该交通波项目的教授，P_0 为该项目的学生负责人，角色分析的结果与实际的担任的角色相符合的，对过程参与者的角色分析可以明确各个参与者在该过程中的职责，以及不同角色之间的互动模式，为人员的合理分配提供支持。

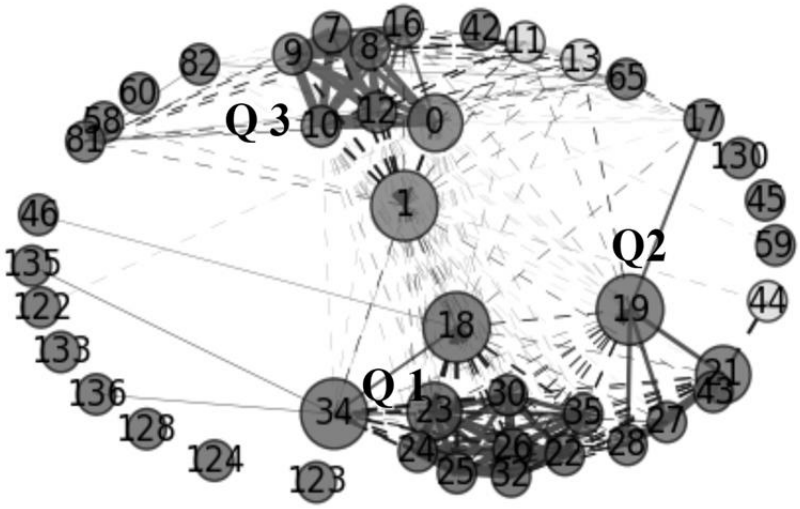
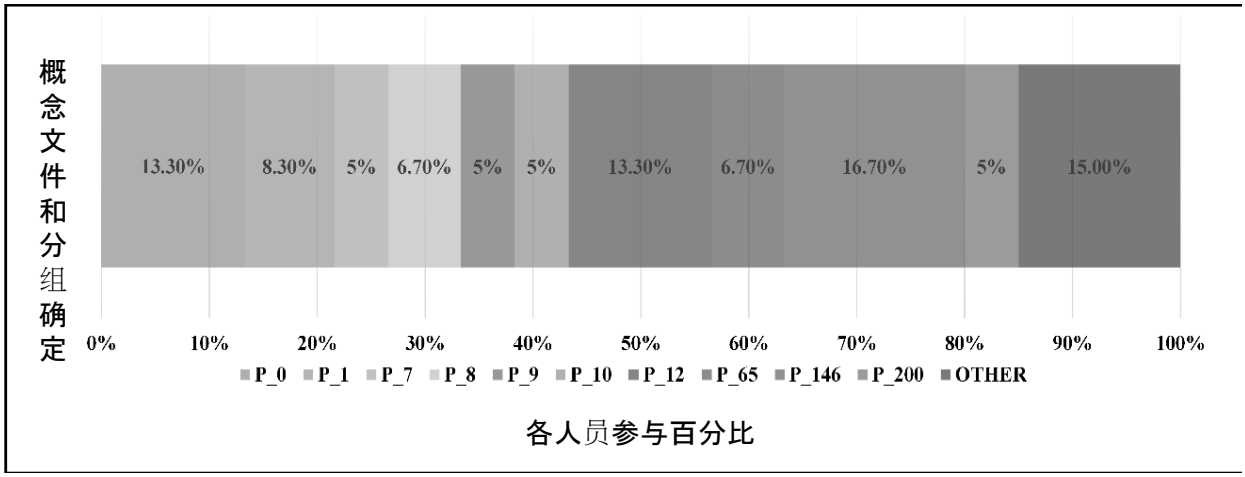


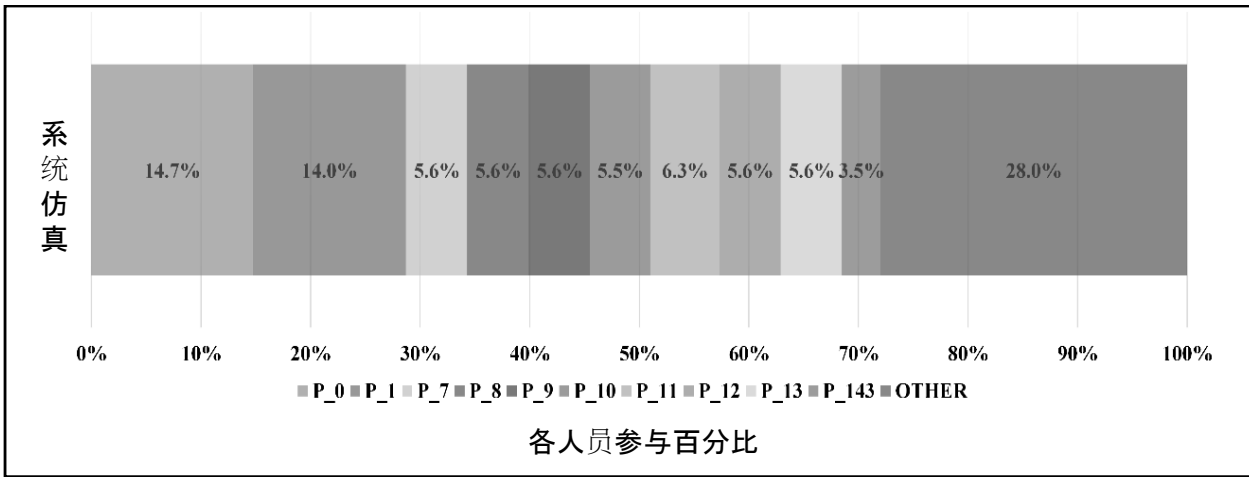
图 7 角色分析

（3）资源分配分析

以本研究中的交通控制系统设计过程顶层任务中的任务 1 和任务 3 为例，描述其人力资源分配情况，如图 8 所示。定义一个执行者对过程中一个任务的参与度和贡献为该执行者参与这个任务中的活动的频率。图 8（a）中可以看出任务 1 中，P_146 发挥了重要作用，承担了该任务中主要活动的执行。图 8（b）中看出 P_0 和 P_1 发挥了主要作用。因此，可以推断，P_146 有能力在 concept paper 这类任务中担任主要的执行者，P_0 和 P_1 在 transportation system design 上具有较强的专业能力，可以在新过程中承担设计类任务。



（a）任务 1 中的主要人员参与程度



（b） 任务 3 中的主要人员参与度

图 8 资源分配分析

4.3.3　时间维度分析结果

（1）任务执行的时间分析

对该项目任务执行的时间进行分析，结果如图 9 所示。

图 9(a)描绘了 48 个子任务的时间线，纵轴列出任务名，横轴代表项目时间，矩阵的长度和间隔反映了任务的执行时间和等待时间。图 9(c)展示了各子任务的相对持续时间，突出任务 11 执行时间最长且频繁中断，暗示其可能构成瓶颈，需深入分析。图 9(b)显示事件吞吐量变化，低吞吐时段指示潜在瓶颈位置，数据指出 2011 年 9 月至 12 月期间任务 11 的事件数量骤减，可能是项目延迟的主因。

（2）参与人员的时间行为分析

对该项目参与者进行时间行为分析，结果如图 10 所示。

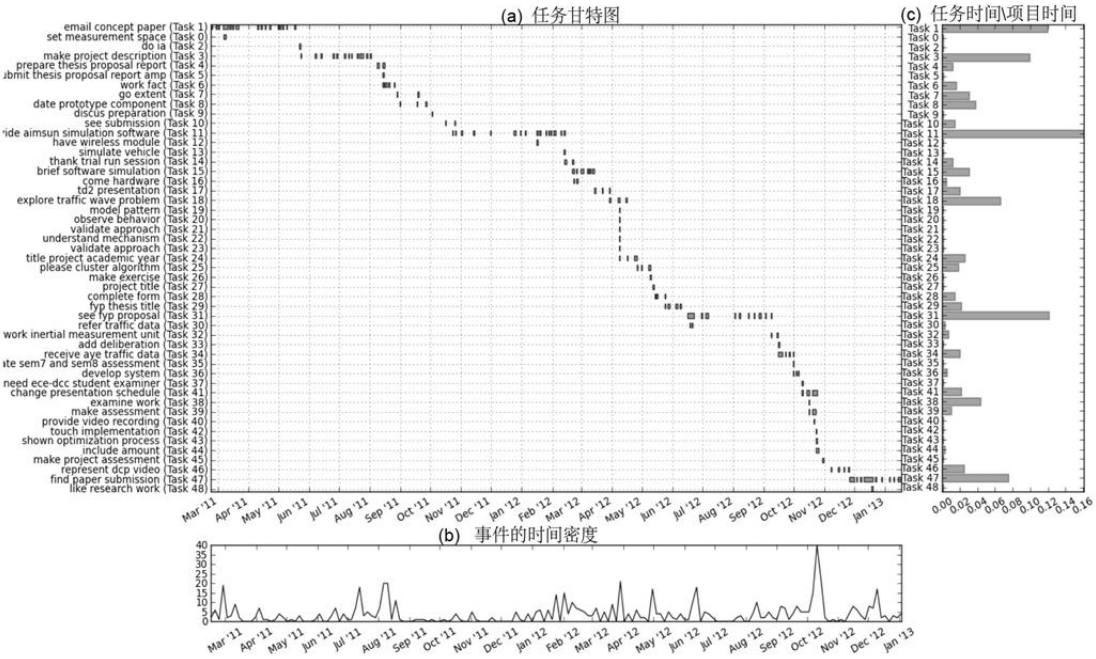


图 9 任务执行的时间分布情况

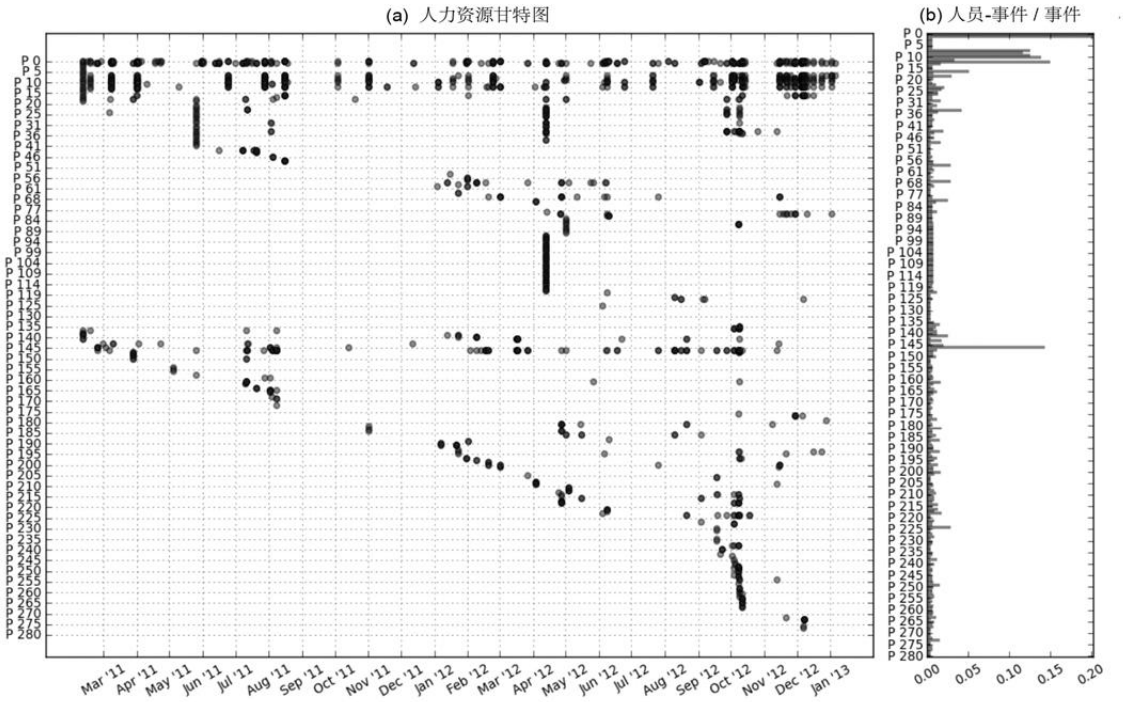


图 10 执行人员的参与时间分布情况

图 10(a)展示了参与人员随时间的任务执行情况，每个点标识个人在特定时间的任务参与，点数多寡反映参与度。图 10(b)则将个人绝对参与时间转换为相对时间，凸显各人在项目中的时间投入对比。核心成员 people_0 至 people_12 贯穿项目始终，与角色分析吻合，显示他们为主要贡献者。相比之下，people_4 和 people_5 仅限初期参与，people_235 和 people_280 则在项目后期加入，体现参与模式的多样性。

5 结论

过程挖掘技术从过程数据中挖掘有效信息来发现、分析、改进实际过程，过程分析聚焦于发现过程执行中的特征，通过过程分析可以有针对性地汲取过程的优势，改进过程的不足。本文针对过程分析视角单一，缺乏系统性的不足，提出了一种基于过程挖掘的多维度过程分析方法。主要贡献为：（1）设计了多维度过程分析框架，不仅关注任务的执行，还关注人员的参与度和时间行为，通过交叉维度分析，揭示了过程中的隐含关联。（2）在交通控制系统设计过程中进行了案例，验证了所提出的方法能够准确地识别出过程中的关键环节，如耗时较长的任务和人员参与模式，为过程改进提供了具体的方向，为复杂过程的管理和优化提供了一种系统化的视角。

参考文献：（参考文献格式参照 2015 年新标准 GBT 7714-2015）

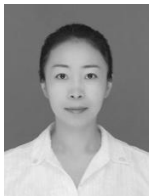
[1] Wil M.P. van der Aalst. Process mining[J]. Communications of the ACM, 2012, 55(8): 76-83.
[2] Laura Maruster, Alex Alblas. Tailoring the engineering design process through data and process mining[J]. IEEE Transactions on Engineering Management, 2020, 69(4): 1577-1591.
[3] Rafael Lorenz, Julian Senoner, Wilfried Sihn, Torbjørn Netland. Using process mining to improve productivity in make-to-stock manufacturing[J]. International Journal of Production Research, 2021, 59(16): 4869-4880.
[4] Onur Dogan. Process mining based on patient waiting time: An application in health processes[J]. International Journal of Web Information Systems, 2022, 18(5/6): 240-254.
[5] Repta, D, Moisescu M A, Sacala I S, Dumitrache I, Stanescu A M. Towards the Development of Semantically Enabled Flexible Process Monitoring Systems[J]. International Journal of Computer Integrated Manufacturing, 2017, 30(1), 96-108.
[6] Nannapaneni S, Mahadevan S, Dubey A, Lee Y T T. Online monitoring and control of a cyber-physical manufacturing process under uncertainty[J]. Journal of Intelligent Manufacturing, 2021, 32(5): 1289-1304.
[7] Burattin A, Cimitile M, Maggi F M, & Sperduti, A. Online discovery of declarative process models from event streams[J]. IEEE Transactions on services computing, 2015, 8(6): 833-846.
[8] R G de Sousa, Peres S M, Fantinato M, & Reijers H A. Concept drift detection and localisation in process mining: An integrated and efficient approach enabled by trace clustering[C]. Proceedings of the 36th Annual ACM Symposium on Applied Computing. 2021, 364-373.
[9] Zaman R, Cuzzocrea A, Hassani M. An innovative online process mining framework for supporting incremental gdpr compliance of business processes[C]. Proceedings of the IEEE International Conference on Big Data (Big Data). IEEE, 2019, 2982-2991.
[10] Ferilli S. Incremental declarative process mining with woman[C]. Proceedings of the IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS). IEEE, 2020, 1-8.
[11] Schuster D, Zelst S J, van der Aalst W M P. Incremental discovery of hierarchical process models[C]. Proceedings of the International Conference on Research Challenges in Information Science. Springer, Cham, 2020: 417-433.
[12] Armas Cervantes A, van Beest N R, La Rosa M, Dumas M, García-Bañuelos L. Interactive and incremental business process model repair[C]. Proceedings of the Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer, Cham, 2017, 53-74.
[13] Tang J, Liu Y, Lin K, Li L. Process bottlenecks identification and its root cause analysis using fusion-based clustering and knowledge graph[J]. Advanced Engineering Informatics, 2023, 55: 101862.
[14] Tang J, Lin K Y, Li L. Using domain adaptation for incremental SVM classification of drift data[J]. Mathematics, 2022, 10(19): 3579.
[15] Junya Tang, Li Li, Ying Liu, Kuo-Yi Lin. Automatic Identification of Bottleneck Tasks for Business Process

Management using Fusion-based Text Clustering[C]. The Proceedings of 17th IFAC Symposium on Information Control Problems in Manufacturing, (INCOM), 2021.
[16] W M.P. Van der Aalst. The application of petri-nets to workflow management [J]. Journal of Circuits, Systems and Computers, 1998, 8(1): 21-66.
[17] Phalp, K., Shepperd, M. Quantitative analysis of static models of processes [J]. Journal of Systems and Software, 2000, 52(2-3): 105-112.
[18] Park, M., Song, M., Baek, T.H., et al. Workload and delay analysis in manufacturing process using process mining [C]. Proceedings of 2015 Asia-Pacific Conference on Business Process Management. Cham: Springer, 2015: 138-151.
[19] Park, J., Lee, D., Zhu, J. An integrated approach for ship block manufacturing process performance evaluation: case from a Korean shipbuilding company [J]. International Journal of Production Economics, 2014, 156: 214-222.
[20] Knoll, D., Reinhart, G., Prüglmeier, M. Enabling value stream mapping for internal logistics using multidimensional process mining [J]. Expert Systems with Applications, 2019, 124(10): 130-142.
[21] Rebuge, Á., Ferreira, D.R. Business process analysis in healthcare environments: a methodology based on process mining [J]. Information Systems, 2012, 37(2): 99-116.

[作者简介]

汤珺雅（1993），女，博士，主要研究方向：过程挖掘、数据分析、过程优化、机器学习。

于青云（1989），女，博士，助理教授，主要研究方向：调度优化、数据分析、路径规划。



李莉（1975），女，博士，教授，主要研究方向：调度优化，人工智能乐观、数据分析、过长挖掘、自主无人系统。

面向柔性制造的通信感知控制协同系统优化方法

周映，冯志勇，尉志青，马丁友，孟泽洋，范颖龙

摘　要：未来大规模智能机器低时延大连接的通信和控制需求，以及动态复杂变化的工业环境给工业无线网络控制和工业互联网性能优化带来新的挑战。针对该问题，本文提出一种面向柔性制造的通感控协同系统优化方法。具体地说，我们分析了通信、感知和控制功能之间耦合关联对闭环控制过程的影响，提出一种基于闭环交互周期的轨迹优化控制方法，保障 AGV 高速移动期间快速响应环境变化。然后，为了满足大规模 AGV 高效控制和低时延通信服务需求，设计了一种物理域与数字域双标识匹配的感知方法，以及通感控协同的通信传输机制，有效提高了工业互联网络支持的 AGV 数量，增强通感控协同的网络化控制系统性能。仿真实验表明，本文算法可控制 AGV 数量至少提升 66.7%，在通信和控制性能方面优于传统算法。

关键词：闭环控制；工业无线网络；通信感知控制协同；双标识；AGV

Design and Optimization of the Sensing, Communication, and Control Coupled System for Flexible Manufacturing

Ying Zhou, Zhiyong Feng, Zhiqing Wei, Dingyou Ma, Zeyang Meng, Yinglong Fan

Abstract: The future demands of low-latency, high-connectivity communication and control for large-scale intelligent machines, as well as the dynamic and complex industrial environments, bring new challenges to industrial wireless network control and industrial internet performance optimization. To address the challenges, this paper introduces an optimization method for an integrated sensing, communication, and control coordinated system tailored for flexible manufacturing. Specifically, according to analyze the coupling effects of communication, sensing, and control functions on the closed-loop control process, we propose a trajectory optimization control method based on the closed-loop interaction cycle to ensure AGVs can quickly respond to environmental changes during high-speed movement. Additionally, to meet the demands of large-scale AGV efficient control and low-latency communication services, we design a dual-domain identity matching method for physical and digital domains and a communication transmission mechanism for sensing-communication-control collaboration. These designs aim to increase the number of AGVs supported by industrial internet networks and enhance the performance of networked control systems. Simulation results reveal that the proposed method increases the controllable number of AGVs by at least 66.7% and outperforms traditional methods in communication and control performance.

Key words: Closed-loop control; industrial wireless network; integrated sensing, communication, and control;

dual domain identity; AGV

1 引言

随着人工智能、边缘计算等技术在制造业的广泛应用，未来智能制造车间中大规模部署智能机器和移动平台成为趋势。柔性制造作为未来智能制造的典型应用场景，利用先进的通信、感知和控制技术部署以自动导引车（Automated Guided Vehicle，AGV）为代表的智能机器，实现了智能制造车间高效自动化和智能化管理，进而释放人力资源，显著提高生产效率，基于 AGV 的高效智能闭环控制系统在制造车间生产中扮演着越来越重要的角色。本文以多 AGV 控制为示例，研究了工业互联网络中的大规模智能机器闭环交互过程，对闭环控制系统中的通信-感知-控制功能联合优化，旨在改善通信系统服务质量的同时，满足大规模智能机器低时延高效控制需求。

传统闭环控制系统设计方案依赖于智能机器通信与感知功能，以及通信与控制功能之间的约束关系，设计相应的优化方法满足智能机器稳定控制和低时延通信需求。一方面，通信-感知协同的系统方案往往侧重于协助 AGV 进行跟踪定位和群体导航等应用，对定位精度和路径引导进行优化，以保证系统通信性能前提下控制系统稳定性。Kobayashi 等人[1]提出了一种物理上下文感知通信控制方法，结合物理环境信息来预测可能的 AGV 碰撞概率，考虑到 AGV 移动时信道状态发生变化对通信质量造成影响，并基于预测的碰撞时间调整 AGV 的状态报告间隔，以实现无碰撞和平稳的 AGV 运行。此外，随着 AGV 数量的增加，有限的无线资源可能导致过高的传输延迟，从而引起 AGV 碰撞和堵塞，降低生产效率。OHORI 等人[2]提出一种最优接入点（Access Point，AP）选择方法，通过多传感器协同感知来监控频谱占用情况，预测 AP 和 AGV 之间链路的通信质量，以降低数据包重传率和时延，改善生产效率。值得注意的是，上述工作仅考虑的 AGV 沿固定路径移动，并且可能需要大量的基础设施改造才能使 AGV 导航新路径。该生产模式下 AGV 系统部署成本高，累积控制误差较少，对于通信系统的性能需求低，考虑的网络结构模型相对简单。然而，随着制造车间内大量部署 AGV 等移动智能机器，复杂的物理环境和有限的通信资源无法满足 AGV 实时控制和执行工业任务的需求。

另一方面，实际智能制造中，均衡控制与通信成本在大量智能机器闭环交互中扮演了重要角色，如何保证工业无线网络中智能机器高效低时延交互尤为重要，通信-控制协同的系统方案引起人们广泛关注[3-5]。Qiao 等人[6]提出了两种通信-控制协同设计方法，分别基于具有通信约束的控制优化问题和具有控制约束的通信优化问题，对控制增益、收敛率参数进行优化，实现了更高的编码速率阈值和更低的系统不稳定概率。此外，考虑到智能机器需要高速移动，来满足不断增长的生产交付和高效物料流动等需求，AGV 与基站之间将以更低时延交换控制、感知等内容，控制和通信性能需求进一步提升。Tayade [7]等人提出一种改进的 AGV 控制系统，分析有限块长度状态下 AGV 控制系统的稳定性性能。通过调整控制参数，保证 AGV 在高速运动下依旧实现恒定的稳定性，实现无缝服务。然而，上述的研究工作侧重于研究局限于单向链路

中空口时延以及可靠性等参数，忽视了实际智能机器闭环信息流的闭环交互特性，导致智能机器网络很难满足信息流高效交互需求。同时，随着 AGV 数量和运行速度等需求增加，大部分工作忽视了通信-感知-控制之间的耦合关系，进而导致传输过多冗余的数据，并增加了通信开销。

本文的研究朝着在工业互联网中实现大规模智能机器高效闭环交互迈出了有意义的一步。本文的目标在于提出了一种面向柔性制造的通感控协同的网络化控制系统设计方案，解决感知、通信和控制功能分离设计导致的通信开销大、闭环时延高和控制误差大的问题。具体地说，为了保证 AGV 高速移动期间快速响应环境变化，联合优化通信感知和控制参数，设计了一种基于闭环交互周期的轨迹优化控制方法。在此基础上，设计了物理域与数字域双标识匹配的感知方法，通过感知辅助通信波束对准和控制决策，有效减少控制和失准误差。在此基础上，进一步设计了通感控协同的通信传输机制，根据不同通信需求和控制系统状态，动态调整闭环交互周期，提高了工业互联网络支持的 AGV 数量，降低闭环时延。仿真结果表明，该方法在通信和控制性能上均优于传统方法，显著提高了工业互联网支持的 AGV 数量并降低闭环时延。本文的主要贡献总结如下：

- 为了更准确地描述 AGV 在工业环境中的闭环控制过程，构建了一种面向柔性制造场景的通感控协同网络化控制系统，通过联合优化通信、感知和控制参数，解决了传统方法中感知、通信和控制功能分离设计导致的高通信开销、高闭环时延和大控制误差的问题。
- 为了实现低开销下快速环境响应，设计了一种基于闭环交互周期的轨迹优化控制方法以及物理域与数字域双标识匹配的感知方法，通过新颖的感知方法辅助优化通信和控制过程，确保多 AGV 闭环控制系统的实时性和稳定性。并且，设计了动态调整闭环交互周期的通感控协同通信传输机制，根据不同的通信需求和控制状态，优化资源分配，显著改善闭环时延和可控制 AGV 数量。
- 仿真分析了柔性制造车间内 AGV 执行不同工业任务下系统性能变化规律，仿真结果表明与传统算法相比，本文算法在通信和控制性能等方面取得了较好的表现。

2　系统模型

本文提出一种面向柔性制造的通感控协同系统优化方法。首先，建立通感控协同系统模型，如图 1 所示。图中，该系统模型由 N 个 AGVs、传感器、基站和边缘服务器组成。其中，AGV 的集合记为 $AGV=\{AGV_1,AGV_2,...,AGV_n,...,AGV_N\}$，负责执行工业任务，周期性与基站建立通信，上传感知数据和接收控制指令。传感器主要由视觉传感器构成，负责主动感知 AGV 的运动状态信息，并将感知数据通过光纤传输给边缘服务器。基站记为 BS，负责控制 AGV 执行工业任务，通过上行链路接收来自 AGV 的感知和任务数据，下行链路传输给 AGV 来自边缘服务器处的控制指令。边缘服务器作为智能制造车间中控制系统的大脑，部署在基站侧，负责分配 AGV 的工业任务，处理 AGV 上传的感知数据和计算控制指令，并将计算决策结果通

过基站传输给 AGV。

在系统模型中，AGV 在 t 时刻，通过基站的下行链路接收控制指令 $u_n(t)$，开始按照指定路线执行工业任务。首先，将自身传感器感知的轨迹信息 $X_n(t+T_s)$ 通过上行链路传输给基站侧的边缘服务器。边缘服务器基于来自 AGV 和车间内传感器采集的实际轨迹信息，与本地的参考轨迹信息比对，计算控制误差 $\varepsilon_n(t)$，并生成新的控制指令 $u_n(t)$，通过下行链路，发送给指定的 AGV，该 AGV 开始执行新一轮工业任务，形成一个闭环交互过程。本文构建的系统模型中，AGV 实现闭环信息交互过程由通信、感知和控制模型组成。

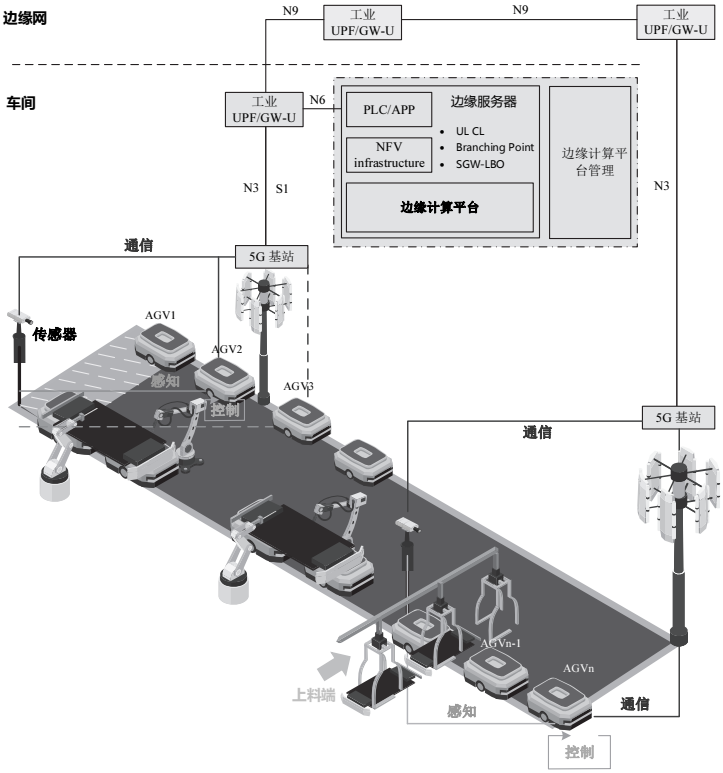


图 1 面向柔性制造的通感控协同系统模型

2.1 通信模型

在 5G NR 标准中大规模机器类通信场景下，为了支持大规模机器高密度通信，智能机器通常会根据预先分配的独立的导频序列并选择一个传输时隙来免授权访问基站，其中发送包含前导码和调制数据的有限块长度数据包。然而，当大量智能机器与基站每秒钟进行上千次数据交互时，有限数量的前导码序号无法满足到达数据包需求，导致多个分配了相同序号的数据包冲突，数据解码失败，大大提高了数据包重传的次数和通信闭环时延。假设当前一组 AGVs 已经准备好传输它们的数据包，每个数据包传输在频域上占用 B Hz 的带宽，在时域上占用 N_1 个传输次数。此时，单个 AGV 的在 K 次重复中成功传输数据包的概率为：

$$P_{n_i}(n_{Ret}=K)=\sum_{k=1}^{K}\binom{K}{k}p_{ret}^{k}(1\text{-}p_{ret})^{K-k}=1-(1\text{-}p_{ret})^{K} \tag{1}$$

其中，p_{ret} 为任意 AGV 在上行免授权接入后成功传输其数据包而不发生碰撞的概率。此外，对于单个用户平均重传次数为 $\mathbb{E}(n_{Ret})=\sum_{n_{Ret}=1}^{K}n_{Ret}\cdot P_{n_i}(n_{Ret})$。

AGV_n 与基站之间上下行传输过程中 t 时刻 AGV_n 的通信闭环时延 $T_n^C(t)$ 包括 AGV 每次业务请求过程中的上下行传输时延，$T_n^C(t)=T_n^U(t)+T_n^D(t)$。根据[8, 9]，短包数据传输速率 R_n 近似为：

$$R_n = B\left(\ln(1+SNR_n)-\sqrt{\frac{V_n}{t_n^d B}}Q^{-1}(\text{ɔ})\right) \tag{2}$$

其中，SNR_n 为 AGV_n 的信噪比，t_n^d 为短包传输时长，B 为通信带宽；ɔ 为短包解码错误率，V_n 为信道色散；$Q^{-1}(\cdot)$ 为高斯 Q 函数的逆函数，如 $Q(x)=\int_x^{\infty}(1/\sqrt{2\pi})\exp(-t^2/2)dt$。

2.2　感知模型

制造车间内部署大量传感器，对 AGV 的状态进行采样，并将采样值经过光纤实时上传到基站，基站侧服务器根据 AGV 状态计算控制指令，并周期性地进行波束对准和建立无线通信链路，将控制信息发送给 AGV。在式(2)中，$SNR=\left(|h|^2\cdot P\right)/N_0$，$h$ 为慢衰落无线信道参数，P 为传输功率，为加性高斯白噪声，$h=h_g h_f h_m$ 由路径损耗 h_g、多径衰落 h_f 与失调衰落 h_m 三部分组成。由于 h_g 与 h_f 对波束对准不产生影响，因此后文中主要关注失调衰落 h_m。具体地说，由于传感器的感知精度影响，感知到的 AGV 的实际位置与感知的位置存在偏差，同时，由于 AGV 动态移动，感知获取的 AGV 位置存在滞后性，无法保证 AGV 能一直在有效波束宽度内与基站进行数据传输。这些都导致波束径向误差，影响通信传输速率和时延。其中，h_m 的表达式如下：

$$h_m(l;d)=S_0 e^{-\frac{2l^2}{R_{eq}^2}} \tag{3}$$

其中，l 为波束径向误差，d 为收发端之间的距离，R_{eq} 为等效波束宽度，S_0 为当径向误差 $l=0$ 时的接收功率，a 为接收端探测波束有效覆盖半径，R_d 为波束在收发器距离为 d 时的最大半径。

假设每次闭环交互中有 M 个传感器观测到 AGV_n 的当前运动状态 $\mathbf{X}_n$，其中传感器感知 AGV_n 的原始数据集记为 $\{S_1,S_2,...,S_M\}$，经过 PLC 处理后的状态观测值为 $\left\{\mathbf{X}_n^1,\mathbf{X}_n^2,...,\mathbf{X}_n^M\right\}$。$\mathbf{X}_n$ 的估计值 $\hat{\mathbf{X}}_n$ 的均方误差为 $\varepsilon_n=\mathbb{E}\left\{\left(\hat{\mathbf{X}}_n-\mathbf{X}_n\right)^2\right\}$。

2.3　控制模型

第 t 个时刻，服务器基于当前接收到的 AGV_n 轨迹数据，结合本地参考轨迹数据计算出轨迹误差 $\varepsilon_n(t)$ 和生成新一轮的车辆行驶轨迹 $X_n(t)$，然后将结果打包成控制指令 $u_n(t)$ 通过下行链路发送给 AGV_n。其中，上行传感数据包括 AGV_n 的位置坐标 $(x_n(t),y_n(t))$、行进方向 $\theta_n(t)$ 等。AGV_n 在接受新的控制指令后，新的行驶轨迹为 $X_n(t+1)$，即

$$X_n(t+1)=X_n(t)+T_s\cdot\mathbf{J}\cdot u_n(t) \tag{4}$$

其中，T_s 为两次接收控制指令的间隔持续时间，$u_n(t)=f\left(X_n^r(t),\varepsilon_n(t)\right)$ 为基站侧服务器基于参考轨迹和轨迹误差，计算出的 AGV_n 轨迹控制函数。$\mathbf{J}$ 为转置矩阵。

3　面向柔性制造的通感控协同系统优化方法

本文研究 AGV 闭环交互过程中通信、感知和控制功能之间的耦合影响关系，旨在减少传统优化算法

在三者之间的冗余设计过程，互补增强通信、感知和控制性能。例如，对于传统通信系统设计而言，当多辆 AGV 在非装配区域运动时，控制系统处于稳定状态，基站在多个控制周期内计算并发送相同的控制指令，尽管相同控制指令的发送具有冗余性，但基站仍会考虑控制系统中拥塞、碰撞等最坏的情况，严格按照 5ms 固定交互周期继续向 AGV 发送这些指令，进而造成通信资源的浪费。因此，需要联合设计通信、感知和控制，不同系统之间相互协作，以扩展系统可控制 AGV 数量和工作速度的同时，改善通信质量和控制性能。

3.1 基于闭环交互周期的轨迹优化控制方法

本文提出一种基于闭环交互周期的轨迹优化控制方法，根据控制系统状态和通信闭环时延控制多 AGV 运动轨迹。与传统的动力学模型[10]不同，本文引入新的通信-感知-控制系统的联合变量参数，闭环交互周期 T'_{ns}，$T'_{ns}=T_n^C+T_n^{Con}$，T_n^{Con} 为控制系统反馈时延，分析 AGV 执行控制决策期间的轨迹变化规律。

在闭环交互周期内，AGV 通过自身传感器感知的环境信息，判断是否是在装配区域，以此来触发是否符合自适应调整闭环交互周期，向服务器发送控制决策请求。当感知到 AGV 在装配区域的动态环境，AGV 的轨迹控制指令主要来自固定交互周期下的 PLC 控制决策，执行缓慢且高精确的循环步进式移动，保证生产工序高效运行；此外，AGV 在非装配区域内会沿环形装配线稳定状态运行，任意 AGV 之间不存在机械臂装配工位和其他障碍物。因此，该区域 AGV 可以在宽松的通信网络下平稳运行，此时以其他 AGV 为避障目标，通过动力学模型推导出来的系统稳定条件下轨迹优化函数 $v_{\mathrm{n}}(\mathrm{t}+T_n^C)$ 得到闭环交互周期，自适应调整交互周期，进而非周期性地接收 PLC 的控制指令。

3.2 物理域与数字域双标识匹配的感知方法

本文提出一种物理域与数字域双标识匹配的感知方法，通过匹配数字域中数字标识，以及物理域和数字域中物理标识，精确识别多目标以及状态位置信息，进而有效降低波束失准发生概率，改善通信闭环时延。具体地说，基站精准匹配来自数字域物理和数字标识信息以及物理域的数字标识信息等多维感知信息，并实时更新 AGV 的位置信息，快速进行波束跟踪，保证在闭环交互周期上界内降低控制误差 $\varepsilon_n(t)==\mathbf{J}_e\cdot\left(X_n^r(t)-\widehat{X}_n(t)\right)$ 的同时，降低闭环时延。其中 $\mathbf{J}_e$ 为旋转矩阵，$X_n^r(t)$ 为参考轨迹，$\widehat{X}_n(t)$ 为传感器感知轨迹。算法具体内容如下。

对于基站从物理域获取信息 PX_n^r 而言，由于视觉感知的位置精度往往高于无线电感知精度，此时基站希望通过物理域的信息与数字域的信息对应匹配，来快速进行波束跟踪。基于此，根据余弦相似度 S_n 来衡量物理域 AGV_n^P 的 PX_n^r 与任意一个数字域 $AGV_{n'}^D$ 的 $DX_{n'}^r$ 之间的相似性，即 $\underset{n,n'\in N}{S(n,n')}=\left(\overrightarrow{I_n}\cdot\overrightarrow{I_{n'}}\right)\Big/\left(\left\|\overrightarrow{I_n}\right\|\times\left\|\overrightarrow{I_{n'}}\right\|\right)$。匹配规则为：

$$AGV_n^P:AGV_{n'}^D\succ AGV_{n''}^D\Leftrightarrow n''=\underset{n''=1,2,\ldots,n,\ldots n',\ldots,N}{arg\ \max}S(n,n'') \tag{5}$$

$AGV_n^P:AGV_{n'}^D\succ AGV_{n''}^D$ 表示在 $AGV_{n'}^D$ 与任意 $AGV_{n''}^D$ 之间，AGV_n^P 更倾向于识别 $AGV_{n'}^D$ 为同一目标。同理，对于基站从数字域获取信息 DX_n^r 而言，考虑到基站视觉传感器存在障碍物遮挡非视距区域和感知重叠区域

等环境复杂区域。这些复杂区域内可能存在多个 AGV 无法被感知或匹配，导致数字域中待匹配的节点将普遍多于物理域的节点，引入新信息并更新物理域标识的匹配矩阵 $P'X_n^r(P\mathbf{P}_n^{ID},X_n)$，进一步实现双域标识细粒度匹配映射，匹配规则为：

$$AGV_n^D : AGV_{n'}^P \succ AGV_{n''}^P \Leftrightarrow n'' = \underset{n''=1,2,\ldots,n,\ldots n',\ldots,N}{arg\ \max} S'(n,n'') \tag{6}$$

匹配过程中，会出现阻塞对，与当前的匹配对象相比，阻塞对的两个用户都更满意对方而不满意各自现有的匹配对象。一对一稳定匹配的条件是匹配不包含任何阻塞对。综上，设计物理域与数字域双标识匹配的感知方法：

算法 1：物理域与数字域双标识匹配的感知方法

```
Input：数字域标识信息 DX_n^r(DD_n^ID, DP_n^ID)，物理域标识信息 PX_n^r(PP_n^ID)。
Output：双标识匹配结果 Φ(AGV_n^P, AGV_n^D)
while 阻塞对存在 do
  for n from 1 to N do
  通过(5)，AGV_n^P 待匹配的目标寻找最优匹配结果，保存并更新临时匹配结果。
    if AGV_n^P 所有目标基于稳定匹配算法[11]完成匹配，且 AGV_n^P 目标数量与 AGV_n^D 相同
      break
    else if AGV_n^P 所有目标未完成匹配，或 AGV_n^P 目标数量与 AGV_n^D 不相同
      扩展并更新物理域标识的匹配矩阵 P'X_n^r(PP_n^ID, X_n)
      通过(6)，AGV_n^D 寻找最优匹配结果，基于稳定匹配算法进行匹配，更新临时匹配结果。
    end if
  end for
end while
```

3.3　通感控协同的通信传输机制

本文设计了更加灵活、冗余度更低的通感控协同通信传输机制，根据交互周期时间、安全间隔距离、行驶速度等参数对控制稳定性的影响，自适应提高 AGV 的闭环交互周期，以减少了 AGV 访问基站的次数和通信开销，支持网络化控制更多数量的 AGV。

一般来说，AGV 控制系统稳定性是指处于系统平衡状态的 AGV，在受到扰动之后，其运动状态是否会自动调节回初始的平衡状态。如果系统不稳定，扰动会随之扩散，最终演变成 AGV 堵塞、碰撞等现象。如果系统稳定，则在传播过程中扰动逐渐减小消失，车辆间距在波动一段时间后继续保持最佳车距。因此，通过考虑多样化工业任务通信质量需求、时变的运动状态参数等因素，推导基于闭环交互周期动力学模型 $v_n(t+T_n^C)$ 在扰动下保持稳定运行的临界稳定性条件 $\kappa \geq \kappa_{th}$，其中 κ 为稳定性系数，$\kappa=1/T'_{ns}$，得到了系统稳态下可自适应调整闭环交互周期上界 $\hat{T}'_{ns}$。具体地说，AGV 在闭环交互周期间隔内，根据控制状态和网络性能等因素计算出控制系统稳定前提下最大容忍闭环交互周期，自适应调整与基站交互数据的闭环交互周期 T'_{ns}，有效减少了 AGV 访问基站的次数和通信开销，降低通信闭环时延。此外，在闭环交互周期时，基站基于双标识匹配结果，实时感知并更新 AGV 的参考轨迹，降低基站侧的控制误差和波束失准误差，改善系统稳定性并降低上下行传输时延。

4 仿真分析

本文基于 Anylogic 工业级仿真软件，模拟 $20m\times100m$ 的智能工厂车间环境，生成 100 辆 AGV 参与物料生产和运输的过程，并导出 AGV 的行驶轨迹作为基站处参考路径的数据集。在此基础上，基于 MATLAB 平台进行下列实验验证对本文所提出优化方法。

表 I 系统参数

符号	仿真参数	数值
N	AGV 数量	100
T_n^C	参考交互周期 cycle time	5ms
э	误码率	1e-5
H_c	安全间距	5m
f	载波频率	28GHz

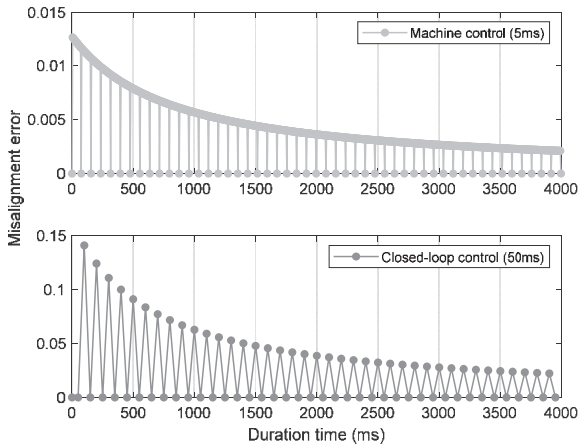


图 2 不同工业任务下失准误差变化规律

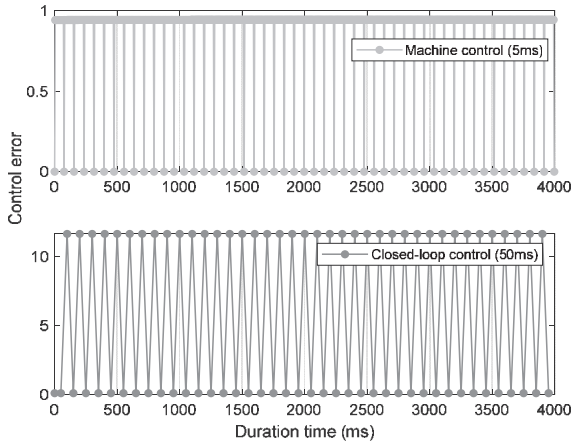


图 3 不同工业任务下控制误差变化规律

图 2 的第二列子图可以看出，随着系统运行时间逐渐增加，并且每隔 100ms，波束失准误差归零一次。这是因为 50ms 的工业任务下，基站侧的 PLC 计算出 5ms 的工业任务下，控制系统稳定下的闭环交互周期上界在 110ms。这意味着每个 AGV 与基站交互控制指令的 Cycle time 从初始 50ms 自适应调整到 100ms，每次 AGV 和基站同步校对轨迹时，失准误差为 0。此外，对比两种工业任务可以发现，Cycle time 为 5ms 的工业任务失准误差小于 Cycle time 为 50ms 的工业任务。这是因为工业任务的 Cycle time 越小，该 AGV 对于控制精度和任务指令的依赖程度越大，轨迹校准和匹配的精度需求更大，进而可容忍的波束失准误差更小。

同理，图 3 的第二列子图可以看出，随着系统运行时间逐渐增加，控制误差在[0，12]之间上下波动，并且每隔 100ms，控制误差归零一次。与**错误!未找到引用源。**同理，这是因为面对 Cycle time 为 50ms 的 Closed-loop control 时，AGV 和基站每隔 100ms 同步校对轨迹，此时控制误差为 0。随后，AGV 在下一次同步信息之前，控制误差逐步累积；当控制误差达到 12 时，控制误差大于给定阈值，此时通感控系统通过轨迹优化，使控制系统逐渐达到稳定状态，同时基站通过双标识进行粗粒度感知匹配，更新参考轨迹，

进一步减小控制误差，该过程中控制误差逐渐减小。

错误!未找到引用源。中看出 AGV 执行 5ms 的工业任务时，网络化控制系统满足该业务闭环时延需求的前提下，不同算法最大可支持 AGV 数量变化规律。其中，本文方案中网络化控制系统单位面积内最大可支持的 AGV 数量为 100，Classic ISAC algorithm（CISACA）[12]，Traditional algorithm with Nmax Outage tolerance（TANOT）[7]，和 Traditional algorithm（TA）[13]的最大可支持的 AGV 数量分别为 60，20 和 20 左右，至少提升了 66.7%。这是因为本文提出算法综合考虑波束失准、控制误差对通信传输造成的影响，计算出控制系统稳定状态下的闭环交互上界，有助于 AGV 自适应调整最大的上下行感知和控制数据传输间隔，大幅度减少数据包冲突，改善网络负载压力，从而允许更多的 AGV 执行工业任务。CISACA 可以通过主动感知和匹配 AGV 的运动状态，降低波束跟踪和对准时延，却也无法有效解决大量 AGV 高频率访问基站带来的数据包冲突、排队时延高等问题，无法对 AGV 数量进行优化。而 TANOT 通过调整编码速率来缓解 AGV 控制系统保持稳定下的 AGV 的中断重传对控制系统稳定性的影响，却忽略了每次中断重连过程中波束失准误差对于通信时延的影响，对于网络负载缓解效果较弱。TA 同理，固定闭环交互周期的传输机制下有限的前导码无法支持大量 AGV 访问基站，进而导致数据包冲突、排队时延高等问题，可支持的 AGV 数量少。综上所述，本节验证了本文提出方法的有效性，可以低时延无线控制单位区域内百台 AGV 搬运和运输零件，保证系统通信和控制性能。

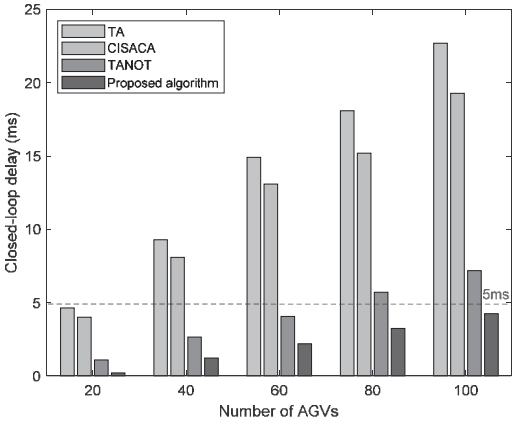


图 4 不同算法下闭环时延随 AGV 数量变化规律

5　结束语

本文提出一种面向柔性制造的通感控协同系统优化方法，通过基于闭环交互周期的轨迹优化控制方法，以及物理域与数字域双标识匹配的感知方法，将通信、感知和控制的耦合关系联系起来，实现高速 AGV 的实时稳定控制，减少控制和失准误差。随后设计了通感控协同通信传输机制，支持 AGV 自适应调整控制轨迹和闭环信息交互周期，显著增加网络可支持 AGV 数量，降低闭环时延。仿真结果验证了本文方法的有效性，与传统算法相比，在通信和控制性能方面取得了良好的表现。未来，将进一步考虑计算模

块对于感知-计算-控制协同系统的影响，设计灵活地智能资源分配算法，致力于构建感知-通信-计算-控制一体化系统架构，为智能制造场景大规模智能机器协作提供更好地服务。

参考文献：

[1] Kobayashi K, Iwai T. Physical Context-Aware Communication Control Method for Efficient AGV Operation [C]. 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 1-5.

[2] F O, S I, T O, et al. Estimating Wireless Link Quality using Multiple Remote Sensors for Wireless Control of AGV in a Factory [C]. 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC), Okayama, Japan, 1-6.

[3] Javaid S, Saeed N, Qadir Z, et al. Communication and control in collaborative UAVs: Recent advances and future trends [J]. IEEE Transactions on Intelligent Transportation Systems 2023, 24(6): 5719-5739.

[4] Mason F, Chiariotti F, Zanella A, et al. Multi-agent reinforcement learning for coordinating communication and control [J]. IEEE Transactions on Cognitive Communications and Networking, 2024, 10(4): 1566 - 1581.

[5] Han Z, Li X, Zhou Z, et al. Wireless Communication and Control Co-Design for System Identification [J]. IEEE Transactions on Wireless Communications, 2024, 23(5): 4114-4126.

[6] Qiao Y, Fu Y, Yuan M. Communication–Control Co-Design in Wireless Networks: A Cloud Control AGV Example [J]. IEEE Internet of Things Journal, 2023, 10(3): 2346-2359.

[7] Tayade S, Rost P, Maeder A, et al. Impact of Short Blocklength Coding on Stability of an AGV Control System in Industry 4.0 [C]. 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 1-6.

[8] Nasir A A, Tuan H D, Nguyen H H, et al. Resource Allocation and Beamforming Design in the Short Blocklength Regime for URLLC [J]. IEEE Transactions on Wireless Communications, 2021, 20(2): 1321-1335.

[9] Shi E, Zhang J, Zhang J, et al. Decentralized Coordinated Precoding Design in Cell-Free Massive MIMO Systems for URLLC [J]. IEEE Transactions on Vehicular Technology, 2023, 72(2): 2638-2642.

[10] Li X, Qie L, Liu Z, et al. Numerical simulation of Car-Following Model Considering Multiple-Velocity Difference and Changes with Memory [C]. 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT), Sanya, China, 777-782.

[11] Zhang Y, Zhou Y. Resource Allocation Strategy Based On Tripartite Graph in Vehicular Social Networks [J]. IEEE Transactions on Network Science and Engineering, 2023, 10(5): 3017-3031.

[12] Arnold M, Bauhofer M, Mandelli S, et al. MaxRay: A Raytracing-based Integrated Sensing and Communication Framework [C]. 2022 2nd IEEE International Symposium on Joint Communications & Sensing (JC&S), Seefeld, Austria, 1-7.

[13] Kampen A L, Cupek R, Fojcik M, et al. Case Study of AGV in Industry 4.0 Environments – An Evaluation of Wireless Communication Protocols [C]. 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Prague, Czech Republic, 2049-2055.

[作者简介]

周映（1997-），男，博士生，研究领域为工业无线网络、网络化控制系统、通信感知控制一体化等。

冯志勇(1971-)，女，博士，教授，博士生导师。研究领域为第五代移动网络 (5G) 中的无线网络架构设计和无线电资源管理、认知无线网络中的频谱感知和动态频谱管理、通用信号检测和识别以及网络信息理论等。

尉志青(1987-)，男，博士，副教授，博士生导师。研究领域为移动自组织网络性能分析与优化等。

马丁友(1993-)，男，博士，讲师。研究领域为通信信号处理、雷达信号处理和双功能雷达通信系统等。

孟泽洋（1998-），男，博士生，研究领域为工业无线网络，网络化控制系统等。

范颖龙(2000-)，男，博士生，研究领域为工业无线网络、通信感知控制一体化等。

5G-TSN 融合网络中面向负载均衡的资源分配技术

苏慧，贾杰，薛祎，陈剑，王兴伟

（东北大学 计算机科学与工程学院，辽宁 沈阳 110819）

摘　要：针对传统的 5G 与时间敏感网络（Time Sensitive Networking，TSN）融合网络在调度灵活性与可扩展性等方面的局限性，提出一种支持数据以有线和无线自适应选择的新型 5G-TSN 融合架构。基于此架构，设计一种面向时间敏感（Time Triggered，TT）流量的联合调度机制，分别对 TSN 域的队列资源和 5G 域的带宽资源进行分配优化，在满足负载均衡的基础上，最大化调度成功率。实验结果显示，所提网络架构及资源分配方法相比于传统方法具有更优越的性能。

关键词：5G；时间敏感网络；流量调度；资源分配

Resource allocation technology for load balancing in 5G-TSN converged network

Su Hui, Jia Jie, Xue Yi, Chen Jian, Wang Xingwei

（*Department of Computer Science and Engineering*，*Northeastern University*，*Liaoning Shenyang 110819*）

Abstract: In view of the limitations of the traditional 5G and Time Sensitive Networking (TSN) converged network in terms of scheduling flexibility and scalability, a novel 5G-TSN converged architecture is proposed to support the adaptive selection of data in terms of wireline and wireless. Based on this architecture, a joint scheduling mechanism is designed for Triggered (TT) traffic, where the allocation of queue resources in the TSN domain and bandwidth resources in the 5G domain are jointly optimized, respectively. Thus, the scheduling success rate can be maximized on the basis of load balancing. The experimental results show that the proposed network architecture and resource allocation method have superior performance compared with the traditional method.

Key words: 5G; Time Sensitive Networks; traffic scheduling; resource allocation

1 引言

在工业 4.0 的推动下，工业互联网迎来了前所未有的机遇和挑战。新兴的工业应用不仅对数据的传输时延、抖动和可靠性的要求更为严苛，同时也对网络的灵活性和可扩展性提出了更高的期望。基于以太网的 TSN 技术为工业应用提供了前所未有的确定性服务水平和近乎完美的有限延迟，正逐步成为工业 4.0 环境下的标准有线技术，但该技术仍面临有线基础设施布线成本较高、可扩展性受限等难题[1]。与此

本文受到国家自然科学基金项目（92167103，62172084）、辽宁省应用基础研究计划（2023JH2/101300196）资助

同时，5G 技术作为工业应用中无线通信的关键使能技术，在提升网络的灵活性和可扩展性方面展现出巨大潜力，有望成为克服有线网络在移动性和扩展性方面局限性的有效技术方案。TSN 与 5G 网络的融合已成为应对复杂多变的应用场景与保障端到端确定性传输的重要方向，二者的创新性集成对于推动工业互联网的高质量发展具有重要作用[2–4]。

3GPP R16[5]定义了 5G 与 TSN 融合的标准架构，将 5G 系统（5G Systems，5GS）封装为一个“黑盒”，以逻辑网桥的形式集成到 TSN 网络中，对外表现为虚拟 TSN 网桥（Virtual TSN Bridge，VTB），TSN 用户无需关注 5G 网络的具体实现方式。文献[6]基于现有的 TSN 模型 NeSTiNg 和轻量级 5G 用户平面模型，提出一种将 5G 作为透明桥梁集成到 TSN 中的仿真方法，并在 OMNeT++中加以实现。文献[7]针对基于循环排队与转发机制（Cyclic Queuing and Forwarding，CQF）的 5G-TSN 中的联合时频资源调度问题，提出一种面向 5GS 的时间感知包转发策略，对端到端的 CQF 进行调度，以提升可调度流数量。文献[8]聚焦于在公司场所内部署的 5G 非公用网络上采用 TSN 标准的场景，基于自动机学习的 5G 网络模型的构建，提出一种实现私有 5G 网络零接触自配置的新方法，并在一个新实验测试平台上进行了验证。文献[9]提出通过智能选择 5G 中的 CG 来实现 5G-TSN 的无缝传输，并提出一种基于 Actor-Critic 强化学习的信息年龄感知的分布式确定性调度方案，用于引导时间敏感的流主机自主地做出数据包采样-传输决策，从而通过无冲突的 5G-TSN 传输满足基于时效性的年龄约束。

上述研究虽然对 5G-TSN 网络仿真、流量调度等做了相关研究与优化，但在融合网络架构方面仍然局限于传统的桥接模型，在资源调度、网络扩展以及设备移动等方面缺乏一定的灵活性。随着未来工厂对于确定性传输和网络架构灵活性需求的日益提高，在 5G 与 TSN 的融合方面势必需要寻求更为灵活的网络框架，以适应未来工厂的需求。因此，本文致力于探索一种更加灵活、扩展性更强的 5G-TSN 融合网络架构，并在该架构下重新对流量调度进行优化，从而充分发挥 TSN 确定性传输与 5G 高度灵活通信的优点。本文的主要贡献如下：

1) 基于 3GPP R16 标准中所提出的 5G-TSN 集成架构，构建一种能够支持数据有线和无线双模传输方式的 5G-TSN 融合网络架构，进一步增强融合网络的可扩展性和灵活性。

2) 提出 5G-TSN 融合架构下的协同调度机制，以最大化流量的调度成功率为目标，构建流量调度优化模型，设计相应的分流策略。

3) 分别在有线域和无线域提出面向负载均衡的注入时隙规划算法和基于快速非支配排序的带宽分配算法，进行调度资源分配，通过均衡有线域和无线域的负载水平，最大化网络的调度性能。

4) 针对所提 5G-TSN 融合网络架构及协同调度机制，设计了一系列对比实验，以验证其在流量调度方面的有效性和优越性。

2 5G-TSN 融合架构及协同调度机制设计

2.1 5G-TSN 融合架构设计

本文在 3GPP R16 中所定义的 5G-TSN 传统融合架构的基础上加以改进，设计了一种新型 5G-TSN 融合网络架构，如图 1 所示。该架构中主要包括 TSN 网桥、5G 节点以及工业设备，整个网络被划分为具有相同拓扑结构的有线 TSN 域和无线 5G 域两部分，确保了网络的一致性和稳定性。为了在开放的无线环境中实现 TSN 级性能，需要借助能够规划部署的单一实体管理无线网络，并在网络部署和配置阶段解决重叠网络之间的干扰[10]。此外，要求所有设备都能实现在该模式下运行所需的最小功能集，其中包括集中式用户配置（Centralized User Configuration，CUC）和集中式网络配置（Centralized Network Configuration，CNC）。在全集中式管理模式下，CUC 收集关键业务流的信息，CNC 利用这些信息执行准入控制，同时定义并部署资源分配策略，以满足所需的时间敏感性能。TSN 和 5G 域之间通过 IEEE802.1 AS 协议并依赖于 NW-TT 和 DS-TT 两个转换器进行周期性的时钟同步协同工作，相互配合完成流量传输调度工作[11]。

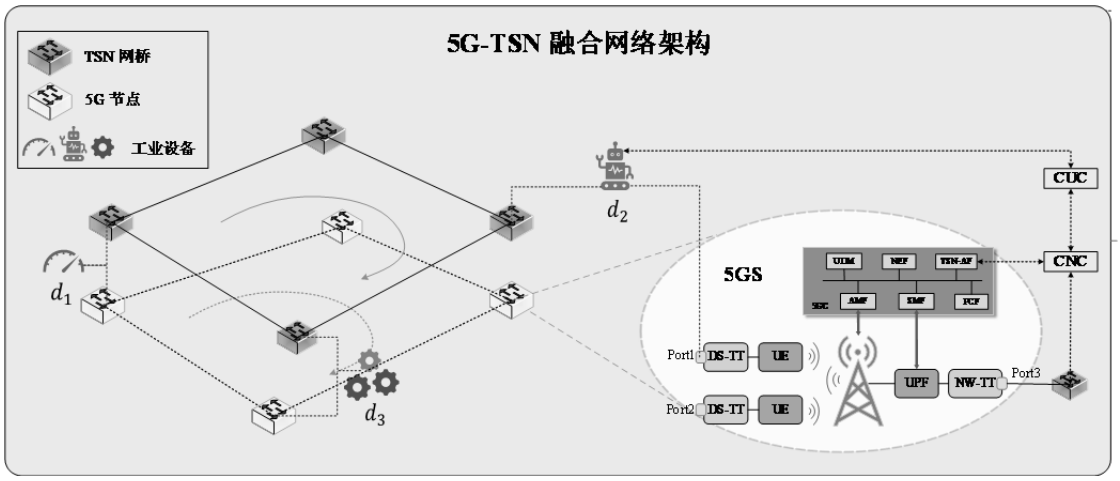


图 1 5G-TSN 融合网络架构示意图

与传统融合网络架构相比，该架构为通信过程提供了高度的灵活性。以上图d_1作为源端设备向d_3发送流量为例，当d_1发送大规模突发流量时，传统融合架构中的 5GS 仅作为 VTB 参与流量传输，TSN 网桥队列阻塞时，5GS 难以发挥其灵活接入的优势，整体网络调度性能下降。而本文所设计的新型融合架构支持流量以自适应方式选择有线或无线传输，由d_1发送的数据帧首先按照自身的偏移量注入网络，根据 CQF 队列资源约束计算分流比例并进行分流，然后分别占用一定的有线队列资源和无线带宽资源进行传输，最终在目的端d_3处重组，得到原始的数据帧。该架构在避免队列拥塞的同时最大限度地融合了 5G 技术的优势，不仅保证了流量的确定性传输，还充分提升了整体融合网络的调度性能。

2.2 网络拓扑与流量模型

网络拓扑定义为由网络节点集合$\mathcal{V}$与网络中相邻节点之间的链路集合 $\mathcal{E}$ 构成的有向图：$\mathcal{G} \equiv (\mathcal{V}, \mathcal{E})$，

如图 2 所示。网络节点主要包括 TSN 网桥$\mathcal{V}_{TSN}$、5GS 节点$\mathcal{V}_{5GS}$以及工业设备节点$\mathcal{D}$，即$\mathcal{V}=\mathcal{V}_{TSN}\cup\mathcal{V}_{5GS}\cup\mathcal{D}$。其中，$\mathcal{V}_{TSN}=\{v_1^{TSN},v_2^{TSN},\dots,v_m^{TSN},\dots v_{N^{TSN}}^{TSN}\}$，$N^{TSN}\in\mathbb{N}^+$；$\mathcal{V}_{5GS}=\{v_1^{5GS},v_2^{5GS},\dots,v_l^{5GS},\dots v_{N^{5GS}}^{5GS}\}$，$N^{5GS}\in\mathbb{N}^+$；$\mathcal{D}=\{d_1,d_2,\dots,d_j,\dots,d_{N^D}\},N^D\in\mathbb{N}^+$。节点$v_a$到$v_b$的链路表示为$e\equiv[v_a,v_b]$，且有$v_a,v_b\in\mathcal{V}$。

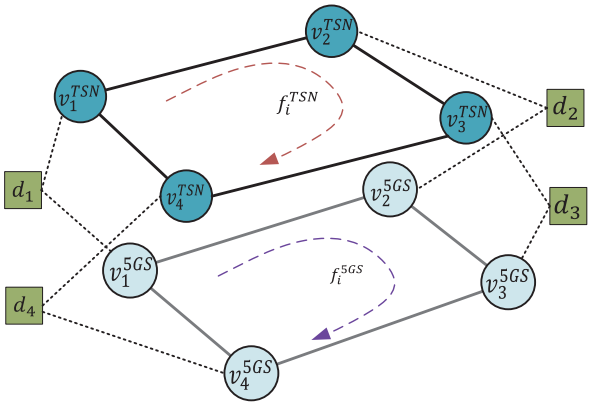


图 2 5G-TSN 网络拓扑图

TT 流在时隙t_0生成数据帧并按照固定的周期发送。定义$\mathcal{F}=\{f_1,f_2,\dots,f_i,\dots,f_{N^F}\}$为网络中流的集合，$f_i\in\mathcal{F}$的属性元组可以表示为：

$$f_i=<id,src,dest,period,size,path,cp,delay,ddl,offset,gain,prop>, \tag{1}$$

其中，$f_i.id$表示 TT 流f_i的标号；$f_i.src$、$f_i.dest$分别为f_i的源节点和目的节点；$f_i.period$为f_i的发送周期；$f_i.size$为f_i所发送的数据帧的大小；$f_i.path$为f_i从源节点到目的节点所经过的路径；$f_i.cp$为f_i的候选路径集合，即$f_i.path\in f_i.cp$；$f_i.delay$表示f_i从源到目的节点所经历的延迟；$f_i.ddl$表示所允许的最大端到端延迟；$f_i.offset$为f_i的注入时间偏移量，即f_i中第一个数据帧从源设备发送的时间；$f_i.gain$表示流f_i中的数据帧在 5G 域中所处的信道增益；$f_i.prop$表示 TT 流f_i中每个数据帧需分给 5G 域的比例。

定义集合$\mathcal{F}_i=\{f_i^1,f_i^2,\dots,f_i^j,\dots,f_i^{n_i}\}$表示$f_i$在一个超周期内发送的数据帧集合。其中，$n_i=T_{hyper}/f_i.period$；$f_i^j.st$表示$f_i^j$的开始发送时间，且$f_i^j.st=f_i.offset+(j-1)f_i.period$；$f_i^j.rp$是数据帧$f_i^j$的路由路径，决定了$f_i^j$的最终转发过程。

2.3 TSN 调度机制

TSN 域采用 CQF 机制进行 TT 流的调度传输。作为一种常用的流量整形方法，CQF 机制能够为 TT 流提供确定性且易于计算的延迟和抖动。该机制通常采用一个公共的时间周期T作为参考时间，并将调度时间划分为n个长度均为T_{slot}的时隙：$T=\{T_0,T_1,T_2,\dots,T_{n-1}\}$。每个网络节点的输出端口处维护两个交替工作的队列，用以存储或转发数据帧。上述模型一般由一个全局定时器和一对 Ping-Pong 队列组成，如图 3 所示。

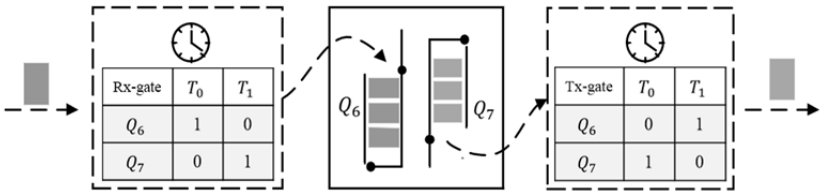


图 3 CQF 机制示意图

在 GCL 的驱动下，Rx 门和 Tx 门在出端口交替地执行入队和出队操作。TSN 网桥的每个出端口维护 8 个优先级队列，其中优先级最高的队列Q_6, Q_7用于转发 TT 流。在偶数周期T_0中，偶数队列Q_6打开 Rx 门，接收来自上游节点的数据帧；奇数队列Q_7则打开 Tx 门，将本节点的数据帧转发到下游节点。在奇数周期T_1中，执行相反的操作。CQF 机制通过周期性地切换两个队列的传输状态，能够保证 TT 流量的确定性延迟通信。TT 流的延迟和抖动界限按照如下公式确定：

$$delay_{max}^{CQF} = (h + offset + 1) \times T_{slot}\,, \tag{2}$$

$$delay_{min}^{CQF} = (h + offset - 1) \times T_{slot}\,, \tag{3}$$

$$jitter^{CQF} \le 2T_{slot} \tag{4}$$

为了避免不同周期流量的相互干扰，CQF 机制将所有流周期的最小公倍数（Least Common Multiple，LCM）定义为调度超周期，可以表示为

$$T_{hyper} = LCM\left(\mathcal{F}_{period}\right), \tag{5}$$

则待调度的时隙集合为$\mathcal{T} = \left\{t_0, t_1, \ldots, t_{T_{hyper}-1}\right\}$。

CQF 机制要求队列中所有数据帧都必须在一个时隙内转发，时隙长度应该足以完成帧的转发，因此有

$$T_{slot}^{min} = \frac{Q_{len}}{BW} + daly_{proc} + daly_{prop} + Sync_{prec}\,, \tag{6}$$

其中，Q_{len}为每个 CQF 队列能容纳的最大字节数，BW 为链路带宽；$daly_{proc}$和$daly_{prop}$分别为数据帧的处理时延和传播时延，$Sync_{prec}$为时钟同步精度。为了最小化延迟抖动，本文规定调度时隙长度为$T_{slot} = T_{slot}^{min}$。

2.4 5G 通信模型

有别于有线媒体，5G 域信道容量的大小取决于信道衰落、干扰和距离等因素，难以保证总是能够提供具有高可靠性和有界延迟的无线资源。为了评估无线网络可实现的延迟、可靠性以及容量，需要建立无线信道模型[12]。

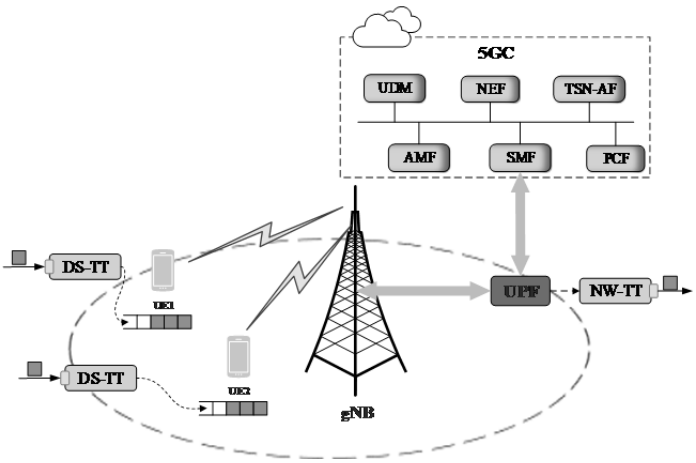


图 4 5G 传输模型

考虑如图 4 所示的上行传输场景下的 5G 移动无线网络模型。5G 节点v_l^{5GS}包含一个 gNB 和M_l个移动 UE。在时隙$t \in \mathcal{T}$处，v_l^{5GS}中 UE 的集合表示为$\mathcal{M}_l = \{1, 2, \dots, m, \dots, M_l\}$。由于 5G 域受到信道条件的可变性和通信环境中噪声的影响，在带宽受限和大规模 TT 流突发的情况下无法保证 CQF 机制的成功执行，因此，本文在每个 UE 侧设计了一个上行传输队列，使得 gNB 能够模拟 CQF 的运行机制，在每个时隙下根据缓冲区中的数据包和最新的 CQI 进行资源配置[13]。

v_l^{5GS}中的用户 UE m侧的上行传输队列表示为$Q_l^m(t)$，定义$h_l^m(t) \in \mathbb{C}$为 UE m 的上行信道增益，并假设$h_l^m(t)$服从瑞利衰落，即

$$h_l^m(t) = \sqrt{PL_l^m(t)}\tilde{h}_l^m(t)\,, \tag{7}$$

其中，$PL_l^m(t)$表示与 UE-gNB 链路的距离相关的路径损失，$\tilde{h}_m(t) \sim \mathcal{CN}(0,1)$表示小尺度衰落。gNB 在时隙$t$接收到的来自 UE m的信号可以表示为

$$y_l^m(t) = h_l^m(t)\sqrt{p_l^m(t)}s_l^m(t) + \delta_l^m(t)\,, \tag{8}$$

其中，$p_l^m(t)$和$s_l^m(t)$分别代表 UE m的传输功率和传输信号，且有$\mathbb{E}[|s_l^m(t)|^2] = 1$；$\delta_l^m(t) \sim \mathcal{CN}(0, \sigma^2)$表示信道$m$中的加性高斯白噪声（Additive White Gaussian Noise，AWGN）。根据以上分析，能够得到 UE m 的上行传输信噪比为

$$SNR_l^m(t) = \frac{|h_l^m(t)|^2 p_l^m(t)}{\sigma^2}\,. \tag{9}$$

假设 5G 节点v_l^{5GS}的上行总带宽为$\mathcal{B}^{uplink}$ Hz，分配给信道m的带宽表示为$B_l^m(t)$，且每个信道的带宽是可配置的。根据香农定理，可以得到每个 UE 的实时信道容量（即信道的传输速率）为

$$R_l^m(t) = B_l^m(t)\log\big(1 + SNR_l^m(t)\big)\,. \tag{10}$$

3 问题建模

3.1 优化问题表述

针对本文所提出的 5G-TSN 融合网络架构，首先需要规划流量注入网络的时隙，以尽可能均衡 CQF 队列负载；接下来，通过分流将超出 CQF 队列容量上限的数据帧部分交由 5G 域传输；5G 域的流量传输依赖于无线带宽资源调度，需要设计合理的带宽分配方案以满足流量传输。因此，对于$\forall m \in \mathcal{M}_l, i \in [1,2,\dots,N^F], j \in [1,2,\dots,n^i]$，总体优化目标可以表示为

$$\max_{\mathcal{F}.offset,\mathcal{F}.prop,\mathcal{B}^t} \frac{\sum_{i=1}^{N^{TT}} F_i^{suc}}{N^F}, \tag{11}$$

具体来说，该优化目标是指在偏移量、CQF 队列长度以及带宽资源约束的条件下，计算分流比例，并分别在 TSN 域和 5G 域进行面向负载均衡的 CQF 队列资源和无线带宽资源的分配，以最大化流量的调度成功率。上述问题可以解耦为注入时隙规划、分流比例求解以及无线带宽分配三个子问题。

3.2 注入时隙规划问题

考虑到每一时隙下的 CQF 队列资源有限，当有大量数据帧同时到达队列时，超出队列部分的数据帧将会被丢弃，进而导致整条流量调度失败，对整个网络的调度性能有较大影响[14]。因此，通过合理调整每条流量注入网络的时隙，均衡 CQF 队列的负载，不仅能够在缓解网络拥塞的同时提升流量的调度成功率，还有助于优化 CQF 队列资源的利用效率。

假设 TSN 交换机v_k^{TSN}在时隙t等待转发的数据帧集合为$\mathcal{F}_k^t$ ($\mathcal{F}_k^t \subseteq \mathcal{F}$)，其邻居节点集合表示为$\mathcal{V}_k \subset \mathcal{V}_{TSN}$，该节点与邻居节点之间的负载取决于$\mathcal{F}_k^t$中所有数据帧的路由路径$f_{i\cdot rp}^j$。$v_k^{TSN}$与$\mathcal{V}_k$中各个节点$v_k^r$之间出端口所占用的队列资源表示为

$$Q_k^r(t) = \sum_{f_i^j \in \mathcal{F}_k^t} \pi_i^j\left(v_k^{TSN}, v_k^r\right), \tag{12}$$

其中，$\pi_i^j(sw_k, v_k^r)$用于表征数据帧f_i^j是否经过链路$[sw_k, v_k^r]$，具体描述为

$$\pi_i^j\left(v_k^{TSN}, v_k^r\right) = \begin{cases} 1, [sw_k, v_k^r] \in f_{i\cdot rp}^j \\ 0, [sw_k, v_k^r] \notin f_{i\cdot rp}^j \end{cases}. \tag{13}$$

本质上，$Q_k^r(t)$表示在时隙t，节点v_k^{TSN}到v_k^r出端口处所占用的 CQF 队列资源。要在 TSN 网络中实现负载均衡，也就是使得$\mathcal{V}_k$中各个节点出端口处队列的最大、最小负载量之间的差值最小。因此，定义队列负载均衡指标为

$$LB_k^r(t) = \max\{Q_k^r(t)\} - \min\{Q_k^r(t)\}. \tag{14}$$

综合上述分析，基于负载均衡的流量调度问题可由 P1 描述。

$$P1: \min_{\mathcal{F}.offset} LB_k(t), \tag{15}$$

$$\text{s.t.}\quad 0 \le f_i.offset \le offset_i^{max}, \forall i \in [1,2,\dots,N^F], \tag{15a}$$

$$f_{i\cdot rp}^j \in f_{i\cdot cpath}, \forall f_i^j \in \mathcal{F}_k^t, \tag{15b}$$

其中，（14a）限制了每条 TT 流偏移量的取值范围。其中，$offset_i^{max} = \min\left\{\frac{f_{i\cdot period} - f_{i\cdot delay}}{T_{slot}}, \frac{f_{i\cdot ddl}}{T_{slot}} - hop_i - 1\right\}, \forall i \in [1,2,\dots,N^F]$。$hop_i$表示 TT 流从源节点到终端节点所经过的最大跳数，即$hop_i = \max\{hop_i^j\}$。(14b) 限制了路由的搜索空间。

3.3 分流问题

定义 TT 流f_i的分流比例为$p_i \in [0,1]$，表示 TT 流f_i中的数据帧分配给 5G 域的比例。f_i经过分流处理后在 TSN 域和 5G 域的数据帧集合可以分别表示为：$\mathcal{F}_{i,tsn} = \{f_{i,tsn}^1, f_{i,tsn}^2, \dots, f_{i,tsn}^j, \dots, f_{i,tsn}^{n_i}\}$，$\mathcal{F}_{i,5g} = \left\{f_{i,5g}^1, f_{i,5g}^2, \dots, f_{i,5g}^j, \dots, f_{i,5g}^{n_i}\right\}$。其中，$f_{i,tsn}^j = (1-p_i)\cdot f_i.size$和$f_{i,5g}^j = p_i \cdot f_i.size$分别为数据帧$f_i^j$在 TSN 域和 5G 域的数据量。因此，整条流$f_i$分配给 TSN 域和 5G 域的数据量分别为$f_{i,tsn} = (1-p_i)\cdot f_i.size \cdot f_i.num$和$f_{i,5g} = p_i \cdot f_i.size \cdot f_i.num$。

定义$Q_{k,l}^{CQF}$为有线链路$[b_k, b_l]$（$b_k, b_l \in \mathcal{V}_{TSN}$，$[b_k, b_l] \in \mathcal{E}$）的出端口队列。为了在确保数据确定性传输的同时提高流量调度的成功率，需要使用 5G 域辅助流量调度，为有线域 CQF 队列分担一部分负载；同时考虑到无线资源有限，需要在满足 CQF 队列约束的前提下，尽可能地节约无线网络资源。因此，可将分流问题定义为 P2 所示的线性规划问题。

$$P2:\quad \min_{p_i} \sum_{f_i \in \mathcal{F}} f_{i,5g}\,, \tag{16}$$

$$\text{s.t.}\quad (12\text{a}), (12\text{b})\,, \tag{16a}$$

$$\sum_{i=1}^{N^{TT}} \left(F_i^{suc} * (1-p_i) * f_i.size * \sum_{j=1}^{n^i} A_{k,l}^t\left(f_i^j\right)\right) \le Q_{len}^{CQF}, \tag{16b}$$

$$0 \le p_i \le 1\,. \tag{16c}$$

其中，（15a）为偏移量与路由约束。（15b）表示 TSN 域 CQF 队列资源的约束，$A_{k,l}^t\left(f_i^j\right)$表示在时隙 t 时数据帧f_i^j在队列$Q_{k,l}^{CQF}$处的到达状态，若f_i^j在时隙 t 到达队列$Q_{k,l}^{CQF}$，则$A_{k,l}^t\left(f_i^j\right) = 1$；反之为 0。（15c）限制分流比例$p_i$的取值范围在 0~1 之间。

3.4 无线带宽分配问题

为了保证无线域的调度性能，定义无线带宽分配的优化问题为：根据调度情况实时分配带宽资源，使得 TT 数据帧在 5G 域的调度成功率达到最大。定义节点v_l^{5GS}处的带宽分配策略为$\mathcal{B}_l(t) = \{B_l^m(t) | \forall m \in \mathcal{M}_l\}$，上述优化问题可由 P3 描述。

$$P3:\ \max_{\mathcal{B}_l(t)} \frac{\sum_{m\in\mathcal{M}^k}\sum_{i=1}^{N^F}\sum_{j=1}^{n_i}\phi_{l,m}^{i,j}(t,\mathcal{B}^t)}{\sum_{i=1}^{N^F} f_{i,5g}}, \tag{17}$$

$$s.t.\ \ B_l^m(t) \geq \beta_{l,m}^t B_{min}, \tag{17a}$$

$$\sum_{m\in\mathcal{M}^k} B_m^k(t) \leq \mathcal{B}^{uplink}. \tag{17b}$$

其中，$\phi_{l,m}^{i,j}(t,\mathcal{B}^t)$用于表征由 5G 节点$v_l^{5GS}$中的 UE m所转发的数据帧f_i^j是否调度成功，成功时为 1；反之为0。（16a）规定了在每个时隙下分配给需要传输数据的 UE 的最小带宽为B_{min}，且$B_{min} < \mathcal{B}^{uplink}/M_l$，UE m 处的队列$Q_l^m(t)$非空时$\beta_{l,m}^t = 1$。（16b）为上行总带宽约束。

4 问题求解

4.2 面向负载均衡的注入时隙规划算法

在 CQF 调度机制下，TT 流的调度顺序对于整体调度成功率具有举足轻重的影响，不同的流排序策略往往会产生不同的调度结果。由于流量的最大允许端到端延迟、生成周期以及数据帧大小都对流量调度具有直接的影响与约束，因此本文同时考虑这三项特征，根据其归一化后的结果计算流量的权重值，进而对 TT 流进行排序以得到新的流量集合$\mathcal{F}'$。

在此基础上，针对 P1 设计了一种面向负载均衡的注入时隙规划算法（Injection Slot Planning Algorithm for Load Balancing，ISPA-LB），如算法 1 所示。具体来说，该算法首先遍历$\mathcal{F}'$中的每条 TT 流，并计算其在不同偏移量取值下的时隙-队列资源映射表，进一步得到 CQF 两个队列的负载均衡指标值，选择最小负载均衡指标所对应的$f_i.offset$值写入列表$\mathcal{F}_{offset}^*$中。经过$iter$轮循环迭代后，$\mathcal{F}_{offset}^*$中最终记录了所有 TT 流的最佳偏移量取值。在给定的迭代次数$iter$下，ISPA-LB 算法对流量集合内的每条流量尝试所有可能的偏移量，并根据 CQF 队列的负载均衡指标来更新其偏移量值，保证算法在每次迭代中都朝着使负载均衡指标更小的方向进行。在搜索空间足够大的情况下，该算法能够以较少的迭代次数找到使得 CQF 队列负载均衡指标最小的偏移量集合。

算法 1：面向负载均衡的注入时隙规划算法

输入：$\mathcal{F}'$，T_{hyper}，$iter$

输出：优化后的偏移量调度策略 $\mathcal{F}_{offset}^*$

```
FOR i in iter，DO
    FOR f_i in F，DO
        初始化lb1_min、lb2_min为正无穷，代表 CQF 两个队列的负载均衡指标
        FOR 0 ≤ f_i.offset ≤ offset_i^max，DO
            T_Q = cal_T_Q (F, T_hyper, f_i·offset)  # 计算时隙-队列资源映射表
            根据式(11)计算 lb1、lb2
        END FOR
```

```
        更新lb1_min、lb2_min
        将lb1、lb2取到最小值时对应的 f_i.offset 写入 F*_offset
    END FOR
END FOR
RETURN F*_offset
```

ISPA-LB 的时间复杂度主要取决于迭代次数、流量数目以及偏移量的搜索范围，每次迭代中调用$cal_T_Q()$计算时隙-队列资源映射表，其复杂度仅与调度的流量数目N_l有关，即为$O(N_l)$，因此算法总的时间复杂度为$O(iter \times N_l \times \lfloor \max(offset_i^{max}) \rfloor)$。算法的空间复杂度主要来自于存储数据结构和辅助变量以及调用$cal_T_Q()$时产生的额外空间。保存中间结果和最优值的辅助变量$f_i.offset$、$lb1_{min}$、$lb2_{min}$占用的空间与输入规模无关，其空间复杂度可视为常数级别。$cal_T_Q()$中会创建一个大小为$T_{hyper} \times 2$的矩阵，其空间复杂度可以视为$O(T_{hyper})$。因此，整体空间复杂度为$O(T_{hyper})$。

4.3 基于线性规划的分流比例求解

由于分流问题 P2 的目标函数为线性，其约束条件也均为线性不等式，因此可以将其抽象为形如式（18）所示的线性规划问题。

$$\min\ C^T P\,, \tag{18}$$

$$s.t.\ \begin{cases} AP \le b \\ 0 \le p_i \le 1 \end{cases}, i \in [1, 2, \dots, N^F]\,, \tag{18a}$$

其中，目标变量P代表 TT 流的分流比例向量，目标函数系数矩阵C表征数据量，具体表示为

$$P = [p_1, p_2, \dots, p_{N^F}]^T, \tag{19}$$

$$C = [f_1.size * f_1.num, f_2.size * f_2.num, \dots, f_{N^F}.size * f_{N^F}.num]^T, \tag{20}$$

不等式系数矩阵A的维度为$(N^{TSN}-1)T_{hyper} \times N^F$，不等式右侧矩阵$b$的维度为$(N^{TSN}-1)T_{hyper} \times 1$，分别由式（21）和（22）表示。

$$A = \begin{bmatrix} F_1^{suc} * \sum_{j=1}^{n^i} A_{1,2}^{t_0}(f_i^j) * f_i.size & \dots & F_{N^F}^{suc} * \sum_{j=1}^{n^i} A_{1,2}^{t_0}(f_i^j) * f_i.size \\ \vdots & \dots & \vdots \\ F_1^{suc} * \sum_{j=1}^{n^i} A_{1,2}^{t_{T_{hyper}-1}}(f_i^j) * f_i.size & \dots & F_{N^F}^{suc} * \sum_{j=1}^{n^i} A_{1,2}^{t_{T_{hyper}-1}}(f_i^j) * f_i.size \\ \vdots & \dots & \vdots \\ F_1^{suc} * \sum_{j=1}^{n^i} A_{3,4}^{t_0}(f_i^j) * f_i.size & \dots & F_{N^F}^{suc} * \sum_{j=1}^{n^i} A_{3,4}^{t_0}(f_i^j) * f_i.size \\ \vdots & \dots & \vdots \\ F_1^{suc} * \sum_{j=1}^{n^i} A_{3,4}^{t_{T_{hyper}-1}}(f_i^j) * f_i.size & \dots & F_{N^F}^{suc} * \sum_{j=1}^{n^i} A_{3,4}^{t_{T_{hyper}-1}}(f_i^j) * f_i.size \end{bmatrix}, \tag{21}$$

$$b=\begin{bmatrix}\sum_{i=1}^{N^{TT}}\left(F_i^{suc}*\sum_{j=1}^{n^i}A_{1,2}^{t_0}(f_i^j)*f_i.size\right)\\ \vdots\\ \sum_{i=1}^{N^{TT}}\left(F_i^{suc}*\sum_{j=1}^{n^i}A_{1,2}^{t_{T_{hyper}-1}}(f_i^j)*f_i.size\right)\\ \vdots\\ \sum_{i=1}^{N^{TT}}\left(F_i^{suc}*\sum_{j=1}^{n^i}A_{3,4}^{t_0}(f_i^j)*f_i.size\right)\\ \vdots\\ \sum_{i=1}^{N^{TT}}\left(F_i^{suc}*\sum_{j=1}^{n^i}A_{3,4}^{t_{T_{hyper}-1}}(f_i^j)*f_i.size\right)\end{bmatrix}-Q_{len}^{CQF}. \tag{22}$$

确定目标函数和不等式约束各项系数的形式后，上述问题可通过单纯形法求解[15]。为了找到线性规划问题初始的基可行解，需要在式（18）的不等式约束中引入松弛变量（Slack Variable，SV）将其化为标准型，如式（23）所示。

$$\max\ -C^T P\,, \tag{23}$$

$$s.t.\quad AP+SV_1=b\,, \tag{23a}$$

$$P+SV_2=1\,, \tag{23b}$$

$$p_i\geq 0, i\in[1,2,\dots,N^F], \tag{23c}$$

其中，SV_1和SV_2由非负常数组成，分别表示为：$SV_1=[p_1',p_2',\dots,p'_{(N^{TSN}-1)T_{hyper}}]$，$SV_2=[p_1'',p_2'',\dots,p'_{N^F}]$。

经过上述分析和标准化处理后，本文采用 Python 所提供的 SciPy 库中的 linprog 函数来求解分流问题 P2，得到每条流量的分流比例。

4.4 基于快速非支配排序的无线带宽分配算法

为了尽可能地提高 5G 域无线资源利用率，本文设计了一种动态按需分配的无线带宽分配方案，首先根据用户队列中的数据量，为每个用户信道计算带宽分配的权重值，节点v_l^{5GS}中信道m在时隙t的权重计算公式为

$$w_{l,m}^t=\frac{\sum_{i=1}^{N^F}\sum_{j=1}^{n_i}\phi_{l,m}^{i,j}(t,\mathcal{B}^t)\cdot f_i.size}{\sum_{f_i\in\mathcal{F}}f_{i,5g}}, \tag{24}$$

上式表示在时隙t，节点v_l^{5GS}中信道m中的数据量与 5G 域总数据量的比例，即为该信道的权重值。为其分配的带宽为

$$B_l^m(t)=w_{l,m}^t\cdot\mathcal{B}^{uplink}. \tag{25}$$

当调度流量的数目增多导致无线带宽资源不足时，本方案以数据帧大小$f_i.size$及其所处信道的增益$f_i.gain$两项特征作为指标进行优先级排序，优先舍弃$f_i.size$较大且$f_i.gain$较小的数据帧，从而节约部分带宽资源来调度其他数据帧。在这种方法下，有限的无线带宽资源能够通过更加合理和充分的利用来满足

大规模流量的调度，避免了大部分数据帧因网络阻塞而调度失败的问题。

$$\max_{\mathcal{B}_l(t)} \{f_i.size, -f_i.gain\}, \tag{26}$$

$$s.t.\quad (14a), (14b). \tag{26a}$$

此时，无线带宽分配问题转换为了式（26）所示的多目标优化问题（Multi-Objective Optimization Problem，MOP），这类问题的解在数学上一般用非支配点来表示，其求解一般是通过 Pareto 改进而达到 Pareto 最优的过程。在多目标优化问题中，Pareto 最优代表了一种资源分配状态，指在不损害任何目标的情况下，不可能再进一步改善某些目标的情况[16]。将数据帧f_i^m、f_j^n（i、$j \in [1,2,\dots,N^F]$，m、$n \in [1,2,\dots,n_i]$）的支配关系定义为

$$\begin{cases} f_i^m \prec f_j^n, (f_{i\cdot size}^m > f_{j\cdot size}^n)\ or\ (f_{i\cdot size}^m = f_{j\cdot size}^n\ and\ f_{i\cdot gain}^m < f_{j\cdot gain}^n) \\ f_i^m \parallel f_j^n, f_{i\cdot size}^m = f_{j\cdot size}^n\ and\ f_{i\cdot gain}^m = f_{j\cdot gain}^n \end{cases}. \tag{27}$$

快速非支配排序（Fast Non-dominated Sorting，FNS）算法作为求解 MOP 的常用方法，其主要思想是对问题的解集进行排序，然后根据各个解之间的支配关系将解集划分为多个称为 Pareto 前沿的层级，然后在每个层级中进一步判断解之间的支配关系，以确保每个解都被正确地分类到相应的层级中。

基于上述分析，本文提出一种基于快速非支配排序的带宽分配算法（Bandwidth Allocation Algorithm Based on Fast Non-dominated Sorting，BA-FNS）用于实现本节所设计的无线带宽分配方案，如算法 2 所示。假设 5G 节点v_l^{5GS}中 UE $m(m \in \mathcal{M}_l)$处的缓冲队列中的数据帧集合为$\mathcal{F}_l^m = \{f_{l,1}^m, f_{l,2}^m, \dots, f_{l,i}^m, \dots, f_{l,n}^m\}$，定义由数据帧$f_{l,i}^m$所支配的帧集合为$f_i^{dom} = \{f_{i,1}^{dom}, f_{i,2}^{dom}, \dots, f_{i,n_i}^{dom}\}$，$f_{l,i}^m$被支配的次数记为$count_i^{dom}$。

算法 2：基于快速非支配排序的带宽分配算法

输入：$\mathcal{F}_l^m$，5G 节点v_l^{5GS}在时隙 t 下的无线通信相关参数
输出：无线带宽优化调度策略$\{\mathcal{B}_l(t)^*\}$
BEGIN
1：初始化已分配的带宽$\mathcal{B}_l(t) = \phi$，$A_l^t = 0$
2：**FOR** m in M_l，DO
3：　IF $\beta_{l,m}^t = 1$，DO
4：　根据式（22）分配带宽
5：**END FOR**
6：**IF** $A_l^t > \mathcal{B}_l$，**THEN**
7：　$\mathcal{P}_l^m = FNS(\mathcal{F}_l^m)$ # 对节点中的数据帧进行 FNS 排序
8：　**WHILE** $A_l^t > \mathcal{B}_l$ and $\mathcal{F}^i$ in $\mathcal{P}_l^m$，**DO**
9：　　**FOR** $f_{l,i}^m$ in $\mathcal{F}^i$, **DO**
10：　　从队列 Q_l^m中移除数据帧 $f_{l,i}^m$，并将该帧的传输状态设为失败
11：得到$\{B_l^m(t)^*\}$
END

BA-FNS 算法首先采用按需分配的原则为 UE 分配带宽，其时间复杂度取决于 UE 的数量，即$O(l)$；当带宽不足时，FNS 首先初始化每个解的支配解集和非支配次数，并与其他解进行比较，以确定是否存在支配关系，时间复杂度为$O(n^2)$[17]；调整带宽分配的时间复杂度为$O(n)$；因此，BA-FNS 算法总的时间

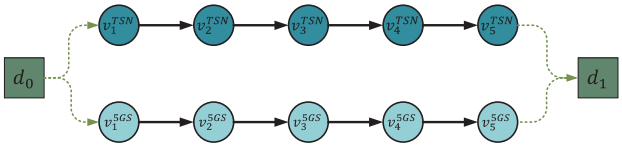
复杂度为$O(l+n^2+n)$。由于算法需要存储每个 UE 的带宽分配情况以及每个数据帧的传输状态，因此总的空间复杂度为$O(l+n)$。

5 仿真分析

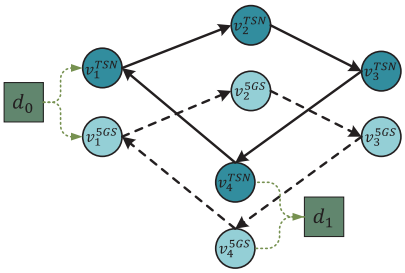
针对本文所提出的 5G-TSN 融合网络架构及协同调度机制，本节设计了一系列仿真实验，以流量的调度成功率为主要指标，在 Python 仿真环境下进行了测试与验证。

5.1 仿真设置

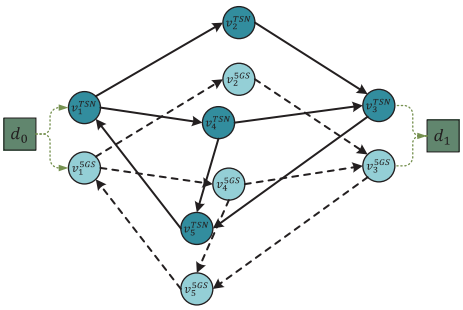
为了评估所提模型与算法的可扩展性，设计了线型、环型以及混合型三种拓扑结构，如图 5 所示。在有线域，链路带宽为$1000\ Mbps$，每个 TSN 网桥出端口 CQF 队列长度为$10\times1500\ B$。在无线域，5G 节点的上行总带宽$\mathcal{B}^{uplink}$为$100MHz$，上行额定功率为$3W$，AWGN 的方差$\sigma^2=-90dB$。



(a) 拓扑 1



(b) 拓扑 2



(c) 拓扑 3

图 5 仿真网络拓扑

TT 流根据式（1）所列的流特征随机生成，其数据帧大小$\mathcal{F}_{size}$为$100\sim1000B$范围内的随机整数。此外，为了进一步评估网络模型与调度算法的鲁棒性，本文选定了三种$f_i.period$和$f_i.ddl$组合方案，如表 1 所示。其中的数值均以时隙长度为单位，$1slot=125\mu s$。

表 1 $f_i.period$和$f_i.ddl$组合方案

组合方案	$f_i.period$	$f_i.ddl$	T_{hyper}
方案 1	{16，48，80}	{8，16，32}	240
方案 2	{32，48，64}	{16，24，32}	192
方案 3	{32，40，48}	{8，16，32}	480

5.2 结果分析

针对 ISPA-LB 算法，本文采用差分进化（Differential Evolution，DE）、禁忌搜索（Tabu Search）算法以及 Naïve 方法作为基线方案，选择如图 5（b）所示的拓扑结构，并仅在有线域中与 ISPA-LB 算法进行对比实验。经前期验证，ISPA-LB 算法在迭代三次时即可达到较好效果，因此设置该算法的迭代次数为 3。

在综合考虑算法的搜索空间与计算成本后，设置 DE 算法的迭代次数和种群大小分别为 10 和 100，缩放因子和交叉概率分别设置为$F = 0.4$和$Cr = 0.5$；Tabu 算法的列表大小设置为 20，最大迭代次数和重复次数分别为 10 次和 20 次；在每次迭代产生 10 个候选解。

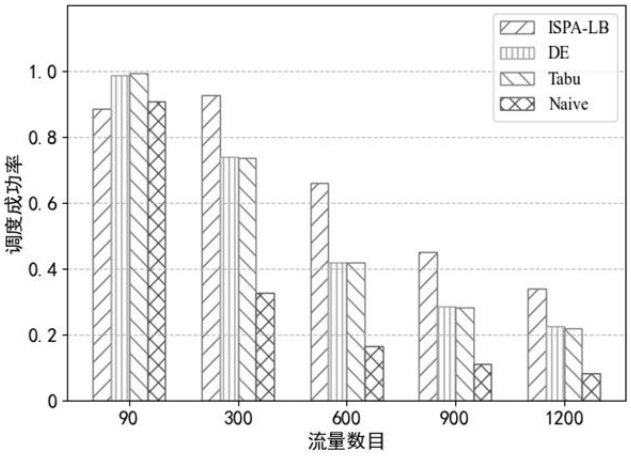


图 6 负载均衡算法对比

算法对比结果如图 6 所示。当流量数目为 90 时，可能由于流量周期与截止期限的限制，导致小部分流量调度失败，ISPA-LB 算法的调度成功率为 98.79%，与 DE 和 Tabu 相比，其优势并不明显；随着流量数目增多，ISPA-LB 算法在提升网络调度能力方面整体效果突出。以 900 条流量为例，负载均衡前（Naive）的调度成功率仅为 10.91%，而在使用 ISPA-LB 算法进行负载均衡后，成功率提升到了 46.42%，相比于 DE 和 Tabu 算法也有 40%左右的提升。

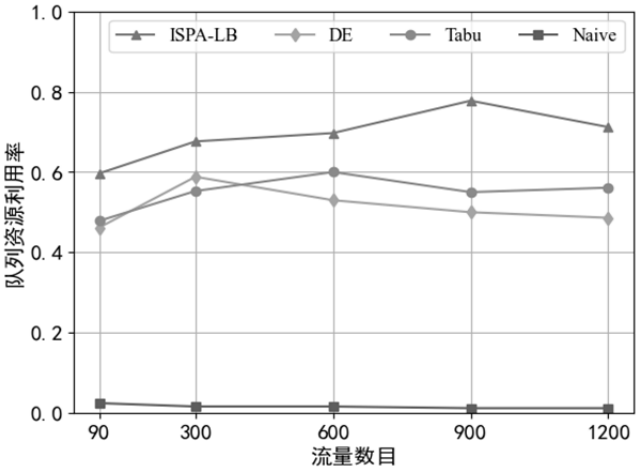


图 7 队列资源利用率对比

图 7 展示了 TSN 中使用 ISPA-LB、DE、Tabu 以及未进行偏移量调度四种情形下的 CQF 队列资源利用率情况。队列资源利用率定义为在流量调度过程中参与调度的 CQF 队列占网络中总队列数量的比例。由上图可知，ISPA-LB 算法对于队列资源利用率的提升效果明显，使得 CQF 队列资源得到更为充分的利用。

针对无线域的 BA-FNS 带宽分配算法，选用平均分配法（Equal Allocation，EA）、最大-最小公平性法（Max-Min Fairness，MMF）以及比例公平性法（Proportional Fairness，PF）三个基线方案，在图 5（b）所示的拓扑下设置对比实验。在 TSN 域采用 ISPA-LB 算法，5G 域采用不同带宽分配方案时整体网络的调度效果对比如图 8 所示。

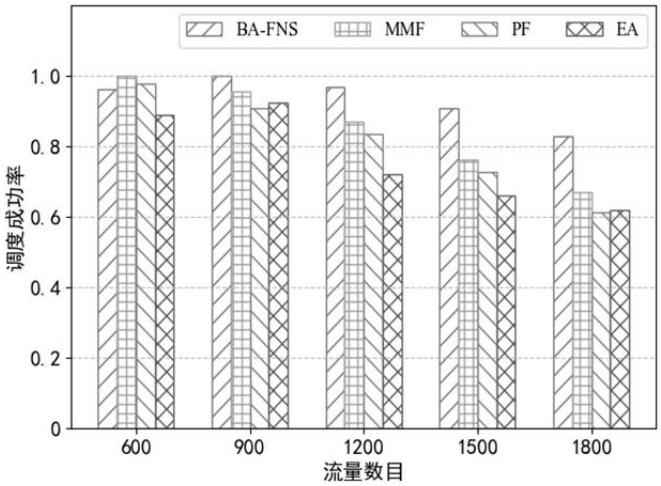


图 8 带宽分配方案对比

相比于单层的 TSN 网络，5G-TSN 融合网络整体的调度能力有大幅提升，对于 1800 条以内的流量，其成功率均在 60%以上。当 5G 域采用 BA-FNS 带宽分配算法时，调度成功率均在 80%以上。当流量数目为 1500 时，BA-FNS 算法的调度成功率为 90.69%，比 MMF 方案高 14.42%；当流量数目为 1800 时，BA-FNS 算法的调度成功率为 82.91%，比 EA 方案高 16%。由此能够推断，在大规模待调度流量的情形下，BA-FNS 算法的优势更加突出。

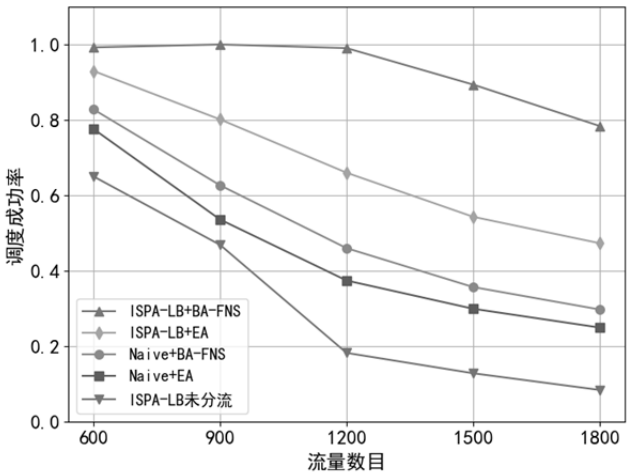


图 9 联合优化算法有效性测试

图 9 展示了在无线域使用 EA 分配带宽、分流前后等情况与采用联合优化算法 ISPA-LB+BA-FNS 时的调度成功率对比。当只调用 ISPA-LB 算法调整流量的注入时隙但不进行分流时，整体调度成功率最低。Naive+EA 和 Naive+BA-FNS 曲线代表不进行注入时隙规划而直接分流的情况，由于有线域 CQF 队列拥塞，

大部分数据被分到了无线域，虽然优于未分流的情况，但由于无线资源的限制，其成功率随流量数目的增加明显降低。由于 BA-FNS 算法能够更好地应对大规模流量调度场景，因此 Naive+BA-FNS 的成功率高于 Naive+EA。ISPA-LB+EA 与 ISPA-LB+BA-FNS 两条曲线的走势与图 8 中所呈现的趋势一致。通过以上分析能够推断出：通过分流使用无线域对有线域的调度进行辅助，能够明显地提升整体网络的调度性能；在调度之前，对流量进行注入时隙规划以尽可能地均衡负载对于后续调度过程至关重要。

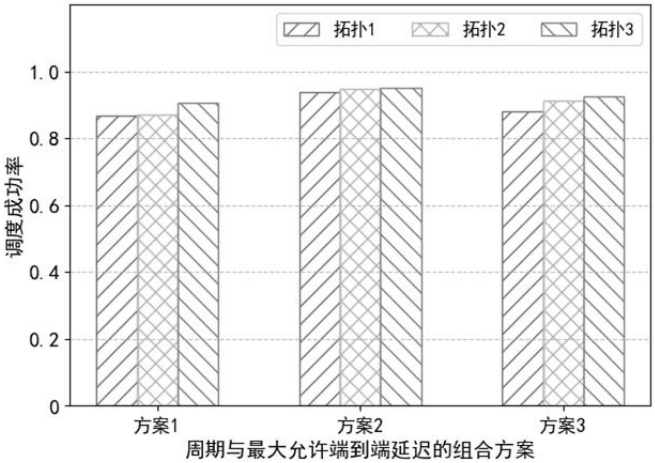


图 10 不同组合方案和网络拓扑的调度成功率对比

图 10 呈现了算法在不同组合方案下、不同拓扑中调度 900 条流的性能表现。与前两种拓扑相比，拓扑 3 中由于存在更多的路由路径，在调度流量时具有更多优势，因此其调度成功率均在 90%以上。在不同$\mathcal{F}_{period}$、$\mathcal{F}_{ddl}$组合方案下，联合优化算法确保了网络的流量调度成功率均在 80%以上。因此，本文所提出的 ISPA-LB+BA-FNS 联合优化算法能够较好的适应不同的$\mathcal{F}_{period}$、$\mathcal{F}_{ddl}$组合和不同的网络拓扑，具有良好的鲁棒性。

6 结束语

本文提出一种新型 5G-TSN 融合网络架构，并针对该网络架构设计了相应的流量调度方案与优化算法，旨在实现网络调度性能的最优化。本文所构建的 5G-TSN 融合网络能够支持数据帧以有线和无线自适应的方式进行传输，在该架构下，提出一种面向负载均衡的注入时隙规划算法对流量的偏移量进行求解，根据实际调度的数据量采用线性规划的方法求解分流比例，进一步，在无线域提出一种基于快速非支配排序的带宽分配算法对无线带宽资源进行调度。与基线方案相比，本文算法在提升流量调度成功率方面效果显著，5G-TSN 融合网络架构展现出了强大的灵活性与调度能力。

参考文献

[1] Farkas J, Bello L L, Gunther C. Time-Sensitive Networking Standards[J]. IEEE Communications Standards Magazine, 2018, 2(2): 20-21.

[2] 未来网络白皮书——确定性网络技术体系白皮书[EB/OL]. [2024-05-06]. http://www.ecconsortium.org/Uploads/file/20210830/1630321593154007.pdf.

[3] 5G+TSN 融合部署场景与技术发展白皮书[EB/OL]. [2024-05-06]. https://aii-alliance.org/uploads/1/20220106/aa59fab3fb22ae7c8e6ed944a103879c.pdf.

[4] Larrañaga A, Lucas-Estañ M C, Martinez I, et al. 5G Configured Grant Scheduling for 5G-TSN Integration for the Support of Industry 4.0[C]//2023 18th Wireless On-Demand Network Systems and Services Conference (WONS). Madonna di Campiglio, Italy: IEEE, 2023: 72-79.

[5] 3GPP. TS 24.535[EB/OL]. [2024-05-06]. Specification # 24.535 (3gpp.org).

[6] Martenvormfelde L, Neumann A, Wisniewski L, et al. A Simulation Model for Integrating 5G into Time Sensitive Networking as a Transparent Bridge[C]//2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA): Vol. 1. 2020: 1103-1106.

[7] Cheng Z, Yang D, Guo R, et al. Joint Time-Frequency Resource Scheduling Over CQF-Based TSN-5G System[C]//2023 15th International Conference on Communication Software and Networks (ICCSN). 2023: 60-65.

[8] Luque-Schempp F, Panizo L, Gallardo M del M, et al. Toward Zero Touch Configuration of 5G Non-Public Networks for Time Sensitive Networking[J]. IEEE Network, 2022, 36(2): 50-56.

[9] Li M, Guo S, Chen C, et al. DecAge: Decentralized Flow Scheduling for Industrial 5G and TSN Integrated Networks[J]. IEEE Transactions on Network Science and Engineering, 2023: 1-13.

[10] Rost P M, Kolding T. Performance of Integrated 3GPP 5G and IEEE TSN Networks[J]. IEEE Communications Standards Magazine, 2022, 6(2): 51-56.

[11] Val I, Seijo O, Torrego R, et al. IEEE 802.1AS Clock Synchronization Performance Evaluation of an Integrated Wired–Wireless TSN Architecture[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 2986-2999.

[12] Jaeckel S, Raschkowski L, Borner K, et al. QuaDRiGa: A 3-D Multi-Cell Channel Model With Time Evolution for Enabling Virtual Field Trials[J]. IEEE Transactions on Antennas and Propagation, 2014, 62(6): 3242-3256.

[13] Li X, Li D, Wan J, et al. A review of industrial wireless networks in the context of Industry 4.0[J]. Wireless Networks, 2017, 23(1): 23-41.

[14] Guidolin–Pina D, Boyer M, Boudec J Y L. Configuration of Guard Band and Offsets in Cyclic Queuing and Forwarding[J]. IEEE/ACM Transactions on Networking, 2023: 23-41.

[15] Dantzig G B. Origins of the simplex method[M]//Nash S G. A history of scientific computing. New York, NY, USA: ACM, 1990: 141-151.

[16] Srinivas N, Deb K. Muiltiobjective Optimization Using Nondominated Sorting in Genetic Algorithms[J]. Evolutionary Computation, 1994, 2(3): 221-248.

[17] Roy P C, Deb K, Islam Md M. An Efficient Nondominated Sorting Algorithm for Large Number of Fronts[J]. IEEE Transactions on Cybernetics, 2019, 49(3): 859-869.

[作者简介]

苏慧（1998-），女，博士研究生，主要研究方向为工业互联网。

贾杰（1980-），女，博士，东北大学教授、博士生导师，主要研究方向包括工业互联网，5G、物联网与大数据分析等。

薛祎（1996-），男，博士研究生，主要研究方向包括优化理论、非正交多址技术（NOMA）、网络切片、5G-TSN 等。

陈剑（1980-），男，博士，东北大学教授、博士生导师，主要研究方向包括 5G/B5G/6G、智能无线通信、大数据、人工智能等。

王兴伟（1968-），男，博士，东北大学教授、博士生导师，主要研究方向包括互联网、云计算和网络空间安全等。

Rolling Bearings Intelligent Fault Diagnosis Method Based on TTS-GAN Model Transfer Learning

Shuang Liu[1],Zhuolun Tan[2], Junan Chen[3],Hongwei Yang[4],Haijiang Zhu[5],Lina Zhao[*]

Abstract — **One of the challenges in rolling bearing fault diagnosis is the limited availability of fault sample data. This necessitates the use of data-driven fault diagnosis models, which require significant time and computational resources during the training process. To enhance the accuracy of fault identification, a transfer learning intelligent fault diagnosis method for rolling bearings based on TTS-GAN (Transformer Time-Series GAN Model Architecture) model was proposed. This employs data augmentation-based mechanical fault generation adversarial network to obtain sufficient expanded fault samples for fault classification. Firstly, the vibration signals of rolling bearings in different health categories are generated into corresponding training set and test set; secondly, the pre-trained TTS-GAN model is transferred to the training set through parameter sharing and fine-tuning to achieve the optimal parameters of the model; finally, the fault diagnosis capability of the model is verified by the test set. The method is validated on the Case Western Reserve University (CWRU) rolling bearing dataset.**

Keywords—**Rolling bearing，Intelligent fault diagnosis, Generative Adversarial Networks, Transformers, Transfer Learning, time series, TTS-GAN**

I. INTRODUCTION

Intelligent fault diagnosis has become a highly recognized and promising approach in the field of smart manufacturing. Typically, deep neural network-based intelligent diagnostic models are based on the analysis of a large amount of machine monitoring data. The more complete the training dataset is and the richer the types of faults contained in it, the better the performance of the trained intelligent diagnosis model will be. However, in engineering scenarios it is difficult to obtain an ideal dataset to train the intelligent diagnostic model due to various reasons. Therefore, the small sample problem becomes a limitation of intelligent fault diagnosis applications in real industrial manufacturing [1]. (1) In engineering, machines usually run normally and rarely fail. Although there are conditional monitoring systems that can collect machine operation data continuously in real time, most of the data collected are health data and only a small amount of fault data. Therefore, in real-world engineering scenarios, it is difficult to obtain enough fault data to support the training of intelligent diagnostic models, especially for the identification and prediction of rare faults. (2) Fault simulation experiments in the laboratory to collect fault data are very expensive in terms of cost. For example, to obtain failure data for gears, researchers

need to purchase gear specimens and artificially create failures by wire cutting or other means. Specialized failure simulation test benches would also need to be set up to collect this data. This type of experiment is not only costly, but also requires a large investment in labor. (3) Failure data obtained through computer simulation has certain limitations in practical applications. High-precision simulation and analysis models of complex mechanical systems are established to obtain samples reflecting different types of failures under actual operating conditions. However, relying only on numerical simulation methods cannot fully ensure that the system dynamics model of the mechanical structure containing faults matches the actual physical system. Different operating environments and operating conditions have a great influence on the fault data, so the fault data obtained through simulation is usually not very applicable [1].

Therefore, when performing intelligent fault diagnosis in engineering scenarios, the typical problem of small sample unbalanced data is faced. Due to the lack of sufficient fault sample data, it is difficult to establish an effective intelligent diagnosis model for accurate fault identification. In recent years, data-driven intelligent fault diagnosis has attracted much attention and achieved good research results.

The current research in intelligent fault diagnosis is mainly:

- Traditional fault diagnosis methods based on signal processing are used to diagnose faults by spectral analysis of signal eigenvalues. Different types of faults cause the measured signals to exhibit different spectral, variance, amplitude, and other eigenvalue representations. Representative methods include wavelet transform [2], empirical modal decomposition [3], and blind source separation techniques [4].
- The machine learning based composite fault diagnosis process of bearings uses training set data to train the machine learning model. Different classification algorithms or regression prediction models can be selected according to different fault types, e.g., Support Vector Machine [5] (SVM), Random Forest [6] (RF), etc. The model can be trained using the data from the training set. During the training process, the parameters of the model need to be adjusted to achieve the best performance. ABBASION et al [7] researchers used wavelet analysis and support vector machine (SVM) to optimize the level of signal decomposition to classify a wide range of faults in bearings. Yin et al [8] reviewed the research and development of Support Vector Machine (SVM) based fault diagnosis and monitoring methods. Widodo et al [9]described the use of Support Vector Machines (SVM) for machine condition monitoring and fault diagnosis.
- Deep Learning (DL) is highly regarded in the field of bearing fault diagnosis. It eliminates the need for elaborate characterization of data, thus reducing the complexity and cost of feature extraction in fault diagnosis. In addition, deep learning has more layers and exhibits more powerful capabilities in feature extraction and fault classification than traditional shallow learning models. Huang et al [10] proposed a novel fault diagnosis method based on a combination of Convolutional Neural Networks (CNNs) and Long Short-Term Memory Networks (LSTMs) with a two-part sliding window processing and CNN-LSTM model; Chen et al [11] proposed an automatic

feature learning neural network using raw vibration signals as inputs, and two convolutional neural networks with different kernel sizes were used to automatically extract different frequency signal features from the raw data. Then the long and short-term memory is used to identify the fault types based on the learned features; Gu et al [12] proposed a hybrid rolling bearing fault diagnosis method based on variational mode decomposition (VMD), continuous wavelet transform (CWT), convolutional neural network (CNN), and support vector machine (SVM) that is suitable for small-sample processing; Wen et al [13] proposed a LeNet-5 based novel CNN for fault diagnosis. By a conversion method that converts signals into two-dimensional (2-D) images, the method can extract features from the converted 2-D images and eliminate the effect of hand-crafted features.

Among them, data augmentation using models such as Generative Adversarial Networks [14] (GANs) has been proved to be an effective way to improve the generalization performance of neural networks, which is of great significance in solving the small-sample intelligent fault diagnosis problem.The GANs give full play to their role in numerical analog simulation and on-line monitoring of the data, and successfully extend the training dataset of the intelligent diagnosis model, and in the direction of augmenting the data achieved success [15][16][17].

Unfortunately, GANs suffer from well-known training instability, and many efforts have been devoted to stabilizing GAN training by introducing various regularization terms [18][19][20] and better losses [21]. One of the important ways to improve GANs is to examine their neural structure. Popular neural architectures perform quite well when used as (generator) backbones, where the neural architectures for time series GANs are mainly RNNs [22][23][24].

Transformer [18] (Transformer), on the other hand, is good at dealing with long sequences of signals and has a strong global feature extraction capability, which can effectively model vibration signals globally. Attempts have been made to apply the transformer model to GAN architectures with the aim of improving the quality of synthetic data or creating a more efficient training process for image and text generation tasks. For the first time in the literature [26], a fully convolution-free GAN model based purely on the transformer architecture was built and verified to perform well in several image synthesis tasks. Based on this, literature [14] applies this transformer-based GAN model to time series data and the authors propose a transformer-based TTS-GAN model for generating realistic time series data.

The generative model proposed in literature [14] can be used as a data engine to alleviate the challenges of data collection. Previous efforts to create time-series GANs have relied heavily on Recurrent Neural Network (RNN)-based architectures. Since transformer was originally invented to handle very long sequence data and does not have the vanishing gradient problem, theoretically, transformer GAN models should outperform other RNN-based models on time series data. The data collected in the intelligent fault diagnosis of rolling bearings are vibration signals, which are also a kind of time series, so the introduction of this model into the field of rolling bearing fault diagnosis should be able to solve the problem of lack of samples very well.

In recent years in the field of data-driven fault diagnosis based, transfer learning has also received

more and more attention, and its main idea is to solve the problem in the relevant neighborhood (target domain) by known domain knowledge (source domain) [28]. Transfer learning simplifies the training process of the network model and requires only a small number of training samples, which saves training time and computational resources. Li et al [29]proposed a parameter-based transfer learning and convolutional auto-encoder (CAE) approach for small-scale wind turbine fault diagnosis. The proposed method can transfer knowledge from similar wind turbines to the target wind turbine; Huang et al [30] proposed a fault diagnosis method based on adversarial transfer learning and multi-task learning. First, known faults and unknown faults are distinguished by an adversarial transfer method with sample weights. Second, the fault classification module and fault localization module trained by multi-task learning are used to classify and localize the known faults; Pan et al [31] proposed a transfer learning fault diagnosis method based on Improved Completely Integrated EMD (ICEEMDAN), which extracts the fault features in the original signals using ICEEMDAN, and the pre-trained one-dimensional VGG16 model through the target dataset is training and fine-tuning the related parameters.

Based on this, this paper proposes a transfer learning fault diagnosis method based on TTS-GAN model.The basic idea is to use the weight values of the pre-trained network model as the initialized weight values, migrate to the target domain to continue training and fine-tuning, in order to obtain the optimal parameters of the diagnostic model for the accurate diagnosis of faults. Our contribution:

- The proposed transfer generation model can serve as a data engine to alleviate the challenge of collecting rolling bearing fault data and solve the small sample problem of bearing faults;
- The proposed transfer generation model simplifies the training process of network models, requiring only a small number of training samples, saving training time and computational resources.
- The GAN model based on the Transformer architecture is more suitable for applying to time series data compared to other GAN models that rely on neural architectures such as RNN and CNN, and the training is more stable;
- For the first time, the GAN model based on Transformer architecture was applied to bearing fault diagnosis and tested on the CWRU dataset.

Manuscript received 7. 10, 2024; accepted XX. XX, 2018.

XXXX XXXX XXXX XXXX, Beijing 100000, China; XXXX XXXX XXXX XXXX, Cambridge CB21QY, UK.

This work is supported by the National Natural Science Foundation of China under Grant 92367111.

II. Model-based transfer learning

2.1 TTS-GAN model

Li et al [14] proposed a new neural network model, TTS-GAN, which has a generator discriminator approach as shown in Fig. 1. Through experimental studies on three datasets Simulated sinusoidal waves, UniMiB human activity recognition (HAR) dataset and

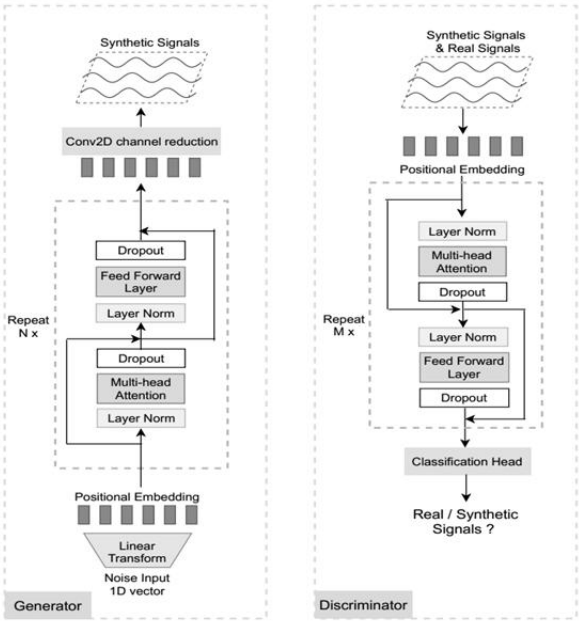


Figure 1 TTS-GAN model architecture

the PTB Diagnostic ECG Database, TTS-GAN is demonstrated to serve as a real time series generator of real time series.

The structure of the model consists of two core components: the generator and the discriminator. Both components are designed based on the transformer encoder architecture [6]. The encoder consists of two composite modules, the first of which employs a multi-attention mechanism to capture the global information of the input sequence, while the second is a feed-forward MLP with a RELU activation function for further processing of the encoder's output. Before each block, the encoder applies a normalization layer to speed up the training process and improve the generalization ability of the model. In addition, after each block, a culling layer is added to prevent the occurrence of overfitting phenomenon. In order to better utilize the past information, residual concatenation is applied to both blocks. This design helps to improve the stability and accuracy of the model.

2.2 TTS-GAN transfer learning model

The purpose of transfer learning is to solve the problem of less labeled or unlabeled data in the target domain as well as large differences in the characteristics of the source and target domains, and the current research methods can be summarized and categorized into three types of model transfer and parameter fine-tuning based methods, feature matching based methods, and adversarial adaptive based methods. The model transfer and parameter fine-tuning based mechanical diagnosis method is the most commonly used method, which utilizes the parameters of the pre-trained network model as initialization parameters and migrates to the target domain to continue training and fine-tuning, and the typical structure is shown in Figure 2.

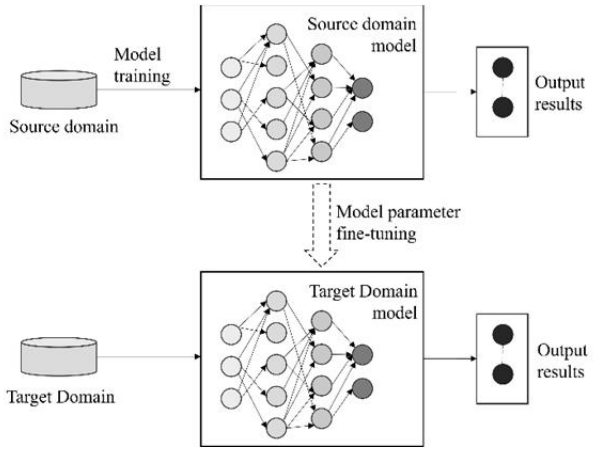


Figure 2 Transfer structure based on model transfer and parameter fine-tuning

The TTS-GAN model can well expand the physiology-based time series signals, taking into account the similarity of the generated sequences, and at the same time learning the temporal and spatial information contained in the time series signals. The parameter sharing and fine-tuning (fine-tune) in transfer learning is applied to the rolling bearing dataset to complete the training of the network model on the target domain and solve the problem of insufficient fault sample data. Firstly, the TTS-GAN model is used as the backbone model and its parameters trained in the source domain are frozen to realize parameter sharing; then the inputs of the TTS-GAN model are replaced with the target domain dataset to train the network model using the data in the target domain, to complete fine-tuning of the parameters of the whole network and to train to get the parameters of the final classification. As shown in Fig. 3, by migrating the model and using parameter sharing and fine-tuning, the training process of the model in the new domain is greatly simplified.

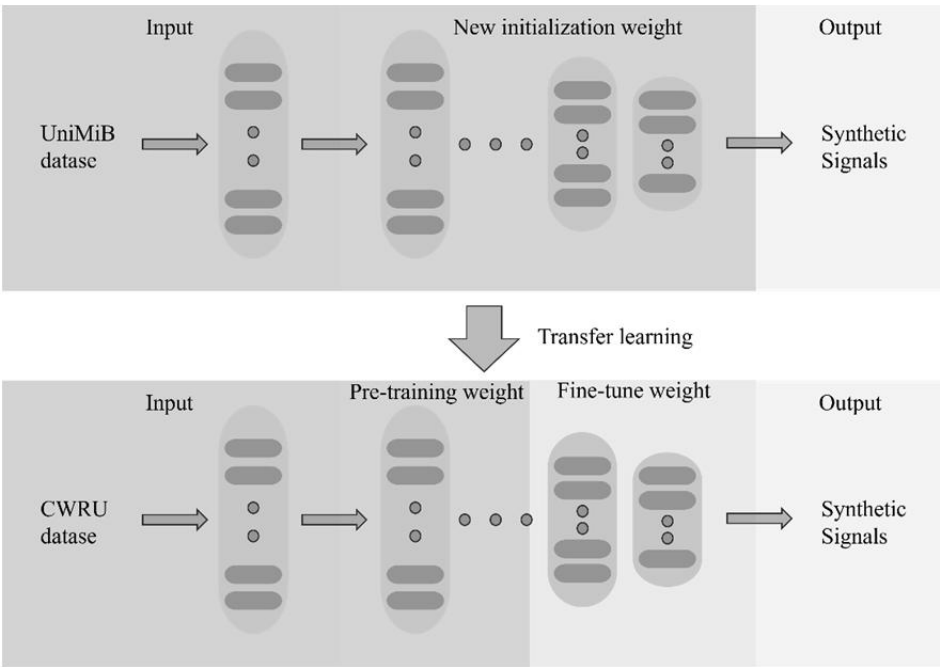


Figure 3 Model-based transfer learning

2.3 Fault diagnosis method based on model transfer learning

Generator A one-dimensional vector with N uniformly distributed values in the range (0,1) is first received, and the generator maps this vector into a sequence with the same length as the real signal and embedding dimension M. The generator splits the sequence into segments, and a position encoding value is added to each segment in order to preserve the segment's positional information in the sequence. These segments are then fed into a transformer encoder block, which generates the corresponding encoding based on the input information. The dimension of the

synthesized data is reduced after the output of the encoder block is processed by the Conv2D layer.

The synthetic data sequence obtained after processing in the transformer encoder layer of the generator will be mapped to (real data dimension, 1 , time step) in terms of shape, so that it is able to convert random noise vectors into sequences that have the same shape as the real signals, thus achieving the purpose of simulating real signals. In this process, the generator makes full use of the tuning space of the hyperparameters, as well as the processing power of the transformer encoder module, so that the synthesized signal is much closer to the real signal in both shape and content.

Discriminator The structure is similar to the ViT model, which is a binary classifier used to distinguish whether the input sequence is a real or synthesized signal. In the ViT model, the image is divided equally into multiple patches with the same width and height. However, in this experiment, we treat any input sequence as an image with height 1. Therefore, to add positional coding to the time series input, we simply divide the width equally into multiple patches and keep the height of each patch constant.

Generator and Discriminator Parameter Updates The parameters are updated using mean square error loss. z denotes the input vector of the generator and $G(z)$ denotes the synthetic data generated by the signal generator, using the prefix real to denote the real input signal. $d(x)$ is the classified output of the discriminator. x can be either a real signal or a synthetic signal. $real_label$ is set to 1 and $fake_label$ is set to 0.

The loss of the discriminator is the sum of the loss of the real data and the loss of the synthesized data, and the discriminator loss can be expressed as:

$$d_real_loss = MSELoss(D(real), real_label)$$
$$d_fake_loss = MSELoss(D(G(z)), fake_label)$$
$$d_loss = d_real_loss + d_fake_loss$$

The generator loss can be expressed as:

$$g_loss = MSELoss(D(G(Z)), real_label)$$

III. Experimentation and analysis

3.1 Experimental setup

Experimental platform [32] As shown in Figure 4, the CWRU bearing test platform consists of: a 1.5KW (2 hp) motor (left side of the figure); a torque transducer/translator (connection in the middle of the figure); a power test meter (right side of the figure); and an electronic controller (not shown in the figure).

The bearings to be tested support the motor's rotating shaft; the drive-side bearings are SKF6205, with sampling frequencies of 12Khz and 48Khz; the fan-side bearings are SKF6203, with a sampling frequency of 12Khz.

Signal Acquisition Since the location of the outer ring damage is relatively fixed, the different locations of the damage point relative to the bearing load zone have a direct effect on the vibration response of the motor/bearing system. In order to quantify this effect, the damage points on the outer ring of the drive-end and fan-end bearings were placed at three different locations: 3 o'clock, 6 o'clock, and 12 o'clock, respectively. The vibration signals were acquired by a 16-channel data logger. By placing accelerometers on the drive end, fan end, and base (normal data) of the motor housing, vibration data can be acquired at three different locations. These data are distinguished by the fact that the vibration signals they measure reflect different physical phenomena and characteristics, thus providing different information for troubleshooting and

monitoring. Power and speed are measured by means of a torque transducer/translator. The machined faulty bearings were reloaded into the test motor and the vibration acceleration signal data were recorded at 0, 1, 2 and 3 horsepower motor load operating conditions.

Normal samples obtained using this test bench 8, outer ring damage samples 53, inner ring damage samples 23 and rolling element damage samples 11.

Dataset The Western Reserve University bearing dataset provides experimental data under different operating conditions, including different rotational speeds, loads and other parameters. There are several samples of different working conditions in each failure mode. In this paper, accelerometer data from the drive end of a 0.007-inch inner ring failed bearing under normal operating conditions and 0 hp load are selected as real data samples for testing.

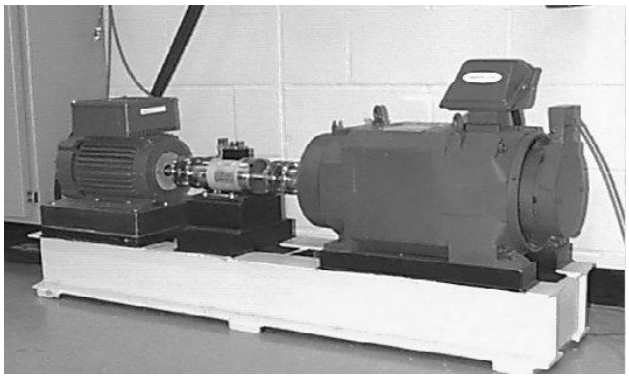


Figure 4 Bearing Fault Experimental Platform

3.2 Data Preprocessing

For the real normal data samples and real fault data samples, 120,000 of them are selected as the dataset to be processed. Next, the dataset to be processed is sliced. As in Fig. 5, the data are sliced according to the step $time_step$=150 and $overlap_ratio$=0.5.

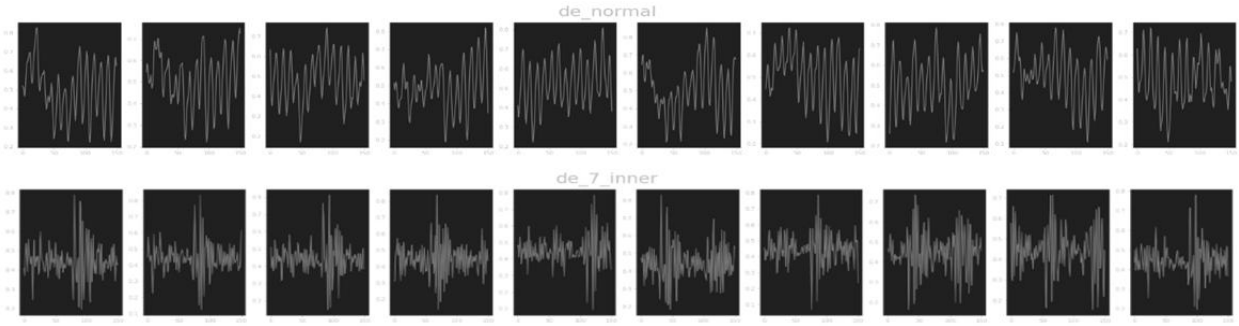


Figure 5 Sliced data

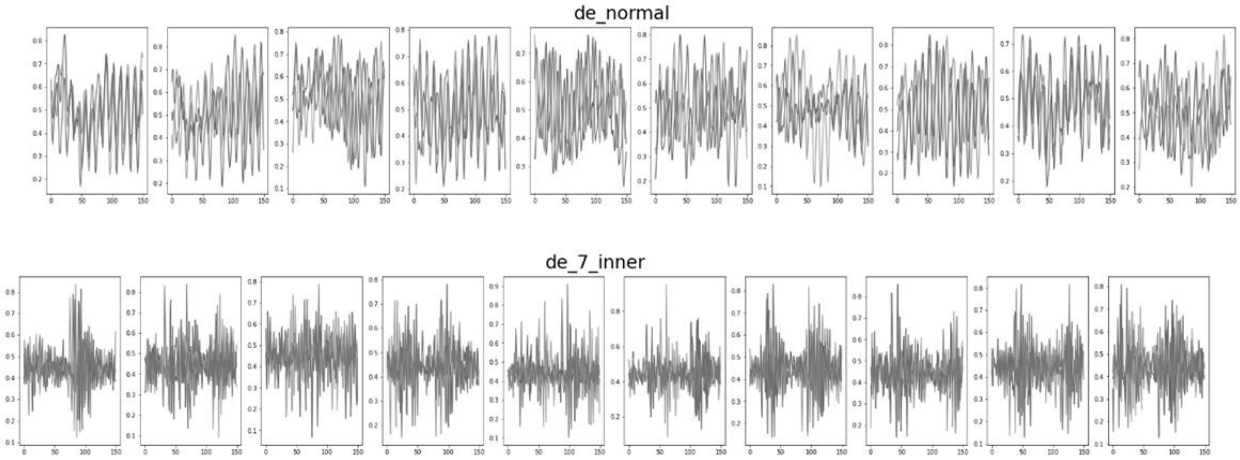


Figure 6 Results of data pre-processing

In order to expand the dataset we use to train the GAN model, we start from the 1st data point in the first slicing, and the second time, we start from the 11th data point, i.e., the nth time, we start from the 10th

$(n-1)+1$ data point, and here n=8.

As in Fig. 6, in order to simulate three channels of image data, we overlap every three data (which are not duplicated) into one set of data, obtaining 2968 sets of training normal data and 2998 sets of training fault data.

3.3 Experimentation

For the CWRU dataset, signal data from normal signals and 0.007-inch inner-ring faults at 0 hp load were selected to train the GAN model.

As in Fig. 7, the change in loss for generating normal data is shown at the top, the change in loss for generating faulty data is shown at the bottom, the discriminator's loss is shown at the left, and the generator's loss is shown at the right. The generator's loss oscillates within a range after a brief rise, and is overall less than 0.3. The discriminator's loss drops to 0.3 or less.

We evaluated the model using qualitative visualizations and quantitative metrics.

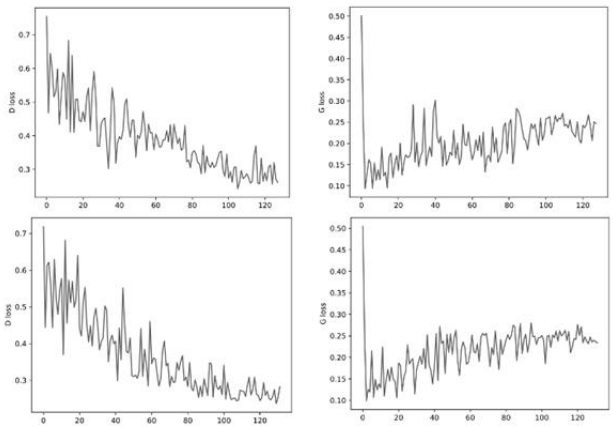


Figure 7 Training loss

Visualizations with PCA and t-SNE: To further illustrate the similarity between real and synthetic data, we plotted example visualizations of the distribution of data points mapped to the two dimensions using PCA and t-SNE.

Average Cosine Similarity For each pair of real signal feature vector fa and synthetic signal feature vector fb, the vector has the size m, we can compute its

cosine similarity as:

$$\cos_sim_{ab} = \frac{f_a \cdot f_b}{\| f_a \| \| f_b \|} = \frac{\sum_{i=1}^{m} f_{ai} f_{bi}}{\sqrt{\sum_{i=1}^{m} f_{ai}^2} \sqrt{\sum_{i=1}^{m} f_{bi}^2}}$$

The average cosine similarity score is the average of each cosine similarity between pairs of feature vectors corresponding to real and synthetic signals of the same class. The average cosine similarity is computed as follows, where n the total number of signals:

$$avg_\cos_sim = \frac{1}{n}\sum_{i=1}^{n} \cos_sim_i$$

3.4 Results and analysis

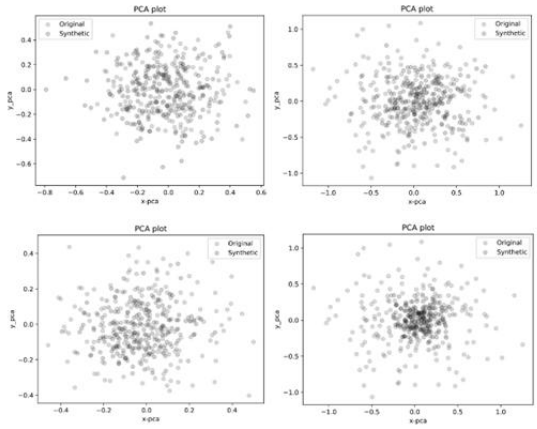


Figure 8 The PCA test for real and synthetic data generated by TTS-GAN

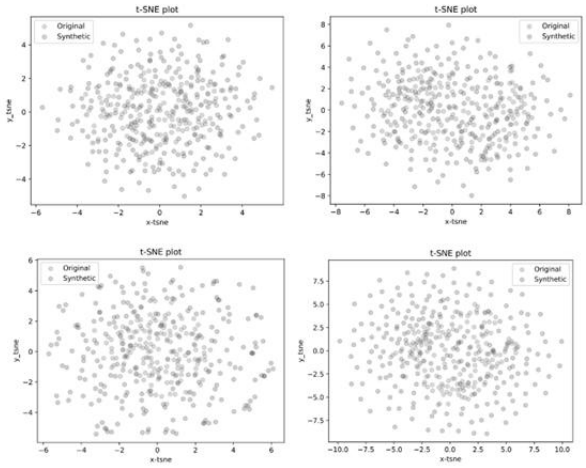


Figure 8 The t-SNE test for real and synthetic data generated by TTS-GAN

As in Figures 8 and 9, the left column shows the visualization results of real normal data and generated

normal data, and the right column shows the visualization results of real fault data and generated fault data. The top and bottom are the results of 20 epochs and 40 epochs in that order.

The visualization results show that the generated dataset and the real dataset have been generated relatively well, with basically similar distributions. The reason for the small difference between the generated data and the real data is mainly due to the insufficient training of the model, insufficient parameter settings, insufficient model design, insufficient data used for training, etc. The proposed solutions include modifying and adjusting the model. The solutions proposed so far include modifying and adjusting the model parameters; optimizing the design of the model structure; improving the epoch of training; and using other data enhancement methods to expand the dataset used to train the GAN model. Meanwhile, the tendency of model overfitting occurs when increasing the epoch, and the proposed method with higher feasibility is to continuously adjust the dropout rate of the dropout layer.

Table 1 The similarity scores between real data and synthetic data. avg_cos_sim, the bigger the better. avg_jen_dis, the smaller the better.

Dataset	Epoch	avg_cos_sim
Normal data	20	0.8022
	40	0.7733
Failure data	20	0.9009
	40	0.8949

According to Table 1 similarity scores indicate that the model training is better and increasing epoch has better improvement in generation. Therefore optimization is considered by increasing epoch or increasing the amount of data used for training.

IV. Conclusion

In this paper, a transformer-based GAN model is used for bearing fault diagnosis, which is capable of generating time-series data of fault samples of different lengths. By visualizing the signals, making intuitive comparisons, and using similarity scores to further quantitatively verify the authenticity of the synthesized data, the following conclusions are obtained when compared with previous classical methods:

1. Despite the small number of iterations, the trained dataset similarity scores have relatively good results, and the visualization results show the similarity between the real and synthetic data.

2. with the increase in the number of iterations, there is an improvement in the results of the trained dataset, but there is a tendency of overfitting.

3.The experimental results show that realistic bearing time series data can be generated after training on real samples.

Acknowledgements

Lina Zhao’s work is in part supported by the National Natural Science Foundation of China under Grant 92367111.

References

[1] Zhang T, Chen J, Li F, et al. Intelligent fault diagnosis of machines with small & imbalanced data: A state-of-the-art review and possible extensions[J]. ISA transactions, 2022, 119: 152-171.

[2] Zhang D, Zhang D. Wavelet transform[J]. Fundamentals of image data mining: Analysis, Features, Classification and Retrieval, 2019: 35-44.

[3] Rilling G, Flandrin P, Goncalves P. On empirical mode decomposition and its algorithms[C]//IEEE-EURASIP workshop on nonlinear signal and image processing. Grado: IEEE, 2003, 3(3): 8-11.

[4] Choi S, Cichocki A, Park H M, et al. Blind source separation and independent component analysis: A review[J]. Neural Information Processing-Letters and Reviews, 2005, 6(1): 1-57.

[5] Suthaharan S, Suthaharan S. Support vector machine[J]. Machine learning models and algorithms for big data classification: thinking with examples for effective learning, 2016: 207-235.

[6] Rigatti S J. Random forest[J]. Journal of Insurance Medicine, 2017, 47(1): 31-39.

[7] Abbasion S, Rafsanjani A, Farshidianfar A, et al. Rolling element bearings multi-fault classification based on the wavelet denoising and support vector machine[J]. Mechanical systems and signal processing, 2007, 21(7): 2933-2945.

[8] Yin Z, Hou J. Recent advances on SVM based fault diagnosis and process monitoring in complicated industrial processes[J]. Neurocomputing, 2016, 174: 643-650.

[9] Widodo A, Yang B S. Support vector machine in machine condition monitoring and fault diagnosis[J]. Mechanical systems and signal processing, 2007, 21(6): 2560-2574.

[10] Huang T, Zhang Q, Tang X, et al. A novel fault diagnosis method based on CNN and LSTM and its application in fault diagnosis for complex systems[J]. Artificial Intelligence Review, 2022, 55(2): 1289-1315.

[11] Chen X, Zhang B, Gao D. Bearing fault diagnosis base on multi-scale CNN and LSTM model[J]. Journal of Intelligent Manufacturing, 2021, 32(4): 971-987.

[12] Gu J, Peng Y, Lu H, et al. A novel fault diagnosis method of rotating machinery via VMD, CWT and improved CNN[J]. Measurement, 2022, 200: 111635.

[13] Wen L, Li X, Gao L, et al. A new convolutional neural network-based data-driven fault diagnosis method[J]. IEEE Transactions on Industrial Electronics, 2017, 65(7): 5990-5998.

[14] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. Generative Adversarial Networks[J]. 2014.

[15] Xu T, Zhang P, Huang Q, et al. Attngan: Fine-grained text to image generation with attentional generative adversarial networks[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2018: 1316-1324

[16] Liang X, Hu Z, Zhang H, et al. Recurrent topic-transition gan for visual paragraph generation[C]//Proceedings of the IEEE international conference on computer vision. 2017: 3362-3371.

[17] Zhang Y, Gan Z, Fan K, et al. Adversarial feature matching for text generation[C]//International conference on machine learning. PMLR, 2017: 4006-4015.

[18] Kurach K, Lučić M, Zhai X, et al. A large-scale study on regularization and normalization in GANs[C]//International conference on machine learning. PMLR, 2019: 3581-3590.

[19] Roth K, Lucchi A, Nowozin S, et al. Stabilizing training of generative adversarial networks through regularization[J]. Advances in neural information processing systems, 2017, 30.

[20] Zhang H, Zhang Z, Odena A, et al. Consistency regularization for generative adversarial networks[J]. arxiv preprint arxiv:1910.12027, 2019.

[21] Gulrajani I, Ahmed F, Arjovsky M, et al. Improved training of wasserstein gans[J]. Advances in neural information processing systems, 2017, 30.

[22] Esteban C, Hyland S L, Rätsch G. Real-valued (medical) time series generation with recurrent conditional gans[J]. arxiv preprint arxiv:1706.02633, 2017.

[23] Yoon J, Jarrett D, Van der Schaar M. Time-series generative adversarial networks[J]. Advances in neural information processing systems, 2019, 32.

[24] Liao S, Ni H, Szpruch L, et al. Conditional sig-wasserstein gans for time series generation[J]. arxiv preprint arxiv:2006.05421, 2020.

[25] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need[J]. Advances in neural information processing systems, 2017, 30.

[26] Jiang Y, Chang S, Wang Z. Transgan: Two pure transformers can make one strong gan, and that can scale up[J]. Advances in Neural Information Processing Systems, 2021, 34: 14745-14758.

[27] Li X, Metsis V, Wang H, et al. Tts-gan: A transformer-based time-series generative adversarial network[C]//International conference on artificial intelligence in medicine. Cham: Springer International Publishing, 2022: 133-143.

[28]Gupta J, Pathak S, Kumar G. Deep learning (CNN) and transfer learning: a review[C]//Journal of Physics: Conference Series. IOP Publishing, 2022, 2273(1): 012029.

[29] Li Y, Jiang W, Zhang G, et al. Wind turbine fault diagnosis based on transfer learning and convolutional autoencoder with small-scale data[J]. Renewable Energy, 2021, 171: 103-115.

[30] Huang J, Ma L, Wang J. Unknown Fault Diagnosis Based on Transfer Learning Under Multiple Working Conditions[C]//2023 China Automation Congress (CAC). IEEE, 2023: 6489-6494.

[31] Pan C, Xue S, Zhang Y, et al. Bearing Fault Diagnosis Using Transfer Learning with ICCEMDAN[C]//International Conference on Rotor Dynamics. Cham: Springer International Publishing, 2023: 111-129.

[32] Smith W A, Randall R B. Rolling element bearing diagnostics using the Case Western Reserve University data: A benchmark study[J]. Mechanical systems and signal processing, 2015, 64: 100-131.

About the authors

Liu Shuang is pursuing a master's degree at Beijing University of Chemical Technology. Her research focuses on deep learning, sparse low rank models, and bearing fault diagnosis research (Email: 2022201083@ buct.edu.cn)

Tan Zhuolun is a graduate student in the Department of Mathematics at the School of Science, Beijing University of Chemical Technology. He completed his undergraduate studies at Sichuan University.

Lina Zhao received the Ph.D. degree in applied mathematics from the Chinese Academy of Sciences, Beijing, China, in 2004. She is currently a Professor with the Beijing University of Chemical Technology, Beijing, China. Her research interests include computational and applied mathematics, which includes geometric problems in computer vision, image processing, and information mining from 3-D Big Data.

Hai-Jiang Zhu received the Ph.D.degree in pattern recognition and intelligent system from the National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 2004. From 2006 to 2007, he was a Visiting Scholar with the Faculty of Engineering, Iwate University, Japan. He is currently a Professor with the College of Information Science and Technology, Beijing University of Chemical Technology. He is interested in image processing and computer vision.

Hongwei Yang received the Ph.D. degree in College of Computer Science and Technology, Zhejiang University in 2008. She is currently an engineer with the Beijing University of Chemical Technology, Beijing, China. Her research interests: Machine learning and large model research.

确定性系统功能安全确保技术：挑战与趋势

张志为[1]，汤贵源[1]，赵浚淇[1]，习宁[2]，沈玉龙[1]，焦成伟[3]

摘　要：智能系统是现代工业发展的重要组成部分，是未来工业互联网和智能制造的核心力量。尽管智能系统复杂性和互联性不断增加，但其系统功能运行表现出显著的确定性，深入研究确定性系统功能安全确保技术，将为未来工业互联网发展提供安全保障。本文在分类调研总结现有各种功能安全确保防护理念和研究路线的基础上，分析了智能系统的功能安全确保需求与愿景，阐述了功能安全确保的内生身份管理、攻击智能检测、攻击主动防御等关键技术。针对依赖攻击先验知识导致的被动、滞后、低效防御问题，利用系统内在的多维度确定性信息，设计了智能系统确定性功能安全确保理论模型，构建了智能系统确定性功能安全保障技术框架，围绕身份确保、行为确保和权限确保等功能安全确保目标，探讨了实现智能系统功能安全确保所面临的挑战。

关键词：智能系统；功能安全确保；系统安全；攻击检测

Functional Safety Assurance Techniques for Deterministic Systems: Challenges and Trends

ZHANG Zhiwei[1], Tang Guiyuan[1], ZHAO Junqi[1], XI Ning[2], SHEN Yulong[1], JIAO Chengwei[3]

Abstract: Intelligent systems are a crucial component of modern industrial development and the core force of future industrial Internet and intelligent manufacturing. Despite the increasing complexity and interconnectivity of intelligent systems, their functional operations exhibit significant determinism. In-depth research into deterministic system functional safety assurance technology will provide security guarantees for the future development of the Industrial Internet. Based on a classified review and summary of existing functional safety assurance protection concepts and research pathways, this paper analyzes the functional safety assurance requirements and visions for intelligent systems. It elaborates on key technologies such as intrinsic identity management, intelligent attack detection, and proactive attack defense for functional safety assurance. To address the issues of passive, lagging, and inefficient defenses resulting from the reliance on prior knowledge of attacks, this paper leverages the intrinsic multidimensional deterministic information of systems to design a deterministic functional safety assurance theoretical model for intelligent systems. It constructs a deterministic functional safety assurance technology framework for intelligent systems, focusing on functional safety assurance goals such as

1. 西安电子科技大学计算机科学与技术学院，陕西 西安 710071；2. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；3. 华为技术有限公司，广东 深圳 518116

基金项目：国家自然科学基金项目重大研究计划（No. 92267204）

identity assurance, behavior assurance, and permission assurance. The challenges faced in achieving functional safety assurance for intelligent systems are also explored.

Keywords: intelligent system, functional safety assurance, system security, attack detection

1　引言

工业互联网是第四次工业革命的基石和国家新基建重要战略方向。工业互联网加速了智能制造、能源电力、轨道交通、国防工业等领域深度融合，是引领国家经济发展的核心驱动力。工业机器人、无人车等智能系统通过整合人工智能技术和自动化技术，实现自主决策和高效运作，极大地提高了工业互联网的整体性能和响应速度，是工业互联网的核心组成部分。然而，随着系统复杂度的增加和应用范围的扩大，智能系统面临更加多样的已知/未知安全威胁，突破了传统安全理论与技术的保护能力范畴，传统“事后完善”的被动式安全防护理论由于其滞后性，难以及时响应。而工业互联网对功能确定性、实时性、精准性、可靠性要求高，如果不能及时发现并处置安全威胁，将导致严重事故。为此，我们从智能系统本源确定性特征入手，以人工智能技术为支撑拓展和完善现有安全机制，提出确定性系统功能安全确保技术理论与框架，实现工业互联网智能化的主动安全防御，确保工业系统安全、可靠运行。

工业互联网中智能系统所面临的安全威胁主要包括不可避免的软硬件缺陷、不可预知的内外部威胁、不可控制的主客观环境、不可测量的进出口边界等四种来源。针对智能系统的安全威胁特点，国内外研究团队和企业先后突破传统安全思维[1]，从系统内部及特征入手，使其聚合产生自适应、自演进的安全能力，具备安全能力演化增强的安全机制，从根本上提升系统安全性能，最终形成面向确定性系统的功能安全确保能力。

为实现功能安全确保能力，智能系统安全愿景需要达到以下五个目标[1-2]。

（1）**目标 1：系统功能确保。**安全机制应保障智能系统的软硬件在合理区间内合规运行，同时确保系统实施相应的安全功能。

（2）**目标 2：未知攻击防御。**安全机制应能够在缺少攻击者先验知识、没有明确防御目标的情况下，构建形成基于系统内在确定性知识的防御功能，实现对攻击的有效识别与主动防御。

（3）**目标 3：安全机制演进。**安全机制应能适配不同场景下的安全防御需求，通过系统已有的内在要素与能力的优化组合调配，自适应地调整安全机制。

（4）**目标 4：安全决策可解释。**安全机制基于系统确定性知识所得出的各类异常、攻击信息、防御结论应具有可解释性，为安全漏洞和事故的调查和分析提供重要的信息和证据。

（5）**目标 5：兼容已有安全机制。**功能安全确保技术应不影响现有的已部署的安全产品和方案，并可与现有机制协同配合。

本文基于智能系统面临的安全隐患及相关的功能安全确保理念，分析智能系统的威胁特点与需求趋

势，从时间角度、威胁角度和属性角度对功能安全确保的现有研究进行调研和梳理，并对其关键技术进行总结，最后提出了确定性智能系统功能安全确保机理，探讨了实现智能系统功能安全确保所面临的挑战。

2 功能安全确保技术研究现状

功能安全确保指系统通过自适应和自生长的内在特征及机制，主动演化和增强其安全能力，以应对和抵御外部的不确定性威胁。根据功能安全确保的不同侧重点和实现思路，目前主流的功能安全确保研究可以从时间、威胁和属性三个角度来进行分析。

2.1 时间角度的功能安全确保研究

时间角度功能安全确保的基本思路是将安全贯穿研发运维的全过程，侧重于解决系统内在产生的安全问题。主要研究成果包括国外提出的零信任与国内的奇安信网管内生安全、中兴点面防御。

零信任于 2010 年由 John Kindervag 正式提出，核心理念为默认情况下所有网络流量均不可信，应对任意访问资源的请求实施安全控制[3]。2019 年，奇安信提出网络安全管理新模式[2]，强调依靠聚合应变，从信息化系统内产生自适应、自主和自成长的安全能力，即网管内生安全[4]。2020 年，奇安信发布新一代网络安全框架，将内生安全与系统工程方法论相融合，使系统中的安全能力转化为可构建、可执行的网络安全能力部件[5]。2021 年，中兴提出有效保障 5G 行业应用的安全机制，即三点一面的安全机制[6]，通过把安全嵌入到业务流程设计中，实现安全与业务的深度融合。

由于时间角度功能安全确保强调在设计和构建系统的同时考虑其安全能力的产生，以确保系统在生命周期内的安全性，导致系统所面对的环境、所能处理的安全问题类别、所具有的安全防御能力需要在设计时就考虑完全。搭建完成后，系统专用性较强，对于能够应对的未知威胁，通过一系列策略联动、态势感知等流程，监测防御效果显著。但这也限制了系统的普适性，使其难以有效地应用于其他领域的安全防御。因此，时间角度功能安全确保普遍具有针对性强，普适性弱的问题，需要仔细权衡其适用性和实际效益。

2.2 威胁角度的功能安全确保研究

威胁角度功能安全确保的基本思路是针对性地解决系统内源性安全威胁，侧重于解决系统内在产生的安全问题，专注于提出内在要素驱动的安全机理。主要研究成果包括国外提出的移动目标防御与国内的拟态安全、人工智能安全箍和免疫安全。

移动目标防御（MTD, Moving Target Defense）于 2011 年由美国提出，核心思想是通过不断的动态变化来提高系统内部结构的复杂度[7]，通过多种技术赋予系统动态性、随机性和多样性，从而阻断攻击链[8]。2014 年，邬江兴院士团队正式提出一种网络空间安全防御理论，即拟态安全[9]。通过动态地、伪随机地选择执行各种软硬件变体，使攻击者难以构建起攻击链，从而达到增强系统安全的目的。2020 年，方滨兴院士团队提出人工智能安全箍（AI 保险箍），从安全机制、安全围栏等方面对人工智能行为体实施防控[10]。

根据计算机免疫学运用生物原理处理网络威胁的思路[11]，于全院士团队提出免疫安全。利用多元安全

态势融合，实时对被感染区域或节点进行隔离。然而，目前的免疫安全机制仍处于理论阶段，发展较缓，缺乏具体技术实践与评估方法。

综上，威胁角度功能安全确保更关注防御对象内在特有的安全威胁与安全需求，对防御对象的安全防护更有针对性，对未知威胁的防护效果也更突出。然而，从 MTD 到拟态防御、再到免疫安全，都需要在系统中部署相应的安全构件，增大了构建成本和防御开销。因此，威胁角度功能安全确保普遍具有预期效果好，但防御开销大的问题。

2.3　属性角度的功能安全确保研究

属性角度功能安全确保的基本思路是利用系统的内在特征开展安全防御，聚焦于提出内在要素驱动的安全机理。主要研究成果有国外的 VMware 原生安全与国内的可信计算安全、西电网络行为功能安全确保。

1985 年，美国首次提出可信计算，利用可信根形成逐层度量的信任链，实现系统环境安全[12]。基于此，沈昌祥院士团队通过主动免疫原理构建了可信免疫架构，以双系统体系架构的模式实现可信计算，形成可信计算内生安全[13]。2020 年，VMware 提出原生安全解决方案，打造内建而非外挂、整合而非孤立、变被动为主动的原生安全性。通过构建信息安全控制点模型，将安全系统嵌入工作负载、端点设备、身份认证、网络、云端这五个控制点中，对每个控制点实施深度监控和行为分析，实现全面的情景感知，提高整个系统的安全性。

面向智能网络系统，西安电子科技大学团队提出基于行为的功能安全确保，从海量、多样的网络交互中形成对网络实体行为的经验与理解，识别已知和未知攻击行为。以零信任理念为借鉴，以功能行为为核心，通过确保有限的功能安全，来保障整个网络系统的安全，以确定性的防御抵御不确定性的未知攻击，极大地减少了资源开销，使系统具有功能安全确保能力。

综上，属性角度功能安全确保基于系统本身具有的特征与属性实施安全防御，促进安全防护与系统特性深度融合，提高系统的自我保护能力，使系统具有功能安全确保特性，防御效果明显。然而，该思路很大程度上依赖于系统内在特征的完备性与正确性，需要对系统的物性及逻辑特征进行详细分析，并设计相应的安全机理，才能进一步使方案合理实施，避免防御策略的误判。因此，属性角度功能安全确保普遍具有防御效能佳，但机理不健全的问题。

根据智能系统的安全需求和愿景，现有研究在不同程度上均满足了攻击防御的需要，同时也兼顾体现了合规交互、动态调动、功能确保等安全需求，为后续功能安全确保相关研究提供了理论思路与实现技术。

3　功能安全确保关键技术

基于第二节所述的功能安全确保理论与研究，从内生身份管理、攻击智能检测、攻击主动防御等防护阶段出发，对功能安全确保所涉及的关键技术进行阐述。

3.1 内生身份管理

内生身份要素表征和内生身份构建是身份管理的主要内容，主要涉及系统实体的多维度多层次的物性特征和逻辑特征等内在特征的提取与表征。

物性特征包括器件物性特征和网络信道特征，这类特征与生俱来且不可更改。在设备认证方面，物理不可克隆函数（PUF, Physical Unclonable Function）是一种轻量高效的解决方案，可以使用 PUF 的输出生成同样唯一且不可克隆的密钥或匿名标识[14]，用于身份认证和密钥生成领域[15-17]。与 PUF 类似，CPU 模块之间本质上存在硬件差异，基于激励响应的设备指纹识别技术，利用外部测量信息，CPU 芯片及其附属电源电路组成的 CPU 模块发出的磁感应可以产生可用的设备指纹，难以修改或模仿[18]。

逻辑特征包括实体行为特征和 I/O 时序特征，可以通过智能系统中的逻辑特征构建设备特征集合，并基于应用场景的多维逻辑特征属性构建身份认证体系。鉴于资源和数据共享的动态性，访问控制策略需要不断更新，文献[19]介绍一种用于监视访问控制行为的实用工具，可以持续监控访问日志并从中推断访问控制策略。基于设备内部时钟信号的差异，文献[20]提出一个双时钟模型，可以测量主体时钟的瞬时相位并用于构建相位图像，从瞬时相位图中提取基于时钟信号的设备指纹。

多维度内生身份管理技术已在各类场景中被广泛关注、研究和应用。然而，现有技术存在特征维度采集率低、采集方式复杂、易受环境影响、普适性有限等问题，需要进一步提高身份管理技术的可靠性和便捷性，增强跨平台和互操作的支持能力。

3.2 攻击智能检测

威胁检测通过实时监控系统网络流量，对异常流量或行为进行分析，并对可能的威胁进行分类和预测。在此基础上，攻击研判对于潜在的异常威胁进一步确认，实现对攻击的检测与识别。

目前主流威胁分析框架和防御方法依靠大量的专家知识和攻击先验规则，基于已知的威胁特征和行为模式进行检测，没有充分考虑系统本身的安全特性和任务确保需求，同时还需要大量的计算资源进行模型训练和特征提取。需要进一步发展以适应更多新型威胁，减少对标记数据和计算资源的依赖，提高检测结果的可解释性。

针对复杂攻击的攻击意图难以识别的问题，文献[21]提出一种基于攻击路径图的攻击意图分析方法，提高了攻击识别的效率和准确性。文献[22]利用因果图建立了行为关键模式，设计了基于序列模型的 ATLAS 框架，以此识别对攻击有贡献的节点并描述完整的攻击故事。针对 APT 等新型攻击的规范化描述困难、结构化知识缺失等问题，文献[23]提出一种融合实体识别和实体对齐的 APT 攻击知识自动抽取方法。

现有攻击行为研判技术的主流趋势可归结为研究利用数据源图等确定性知识实现对 APT 攻击等新型攻击的检测识别与追踪溯源，但是知识收集和管理的规范性与系统性不足，没有充分考虑实体多源异构知识的融合及应用，导致其可能受到不同威胁情境和环境的影响，从而限制技术的精度和可行性。

3.3　攻击主动防御

结合威胁检测与攻击研判给出的结果，需要快速选择成本低、效果好的阻断方式完成攻击主动防御。

文献[24]针对如何选择防御策略、降低防御成本，提出基于攻防博弈模型的最优主动防御选择算法，通过生成防御策略的效用矩阵，判断采用何种防御方式。文献[25]提出基于数据包排队控制的主动防御方法，通过评估应用层未知攻击和新型攻击对网络造成的风险程度来阻断攻击。文献[26]利用流表报文过滤实现对攻击流量的阻断，能够将出现异常的网络恢复到正常运行的状态。文献[27]针对软件定义物联网的DDoS 攻击，提出通过提取网络节点流量特征，对节点进行聚类，从而利用网络拓扑确定攻击节点的地址，实现攻击防御。

已有的攻击阻断防御研究仍具有显著的对象针对性和场景局限性，其迁移性较差，适用范围有限；阻断方式仍主要采用流量过滤、区域隔离等传统手段，存在难以应对隐蔽逃逸性强、伪旗误导性高的新型有组织攻击的问题；攻击阻断防御的多样化、主动性和适用性有待进一步提高。

4　功能确定性智能系统的功能安全确保模型与关键技术

智能系统的确定性基础主要体现在系统设备的有限性、系统功能的固定性、系统运行的规律性和系统生态的可控性。利用这些确定性基础，本章节面向功能确定性的智能系统提出确定性功能安全确保，并对实现智能系统功能安全确保进行探讨。

4.1　确定性功能安全确保理论模型

与传统安全机制的“被动防御”思想不同，本节提出智能系统确定性功能安全确保理论模型，利用系统的内在属性和特征开展安全防御，通过确定性的系统安全防御抵御不确定性的威胁攻击。如图 1 所示，理论模型主要由“四维内生信息、四类对象、三个区划、两条界限、一套测评”组成。

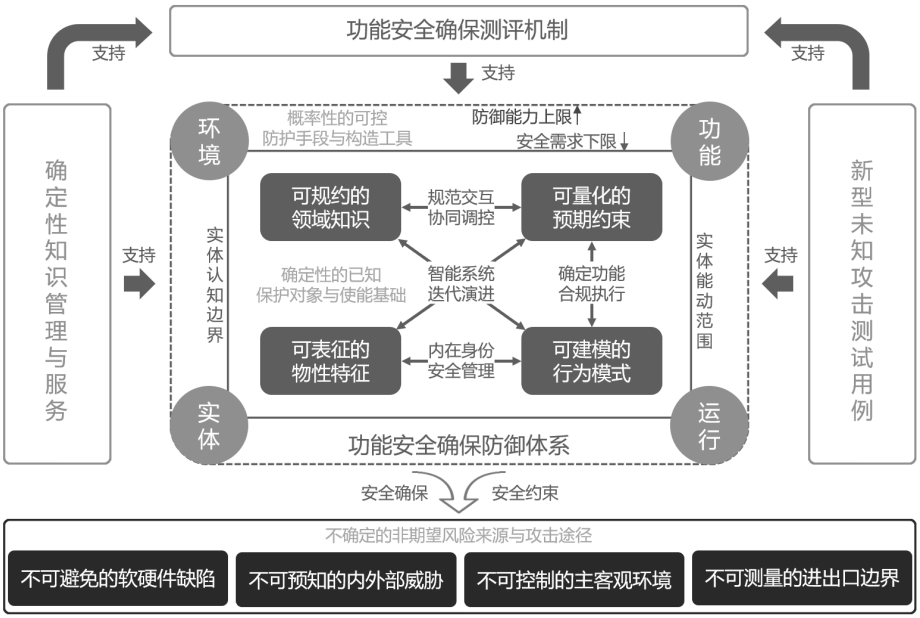


图1　智能系统确定性功能安全确保理论模型

（1）四维内生信息。可机读的领域知识是构建确定性知识库的基础。可量化的预期约束是根据可机读的领域知识形成的判断系统运行是否正常的依据。可表征的物性特征是指可以被量化和描述的内在物理或逻辑属性。可建模的行为模式是指实体在一定的时间和空间范围所表现出来的可形式化表征的规律。

（2）四类对象。实体指特征明确的设备、组件或服务等。功能指具有明确目标的确定性实体功能。场景指智能系统的应用环境，会对实体表现和功能实现造成影响。针对实体和功能明确的系统，运行条件、运行状态、运行结果等信息随即确定，得到确定的系统运行规律。

（3）三个区划。确定性区域是功能安全确保防御的目标和对象，是功能安全确保防御的起点和基础。概率性区域是功能安全确保防御的作用范围，防御效果受到内外部因素的影响。不确定性区域是威胁攻击的来源，攻击主客体、时间等知识和情报信息未知。

（4）两条界限。安全需求确定智能系统功能安全确保能力下限，是维持系统功能性能正常运行的最低要求。安全能力上限是安全防御所能对抗的攻击强度的最大能力。

（5）一套测评。针对智能系统的组合攻击方法与功能安全确保防御功能反馈评估测评机制，基于对抗技术的专用原子攻击设计组合方案，制定安全防护功效多维测评指标体系，实现高威胁攻击测试用例自动化组合攻击，为功能安全确保防御评估提供功能性能的定量和定性测评方案。

整个理论模型围绕安全约束和安全确保的需求与目标，研究内生身份表征与认证、内在知识驱动与更新、实时异常检测与研判等功能安全确保关键技术，设计基于确定性和不确定性博弈的功能安全确保构造框架，实现对不确定性非预期因素引发的已知和未知攻击的主动防御，确保任务符合系统约束地可靠执行。

4.2 确定性功能安全确保技术框架

基于智能系统的功能安全确保理论模型，探索确定性系统与非确定性威胁之间的内在关系，设计四维的立体化功能安全确保构造框架，以身份确保、行为确保、权限确保和攻击防御为核心，通过保障有限的功能安全，解决面向已知威胁和边界防御的传统安全机制难以应对非预期未知攻击的问题，具体框架如图2所示。

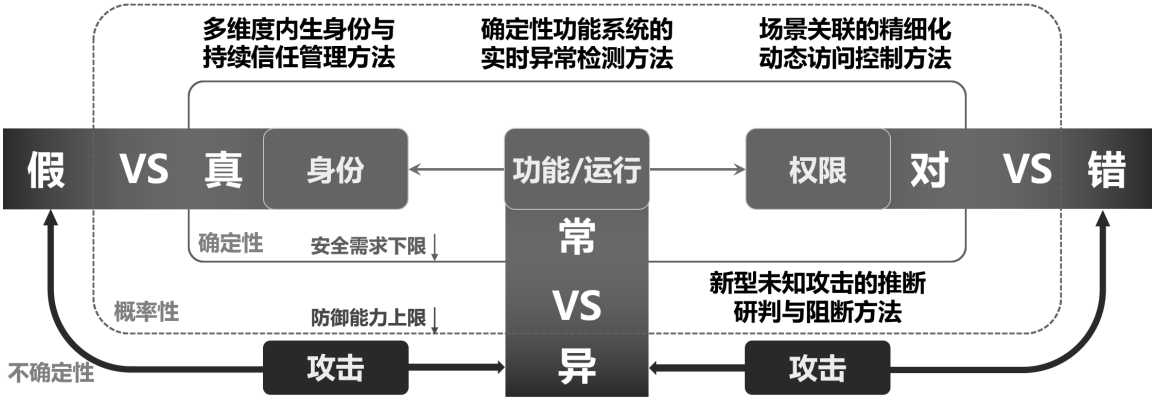


图2 智能系统确定性功能安全确保技术架构

整个架构以真实身份、正确权限与合规行为所构成的确定性区域作为功能安全确保防御的起点和基础，以虚假身份、错误权限或异常行为所形成的不确定性区域表示威胁攻击的来源，最终确定性功能安全确保在两者中的概率性区域实现防御，其效果受到内外部因素共同影响。

（1）身份确保。通过多维度内生身份与持续信任管理方法，以实体的物性和逻辑特征为基础建立其唯一的内生身份，使用上下文信息和业务规则确定不同情况下用户或设备的多因素身份验证方法，打造动态自适应的身份认证体系。

（2）权限确保。结合认证因素的不同安全等级与适用范围，综合分析和权衡不同因素的权重，以更准确地确定用户身份并控制其访问权限，形成场景关联的动态访问控制模型，实现多因素精细化身份认证与访问控制。

（3）行为确保。从智能系统的关键信息出发，收集各个设备的功能和行为关键信息，构建设备任务关联的确定性知识数据库，形成对系统功能与行为的安全约束，实现对设备实时行为的监测与异常判别。

（4）攻击防御。基于异常检测与确定性知识库进行知识推理分析任务被破坏程度，研判异常事件是否形成攻击，构建攻击语义知识库，支撑可回溯的攻击研判，进而对遭受攻击的设备权限、数据、资源进行精确调控与隔离阻断。

4.3　确定性功能安全确保防护实例

以 CT（Communication Technology）领域中的智能系统为例，对确定性功能安全确保进行应用与分析。由于 CT 领域系统的实体规模、功能、业务、管辖有限，实体的软硬件功能具有一定的表征稳定性，实体运行状态、动作行为具有周期性或固定模式，系统生态都可由运营商或所有者调配控制，因而 CT 领域系统具有确定性，能够使用确定性功能安全确保实现安全防护。整个 CT 领域典型应用场景如图 3 所示。

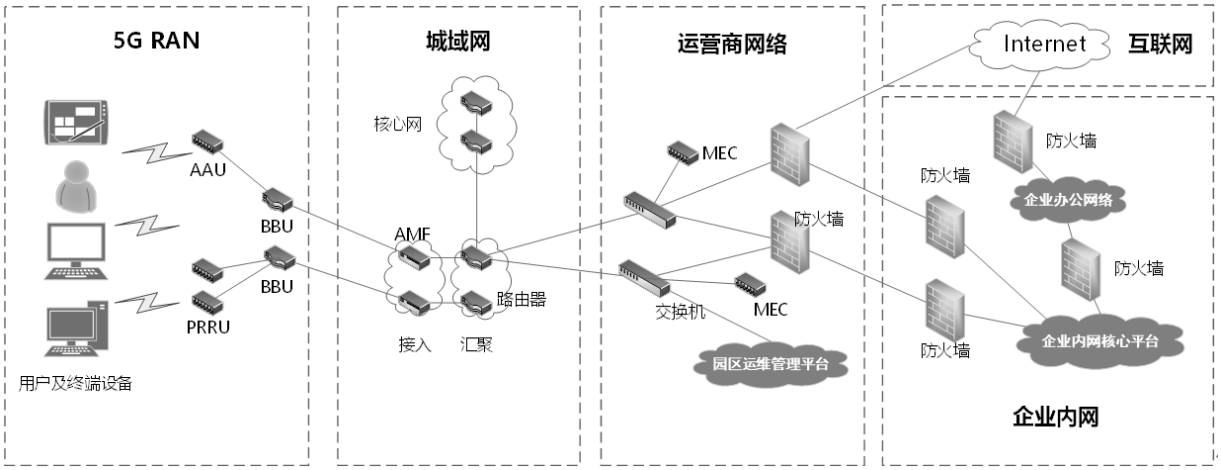


图3　CT领域典型应用场景

（1）内生身份与信任管理技术

基于实体可表征物性特征和逻辑特征，构建 CT 领域实体内生身份，实现实体的持续无感认证，如图

4 所示。其中，物性特征借助实体物理构造的差异性与独特性实现身份表征与认证，可分为实体器件特征和网络信道特征两类；逻辑特征通过对实体行为特征的监测与审计实现异常检测和任务约束，可分为实体行为特征和 I/O 时序特征两类。

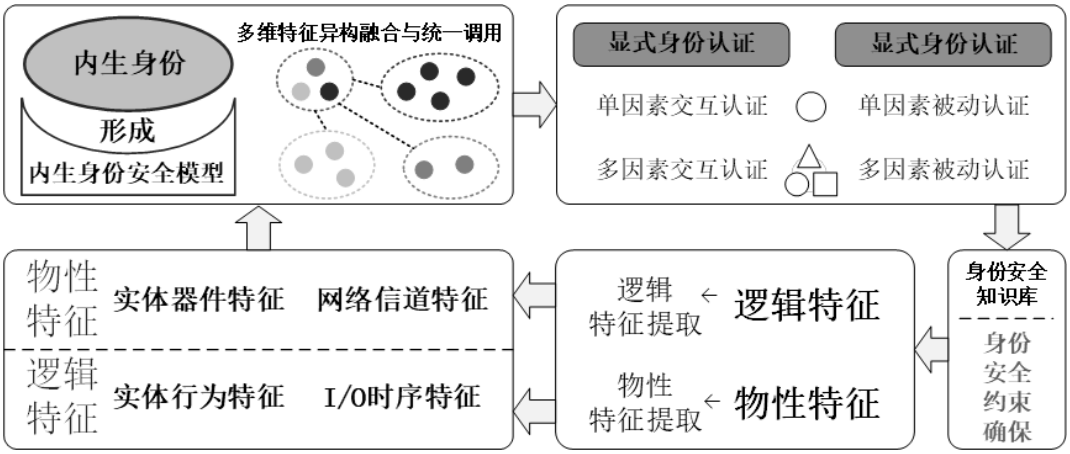


图4　内生身份与信任管理技术

提取上述多维度特征，构建设备特征集合。利用实体执行任务所需资源属性，建立任务安全等级分类方法，基于实体任务属性，综合考虑实体各特征身份表征能力和特征间冗余相似程度，动态构建实体多维内生身份，提出多维内生身份动态构建模型，有效提高实体身份验证的灵活性。

在身份构建的基础上，提出持续信任管理方法实现 CT 领域的动态自适应身份验证，使用上下文信息和业务规则来确定在特定情况下应用于不同用户或设备的多因素身份验证方法。通过非侵入式身份验证因素可以帮助动态自适应身份验证系统量化每个操作的风险等级，根据不同的风险等级选择不同的身份验证策略，实现隐式无感的高效持续认证。

（2）精细化动态访问控制技术

联系时空连续变换场景的敏感性，结合认证因素的不同安全等级与适用范围，形成场景关联的多因素精细化动态访问控制模型，如图 5 所示。

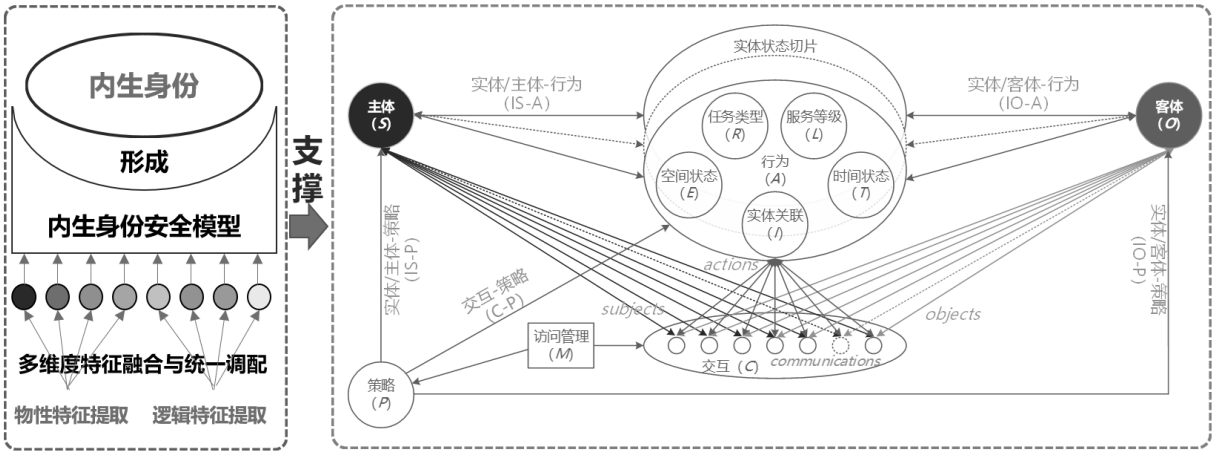


图5　精细化动态访问控制技术

基于认证因素和任务场景的关联性，通过场景敏感的多因素组合与融合方法，实现多因素精细化身份认证与访问控制灵活性的提升；基于 CT 领域场景下资源的多级权限特征，建立 CT 领域资源的多级权限特征集，通过面向任务全生命周期的细粒度熔断访问控制方法，提高资源管控精细度和业务连贯性；结合任务的可划分性和资源的安全敏感性，通过基于任务的动态持续资源访问控制方法，实现资源权限的细粒度熔断和资源利用率的提高。

（3）实时异常行为检测技术

部署粗细两种粒度的收集器在各个设备收集行为关键信息，构建 CT 领域网络系统确定性知识库，形成对 CT 领域网络系统功能与行为的安全约束，基于已生成的安全约束对设备的实时行为进行合规判别，如图 6 所示。

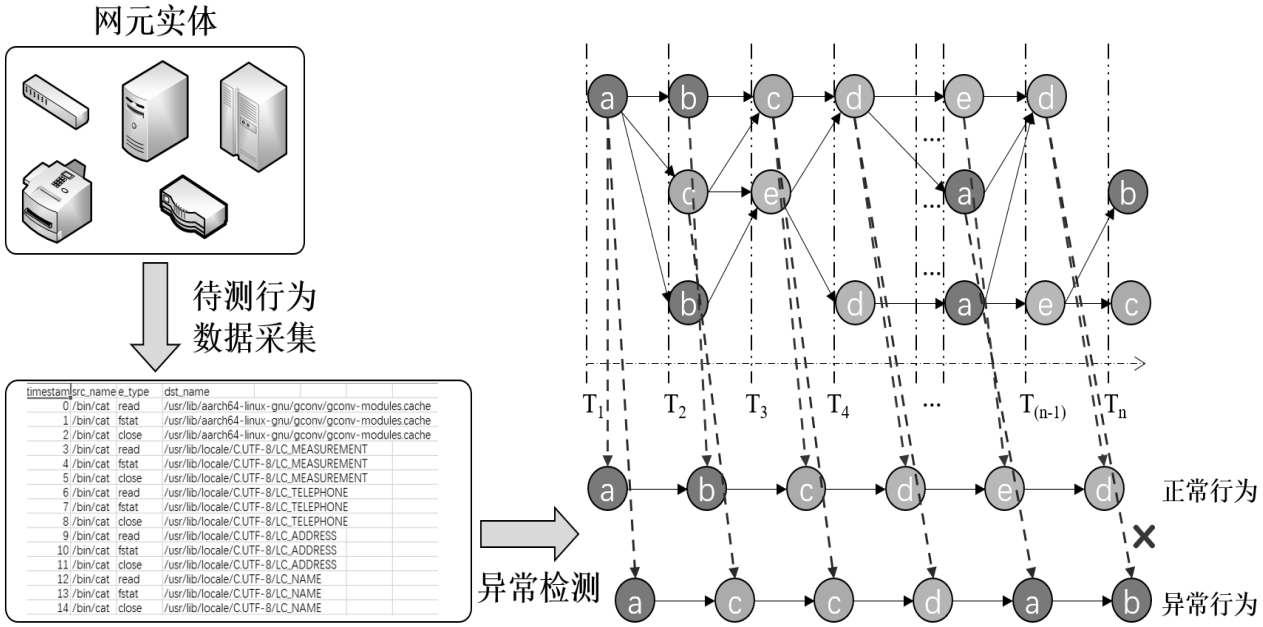


图6　实时异常行为检测技术

其中，确定性知识库以实体任务为中心，通过在良性环境中分别执行网元基本功能和任务，从行为审计中收集正常行为信息，从产品文档收集与任务相关的设备信息，从自定义输入规则信息，获得确定性的良性任务知识，以此作为正常与异常信息判断的依据。

基于确定性知识库，使用实体行为谓词对正常网络行为进行建模。对知识库中的每一个实体行为，均生成特定的谓词规范，最终形成正常行为约束模型，利用正常行为约束模型进行异常检测，将实时行为与约束模型进行对比匹配，判断是否超出约束，超出即判定为异常行为，符合约束即为正常行为。

（4）攻击推理研判与阻断技术

基于已检测出的异常与确定性知识进行知识推理分析任务破坏程度，研判异常事件是否形成“攻击”，构建攻击语义知识库，为后续解析异常提供先验指导，支撑可回溯的未知攻击研判，如图 7 所示。

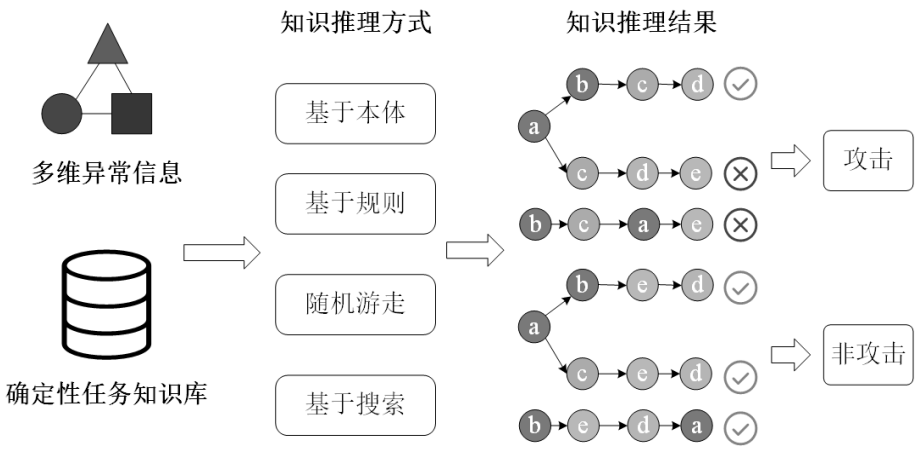


图7　攻击推理研判技术

构建攻击语义知识库，对于检测出的异常进行知识库的对比检测，如果异常信息已经在攻击语义知识库中，可直接判定为已知攻击，进行攻击阻断，对于不在攻击语义知识库中的异常，通过知识推理进行研判是否形成攻击。

知识推理基于确定性的任务知识与异常信息，可采用基于本体、基于规则、随机游走、基于搜索等推理手段，研判对任务的破坏程度，进而判定是否形成攻击。知识推理可能有多个结果，每个结果对任务的破坏性程度不同，计算每个结果出现的概率，将其视作权重，根据每个推理结果的权重及其对任务的破坏程度综合判断是否形成攻击。

通过动态未知攻击实时阻断方法，对遭受攻击的 CT 网元设备权限、数据、资源的精确调控与隔离阻断，实现协同式、多层次、高灵活的网元设备任务运行时的攻击阻断。

5　结束语

功能安全确保作为一种新兴安全防御理念，为应对当前网络边界日益模糊的安全形势提供了新思路。本文面向智能系统的安全特性与需求，按照实现思路从时间、威胁和属性角度归类分析了功能安全确保的主流研究趋势和研究内容，对功能安全确保涉及的关键技术进行了阐述，提出了智能系统确定性功能安全确保机理，探讨了为实现确定性系统功能安全确保所面临的挑战，以期为未来智能系统功能安全确保研究提供新的解决思路和借鉴参考。

参考文献：

[1] 徐恪, 付松涛, 李琦, 等. 互联网内生安全体系结构研究进展[J]. 计算机学报, 2021, 44(11): 2149-2172. XU K, FU S T, LI Q, et al. The research progress on intrinsic internet security architecture[J]. Chinese Journal of Computers, 2021, 44(11): 2149-2172.

[2] 奇安信战略咨询规划部, 奇安信行业安全研究中心. 内生安全：新一代网络安全框架体系与实践[M]. 北京：人民邮电出版社, 2021.

QI'AN XIN STRATEGIC CONSULTING PLANNING DEPARTMENT, QI'ANXIN INDUSTRY SECURITY RESEARCH CENTER. Endogenous security: a new generation of network security framework system and practice[M]. Beijing: People's Post and Telecom Press, 2021.

[3] 张宇, 张妍. 零信任研究综述[J]. 信息安全研究, 2020, 6(7): 608-614.

ZHANG Y, ZHANG Y. A survey of zero trust research [J]. Journal of Information Security Research, 2020, 6(7): 608-614.

[4] 齐向东. 面向新基建，用内生安全框架支撑网络安全体系建设[J]. 中国科技产业, 2020(8): 18-21.

QI X D. Support network security system construction with endogenous security framework for new infrastructure[J]. Science & Technology Industry of China, 2020(8): 18-21.

[5] 韩永刚. 基于内生安全框架的面向数字化转型的网络安全防御体系[J]. 中兴通讯技术, 2022, 28(6): 29-35.

HAN Y G. A cybersecurity defense system for digital transformation based on an endogenous security framework[J]. ZTE Technology Journal, 2022, 28(6): 29-35.

[6] 中兴通讯. 2030+网络内生安全愿景白皮书[R]. 2021.

ZHONGXING TELECOM. 2030+ Cyber endogenous security vision white paper[R]. 2021.

[7] 樊琳娜, 马宇峰, 黄河, 等. 移动目标防御技术研究综述[J]. 中国电子科学研究院学报, 2017, 12(2): 209-214.

FAN L N, MA Y F, HUANG H, et al. The research summary of moving target defense technology[J]. Journal of China Academy of Electronics and Information Technology, 2017, 12(2): 209-214.

[8] KAMPANAKIS P, PERROS H, BEYENE T. SDN-based solutions for Moving Target Defense network protection[C]//Proceedings of Proceeding of IEEE International Symposium on a World of Wireless. Mobile and Multimedia Networks 2014, 2014: 1-6.

[9] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.

WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1-10.

[10] 方滨兴. 人工智能安全[M]. 北京：电子工业出版社, 2020.

FANG B X. Artificial intelligence security[M]. Beijing: Publishing House of Electronics Industry, 2020.

[11] 樊佩佩, 杨德义. 浅析计算机网络入侵检测中免疫机制的应用[J]. 科学技术创新, 2018(18): 69-70.

FAN P P, YANG D Y. Analysis of the application of immune mechanism in computer network intrusion detection[J]. Scientific and Technological Innovation, 2018(18): 69-70.

[12] 秦中元, 胡爱群. 可信计算系统及其研究现状[J]. 计算机工程, 2006, 32(14): 111-113.

QIN Z Y, HU A Q. Trusted computing system and its current research[J]. Computer Engineering, 2006, 32(14): 111-113.

[13] 沈昌祥. 用主动免疫可信计算 3.0 筑牢网络安全防线营造清朗的网络空间[J]. 信息安全研究, 2018, 4(4): 282-302.

SHEN C X. To create a positive cyberspace by safeguarding network security with active immune trusted computing 3.0[J]. Journal of Information Security Research, 2018, 4(4): 282-302.

[14] LABRADO C, THAPLIYAL H. Design of a piezoelectric-based physically unclonable function for IoT security[J]. IEEE Internet of Things Journal, 2018, 6(2): 2770-2777.

[15] HERDER C, YU M D, Koushanfar F, et al. Physical unclonable functions and applications: A tutorial[J]. Proceedings of the IEEE, 2014, 102(8): 1126-1141.

[16] GAO Y, AL-SARAWI S F, ABBOTT D. Physical unclonable functions[J]. Nature Electronics, 2020, 3(2): 81-91.

[17] KUMAR N, CHEN J, KAR M, et al. Multigated carbon nanotube field effect transistors-based physically unclonable functions as security keys[J]. IEEE Internet of Things Journal, 2018, 6(1): 325-334.

[18] CHENG Y S, JI X Y, ZHANG J C, et al. Demicpu: Device fingerprinting with magnetic signals radiated by CPU[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2019: 1149-1170.

[19] XIANG C C, WU Y D, SHEN B Y, et al. Towards continuous access control validation and forensics[C]//Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. ACM, 2019: 113-129.

[20] MONACO J V. Device fingerprinting with peripheral timestamps[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1018-1033.

[21] CHEN B Q, LIU Y H, LI S J, et al. Attack intent analysis method based on attack path graph[C]//International Conference on Communication and Network Security. ICCNS, 2019: 97-102.

[22] ALSAHEEL A, NAN Y, MA S, et al. ATLAS: a sequence-based learning approach for attack investigation[C]//USENIX Security Symposium. USENIX Security, 2021: 3005-3022.

[23] 杨秀璋, 彭国军, 李子川, 等. 基于 Bert 和 BiLSTM-CRF 的 APT 攻击实体识别及对齐研究[J]. 通信学报, 2022, 43(6): 58-70.

YANG X Z, PENG G J, LI Z C, et al. Research on entity recognition and alignment of APT attack based on Bert and BiLSTM-CRF[J]. Journal on Communications, 2022, 43(6): 58-70.

[24] 姜伟, 方滨兴, 田志宏, 等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报, 2009, 32(4): 817-827.

JIANG W, FANG B X, TIAN Z H, et al. Evaluating network security and optimal active defense based on attack defense game model[J]. Chinese Journal of Computers, 2009, 32(4): 817-827.

[25] 谢柏林, 余顺争. 基于应用层协议分析的应用层实时主动防御系统[J]. 计算机学报, 2011, 34(3): 452-463.

XIE B L, YU S Z. Application layer real-time proactive defense system based oil application layer protocol analysis[J]. Chinese Journal of Computers, 2011, 34(3): 452-463.

[26] 宋宇波, 樊明, 杨俊杰, 等. 一种基于拓扑分析的网络攻击流量分流和阻断方法[J]. 信息网络安全, 2020, 20(3): 9-17.

SONG Y B, FAN M, YANG J J, et al. Multipath solution and blocking method of network attack traffic based on topology analysis[J]. Netinfo Security, 2020, 20(3): 9-17.

[27] 刘向举, 刘鹏程, 路小宝, 等. 基于 SD-IoT 的 DDoS 攻击防御方法[J]. 计算机工程与设计, 2021, 42(11): 3001-3008.

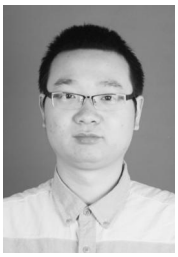
LIU X J, LIU P C, LU X B, et al. SD-IoT based DDoS attack defense method[J]. Computer Engineering and Design, 2021, 42(11): 3001-3008.

[作者简介]

张志为（1986—），男，博士，西安电子科技大学副教授，主要研究方向为身份认证、访问控制、云计算数据存储安全和智能集群内生安全。

汤贵源（1999—），男，福州大学工科学士学位，西安电子科技大学硕士研究生在读，主要研究方向为网络空间安全。

赵浚淇（2000—），女，西安电子科技大学工科学士学位，西安电子科技大学硕士研究生在读，主要研究方向为网络安全。



习宁（1986—），男，博士，西安电子科技大学教授，主要研究方向为无人系统安全、工业互联网安全。

沈玉龙（1978-），男，博士，西安电子科技大学教授，主要研究方向为云计算与数据安全、智能网络内生安全等。

焦成伟，男，华为技术有限公司，安全与隐私保护技术实验室主任，研究方向为智能网络安全。

面向工业互联的星地传输性能评估方法

汪文静[1]，文忠[1]，许鲁彦[2]，丁海川[1*]

1. 北京理工大学网络空间安全学院，北京，100081

2. 电磁空间认知与智能控制技术实验室，北京，100081

摘　要：随着工业互联网的快速发展，工业生产活动逐步向远海、沙漠等偏远区域拓展，在此背景下，以天基平台为核心的星地一体化网络为全球范围内的工业生产活动提供了强力的技术支持。本文以面向工业制造的星地一体化网络为背景，分析了卫星通信系统广域覆盖和星地信道开放性带来的关键信息传输安全挑战，并鉴于现有研究多聚焦于通信链路可靠性的刻画，而缺乏对安全性的全面考虑的现状，提出了一种星地链路安全性评估方法，构建了以负熵、互信息和循环谱密度为核心的综合评价指标体系。通过该体系，能够全面评估星地通信链路在抵御非合作侦测和干扰方面的性能，为工业制造场景下的星地传输方案设计提供了科学依据。本文以直接序列扩频通信为例，通过仿真展示了所提评估指标的具体应用，验证了其有效性。

关键词：工业互联网；星地一体化；安全通信

Satellite- Terrestrial Transmission Performance Evaluation Method for Industrial Internet of Things

Wang Wenjing[1], Wen Zhong[1], Xu Luyan[2], Ding Haichuan[1]

1. School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, 100081

2. Laboratory of Electromagnetic Space Cognition and Intelligent Control, Beijing, 100081

Abstract: With the rapid development of the industrial internet of things, industrial production activities are gradually expanding to remote areas such as the open sea and deserts. In this context, the satellite-terrestrial integrated network provides powerful technical support for industrial production activities worldwide. This paper, focusing on a space-terrestrial integrated network for industrial manufacturing, analyzes the key information transmission security challenges brought about by the wide-area coverage of satellite communication systems and the openness of space-ground channels. In view of the current situation where most existing studies focus on the characterization of communication link reliability while lacking consideration of security, this paper proposes a security evaluation method for satellite-terrestrial links and constructs a comprehensive evaluation index system

* 作者简介：汪文静，女，北京理工大学网络空间安全学院在读硕士研究生，主要研究方向为隐蔽通信。E-mail：3220221457@bit.edu.cn。
文忠，男，北京理工大学网络空间安全学院，主要研究方向为空天安全通信。E-mail：wen_zhong@bit.edu.cn。
许鲁彦，男，电磁空间认知与智能控制技术实验室，主要研究方向为空天安全通信。E-mail：xu_luyan@163.com。
丁海川，男，北京理工大学网络空间安全学院教授，主要研究方向为空天安全通信、隐蔽通信。E-mail：hcding@bit.edu.cn。

which includes negentropy, mutual information, and cyclic spectral density. Through this system, the performance of satellite-terrestrial communication links in resisting non-cooperative detection and interference can be comprehensively evaluated, providing a scientific basis for the design of satellite-terrestrial transmission schemes in industrial manufacturing scenarios. Taking direct-sequence spread spectrum communication as an example, this paper demonstrates the specific application of the proposed evaluation indicators through simulation and verifies their effectiveness.

Key words: Industrial internet of things；satellite-terrestrial integration；secure communication

1　引言

工业互联网通过强大的网络覆盖和实时数据传输，有效连接和协调了全球各地的生产设施与供应链节点，实现了产品设计、原材料采集、制造和运输等各生产环节的高度整合与互联。随着工业互联网技术的进一步发展和应用场景的不断扩展，其在提升生产效率和资源利用效率等方面的作用将愈加显著。例如，借助工业互联网，制造企业可以实时跟踪全球供应链中的每一个环节，从原材料采购到成品交付，实现全流程的可视化管理和优化配置。借助大数据分析和人工智能技术，工业互联网能够实现预测性维护、远程操作和自动化生产控制，实施灵活的生产计划和资源调度，最大限度地提高生产效率和资源利用率，降低生产成本。在未来，随着 5G、人工智能、物联网等技术的不断成熟和融合，工业互联网将进一步推动工业生产向智能化、数字化和网络化方向发展，不断提高生产过程的自动化和智能化水平，推动整个制造业生态系统的协同创新和可持续发展。

目前，工业生产活动向远海沙漠等区域不断拓展：特斯拉在内华达州沙漠地带建造巨型电池工厂、德国能源公司 RWE 和炼钢巨头 ArcelorMittal 共同开发、建设和运营海上风电和制氢设施等。这些工业生产活动不仅需要跨越百公里以上的距离，还要面对极端环境的挑战，对工业互联网的实时数据采集、远程监控、和信息安全传输带来了巨大挑战。以天基平台为核心的星地一体化网络可实现远海远域工业设备的全要素互联，突破地形限制，为远海、偏远地区及太空中的工业生产环节提供广域、泛在、安全的通信能力，因此，工业互联网的网络化和智能化发展离不开以天基平台为核心的星地一体化网络的支持。例如，美国海事卫星公司 Inmarsat 在制造业领域提供的卫星互联服务，为包含偏远地区在内的广域物联网设备提供可靠的连接，改善了生产资源以及人员的分配策略。德国电信物联网公司通过 FlexEnterprise 整合了卫星和地面网络，为工业互联网设备提供企业级连接服务。天基信息星地一体化网络作为工业互联网的重要支撑，不仅能够实现远海、远域工业设备的全要素互联，还有望推动超视距协同作业、跨域智能生产监控、跨时空柔性制造等创新模式的实现，将继续为全球生产制造活动的网络化和智能化发展提供有力支持。

与一般的卫星通信系统不同，面向工业制造的星地一体化网络需要承载图纸信息或者控制指令等关键信息的传输。卫星通信系统的广域覆盖特性和星地信道的开放性使得上述信息的传输极易受到非合作节点

的窃听和恶意干扰。星地通信链路安全保护机制的缺乏轻则造成生产流程的混乱，重则导致工业设备故障和敏感信息的泄露。因此，面向工业制造的星地传输方案设计不仅需要考虑通信链路的可靠性，还需要考虑信息传输的安全性，亟需建立相应的传输性能评估方法来指导具体的链路设计。现有大量关于工业制造场景下通信链路可靠性的研究，特别是针对天基信息网络中的星地链路，需要根据其特殊的传输环境进行精确建模和性能分析，以保障地海天远距离工业设备互联的有效性和可靠性。解放军理工大学的林敏团队推导了星地中继链路遍历容量的上下界，并给出了链路中断概率的解析表达式[1]。面向星地安全通信需求，南京邮电大学的欧阳键教授团队设计了基于非理想信道状态信息(Channel State Information，CSI)和统计CSI 的波束赋形方案来减少基站对卫星通信终端的干扰，并分析了星地链路的平均安全通信速率[2]。北京邮电大学的吕铁军教授团队根据有限状态的马尔可夫信道模型对卫星通信系统进行时间离散化分析，推导了星地链路通信速率的表达式，并对系统中断概率进行了分析[3]。陆军工程大学的张邦宁教授研究了无线环境中的干扰和通信设备的硬件损伤对星地协同传输性能的影响，提出了一种基于信干噪比和硬件损伤特性的中继选择方案，并推导了该方案的中断概率与系统吞吐量[4]。非正交多址接入技术（Non-orthogonal Multiple Access, NOMA）可在相同无线资源上为同时为多个用户提供无线接入服务，能够有效提高频谱资源的利用率，从而满足卫星通信场景下终端设备的大规模接入需求。因此，东南大学王承祥教授团队推导了 NOMA 框架下星地链路中断概率的渐进表达式，并据此得出了高信噪比条件下各终端用户的可达分集阶数与编码增益[5]。加拿大康考迪亚大学 Zhu Weiping 团队在[6]中研究了非正交多址接入技术在星地协同传输场景下的应用，根据各条链路的信道增益确定解码顺序，并得出了星地传输中断概率的闭合表达式。上述研究工作大多聚焦于对星地链路可靠性的分析，而缺乏对安全性的考虑，因此无法直接指导面向工业制造场景的星地传输方案设计。针对这一问题，本文在现有工作的基础上，进一步探究了星地链路安全性评估方法。为保证工业制造活动的顺利进行，星地传输方案不仅需要确保信息不被窃听更需要避免非合作节点对关键信息传输的恶意干扰。为满足工业制造场景下高层次的星地安全通信需求，本文从信号与背景电磁环境的不可分辨性出发，建立以循环谱、负熵和互信息率为核心的星地链路安全性综合评价指标，进而为工业制造场景下的星地传输方案设计提供指导。

2 星地传输安全性评估方法

信号与背景电磁环境的可分辨性不仅取决于信号自身的特性，还取决于非合作方的信号侦测方法。因此，本节将从常用的信号侦测方法出发，建立以负熵、互信息率和循环谱密度为核心的星地链路安全性综合评价指标。接下来，本节将对各项指标进行具体的介绍。

2.1 负熵

熵的概念最早起源于热力学领域，用于描述热力学系统的混乱程度或者无序状态。一个系统的熵越高，表示其内部微观状态越混乱，反之则越有序。香农将熵的概念引入信息论领域，他提出用熵来衡量信息的

不确定性：熵越高，信息的不确定度就越大，信息中包含的信息量就越大，反之则表示信息的不确定度越小，携带的信息量越小。熵在信息论中的数学定义如下：

$$H(X) = -E\left[\log_2\left\{p\left(x_i\right)\right\}\right] = -\sum_i p\left(x_i\right)\cdot\log_2\left\{p\left(x_i\right)\right\} \tag{1}$$

其中表示 X 离散随机变量，$E[\bullet]$ 表示期望，$p\left(x_i\right) = P\left\{X = x_i\right\}$。从上式还可以将熵的定义表述为：随机变量和其预测值之间的“距离”。对于连续性型随机变量，上式可以改写为：

$$h(X) = -E[\log_2\{f(x)\}] = -\int f(x)\cdot\log_2\{f(x)\}dx \tag{2}$$

值得注意的是，在所有均有零均值，单位方差的随机变量里，高斯随机变量具有最大的熵值。因此，对高斯（正态）随机变量做非线性变化使之分布改变，都会减少熵，或称为“增加一些负熵”。从广义来讲，熵增（即正熵）表示系统状态变得更加有序，而负熵则表示系统向更无序的状态发展。而在信息论领域中，负熵用于衡量某随机变量的分布与具有相同均值和方差的正态分布之间的“距离”。由于在等均值和方差的前提下，正态分布总是具有最大的熵，当且仅当随机变量服从正态分布时，负熵的值为 0，因此负熵总是非负的。负熵的数学表达式形式如下：

$$J(X) = h_G(X) - H(X) \tag{3}$$

其中 X 表示随机变量，$H(X)$ 为其熵值，$h_G(X)$ 为高斯随机变量的熵值。计算负熵时，对随机变量概率密度估计的准确程度将影响负熵计算的准确性。由于直接计算负熵可能涉及复杂的积分或者求和，计算复杂度较高，因此在实际计算时常采用近似方法。其中一种近似方法为利用随机变量的高阶矩来计算负熵近似值，如下式所示：

$$J(X) \approx \frac{1}{12}E\left[X^3\right]^2 + \frac{1}{48}\left\{E\left[X^4\right] - 3E\left[X^2\right]^2\right\}^2 \tag{4}$$

其中 $E\left[X^2\right]$，$E\left[X^3\right]$ 和 $E\left[X^4\right]$ 分别代表随机变量 X 的二阶原点矩、三阶原点矩和四阶原点矩。

2.2 互信息

根据熵的计算公式，我们令 $I(X) = -\log_2\left\{p\left(x_i\right)\right\}$（对于连续型随机变量则是 $I(X) = -\log_2\{f(x)\}$），在信息论领域中，将 $I(X)$ 定义为随机变量 X 的自信息。结合熵的计算公式，可以看出熵值等价于自信息的期望。自信息描述了某一事件发生的不确定性程度。$p\left(x_i\right)$ 可视为随机事件 x_i 发生的概率，自信息的定义表明，事件的发生概率与信息量之间呈反比，即事件发生的概率越低，一旦事件真实发生后，其传递的信息量就越大。

假设对随机过程 $\{X(t)\}$ 采样后得到 n 个样本 $X_1, X_2, ..., X_n$，用 $\boldsymbol{X}_n \equiv \left[X_1, X_2, \ldots, X_n\right]$ 表示，边缘密度函数

用 $f(x_i)$ 表示，$i=1,2,...,n$。联合概率密度函数用 $f\left(\boldsymbol{X}_n\right)\triangleq f\left(x_1,x_2,\ldots,x_n\right)$ 表示。对于每个样本 X_i，边缘熵衡量了该变量的不确定性，其数学表达式如下：

$$h\left(X_i\right)=-E\left[\log_2\left[f\left(x_i\right)\right]\right] \tag{5}$$

进一步，可推出 $\boldsymbol{X}_n$ 的联合熵：

$$h\left(\boldsymbol{X}_n\right)\triangleq h\left(X_1,X_2,\ldots,X_n\right)=-\int_{\mathbb{R}^n} f\left(x_1,x_2,\ldots,x_n\right)\log_2\left[f\left(x_1,x_2,\ldots,x_n\right)\right]dx_1dx_2\ldots dx_n \tag{6}$$

联合熵用于衡量多个随机变量之间不确定性的总量。

在信息论领域中，互信息可视为一个衡量两个随机变量间统计相关性的重要指标，它刻画了一个随机变量由于另一个已知随机变量而减少的不确定性的程度，通常用随机变量边缘熵与联合熵之间的差值表示。结合上述边缘熵和联合熵的定义，可进一步得到互信息的数学定义：

$$I\left(X_1,X_2,\ldots,X_n\right)=\sum_{i=1}^{n}h\left(X_i\right)-h\left(X_1,X_2,\ldots,X_n\right) \tag{7}$$

根据定义式，如果 $X_1,X_2,...,X_n$ 之间相互独立，即已知其中一个随机变量的取值无法为其他随机变量的取值提供任何信息。此时联合熵可以写为 $h\left(X_1,X_2,\ldots,X_n\right)=\sum_{i=1}^{n}h\left(X_i\right)$，因此互信息 $I\left(X_1,X_2,\ldots,X_n\right)=0$，即同时任意两个随机变量 X_i 和 X_j 之间的互信息 $I\left(X_i,X_j\right)$ 为 0。

2.3 循环谱密度

广义上的平稳信号是指均值不随时间变化，自相关函数只与时间差相关的一类信号，高斯白噪声信号就是常见的平稳信号。而循环平稳信号则是非平稳信号的一种，其统计特性往往随时间呈周期性变化。其中，一阶统计特性（如均值）具有周期性的信号称为一阶循环平稳信号，而二阶统计特性（如自相关函数）呈现周期性的非平稳信号则归类为二阶循环平稳信号。对于循环平稳信号，常常基于循环统计量来进行时频分析，通过将信号的循环分量进行分解，然后逐个进行时频分析来获得。具体的分析手段有计算循环均值和循环自相关函数，以及计算循环谱密度函数等。循环平稳分析是对非平稳信号的有效处理和分析手段，通过捕捉信号的周期性统计特性以及进行循环谱分析，提高信号分析的维度和准确度，并突破传统功率谱分析的局限性，在时间和频率维度上提供更全面的统计特性[7]。

对于具有二阶循环平稳特性的信号 $x(t)$，其自相关函数不仅与时间差有关，还与时间有关，假设自相关函数的周期为 T_0，τ 为时间差，其定义如下：

$$R(t,\tau)\triangleq\lim_{T\to\infty}R_x(t,\tau)_T=\lim_{N\to\infty}\frac{1}{2N+1}\sum_{n=-N}^{N}x\left(t+\frac{\tau}{2}+nT_0\right)x^*\left(t-\frac{\tau}{2}+nT_0\right) \tag{8}$$

由于 $R_x(t,\tau)$ 为周期函数，因此可用傅里叶级数展开为：

$$R(t,\tau)=\sum_{b=-\infty}^{+\infty}R_x^{b/T_0}(\tau)\mathrm{e}^{\mathrm{j}2\pi bt/T_0} \tag{9}$$

令 $\alpha=b/T_0$，可求得傅里叶级数的系数 $R_x^{\alpha}(\tau)$ 为：

$$R^{\alpha}(\tau)\triangleq\left\langle x\left(t+\frac{\tau}{2}\right)x^{*}\left(t-\frac{\tau}{2}\right)\mathrm{e}^{-\mathrm{j}2\pi\alpha t}\right\rangle_t \tag{10}$$

其中 $\langle\cdot\rangle_t$ 表示取时间平均。将上式 $R^{\alpha}(\tau)$ 定义为循环自相关函数，α 定义为循环频率。因此，根据傅里叶级数的定义，上述自相关函数可以写成多个分量和的形式：

$$R(t,\tau)=\sum_{\alpha}R_x^{\alpha}(\tau)\mathrm{e}^{\mathrm{j}2\pi\alpha t} \tag{11}$$

在平稳信号分析中，根据维纳-辛钦定理，功率信号的自相关函数与其功率谱密度函数之间为傅里叶变换对关系。在二阶循环平稳信号分析中，自相关函数同样与循环谱密度函数互为傅里叶变换对关系：

$$S^{\alpha}(f)\triangleq\int_{-\infty}^{\infty}R^{\alpha}(\tau)\mathrm{e}^{-\mathrm{j}2\pi f\tau}\mathrm{d}\tau \tag{12}$$

根据短时傅里叶变换，信号在时间 $\left[t-\frac{T}{2},t+\frac{T}{2}\right]$ 的频谱为：

$$X_T(t,f)\triangleq\int_{t-T/2}^{t+T/2}x(u)\mathrm{e}^{-\mathrm{j}2\pi fu}du \tag{13}$$

循环谱密度函数可以由传统的互谱密度函数推导得到。假设两信号为 $x_1(t)\triangleq x(t)\mathrm{e}^{-\mathrm{j}\pi\alpha t}$，$x_2(t)\triangleq x(t)\mathrm{e}^{\mathrm{j}\pi\alpha t}$，互相关函数为：

$$R_{uv}^{0}(\tau)\triangleq\left\langle x_1\left(t+\frac{\tau}{2}\right)x_2^{*}\left(t-\frac{\tau}{2}\right)\right\rangle_t=R_x^{\alpha}(\tau) \tag{14}$$

对互相关函数做傅里叶变换得到其互谱密度函数：

$$S_{uv}^{0}(f)\triangleq\int_{-\infty}^{\infty}R_{uv}^{0}(\tau)\mathrm{e}^{-\mathrm{j}2\pi f\tau}\mathrm{d}\tau=S^{\alpha}(f) \tag{15}$$

上述推导证明了，如果将信号瞬时谱分别向上和向下搬移相同的频率间隔，若二者相关，则该信号为循环平稳信号，向上和向下搬移的频率间隔即为循环频率。

一种常用的计算循环谱密度函数的方法为周期图法，周期图法利用傅里叶变换来估计信号的循环谱，其计算方式简单，但在数据长度有限的情况下，估计的循环谱密度方差较大[8]。周期图法的具体实现步骤如下：

① 计算信号的循环自相关函数：设循环平稳信号 $x(t)$ 的循环自相关函数为 $R_x^{\alpha}(\tau)\triangleq\left\langle x\left(t+\frac{\tau}{2}\right)x^{*}\left(t-\frac{\tau}{2}\right)\mathrm{e}^{-\mathrm{j}2\pi\alpha t}\right\rangle_t$；

②信号变换：令 $x_1(t)\triangleq x(t)\mathrm{e}^{-\mathrm{j}\pi\alpha t}$，$x_2(t)\triangleq x(t)\mathrm{e}^{\mathrm{j}\pi\alpha t}$；

③傅里叶变换：对上述两个信号 $x_1(t)$ 和 $x_2(t)$ 分别进行傅里叶变换，得到其频谱 $X_1(f)$ 和 $X_2(f)$，假设原始信号 $x(t)$ 的频谱函数为 $X(f)$，根据傅里叶变换的性质，有 $X_1(f)=X(f+\frac{\alpha}{2})$ 以及 $X_2(f)=X(f-\frac{\alpha}{2})$；

④计算循环谱密度：根据公式 $S_{uv}^{0}(f)\triangleq\int_{-\infty}^{\infty}R_{uv}^{0}(\tau)\mathrm{e}^{-\mathrm{j}2\pi f\tau}\mathrm{d}\tau=S^{\alpha}(f)$ 由互谱密度得到原信号的循环谱密度。在实际计算时，由于 α 不确定，因此需要对循环频率域进行划分，α 每次取不同的值，将计算得到的特定循环频率下的 $S^{\alpha}(f)$ 保存到二维矩阵的某一行或某一列，最终得到整个循环频率区间范围内的 $S^{\alpha}(f)$ 的二维表示。

通过计算循环谱密度，观察信号在循环域是否存在谱线，从而有效区分通信调制信号等循环平稳信号与高斯白噪声等平稳信号，还可以根据不同调制方式产生的不同循环频率来识别各种调制方式，提供包括载波频率、带宽、码元速率、相位和时间等在内的丰富时频信息。因此，利用循环谱进行信号检测与识别的方法被广泛应用。

3 典型星地通信方法安全性评估

为证明上述安全性评估指标的有效性，对直扩信号和背景背景高斯白噪声信号进行对比分析。所采用的直扩信号调制方式为 BPSK，扩频比为 64，信号功率为 1。采样率设为 1000Hz。分析并计算其负熵、互信息和循环谱密度，并与相同功率的背景高斯白噪声信号进行对比。

图 1 为 BPSK 调制下直扩通信信号的负熵估计值随信号数据长度的变化曲线。从图中可以看出直扩信号的负熵值较大，平均值约为 0.44，较高的负熵值表明 BPSK 直扩信号的非高斯性较强，在实际的星地传输过程中极易与背景噪声区分开，不利于通信信号隐蔽在背景电磁环境中。

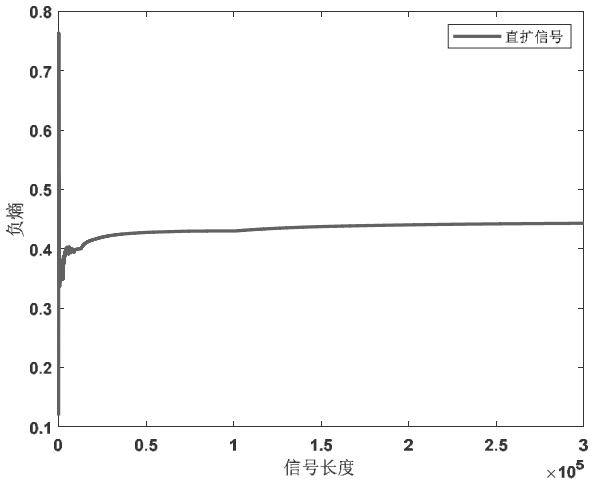


图 1 直扩信号负熵估计曲线

随着信号长度的增加，对信号数据分布的拟合就越准确，所得到的互信息估计值就更接近真实值。从图 2 中可以看出直扩信号的互信息明显高出高斯白噪声，同样地，通过估计互信息值极易区分出背景噪声

信号和直扩通信信号，不利于工业互联背景下的星地链路安全通信传输。

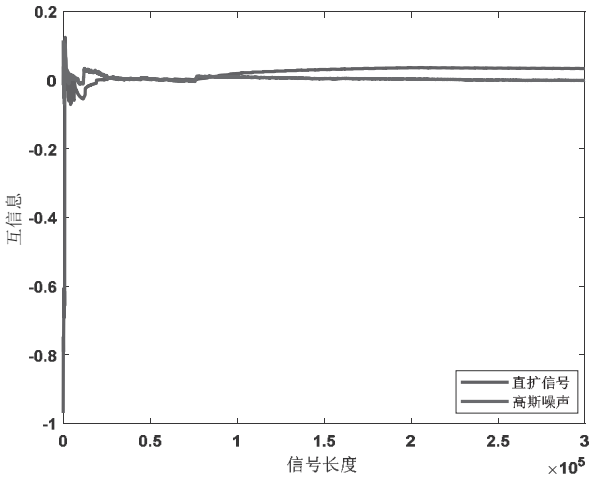
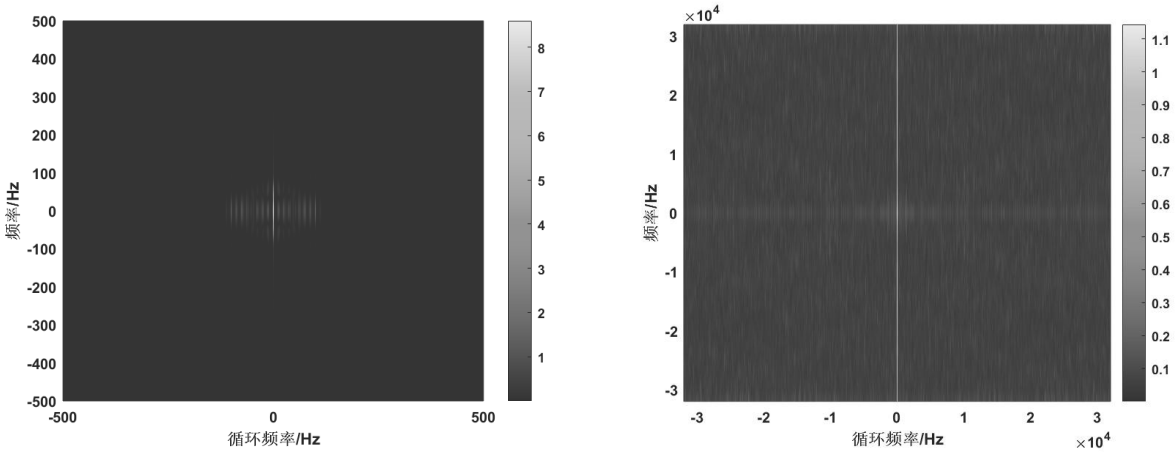


图 2 直扩信号和高斯噪声互信息估计曲线

图 3 中展示了 BPSK 直扩信号和高斯噪声的循环谱密度二维曲线，其中横坐标为循环频率，纵坐标为频率。由图 3（a）可知，BPSK 调制的直扩信号在循环频率域有多条谱线，体现了 BPSK 调制信号的循环平稳特性。而图 3（b）中的高斯白噪声由于不具有循环平稳特性，因此在循环域不存在谱线。结合两图可知，调制信号和高斯白噪声的循环功率谱密度有较大差别，通过对信号做循环谱分析，可以轻易地区分出调制信号和噪声信号，并且可根据循环频率的周期和分布特点进一步推知调制方式，因此循环谱密度可作为衡量星地链路传输安全性的指标。



（a）直扩信号　　（b）高斯噪声

图 3 直扩信号和高斯噪声循环谱密度

4 结束语

随着工业互联网的快速发展，工业生产活动向偏远区域扩展，星地一体化网络为全球工业提供有力支持。本文聚焦于面向工业制造的星地一体化网络传输安全性问题，分析了卫星通信广域覆盖与信道开放性

带来的信息安全挑战，并系统地探讨了星地链路安全评估方法，并构建了以循环谱、负熵和互信息率为核心的综合评价指标体系，为全面评估星地链路安全性提供了有力参考。

参考文献：

[1] AN K, LIN M, LIANG T. On the Performance of Multiuser Hybrid Satellite-Terrestrial Relay Networks with Opportunistic Scheduling[J]. IEEE Communications Letters, 2015, 19(10): 1722-1725.

[2] AN K, LIN M, OUYANG J, et al. Secure Transmission in Cognitive Satellite Terrestrial Networks[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(11): 3025-3037.

[3] MA Y, LV T, LI T, et al. Effect of Strong Time-Varying Transmission Distance on LEO Satellite-Terrestrial Deliveries[J]. IEEE Transactions on Vehicular Technology, 2022, 71(9): 9781-9793.

[4] GUO K, LIN M, ZHANG B, et al. Performance Analysis of Hybrid Satellite-Terrestrial Cooperative Networks with Relay Selection[J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 9053-9067.

[5] YAN X, XIAO H, WANG C, et al. Outage Performance of NOMA-Based Hybrid Satellite-Terrestrial Relay Networks[J]. IEEE Wireless Communications Letters, 2018, 7(4): 538-541.

[6] HAN L, ZHU W, LIN M. Uplink Outage Performance of NOMA-Based Hybrid Satellite-Terrestrial Relay Networks Over Generalized Inhomogeneous Fading Channels[J]. IEEE Transactions on Communications, 2022, 70(4): 2417-2434.

[7] 黄知涛，周一宇，姜文利. 循环平稳信号处理与应用[M]. 北京：科学出版社, 2006.

[8] 张贤达，保铮. 非平稳信号分析与处理[M]. 北京：国防工业出版社, 1998.

绿色集成连铸中包计划研究

魏俊杰， 曹旺， 王庆， 黄敏*

（东北大学 信息科学与工程学院,辽宁 沈阳 110004）

摘 要：在钢铁生产过程中，连铸工艺是企业实现连续、高效生产的核心环节；其中中包不仅是浇铸前的缓冲区，也是实现炼钢与连铸平稳过渡的桥梁。本文在提出集成浇次计划与中包计划的基础上，结合当前钢铁行业倡导可持续发展背景，构建考虑绿色因素的集成连铸中包计划多目标优化模型，并定制化设计改进 NSGA-III算法进行求解，并对算法有效性及绿色因素对模型求解结果的影响进行分析。

关键词：集成计划；绿色计划；多目标优化

Research on the green integrated tundish planning of steel casting process

*WEI Junjie, CAO Wang, WANG Qing, HUANG Min**

（*College of Information Science and Engineering, Northeastern University, Shenyang 110004*）

Abstract: In the process of steel production, continuous casting process is the core link for enterprises to realize continuous and efficient production; and tundish is not only a buffer zone before pouring, but also a bridge to realize a smooth transition between steelmaking and continuous casting. In this paper, on the basis of proposing a suitable integrated pouring plan and tundish plan, combined with the current sustainable development background, we construct a multi-objective optimization model of integrated continuous casting tundish plan considering green factors, and design the corresponding solution method. At the same time, the effectiveness of the algorithm and the influence of green factors on the model solution results are analyzed.

Key words: Integrated planning; Green planning; Multi-objective optimization

1 引言

钢铁行业，作为我国经济结构的重要组成部分，其发展水平与规模直接反映了一个国家的工业化程度和基础设施建设能力。钢铁企业内部生产计划优化问题历年来吸引了众多国内外学者的广泛关注。与此同时，随着全球气候变化问题日益严峻，我国积极响应国际社会号召，国家发展和改革委员会等相关部门逐步推出了钢铁企业温室气体排放核算方法[1]和企业统筹协调及绿色低碳[2]发展等政策，明确提出力争 2030 年前实现碳达峰、2060 年前实现碳中和的目标。因此，冶金工业绿色化、智能化转型已成为时代命题[3]。

其中，连铸工艺作为连接炼钢与热轧工艺的桥梁，其流程优化对资源节约、环保及生产系统持续性至关重要，对钢铁

基金项目：国家自然科学基金重大研究计划重点支持项目(92267206)；国家自然科学基金重点项目(62032013)；辽宁省“兴辽英才计划”(XLYC2202045)。

作者简介：魏俊杰（2002-），男，硕士生，从事生产计划与调度、智能算法等研究，E-mail：weijunjie000@163.com；曹旺（1995-），男，博士生，从事智能制造、鲁棒优化等研究，E-mail：2310265@stu.neu.edu.cn；王庆（1969－），男，副教授，博士，从事系统建模与优化、 供应链与 ERP 系统等研究，E-mail：qwang@mail.neu.edu.cn；黄敏（1968-），女，教授，博士生导师，从事物流与供应链管理、智能算法设计与优化、调度理论与方法等研究，E-mail：mhuang@mail.neu.edu.cn

工业绿色化转型价值提升影响显著。在现有研究中，一部分学者对钢铁企业组批问题进行研究，如易剑等[4]通过多旅行商问题模型解决了连铸计划中的中间包编组问题。Tang 等人[5]则通过动态规划方法重新分配钢坯订单，旨在提升资源利用率和顾客满意度。但上述关于组批问题的研究未考虑绿色因素；另一部分学者对考虑绿色因素的连铸生产过程进行建模求解，李国臣等人[6]聚焦于生产调度的并行批处理优化，以最小化最长作业完成时间为目标，研究了具有相同炉容但功率不同的非均质并行设备的能源消耗约束。蒋胜龙等[7]设置了工序能源负载限制，构建了旨在平衡最晚完工时间和总等待时间最小化的多目标生产调度模型。但上述考虑绿色因素的研究大多是在调度层面展开的。

本文的“绿色集成连铸中包计划”，在炉次组批的基础上考虑绿色因素，通过数学建模和算法优化，为连铸生产提供了优化可行的绿色集成方案，同时验证了本文提出的改进 NSGA-III算法在解决绿色集成连铸中包计划制定问题上所具有的适用性和高效性，为钢铁企业同步实现节能减排与提升生产效率的绿色化经营目标提供了理论基础。

2 绿色集成连铸中包计划

2.1 问题描述

本文绿色集成连铸中包计划核心在于在满足连铸生产过程的工艺规程条件下，对炉次的组批过程进行精心规划和编排，进而降低设备成本、生产中断时间和能耗，同时提高生产效率和产品质量。主要问题优化考量包括：减少中包使用量、优化浇次编组、降低交接坯梯形坯产生率及优化绿色生产指标。

2.2 工艺规程

在绿色集成连铸中包计划中需要遵守一系列工艺规程以确保生产过程的顺利进行、提高产品质量以及优化资源利用。这些规程包含中包寿命、炉次宽度差异、钢级匹配以及生产排序等多个方面内容。

具体工艺规程如下：

（1）同一中包中的炉次必须有同一连浇族代码；

（2）中包拥有生命周期，即中包寿命，一个中包连浇炉次不能超过中包寿命；

（3）同一中包内可存在宽度不同的炉次，但存在限制：宽度差值不可超过 300mm，调宽次数不可超过 1 次；

（4）同一中包中炉次钢级尽量相同；

（5）同一中包中炉次按照宽度非增排序生产；

（6）同一浇次中的中包必须有同一连浇族代码；

（7）同一浇次中相邻中包宽度差值尽量小；

（8）同一浇次内中包按照中包内炉次宽度最大值非增规程生产；

（9）不同连铸机累计运行时间尽量接近；

2.3 模型建立

2.3.1 变量设置

为了清晰地描述本文绿色集成连铸中包问题数学模型，定义了如下参数：

n：炉次总数，炉次集：$\Omega_{\mathrm{n}} = \{1,2,\ldots,\mathrm{i},\ldots,\mathrm{n}\}$.

m：中包总数，中包集：$\Omega_m = \{1,2,\ldots,j,\ldots,m\}$.

P：连浇次个数，连浇序号集：$\Omega_P = \{1,2,\ldots,k,\ldots,P\}$.

Q：连铸机个数，连铸机序号集：$\Omega_Q = \{1,2,\ldots,l,\ldots,Q\}$.

C_i^{code}：炉次连浇族标识.

SG_i：炉次钢级标识.

W_i：炉次宽度标识.

TD_j：中间包j的使用寿命.

TW_j^{max}，TW_j^{min}：中包的最大、最小宽度.

TC_j^{code}：中包继承的炉次的连浇族标识.

n_k^W：调宽次数限制　$if\ W_{(k,i)} - W_{(k,i+1)} \neq 0$，$n_k^W + 1$.

λ^{SG_T}：中包内连续两个炉次存在钢级差异惩罚系数.

λ^{SG_C}：浇次内连续两个中包首尾炉次存在钢级差异惩罚系数.

λ^{W_T}：中包内连续两个炉次存在宽度差异惩罚系数.

λ^{W_C}：浇次内连续两个中包首尾炉次存在宽度差异惩罚系数.

num^{SG_T}：当前中包内连续两炉次存在钢级差异个数.

num^{SG_C}：当前浇次内连续两个中包收尾炉次存在钢级差异个数.

P_l：第l个连铸机上连浇次数.

E_i^{charge}：第i个炉次在连铸过程中能耗.

$E_j^{Tundish}$：连铸过程中更换中包j造成的额外能耗.

E_k^{Con-rt}：不同连浇序号间连铸机重启导致的额外能耗.

$E_l^{Con-stop}$：因连铸机l空闲等待产生的能耗.

T_i^{charge}：第i个炉次连铸过程作业时间.

$T^{Tundish}$：更换中包带来的额外时间.

T^{Con-rt}：连铸机重启带来的额外时间.

决策变量：

x_{ij}：中包j包含炉次i，$x_{ij} = 1$，否则$x_{ij} = 0$.

y_{jk}：浇次号k包含中包j，$y_{jk} = 1$，否则$y_{jk} = 0$.

z_{kl}：浇次k在l号连铸机上加工，$z_{kl} = 1$，否则$z_{kl} = 0$.

$w_{i_1 i_2 j}$：炉次i_2在炉次i_1后立刻被生产在中包内j中，$w_{i_1 i_2 j} = 1$，否则$w_{i_1 i_2 j} = 0$.

$e_{j_1 j_2 k}$：中包j_2在中包j_1后立刻被生产在浇次内k中，$e_{j_1 j_2 k} = 1$，否则$e_{j_1 j_2 k} = 0$.

u_j：中包j被使用，$u_j = 1$，否则$u_j = 0$.

v_k：浇次k被使用，$v_k = 1$，否则$v_k = 0$.

2.3.2 数学模型

$$\min m = \sum_{j=1}^{M} u_j \tag{1}$$

$$\min p = \sum_{k=1}^{P} v_k \tag{2}$$

$$min \sum_{j=1}^{m} \lambda^{SG_T} * num^{SG_T} + \sum_{k=1}^{p} \lambda^{SG_C} * num^{SG_C} \tag{3}$$

$$\begin{aligned} min\ \lambda^{W_T} \sum_{j=1}^{m} \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} \left| W_{i_1} - W_{i_2} \right| w_{i_1 i_2 j} \\ + \lambda^{W_C} \sum_{k=1}^{P} \sum_{j_1=1}^{m} \sum_{j_2=1}^{m} \left| TW_{j_1}^{max} - TW_{j_2}^{min} \right| e_{j_1 j_2 k} \end{aligned} \tag{4}$$

$$\begin{aligned} minE^g + E^s = \sum_{k=1}^{p} \left(\sum_{j=1}^{m} \sum_{i=1}^{n} y_{jk} x_{ij} E_i^{charge} + \sum_{j=1}^{m} y_{jk} E^{Tundish} + E_k^{Con-rt} \right) \\ + \sum_{l=1}^{Q} P^{Con-stop} \left(T^{max} - \sum_{k=1}^{P} z_{kl} T_k^{cast} \right) \end{aligned} \tag{5}$$

其中

$$T_k^{cast} = \sum_{j=1}^{m} \sum_{i=1}^{n} y_{jk} x_{ij} T_i^{charge} + \sum_{j=1}^{m} y_{jk} T^{Tundish} + T^{Con-rt}$$

$$T^{max} = max \left(\sum_{k=1}^{P} z_{k1} T_k^{cast}, \ldots, \sum_{k=1}^{P} z_{kl} T_k^{cast}, \ldots, \sum_{k=1}^{P} z_{kQ} T_k^{cast} \right)$$

$s.t.$

$$\sum_{i=1}^{n} x_{ij} \le 1, j = 1,2, \ldots, m \tag{6}$$

$$\sum_{j=1}^{m} y_{jk} \le 1, k = 1,2, \ldots, P \tag{7}$$

$$\sum_{k=1}^{p} z_{kl} \le 1, l = 1,2, \ldots, Q \tag{8}$$

$$\sum_{i=1}^{n} x_{ij} \le TD_j, \forall j \in \Omega_m \tag{9}$$

$$\left| C_i^{\text{code}} - C_{min\{i'_j\}}^{\text{code}} \right| x_{ij} = 0, \forall i \in \Omega_n, j \in \Omega_m \tag{10}$$

$$\left| TC_{j_1}^{code} - TC_{j_2}^{code} \right| y_{jk} = 0 \tag{11}$$

$$TW_j^{max} - TW_j^{min} < \Delta W，j = 1,2, \ldots, m \tag{12}$$

$$n_k^W < n^{Wmax}, k = 1,2 \dots, P \tag{13}$$

$$0 \le \left(W_{i_1} - W_{i_2}\right) * w_{i_1 i_2 j} \le \sigma, i_1 . i_2 \in 1, \dots, (n-1), j = 1, \dots, M \tag{14}$$

$$0 \le \left(TW_{j_1}^{max} - TW_{j_2}^{max}\right) * e_{j_1 j_2 k} \le \sigma, j_1 . j_2 \in 1, \dots, (n-1), k = 1, \dots, \mathrm{P} \tag{15}$$

其中式(1)表示最小化中包使用数量，式(2)表示最小化浇次个数，式(3)表示最小化交接坯数量，式(3)表示最小化梯形坯数量，式(5)表示最小化能源消耗。式(6-8)分别表示炉次、中包、浇次、连铸机的隶属关系，式(9)表示中包寿命约束，式(10,11)表示中包、浇次内可连浇约束，式(12)表示中包内宽度调整幅度限制，式(13)表示中包内宽度调整次数限制，式(14,15)表示中包、浇次内生产顺序限制。

3 基于改进 NSGA-Ⅲ算法求解方法

本文所研究的优化问题模型优化目标数量超过了三个，这类问题通常被归类为高维度多目标优化问题(many-objective optimization problems, MaOPs)[8]。对于这类问题，K.Deb 等人于 2014 年推出了 NSGA-III (Non-dominated Sorting Genetic Algorithm, the Third Version)[9]，即第三代非支配排序遗传算法，作为对 NSGA-II[10]的重要升级，它在应对高维度目标优化问题上展现出了卓越性能。本文将在 NSGA-Ⅲ算法基础上对针对问题特点设计求解进行模型求解。

3.1 算法流程

本节详细介绍了一种经过改良的NSGA-III算法的执行流程，该算法是在经典NSGA-III基础上的进一步优化，旨在更高效地解决多目标优化问题。具体执行步骤展开如下：

Step 1：算法参数初始化；

Step 2：种群初始化；

Step 3：进行种群的交叉、变异操作并修复不合法解；

Step 4：求解目标值，进行非支配等级排序，并降低完全等效解的支配等级；

Step 5：根据参考点小生境选择策略及同一非支配等级下选择性保留选择精英解进入子代；

Step 6：对子代进行非支配等级排序；

Step 7：判断是否满足终止条件，若满足则输出子代非支配等级最高的解集并结束流程；如果不满足则当前迭代次数＋1，同时转到Step 3。

3.2 编码解码

针对本文提出的数学模型，设计了一种以炉次编号为主体，中包及浇次编号为分隔符的整数编码及对应解码方式，具体方式如下：

假设在问题中拥有18个炉次待分配，预计分配成4个中包2个浇次。在本文使用的编码方式中，使用数字1-18代表炉次编号、19-22代表中包分隔符、23-24代表浇次分隔符，并在最后记录该解码段所包含的中包数及浇次数。

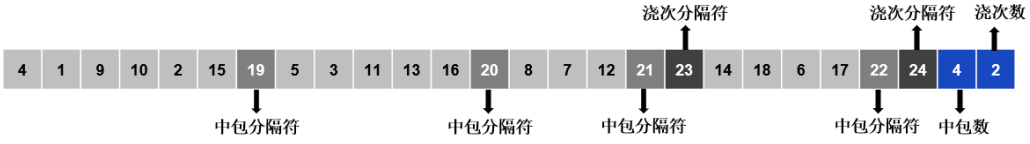


图 1 编码效果

在解码过程中，给定需要处理的炉次总数，通过编码最后的两位获取需解码解的中包个数与浇次个数，从而通过计算出解的中包分隔符及浇次分隔符编号进行解码。

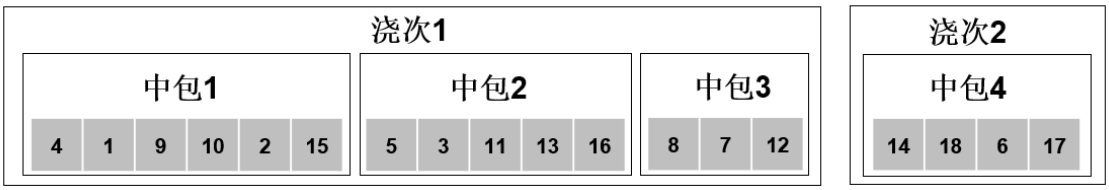


图 2 解码效果

3.3 交叉策略

在遗传算法的优化过程中，交叉算子起着至关重要的角色，它模拟了生物进化中的基因重组现象，通过组合不同父代个体的遗传信息，生成具有新特性的子代个体。在本研究中编码方式，我们设计了一种特定的交叉策略。具体步骤如下：

（1）去除编码末端的中包与浇次数量标志，并在编码长度短的父代末尾补充较长父代缺少的编号。

（2）从两个亲本染色体中任意选取起点和终点，将亲本染色体1此区间内的基因复制到子代1对应位置，随后依照亲本染色体2序列补全子代1缺失的基因。

（3）去除子代多余的编码，复原最后两位中包数与浇次数。另一个子代以类似方式得到。

3.4 变异策略

在遗传算法的优化过程中，变异步骤通过模拟生物进化中的基因突变现象，随机改变个体的某些遗传信息，为算法引入新的遗传特性。在本文研究中设计了三种特定的变异策略。

3.4.1 随机交换算子

在进行遗传算法、模拟生物进化或其他涉及序列操作的算法设计时，随机选取基因序列中的两个元素并交换它们的位置是一种常见的变异操作，旨在引入多样性以跳出局部最优解，促进全局搜索。

3.4.2 标识符剔除算子

对中包或浇次标识符进行随机删除，达到合并中包或浇次的目的。

3.4.3 炉次重插入算子

随机选取炉次并基于其属性与其他炉次进行匹配，进而紧跟插入一个相似炉次后面。

3.5 修复策略

在探讨连铸中包计划的多目标优化问题时，一个关键的挑战在于如何确保生成的计划方案不仅在多个性能指标上达到最优，更需要满足工艺规程要求。为此，本文提出了一种解修复策略。具体步骤如下：

1）遍历中包内所有炉次，剔除与中包内首个炉次连浇族代码不同的炉次。

2）遍历浇次内所有中包，将与浇次内首个中包连浇族代码不同的中包放至下一浇次末尾。

3）在满足中包寿命的前提下，将待分配的炉次按连浇规则顺序放置在中包中。

4）先对中包内炉次按宽度排序，根据中包内宽度规则拆分中包。

5）将浇次内中包按宽度排序。

3.6 精英保留策略

3.6.1 降低完全等效解非支配等级

在连铸生产计划制定过程中，经常会遇到多个连浇族代码、钢级、浇铸宽度等参数完全相同的炉次。这些炉次在工艺要求上没有任何区别，我们称之为“完全等效炉次”。在本文问题求解过程中，也会产生大量在目标函数评估上表现完全相同，但在决策变量上，特别是生产顺序上存在微小的差异的等效解。这里将这些由于完全等效炉次生产顺序不同产生的等效解称为本问题中的“完全等效解”。对于本文的优化问题来说，这些完全等效解是冗余的，因为它们在生产过程上没有任何差异。

针对等效解导致的冗余性影响，本文提出了一种针对连铸生产过程的优化策略，即降低完全等效解的支配等级。该方法的核心思想是通过识别并处理这些等效解，以减少它们在进化过程中的影响力，同时保持种群的多样性和搜索效率。

具体方法包括以下步骤：

（1）完全等效解检测：在每次迭代中，我们首先识别出种群中的完全等效解。具体方法为将解中完全等效炉次使用同一编号替换，再比较解之间是否属于完全解，并将这些解归为一个完全等效解组。

（2）支配等级调整：对于检测到的完全等效解，我们降低它们的支配等级。具体方式为将它们的非支配层级乘以一个系数：

$$R_{new_i} = R_i * e^{0.5k} \tag{16}$$

其中R_i代表这一个体当前支配等级，R_new_i代表新的支配等级，e为自然对数，k代表炉次i在完全等效解组中第k个出现。这样做可以确保在后续的选择过程中，后出现的完全等效解不会被优先选择，从而减少了它们在种群中的数量。

此策略有效解决了完全等效解带来冗余问题，保证解决方案的有效性和实用性，对提升连铸生产调度的优化水平具有重要意义。

3.6.2 同一非支配等级下选择性保留

在NSGA-III算法中将子代和父代种群进行非支配等级排序后统一选择新的父代，当某一层级的个体数量不足以填满新种群时，该层级的所有个体均会被无条件地选入新种群中。当某一层级中的个体数量过于庞大，以至于选入这些个体后会导致新种群的规模超出预设的种群规模限制时，算法会依据个体的拥挤距离进行排序，并选择其中拥挤距离较大的个体加入新种群，以此来保持种群的多样性。

然而，这种精英保留机制在某些特定情况下可能带来问题，即如果大量的相似个体因在某一层级中表现相近而被保留下来，它们可能会占据新种群中的大量空间，导致种群中个体的多样性降低，甚至可能引发算法的过早收敛。

为了增强种群的多样性，进而更有效地解决优化问题，本文提出了一种改进的保留策略：需要针对每个非支配层选取一个需要保留解的个数，然后使用NSGA-III的小生境保留操作选取该支配等级下的个体。

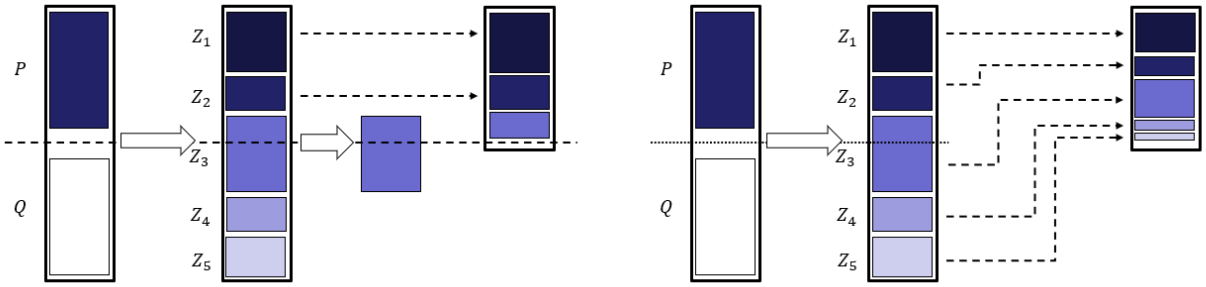


图 3 子代种群选择方式改变

计算保留解个数函数如下：

$$K = popn \cdot \left(1 - \left(1 - \frac{N_{child}}{N_{all}}\right) * P_1 * P_2\right) \tag{17}$$

其中：$P_1 = \frac{ln(R-1)}{ln(R_{sum}-1)}$，$P_2 = tanh\left(\frac{popn}{pointn} - 1\right)$

K代表当前非支配等级最终保留的个体数，$popn$代表当前非支配等级群体个数；N_child为需要保留的种群总数，N_all为当前参与小生境选择的种群总数，$(1-(N_child)/(N_all))$限制种群最大剔除概率，保证有充足的解进入子代。

对于概率P_1，R代表当前群体非支配等级，R_{sum}代表当前种群非支配等级总数，非支配等级越高，保留的解越多。对于概率P_2，$pointn$代表当前非支配等级关联参考点个数，$popn/pointn$越小，保留的解越多，当$popn/pointn = 1$时，当前非支配等级下的解全部保留。概率P_1、P_2随支配等级和$popn/pointn$影响数值变化如图4所示。

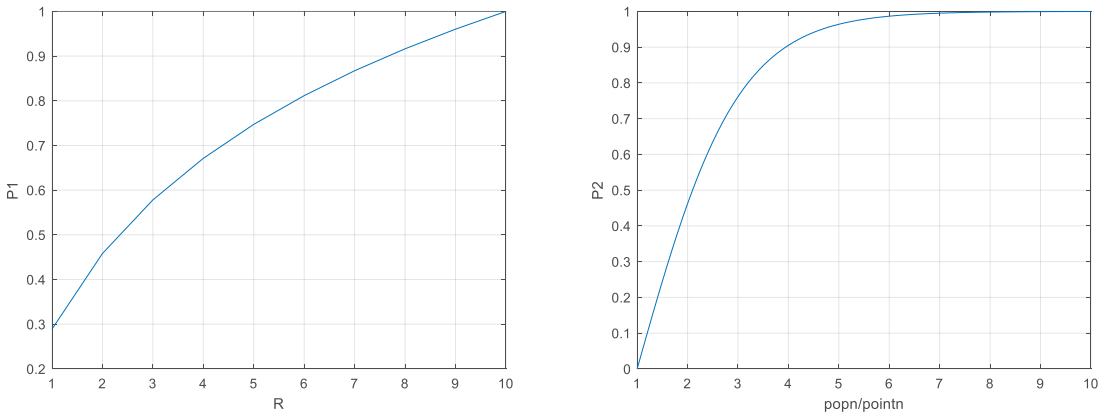


图 4 P_1、P_2函数值变化

此外我们构建一个精英保存池用于未被选择的解，处在精英保存库的解每代进行非支配等级排序，选择非支配等级最高的解进行下一代小生境保留，但不进行交叉和变异操作。

通过引入这一改进的保留策略，我们期望NSGA-III算法在探索解空间时能够展现出更高的灵活性和有效性，进而在处理复杂优化问题时获得更好的性能。

4 数值实验与结果分析

4.1 算例设计

针对所提出的问题，本文设计了50炉次、100炉次、200炉次三个规模不同的算例进行仿真实验。

（1）50炉次算例设计

考虑8种钢级，3种连浇族代码，宽度范围为1000-1450的50个炉次进行数值实验，将其放置在2台连铸机上完成连铸工艺。详细数据见表1。

表 1 50 炉次算例

编号	连浇族号	宽度	钢级	编号	连浇族号	宽度	钢级
1	130160	1000	AP1056E1	26	130160	1450	DN0146D1
2	130160	1000	AP1056E1	27	130160	1450	AQ2060E1
3	130160	1000	AP1056E1	28	130160	1450	AQ2060E1
4	130160	1000	AP1056E1	29	130260	1000	AN0543D5
5	130160	1000	AP1056E1	30	130260	1000	AN0543D5
6	130160	1000	AP1056E1	31	130260	1000	AN0543D5
7	130160	1000	AP1056E1	32	130260	1000	AN0543D5
8	130160	1000	AP1056E1	33	130260	1000	AN0543D5
9	130160	1100	AP0740D5	34	130260	1000	AN0543D5
10	130160	1100	AP0740D5	35	130260	1000	AN0543D5
11	130160	1250	AP0740D5	36	130260	1000	AN0543D5
12	130160	1250	AP0740D5	37	130260	1000	AN0543D5
13	130160	1250	AP0740D5	38	130260	1000	AN0543D5
14	130160	1250	AP0740D5	39	130260	1000	AN0543D5
15	130160	1450	DN0146D1	40	130260	1000	AN0543D5
16	130160	1450	DN0146D1	41	140740	1250	MW9121E2
17	130160	1450	DN0146D1	42	140740	1250	MW9121E2
18	130160	1450	DN0146D1	43	140740	1250	MW9121E2
19	130160	1450	AQ2060E1	44	140740	1250	MW9121E2
20	130160	1450	AQ2060E1	45	140740	1350	MW9121E1
21	130160	1450	AQ2060E1	46	140740	1350	MW9121E1
22	130160	1450	AQ2060E1	47	140740	1350	MW9121E2
23	130160	1450	AQ2060E1	48	140740	1350	MW9121E2
24	130160	1450	AP1056E1	49	140740	1350	MW9121E2
25	130160	1450	DN0146D1	50	140740	1350	MW9121E2

（2）100炉次算例设计

考虑10种钢级，4种连浇族代码，宽度范围为1000-1450的100个炉次进行数值实验。将其放置在3台连铸机上完成连铸工艺。

（3）200炉次算例设计

考虑15种钢级，5种连浇族代码，宽度范围为1000-1450的100个炉次进行数值实验。将其放置在4台连铸机上完成连铸工艺。

其它模型参数设置见下表2：

表 2 模型参数设置

参数	数值	说明
λ^{SG_T}	2	中包内连续两炉次在钢级差异惩罚系数
λ^{SG_C}	1	浇次内连续两个中包首尾炉次钢级差异惩罚系数
λ^{W_T}	2	中包内连续两个炉次存在宽度差异惩罚系数
λ^{W_C}	1	浇次内连续两个中包首位炉次存在宽度差异惩罚系数

E_i^{charge}	10	单个炉次在连铸过程中能耗
E_i^{charge}	10	连铸过程中更换中间包造成的额外能耗
$E_l^{Con-stop}$	10	连铸机待机能耗
E_k^{Con-rt}	100	不同连浇序号间连铸机重启造成的能耗
$T^{Tundish}$	1	更换中包带来的额外时间消耗
T^{Con-rt}	6	不同连浇序号间连铸机重启时间消耗
T_i^{charge}	10	单个炉次在连铸过程中时间消耗
n_k^W	1	中包内调宽次数限制
TD_j	6	中包寿命
ΔW	300	中包调宽幅度限制

4.2 改进算法性能分析

为了分析改进NSGA-III算法相较于标准NSGA-III算法的优势与差异，本部分将分别采用50组、100组、以及200组炉次的算例，将标准NSGA-III算法、只进行完全等效解替代、只进行同一支配等级下选择性保留及同时运行两种精英保留策略的三个改进NSGA-III算法进行30次运算，记录超体积（Hypervolume，HV）指标[11]进行比较。

表 3 不同算例改进算法对 HV 值影响

	50 炉次算例	100 炉次算例	200 炉次算例
标准 NSGA-III算法	0.5733	0.4626	0.5026
只添加完全等效解替代	0.6858	0.6510	0.6618
只添加选择性保留	0.6804	0.6239	0.6325
改进 NSGA-III算法	0.7027	0.6661	0.6887

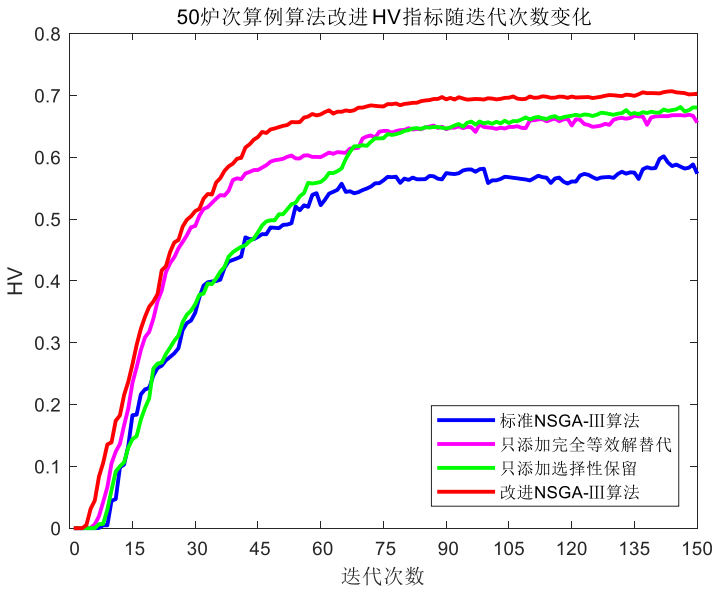


图 5 50 炉次算例不同改进方式 HV 指标随迭代次数变化

改进NSGA-III算法通过结合完全等效解替代和选择性保留策略，在提高解集质量（以HV衡量）方面表现显著。此外完全等效解替代策略和选择性保留策略单独使用时也显示出较好的效果；验证了精英保留策略对提升种群多样性、防止出现局部最优的有效性。

4.3 绿色因素分析

在仅考虑中间包及浇次数量、交接坯及梯形坯惩罚等因素而不考虑绿色因素时，使用改进NSGA-III算法对连铸中包计划问题进行求解，运行10次后，记录所有炉次完成连铸工序产生的组批能耗、待机能耗及完工时间如下表所示：

表 4 不考虑绿色因素下的能耗值

		组批能耗		待机能耗		完工时间	
		未考虑	考虑	未考虑	考虑	未考虑	考虑
50 炉次算例	平均值	1219.0	1114.6	756.4	203.8	311.7	281.0
	最大值	1630	1660	3230	1270	431	345
	最小值	900	890	140	0	277	267
100 炉次算例	平均值	1836.5	1904.2	3480.9	1686.4	468.8	410.4
	最大值	2370	2520	7160	12050	596	751
	最小值	1580	1580	830	60	379	358
200 炉次算例	平均值	3287.4	3577.1	12046.4	6590.9	824.3	692.4
	最大值	4650	5610	19720	29480	1031	1255
	最小值	2850	2850	3320	340	618	532

通过对绿色集成连铸中包计划在考虑与不考虑绿色因素两种情境下的对比分析，发现以下显著差异变化：组批能耗在考虑绿色因素后可能会轻微上涨，但增幅有限，这是由于一部分解方案为实现产能均衡分布而拆分浇次导致的。待机能耗呈现显著优化，特别是在大规模炉次情形下，如200炉次的平均待机能耗从无绿色考量的12046.4单位降至6590.9单位，降幅接近50%。这归功于绿色规划中生产调度的优化，有效削减了设备闲置状态下的能耗，对节能减排有着实质性的贡献。考虑绿色因素后，三个测试案例的平均完工时间分别缩短了9.85%、12.46%和16.00%，显示生产流程更加紧凑高效，既减少了资源浪费，又提升了产出速度，有利于增强企业市场竞争力和响应能力。

综上所述，将绿色因素融入并通过改良的NSGA-III算法优化，促使能耗结构得到改善，生产效率显著提升。尽管组批能耗出现轻微增长，但待机能耗的大幅缩减及完工时间的缩短，表明了绿色生产模式在提升资源利用效率和减轻环境压力上的显著成效。本研究不仅验证了绿色理念在生产调度中的可行性和优越性，也为钢铁等高耗能行业寻求经济效益与生态责任的平衡提供了重要启示。

5 结束语

本文针对现有研究结合绿色因素与炉次组批问题的不足，构建了考虑绿色因素的集成连铸中包计划问题多目标优化模型，设计改进的NSGA-III算法进行求解，验证了改进算法的有效性和搜索效率，并对绿色因素对模型求解结果的影响进行分析，展示了本文所提方法在降低组批能耗、待机能耗和缩短完工时间方面的优势。本文作为深化绿色生产技术和算法设计探索性研究，为推动产业绿色转型、达成碳中和愿景的提供了有效借鉴。

参考文献：

[1]　国家发展和改革委员会.国家发展改革委办公厅关于印发首批 10 个行业企业温室气体排放核算方法与报告指南(试行)

的通知[EB/OL].(2013-10-15)[2019-07-10].

[2] 关于促进钢铁工业高质量发展的指导意见.工信部联原〔2022〕6 号.

[3] 殷瑞钰.冶金学的时代命题——打通流程,沟通层次,开新说[J]. 钢铁, 2021, 56(08): 4-9.

[4] 易剑,谭树彬,李维刚等.连铸组中间包问题的 MTSP 模型及混合优化算法[J].东北大学学报(自然科学版), 2012, 33(09):1235-1239.

[5] Tang L , Luo J , Liu J .Modelling and a tabu search solution for the slab reallocation problem in the steel industry[J].[2024-05-25].

[6] 李国臣,乔非,王俊凯,等.考虑能耗约束的并行机组批调度[J].中南大学学报(自然科学版),2017,48(08):2063-2072.

[7] 蒋胜龙,文耀民,唐伟等.一种考虑能源约束的炼钢-连铸调度优化方法[J]. 华中科技大学学报(自然科学版),2022,50(06):118-123+132.

[8] Hughes, E.J. “Evolutionary Many-Objective Optimisation: Many Once or One Many?” 2005 IEEE Congress on Evolutionary Computation 1 (2005): 222-227 Vol.1.

[9] Deb K , Jain H .An Evolutionary Many-Objective Optimization Algorithm Using Reference-Point-Based Nondominated Sorting Approach, Part I: Solving Problems With Box Constraints[J].IEEE Transactions on Evolutionary Computation, 2014, 18(4):577-601.

[10] Deb K , Pratap A , Agarwal S ,et al. A fast and elitist multiobjective genetic algorithm: NSGA-II [J]. IEEE Transactions on Evolutionary Computation, 2002, 6(2):182-197.

[11] Bader, Johannes, and Eckart Zitzler. “HypE: An Algorithm for Fast Hypervolume-Based Many-Objective Optimization.” Evolutionary computation 19.1 (2011): 45–76.

[作者简介]

魏俊杰（2002-），男，硕士生，从事生产计划与调度、智能算法等研究；曹旺（1995-），男，博士生，从事智能制造、鲁棒优化等研究；王庆（1969−），男，副教授，博士，从事系统建模与优化、供应链与 ERP 系统等研究；黄敏（1968-），女， 教授，博士生导师，从事物流与供应链管理、智能算法设计与优化、调度理论与方法等研究；

智能配电网不平衡问题的主动定位与调控恢复

李一泓，潘宜城，马萌，王平

摘　要：本文提出了一套面向配电网的三相不平衡定位与主动闭环调控的方法——PowerCause，能够面向配电网的时间序列指标数据，自动检测异常区间，并基于格兰杰因果关系检验进行异常定位，生成潜在的根因总线列表。此外，PowerCause 能够对特定总线采取调控措施，以缓解异常带来的影响，实现了异常从发生到消除的完整闭环。仿真结果表明，PowerCause 在根因定位精度和时间效率等各方面具有竞争力，并且对测量噪声、数据丢失误差等环境影响具有较好的鲁棒性。

关键词：配电网；不平衡定位；根因分析；主动调控

Active location and recovery of unbalance problems in smart distribution networks

Yihong Li, Yicheng Pan, Meng Ma, Ping Wang

Abstract: This paper proposes PowerCause, a method for three-phase unbalance location and active closed-loop control for distribution networks. It can automatically detect abnormal intervals based on the time series indicator data of the distribution network, locate unbalance based on Granger causality test, and generate a list of potential root cause buses. In addition, PowerCause can also take regulation measures on specific buses to alleviate the impact of unbalance, which realizes a complete closed loop from occurrence to elimination of unbalance. Simulation results show that PowerCause is competitive in terms of root cause location accuracy and time efficiency, and is robust to environmental influences such as measurement noise and data loss errors.

Key words: distribution system, unbalance positioning, root cause analysis, active regulation

1　引言

近年来，配电网及其相关技术蓬勃发展[1]。三相不平衡是配电网最常见的问题现象之一[2]，并广泛存在于中国、欧美等国家和地区[3]。随时间变化的负载水平可能会导致配电网不平衡[4]，而即便配电网的三个相位在最初构建网络时是平衡的，随着时间的推移，随着每个相位添加和移除负载，相位之间的不平衡也会出现并累积[3]。

配电网中的三相不平衡将会增加线路[5]和配电变压器[6]的电能损耗。在该状况下供电，不仅容易造成电压高的一相的用电设备烧坏，也可能使得电压低的一相的用电设备无法使用。因此三相配电网不平衡运行时，电力系统的电能质量和用电安全将受到严重影响。

本文首次将配电网的不平衡定位与时间序列上的因果分析结合起来，提出了一种智能配电网的相位不平衡定位与主动调控的方法——PowerCause。该方法能够自动进行异常区间检测，并基于格兰杰因果检验进行不平衡的定位，回溯搜索并生成潜在的根因总线的列表，随后对特定总线采取调控措施，以缓解不平

基金项目：国家自然科学基金 (92167104, 62072006); 启元实验室创新基金 (S20210201079); 双湖实验室基金项目 (2024JK15)
第一作者：李一泓(1999-)，男，北京大学硕士研究生，研究方向复杂网络系统异常诊断方法。E-mail: liyihong@stu.pku.edu.cn

衡带来的影响。这实现了配电网中的相位不平衡从发生到定位到主动调控的完整闭环。

此外，本文基于 OpenDSS 搭建了一套智能配电网异常仿真与主动调控系统。这套系统能够实现自主可控的不平衡注入，采集包括电压、相位角在内的各个维度的指标，并且带有因果分析、主动异常调控模块，以供方法验证。当它检测到的由各个相位之间的电压不平衡引起异常时，它有能力以更高的准确率定位不平衡的根因所在的总线，其中的主动调控模块能够帮助配电系统脱离异常状态，提供了从异常中进行自恢复的能力，有力地提高了电力系统的稳定性和可用性。

在 IEEE 123 Node Test Feeder[7]等基准模型上的验证结果表明，PowerCause 明显优于其他方法，具有更高的不平衡定位精度和更少的计算时间开销。此外，它不需要模型预训练的过程，也不需要将物理拓扑结构作为输入，具备良好的时间效率，并对环境影响具备鲁棒性。

目前在配电网异常分析的研究主要有：

- 在不平衡的分析与研究方面，参考文献[8]建立了工业园区配电网综合负荷模型，通过混沌粒子群优化算法对模型进行了完整的参数辨识；文献[9]提出了一种针对不平衡配电系统的混合补偿故障分析方法，该方法可以为故障获取合适的边界条件，从而解决各种类型的单一或同时发生的故障；
- 在不平衡的识别与定位方面，参考文献[10]提出了一种从馈线有功功率测量得出的新不平衡指数、一种不平衡贡献定位算法以及一种根因分析算法；参考文献[1]提出了一种通过比较测点处系统侧和负载侧的三相不平衡电压贡献水平来区分主要三相不平衡源位置的方法；
- 在配电网的再平衡方面，参考文献[11]通过不平衡交流最优潮流框架重点研究配电系统的最优网络重构问题；参考文献[4]提出了一种用于配电变压器组与具有径向结构的特定主馈线之间的相位重排以及沿具有径向结构的馈线的动态相位和负载平衡的技术；参考文献[12]设计了一种用于低压配电网的住宅负荷转移装置，可以通过改变负荷的连接相位来处理三相不平衡问题。

然而，上述工作需要相对完备的电压、功率与位置数据，侧重于配电网在构建时的最优，而不是在运行时的最优，并且没有将不平衡的定位与再平衡结合起来，形成一个完整的闭环。

目前在时序因果发现的研究主要有：

- 皮尔逊相关系数[13]是一种衡量两个变量之间强度和方向的经典的统计指标；
- 格兰杰因果关系[14]是依赖于使用过去某些时点上所有信息的最佳最小二乘预测的方差，它是一种是基于时间序列研究因果关系的经典方法；
- NetMedic[15]基于一种直观的技术，使用两个组件过去的联合行为模式来估计它们现在的相互影响程度；
- TBAC[16]基于系统的架构依赖图和解决错误传播的规则集来计算组件异常分数。

现有的时序因果发现方法大多依赖物理上的拓扑结构，考虑的因果关系更静态，而不是动态；且随着网络结构的增大，这些方法的适应能力会出现明显下降。本文侧重于面向大规模网络，面向不完备的时间序列数据，实现配电网的不平衡定位与主动调控。

2　方法

本章提出了配电网中从异常检测与定位到主动调控的闭环方法，其框架如图 1 所示。该方法解决了异常检测、因果分析和主动调控这三个核心问题。配电网在运行时收集时间序列总线数据，当检测到存在不平衡引发的异常时，进行因果分析，以找到不平衡的根因总线，并进行主动调控，使整个配电系统恢复到正常的工作状态。

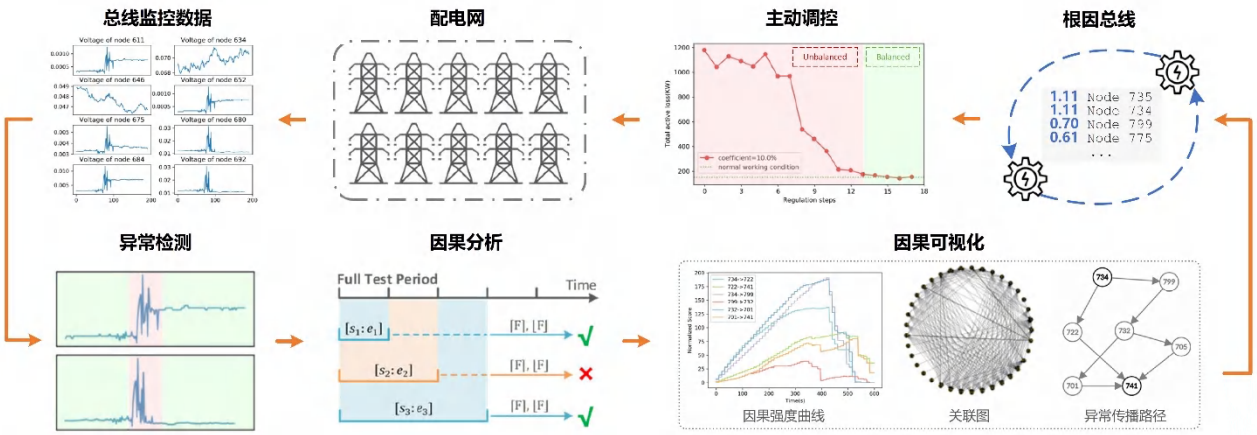


图1　PowerCause框架图

2.1　问题定义

针对不平衡定位任务，假设能够从配电网中获取到定位所需的所有指标，那么每个总线都有多个指标的指标测量值。这些指标测量值可以被视为输入数据，记作$(data_1, data_2, \ldots, data_M) \in \mathbb{R}^M$，其中$M$是输入维度的个数。因此，包含了各种指标测量值的数据样本可以用矩阵$\mathbf{X} \in \mathbb{R}^{N\times M}$表示，其中$N$代表受监控总线的数量。在这种情况下，异常定位问题就可以被转化为一个分类任务。具体来说，给定一个数据样本矩阵$\mathbf{X}_i$，不平衡总线$\hat{r}_i$由$\hat{r}_i = f(\mathbf{X}_i)$映射得到，其中$f$表示对不平衡总线进行分类的具体方法。如果$\hat{r}_i = r_i$，那么就可以准确地定位到引起配电网不平衡的总线，其中r_i表示与$\mathbf{X}_i$相关的不平衡真实根因总线。

针对异常调控任务，假设调控模块可以从配电网中收集正常运行条件下的总系统损耗$loss_N$和当前系统总损耗$loss_C$。基于定位任务中确定的$\hat{r}_i$列表执行异常调控。具体而言，异常调控应针对$\hat{r}_i = r_i$，并将目标总线的功率降低到合适的范围，使得$loss_C$减小，从而得到合理的调控效果。

2.1　异常检测

PowerCause 使用 SPOT 算法[17]作为其初步异常检测器。对于配电网的时间序列监控数据中的每个时间戳，该算法根据过去数据的极值分布生成一个阈值，若当前时间戳的监控值高于高阈值或低于低阈值，则视为异常。随后，统计每个总线中检测到的异常值的数量，一旦统计数据超过预定义的阈值，就会启动诊断。值得注意的是，PowerCause 仅考虑异常间隔内的指标，并丢弃正常数据。

2.2　因果分析

PowerCause 通过扩展传统的格兰杰因果关系检验[14]来发现异常因果关系的时间动态。形式上，总线i和j的度量序列表示为x_i和x_j。通过格兰杰因果关系检验，构建两个用于预测过去观测值的线性回归模型

（部分模型$\mathcal{M}_{part}$和完全模型$\mathcal{M}_{full}$）来预测$x_j(t), t = 1,2,\cdots T$，其中T为时间序列长度。完全模型$\mathcal{M}_{full}$包含更多独立变量$x_i^{(t-l)}, 1 \le l \le Lag$，表示来自总线$i$的附加信息。

$$\mathcal{M}_{part}: \hat{x}_j^{(t)} = \sum_{l=1}^{L_{lag}} \alpha_l^{part} x_j^{(t-l)} + b^{part}$$

$$\mathcal{M}_{full}: \hat{x}_j^{(t)} = \sum_{l=1}^{L_{lag}} \left(\alpha_l^{full} x_j^{(t-l)} + \beta_l^{full} x_i^{(t-l)}\right) + b^{full}$$

这里，$\hat{x}_j^{(t)}$表示预测值，α_l^{part}、b^{part}、α_l^{full}、β_l^{full}和b^{full}是模型参数。通过计算两个模型的误差平方和(SSE_{part}, SSE_{full})，计算公式为$\sum_t(\hat{x}_j^{(t)} - x_j^{(t)})^2$，可以使用 F 分布检验原假设。如果不能拒绝零假设，则意味着这些额外信息无法帮助预测。换句话说，x_i对x_j没有因果影响。因此，可以计算：

$$F = \frac{(SSE_{part} - SSE_{full})/(d_{full} - d_{part})}{SSE_{full}/(T - d_{full} - 1)}$$

这里，SSE_{part}和SSE_{full}分别表示部分模型和全部模型的误差平方和，d_{full}和d_{part}是两个模型的自由度，分别为L_{lag}、$2L_{lag}$，T是时间序列中的样本总数。当F小于给定的阈值α时，零假设不成立，即x_i和x_j之间不存在着格兰杰因果关系。反之，当F大于阈值α时，则可以认为总线i的时间序列x_i对总线j的时间序列x_j存在格兰杰因果关联。阈值α一般取 0.05 或 0.1。

上述过程对每个总线对之间是否存在因果关系进行了检验。然而，因果关系通常动态变化的。因此，采用了枚举滑动窗口的方法$\{[s_q: e_q] | 0 \le s_q \le e_q \le T\}$来进行格兰杰因果检验，而不再仅限于单一的时间窗口$[0, T]$，可以更全面地捕捉因果关系的变化规律，从而更准确地理解总线之间的动态影响关系。如图 2 所示，PowerCause 从配电网的时序数据计算动态因果强度曲线$C_{i,j}$，这些曲线反映了从x_i到x_j的相关性随时间变化的强度。

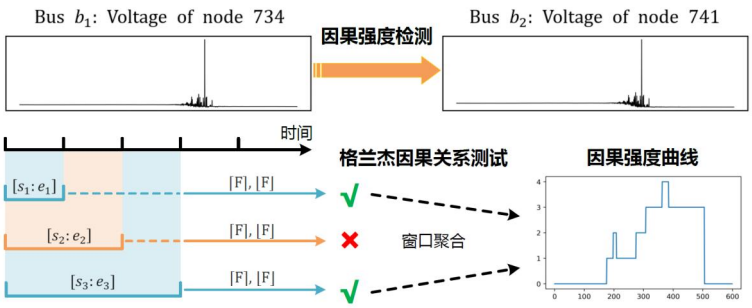


图2　动态因果强度曲线构建示例

形式上，可以使用有向加权图$G(V, E, W)$来表示配电系统，其中V是总线的集合，E是总线间相关性的集合，W是相关性强度的集合。PowerCause 将曲线上的因果强度信息统计成总线相关图，提供高度可解释的系统异常诊断和传播路径可视化。首先通过聚合因果曲线来估计总线b_i到各个总线b_j的关联关系强度。随后计算这组总线的自适应阈值τ_i，用于决定哪些总线之间的关联关系强度足够强，以形成总线相关边和边强度。最后，对权重矩阵W进行列归一化处理，并在每个时间步骤输出总线相关图，如图 3 所示。其中，

条形图的高度代表总线间的相关性强度，红线表示阈值，用于区分总线间关系的显著与否，圆圈上的每个节点代表一个总线，圆圈之间连接边的粗细与相关性的强度成正比。

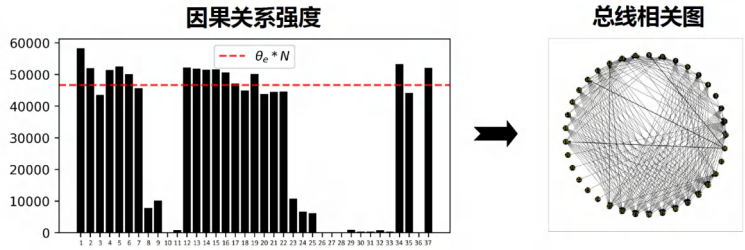


图3　总线相关图构建示例

2.3　回溯根因分析

PowerCause 在总线相关图上回溯根因分析，以确定三相不平衡是如何从根因总线传播到每条受影响的总线的。在此期间，同时考虑自异常总线的路径相关强度和皮尔逊相关系数这两个方面的信息来及计算异常得分。随后统计总线出现的概率排名，按照异常分数从高到低输出候选的根因列表。它还可以输出可能的异常传播路径，这些路径反映了异常扩散时途经的总线。为了避免搜索循环，每个路径中每个总线最多出现一次。

通过以上三个步骤，发生不平衡的配电网各相位的时间序列输入数据被转化为可能的根因总线的排名，这为异常调控提供了必要条件。对于总线数量较多的配电网，可以将其划分为多个区域，对每个区域分别进行因果分析，汇总得到最终结果，提高根因定位的准确率。图 4 展示了由 PowerCause 计算的 IEEE 37 Node Test Feeder[7]的几个典型的因果强度曲线和传播路径，其中一个节点代表一条总线，$C_{i,j}$通过除以其曲线下面积来归一化。该图揭示了根因总线 734 通过影响不同的总线，形成了三条传播路径，最终异常汇入总线 741。

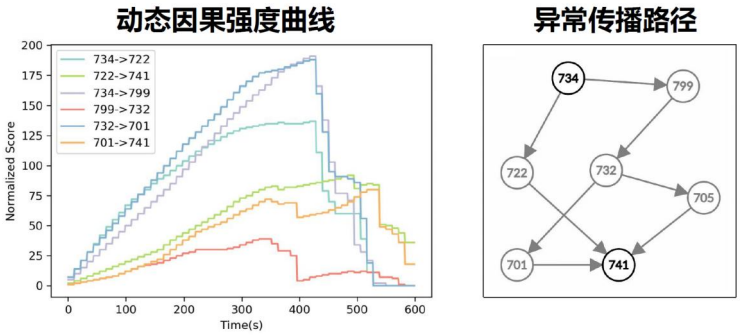


图3　因果强度曲线和异常传播路径生成示例

2.4　主动异常调控

主动异常调控旨在缓解配电网中已发生的不平衡给整个系统带来的影响。实践中，对各种性能指标的监控贯穿了配电系统运行的全过程，以验证调控过程的有效性，进而使 PowerCause 得以闭环。PowerCause 通过逐步降低特定总线的负载来消除不平衡的根源。众多研究表明，当配电网发生三相不平衡引起的异常时，总线电压将发生明显变化，这伴随着系统可用性和安全性的下降。配电网在正常运行时或不平衡被正

确消除时，总线电压只在正常范围内轻微波动，且二者的波动曲线基本吻合。因此，可以通过比较调控前后的电压波动来判断调控方案是否有效。

在理想情况下，异常调控的对象是真实的根因总线，无论该总线有多少异常负载，都应得到有效控制。如果在异常调控阶段对该总线降低的负载不足，那么整个系统将仍然处于不平衡状态；如果对该总线降低的负载过多，虽然与之对应的电压波动曲线与不平衡被正确消除时基本吻合，但会以降低整个系统的输电能力作为代价，产生一定的副作用。因此，PowerCause 将“不多不少”作为其调控原则。

对配电网进行异常调控，该阶段的输入是不平衡定位的根因列表、当前配电网在正常工况下的系统总损耗$loss_N$，以及损耗变化阈值T。T是一个百分数，其典型值为 1%。根据因果分析得到的N个根因总线和它们的排名，依次对各个可能的总线实施异常调控，具体实施方式为每次降低 1%的负载。如果调控的总线正确，整个配电网的损耗$loss_C$会随着时间步的增加而大幅下降，最后维持在正常损耗范围内；如果调控的总线错误，整个配电网的损耗将不会有明显的变化。根据上述特征，异常调控阶段对每个总线尝试调控 3 个时间步后，若系统当前总损耗$loss_C$没有出现明显下降，则认为当前总线不是实际的根因总线，它将从根因排名中选取下一个总线，继续尝试异常调控；若系统总损耗已经出现明显下降，则当总损耗$loss_C$近似于正常工况时的值$loss_N$，并且两者相差不超过阈值T时，异常调控成功结束。

3 验证

3.1 环境设置

为了验证 PowerCause，本文设计并实现了一套智能配电网异常仿真与主动调控环境。配电网的功能基于 OpenDSS[18]实现。在此基础上，验证环境由以下 4 个闭环模块构成：

- **配电网仿真平台**：同时扮演工作集群与集群管理器的角色，能够生成各总线电压、相位角等多维时间序列，并存储于配电网性能数据库中；
- **配电网性能数据库**：用于存储各个总线在运行中的电压和相位角等指标数据，具备数据预处理能力，能够实现同维度指标的自动汇总和无关数据的自动剔除，并供配电网性能预测与异常分类器和配电网因果分析器调用；
- **配电网因果分析器**：是对 PowerCause 的不平衡定位方法的应用，基于因果关系实现对不平衡根因总线的动态定位，并深入揭示异常的传播过程；
- **配电网主动调控器**：是对 PowerCause 的主动调控方法的应用，可以逐步、稳定地调控已识别的根因总线，以主动减轻异常带来的影响。

3.2 验证数据生成

在 IEEE 13 Node Test Feeder、IEEE 37 Node Test Feeder 和 IEEE 123 Node Test Feeder[7]三个测试馈线上注入不平衡、定位不平衡根因，并进行主动调控。这些测试系统的规模从 16 到 132 个总线不等，其实现细节如表 1 所示。

表1　配电网测试馈线实施细节

IEEE Test Cases	13bus	37bus	123bus
电压(V)	[115,4.16,0.48]	[230,4.8,0.48]	[115,4.16,0.48]
基准频率(Hz)	60	60	60
总线个数	13	37	123
总负载(MW)	0.02	2.59	3.62
采样间隔(s)	1	1	1

总线的监控数据以时间步为单位，一个时间步的长度可以是 1 秒到若干天。采集的数据包括总线级、线路级和系统级。总线级数据包括各总线的电压、相位角；线路级数据包括各线路的电流、相位角、有功损耗、无功损耗等；系统级数据是线路、变压器等所有功率传输部件的损耗。数据采集维度最高可达10^4，支持添加高斯噪声、随机数据损耗等。

通过改变负载来手动注入不平衡，生成所需的异常数据集。在实践中，需要使各负载的有功功率和无功功率在波动过程中服从正态分布，其中正常工作负载的平均功率为负载的标称功率，异常工作负载的平均功率为负载标称功率的e倍负载的功率升压系数。它们功率的标准差是标称功率的四分之一。

随机选取总线的一个或多个相位进行不平衡注入，不平衡总线的功率提升系数e被设为正常功率的1%到30%，而其他总线则在正常功率上下波动。所有总线的功率均满足正态分布，采样间隔设置为 1 秒。我们从总线上获取以 p.u.（per unit）为单位的电压。对于每一个测试馈线，均选择五个最具代表性的数据集进行实验，数据集示例如图 4 所示。

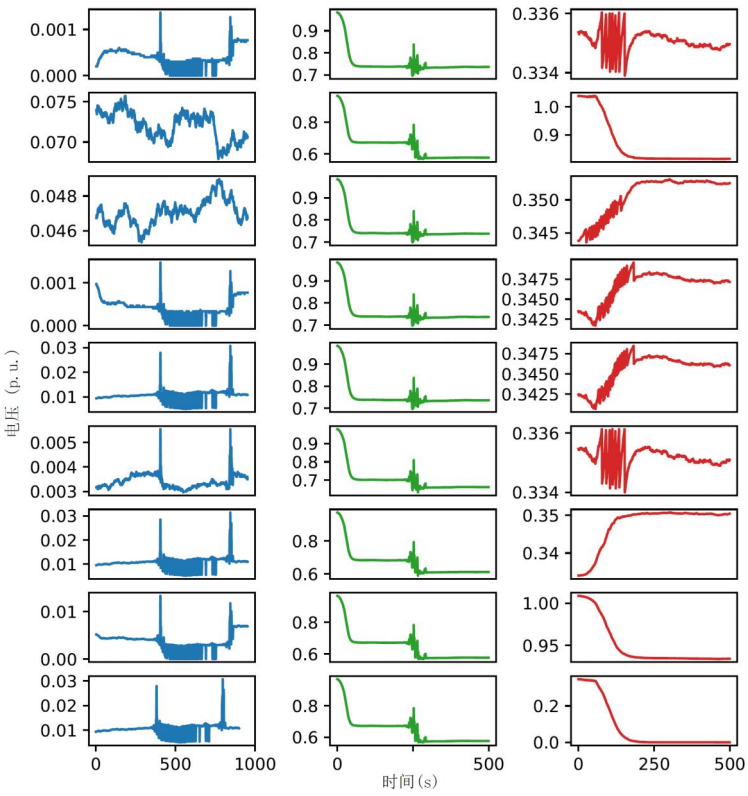


图4　配电网具有代表性的异常数据集

3.3 评估指标

使用 RankScore 来评估根因分析的排名表现，如下式所示。其中，$\mathrm{rank}\,(\mathrm{v_r})$是总线$\mathrm{v_r}$在预测根因列表中的排名，它的范围是1到$N$。RankScore 扩展了 FacGraph[19]和 TBAC[16]中提出的简单形式，以支持定位多个根因。RankScore 计算每个真实根因总线的排名的平均值，特别地，如果配电网络中存在m个根因，当预测的根因总线$\mathrm{v_r}$在前m名时，其$\mathrm{rank}\,(\mathrm{v_r})$将为 1.0，并随其位置的下降而线性下降，当其位置接近最后时减小到 0。当所有m个根因总线均位于预测根因列表中的前m名时，RankScore 将为100%。这里，$\mathrm{R^{true}}$ 是真实根因总线的集合，$\mathrm{R^{pred}}$ 是预测的根因列表。

$$\mathrm{RankScore} = \frac{1}{|\mathrm{R^{true}}|}\sum_{\mathrm{v_r}\in \mathrm{R^{true}}} \mathrm{s}(\mathrm{v_r})$$

$$\text{where } \mathrm{s}(\mathrm{v_r}) = \begin{cases} \dfrac{\mathrm{N} - \max(0, \mathrm{rank}\,(\mathrm{v_r}) - |\,\mathrm{R^{true}}\,|)}{\mathrm{N}} & \text{if } \mathrm{v_r} \in \mathrm{R^{pred}} \\ 0 & \text{otherwise} \end{cases}$$

PowerCause 旨在准确稳定地调控配电网不平衡。为此，通过比较异常调控前后的总损耗来衡量调控的准确率，用尝试调控的总线数量和尝试调控的时间步数来衡量调控的效率。其中理想情况是只尝试一个总线就找到了真实的根因，而尝试步数与功率提升系数呈现正相关。对异常的调控也可能给配电网带来副作用，可以用调控准确率与 100%的差值的绝对值来衡量调控的代价。

异常调控精度和成本的计算方法如下式所示，其中$Loss$和$Loss'$分别为调控前和调控完成后的配电网总损耗。$Loss_{normal}$是配电网正常运行时的总损耗，该值在配电网的运行过程中基本不变。

$$Acc_r = 100\% - \left|\frac{Loss' - Loss}{Loss - Loss_{normal}} + 1\right|$$

$$Cost_r = |\,1 - Acc_r\,|$$

3.4 不平衡定位性能

本研究选取了若干基准方法用于对比验证，包括 Pearson 相关系数[13]、NetMedic[15]和 TBAC[16]，使用前文提到的 RankScore 和根因定位计算开销来进行性能评估。所有实验都是在相同的数据集和相同的计算平台环境中实现的，装备有 AMD Ryzen 7 PRO 4750U 处理器和 16GB RAM。不同方法的定位精度如表 2 所示，时间开销如表 3 所示，其中分别报告了未经预处理和预处理后所得到的结果。值得注意的是，预处理只有初次定位需要，之后的定位则不需要。

表2 配电网不平衡定位精度

方法	13 bus	37 bus	123 bus
NetMedic	69.23%	94.60%	60.48%
TBAC	84.62%	87.84%	95.16%
Pearson	71.79%	39.19%	16.13%
PowerCause	**94.87%**	**98.65%**	**99.19%**

随着配电网的结构变得复杂，相互影响、相互耦合的总线变多，不平衡定位变得更加困难，皮尔逊相关系数的定位表现随着配电网规模增大而大幅降低。NetMedic的定位准确率也不稳定，且它的时间开

销是其他方法的数倍，随着电网拓扑结构变得复杂，它的时间开销与其他方法的时间开销的比值也变得越大。TBAC在具备更优的时间性能，尤其是在小规模配电网中，但它的定位准确率仍低于PowerCause。因此可以得出结论，PowerCause在性能和计算开销的综合性能优于其他方法。

表3　配电网不平衡定位时间开销

方法	13 bus	37 bus	123 bus
NetMedic	23.0177/0.1121	310.6581/0.2806	7786.4256/2.0682
TBAC	13.5276/0.0724	115.4552/0.2041	1251.4389/1.5440
Pearson	0.0146	0.1099	0.9455
PowerCause	**24.0810/0.4127**	**138.4822/1.1285**	**884.8850/6.8536**

3.5　主动调控性能

调控效率的高低取决于真实根因的总线在根因排名的先后。表 4 展示的是在三张配电网中，不平衡在不同的相位注入，功率提升系数也不同的情况下的主动调控性能。PowerCause 的异常调控成功率不低于 96%，调控过程中尝试的总线数量一般不大于总线总数的四分之一，调控给配电网带来的代价不大于 4%。

表4　配电网主动调控性能

目标电网	13 bus	37 bus	123 bus
注入总线	646	734	65
注入相位	abc	c	a
功率提升系数	5.00%	2.00%	3.00%
调控尝试总线数	2	2	14
调控尝试时间步	9	7	43
调控准确率Acc_r	99.32%	97.60%	96.74%
调控开销$Cost_r$	0.68%	2.40%	3.26%

图 5 展现了 IEEE 37 Node Test Feeder 的一个典型调控过程，其中配电网正常工作时的平均总损耗为 152.16KW。第 0 个时间步是不平衡发生之时，第 1 到 3 个时间步和第 4 到 6 个时间步分别是第一次和第二次调控的尝试，期间电网的总损耗均未发生显著的下降。从第 7 个时间步开始，主动调控器尝试的总线是真实的根因总线，电网的总损耗大幅下降，并最终被调控到正常工作时的平均损耗附近，主动调控器在合计尝试了 3 个总线和 17 个步时间，成功完成了它的任务。

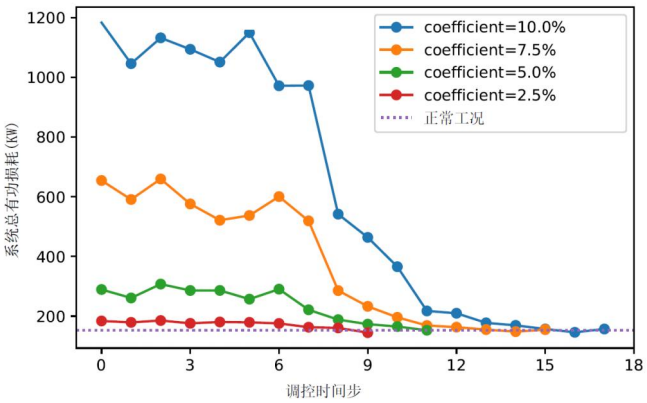


图5　IEEE 37 Node Test Feeder典型异常调控过程图

3.6 有效性验证

为了验证PowerCause应对测量噪声的有效性，在测量中添加噪声进行实验和分析。在真实环境中，噪声是由传感器、量化和信号处理中的误差引起的，无论电压电平和测量参数如何，这些误差都保持相似。并且对于所有的PMU（Phasor Measurement Unit，相量测量单元）的数据来说，45dB的SNR（信噪比）可能是一个很好的近似值[20]。

除此之外，还模拟了一系列的数据丢失的场景，包括丢失部分总线的全部测量数据、丢失部分总线的部分相位的全部测量数据、随机丢失部分采样点的数据。数据丢失的比例均不超过20%。值得注意的是，真实根因的总线的测量数据不在第一种情况下丢失，以免数据中不存在真实的根因总线以供结果分析。

表5展示了正常采样、包含噪声采样和包含数据丢失的采样的各种情况在IEEE 13 Node Test Feeder中的异常定位性能表现。用于对比的其他方法在总线和相位的部分数据丢失的情况下的异常定位准确度出现了不降反升的现象，可能的原因是与真实根因总线无关的采样数据减少了，也就帮助提高了定位精度。

表5 PowerCause应对噪声和数据丢失的性能表现

方法	None	Noise	Bus	Phase	Random
NetMedic	69.23%	64.10%	79.26%	74.36%	51.28%
TBAC	89.74%	84.61%	80.65%	89.74%	74.36%
Pearson	71.79%	69.23%	81.82%	64.57%	62.70%
PowerCause	**97.44%**	**92.31%**	**93.94%**	**92.31%**	**92.31%**

在添加了高斯噪声的测量数据中，各个方法的准确度均出现了下降，但PowerCause的准确度仍旧表现出强大的竞争力，在数据丢失的情况下也是如此。在各种测量修改的情况下，PowerCause的定位准确度均不低于90%，有力地验证了它的有效性。

3.7 态势熵连续分析

态势熵反映的是复杂网络中各种因素的不确定性和变化趋势。PowerCause通过总线相关图对当前配电网的态势熵进行建模。在运行过程中，PowerCause持续构建各总线之间的相关图，对配电网拓扑结构的态势熵进行连续分析，从而实现异常态势根因溯源、异常态势自主调控等功能。

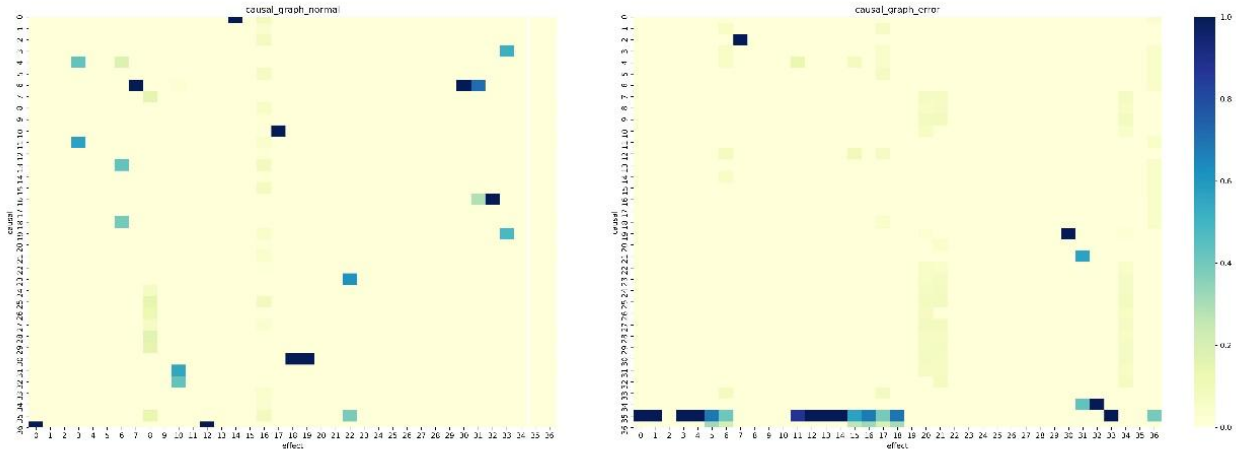


图6 配电网动态总线相关图

在正常工况、异常工况随机抽取一幅各总线的相关图，如图6所示。其中每个方格表示横坐标总线对纵坐标总线的影响，图中颜色越深，表示影响程度越高。在左图的正常工况下，图中没有呈现明显的异常影响关系；而在右图的异常工况下，注入异常的35号总线影响到了大量的其他总线，且受影响的程度也较大，因此该总线所在的一行出现了较多的深色值。从该图可以看出，从正常工况到异常工况，配电网的各总线之间的相互影响发生了变化，即态势熵在动态变化。

4　总结与展望

本文提出了面向配电网的三相不平衡定位与主动闭环调控的方法——PowerCause，并搭建了闭环验证环境。实验结果表明，不平衡定位准确率超过90%，主动调控成功率超过95%，系统开销不超过5%。本文通过深入的实验，验证了PowerCause在定位性能和计算开销等方面与其他方法具有竞争力，并对测量噪声和数据丢失误差具有很强的鲁棒性。PowerCause实现了配电网的三相不平衡异常从发生到定位再到主动调控的完整闭环，这大大提高了电力系统的态势感知能力。

在将来，PowerCause将支持多点异常调控、提供更强大的结构自适应能力，着眼于设计和实现更加智能化和高效性能的不平衡预测方法以及相应的故障调控模块，以实现配电网异常发生前的主动干预。

参考文献：

[1] Bairami S, Salimi M, Mirabbasi D. A novel method for maximum power point tracking of the grid-connected three-phase solar systems based on the PV current prediction[J]. Chinese Journal of Electronics, 2023, 32(2): 353-364.

[2] Yue L, Xu K, Sun J, et al. Research on the Source Tracing Method of Three-Phase Unbalance Based on Equivalent Circuit[C]//2023 International Seminar on Computer Science and Engineering Technology (SCSET). IEEE, 2023: 687-689.

[3] Ma K, Fang L, Kong W. Review of distribution network phase unbalance: Scale, causes, consequences, solutions, and future research directions[J]. CSEE Journal of Power and Energy systems, 2020, 6(3): 479-488.

[4] Siti M W, Nicolae D V, Jimoh A A, et al. Reconfiguration and load balancing in the LV and MV distribution networks for optimal performance[J]. IEEE transactions on power delivery, 2007, 22(4): 2534-2540.

LI Q, WANG H, WANG L C. Research of P2P based distributed network management[J]. Computer Engineering, 2006, 32(13): 1-13.

[5] L. F. Ochoa, et al., “Evaluation of distribution system losses due to load unbalance,” in 15th Power Systems Computation Conference (PSCC’05), Power Systems Computation Conference (PSCC), 2005.

[6] R. Salustiano, et al., “The unbalanced load cost on transformer losses at a distribution system,” in 22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013), IET, 2013, pp. 1–3.

[7] Kersting W H. Radial distribution test feeders[C]//2001 IEEE Power Engineering Society Winter Meeting.

Conference Proceedings (Cat. No. 01CH37194). IEEE, 2001, 2: 908-912.

[8] Wang T, Yan X, Zhang Y. Research on Modeling and Parameter Identification of Comprehensive Load Model of Distribution Network in Industrial Park[J]. Chinese Journal of Electronics, 2024, 33(1): 264-273.

[9] Lin W M, Ou T C. Unbalanced distribution network fault analysis with hybrid compensation[J]. IET generation, transmission & distribution, 2011, 5(1): 92-100.

[10] Singh U, Solomon R, Alizadeh-Mousavi O. Monitoring-Based Localization of Unbalances and Root Cause Analysis in Low-Voltage Distribution Systems[J]. IEEE Systems Journal, 2023, 17(3): 4177-4188.

[11] Liu Y, Li J, Wu L. Coordinated optimal network reconfiguration and voltage regulator/DER control for unbalanced distribution systems[J]. IEEE Transactions on Smart Grid, 2018, 10(3): 2912-2922.

[12] Bao G, Ke S. Load transfer device for solving a three-phase unbalance problem under a low-voltage distribution network[J]. Energies, 2019, 12(15): 2842.

[13] Pearson K. VII. Mathematical contributions to the theory of evolution.—III. Regression, heredity, and panmixia[J]. Philosophical Transactions of the Royal Society of London. Series A, containing papers of a mathematical or physical character, 1896 (187): 253-318.

[14] Granger C W J. Investigating causal relations by econometric models and cross-spectral methods[J]. Econometrica: journal of the Econometric Society, 1969: 424-438.

[15] Srikanth K. Detailed diagnosis in enterprise networks[J]. Sigcomm, August 2009, Barcelona, Spain, 2009.

[16] Marwede N, Rohr M, van Hoorn A, et al. Automatic failure diagnosis support in distributed large-scale software systems based on timing behavior anomaly correlation[C]//2009 13th European Conference on Software Maintenance and Reengineering. IEEE, 2009: 47-58.

[17] Siffer A, Fouque P A, Termier A, et al. Anomaly detection in streams with extreme value theory[C]//Proceedings of the 23rd ACM SIGKDD international conference on knowledge discovery and data mining. 2017: 1067-1075.

[18] R. C. Dugan and T. E. McDermott, “An open source platform for collaborating on smart grid research,” in 2011 IEEE power and energy society general meeting, IEEE, 2011, pp. 1–7.

[19] Lin W, Ma M, Pan D, et al. FacGraph: Frequent anomaly correlation graph mining for root cause diagnose in micro-service architecture[C]//2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC). IEEE, 2018: 1-8.

[20] Brown M, Biswal M, Brahma S, et al. Characterizing and quantifying noise in PMU data[C]//2016 IEEE Power and Energy Society General Meeting (PESGM). IEEE, 2016: 1-5.

[作者简介]

李一泓（1999—），男，于 2024 年获得北京大学软件工程硕士学位，研究兴趣包括微服务、配电网等复杂网络系统中的故障模拟和数据驱动的异常诊断方法。邮箱：liyihong@stu.pku.edu.cn

潘宜城（1997—），男，于 2024 年获得北京大学计算机科学与技术博士学位，研究兴趣包括网络服务系统故障分析诊断、复杂系统动态因果分析等。邮箱：aqpyc@pku.edu.cn

马萌（1986—），男，北京大学副研究员，研究兴趣包括态势表征计算、网络服务系统故障分析诊断、智能交通系统分析等。邮箱：mameng@pku.edu.cn

王平（1961—），男，北京大学教授，研究兴趣包括信息安全与隐私保护、智能计算与感知、大数据计算与人工智能。邮箱：pwang@pku.edu.cn

工业互联网 AI 安全的挑战与发展趋势

周晓茂[1]，贾庆民[1]，胡玉姣[1]，谢人超[1,2]，

（1. 紫金山实验室，江苏，南京 211111；

2. 北京邮电大学，北京 100876）

摘　要：AI 是开启网络应用新范式的关键技术，在赋能工业互联网的同时，也带来了前所未有的安全风险。本文在介绍 AI 技术使能工业互联网自动化和智能化的基础上，分析了 AI 在工业互联网应用中因技术局限性、人为滥用等带来的安全风险，分别从数据层面、模型层面、算法层面、以及应用层面来对工业互联网 AI 安全进行了分类和阐述，详细分析了相关的风险内容和产生原因，并从上述几个维度对工业互联网 AI 安全的应对策略进行介绍，重点突出“AI 安全风险源于 AI，也将终于 AI”的思想，最后，总结了工业互联网 AI 安全的发展趋势与建议。

关键词：工业互联网；AI 安全；数据安全；应用安全

Challenges and Development Trends of Industrial Network Convergence AI Security

Zhou Xiaomao[1], JIA Qingmin[1], HU Yujiao[1], XIE Renchao[1,2]

1. Purple Mountain Laboratories, Nanjing, 211111, China

2. Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: Artificial Intelligence (AI) is the key technology to open a new application paradigm of Industrial Networks. While enabling computing network, it also brings unprecedented security risks and security challenges. On the basis of introducing the automation and intelligence of IoT enabled by AI technology, this paper analyzes the security risks brought by the technical limitations and human abuse of AI in the application of Industrial Networks, and classifies and expounds the security of computing network AI from the data level, model level, algorithm level and application level, respectively. The relevant risk content and causes are analyzed in detail, and the copying strategies of AI security are introduced from the above several perspectives, focusing on the idea that "AI security risks originate from AI and will eventually be solved by AI". Finally, the development trends and suggestions of the Industrial Network AI security are summarized.

Key words: Industrial network, AI security, data security, model security, system security, application security.

1　引言

在工业互联网推进各行业数字智能化转型过程中，随着行业应用涉及的需求逐渐多样化、系统更加复杂化，新业务、新需求、新场景的多样化多对网络服务的灵活性、自动化和智能化提出了更高的要求。为

应对上述挑战，智能化已经成为工业互联网的重要发展方向之一[1]。具体来说，通过将 AI 技术与网络的基础设施、功能流程、服务应用等深度融合，把 AI 的解决目标和承载方式都设在网络内部，利用 AI 技术赋予网络基础设施智能化、业务流程一体化、服务能力自优化、网络运维自动化等能力。AI 技术的创新突破及迅猛发展, 尤其是大模型[2]、生成式 AI[3]等技术的突破，为应对上述挑战并超越传统工业互联网设计理念与性能提供了潜在的可能性。

然而，随着 AI 在工业互联网全生命周期中的深度融合与广泛应用，安全问题也愈发凸显，需要全行业共同努力来应对和保障。一方面，当前的 AI 技术本身仍面临着可解释性、公平性、安全和隐私等方面的挑战[4]，大部分的 AI 模型算法尚未完成从感知智能到认知智能的技术突破，而且缺少预警、常识分析、逻辑推理、历史回溯等功能和保障机制，在训练和推理过程中容易受到数据、先验知识、对抗攻击等影响[5]，无法保证生成结果的可信度和可靠度。另一方面，AI 在赋能工业互联网业务流程的过程中将会赋予其自主决策、自动执行等能力，而网络系统自主性提高的同时会带来决策结果难以预测、执行过程无法控制、容易被恶意使用等问题，当系统完全具有自主学习和决策能力时，还可能会超出人类的控制范围，造成不可预见的后果。

因此，为充分发挥 AI 在工业互联网中的潜力，确保网络 AI 系统的正常运行和信息安全，保障网络 AI 的安全至关重要。当前，工业互联网 AI 安全也已经引起业界和学术界的广泛关注。本文围绕工业互联网 AI 安全的最新研究进展与发展动向，首先介绍工业互联网 AI 安全的背景和研究现状，然后阐述了工业互联网 AI 的安全挑战、潜在威胁、安全重要性等，并分析了工业互联网 AI 安全的发展趋势与解决方案，最后对工业互联网 AI 安全做出总结和呼吁。

2　工业互联网 AI 安全的风险分类

从系统实现的技术角度来看，AI 是使能工业互联网具备智能的根本途径，AI 技术本身存在的安全问题会被工业互联网 AI 安全全部继承，而由于使用 AI 技术所衍生出来的对系统的安全影响也是工业互联网 AI 所需要考虑的重要部分。具体来说，AI 技术作为一种赋能手段，存在由于设计、构建、使用环境或受到攻击而产生的风险, 这种由于自身技术特点、缺陷、脆弱性而产生的安全问题称为**“内生 AI 安全问题”**。此外，AI 技术的引入将给工业互联网注入新的技术活力，开启前所未有的可能性，而这势必会衍生出一系列涵盖技术和工程系统、社会和国家安全等各个领域的安全问题，这种（与 AI 是否正常行使特定功能无关）所产生的安全问题称为称为**“衍生 AI 安全问题”**。例如，由于 AI 系统具有学习能力、自主决策、自主行动等智能行为而产生的不受控问题；由于 AI 广泛取代人类工作从而造成部分人群思维变得懒惰、认知能力下降的社会性问题等。从安全的诱因角度来看，工业互联网 AI 安全大致可以将分为两类：一类是 AI 技术客观因素导致的安全问题，例如，由于 AI 技术的不稳定性导致的系统决策失误、由于 AI 技术的

不确定性导致的系统稳定性不足等。另一类则是人为主观因素导致的安全问题，例如，不法分子利用 AI 技术进行网络攻击和信息窃取等。

总的来说，不同领域对工业互联网 AI 的理解和着眼点不同，本节从系统服务的角度出发，按照从底向上的层次逻辑，分别从数据层面、模型层面、算法层面、以及应用层面来对工业互联网 AI 安全进行分类和阐述，并详细分析相关的风险内容和产生原因。

3 工业互联网 AI 安全的应对策略

工业互联网 AI 安全问题是工业互联网应用与发展过程中不可忽视的挑战，涉及到数据安全、模型安全、系统安全和应用安全等多个维度，需要从技术防范、安全管理和监管、法律法规、公众安全意识以及多方合作与交流等多个方面出发，共同应对这一挑战。本节分别从上述几个维度对工业互联网 AI 安全的应对策略进行介绍，重点突出“AI 安全风险源于 AI，也将终于 AI”的思想。

3.1 数据安全的应对策略

数据安全贯穿整个工业互联网 AI 安全体系，相关安全应对措施需要围绕数据全生命周期展开，不仅包括数据库防御、数据加密、数据容灾备份及安全存储等基础流程，也涵盖云存储、隐私计算、跨平台共享、数据生成等应用场景。

在数据应用的过程中，AI 作为实现数据价值转化和释放的重要手段，在带来安全风险的同时，也能够用来为数据安全治理提供底层技术支撑。对于复杂的数据安全治理问题，AI 能够显著提高数据处理能力，支持在大范围内快速地对数据进行标签分类、内容识别、相关性筛选、异常检测等，在准确率和效率方面显示出超越人类专家的数据安全治理能力。同时，AI 能够直击数据安全治理的痛点，提高数据安全治理的智能性，例如，通过关联查询、智能搜索等方法自动构建数据关联关系图谱，对数据安全风险进行智能评估、量化和预测，并支撑安全风险根因快速定位。本节就几个典型的 AI 助力数据安全措施的案例进行分析，旨在展示 AI 赋能数据安全治理的可能性。

（1）数据加密：数据加密是一种将数据从明文（未加密）转换为密文（加密）的方法，主要有非对称加密和对称加密两种方法[4]。从技术角度来说，密码系统有效性通常依赖于复杂的数学运算和算法，其核心是设计和分析密码算法以及构建安全的协议。AI 能够在大规模数据和复杂模型情况下高效执行计算，在密码安全攻防中的重要性凸显。同时，AI 可赋能密码系统所需的混沌性、随机性等属性，例如，深度学习的非线性特性和随机性可用于生成强密码、随机密钥和初始化向量，基于细胞神经网络的哈希函数构造等[32]，为密码系统的设计、强化提供新方案。在加密算法设计方面，传统的加密算法设计需要依赖密码学专家的经验和知识，需要大量的人工参与而且容易受到个体主观因素影响，难以设计出足够强大和安全的加密算法。AI 可以通过分析大量的密码学数据和算法模型，利用强大的推理和学习能力发现更加复杂和安

全的密码算法可以生成更加复杂和安全的密码算法，并可以根据实时数据和反馈来调整密码生成过程，以应对不断变化的安全威胁。

（2）隐私计算：隐私计算通过在保护数据本身不对外泄露的前提下，对数据进行分析计算，可以保障数据以“可用不可见”的方式实现数据价值的转化和释放。当前的隐私计算的主流技术路线可分为以下三类：一类是采用密码学和分布式系统，例如多方安全计算、同态加密等；另一类是采用基于硬件的可信执行环境；最后一类是以联邦学习为代表的机器学习方法，通过在多个数据源上独立训练模型，各个参与方之间交换不包含隐私信息的中间运算结果，并对这些中间结果进行联合优化，最终获得联邦学习模型。目前，联邦学习已被广泛用于金融风控、医疗诊断、智能物联网等应用场景，能够有效解决协同计算过程中的数据安全问题[5]。

（3）数据合成：数据合成通过使用 AI 算法或模型来生成模拟数据来替代现实世界中采集的真实数据。由于不存在法律约束的敏感内容和私人用户的隐私，合成数据可以在不暴露真实数据的情况下进行数据分析、模型开发和算法测试，还可以解决数据稀缺、样本不平衡等问题，从而为各种 AI 学习任务提供更多的数据资源。目前，生成对抗网络（GANs）、变分自编码器（VAEs）、扩散模型（DMs）等被广泛用于图片、文本、语音、时序数据等数据的高质量可控生成[6]。从数据的角度来看，数据合成更能从根本解决数据安全问题。然而，合成数据的使用可能涉及到法律和伦理问题，尤其是在涉及信任和透明度、知识产权和法律合规等方面。

3.2 模型安全的应对策略

作为工业互联网 AI 安全的核心，模型安全并非一个单独的问题，而是一个复杂的、体系化的，涉及多个主体和多个方面的系统工程。从模型全生命周期视角出发，模型安全涉及到模型设计、模型训练、模型部署、模型推理等各个阶段，需要确保 AI 模型的完整性、可靠性、稳定性、鲁棒性、保密性等，保证其在不同的业务场景下，即使在被攻击的情况下也能够输出正确结果和避免数据泄漏。本节将分析模型在不同生命周期阶段所面临的安全风险与业务挑战，并阐述相应的应对策略。

在模型设计阶段，尽管生物智能原型提供了很多灵感和指导，包括结构、功能等，模型还需要根据业务需求明确要解决的问题和实现方式，包括模型结构、系统框架、训练数据、评估指标等。一方面，当前对生物智能的认知水平和复现能力尚无法支撑具备更高智能能力的模型的设计，另一方面，模型的设计过程在理想情况下应该是客观中立的，然而偏见总是普遍存在的，例如，业务需求解析的用户歧视、算法设计时的个人偏好、数据采集和标注的人类偏见等，从而导致训练后的模型存在认知偏见性、输出结果有悖道德和法律等安全风险。此外，模型在设计实现过程中，由于芯片、深度学习框架、软件代码等 AI 基础设施不完善，极易存在算法后门、代码安全漏洞等问题，对模型本身的安全性产生威胁。为解决上述问题，

模型形式化检测技术，例如，黑盒、白盒测试等，通过检查模型是否存在违反指定规约或性质的风险，能够帮助发现模型中的错误、缺陷或不一致性。模型验证技术，例如，简单交叉验证、k 折交叉验证等，通过模型在未见过的数据上的表现来评估模型性能和准确性，检验模型是否达到预期的性能水平。更进一步的，模型可解释性分析通过对模型的输入、输出、中间信息的依赖关系进行分析、可视化和验证等，例如，对隐藏激活函数做可视化分析、对图形识别的显著性检测、大模型的思维链等[7]，尝试从原理上对模型的内部机制和结果进行理解，能够帮助发现潜在的安全问题，并提高模型的可信度和稳健性，从而进一步提升模型的安全性。

在模型训练阶段，模型通过使用大量的数据来对自身参数进行调整，从而学习到特征和模式并达到预期的性能水平。模型训练是 AI 应用中至关重要的一步，其质量和效果直接决定着最终模型的性能和应用效果，同时，也影响着模型是否具备应对各类恶意攻击的能力，例如数据投毒、对抗攻击等。为此，除了从训练数据的角度出发，例如，增加训练数据样本量、提高训练数据多元性、保证数据标注的公正性等，还可以对训练方式和学习机制来进行提升优化。例如，基于人类反馈的强化学习（RLHF）将人类反馈纳入奖励功能，训练模型做出更符合人类目标、愿望和需求的决策，保证模型训练结果与对人类价值观或偏好[8]。上下文学习（In-Context Learning）通过将学习置于相关环境或情境中，以促进知识的理解和应用，在自然语言处理中，能够更好地理解文本中的语义信息，并根据文本的上下文信息来纠正或调整模型中的偏见[40]。此外，通过联合先验知识和数据驱动的方式进行模型训练[9]，例如，外挂领域知识库或对领域相关内容进行额外学习，可以充分利用专家知识和大量数据的优势，提高模型的准确性、稳定性和可解释性。

在模型部署阶段，训练完成的模型需要在目标环境中完成安装配置，以便实际应用中使用。然而，部署的软硬件环境存在不可信的风险，模型在传输、存储过程中可能会受到未经授权的访问和攻击，如网络攻击、模型窃取等，需要采取措施保证模型部署环境的安全性，包括加密通信、访问控制、漏洞修复等。同时，分布式模型部署策略，例如，云边端协同的模型部署策略，会进一步地加剧上述安全风险，而且存在模型中间结果被窃取的风险。此外，模型部署的过程中需要解决模型转换、硬件适配、性能优化等问题，通常会使用算子融合、量化、剪枝、并行计算等手段，在进行上述操作过程中，模型结构和参数暴露和被窃取的风险极大，需要保证执行人员、使用工具、输出结果等的可信安全。

在模型推理阶段，模型需要对实际应用中的数据产生预测、分类或其他类型的输出，由于要与应用场景中的各种请求直接交互并产生响应，模型最容易受到各类恶意攻击，例如，通过修改输入来让 AI 模型无法对其正确识别的闪避攻击[10]、通过在正常样本上加入微小扰动来愚弄 AI 模型的对抗攻击、通过构造和设计特定的 Prompt 来绕过大语言模型的过滤策略的提示注入、通过逆向工程还原模型的架构、权重的模型知识窃取[11]等。一般来说，各类攻击方式主要通过修改模型输入来影响模型输出或根据模型输出来窃取模型信息。因此，对输入数据进行检测、过滤、去毒等，可以初步避免恶意数据被模型误信或误用。同

时，构建可信执行环境和进行模型加密可以对模型进行有效保护，但前者依赖特定可信硬件，难以支撑大规模部署，而后者通常面临较大的计算或通信开销问题，且无法保护模型结构信息。而基于混淆的模型保护方案通过对模型的计算逻辑进行加扰，例如，对模型计算图的网络结构加扰、对模型计算图的节点匿名化、对模型计算图的参数权重加扰、算子接口变换等，能够在较小的开销情况下有效保证模型运行时的机密性，同时不影响模型原本的推理结果。除了存在于技术层面，安全风险还存在于人为因素中，攻击者可能利用社会工程技术欺骗模型的操作员，从而获取模型的访问权限或敏感信息。为了预防这种风险，应加强对操作员的安全意识培训，强化身份验证和访问控制机制。

3.3 系统安全的应对策略

随着 AI 的广泛使用带来更多、更复杂的新型安全风险，传统的安全防护手段已经不能完全适用泛在计算的安全防护需求。为此，需要结合工业互联网的系统架构、功能特点和业务需求等，分析判断 AI 模型使用风险，探索内生安全能力的实现方案，以及一体化全程可信的技术路线，保障基础设施安全、业务功能安全和服务安全。具体来说，在系统设计阶段就考虑安全性，采用安全设计原则，例如最小权限原则、完整性原则、最小暴露原则等，将安全与业务同步规划建设，确保系统架构和功能设计能够最大程度地降低安全风险。在系统运行过程中，综合利用预测、检测、隔离、熔断和冗余等安全机制保证系统稳定运行和功能安全执行。例如，基于系统的历史数据、环境信息、行为模式等多种数据来源，利用 AI 技术对系统可能面临的各种风险进行预测和评估，提前采取相应的预防和控制措施，降低风险对系统的影响；建立完善的监控机制和安全审计，实时监测系统的运行状态和用户行为，及时发现异常行为并采取相应措施应对，以防止安全事件的发生和蔓延；定期对系统进行漏洞扫描和安全评估，发现和修复系统中的安全漏洞，及时更新系统和依赖组件，确保系统的安全性能够即使更新。当系统发生安全事件时，能够实现安全单点或多点可控和应急响应，包括安全事件的识别、处理和恢复措施，确保在安全事件发生时能够迅速有效地应对和处理。例如，通过容器化技术、权限控制、网络隔离等技术将 AI 系统分隔，防止模型之间或模型与外部系统之间发生干扰或冲突，可以有效降低 AI 模型运行过程中的安全风险，并保证安全影响范围可控；通过对关键业务部署多个 AI 模型，利用冗余机制来提升系统的强壮性。

3.4 应用安全的应对策略

工业互联网的应用场景广泛，并持续在更多的领域发挥越来越重要的作用，在为多元业务和应用提供服务的过程中，工业互联网要严格遵守所应用的具体场景和行业的规则标准、道德约束、法律法规等，以确保其合法、安全、可靠地运行并保护用户的利益。具体来说，工业互联网的设计和使用应当符合相应的技术标准和规范，包括技术、安全、隐私、合规等方面；工业互联网需要在不同的司法管辖区注册和运营，并遵守当地的法律法规和监管要求，确保合规运营；在用户使用工业互联网服务时，需要明确用户的权益和责任，保障用户的合法权益，防止用户受到损害。因此，需要制定和完善面向工业互联网应用的应用规

范、行业标准、法律法规等，建立工业互联网应用安全的生态体系。此外，工业互联网应用安全风险主要来源之一是人为因素，可能来自工业互联网建设者、工业互联网运营者、工业互联网使用者等多方主体。因此，需要促进安全意识的提高，使所有相关方能够更好地理解和应对安全挑战。对于行业组织和机构，可以建立自律机制，制定行业准则和道德规范，引导从业者遵守法律法规和行业标准，同时监督和约束行业内不当行为，保障用户利益和行业良性发展；对于工业互联网从业者和相关人员，可以开展合规培训和认证，提高其对法律法规和行业标准的理解和遵守能力，确保其在工业互联网应用中的合规性和专业性；对于工业互联网的用户，需要加强对其的教育和指导，提高其对工业互联网应用的理解和风险意识，同时保障其合法权益，防止受到不当侵害。

4 工业互联网 AI 安全的发展趋势与建议

随着 AI 与工业互联网的深度融合，网络安全的重要性愈加凸显，相关风险也日趋严峻，需要各方共同努力，从技术保障、法律法规、政策支持、生态体系等多方面协同保证安全，才能有效应对工业互联网安全面临的挑战，促进工业互联网的健康发展。例如，开展工业互联网 AI 安全防护技术研究，将 AI 技术作为 AI 安全治理提供底层通用技术支撑，直击工业互联网 AI 安全治理痛点；完善工业互联网 AI 安全顶层设计，制定和完善 AI 安全相关的政策法规是确保工业互联网安全稳定运行的重要举措；培养工业互联网中各方对安全的重视和关注，建立积极的安全意识文化，将安全意识融入到日常工作和生活中，成为每个人的自觉行为；构建工业互联网 AI 安全生态体系，加强 AI 安全跨界合作和信息共享，包括政府、企业和学术界等，共同应对安全挑战，形成工业互联网 AI 系统全流程、全维度的安全规范体系。

5 结束语

随着 AI 与工业互联网的深度融合以及广泛应用，工业互联网 AI 安全问题日益突出，此时具有针对性的安全研究和建设工作刻不容缓。本文首先介绍了工业互联网与 AI 深度融合的发展现状和当中凸显的安全问题如数据隐私暴露、AI 模型解释性差、系统不受控、AI 滥用等，然后针对工业互联网 AI 安全相关的数据安全、模型安全、系统安全、应用安全进行了阐述，并从上述几个维度分析了 AI 安全的风险内容和产生原因，以及给出了相应的安全应对策略，旨在协助构建完备的工业互联网 AI 安全防护体系。最后，从开展 AI 安全防护技术研究、完善 AI 安全政策法规、提升 AI 安全防护意识以及构建 AI 安全生态体系的四个角度提出对工业互联网 AI 安全未来建设方向的建议。

参考文献：

[1] 周晓茂, 贾庆民, 胡玉姣, 郭凯, 马千飘, 刘辉, 谢人超. 自智算力网络：架构、技术与展望[J]. 物联网学报, 2023, 7(4): 1-12.

ZHOU X. M, JIA Q M, HU Y J, et al. Autonomous computing and network convergence:architecture, technologies, and prospects[J]. Chinese Journal on Internet of Things, 2023, 7(4): 1-12.

[2] Shen, X., Gao, J., Wu, W., Lyu, K., Li, M., Zhuang, W., Li, X. and Rao, J., 2020. AI-assisted network-slicing based next-generation wireless networks. IEEE Open Journal of Vehicular Technology, 1, pp. 45-66.

[3] Park, C., Lee, J., Kim, Y., Park, J.G., Kim, H. and Hong, D., 2022. An enhanced AI-based network intrusion detection system using generative adversarial networks. IEEE Internet of Things Journal, 10(3), pp. 2330-2345.

[4] ABDALZAHER, M.S., FOUDA, M.M. AND IBRAHEM, M.I., 2022. DATA PRIVACY PRESERVATION AND SECURITY IN SMART METERING SYSTEMS. ENERGIES, 15(19), P.7419.

[5] Fan, Y., Bai, J., Lei, X., Lin, W., Hu, Q., Wu, G., Guo, J. and Tan, G., 2021. PPMCK: Privacy-preserving multi-party computing for K-means clustering. Journal of Parallel and Distributed Computing, 154, pp.54-63.

[6] Iqbal, T. and Qureshi, S., 2022. The survey: Text generation models in deep learning. Journal of King Saud University-Computer and Information Sciences, 34(6), pp. 2515-2528.

[7] Miao, J., Thongprayoon, C., Suppadungsuk, S., Krisanapan, P., Radhakrishnan, Y. and Cheungpasitporn, W., 2024. Chain of thought utilization in large language models and application in nephrology. Medicina, 60(1), p.148.

[8] Kirk, R., Mediratta, I., Nalmpantis, C., Luketina, J., Hambro, E., Grefenstette, E. and Raileanu, R., 2023. Understanding the effects of rlhf on llm generalisation and diversity. arXiv preprint arXiv:2310.06452.

[9] Zhang, Y., Zhou, K. and Liu, Z., 2024. What makes good examples for visual in-context learning?. Advances in Neural Information Processing Systems, 36.

[10] Wu, Y., Wei, D. and Feng, J., 2020. Network attacks detection methods based on deep learning techniques: a survey. Security and Communication Networks, 2020(1), p. 8872923.

[11] Khan, I.U., Javeid, N., Taylor, C.J., Gamage, K.A. and Ma, X., 2021. A stacked machine and deep learning-based approach for analysing electricity theft in smart grids. IEEE Transactions on Smart Grid, 13(2), pp.1633-1644.

[作者简介]

周晓茂（1993— ），男，博士，紫金山实验室研究员，主要研究方向为边缘计算、人工智能、算力网络、工业互联网等。

贾庆民（1990— ），男，博士，紫金山实验室研究员，主要研究方向为算力网络、工业互联网、确定性网络、人工智能等。

胡玉姣（1993— ），女，博士，紫金山实验室组研究，主要研究方向为算力网络、工业互联网、确定性网络、人工智能等。

谢人超（1984— ），男，北京邮电大学教授，博士生导师。主要研究方向为未来网络体系架构设计、信息中心网络、移动网络内容分发等。

基于蒙特卡洛树搜索的自组织制造车间任务调度优化

王立平 [1]，刘长春 [1]，唐敦兵*[1]，张泽群 [1]

（1. 南京航空航天大学机电学院，南京 210016）

摘　要：自组织制造模式结合并发展了现有的工业互联技术、无线网络技术、分布式计算技术和人工智能技术，将传统制造资源封装为具有高自主性、高适应性和高功能性的制造单元，并通过与其他制造单元的交互，完成制造任务的自组织协商分配。在这个过程中，为了构建制造任务智能分配和自组织资源配置的快速响应机制，实现制造任务与制造资源的高效、动态匹配，本文将多智能体合同网协议（Contract Net Protocol, CNP）与蒙特卡洛树搜索算法（Monte Carlo Tree Search, MCTS）相结合，提出了制造车间控制系统自组织运作机制与制造任务调度优化方法。最后，通过离散车间任务分配案例对所提方法的实际可行性进行了验证，结果证明，该方法更能实现“单步协商、全域寻优”这一目标。

关键词：多智能体系统；自组织运作；蒙特卡洛树搜索；制造任务分配；智能制造

Optimization of Task Scheduling in Self Organizing Manufacturing Workshop Based on Monte Carlo Tree Search

Wang Liping[1], Liu Changchun[1], Tang Dunbing*[1], Zhang Zequn[1]

Abstract: The self-organizing manufacturing model combines and develops existing industrial interconnection technology, wireless network technology, distributed computing technology, and artificial intelligence technology, encapsulating traditional manufacturing resources into manufacturing units with high autonomy, adaptability, and functionality. Through interaction with other manufacturing units, it completes self-organizing negotiation and allocation of manufacturing tasks. To develop a rapid response mechanism for the intelligent allocation of manufacturing tasks and self-organizing resource distribution, and achieve efficient and dynamic matching between manufacturing tasks and resources, this paper integrates the multi-agent Contract Net Protocol (CNP) with the Monte Carlo Tree Search (MCTS) algorithm. This integration leads to the proposal of a self-organizing operational mechanism and an optimization method for the scheduling of manufacturing workshop control systems. Finally, the practical feasibility of the proposed method was verified through a discrete workshop task allocation case, and the results showed that the method can better achieve the goal of "one-step negotiation and global optimization".

Key words: Multi-agent systems; Self organizing operations; Monte Carlo tree search; Manufacturing task allocation; Intelligent manufacturing

基金项目：国家自然科学基金(92267109, 52075257)，中国博士后科学基金面上项目(2024M754122)，国家资助博士后研究人员计划(GZB20240972)，江苏省卓越博士后计划(2024ZB194)

***通信作者：**唐敦兵，教授，博士生导师，d.tang@nuaa.edu.cn

1 引言

近年来，随着工业化和信息化的不断融合，尤其是后疫情时代给全球经济带来的巨大影响，我国制造业正朝着生产规模扩大化、产品订单定制化、决策需求动态化的方向发展。在这样的背景下，具备自感知、自学习、自决策和自适应能力的“智能制造系统”成为制造业的未来趋势。智能制造的目的是将新一代的传感技术、信息技术、物联技术、人工智能技术与制造技术相结合，进而实现单台设备、单个产线、直至整个工厂等制造服务提供者的自主智能运行。在这个过程中，具备状态感知、数据分析、协商决策和精准控制等特征的多智能体系统（Multi-agent systems，MAS）逐渐成为主流的研究方向。

然而，尽管 MAS 在学术界已经成为大家公认的一种智能制造模式，但在实际的使能化过程中，由于缺乏公认统一的体系架构和与之对应的生产过程动态优化方法，导致 MAS 在传统离散车间应用时缺乏应对各种不确定因素的灵活性和自适应性[1]。基于当前的应用基础和实证研究，MAS 使能化过程中存在的关键问题可以概括为：现有生产模式由于面临着生产环境复杂、生产需求多样、生产条件动态和信息不对称等问题，再加上设备间无法通过自主协作完成制造任务的分配，进而导致制造系统组织效率低下、生产柔性不足。

针对上述问题，学术界分别在制造系统建模与制造单元协商等方面做出了大量的探索。首先，在制造系统建模方面，基于 Holon 和 MAS 技术的制造单元封装方式是最常见的两种建模方法。王世进[2]提出了基于 Holon 概念模型的、集成强化学习机制的合同网协议和改进过滤定向搜索算法，实现了基于自治与协商机制的柔性作业车间智能调度。Wang 等[3]基于 RFID 与 Holon 开发了敏捷制造计划与控制系统，以响应动态变化的制造活动与异常。Pujo 等[4]提出了一种无线 Holon 网络，通过 Holon 为 CPS 系统中的实体进行建模，通过 Holon 间合作产生群体智能。Reaidy 等[5]基于“协同竞争=协同+竞争”的新范式提出了一种基于 MAS 的协商方法，以提高分布式生产系统的按需生产和反应能力。Barenji 等[6]提出了一种用智能体来部署基于 RFID 的分布式控制与监控系统的体系架构，通过智能体间的相互协作提升系统的可重构性。Cheng 等[7]提出了一种基于 MAS 的数控实体网络化和智能化封装方法。Nelson 等[8]提出了一种基于智能体的制造系统服务重构方法，并利用智能体动态识别实现了重构。Nejad 等[9]提出了基于智能体的动态工艺规划制造系统体系结构，将启发式搜索算法与协商协议相结合来处理动态干扰。

然后，在制造单元交互协商方面，Wang 等[10]提出了一个智能工厂框架，在基于 MAS 的基础上增加了协调智能体，通过大数据反馈以提高生产过程的柔性。Wang 等[11]提出了一种基于 MAS 的实时调度架构，采用博弈论协调各智能体行为，并根据设备实时状态进行最优分配。Kim 等[12]提出了一种融合 MAS 与强化学习的智能制造系统，通过智能体决策与交互，提升动态环境下的竞争力。Wang 等[13]通过基于议价博弈的协商机制，研究了基于智能体的物联网制造业柔性作业车间的实时调度问题，实现了任务的最优分配。Guo 等[14]从减少协商沟通、提高多智能体协调能力、改进任务资格评估策略三个方面改进了合同网协议（Contract Net Protocol, CNP）。Zhu 等[15]使用强化学习来执行任务分配过程，并改进 CNP 来实现通

信负载均衡。Reaidy 等[16]针对动态制造环境下的局部调度问题，建立了一种新的竞争与合作协商模型，该模型基于合作请求会话原理和竞争博弈理论，实现了智能体间的高效协商。Lok 等[17]通过受众限制策略提出了一种改进的 CNP 来减少消息拥塞。

从上述研究可以看出，在制造系统建模方面，虽然现有的 MAS 或者 Holon 等封装技术可以将 RFID、个体自治、群体协商等分布式人工智能应用于传统制造车间，但是多数研究对于采用何种方式将车间层的这些物理设备（机床、机器人等）封装成为具有相互通讯、自我决策功能的智能体，这方面的使能技术却鲜有人深入探究，亟需进行完善。在制造单元交互协商方面，现有研究中以合同网、博弈论为代表的协商机制，仍然无法实现策略探索与现有经验知识利用的有效平衡，如何构建设备状态自评估、加工过程自适应、生产管理自组织的制造系统多智能体运行模型，通过 MAS 间的协作与竞争来实现更高效资源分配，成为当前亟需解决的另一关键问题。

2　多智能体制造系统

2.1　基于自组织的多智能体制造系统建模

智能体的标准化范式于 20 世纪就被提出，以应对未来工厂的挑战。智能体被定义为具有自主性和协作性的个体，能够做出决策并与其他智能体进行交互，最终完成系统性的目标。在制造系统领域，多品种、小批量、定制化的制造任务、智能决策和分布式制造结构推动了多智能体制造系统（Multi-agent Manufacturing System，MAMS）的研究。因此，智能体作为设备级执行和控制标准也被认为是分布式制造系统建模的理想方法，可以实现对制造资源的建模与封装。通过智能体封装技术，可以实现制造设备的自感知、自决策与自学习，进而传统制造系统被建模为多智能体制造系统。因此，基于 MAS 的自组织智能制造系统是一个反应式的自适应系统，该系统可以动态修改自身各层级行为和结构，持续不断的进行从输入到输出的交互，以应对物理世界的动态性和不确定性因素的持续增长。

通过上述分析，基于 MAS 的智能制造系统架构如图 1 所示，依据制造系统的角色划分，MAMS 最少需要具备机器智能体、工件智能体、调度智能体和监控智能体四种角色。其中，工件智能体根据工件状态决定是否发起协作请求，并请求调度智能体选择合适的机器智能体进行加工；工件智能体用数据标签取代了传统的物联网跟踪方法（如 RFID、二维码等），而监控智能体为调度智能体的决策提供实时信息支持。

（1）机器智能体

在传统的制造车间中，由于多采用分层控制系统架构，制造设备间无法相互连接。为了实现车间制造资源间的互联，通过 MAS 技术，将制造资源封装为具备感知、计算、通信和控制等功能的机器智能体。同时，基于 MAS 的设计理念与制造系统自组织运作机制，每个制造单元均具备一定的决策能力，他们首先要与对应的实体设备建立连接，然后通过与其他制造单元的信息交互完成制造任务协商，最终实现对设备的精准控制。因此，机器智能体是物理实体在信息空间的映射，对应其感知、计算、通信、控制四个基本属性，机器智能体也是由这四个主要模块组成的，并分模块进行实现。

机器智能体主要包括以下两个功能：首先，通过统一的通讯协议组件实现分布式异构物理实体的互联；其次，通过对来自物理实体的实时信息进行分析处理，为实时调度和异常处理提供信息支持。在这个过程中，由于机器智能体的计算与通信压力过大，单个线程往往无法满足所有的需求，因此机器智能体采用多线程模型进行开发。这些线程分别负责制造单元控制、实时状态监控、智能体之间的交互和协商等功能。

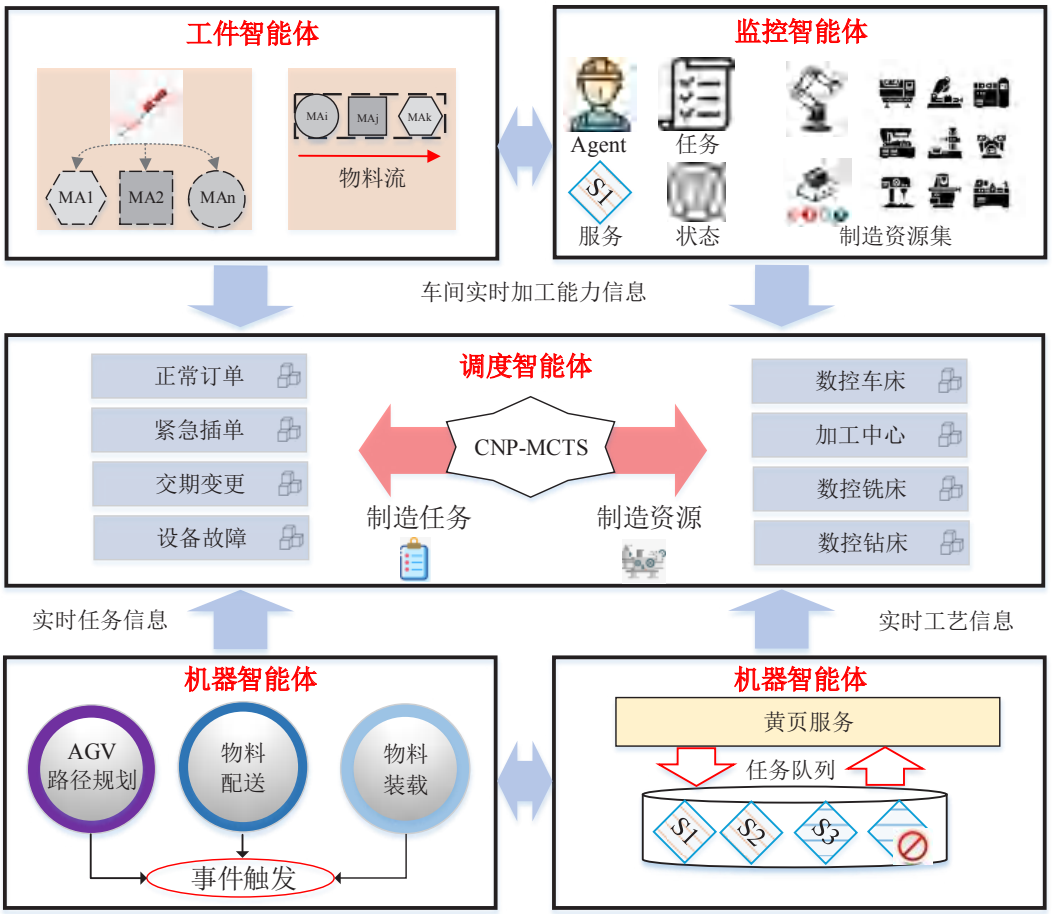


图1　基于MAS的智能制造系统架构

（2）工件智能体

在众多关于 MAS 的研究中，专家和学者们在深入研究之前都默认为车间中每台设备和每个工件配备一个机器智能体和工件智能体，当制造系统规模较小或工件数量较少时，这种默认操作无论从运行逻辑还是系统开发都较易于实现。然而，随着制造系统规模的扩大和工件数量的急剧增加，导致现有工件智能体的计算复杂度和通信负荷都变的很高，进而影响系统正常运行。

虽然工件智能体数量的激增对系统的性能有负面影响，但如果没有独立的单元来管理制造任务也是不合理的。在这样的背景下，本文采用单一工件智能体模式下工件接力协作加工控制的方法对制造任务和生产过程进行管理。该方法将工件视为一根在制造资源之间连续改变状态的“接力棒”，这个接力棒记录着完整的生产过程、消耗材料和加工细节等，具体以 n 维矩阵的形式存在并传递，并由工件智能体进行管理。

（3）调度智能体

调度智能体是智能体协商的发起者与协商结果的评判者，工件智能体通过请求调度智能体发起当前加

工任务的招标，各机器智能体根据自身状态决定是否投标，调度智能体逻辑模块进而完成可行投标集的计算和筛选。调度智能体的决策算法设计是影响制造车间自组织运作效率的关键，当针对某工序接收到机器智能体集群的可行投标集后，调度智能体可以根据不同的决策目标进行计算和筛选，常用的决策目标有：最小完工时间、最小加工成本、制造资源负载均衡等。

（4）监控智能体

在 MAMS 中，由于单个智能体视野的局限性，很难独立完成复杂的决策任务，这就需要每个智能体与其他智能体协作以完成制造任务的优化。然而，由于每个智能体对全局信息的利用率较低，进而导致协商结果的局部最优。针对这个问题，本文解决方案是设置一个面向全局制造信息的监控智能体，该监控智能体既能提供来自所有制造资源的属性信息，包括实时负载信息和设备状态信息，又能提供全局制造任务信息，包括任务的交货期和预计完工时间。

在实际生产过程中，参与投标的单个机器智能体由于观测视野受限容易导致做出不合理的决策。因此，为了保证调度结果的合理性，需要通过监控智能体来引入全局的制造信息，主要提供实时的在制品信息和设备状态。监控智能体的存在保证了整个系统朝着全局优化的方向努力，调度智能体决策时只需要与监控智能体订阅所需的信息即可实现决策优化。

2.2　智能体间的协作过程

MAMS 由多个独立的、分散的智能体组成，通过有效的协商机制相互协作，最终实现实时动态调度。这些智能体通常是分布式的，并且在逻辑上是隔离的。同时，它们的行为是高度自治的，在单智能体行为高度自治的基础上，如何通过特定的协商机制来组织现有的智能体并分配制造任务，是一个亟需突破的问题。因此，多智能体协作的实现依赖于具有交互和决策功能的单个智能体。

制造任务到达后，智能体之间通过交互协商的方式实现制造任务的分配，然而由于单一智能体收集信息的局部性导致决策不够准确，难以获得最优的调度结果。在制造资源有限的情况下，MAMS 中的功能智能体（机器智能体、工件智能体）和服务智能体（调度智能体、监控智能体）协同工作，进而实现动态调度。此外，当制造现场发生异常事件时，智能体能够准确识别干扰类型，并通过协作的方式进行处理。MAMS 采用分布式控制策略对协商结果进行验证，从而保证了自组织运作结果在任务分配生产过程中朝着正确的方向前进，制造车间中的多智能体协作过程如图 2 所示。

基于 MAS 在个体自治、群体协商等方面的特性，与制造系统融合的多智能体制造系统也越来越多的为生产计划提供了更为广泛的功能，然而，每个自治制造单元的决策问题本质上都是由相应智能体的局部决策驱动的，目的是优化自己的目标函数，因此很少取得全局最优，只能产生一个局部较优解。在这样的背景下，本文在传统多智能体合同网协商机制的基础上，引入了自博弈搜索方法中的蒙特卡洛树搜索算法（Monte Carlo Tree Search, MCTS），在调度智能体决策时，通过 MCTS 进行全域寻优，保证调度结果的优化。

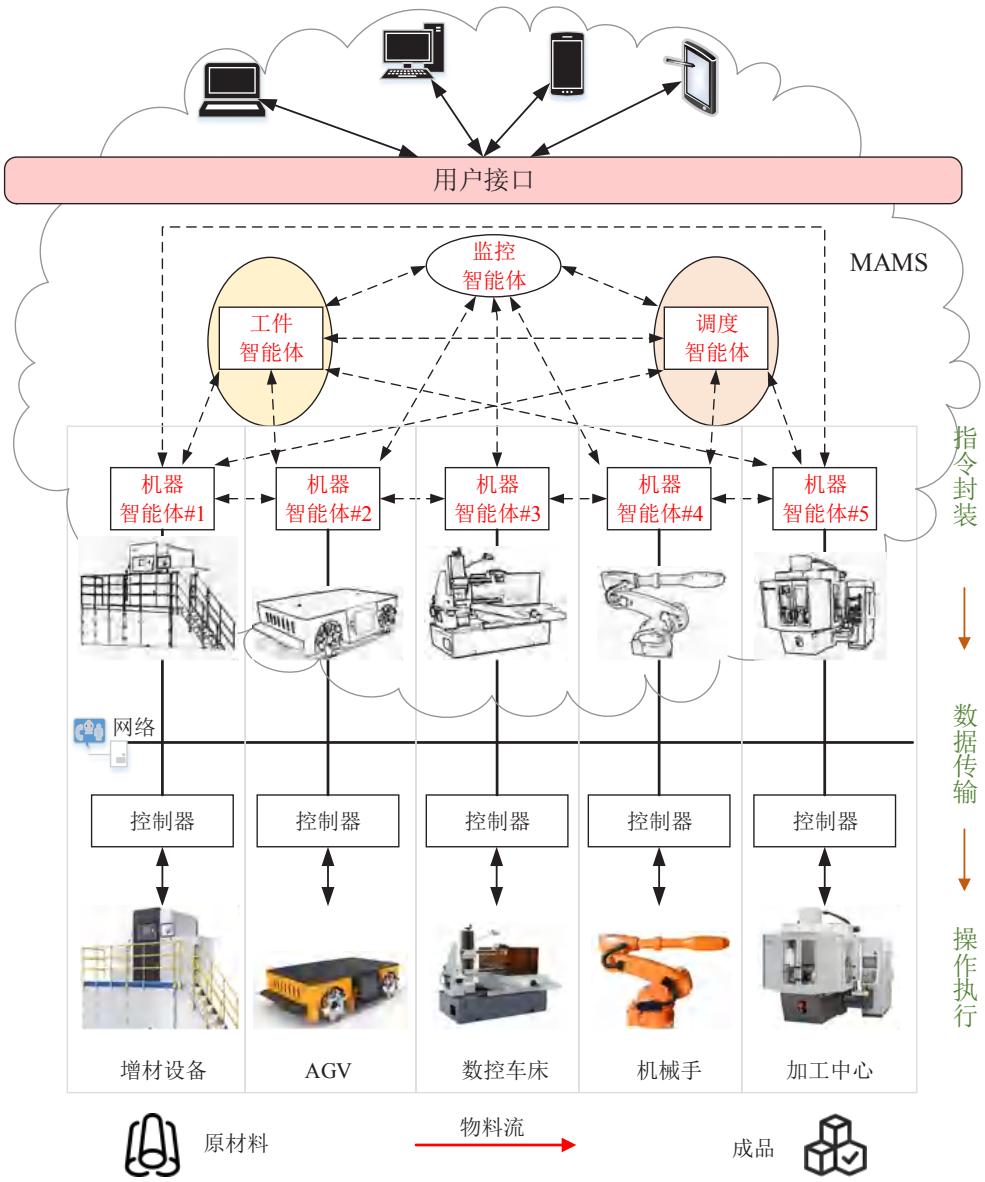


图2　自组织制造车间中的多智能体协作过程示意

3　集成 CNP-MCTS 的制造车间控制系统自组织运作机制

3.1　CNP-MCTS 协商机制模型

单独的 CNP 协商机制具有单步寻优、无法保障全局优化能力的短板，通过引入 MCTS 自博弈搜索机制，可以在有限的计算开销内为当前制造任务找到最优的加工路线，从而确保订单完工时间、设备负载均衡等目标的优化。本文提出的集成合同网协议与蒙特卡洛树搜索算法（CNP-MCTS）的协商分配机制，以适应性行为的方法为指导，通过强化学习多智能体博弈过程，利用单个智能体强化学习与环境的相互作用，实现智能制造系统内制造任务的实时动态调度。同时，在决策的过程中，利用一系列规则保障了 MCTS 搜索结果的精度。CNP-MCTS 协商分配机制的基本流程如图 3 所示，在任务分配过程中，主要的协商过程发生在调度智能体与机器智能体之间。智能体间的交互依托合同网协议，调度智能体决策模块内嵌 MCTS 算法，可以避免基本合同网协议决策时的单步最优，进而实现“单步执行，全域寻优”这一目标，具体工作流程如下。

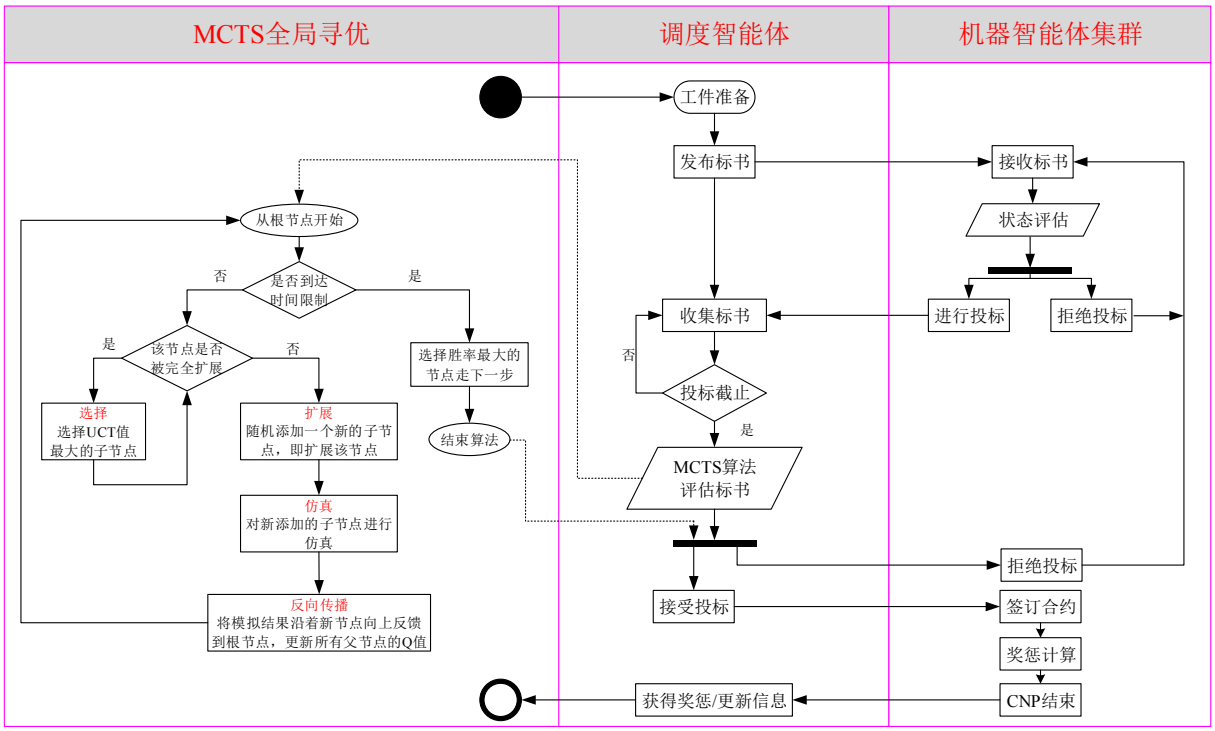


图3　CNP-MCTS协商分配机制基本流程

（1）生产订单进入智能制造系统后，会被分解为最小的原子任务，由原料库备料并由工件智能体生成与该物料对应的数据包，每个数据包内置从管控平台和数据库中获取任务调度所需的信息，包括产品的工艺信息、每道工艺可供替换的加工单元、NC 代码、交货期等信息。

（2）根据加工特征与工艺约束，每个任务可分解为具有约束关系的工序集$\{Process_1, Process_2, \cdots, Process_j\}$，每道工序可在一个或多个制造单元内$\{C_{j1}, C_{j2}, \cdots C_{jk}\}$完成加工。调度智能体在当前加工任务紧前工序完成时向所有能够加工下一工序的机器智能体发布招标公告，开启新一轮招标。

（3）具有紧后工序加工能力的机器智能体在接收到调度智能体发起的招标后，首先查询与该任务相关的加工信息数据包，如任务优先级、加工时间、交货期等，然后预估完成该任务所需的性能指标，如缓冲区数量、在制品（Work In Progress，WIP）的剩余加工时间、加工该任务的最早开始时间等，最后通过综合计算这些加工信息和性能指标决定是否做出投标。

（4）发起招标的调度智能体收集到机器智能体返回的投标结果后，根据 MCTS 算法定义的树节点进行搜索，通过对各投标结果进行策略评估，并根据搜索策略从机器智能体候选集中选择合适的制造资源进行加工。

（5）发起招标的调度智能体确定紧后工序的制造资源后，还需要选择 AGV 来进行工件的运输，选择 AGV 的过程同样采用合同网协议，与选择机器智能体不同的是，调度智能体选择 AGV 时只考虑最早服务时间这一要素。

（6）工件到达所选制造设备的缓冲区后，直至当前工序加工完成调度智能体再发起下一工序的招标，调度智能体会根据所选机器智能体的实际完成时间与投标预估完成时间进行对比，对机器智能体做出奖励或惩罚，该奖励可在后续的投标中提供相关的参考。

3.2 CNP-MCTS 机制的决策过程和学习过程

在强化学习（Reinforcement Learning，RL）中，智能体通过与环境的交互实现目标的决策或行动，进而获得相应的惩罚或奖励。针对当前任务生成对应的正向工序关系有向图作为 MCTS 的探索地图，然后依据搜索策略及环境状态进行可行解模拟搜索，最终生成最优的分配方案。

（1）正向工序关系有向图

为了便于表达加工过程中各工序之间的时序依赖关系，需要基于制造任务的工序约束构造正向工序关系有向图。如图 4 所示为制造任务 T 的正向工序关系有向图，其中每条从根节点至叶节点的路径代表一条可行的加工路线，选择不同的加工路线会产生不同的完工时间和加工成本。

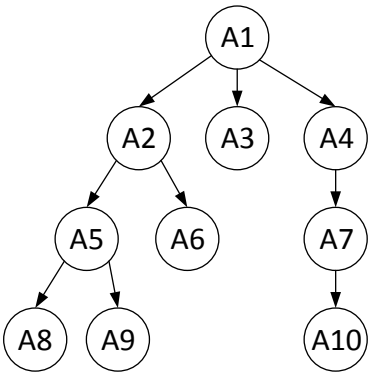


图4　任务T的正向工序关系有向图

正向工序关系有向图表达了制造任务工序间的依赖关系，通过检索每个工序对应的制造资源可以生成一条加工路径，这种树形工序关系为 MCTS 算法的选择、拓展、仿真、回溯四个核心过程提供了搜索路径引导。

（2）CNP-MCTS 机制的决策与学习过程

基于 CNP-MCTS 机制的制造任务协商分配包含 CNP 协商与 MCTS 决策两个过程：首先由调度智能体根据 CNP 规则发起首轮加工招标，等待满足当前工序加工能力的制造资源进行投标；然后调度智能体根据 MCTS 算法通过对当前任务加工路径进行全局搜索，进而确定当前投标集合中最适合的制造资源。在调度智能体进行下一工序的全局搜索过程中，各层级制造资源需要返回包括该任务的开始加工时间、预计完工时间和加工成本等信息，而计算开始加工时间常用的策略有先进先出、最短加工时间优先和最长加工时间优先三个。

根据CNP机制，在调度智能体选择合适的制造资源时，容易造成基于当前状态生成过多劣质解，进而影响最大完工时间等优化目标。本文针对遗传算法的贪婪竞价和短视的缺点，提出了一种新的初始解生成策略——在调度智能体决策过程中，将全局信息与制造资源负载均衡相结合，选择合适的制造资源。该过程详细描述如下：

$$M_k = f_{min} \tag{1}$$

$$L_{min} = L_{min} + t_{ik} \tag{2}$$

其中，假设当前最小加工负载设备为M_k，调度时要求其负载值为L_{min}，同时，假设在设备M_k上加工O_i的

处理时间为t_{ik}，当满足以下条件时，上述步骤生成的初始解是负载平衡的：

$$|L_a - L_b| < max\{t_{ik}\} \tag{3}$$

假设对于任意不同的制造资源a和b在添加第i个任务后满足负载平衡，则对于除f_{min}外的任何制造实体b，满足$L_{min} - L_b \leq 0$，第k次操作后，f_{min}中添加的任务j的负载与其他任何制造资源b的负载之差描述如下：

$$|L_{min} + t_{ik} - L_b| \leq t_{ik} \leq max\{t_{ik}\} \tag{4}$$

其中，在添加新任务后，资源f_{min}与其他制造资源之间的负载差满足负载平衡，则其他设备之间的负载差不受新添加任务的影响。

在经过上述过程的计算评估后，形成的备选竞价集合描述如下：

$$\begin{cases} S_i = \{U_i(s^1), U_i(s^2), \dots U_i(s^k)\} \\ U_i(s^k) = \sum_{i=1}^{N_i}\sum_{j=1}^{N_j} V_{ijk}\, T(O_{ij}, M_k) \end{cases} \tag{5}$$

其中，S_i表示考虑全局设备负载平衡的备选竞价集，$U_i(s^k)$是合同网协议的最大投标值，最大投标值中的V_{ijk}取值描述如下：

$$V_{ijk} = \begin{cases} 1，\text{工序}O_{ij}\text{在设备}M_k\text{上加工} \\ 0，\qquad\qquad\qquad\text{其他情况} \end{cases} \tag{6}$$

其中，当工序O_{ij}在设备M_k上加工时，V_{ijk}取值为1。另外，基于工序约束的接力协作模型可以通过CNP求出$U_i(s^k)$。

最终，为了分配制造任务O_i，定义决策函数描述如下：

$$\arg = \min_{m\in\mathbb{M}_{\phi(j)}} \left(\underbrace{C^L_{m_i m_j}}_{\text{LogisticsCosts}} + \underbrace{C^P_{m_j}}_{\text{ProcessingCosts}} \underbrace{\frac{\sum_{\bar{j}\in J^{\bar{m}}} x_{\bar{j}\bar{m}} dur_j}{\sum_{\bar{m}\in\mathbb{M}_{\phi(j)}} \sum_{\bar{j}\in J^{\bar{m}}} x_{\bar{j}\bar{m}} dur_j}}_{\text{MachineUtilizationWeight}} \right) \tag{7}$$

其中，m_i是制造任务O_i的时序工艺约束中的紧前工序的加工设备，m_j是投标当前工序的加工设备，如果当前工序为该任务的第一道工序，则m_j对应的仓库；$\mathbb{M}_{\phi(j)}$是制造任务o_i当前工序具备加工能力的所有可供选择的制造资源集合。该决策函数同时考虑了物流成本和生产成本，并将竞标设备当前的相对利用率与所有兼容设备的利用率进行了权衡，引入此权重是为了防止只使用特定设备的作业分配。这个决策函数是队列长度估计的一种变体，其中一台设备的队列长度是通过特定设备的相对工作量与所有兼容设备的总工作量的比较来加权的。

在调度智能体通过 CNP 完成一轮招标后，还需要借助 MCTS 算法进行标书评估。通过建立的树结构正向工序关系有向图，MCTS 以此为路径地图进行自博弈搜索，CNP-MCTS 机制的决策过程如图 5 所示。一般情况下，调度智能体根据任务 Jx 的工艺特征将其分解为具有工序约束的制造任务集$\{O_x^1, O_x^2, \dots O_x^y\}$，每道工序可由一个或多个可替换单元集$\{M_{x1}^y, M_{x2}^y, \dots M_{xk}^y\}$完成。CNP-MCTS 机制的决策过程主要在调度智能体接收到各制造单元的加工投标后进行评估，确定当前状态下最适合的加工单元。其中，车间内各设备状态的可考虑任务发出时刻，各制造单元的加工特性和该任务在各单元上的加工特性，最终确定该任务

的加工路径。

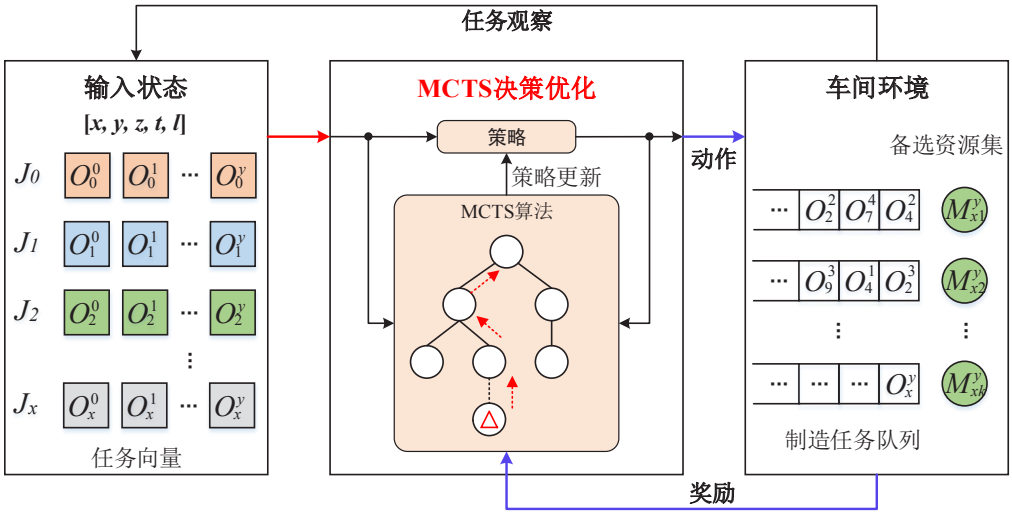


图5　基于MCTS的决策优化过程

在图 5 中，任务 O_x^y可由三个单元M_{x1}^y，M_{x2}^y和M_{xk}^y进行加工，则任务 O_x^y在当前状态 $S1$ 下，有动作集 $A(S_1)=\{a1(s1)，a2(s1)，a3(s1)\}$，利用 MCTS 的搜索策略——上限置信区间算法（Upper Confidence Bound Apply to Tree, UCT），决定加工该任务的制造资源为M_{xk}^y。在任务 J_x 加工完成时刻，利用同样 UCT 策略决定后续加工任务 J_{x+1} 的制造资源为$M_{(x+1)k}^y$。

为实现优化决策，必须结合 MCTS 的回溯和迭代这一过程。首先，工件（或任务）在当前状态 $s1$ 选择特定动作 $a1$（即确定加工单元）后，由当前局面建立根节点，根据正向工序关系有向图生成全部子节点，分别进行模拟；然后，从根节点开始，进行最佳优先探索，在探索过程中利用 UCT 算法分别计算每个节点的 UCT 值并选择具有最大值的子节点，如果该子节点不是叶节点，则以此节点作为根节点，重新开始进行探索，直至找到叶节点；搜索到叶节点后，如果叶节点未曾被模拟加工过，则对叶节点进行模拟加工，否则需要为这个叶节点根据正向工序关系有向图继续生成子节点，并进行模拟加工；将模拟加工的时间与成本更新该节点及各级父节点，同时增加该节点以上所有节点的访问次数并回溯回根节点；最后，根据预先设定的搜索时间或者次数进行停止，从当前局面的子节点中挑选完工时间或完工成本最低的给出决策。

针对当前任务 t 和状态 s，在给定决策过程和默认的 Rollout 策略的情况下，CNP-MCTS 在计算开销（如最大决策时间 100ms、最大迭代次数 100 次）内反复调用选择、扩展、仿真、回溯四个过程，最后根据返回值选择当前状态下最优机器智能体完成任务分配。上述探索学习过程的最终目的是在确定 MCTS 算法因素（选择、扩展、仿真、回溯）的情况下，控制智能体在探索和利用之间的平衡，进而确定可加工单元的动态选择以最优化既定的优化指标（最短完工时间、最小加工成本等）。

3.3　CNP-MCTS 机制中 MCTS 算法各过程的具体定义

与一般的树类似，无论是前面定义的基于时序工艺约束的正向工序关系树，还是 MCTS 中的自博弈搜索树，都要先定义树的根节点和叶节点，根节点定义为搜索开始的节点，叶节点定义为没有子节点的节点。一棵完整的树中，除了根节点和叶节点，剩余的中间节点均为子节点。在基于 CNP-MCTS 的自组织协商

分配机制中，自博弈树的每个节点代表当前车间环境的生产状态，包含当前状态下价值估计、当前节点被选择的次数、当前节点的父节点和当前节点的子节点。将上述自博弈树的节点与状态对应到实际的制造任务协调场景中，根节点为发起任务招标的调度智能体，下面的每个子节点代表具备对应工序加工能力的制造资源，当前状态下的价值估计为根据机器智能体投标的标书加权求和得到的投标价格，当前节点被选择的次数为经过若干次搜索该制造资源被选择的次数，当前节点的父节点和子节点分别对应着的当前工序的紧前工序和紧后工序。

如图 6 所示，CNP-MCTS 机制中 MCTS 算法搜索过程主要分为四步：选择、扩展、仿真和回溯。经过反复执行这四步操作，直至探索完成或者达到搜索的停止条件，再进行最终的决策，下面逐一介绍这些步骤的意义和算法的具体细节。

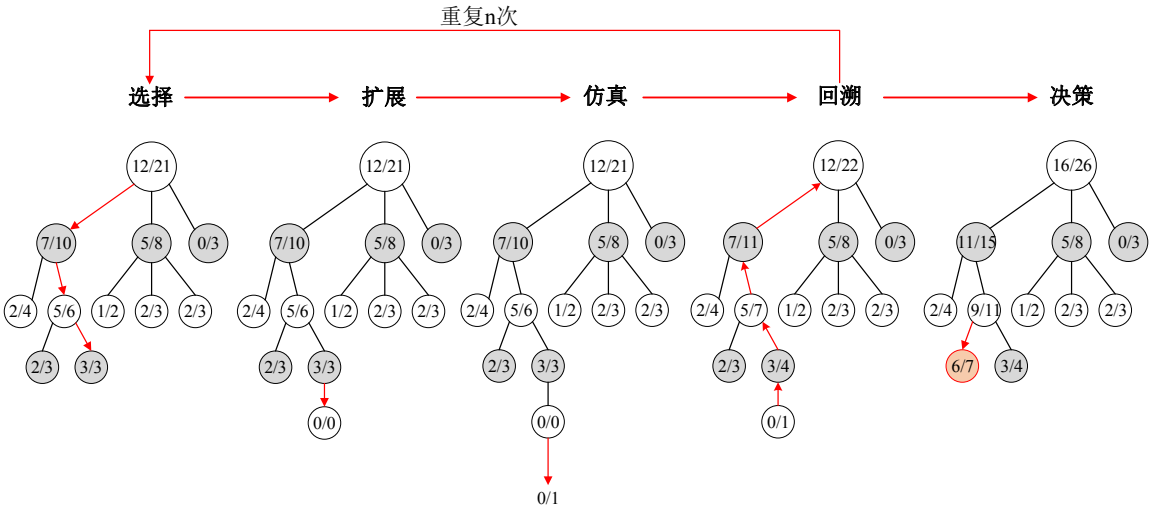


图6　CNP-MCTS机制中MCTS算法的四个阶段

（1）选择。这一步从根节点开始，根据评估函数递归地选择最佳子节点，直到到达可扩展的下一个子节点。这个可扩展的子节点包含一个或多个未访问的子节点，因此它是非终端状态。选择阶段的具体搜索规则采用上限置信区间算法，根据这个算法为每个子节点计算一个分数，然后不断遍历分数最高的子节点，直至到达叶节点，详细计算过程描述如下：

$$UCT(v_i, v) = \frac{Q(v_i)}{N(v_i)} + c\sqrt{\frac{\log(N(v))}{N(v_i)}} \tag{8}$$

其中，第一部分$\frac{Q(v_i)}{N(v_i)}$为子节点 v_i 的价值估计，这个价值越大，表示探索这个节点越有可能获得更大的奖励，其公式定义为：平均收益=总收益/总次数。另外，第一部分的取值与 CNP 的投标值正相关，在传统的 CNP 决策中，通常只用第一项作为决策目标，这也间接导致决策的单步最优，无法保证全局性能。为了避免这种贪婪寻优方式的搜索错过最优解，MCTS 算法引入了第二部分$c\sqrt{\frac{log(N(v))}{N(v_i)}}$，这一部分更倾向于那些未被探索过的节点（即$N(v_i)$较小的节点），c为常数。综上，UCT$(v_i, v)$的第一项和第二项分别代表了智能体的利用和探索部分，系数c控制了这两部分之间的平衡，通过调节c的大小，可以实现 MCTS 偏向于利用更好

的节点和探索尽可能多的节点。特别情况下，当 c=0 时，智能体就变为单步寻优，失去全局探索能力。

（2）扩展。在遍历迭代过程中选择了一个子节点后，需要根据正向工序关系有向图查询该子节点是否可以展开并继续添加子节点，然后根据可用操作选择所有未访问的子节点，除非在当前节点上无法执行更多操作。在 MCTS 算法中，子节点代表的是当前自博弈树的一个状态，这个状态下的所有可行步骤都是由强化学习的环境决定的。也就是说，如果当前子节点不是最终的节点，可以根据当前的强化学习环境（制造任务工艺进度和制造资源任务队列）获取当前匹配制造资源集合的所有可能动作集合，然后根据这些状态扩展子节点，当新添加的子节点成为叶节点后，当前自博弈树状态更新描述如下：

$$s_{t+1} \sim S(s_t, a_t) \tag{9}$$

$$Q(s,a) \leftarrow Q(s,a) + \alpha\left[r + \gamma \max_{a'} Q(s',a') - Q(s,a)\right] \tag{10}$$

其中，在选择过程中，选中的动作（选择制造资源）记为 a_t，它只是一个假想的动作，是在 MCTS 搜索过程中“仿真”执行的。同时，s_t为动作 a_t执行前的状态，s_{t+1}为更新后的环境状态。

在扩展阶段，如果该节点为完全扩展状态，即该节点的所有子节点均被访问过，则可以继续执行下一步；如果还存在子节点未被访问过，则该节点被称为未完全扩展，因此需要继续搜索。在 MCTS 实际运行过程中，由于刚开始时根节点的所有子节点均未被访问过，因此可以从子节点中随机选择一个进行第一次仿真。

（3）仿真。仿真过程中根据滚出策略的评估函数选择一条随机下行路径，以到达叶节点，然后计算该条加工路径下的完工时间与成本。按照博弈论观点，滚出策略最适合选出一条未必多目标最优但加工路径最短的策略。因为如果这个策略走得慢，虽然全局优化能力会更强，结果也更准确，但由于耗时多了，在单位时间内模拟的次数就少了，从而间接导致全局能力变弱。所以，MTCS 也是一种基于模型的 RL，由两部分组成：一个是状态转换模型，预测 RL 主题做出动作后的下一个状态；另一个是奖励模型，预测相应状态转换后的预期计算奖励。一旦马尔科夫决策模型构建完成，便可通过 MCTS 模拟计算最优策略或最优值。

（4）回溯。把仿真的结果加到该节点的所有父节点上，在一次搜索的选择-扩展-仿真阶段，得到了从根节点到叶节点的路径，当路径的叶节点更新以后，需要考虑叶节点的扩展对父节点的影响，这里就要从叶节点出发，反向回传对应的决策路径并更新对应的价值函数描述如下：

$$Q(s,a) = \frac{1}{N(s,a)} \sum_{s'|s,a\to s'} V(s') \tag{11}$$

其中，$V(s')$为最终到达的叶节点的价值函数值，在更新价值函数的同时，也需要更新回传路径上每个节点的访问次数。在跟踪仿真结果后，从仿真开始的节点到根节点的路径上更新所有树节点的统计信息，MCTS 常用的两种反向传播统计是：每个节点的仿真奖励和每个节点的访问次数。

（5）决策。在 MCTS 算法中，“选择→扩展→仿真→回溯”这个过程要重复执行很多次，常用的终止条件有两个：达到一定的迭代次数和达到规定的搜索时间，当搜索程序结束时，最佳的制造资源对应着

访问次数最多的那个节点，也是 UCT 最大的节点。该节点访问的次数越高，代表当前节点的价值越高，也越应该被选择。

MCTS 算法在许多规划问题中具有出色的性能表现，同时，随着问题规模的增大会出现巨大的状态空间，从而使得 MCTS 在在线任务规划中需要花费巨大的计算开销。然而，在 CNP-MCTS 任务规划背景下，参与每道工序投标的智能体数量相对较少，因此能够在有限时间内达到较好的任务调度性能。

4　基于 MAS 的制造车间自组织运作实验验证

4.1　案例描述

基于 MAS 的智能制造系统实验场景布置如图 7 所示。该系统主要由以下制造实体组成：一个用于原材料存储的自动化立体仓库、一个用于成品存储的自动化立体仓库、两台磁导引 AGV、三台六自由度机械手、两台数控车床、两台数控铣床、两台数控雕刻机，上面提到的每个加工单元都配有四个物料缓冲区。

图7　自组织制造车间应用场景布局

传统车间调度问题的求解主要用元启发式方法或静态调度算法，一般不使用协商交互等动态调度的方式减小搜索空间。在这些静态调度算法中，有各种各样的基准调度规则，如先进先出（First Input First Output，FIFO）、最短作业优先（Shortest Job First，SJF）和最长作业优先（Longest Job First，LJF）等。由于其简单的结构和易于决策的优势，这些基准规则被广泛用于车间现场以解决调度问题。此外，在智能制造系统运行期间，由工件智能体管理生产执行的信息跟踪，取代传统的 RFID、条形码等物理标签，关于加工任务实例的详细信息如表 1 所示。该任务实例总共有 6 台加工设备、3 个制造订单、12 个加工任务、28 道具体工序组成，此外，根据两台加工设备的距离将 AGV 的物料运输时间也考虑了进来。传统静态调度的目

的就是根据这些约束关系将这 28 道工序进行排序、重组，直至找到最小的完工时间，而在自组织制造车间中，以加工任务作为调度的发起方，由各制造单元相互竞争，直至完成所有制造任务的分配。

表1　自组织制造车间加工任务实例

订单号	任务号	工艺路线	每道工序对应加工时间/(s)	运输及准备时间/(s)
01	T1	铣削→车削→雕刻	12.3→15.6→13.3	70
	T2	铣削→车削→雕刻	12.3→15.6→13.3	
	T3	车削→铣削	20.0→5.3	
	T4	雕刻→铣削	10.6→7.3	
02	T5	车削→铣削	20.0→5.3	75
	T6	铣削→车削→雕刻	12.3→15.6→13.3	
	T7	雕刻→铣削	10.6→7.3	
	T8	雕刻→铣削	10.6→7.3	
03	T9	雕刻→铣削	10.6→7.3	80
	T10	雕刻→铣削	10.6→7.3	
	T11	铣削→车削→雕刻	12.3→15.6→13.3	
	T12	雕刻→铣削	10.6→7.3	

4.2　实验结果与分析

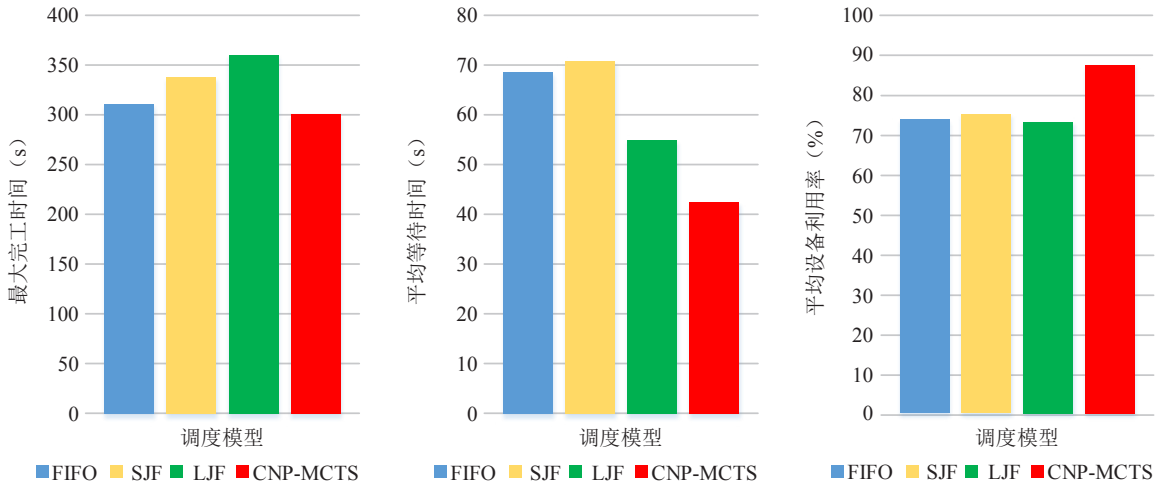
基于 MAS 的制造车间自组织运作属于柔性车间作业调度问题（Flexible Job-Shop Scheduling Problem，FJSP），对于存在缓冲区的 FJSP 根据资源选择条件的不同，调度过程可分为工件选机床和机床选工件两个阶段，通过这两个阶段的选择可大致确定该任务的预计完工时间，进而确定整个订单的交货期。

本文所提出的 CNP-MCTS 方法与三个基线调度技术进行对比，其中，三个基线调度技术分别是：FIFO、SJF、LJF。使用 MCTS 算法与这三个基线调度规则对比，以寻找最佳策略来实现智能制造系统的动态调度。CNP-MCTS 协商分配机制通过 MDP 接口与智能制造系统环境集成，并实现了探索最优调度策略的目标。实验结果根据以下三个性能标准进行评估：

- 最大完工时间（C_{max}）——这个性能标准用于计算制造任务队列的总完工时间，决定了算法的整体性能；
- 平均等待时间（Average Waiting Time，AWT）——作业等待时间包括等待时间和频率、完成时间和响应时间，AWT性能标准用于确定作业平均等待时间是否减少；
- 平均设备利用率（Average Resource Utilization，ARU）——代表每台机器的总有效利用时间，这个性能标准用来判断所应用的调度方法是否提高了调度系统的效率。

（1）CNP-MCTS 自组织协商分配效率

使用上述三个性能标准进行图形比较的结果如图 8 所示。其中，CNP-MCTS 算法确定了 18 个作业的时间表，其最大完成时间（Makespan）为 300s，图 8（a）中的 FIFO、SJF 和 LJF 的值分别为 310s、340s 和 360s，本文所提方法明显优于所有基线调度规则，这是因为 CNP-MCTS 通过应用 UCT 评估函数来模拟提前获取入站操作的处理时间和相应可用机器的信息。



(a) 完工时间　　(b) 工件平均等待时间　　(c) 平均设备利用率

图8　常见任务队列策略下的对比实验

本文所提 CNP-MCTS 方法还导致所有工件的平均等待时间在整个生产过程中下降，当与基准调度规则相比时，平均等待时间只有 42.6s，而这些基准调度方法的平均等待时间都超过 50s，详细结果如图 8（b）所示。由于平均等待时间的减少，到达作业在调度系统中的任务完成时间也相应减少，从而导致整体计划提前完成。相反，CNP-MCTS 通过最大化资源利用率获得了所有机器中最高的平均设备利用率，如图 8（c）所示，相较于 FIFO、SJF 和 LJF 三种基线调度规则，CNP-MCTS 方法平均设备利用率高达 86.94%，提高了制造系统的整体效率。

表 2 针对三种不同场景下比较了 CNP-MCTS 算法与基线调度规则，这三个场景包含具有不同数量的任务和工序但可用机器数量相同的示例问题。通过不同场景下的对比，可以检查本文所提算法在不同大小的样本问题中的有效性。实验结果表明，在所有三个场景中，CNP-MCTS 算法的表现优于所有基线调度规则，并且三个评估指标均实现了最佳效果。

表2　四种策略下的对比实验数据表

场景	$n\times m\times o$	算法类型	最大完工时间（s）	平均等待时间（s）	平均设备利用率（%）
1	6×6×18	FIFO	310	68.3	74.05
		SJF	340	70	75.19
		LJF	360	55	72.39
		CNP-MCTS	300	42.6	86.94
2	12×6×36	FIFO	590	229.17	77.91
		SJF	690	202.5	79.84
		LJF	650	196.67	65.99
		CNP-MCTS	540	132.36	89.72
3	24×6×72	FIFO	1090	459.58	81.58
		SJF	1190	423.33	83.01
		LJF	1210	395.42	68.51
		CNP-MCTS	970	206.78	90.62

图 10 显示了所有调度算法随着作业数量增加的最大完工时间变化曲线。从图中可以看出，在开始时间到 CNP-MCTS 算法探索前 16 个作业时，它的性能与所有基线调度规则持平，这是由于这些基准调度规

则采用贪婪搜索方法。然而，随着每个作业数量的增加，CNP-MCTS 的探索能力也在增强，并且性能越来越好，最终当达到第 37 个作业时，它优于所有基线方法。这是因为随着任务的增加，MCTS 算法应用更多的模拟次数，并在每个周期访问额外的子节点以改进搜索策略。因此，CNP-MCTS 算法更适合于求解较大规模的实时动态调度问题。

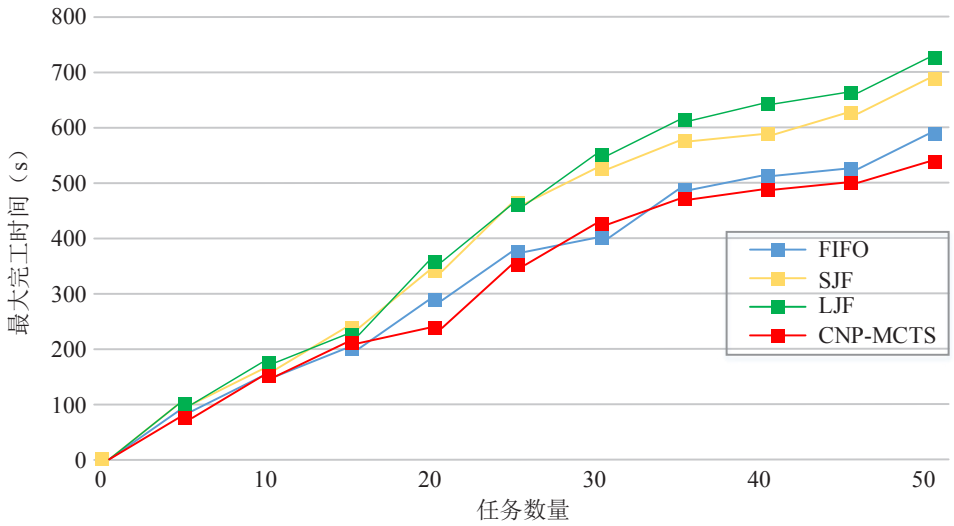


图9　任务数量增加情况下四种调度策略的完工时间对比

（2）CNP-MCTS 算法利用与探索的平衡

CNP-MCTS 算法在动态调度实验中取得较好的效果，相较于调度结果来说，MCTS 算法本身还能够实现利用与探索的平衡。在每一轮的算法迭代中，只要选择胜率高的节点进行下一步仿真即可，但贪婪方式的搜索会很快导致搜索结束，这往往会导致搜索不充分，进而错过最优解。因此 UCT 算法增加了第二项，称为探索单元，这个单元更倾向于那些未被探索的节点（奖励值较小的节点）。在 MCTS 搜索过程中探索单元的权重取值趋势大概如图 11 所示，随着迭代次数 N 的增加其值也在不断下降，这种趋势与决策优化过程是相似的：初期探索时需要更大的搜索空间，后期决策时需要算法收敛。

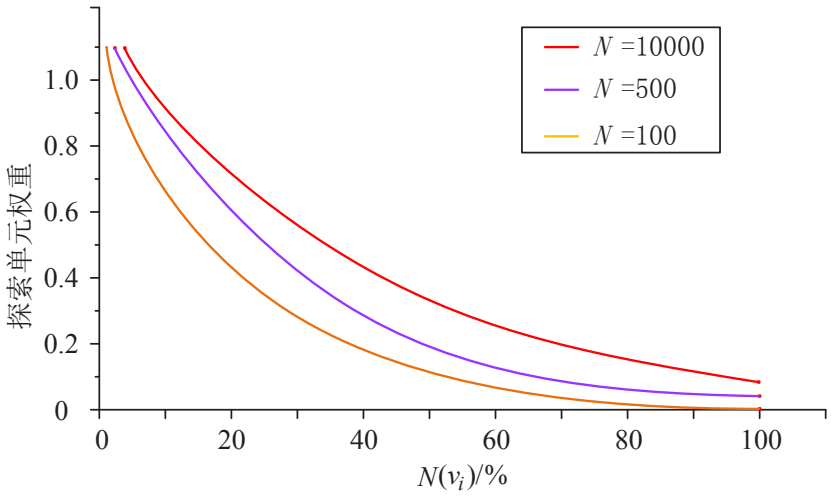


图10　CNP-MCTS机制下UCT算法探索单元的取值趋势

5 结束语

本文将多智能体合同网协议与蒙特卡洛树搜索算法相结合，提出了制造车间控制系统自组织运作机制与制造任务调度优化方法。首先，基于 MAS 技术对车间制造资源进行了封装，使其成为具备通信功能的自治实体，在此基础上对传统的 CNP 协商分配策略进行优化，在智能体决策时调用 MCTS 算法对标书进行评估，以确保决策的全局有效性。然后，在 MAMS 框架下，各制造单元通过智能体间的协商机制实现制造单元间的互联。最后，通过实验表明，CNP-MCTS 算法较传统的先进先出、最短作业时间优先和最长作业时间优先具有更好的全局优化效果。

参考文献

[1] ACATECH. Cyber-Physical Systems: Driving Force for Innovations in Mobility, Health, Energy and Production[M]. Springer. 2012.

[2] 王世进. 基于自治与协商机制的柔性制造车间智能调度技术研究[D]. 上海交通大学, 2008.

[3] WANG L C, LIN S K. A multi-agent based agile manufacturing planning and control system[J]. Computers & Industrial Engineering, 2009, 57(2): 620-640.

[4] PUJO P, OUNNAR F, POWER D, et al. Wireless Holon Network for job shop isoarchic control[J]. Computers in Industry, 2016, 83: 12-27.

[5] REAIDY J, MASSOTTE P, DIEP D. Comparison of negotiation protocols in dynamic agent-based manufacturing systems[J]. International Journal of Production Economics, 2006, 99(1-2): 117-130.

[6] BARENJI R V, BARENJI A V, HASHEMIPOUR M. A multi-agent RFID-enabled distributed control system for a flexible manufacturing shop[J]. The International Journal of Advanced Manufacturing Technology, 2014, 71(9-12): 1773-1791.

[7] CHENG T, WU B, YANG S Z , et al. Study on Intelligent CNC System for Distributed Networked Manufacturing (in Chinese) [J]. CHINA MECHANICAL ENGINEERING, 2004(08): 32-37.

[8] RODRIGUES N, OLIVERIA E, LEITAO P. Decentralized and on-the-fly agent-based service reconfiguration in manufacturing systems[J]. Computers in Industry, 2018, 101:81-90.

[9] TEHRANI H, NEJAD N, SUGIMURA N, et al. Multi agent architecture for dynamic incremental process planning in the flexible manufacturing system[J]. Journal of Intelligent Manufacturing, 2010, 21(4): 487-499.

[10] WANG S, WAN J, ZHANG D, et al. Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination[J]. Computer Networks, 2016, 101: 158-168.

[11] WANG J, ZHANG Y, LIU Y, et al. Multiagent and bargaining-game-based real-time scheduling for internet of things-enabled flexible job shop[J]. IEEE Internet of Things Journal, 2018, 6(2): 2518-2531.

[12] KIM Y G, LEE S, SON J, et al. Multi-agent system and reinforcement learning approach for distributed

intelligence in a flexible smart manufacturing system[J]. Journal of Manufacturing Systems, 2020, 57: 440-450.

[13] WANG J , ZHANG Y F , LIU Y , et al. Multi-agent and Bargaining-game-badacorased Real-time Scheduling for Internet of Things-enabled Flexible Job Shop [J]. IEEE Internet of Things Journal, 2018:1-1.

[14] GUO C, XIONG W, LIU C X, Prospects and current researches on improvement of contract net protocol (in Chinese) [J]. Journal of Equipment Academy, 2016(27): 82-89.

[15] ZHU Y F, LOU P H, QIAN X M, et.al. Research on job shop scheduling method based on improved contract net protocol (in Chinese) [J]. Machine Design and Manufacturing Engineering, 2018(47): 97-102.

[16] REAIDY J, MASSOTTE P, DIEP D. Comparison of negotiation protocols in dynamic agent-based manufacturing systems [J]. International Journal of Production Economics, 2006, 99(1/2):117-130.

[17] YEUNG W L . Agent-based manufacturing control based on distributed bid selection and publish-subscribe messaging: a simulation case study [J]. International Journal of Production Research, 2012, 50(22):6339-6356.

[作者简介]

王立平（1990 年生），男，博士，主要研究方向为自组织智能制造系统及其关键使能技术。

刘长春（1995 年生），男，博士，助理研究员，主要研究方向为基于深度强化学习的设备状态分析与人机协作。

唐敦兵（1972 年生），男，博士，教授，主要研究方向为工业互联网与数字孪生。

张泽群（1991 年生），男，博士，讲师，主要研究方向为多智能体制造系统。

面向低功耗嵌入式设备的可信软件栈设计与应用

杨轩，马承彦，习宁

(西安电子科技大学网络与信息安全学院，陕西 西安 710071)

摘　要：嵌入式设备因其体积小、成本低、操作易、效率高等特点，已广泛应用于工业物联网、工业自动化等领域。然而，这些设备计算资源有限、物理接口开放，常常面临固件篡改、硬件替换等安全威胁。本文针对现有可信软件栈无法应用于低功耗嵌入式设备的问题，提出了一种适用于低功耗嵌入式设备的可信软件栈。该软件栈由驱动层的串行外设接口驱动、协议层的字节流转换协议、内核层的可信接口三大部分构成，为低功耗嵌入式设备提供哈希计算、数据加解密、完整性度量等可信功能。与现有软件栈相比，基于国产可信计算模块的低功耗嵌入式可信软件栈时间开销平均减少了 58.98%。针对低功耗嵌入式设备固件易遭受篡改和现有可信启动方法不适用的问题，本文基于低功耗可信软件栈提供的国密哈希算法接口和完整性度量接口，提出一种轻量可信启动方法。通过基于密码分组链接模式的轻量完整性度量算法，实现了在小内存空间下的完整性度量和可信启动。在工业无人系统中测试表明，该方法可以抵御固件篡改和挂载替换等多种攻击，具备较高的安全性，且时间开销仅为 571 毫秒。

关键词：低功耗嵌入式设备；可信计算；可信密码模块；可信软件栈

Design and Application of Trusted Software Stack for Low-end Embedded Devices

YANG Xuan, MA Chengyan, XI Ning

(School of Cyber Engineering, Xidian University, Xi’an 710071, China)

Abstract: Embedded devices, due to their small size, low cost, ease of operation, and high efficiency, have been widely used in fields such as Industrial Internet of Things and automation. However, these devices often face security threats such as firmware tampering and hardware replacement due to their limited computing resources and open physical interfaces. This paper addresses the problem that existing high-power trusted software stacks cannot be applied to low-end embedded devices by proposing a trusted software stack suitable for low-end embedded devices. This software stack consists of three main components: the serial peripheral interface driver at the driver layer, the byte stream conversion protocol at the protocol layer, and the trusted interface at the kernel layer. It provides trusted functions such as hash computation, data encryption and decryption, and integrity measurement for low-end embedded devices. Testing on a low-end embedded system based on a domestically

通信作者：习宁（nxi@xidian.edu.cn）
基金项目：国家自然科学基金项目重大研究计划（No.92267204）

produced trusted computing module shows that, when performing the same security functions, the time overhead of this software stack is reduced by an average of 58.98% compared to existing software stacks. To address the issues of firmware tampering and the inapplicability of existing trusted boot methods for low-power embedded devices, this thesis proposes a lightweight trusted boot method based on the national cryptographic hash algorithm interface and integrity measurement interface provided by the low-power trusted software stack. By utilizing a lightweight integrity measurement algorithm based on the cipher block chaining mode, integrity measurement and trusted boot are achieved in a small memory space. Testing in an unmanned vehicle system shows that this method can resist various attacks such as firmware tampering and mounting replacement, providing high security with a time overhead of only 571 milliseconds.

Key words: low-end embedded devices, trusted computing, Trusted Cryptographic Module, Trusted Software Stack

1 引言

嵌入式设备因其体积小、成本低、操作易、效率高的特点，在工业物联网领域得到了日益广泛的应用，成为了工业自动化、无人设备、智能电网、智慧城市等系统的基石。

然而，大多数嵌入式设备基于计算资源受限、物理接口开放的低功耗芯片构建。因此，这些设备极易遭受物理捕获、固件篡改、挂载替换等安全威胁[1-2]。如 Stuxnet 病毒作为第一个专门定向攻击真实世界中基础能源设施的“蠕虫”病毒，通过对监控和数据采集系统（SCADA）的破坏，影响了数据在电力设备间的正确传递，直接导致了 2015 年乌克兰电厂事件。2019 年，武汉网警破获湖北省首例入侵物联网系统案，经统计共 100 余台物联网设备被恶意升级无法使用、10 万台设备离线。2023 年，攻击者利用 CVE-2023-20198 漏洞向超过 10000 台的 Cisco IOS XE 设备植入恶意程序，使受感染设备可被远程操控执行任意命令。这些安全事件造成了重大经济损失，甚至危害国家安全。因此，确保嵌入式设备的稳定运行和数据安全具有重要的意义。

可信计算技术是解决上述问题的有效手段之一，它的核心是可信平台模块和可信软件栈。随着我国可信计算技术的发展，为了确保数据处理与信息安全的自主性和可靠性，我国提出了符合国密标准的可信平台模块——可信计算模块（Trusted Cryptography Module，TCM）。它在原有的可信平台模块的基础上实现了对我国国密算法的支持，从而有效增强了可信计算技术的安全可控性。

TCM 通过为设备构建一个可信根，再建立一条信任链[3]。从可信根开始，到可信硬件平台，再到可信操作系统，最后到可信应用，逐级向上，从而确保整个设备的安全性。在确保设备安全的同时，TCM 还可以为设备提供远程证明、安全存储、数据加解密等可信服务，从而解决身份伪造、数据窃听等网络攻击问题，为设备构建可信的网络环境。

为更便捷的使用 TCM 的可信功能，现有工作开发了能访问可信平台模块的开源可信软件栈

TPM2-TSS[4]。目前，基于 TPM2-TSS 和可信平台模块的安全保护技术已经在通用计算系统中进行了大规模的应用。然而，与此现状不同，面向低功耗嵌入式设备的 TCM 可信软件栈却鲜有研究。首先，相比电脑，低功耗嵌入式设备运算能力较为逊色且存储能力有限，而 TPM2-TSS 因其架构复杂臃肿，难以直接移植并运行在低功耗嵌入式设备中。此外，电脑中有专有驱动程序可直接与 TCM 通信，而低功耗嵌入式设备则需要开发特定的驱动才能实现 TCM 与嵌入式设备中程序的通信。因此，亟需设计与开发面向低功耗嵌入式设备的 TCM 可信软件栈。

本文针对 TPM2-TSS 无法应用于低功耗嵌入式设备的问题和现有的可信启动方法不适用的问题，设计并实现了一套面向低功耗嵌入式设备的可信软件栈，并基于该软件栈实现了一种轻量可信启动方法。最终，在基于低功耗芯片 STM32F103 和国产 TCM 芯片 Z32H330TC 的无人航行器系统中进行了实验验证。主要贡献包括：

1) 设计并实现了面向低功耗嵌入式设备的可信软件栈：该软件栈由驱动层的串行外设接口驱动、协议层的字节流转换协议、内核层的可信接口三大部分构成，为低功耗嵌入式设备提供哈希计算、数据加解密、完整性度量等可信功能支持。

2) 提出了一种适用于低功耗嵌入式设备的轻量级可信启动方法：通过调用低功耗可信软件栈的国密哈希算法接口和度量值拓展接口，对设备的软硬件进行完整性度量，并与 TCM 中预存的正确值进行比对，从而实现低功耗嵌入式设备的可信启动。

3) 本文实验在基于 TCM 的低功耗嵌入式系统中对软件栈进行了功能测试和分析，并在工业无人系统中测试并分析了轻量可信启动方法的安全性和性能。

2　研究现状

2.1　x86 平台

为了解决计算机安全问题，美国国防部 1983 年推出了世界上第一个《可信计算机系统评价准则（Trusted Computer System Evaluation Criteria, TCSEC）》，首次提出了可信计算机和可信计算基（Trusted Computing Base, TCB）的概念，并将 TCB 作为计算机系统安全的基础。1999 年 10 月，由 IBM、HP、Intel、Compaq 和 Microsoft 等发起成立了“可信计算平台联盟”（Trusted Computing Platform Alliance, TCPA）。2003 年 3 月，TCPA 改组为可信计算组织（Trusted Computing Group, TCG）。TCG 是专门致力于制定可信计算标准的非营利性机构，该组织致力于促成新一代具有安全和信任能力的硬件运算平台——可信平台模块。TCG 在强调安全硬件平台构建的同时，进一步增加了对软件安全性的关注，从跨平台和操作环境的硬件组件和软件接口两方面，促进不依赖特定厂商的可信计算平台工作标准的制定。2007 年 12 月，国家密码管理局颁布了《可信计算密码支撑平台功能与接口规范》，提出了适配国密算法的可信平台模块——TCM。目前，在 X86 架构的计算机系统中，可信平台模块有着较为成熟的应用：比如在最新的操作系统 Window 11 中，可信平台模块 2.0 作为最低硬件要

求，必须默认实现并被开启。此外，有很多研究者展开对 Intel SGX 技术[5-6]和可信计算技术结合的研究。现阶段，通过将虚拟化的 TPM 分配给虚拟机，虚拟机的使用者也像使用物理 TPM 一样调用加解密和完整性度量等功能，从而保护云计算的安全性[7-11]。但是，由于 X86 架构具有高功耗的特性，这些基于可信计算的安全保护方法难以应用到以低功耗嵌入式设备为主的工业物联网中。

2.2 ARM 平台

近些年，可信平台模块的应用逐渐推广至嵌入式系统中。2016 年，Choi 等人[12]提出了一种适用于家庭网络环境下的设备安全固件验证和更新方案，该方案中会进行固件验证以确保固件的完整性，从而检测固件篡改攻击。2020 年，Lu D 等人[13]针对智能医疗设备提出了基于可信平台模块的 xTSeH 方案，医疗嵌入式设备在开机启动时会进行安全性检查，以保证设备未受到恶意攻击和篡改。2021 年，Zhao H 等人[14]设计了一个安全可信的电路，利用可信平台模块在启动过程中对嵌入式系统进行完整性度量，来实现系统的安全可信启动。智能电网中，可信平台模块也被用于实现终端的可信网络连接和用户数据的隐私保护[15-17]。但是，这些基于可信平台模块安全保护方法仍需要使用 TPM2-TSS 与可信平台模块进行通信。而 TPM2-TSS 因其架构复杂臃肿，需要运行在 Linux 等通用操作系统上。而本文面向的低功耗嵌入式设备并不具备搭载这类操作系统的能力。因此这些基于可信计算的可信启动方法也无法应用到低功耗嵌入式设备。

3 系统设计

低功耗嵌入式可信软件栈的基石是国产 TCM 芯片。依托国产 TCM 芯片，整个软件栈可以分为四层，自下而上分别为驱动层、协议层、内核层和业务层，如图 1 所示。

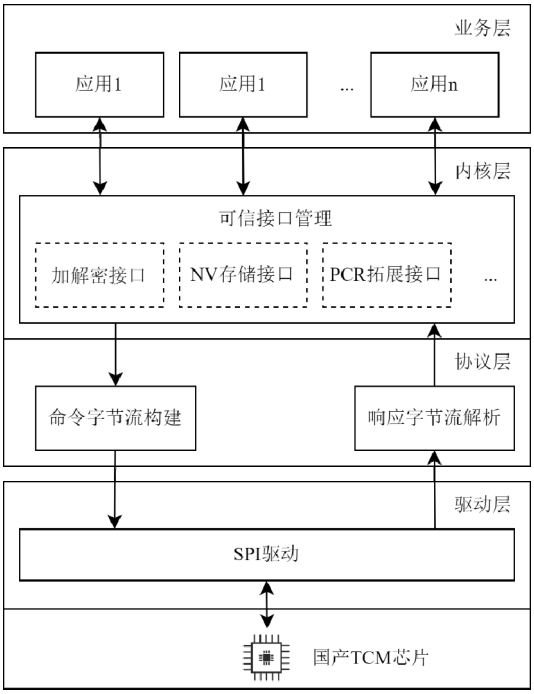


图1 低功耗嵌入式可信软件栈系统架构图

1) 驱动层

驱动层实现了 SPI 驱动。国产 TCM 芯片中定义了一系列基于 SPI 协议的命令字节流和响应字节流。SPI 驱动主要负责命令字节流和响应字节流与 SPI 信号的转换。它将来自上层的命令字节流命令转化为 SPI 信号，通过 SPI 总线发送给国产 TCM 芯片，将 SPI 总线上来自国产 TCM 芯片的 SPI 信号转换为响应字节流发回上层。

2) 协议层

协议层实现了命令字节流和响应字节流的解析。具体来说，本文在国产 TCM 芯片中定义的基于 SPI 协议的命令字节流和响应字节流基础上进行了一层封装。通过将字节流划分为命令属性、命令大小、命令代码、命令参数四大部分，使各类可信接口可以更方便发起命令和解析命令结果。

3) 内核层

内核层实现了一系列可信接口以及统一的管理程序。上层应用可以直接调用可信接口从而实现对应的可信功能。

4) 业务层

业务层基于低功耗可信软件栈提出一种轻量可信启动方法，该方法可以在一定程度上防止低功耗设备的软硬件被篡改，从而有效保护低功耗嵌入式设备的软硬件安全。

3.1　驱动层设计

依托 SPI，本文基于 STM32 的 HAL 库设计并实现了一套用于 TCM 的 SPI 驱动程序。该驱动程序包含以下模块：TCM 初始化模块、TCM 寄存器读取模块、TCM 寄存器写入模块以及 TCM 命令执行模块，如图 2 所示。

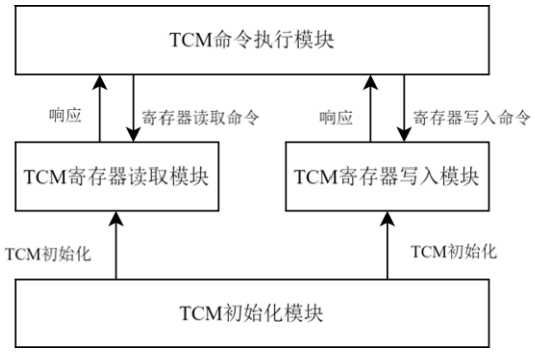


图2　SPI驱动架构图

其中，TCM 初始化模块负责配置与 TCM 相关的通信接口，是整个驱动程序的基础。TCM 寄存器读取模块和 TCM 寄存器写入模块通过 SPI 对 TCM 内部的寄存器进行读取和写入，从而实现与 TCM 的数据交换。命令执行模块通过多次调用 TCM 寄存器读取模块和 TCM 寄存器写入模块，不断读取 TCM 状态寄存器和 TCM 命令寄存器，将上层的字节流命令发送给 TCM 执行。

3.2 协议层设计

为了各类可信接口可以更方便发起命令和解析命令结果，需要设计通用化可定制的协议层字节流转换协议。本文在协议层实现了一种字节流协议，如图 3 所示：

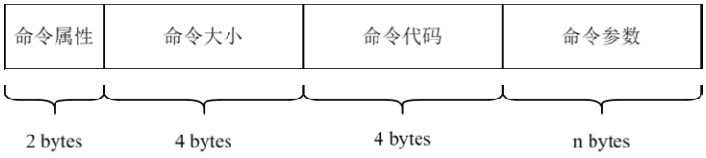


图3 字节流协议格式

该协议由 2 字节大小的命令属性、4 字节大小的命令大小、4 字节大小的命令代码和 n 字节大小的命令参数组成。

其中，命令属性可以为会话属性和非会话属性。TCM 的命令中，不同与非会话属性的命令，具有会话属性的命令需要在命令中添加相关的会话控制信息。因此，有必要区分会话命令和非会话命令。

命令大小指示着该命令参数的大小，通过该参数可以知晓后续命令参数的长度。

命令代码代表此次命令所执行的命令，与 TCM 中定义的命令字节流一一对应。

命令参数代表此次命令所需的各类参数，例如句柄、寄存器选择信息等。

TCM 与低功耗嵌入式设备的通信字节流分为命令字节流和响应字节流。命令字节流发送至 TCM 后，TCM 首先根据命令属性判断命令是否为会话命令；接着，TCM 根据命令大小将与命令有关的所有字节读取到缓冲区；最后，TCM 根据命令代码和命令参数执行对应的操作。进行命令响应时，TCM 也会将数据包构造为相同的格式并回传。

3.3 内核层设计

表 1 可信接口提供的功能

功能名称	功能作用	功能名称	功能作用
lp_tcm_startup	启动 TCM	lp_tcm_getrandom	使用 TCM 获取随机数
lp_tcm_shutdown	关闭 TCM	lp_tcm_createprimary	创建 TCM 中的主密钥
lp_tcm_clear	重置 TCM	lp_tcm_create	创建 TCM 中的子密钥
lp_tcm_pcrextend	对 TCM 中指定的 PCR 进行拓展操作	lp_tcm_load	将密钥加载到 TCM 中
lp_tcm_pcrread	读取 TCM 中指定的 PCR	lp_tcm_sm4encry	调用 TCM 使用 SM4 算法加密数据
lp_tcm_pcrreset	重置 TCM 中指定的 PCR	lp_tcm_sm4decry	调用 TCM 使用 SM4 算法解密数据
lp_tcm_hash_sm3	调用 TCM 的 SM3 算法	lp_tcm_rsaencry	调用 TCM 使用 RSA 算法加密数据
lp_tcm_hash_sha256	调用 TCM 的 SHA256 算法	lp_tcm_rsadecry	调用 TCM 使用 RSA 算法解密数据

可信接口主要有两方面的功能。一方面，可信接口封装了 TCM 的常用功能接口，用户可以直接调用可信接口中的函数从而调用 TCM 的功能。另一方面，可信接口具有管理这些可信功能的程序，可信应用可以随时随地调用可信功能，而不必担心发生抢占冲突。

TCM 的常用功能可以分为四类：基础功能、度量功能、哈希功能和加解密功能。其中，基础功能包括 TCM 的启动、关闭和重置；度量功能包括对 TCM 中特定 PCR 的拓展、读取和重置；哈希功能包括使用 TCM 进行 SM3 哈希和 SHA256 哈希；加解密功能包括生成随机数、生成主密钥、生成子密钥、加载密钥、SM4 加密、SM4 解密、RSA 加密和 RSA 解密。表 1 展示了本文可信软件栈提供的各类接口。

其次，对于可信接口管理。本文使用优先级队列对可信接口的调用进行管理，从而避免各个可信应用在同一时间调用 TCM 的可信接口从而发生冲突。

通过优先级可以防止 TCM 陷入死循环。本文将可信接口划分为两个等级，与 TCM 的基础功能相关的命令具有高优先级，其余命令的优先级均在其优先级之下。因为 TCM 基础功能中的命令都是与 TCM 功能密切相关的命令，影响着 TCM 其他功能的执行，因此需要优先执行这些命令。

通过队列可以防止多个可信应用同时调用可信接口从而发生冲突。当一个可信应用需要调用特定接口时，它不会直接执行操作，而是将调用指令的字节流协议命令放入命令执行队列中。命令执行队列负责暂存所有待处理的 TCM 可信接口调用指令，这些指令按照先进先出的原则排队执行并依次返回执行结果。

3.4　功能应用

本节设计并实现了基于低功耗嵌入式可信软件栈的轻量可信启动方法，该方法包含三大模块：数据读取模块、TCM 哈希模块以及 TCM 度量值扩展模块。

其中，数据读取模块负责从外部空间中读取数据。TCM 哈希模块负责接收数据读取模块的数据并调用低功耗嵌入式可信软件栈的 SM3 哈希接口 lp_tcm_hash_sm3 对接收到的数据进行哈希计算；TCM 度量值扩展模块负责将本次的度量值计算结果拓展至 TCM 的平台配置寄存器中，从而确保度量结果的安全存储与可追溯性。如图 4 所示。

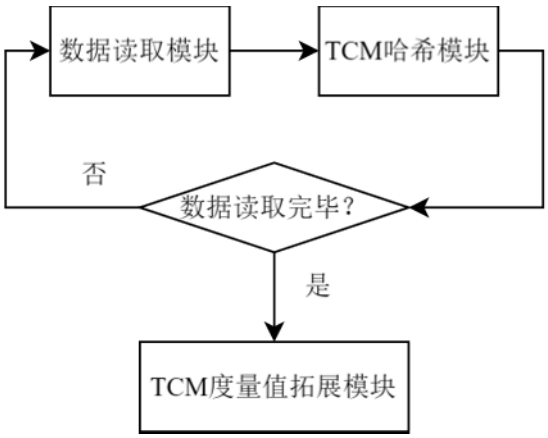


图4　可信启动方法架构图

在算法实现层面，为了适应低功耗嵌入式设备小 RAM 的特点，本文采用基于密码分组链接模式的轻量完整性度量算法。这一设计将数据读取与哈希运算过程融合，每读取一块数据即实施哈希计算，并将前一块数据的哈希结果作为下一块数据哈希运算的输入，从而实现对 RAM 资源的高效利用，如图 5 所示。

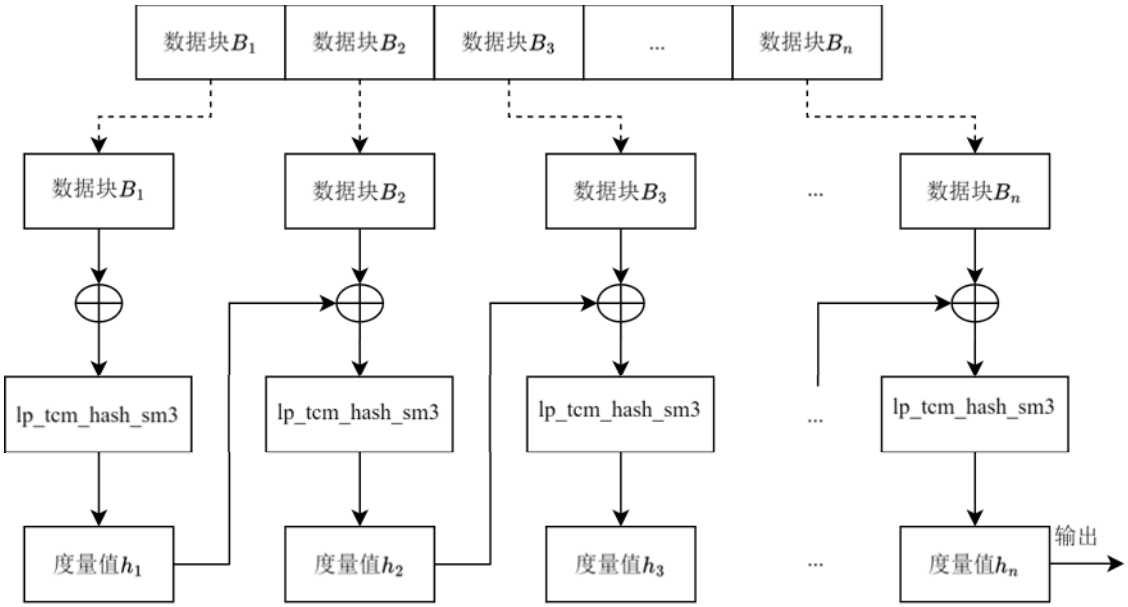


图5　轻量完整性度量算法

基于低功耗嵌入式可信软件栈的轻量可信启动方法的具体步骤如下：

（1）设备内部硬件度量：引导程序收集设备内部的硬件信息，包括主板 MCU 的序列号MCU_{id}、闪存的序列号$Flash_{id}$，并调用低功耗可信软件栈的 SM3 哈希接口 lp_tcm_hash_sm3，按照公式 1 计算设备内部硬件信息的度量值h_1。

$$h_1 = lp_tcm_hash_sm3(MCU_{id} \| Flash_{id}) \tag{1}$$

（2）设备固件信息度量：引导程序根据设备闪存中存储的固件的开始地址$addr$和数据块大小$size$，按照轻量完整性度量算法 1 计算设备固件信息的度量值h_2。

（3）设备外部挂载硬件度量：引导程序收集设备上挂载的外部硬件信息$Peripheral_{id}$并调用低功耗嵌入式可信软件栈的 SM3 哈希接口 lp_tcm_hash_sm3，按照公式 2 计算外部挂载硬件的度量值h_3。

$$h_3 = lp_tcm_hash_sm3(Peripheral_{id}) \tag{2}$$

（4）综合度量：引导程序调用低功耗嵌入式可信软件栈的 SM3 哈希接口 lp_tcm_hash_sm3，按照公式 3 计算综合度量值Z：

$$Z = lp_tcm_hash_sm3(h_1 \| h_2 \| h_3) \tag{3}$$

（5）度量值拓展：引导程序调用低功耗可信软件栈中的 PCR 拓展接口 lp_tcm_pcrextend 将本次的综合度量值Z拓展到 TCM 的 PCR 中。

（6）度量值验证：引导程序调用低功耗可信软件栈的 PCR 读取接口 lp_tcm_pcrread 读取本次的完整性度量值和 TCM 中预先存储的完整性度量值，检查两者是否相同。如果相同则启动成功，否则启动失败。

算法 1　轻量完整性度量算法

Input:　数据块开始地址 addr，数据块大小 size

Output:　度量值h_2

Begin

1:　初始化 tem，h_2

2:　**for** p ← addr to size - 1 **do**

3:　　tem ← flash_func_read_word(p) // 读取 Flash 中的数据

4:　　h_2 ← lp_tcm_hash_sm3(h_2 + tem) // 计算前一块数据与本块数据的度量值

5:　**end for**

6:　**return** h_2

End

4　实验测试

4.1　实验平台

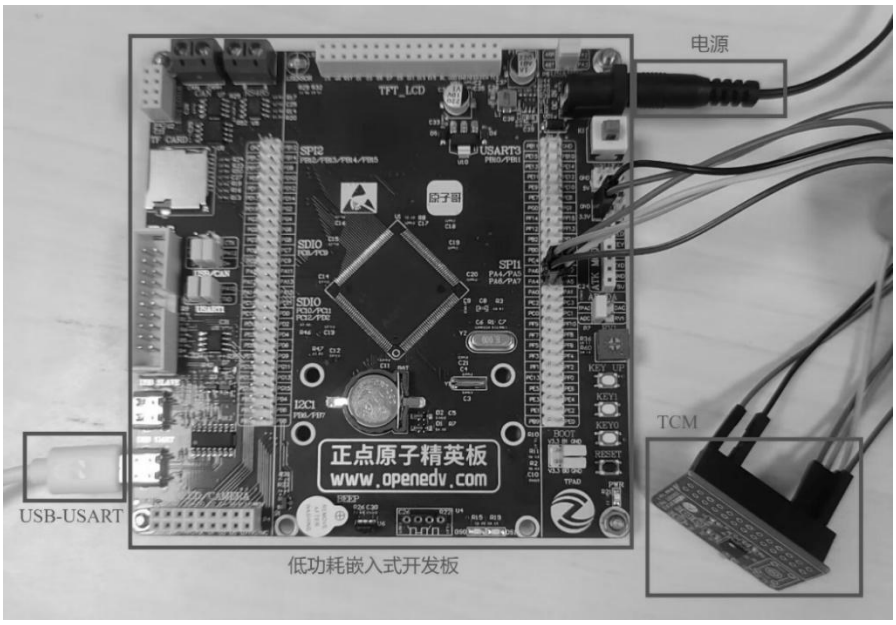


图6　软件栈测试平台接线图

如图 6 本文实验运行在 STM32F103 开发板上，并配备了实体 TPM 芯片 NationZ Z32H320TC[18]。STM32F103 采用 ARM Cortex-M3 架构的处理器，主频为 72MHz，具有 128KB 的 Flash。TPM 芯片 Z32H320TC 遵循 TPM 2.0 标准并兼容 TCM 规范，通过 SPI 接口与 STM32F103 连接，并支持 SHA256、SM3、AES256、SMS4 等多种安全算法。

4.2 功能测试

为了验证低功耗嵌入式可信软件栈的基本功能，本文测试了部分具有代表性的可信接口的时间开销，并将其与部署在高性能树莓派4B上的TPM2-TSS进行对比，实验结果如表2所示。

表 2 软件栈实验结果（单位：ms）

可信接口功能	低功耗软件栈耗时	TPM2-TSS 耗时	可信接口功能	低功耗软件栈耗时	TPM2-TSS 耗时
SM3 哈希	77	不支持	SHA256 哈希	76	226
SM4 密钥生成	804	不支持	RSA 密钥生成	816	15718
SM4 加密	54	不支持	RSA 加密	74	248
SM4 解密	256	不支持	RSA 解密	287	734
PCR 拓展功能	60	78	PCR 读取功能	43	70

在对国产 TCM 的支持方面，本文的低功耗嵌入式可信软件栈能够有效执行 TPM2-TSS 不支持的国密算法，如 SM3 和 SM4。在对低功耗设备的支持方面，本文的低功耗嵌入式可信软件栈支持超低功耗的嵌入式设备，且无需操作系统的支持。在时间开销方面，与 TPM2-TSS 相比，本文的低功耗嵌入式可信软件栈时间开销平均减少了 58.98%。

4.3 安全性分析

为了验证基于低功耗可信软件栈的轻量可信启动方法的安全性，本文设计以下两个实验。

固件篡改攻击测试：工业无人系统的系统固件被攻击者替换，其他硬件和软件均正常。

挂载替换攻击测试：工业无人系统的挂载设备被恶意攻击者替换，其他硬件和软件均正常。

首先，对未遭受任何攻击的工业无人系统进行可信启动，结果如图 7 所示。TCM 中预存储的系统正确度量值与新计算的主控硬件和固件度量值一致，可信启动成功。

```
pi@boat01:~/trust_start $ sudo python3 trust_start.py
成功连接到无人航行器!
舰载计算机正在向主控发送指令，请求计算主控硬件和固件的度量值
舰载计算机，接收到主控硬件和固件的度量值: 1f061c46ae259e95d1b90297babbd4404c1ee517a4d01aaefa558112d2ff81d5
舰载计算机的度量值: c4a740126088899ca0131ad47421c552ff3e1943eb2f68288f39d96174772df7
舰载计算机与主控混合计算出最终的度量值: 0dc59b28ecfa72f806441c88a195039a87e084324e05c56360776657157ac27b
将最终的度量值，与TCM模块中的预先值，进行比对验证中
将此次开机启动的摘要值，扩展到TCM的PCR寄存器中，并进行读取PCR值,PCR_Value: 10EA6E0B0AEC8A6A58D80D873CA1C0C8D28E1C112B83429F59C5496971C81B36
TCM中预先设定的正确的开机度量值,True_Value: 10EA6E0B0AEC8A6A58D80D873CA1C0C8D28E1C112B83429F59C5496971C81B36
>>> 【验证成功】，舰载计算机开始向主控发送指令，请求启动航行!
>>> 启动成功!
```

图7 工业无人系统可信启动成功

固件篡改攻击测试实验中，工业无人系统的固件被攻击者恶意替换，此时对工业无人系统进行可信启动，结果如图 8 所示。TCM 中预存储的系统正确度量值与新计算的主控硬件和固件度量值不符，因此无

法正常启动。

```
pi@boat01:~/trust_start $ sudo python3 trust_start.py
成功连接到无人航行器!
舰载计算机正在向主控发送指令，请求计算主控硬件和固件的度量值
舰载计算机，接收到主控硬件和固件的度量值: 2cdc9bd2ef0e83f9921c088b0a81fe566f4022066f14c032b436704adaa07646
舰载计算机的度量值: c4a740126088899ca0131ad47421c552ff3e1943eb2f68288f39d96174772df7
舰载计算机与主控混合计算出最终的度量值: 6d8e177b482c74413815f7f38173fcb1980e06b6b9b6e82288a55f792ee17e47
将最终的度量值，与TCM模块中的预先值，进行比对验证中
将此次开机启动的摘要值，扩展到TCM的PCR寄存器中，并进行读取PCR值,PCR_Value: E02689249C10A5251E54FC054BB9E049F06D386785B581473E725DFBA8458B28
TCM中预先设定的正确的开机度量值,True_Value: 10EA6E0B0AEC8A6A58D80D873CA1C0C8D28E1C112B83429F59C5496971C81B36
>>>  【验证失败】，无法正常启动!
```

图8　工业无人系统固件被替换后可信启动结果

挂载替换攻击测试实验中，工业无人系统的外挂传感器被攻击者恶意替换，此时对工业无人系统进行可信启动，结果如图 9 所示。新计算的主控硬件和固件度量值在该实验中也发生了变化，因此设备无法正常启动。

```
pi@boat01:~/trust_start $ sudo python3 trust_start.py
成功连接到无人航行器!
舰载计算机正在向主控发送指令，请求计算主控硬件和固件的度量值
舰载计算机，接收到主控硬件和固件的度量值: 1f061c46ae259e95d1b90297babbd4404c1ee517a4d01aaefa558112d2ff81d5
舰载计算机的度量值: 3d5b056bd68efadfcf70fa253ca2ce3be9ca98b52ae1eff9a6ac9922b2f27b0b
舰载计算机与主控混合计算出最终的度量值: c0afdcb2479a8cc50341a7cdac4bf04e781e409cd4d3915834cbcc799abe51d4
将最终的度量值，与TCM模块中的预先值，进行比对验证中
将此次开机启动的摘要值，扩展到TCM的PCR寄存器中，并进行读取PCR值,PCR_Value: AC065A92E7D39257C3EAE36E52D31C53BA7564B9AEB07BFF079052C6018EAF4C
TCM中预先设定的正确的开机度量值,True_Value: 10EA6E0B0AEC8A6A58D80D873CA1C0C8D28E1C112B83429F59C5496971C81B36
>>>  【验证失败】，无法正常启动!
```

图9　工业无人系统挂载替换后可信启动结果

4.4　性能测试

为了测试基于低功耗嵌入式可信软件栈的轻量可信启动方法的性能，本文测试不同固件大小下基于低功耗可信软件栈的轻量可信启动方法的时间开销，测试结果如表 3 所示。

表 3　可信启动时间（单位：ms）

固件大小	（1）	（2）	（3）	（4）	总时间
1KB	128.88	123.79	127.14	151.38	531.19
16KB	125.48	124.49	127.05	153.18	530.2
32KB	126.95	149.93	128.72	152.2	557.8
64KB	124.92	151.82	126.02	151.34	554.1
128KB	127.6	154.92	125.81	151.55	559.88
256KB	125.89	160.16	125.58	152.61	564.24
480KB	128.39	165.99	125.95	151.24	571.57

表 3 中序号与可信启动方法的阶段对应如下：（1）表示设备内部硬件度量阶段；（2）为设备固件信息度量阶段；（3）是设备外部挂载硬件度量阶段；（4）为综合度量阶段。通过实验结果可以发现，随着固件大小的提升，硬件信息和板载数据采集及哈希值计算和拓展步骤的时间开销也随之提升。同时，固件大小不影响设备内部硬件度量和设备外部挂载硬件度量的时间消耗。尽管随着固件大小的提升，总耗时有所提升，但其最多也仅有 571.57 毫秒，耗时较短，不影响工业无人系统的正常启动。

5　结束语

本文针对现有 TPM2-TSS 无法应用于低功耗嵌入式设备的问题和现有的可信启动方法不适用的问题，

设计并实现了面向低功耗嵌入式设备的可信软件栈和轻量可信启动方法，该软件栈可以有效保证低功耗嵌入式设备的稳定运行和数据安全。但是，该软件栈还存在一定的局限性，例如：低功耗嵌入式可信软件栈目前支持的可信功能偏少，没有实现 TCM 芯片所支持的所有功能。因此，未来工作中，本文所设计的低功耗可信软件栈功能需要进一步扩展。

参考文献：

[1] 於志渊. 基于嵌入式虚拟机技术的物联网终端安全解决方案及架构[J]. 数字化用户, 2020(32): 0160-0163.

[2] 崔传文. 嵌入式系统在物联网时代的应用[J]. 现代工业经济和信息化, 2022, 12(12): 168-170.

[3] 郭晨雪, 王超, 姬胜凯. 可信计算信任链技术研究[J]. 网络安全技术与应用, 2023(06): 19-20.

[4] TPM2 Software Community. Linux TPM2 & TSS2 Software [EB/OL]. [2023-11-10]. https://github.com/tpm2-software.

[5] 王鹃, 樊成阳, 程越强等. SGX 技术的分析和研究[J]. 软件学报, 2018, 29(9): 2778-2798.

[6] 赵波, 袁安琪, 安杨. SGX 在可信计算中的应用分析[J]. 网络与信息安全学报, 2021, 7(6): 126-142.

[7] Perez R, Sailer R, van Doorn L. vTPM: virtualizing the trusted platform module[C]//Proc. 15th Conf. on USENIX Security Symposium. 2006: 305-320.

[8] Wang J, Xiao F, Huang J, et al. A security-enhanced vTPM 2.0 for cloud computing[C]//Information and Communications Security: 19th International Conference, ICICS 2017, Beijing, China, December 6-8, 2017, Proceedings 19. Springer International Publishing, 2018: 557-569.

[9] 田洪亮. 云环境下基于可信硬件的数据机密性保护技术研究[D]. 北京: 清华大学, 2019.

[10] 胡俊, 刁子朋. vTCM:一种基于物理可信计算环境虚拟化的虚拟可信密码模块[J]. 山东大学学报(理学版), 2019, 54(07): 77-88.

[11] 张立强, 吕建荣, 严飞等. 可信云计算研究综述[J]. 郑州大学学报(理学版), 2022, 54(04): 1-11.

[12] Choi B C, Lee S H, Na J C, et al. Secure firmware validation and update for consumer devices in home networking[J]. IEEE Transactions on Consumer Electronics, 2016, 62(1): 39-44.

[13] Lu D, Han R, Shen Y, et al. xTSeH: A trusted platform module sharing scheme towards smart IoT-eHealth devices[J]. IEEE Journal on Selected Areas in Communications, 2020, 39(2): 370-383.

[14] Zhao H, Xu C, Zhou F. Research on embedded startup method of trusted module[C]//2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2021, 5: 953-957.

[15] 高爽. 主动配电网信息安全防护关键技术研究[D]. 北京: 华北电力大学, 2019.

[16] 张磊. 电力物联网下的采集终端可信计算技术研究[J]. 电子元器件与信息技术, 2019, 3(12): 113-116.

[17] 高昆仑, 辛耀中, 李钊等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化, 2015, 39(01): 48-52.

[18] 国民技术股份有限公司. Z32H330TC 可信计算芯片[EB/OL]. [2023-11-10]. https://www.nationstech.com/Z32H330TC/.

[作者简介]

杨轩（2002—），男，硕士研究生，主要研究方向为嵌入式系统安全、云计算安全。

马承彦（1994—），男，博士，主要研究方向为无人系统安全、可信计算。

习宁（1986—），男，博士，西安电子科技大学教授、博士生导师，主要研究方向为括异构网络融合安全、服务组合安全、信息流安全等等。

基于多特征融合的工业时序异常检测方法

乔怡群，刘克新，王田

摘　要：工业互联网中存在着众多复杂的时序数据流，这些数据流通常蕴含着多种周期性模式和变量间的相关性。及时检测并识别数据流中存在的异常模式对于确保生产系统的高效运行至关重要。然而,由于数据的异质性和高维特征，构建一个能够有效捕捉异常特征的模型仍然是一项挑战。为解决上述问题，本文提出了一个多特征融合的工业时序异常检测方法。所提出的特征提取框架通过时序、周期多模块协同，全面地提取时序数据的复杂特征，提升了异常检测的性能。实验结果表明我们方法可以取得较好的精度。

关键词：工业互联网；数据分析；时序数据

Industrial timing anomaly detection method based on multi-feature fusion

Qiao Yiqun, Liu Kexin, Wang Tian

Abstract: Industrial Internet is characterized by numerous complex time-series data streams, which usually contain multiple periodic patterns and correlations between variables. Timely detection and identification of anomalous patterns present in data streams are crucial to ensuring the efficient operation of production systems. However, due to the heterogeneity and high dimensionality of the data, it is still a challenge to construct a model that can effectively capture the anomalous features. To address the above issues, this paper proposes a multi-feature fusion approach for industrial time-series anomaly detection. The feature extraction framework proposed in this paper comprehensively extracts the complex features through the multi-module synergy of temporal, period, and channel, and enhancing the accuracy of anomaly detection. The experimental results show that the method can achieve better accuracy.

Key words: Industrial Internet of Things (IIOT), Data analysis, Time series data

1　引言

现代制造业正经历巨大飞跃，工业互联网将设备、机器和系统紧密融合，汇聚物联网技术、大数据、云计算和人工智能等多种技术手段，推动工业设备和系统的智能化互联[1]。设备运行数据通过传感器连续采集，蕴含工业设备的状态信息，为预测维护[2]和决策优化提供了依据。因此，时间序列分析在工业领域备受关注。

异常检测是一种识别数据异常模式的分析技术，在工业领域尤为关键，能够及时发现设备或系统的潜在异常状况[3]。时序数据通常可以体现时间连续性与变化特征。然而，现实场景下的时序数据往往包含多种频率和波动叠加，这使得其建模过程复杂并具有挑战性。

近年来，许多研究者提出了一系列的工作应用于时序的异常检测。一类方法采用的是基于循环神经网

络（Recurrent Neural Network，RNN）及其变体**错误!未找到引用源。错误!未找到引用源。**对时序特征进行提取。尽管上述方法尝试捕捉时序数据的时间依赖性，但对于较长序列来说，其捕获能力有限。与此同时，由于这些方法的计算范式是基于顺序的，因此在效率方面也不高。近些年提出了基于注意力机制（Attention mechanism）的方法**错误!未找到引用源。**[7]来获取时间上的依赖关系。虽然这些方法擅长捕捉不同时间点之间的关联性，然而现实世界中的时序数据往往含有多个周期。这些不同的周期特征往往交织在一起，形成复杂的内在模式。然而，现有的注意力机制方法通常难以很好地捕捉和利用这些周期性模式，从而可能影响模型对数据内在特征的有效提取和表。

考虑到建模时间序列中众多的动态变化和相互依赖关系是一项挑战。这包括但不限于周期性时间依赖性、周期之间的相互作用等。现实世界的时序数据通常包含着复杂的、多重周期性特征。这些因素叠加作用使得简单的模型很难胜任。虽然研究人员在领域取得了一些进展，然而有效的时间序列建模方法仍然是个开放性的问题。

为了处理数据中复杂的变化和依赖关系，本文提出了一种新的多特征融合（Mulit-Feature Fusion，MFF）异常检测方法，通过捕获时间序列中存在的不同的周期性信息与不同的依赖关系来进行异常检测。基于时间序列的多周期性，通过多个周期的信息，提升对时间序列不同粒度下的周期信息的理解。考虑到特定周期下的表征的多样性，分别针对时序上的特征、周期间的特征进行提取，从而更加细致地捕捉时间序列的动态变化规律。最终将提取的所有特征进行融合，从而充分利用数据中的信息。

本文的主要贡献概括如下。

（1）我们提出了一种名为 MFF 的新框架，用于执行工业时间序列的异常检测。MFF 方法采用了周期的自然特性，以增强对于不同时间尺度周期性的理解和分析。

（2）其次，我们设计了若干特征提取模块，用于从多个维度提取特征，这包括时序数据本身的特征，周期之间的关联特征。这些模块的设计是互补的，它们通过多维分析相互配合，旨在全面抓取和理解数据的复杂动态。此方法不只提升了特征提取的效果，同时也增加了对数据内潜在异常的检测能力。

（3）我们在数据集上的实验结果表明，所提出 MFF 方法的有效性。此外，通过消融实验进一步验证了各个模块设计的必要性，每个模块都在提升整体性能方面起到了关键作用。

2　模型的建立

如前文所述，为了捕获多元时间序列的不同特征，我们提出了 MFF 方法在不同的尺度上对数据进行表征。本小节将首先介绍总体的框架结构，随后分别介绍各个模块。

2.1　总体框架

在异常检测任务中，给定多元的时序数据序列 $\mathbf{X}=[\mathbf{x_1},\mathbf{x_2},...,\mathbf{x_h}]^{\mathrm{T}}\in\mathbb{R}^{h\times d}$，$\mathbf{x_i}\in\mathbf{X}$ 代表每个时间步的维

度是 d 。目标是评估时间序列 t 中的数据点是否展现出异常行为。我们介绍的 MFF 模型被设计为如图 1 所示结构。输入模型的多维数据张量首先通过周期提取模块确认周期，随后经过多尺度特征提取模块处理。这一模块由两部分构成：一部分负责抽取与时间序列相关的特征，而另一部分则专注于提取周期性特征；这些模块并行工作以捕捉数据在不同层次上的特性。最后，使用聚合的方法将不同尺度的特征以及不同周期下的特征进行聚合与映射，得到最终融合后的特征。

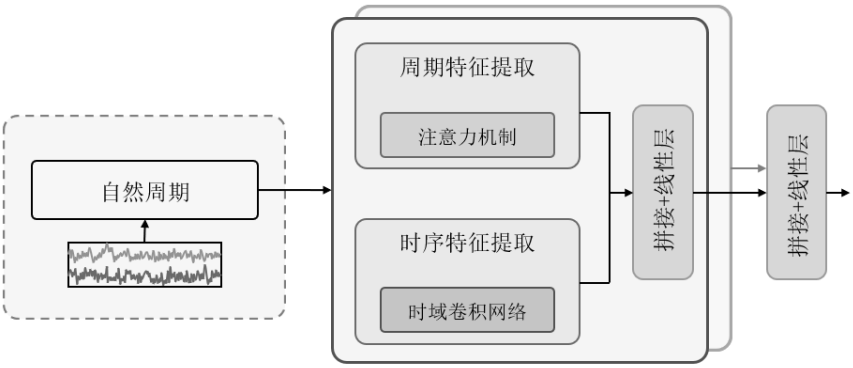


图 1　模型的整体框架图

2.2　周期提取模块

在进行多周期提取时，我们考虑具有明显意义的自然频率作为周期参考。根据选择的频率 $F=\{f_1,...,f_k\}$，我们可以确定出频率对应的周期 T 如下。

$$T=\{t_1,...,t_i,...,t_k\},t_i=[h/f_i]$$

其中，h 代表序列的长度。t_k 代表的是数据中的第 k 个周期。一般而言，k 是一个人为选定的参数。随后，将得到的张量分别送入到时序特征提取模块（Temporal Feature Extraction, TFE）、周期特征提取模块（Cyclical Feature Extraction, CFE）中。

2.3　周期注意力机制

周期性在时间序列分析中扮演着一个至关重要的角色，因为它揭示了数据潜在的模式和行为。在周期提取模块提取到时序不同的周期后，将此信息导入到一个注意力模块以探究各个周期成份的相互关系。对于输入到注意力机制中的张量，我们先对其进行重塑，使其符合注意力机制的输入格式。随后，该机制将被用来揭示周期成份间的相互作用。进一步地，通过两层卷积网络，我们能够捕捉到更加详细的局部特征关系。相应的计算公式如下所示。

$$\hat{\mathbf{X}}_{cs}^{i}=Reshape(\mathbf{X})$$

$$\mathbf{X}_{cs1}^{i}=Attention(\hat{\mathbf{X}}_{cs}^{i},\hat{\mathbf{X}}_{cs}^{i},\hat{\mathbf{X}}_{cs}^{i})$$

$$\mathbf{X}_{cs1}^{i}=Layernorm(\hat{\mathbf{X}}_{cs}^{i}+Dropout(\mathbf{X}_{cs1}^{i}))$$

$$\mathbf{X}_{cs2}^{i} = Dropout\left(Relu\left(Conv_1\left(\mathbf{X}_{cs1}^{i}\right)\right)\right)$$

$$\mathbf{X}_{cs}^{i} = Reshape(Dropout(Conv_2(\mathbf{X}_{cs2}^{i})))$$

其中，Attention 代表的是对于 $\hat{\mathbf{X}}_{cs}^{i}$ 做自注意力的操作。$Conv_1$ 和 $Conv_2$ 代表的是采用卷积核为 1 的一维度卷积，沿着 $\mathbf{X}_{cs1}^{i}$ 的周期方向维度进行卷积。$\mathbf{X}_{cs2}^{i}$ 将从 $\mathbb{R}^{t_i \times \{f_i \times d\}}$ Reshape 到维度 $\mathbb{R}^{t_i \times f_i \times d}$。$\mathbf{X}_{cs}^{i}$ 是周期注意力模块的最终输出。

2.4　时序特征提取模块

对于时序之间的时间依赖关系，我们采用 TCN 网络进行特征提取，通过这种网络结构，我们能够捕捉长时间范围内的数据模式和时间相关性，从而提高模型的性能和对复杂时间序列数据的理解能力。具体计算的公式如下。

$$\hat{\mathbf{X}}_{s}^{i} = Transpose(\mathbf{X})$$

$$\mathbf{X}_{s}^{i} = Transpose(Tcn(\hat{\mathbf{X}}_{s}^{i}))$$

其中，$Transpose$ 代表对元素进行维度的转换，$\mathbf{X}_{s}^{i}$ 为时序提取模块最终的输出。

2.5 特征聚合模块

各自从时序特征提取模块（TFE）、周期特征提取模块（CFE）提取到的特征是 $\mathbf{X}_{s}^{i}$，$\mathbf{X}_{cs}^{i}$。这些特征首先经过形状调整操作以使尺寸统一，接着把调整尺寸后的特征经由拼接操作组合在一起，然后应用一个线性层对它们进行预测性的映射，从而实现了从几个不同模块提取的特征的融合。具体的计算公式如下所示。

$$\mathbf{X}_{ps}^{i} = Reshape\left(\mathbf{X}_{ps}^{i}\right) \in \mathbb{R}^{h \times d}$$

$$\mathbf{X}^{i} = Linear\left(concat(\mathbf{X}_{cs}^{i}, \mathbf{X}_{s}^{i})\right)$$

其中，$\mathbf{X}^{i}$ 是投影后得到的张量，其维度为 $\mathbb{R}^{h \times e}$。其中，e 的维度是设定的一个参数。

接着，将各个频率层面上的特征聚合结果输入到一个多尺度融合模块，完成在 k 个不同频率尺度的特征的补充与强化。这一策略能够产出比任何单一尺度特征更为综合的数据洞察。详细的运算过程展示如下。

$$\mathbf{X}^{o} = concat(\mathbf{X}^{1}, ..., \mathbf{X}^{i}, ..., \mathbf{X}^{k}), i \in \{1, 2, ..., k\}$$

$$\mathbf{X}^{O} = Linear(\mathbf{X}^{o})$$

其中，$\mathbf{X}^{o}$ 为融合后的多尺度特征的输出，维度为 $\mathbb{R}^{h \times \{k \cdot e\}}$。$\mathbf{X}^{O}$ 为多尺度融合模块的最终输出，维度是 $\mathbb{R}^{h \times d}$。

3　实验分析

在本章节中，将通过实验来衡量我们所提出的 MFF 方法的有效性。首先在 3.1 小节介绍数据集与数据集的预处理，3.2 小节描述了任务的评价指标，3.3 小节对算法的结果与有效性等不同的方面进行分析，并进行算法的一些讨论。

3.1 基本描述

本部分主要选取 SMAP 数据集进行实验的验证。对于读取的数据，首先进行 Z-score 归一化处理。该归一化方法通过减去均值并除以标准差的方式调整数据分布，降低由于数据在较大范的分布不平衡导致的对模型结果的影响。其计算公式如下所示。

$$X_{norm} = \frac{X - \mu}{\sigma}$$

其中，X 是原始数据值，μ 为数据的均值。

3.2 评价指标

实验中采用精确率，召回率，F1-score 和准确率作为衡量模型性能的指标。各个指标的计算公式如下。

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Precision 评估了模型预测为异常的数据点中真正异常的比例。Recall 衡量了模型能捕获的真实异常数据点占所有真实异常数据点总数的比例。F1-score 取 Precision 和 Recall 的调和平均值。一个较高的 F1 值预示着模型在 Precision 和 Recall 之间取得了一种较为均衡的性能表现。

3.3 实验结果与分析

在本小节中，我们将全面介绍实验结果，并进行详细分析，包括算法的对比、消融实验、算法运行时间分析。

3.3.1 对比实验

本小节将我们所提出的 MFF 方法和其他的方法（Crossformer[8]、Dlinear[9]、Informer[10]）在异常检测任务上的性能进行了对比，结果如表 1 所示。

表 1 不同的方法性能对比

方法（Methods）	Precision	Recall	F1-score
Dlinear	0.9232	0.5541	0.6926
Informer	0.9011	0.5713	0.6992
Crossformer	0.9204	0.5537	0.6914
Ours	0.9229	0.5770	0.7101

如表 1 所示，为我们所提出的方法与其他主流技术在性能上的比较。通过实验，展示出我们的方法在与其他现有的基于 former 的技术以及依赖于线性层次模型如 Dlinear 的方案的比较中，表现出较为卓越的检测效果，达成了 0.7101 的 F1 分数。这些基于 former 的方法在不同周期性特征的捕捉上存在不足，我们的模型却通过一种精心构建的机制，更有效地识别了时序数据中的周期性模式与时序的特征，从而增强了异常检测的准确度

3.3.2　消融实验

为了考察各个模块的有效性，我们进行了以下情况的对比研究：1）去掉 CFE 结构，2）去掉 TFE 结构。我们在数据集上进行了比较。从实验结果可以看出，在去掉 CFE 模块后，模型的 F1 降低为 0.6928，在去掉 TFE 模块后，模型的 F1 降低为 0.6939。移除任一组成部分后，发现模型在异常检测上的效能明显下滑。这些模块各自从不同的角度进行特征抽取和表现，比如提炼时序数据特征和揭示周期性特征从而增加了模型对异常的检测灵敏度。这证实了各个独立部分都对总体检测效能做出了正面贡献，保留这些单独的组成模块是必要的，印证了模型设计的合理性。

表 2　分别去掉各个模块的结果

Method	Precision	Recall	F1-score
Remove CFE	0.9223	0.5547	0.6928
Remove TFE	0.9220	0.9220	0.6939

我们还尝试了对各模块输出的特征执行平均操作以实现特征整合。实验结果如表 3 所示。从表中的结果可以看出，使用平均方法后的模型 F1 得分为 0.6929，这个分数低于采用拼接（Concat）方法的结果 0.7101。这说明拼接操作在保持和整合各个部分提供的特征方面表现得更加出色。

表 3　采用求平均的方法进行特征的聚合

Method	Precision	Recall	F1-score
Mean	0.9221	0.5550	0.6929
Concat	0.9229	0.5770	0.7101

3.3.3 算法运行时间分析

我们在 GPU 和 CPU 硬件平台上分别进行了算法运行时间的实验。在 GPU 上单次的异常检测时间可以达到 5ms，在 CPU 上不超过 18ms。在实际应用中，传感器通常按秒间隔采样信号。这表明，本文介绍的 MFF 算法能够高效并即时识别信号的异常状况，由此该算法在实际应用场合展现出了显著的应用潜力。

表 4　模型以及各个模块的运行时间

Module	GPU	CPU
MFF	0.0048s	0.017066s
CFM	0.0005864s	0.0026155s
TFM	0.0005806s	0.00157080s

表 4 中列出的算法运行时间，是基于模块在处理流程中依照特定序列逐步执行的情况下进行的实时测量。需要指出的是，设计出的模块具备并行处理能力。我们对每个核心模块的执行时长进行了单独评估。CFE 模块以及 TFE 在 GPU 上的运行时间约为 6ms，CFE 模块在 CPU 上的运行时间约为 2.7ms，TFE 模块在 CPU 上的运行时间约为 1.6ms。这些不同模块在经过适当优化后能够实现并行工作，这将有助于减缩模型在硬件上的操作时间，进而促进其在实际环境中的应用效率

4　结束语

本研究提出了一种融合多特征的工业异常监测技术，称为MFF，它可以从多种维度提取序列特性。更确切地说，这种技术结合了周期性特征的提取以及时序依赖性的提取，通过几个不同的组件来捕获数据的固有结构，从而辨别出正常与异常的行为模式。随后，将这些多维度特征通过一个特征聚合模块进行聚合，以形成一个全面的特征表示。该方法的优势在于不仅汇集了各单一模块的优点，并且通过综合多种维度的信息，有效提高了模型在识别和区分异常行为时的性能。

在未来的研究中，我们将进一步对特征提取与局部表征进行探索，同时将致力于模型的实际应用，与工业界合作，以实现模型在现实世界工业系统中的部署。

参考文献：

[1] Sisinni E, Saifullah A, Han S, et al. Industrial internet of things: Challenges, opportunities, and directions[J]. IEEE transactions on industrial informatics, 2018, 14(11): 4724-4734.

[2] Wu H, Xu J, Wang J, et al. Autoformer: Decomposition transformers with auto-correlation for long-term series forecasting[J]. Advances in neural information processing systems, 2021, 34: 22419-22430.2774-2797.

[3] Shaukat K, Alam T M, Luo S, et al. A review of time-series anomaly detection techniques: A step to future perspectives[C]//Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 1. Springer International Publishing, 2021: 865-877.

[4] Nanduri A, Sherry L. Anomaly detection in aircraft data using Recurrent Neural Networks (RNN)[C]//2016 Integrated Communications Navigation and Surveillance (ICNS). Ieee, 2016: 5C2-1-5C2-8.

[5] Malhotra P, Ramakrishnan A, Anand G, et al. LSTM-based encoder-decoder for multi-sensor anomaly detection[J]. arXiv preprint arXiv:1607.00148, 2016.

[6] Zhang Y, Ma L, Pal S, et al. Multi-resolution Time-Series Transformer for Long-term Forecasting[C]//International Conference on Artificial Intelligence and Statistics. PMLR, 2024: 4222-4230.

[7] Liu Y, Hu T, Zhang H, et al. itransformer: Inverted transformers are effective for time series forecasting[J]. arXiv preprint arXiv:2310.06625, 2023.

[8] Zhang Y, Yan J. Crossformer: Transformer utilizing cross-dimension dependency for multivariate time series forecasting[C]//The eleventh international conference on learning representations. 2023.

[9] Zeng A, Chen M, Zhang L, et al. Are transformers effective for time series forecasting?[C]//Proceedings of the AAAI conference on artificial intelligence. 2023, 37(9): 11121-11128.

[10] Zhou H, Zhang S, Peng J, et al. Informer: Beyond efficient transformer for long sequence time-series forecasting[C]//Proceedings of the AAAI conference on artificial intelligence. 2021, 35(12): 11106-11115.

[作者简介]

乔怡群（1994—），男，博士生，主要研究方向为工业互联网、机器学习等。

刘克新（1988—），男，2016 年中国科学院大学获得博士学位，教授，主要研究方向为工业互联网、复杂网络等。

王田（1987—），男，2014 年法国特鲁瓦技术大学获得博士学位，副教授，主要研究方向是计算机视觉与模式识别。

融合注意力机制的 3D 打印缺陷检测算法

张俊杰[1]，沈震[1]，方启航[1]，董西松[1]（通信作者），王迪[2]，熊刚[1]

1. 中国科学院自动化研究所，北京 100190；2. 华南理工大学，广州 510641

摘　要：3D 打印技术，作为增材制造的现代形式，在众多行业中发挥着重要作用。尽管如此，参数配置不当和机械疲劳等问题常常导致打印过程中出现缺陷，这些缺陷会显著影响最终产品的性能。鉴于 3D 打印部件通常具有复杂和高度优化的几何形状，传统的检测技术难以满足其对精确性和效率的要求。为解决这一难题，本文提出了一种基于改进版 YOLOv5 的 3D 打印缺陷检测算法。该算法对 YOLOv5 模型进行了深入改进，通过替换损失函数和引入注意力机制，成功实现了模型的轻量化。新设计的检测系统以较小的参数规模、快速的推理速度、高检测精度和强大的鲁棒性为特点。与原始的 YOLOv5s 模型相比（检测精度 93.3%，参数规模 7.6M，数据大小 14.4MB），改进后的轻量化模型在检测精度上达到了 94.2%，同时在参数规模和数据大小上分别减少至 3.6M 和 7.7MB，几乎减半。这一进步不仅提升了检测效率，还为 3D 打印缺陷检测与故障诊断提供了一种更为有效的技术手段。

关键词：3D 打印；缺陷检测；深度学习；YOLOv5；注意力机制①

A 3D Printing Defect Detection Algorithm Incorporating Attention Mechanism

Junjie Zhang[1], Zhen Shen[1], Qihang Fang[1], Xisong Dong[1](Corresponding Author), Di Wang[2], Gang Xiong[1]

1.Institute of Automation, Chinese Academy of Sciences, Beijing 100190;

2.South China University of Technology, Guangzhou 510641

Abstract: 3D printing technology, as a modern form of additive manufacturing, plays a significant role across various industries. Despite this, improper parameter configuration and mechanical fatigue often lead to defects during the printing process, which can significantly impact the performance of the final product. Given that 3D printed parts typically have complex and highly optimized geometric shapes, traditional detection technologies struggle to meet the demands for precision and efficiency. To address this challenge, this paper introduces a 3D printing defect detection algorithm based on an improved version of YOLOv5. The algorithm makes extensive refinements to the YOLOv5 model, achieving model lightweighting by replacing the loss function and introducing an attention mechanism. The newly designed detection system is characterized by a smaller parameter scale, rapid inference speed, high detection accuracy, and strong robustness.Compared to the original YOLOv5s model (with a detection accuracy of 93.3%, a parameter scale of 7.6M, and a data size of 14.4MB), the improved lightweight model has achieved a detection accuracy of 94.2%, and has nearly halved the parameter scale and data size to

①基金项目：国家自然科学基金（92267103，92360307）

3.6M and 7.7MB, respectively. This advancement not only enhances detection efficiency but also provides a more effective technical solution for 3D printing defect detection and fault diagnosis.**Key words:** 3D printing, defect detection, deep learning, YOLOv5, attention

1　引言

3D 打印技术，作为一种创新的增材制造方式，正在引发一场工业变革。它通过逐层堆叠材料来创建三维物体，已经在制造业、医疗、建筑、教育等多个领域得到广泛应用。3D 打印不仅加快了产品从设计到原型的进程，还通过按需定制生产，显著提高了生产效率和降低了成本，推动了产业创新。

尽管 3D 打印技术具有巨大潜力，但其制造过程中的复杂性也带来了挑战。使用不当的材料、不适宜的打印参数设置、打印机的故障或环境因素，都可能导致打印过程中出现孔洞、裂纹等缺陷，影响成品的质量和性能。

因此，针对 3D 打印过程中的实时情况检测尤为重要，及时发现缺陷的出现并立即报警，能很大程度上减轻材料的浪费，并可以对缺陷形成的原因分析提供实时性材料。对打印过程中的缺陷进行检测的研究对本行业的发展和提高成品性能具有重要意义。

目前在缺陷检测方向的研究主要如表 1 所示：

表 1 主要研究方向

研究方向	核心技术
工业互联网技术	参考文献[1]：通过预测特征层、K-means++聚类、CAM 和相似度量改进工业互联技术，提高 S-YOLOv5s 检测精度 4.92%。
	参考文献[3]：应用深度卷积和编码于故障预测和诊断，实现信号采集和云端故障检测。
计算机视觉	参考文献[2]：结合工业互联网和计算机视觉，提升轮辋焊缝检测效率和精度。
	参考文献[5]：结合工业互联网和深度学习，提出改进的目标检测模型。
	参考文献[6]：提出视觉显著性和阈值融合的缺陷分割方法。
	参考文献[7]：自动检测和分类刀具表面缺陷。
	参考文献[8]：结合 CNN 和 SVM，提出纺织品深层特征提取和缺陷分类方法。
	参考文献[9]：基于 TensorFlow 的 Faster-RCNN 算法，用于铆钉缺陷检测。
	参考文献[10]：提出改进网络结构和优化损失函数的缺陷检测算法，提高检测精度。
	参考文献[11]：使用 ResNet50 和特征金字塔网络检测 PCB 小缺陷。
	参考文献[12]：提出基于自适应注意力融合的 AC-YOLO 网络，用于绝缘子多缺陷检测。
机器学习	参考文献[4]：利用工业互联网数据，建立 AI 模型，提高电网负荷管理和 PCB 缺陷检测精度。

在现代工业检测领域，工业互联网技术、计算机视觉和机器学习已成为提升检测精度和效率的关键技术。通过集成预测特征层、改进聚类算法、上下文增强模块和优化的相似度量方法，如文献[1]、[3]所述，S-YOLOv5s 检测精度实现了近 5%的提升。深度卷积和编码技术在故障预测与诊断中的应用，如文献[3]所述，为信号采集和云端故障检测提供了新的解决方案。计算机视觉的结合，特别是在文献[2]、[5]中提到的各种深度学习模型和方法，显著提高了从轮辋焊缝到 PCB 缺陷的检测能力。此外，机器学习技术，如文献[4]所述，通过分析工业互联网数据，有效提升了电网负荷管理和 PCB 缺陷检测的精度。这些研究成果不仅展示了跨学科技术融合的潜力，也为 3D 打印等新兴制造技术的缺陷检测提供了宝贵的参考和启示。

尽管目标检测技术在多个工业领域取得了显著进展，如在金属材料表面缺陷检测、PCB 印刷电路板瑕疵识别以及手工艺品质量评估中展现出较高的准确性和效率，但在 3D 打印这一新兴且快速发展的领域，现有技术仍面临诸多挑战。如参考文献[5]主要针对的是传统制造业产品表面缺陷的检测，此类缺陷的特点是多样性较低，形状样式较为单一，对模型的泛化能力和鲁棒性要求不高。

然而，3D 打印过程中可能出现的缺陷类型多样，包括但不限于孔洞、裂纹、层间剥离等，这些缺陷的检测需要对模型的几何形状和打印过程有深刻的理解，例如图 1(b)与(d)在形状，面积，周围纹理等方面差异巨大，对模型的抽象特征提取能力和鲁棒性提出了更高的要求。现有的目标检测技术多针对特定目标和环境优化，缺乏对 3D 打印特有缺陷的泛化能力，难以实现精准识别。

针对这一问题，本研究提出了一种创新的算法框架，旨在填补 3D 打印缺陷检测领域的空白。本框架利用工业互联网的实时数据传输优势，结合深度学习模型在特征提取方面的先进性，开发出一套适合 3D 打印特点的缺陷检测系统。主要针对的是打印件平面上可能出现的缺陷类型，如裂缝、孔隙、离型膜脱落。

通过本研究的努力，我们期望能够为 3D 打印行业提供一种新的技术手段，提高缺陷检测的自动化水平，减少人工干预，从而提升生产效率和产品质量。同时，该研究也将推动目标检测技术在更广泛领域的应用和发展。

2 方法

2.1 数据预处理

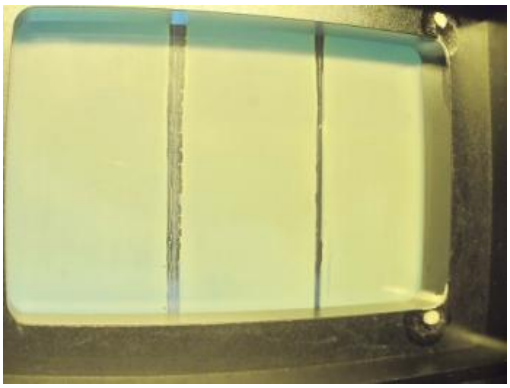
本文选用的数据集是来自中国科学院自动化研究所实验室 3D 打印机打印过程中出现的各种情况：故障，严重错误，损坏，加上正常组成的含有四种情况的数据集，分类标准及数量如表 2 所示：

表 2 种类界定标准及数量

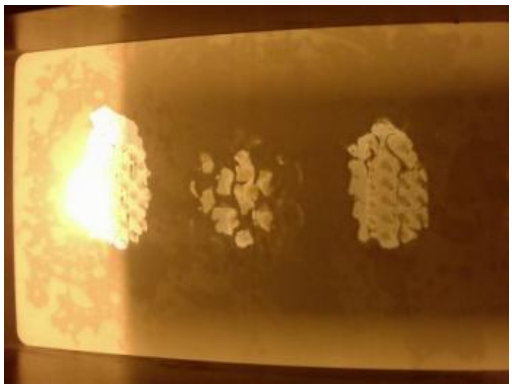
图片种类	界定标准	处理方法	数量
故障	出现 1~2 道不显眼划痕	目标检测	190
严重错误	连续五张以上划痕位置相同	报警暂停	94

损毁	离型膜脱落或大面积空洞	报警暂停	9
正常	无异常	正常打印	260

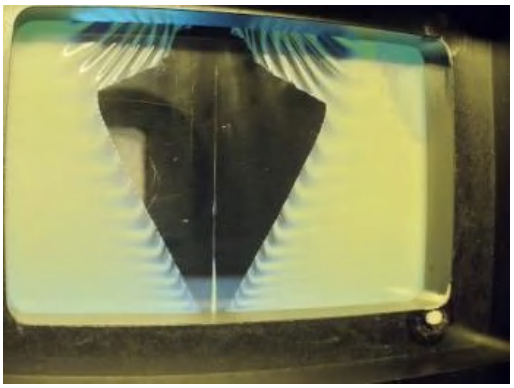
(a)正常



(b)故障



(c)严重错误



(d)损毁

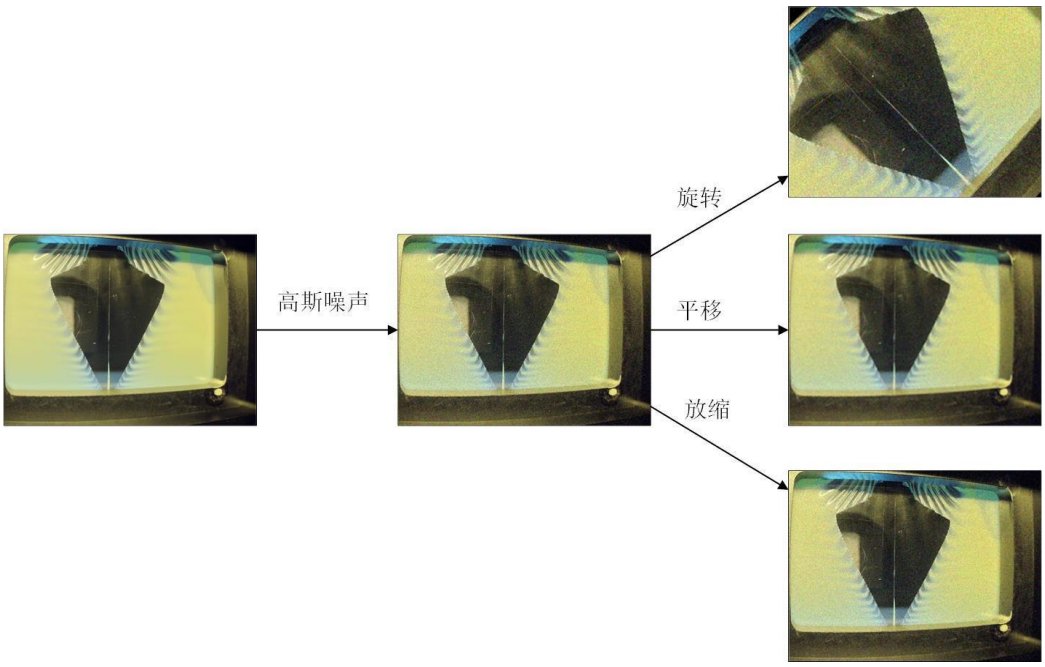
图 1 四种情况

数据增强（Data Augmentation）是指在机器学习和深度学习中通过对原始数据进行一系列变换来生成新的训练样本的技术。对图像进行旋转操作的数学原理如下公式，设像素点在图片坐标轴上的坐标的 $P(x_0, y_0)$，连线为 OP，与 X 轴的夹角为 α，使其绕轴旋转角 β 后的新坐标为 $P(x, y)$。

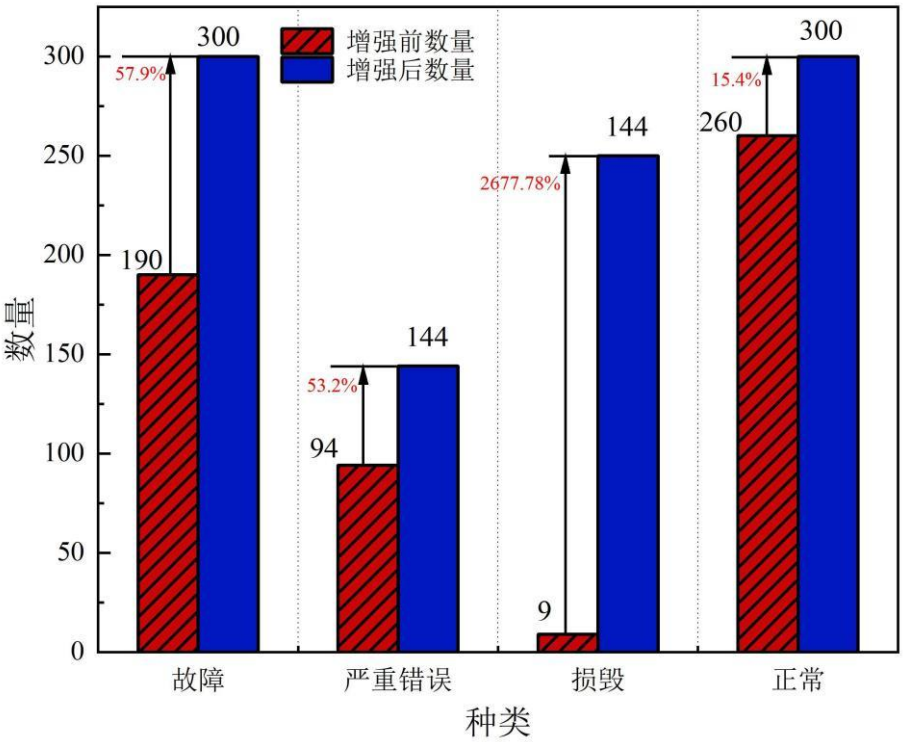
$$\begin{cases} x_0 = r \cdot \cos a \\ y_0 = r \cdot \sin a \\ x = \cos \cdot (\alpha - \beta) \\ y = \sin \cdot (\alpha - \beta) \end{cases} \tag{1}$$

$$\begin{bmatrix} 1 \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\beta & \sin\beta & 0 \\ -\sin\beta & \cos\beta & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ y \\ 1 \end{bmatrix} \tag{2}$$

通过几何变换的处理方法在数据增强中应用最简单也最广，但是此方法本质上并没有改变图像内容，容易造成数据样本不丰富，鲁棒性下降等影响。故此本文在几何变换的基础上采用了颜色变换进行数据增强，向数据集中加入随机高斯噪声，一定程度上可以提高模型鲁棒性，具体如图 2 所示：



(a)数据增强方法



(b)数量对比

图 2 数据集增强前后对比

2.2 网络架构

C3 模块

YOLOv5 中的 C3 模块是指“Cross Stage Partial Network”，其目的是增强深度学习神经网络的感受能力和特征表征能力，方便后续更好地进行目标检测。

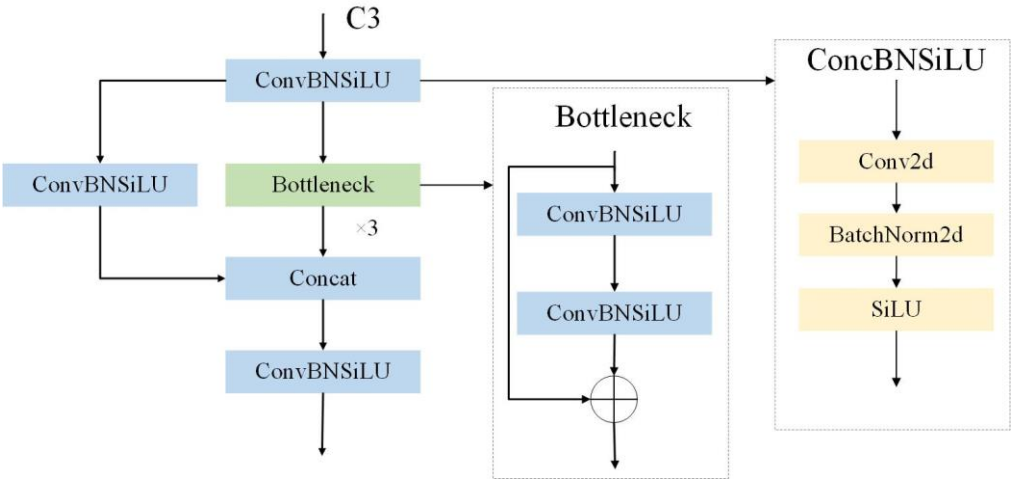


图 3 C3 模块示意图

SPPF 模块

Spatial Pyramid Pooling Fast Module (SPPF) 模块是在 Spatial Pyramid Pooling (SPP) 的基础上创新，将池化的操作由并联改为串联，如图 4 所示。

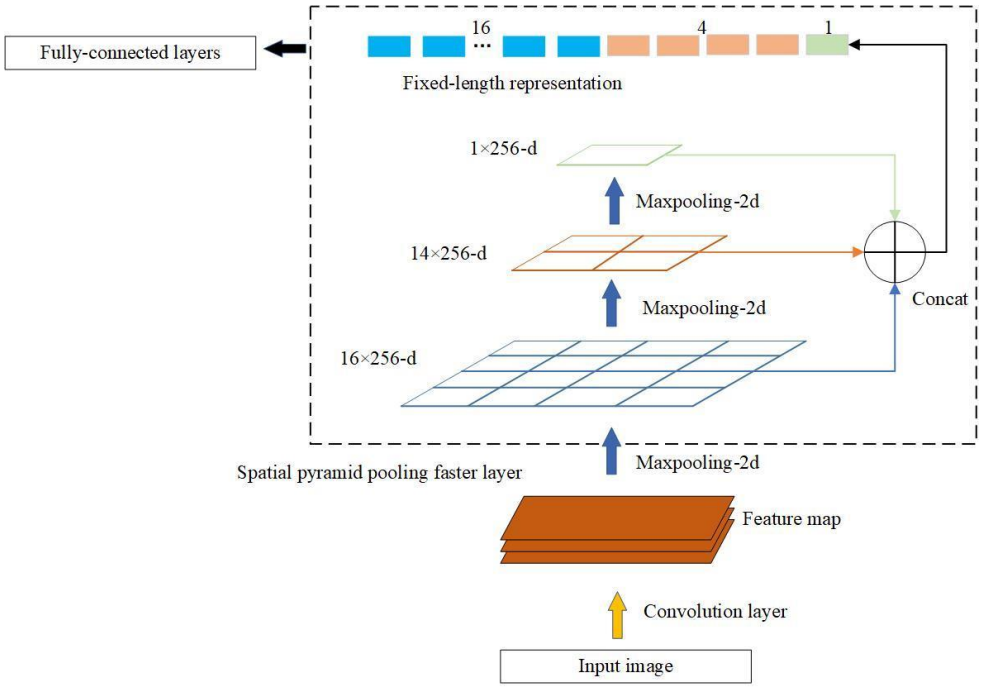


图 4 SPPF 模块示意图

2.3 替换 IoU 损失函数

IoU 全称 Intersection over Union 是一种用于定量化测定指定数据集中对目标物体检测精度的一种函数，损失函数用于边界盒预测，它将预测盒的四个边界作为一个整体单位进行回归。一般情况下，凡是输出中存在一个预测框的任务都可以使用该种函数[13]。

GIoU(Generalized Intersection over Union)相较于 *IoU* 能在更广义的层面上计算 *IoU*，其创新点在于弥

补了 *IoU* 在检测框与真实框没有重叠的情况下，通过引入一个广义的版本作为一个新的损失和一个新的度量标准来解决 *IoU* 的弱点，巧妙地解决了检测框和真实框没有重叠的问题[14]。

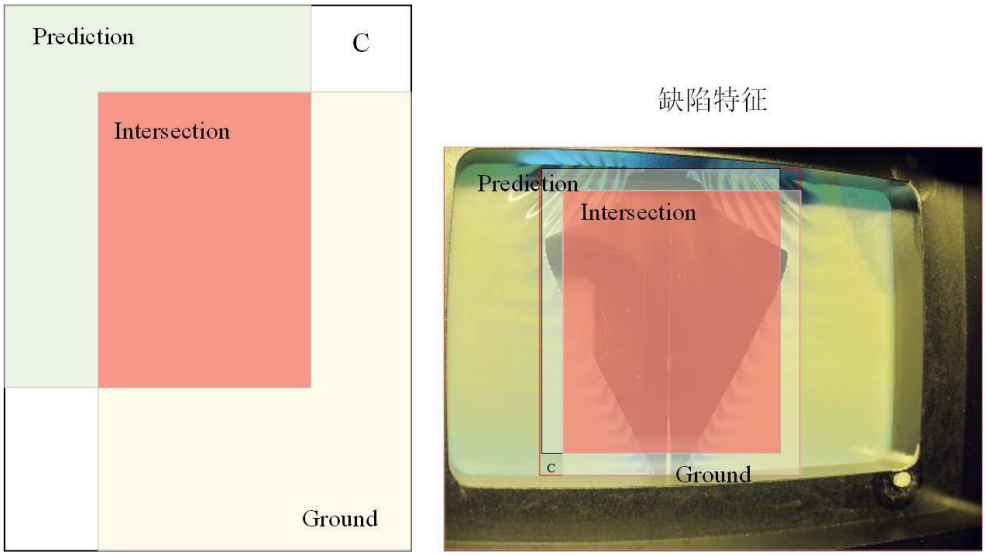


图 5 GIoU 判断原理图

如图 5 所示，预测框记为 Prediction 框，真实框记为 Ground 框，紫色的记为最小封闭框 C，计算 C 框中除去预测框与真实框的面积再除以 C 框的面积，这个比值即为 *GIoU*，如（3）所示：

$$L_{GIoU} = 1 - IoU + \frac{|C - (A \cup B)|}{|C|} \tag{3}$$

DIoU(Distance Intersection over Union)考虑到 *GIoU* 的缺点，其计算的不再是交并比的面积，而是检测框与真实框之间的欧氏距离，通过结合预测框和目标框之间的归一化距离的距离（*DIoU*）损失，它在训练中比 *IoU* 和 *GIoU* 损失收敛得快得多[15]。如图 6 所示：

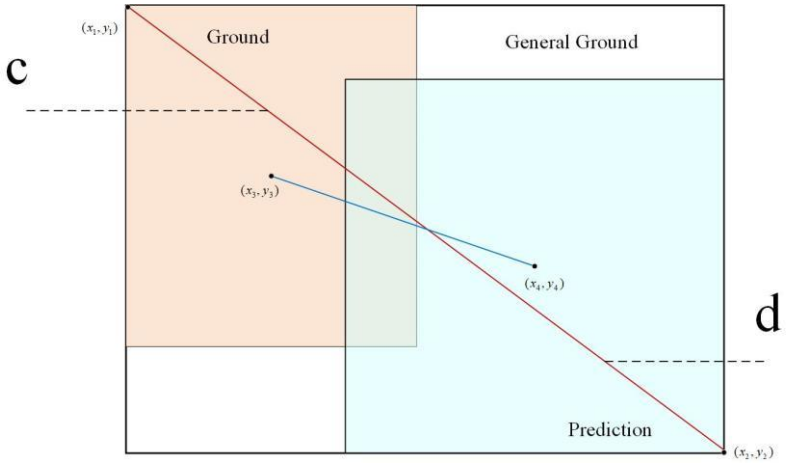


图 6 DIoU 计算原理图

DIoU 比 *GIoU* 更加符合目标框的回归机制，将预测框与真实框之间的面积问题转化为距离问题，更加符合现实世界中生物对目标的位置的捕捉过程，使目标框的回归变得更加的稳定。

$$DIoU = \frac{\rho(A, B)^2}{c^2} \tag{4}$$

其考虑了重叠面积和中心点的距离，当真实框包含预测框时，*DIoU* 直接度量的是两个框的距离，因此相较于 *GIoU*，*DIoU* 更具有收敛性。

CIoU(Complete Intersection over Union)在 *DIoU* 的基础上额外增加了检测框的尺度的损失，通过提高了长和宽的损失，促进了目标框的稳定性进一步提高[15]，避免了像 *IoU* 和 *GIoU* 中出现的发散问题。

$$L_{CIoU} = 1 - IOU(A, B) + \rho\left(A_{ctr}, B_{ctr}\right)^2 / c^2 + \alpha v \tag{5}$$

$$v = \frac{4}{\pi^2} \times (\tan^{-1}(\frac{w^{gt}}{h^{gt}}) - \tan^{-1}(\frac{w}{h}))^2 \tag{6}$$

$$\alpha = \frac{V}{(1 - IoU) + v} \tag{7}$$

式中　A，B 两个框，A_{ctr}-A 框的中心，　B_{ctr}-B 框的中心点。

EIoU(Enhanced Intersection over Union)主要包括三个部分，*IoU* 损失，distance 损失，横框比损失，其相对于 *CIoU* 的创新点在于引入了横框比损失函数，该损失函数直接定量化地描述了预测框与真实框的差异，相较于 *CIoU*，*EIoU* 的收敛速度与定位效果更胜一筹[16]。

$$L_{EIoU} = L_{IoU} + L_{dis} + L_{asp}$$

$$= 1 - IoU + \frac{\rho(b, b^{gt})^2}{c^2} + \frac{\rho(\omega, \omega^{gt})^2}{c_\omega^2} + \frac{\rho\left(h, h^{gt}\right)^2}{c_h^2} \tag{8}$$

其中 *w* 和 *h* 是预测边界框与真实边界框的最小外接矩形的宽度和高度。*p* 是两点之间的欧氏距离.

SIoU(Square Intersection over Union)考虑到期望回归之间向量的角度，重新定义角度惩罚度量，它可以使预测框快速漂移到最近的轴，随后则只需要回归一个坐标（X 或 Y），这有效地减少了自由度的总数[17]。其原理如图 7 所示：

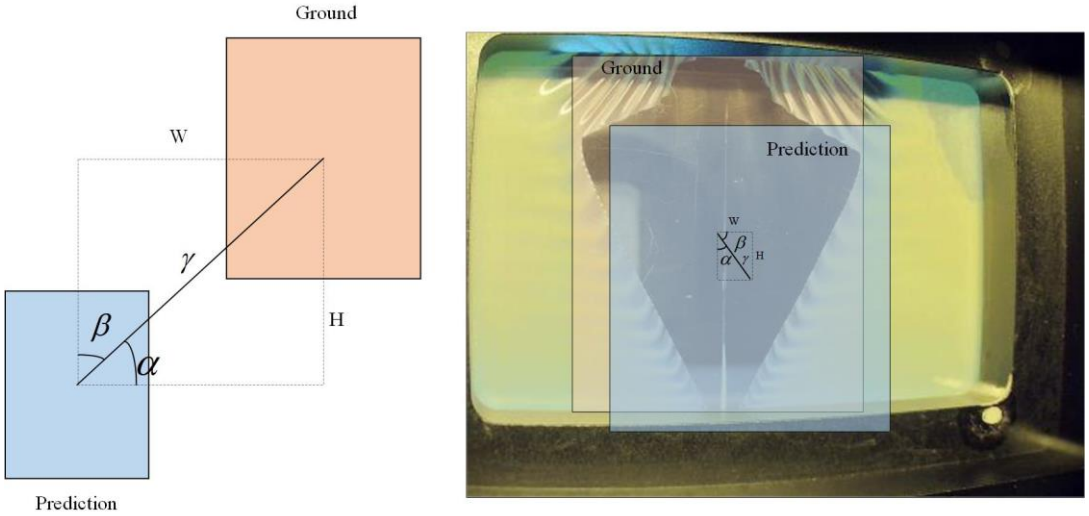


图 7 SIoU 判断原理图

角度损失：当 P 框与 G 框在 x 轴或者 y 轴上中心点对齐时，即图 3.10 中 α 角为 0 或者 β 角为 0 时，其角度损失函数如（9）所示，返回值为 0，代表预测框与真实框的角度损失为 0，在角度维度高度重合，为预测框进一步逼近真实框提供了新的依据标准。

$$\Delta = 1 - 2 \times \sin((\sin^{-1}\theta) - \frac{\pi}{4}) \tag{9}$$

2.4 注意力机制的引进

注意力机制允许模型在不同尺寸和类型的缺陷上进行有效的检测，提高了模型对新数据的泛化能力，可以帮助模型更加关注图像中的关键区域。本文通过在改进损失函数的 YOLOv5s 模型的基础上再引入 SimAM(Simple Attention Module with Adaptively-weighted Multi-inputs)、SE-Attention(Squeeze-and-Excitation Attention)，Shuffle-Attention 注意力机制，并设置对照试验测定本数据集的最佳匹配的注意力机制。

引入 SimAM 注意力机制：SimAM 是一种用于卷积神经网络的虽然概念比较简单却十分有效的注意力机制模块，通过优化一个能量函数来发现每个神经元的重要性，推导出一种能量函数的封闭的解，且此解可以通过不到 10 行代码实现[18]。其一大创新点在于不用向原始网络模块中添加通道数，也就是无需匹配原网络中的通道数，可以自由地加入网络中任何一层，避免了在调整结构上花费大量精力。

为了寻找最简单神经元，度量神经元之间的线性可分性，SimAM 中定义了如（10）的能量函数，最后可化简为（11）.

$$e_t(w_t, b_t, y, x_i)\,(y_t - \hat{t})^2 + \frac{1}{M-1}\sum_{i=1}^{M-1}(y_o - \hat{x}_i)^2 \tag{10}$$

$$X = sigmoid(\frac{1}{E}) \otimes X \tag{11}$$

在原网络架构头部的第 10 层与第 11 层，第 12 层与第 13 层，第 21 层与 22 层之间加入 SimAM 模块，无需输入接收通道数，如图 8 所示：

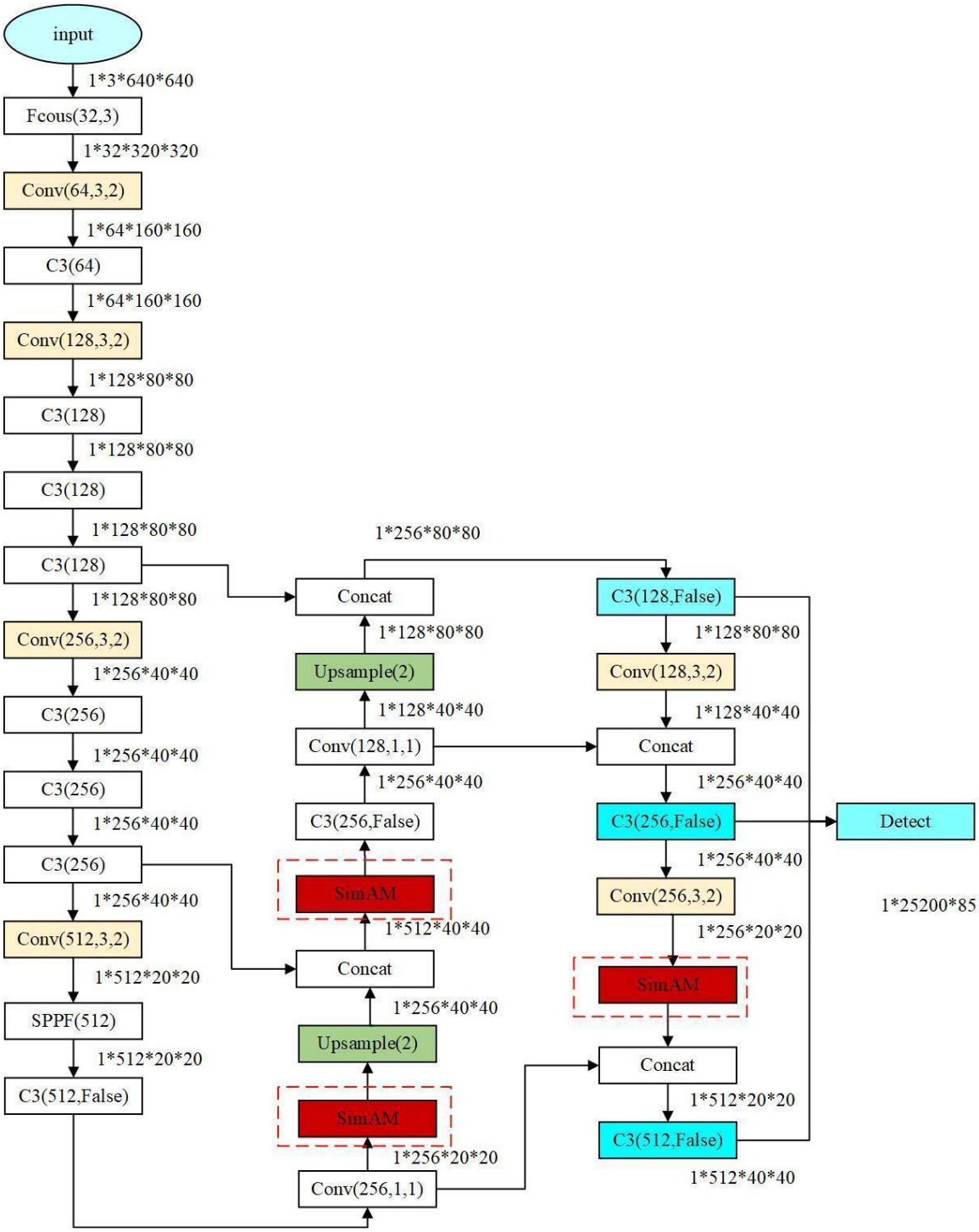


图 8 插入层级示意图

引入 SE 注意力机制：SE Block 并非是一个完整的网络，而是一个子结构，一般用于嵌套在其他分类模块中，其核心思想是根据 loss 的趋势去设置一个使有效的特征图的权重更大，无效或者效果很小的特征图的权重更小的权重分布去训练模型[19]。其操作为将输入的特征图进行一次标准的卷积操作，进行全局平均池化，将前两部所得特征图使用 ReLU 函数激活，乘以线性层后通过 Sigmoid 函数转化为 0-1 分布值，具体如图 9 所示。

$$F_{tr}: X \to U, X \in R^{W' \times H' \times C'}, U \in R^{W \times H \times C} \tag{12}$$

$$u_c = v_c \times X = \sum_{s=1}^{C'} v_c^s \times x^s \tag{13}$$

$$z_c = F_{sq}(u_c) = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} u_c(i,j) \tag{14}$$

$$s = sigmoid(W_2 \times \mathrm{Re}LU(W_1 z)) \tag{15}$$

$$x = F_{scale}(u_c, s_c) = s_c \times u_c \tag{16}$$

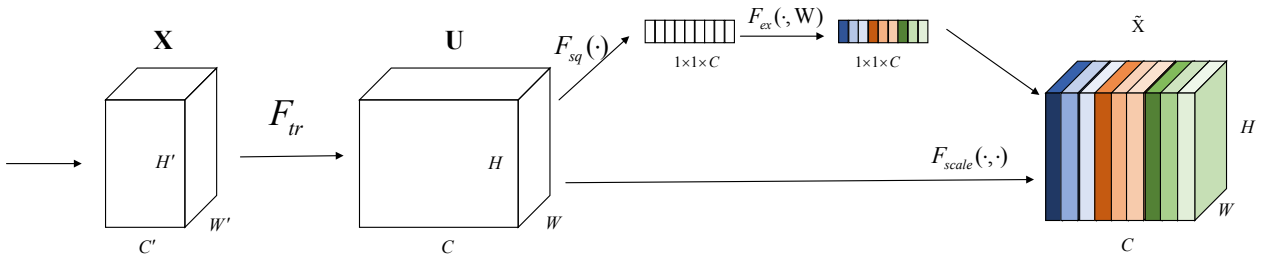


图 9 SE 注意力机制示意图

Qing-Long Zhang 和 Yu-Bin Yang 引入了一种称为 Shuffle Attention 的机制，它融合了通道和空间注意力机制，以增强特征表示[20]。首先使用全局平均池化 GAP 处理输入信息，生成通道统计数据，然后使用一个门控机制配合 sigmoid 激活函数，生成紧凑特征，公式如（18），最后使空间维度与通道维度的注意力机制互补。

$$s = F_{gp}(X_{k1}) = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} X_{k1}(i,j) \tag{17}$$

$$X_{k1}' = \sigma(F_c(s)) \cdot X_{k1} = \sigma(W_1 s + b_1) \cdot X_{k1} \tag{18}$$

$$X_{k2}' = \sigma(W_2 \cdot GN(X_{k2}) + b_2) \cdot X_{k2} \tag{19}$$

2.5 模型轻量化

传统的 YOLOv5 网络架构中，主干网络使用的是 C3 网络架构，其由 3 个 Conv 层，3 个 BottleNeck 与一个 Concat 组成，结构较为复杂，导致模型在推理过程中的计算量大幅度增大，为了解决这个问题，本文更换 YOLOv5 的主干网络与头部网络，引入 Ghostnet 网络架构，作为主干和头部网络的基础组成模块，以达到精简模型结构和减少参数量和加快推理速度的目的。

Ghostbottleneck 是由 Ghost 模块堆叠而成，Ghost 是一种即插即用的模块，旨在使用更少的参数来生成更多的特征图，从而达到减小参数规模的目的[21]。Ghost net 提出了一种新的 Ghost Module，旨在使用一种廉价的线性变换生成更多的特征图：

对输入的特征图进行以此简单的卷积操作，生成 m=n/s 个本征特征图，Y' 为输出本征特征图，f' 为所用滤波器，生成 n 个 Ghost 特征图，通过生成的 m 个本征特征图，对其每一个通道都进行 cheap operation 再生成（s-1）个 Ghost 特征图，共计生成 m（s-1）个特征图，将第一步生成的 m 个本征特征图与第二步生成的 m（s-1）个 Ghost 特征图进行拼接，得到拼接的 m*s 个特征图为最终输出，如图 10 所示。

$$Y' = X * f' \tag{20}$$

$$y_j^i = \phi_j^i(y_i^{'}), \forall_i = 1,...,m, j = 1,...,s, \tag{21}$$

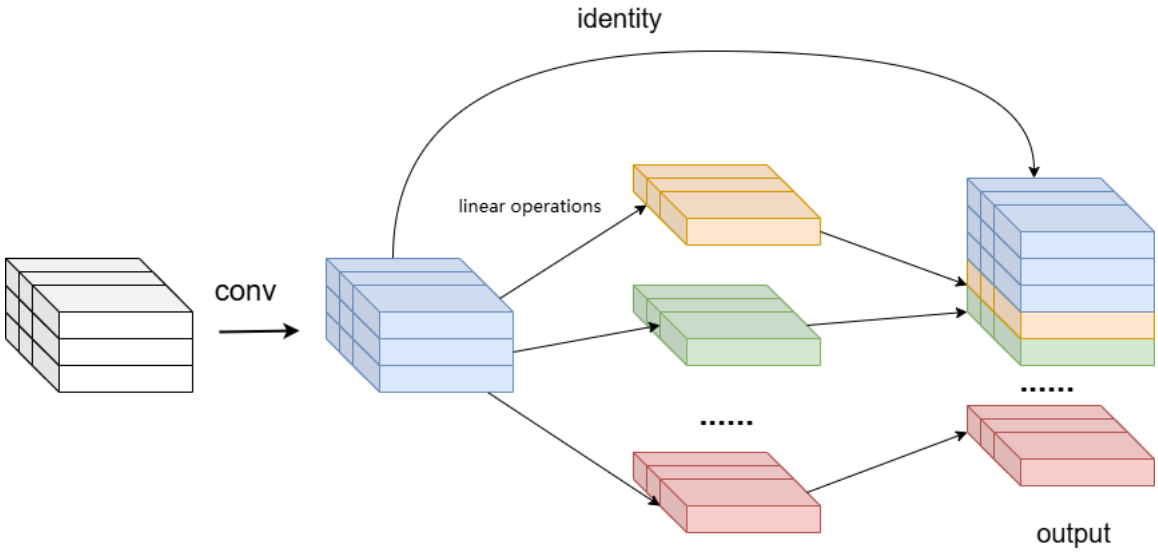


图 10 Ghost 生成特征图

最关心的计算量与参数量， Ghost Module 主要的运算在一次等价映射与 *m*（*s-1*）次廉价的线性变换。假设我们要输出 *n* 个特征图，那么就需要进 *n-m=m×(s-1)=n/s×(s-1)*次线性变换，加上原本 *m* 个本征特征图，假设每次线性变换的 kernels 为 *d×d*，卷积操作的核为 *k×k*，*d* 为超参数，那可得出 Ghost Moudle 与标准卷积的计算比为下式(22)：

$$r_s = \frac{n \cdot h' \cdot w' \cdot c \cdot k \cdot k}{\frac{n}{s} \cdot h' \cdot w' \cdot c \cdot k \cdot k + \frac{n}{s} \cdot (s-1) \cdot h' \cdot w' \cdot d \cdot d} \approx \frac{s \cdot c}{s + c - 1} \approx s \tag{22}$$

换而言之，在第一步生成本征特征图时，本征特征图生成得越少，参数规模削减的效果越好。

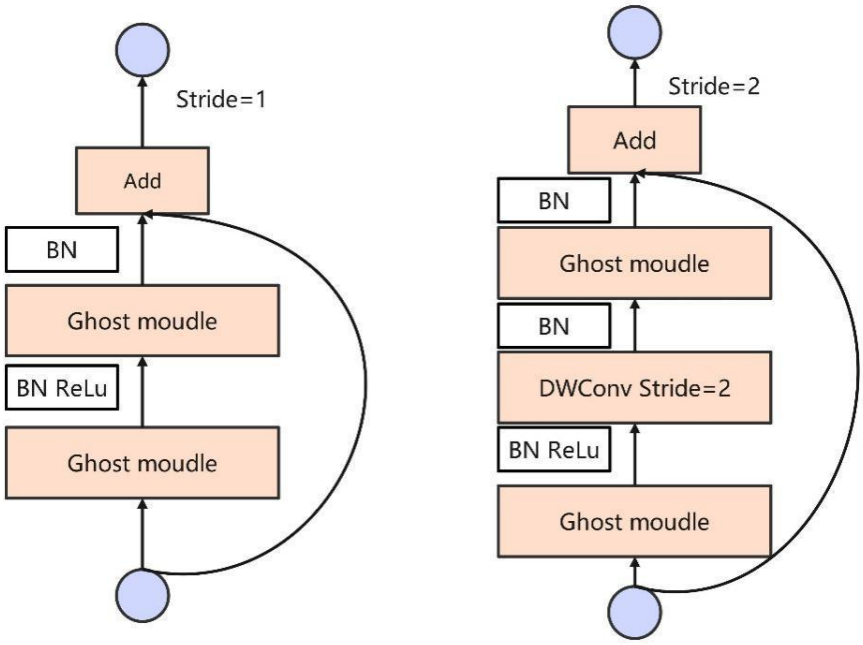


图 11 Ghost Bottle

图 11 左图为 stride=1，右图为 stride=2 的结构。当 stride=2 时，加入的 DWConv 的作用是对特征图的宽和高进行压缩，缩小到原来的 1/2，残差部分也会加入类似下采样的操作，便于 Add 操作时大小可以相匹配。

3 实验结果

3.1 替换 IoU 损失函数

本文引入了五种改进的 IoU 损失函数，并在无预训练权重的情况下，对每一种 IoU 进行三次训练，测定其 mAP 等参数，并取五次原始 YOLOv5s 模型下的平均 mAP 作为原始对照组，以此确定在本数据集前提下的最优的 IoU。

原始对照组在同样在无预训练权重的情况下训练，初始模型为 YOLOv5s 轻量级模型。训练集与验证集的比值为 2：8，经过预处理的数据集图片被设置为 480×480 大小输入模型，初始学习率设为 0.001，权重衰减为 0.0005，训练轮次为 100，批处理大小为 16。训练结果如表 3 所示。

表 3 YOLOv5s 模型无预训练权重训练结果图

指标 / 轮次	mAP_0.5	mAP_0.5:0.95	Precision	Recall
Average	0.933	0.719	0.9202	0.8906

引入五种损失函数，所有训练条件与对照组完全相同，取三次训练结果取平均值作为实验组，与对照组进行对比，结果如表 4 所示。

表 4 改进 IoU 实验结果

平均值 / IoU	mAP_0.5	mAP_0.5:0.95	Precision	Recall
GIoU	0.937	0.751	0.925	0.912
DIoU	0.939	0.751	0.927	0.913
CoU	0.941	0.754	0.929	0.930
SIoU	0.929	0.749	0.929	0.889
EIoU	0.940	0.753	0.932	0.907

CIoU 为最适配本文所用数据集的损失函数。根据其原理推测是数据集中的故障与严重错误虽然整体相似，但是故障的长宽比远大于严重错误，CIoU 损失函数敏锐地识别了这一差别，使故障与严重错误的 mAP 提高，导致整体 mAP 上升近 1%，平均 mAP 上升近 4%。

3.2 引入注意力机制

通过在引入 *CIoU* 损失函数为前提的情况下，加入 SimAM，SE-Attention，Shuffle-Attention 注意力机制，在与原始对照组相同条件下进行训练选定最佳匹配的注意力机制。

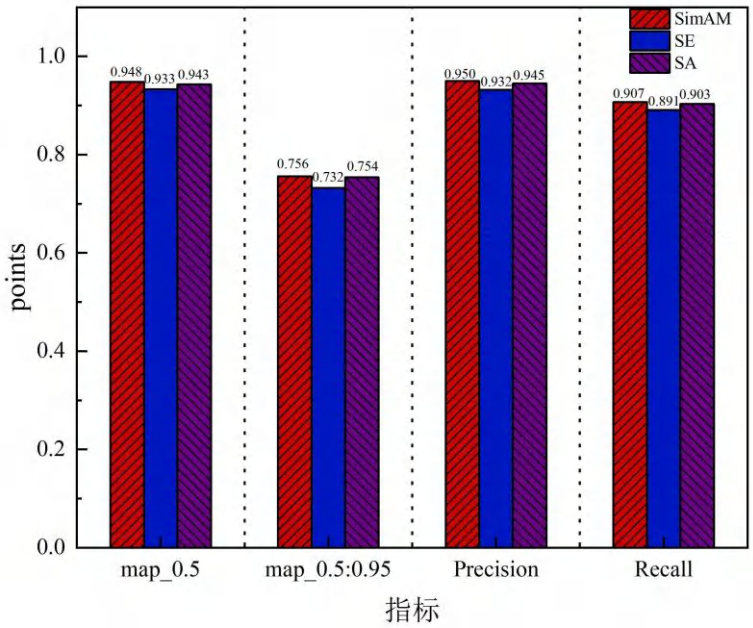


图 12 三种注意力机制对比图

综上所述，测试了不同的损失函数，注意力机制，SimAM 表现最好，推测是因为其没有通道数限制，SimAM 的实现不需要额外的参数，这使得它能够轻松地集成到现有的卷积神经网络中，用于目标检测任务。通过将 SimAM 模块添加到 Backbone 或 Neck 部分，可以捕捉特征图中的重要信息，进而提升模型的检测性能

3.3 轻量化

在改进 YOLOv5 模型的基础上，将原有的主干网络和头部改为由 Ghost Module，Conv 改为 Ghost Conv，C3 改为 Ghost C3，其他层结构不变。为确定模型改进部分（IoU 与注意力机制）对精度的提升所做的贡献，现测定原始模型与改进模型经轻量化后的模型性能，其他实验条件与第二章中的实验条件相同，实验结果如表 5 所示。

表 5 改进前后模型对比

	mAP_0.5	mAP_0.5:0.95	Precision	Recall	参数规模	GFLOPs	数据大小
改进前	0.933	0.719	0.920	0.890	7.12M	16.0	14.4MB
改进后	0.942	0.745	0.949	0.896	3.68M	8.0	7.7MB

从上表可以得出，进度相较于改进模型略有下降，但是参数规模的大幅度下降和推理速度的显著提升更显著，由此可见，网络是成功的，在丢失细微检测精度的牺牲下实现了参数规模等大幅度下降。

综上所述，针对 3D 打印缺陷检测的改进 YOLOv5 算法模型已构建完成，与 ResNet 等当前先进检测算法相比，在检测精度基本一致的情况下，模型大小实现了近半削减。

4 总结

本研究提出了一种基于改进 YOLOv5 算法的 3D 打印缺陷检测技术。使用中国科学院自动化研究所的数据集，通过优化 IoU 损失函数并引入注意力机制，显著提升了检测精度。针对特殊环境下对速度和模型大小的需求，采用 Ghost Net 实现模型轻量化，减少了参数规模，加快了推理速度，同时保持了高准确率。

研究内容包括数据增强、损失函数改进、注意力机制和模型轻量化。首先，通过数据增广扩充了初始数据集，解决了类别不平衡问题。其次，对比多种 IoU 损失函数后，选择了 CIoU，并引入了 SimAM 注意力模块以增强特征识别。最后进行模型轻量化，可实现上传至嵌入式设备等。

实验结果显示了我们改进后的算法不仅保持了高识别准确率，还在运算速度和鲁棒性方面取得了显著提升。这一成就归功于算法的优化，使得系统在面对复杂和多变的数据时，能够更加迅速和稳定地进行处理。

尽管目前我们的系统在数据集的多样性以及实际应用测试方面还有待进一步扩展，但我们已经制定了明确的未来研究方向。我们计划通过扩大数据集的范围，引入先进的图像预处理技术，并开发实时监测 3D 打印过程的算法，来克服这些局限性。

本项研究成功提升了 3D 打印缺陷检测的速度和准确性。此外，通过对模型进行有效的轻量化处理，我们确保了系统在保持高性能的同时，也易于部署和使用。这些成果为 3D 打印领域的缺陷检测技术带来了创新。

我们相信，随着技术的不断进步和数据集的日益丰富，我们的系统将能够更好地服务于 3D 打印行业，

提高生产效率，降低成本，推动 3D 打印技术的发展，为社会带来更多的价值。

致谢

感谢国家自然科学基金提供的资助，感谢多模态人工智能系统全国重点实验室对本文提供的支持。

参考文献：

[1] 喻朝新, 郭松涛, 郭佳哲. 基于工业互联技术的胶料质量缺陷检测模型构建分析[J]. 2023, 50(06): 19-22.

[2] 袁朕鑫. 工业互联网中边缘端轮辋焊缝检测系统设计与实现[D]. 济南大学, 2023.DOI:10.27166/d.cnki.gsdcc.2023.000546.

[3] 袁慧苗. 基于工业互联网的旋转机械系统状态检测与故障诊断研究[D]. 齐鲁工业大学, 2023. DOI:10.27278/d.cnki.gsdqc.2023.000412.

[4] 赵英伟. 面向工业场景的机器学习算法应用研究[D]. 电子科技大学, 2023. DOI:10.27005/d.cnki.gdzku.2023.002064.

[5] 佟星. 工业互联网场景下基于人工智能的图像和数据分析研究[D]. 广东技术师范大学, 2021. DOI:10.27729/d.cnki.ggdjs.2021.000195.

[6] 陈立君. 基于流形支持向量机的木材表面缺陷识别方法的研究[D]. 东北林业大学, 2015.

[7] 刘浩, 陈再良, 王善翔. 基于改进YOLOv3 算法的刀具表面缺陷检测[J]. 组合机床与自动化加工技术, 2021, (11): 87-90. DOI:10.13462/j.cnki.mmtamt.2021.11.021.

[8] Junhao Q, Yihua H, Jinrong C, et al. Textile Defect Classification Based on Convolutional Neural Network and SVM[J]. AATCC JOURNAL OF RESEARCH, 2021, 8 75-81.

[9] 舒琪. 基于机器视觉的铆钉筛选系统设计[D]. 西南交通大学, 2022. DOI:10.27414/d.cnki.gxnju.2022.001884.

[10] Yu Z, Lei Y, Shen F, et al. Application of Improved YOLOv5 Algorithm in Lightweight Transmission Line Small Target Defect Detection[J]. Electronics, 2024, 13 (2):

[11] Hu B, Wang J. Detection of PCB Surface Defects with Improved Faster-RCNN and Feature Pyramid Network[J]. IEEE Access, 2020, 8 108335-108345.

[12] Hu Y, Wen B, Ye Y, et al. Multi-Defect Detection Network for High-Voltage Insulators Based on Adaptive Multi-Attention Fusion[J]. Applied Sciences, 2023, 13 (24):

[13] Yu J, Jiang Y, Wang Z, et al. UnitBox: An Advanced Object Detection Network[J]. CoRR, 2016, abs/1608.01471

[14] Rezatofighi H S, Tsoi N, Gwak J, et al. Generalized Intersection over Union: A Metric and A Loss for Bounding Box Regression[J]. CoRR, 2019, abs/1902.09630

[15] Zheng Z, Wang P, Liu W, et al. Distance-IoU Loss: Faster and Better Learning for Bounding Box Regression [C]//Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34 (07): 12993-13000.

[16] Yi-Fan Z, Weiqiang R, Zhang Z, et al. Focal and efficient IOU loss for accurate bounding box regression[J]. Neurocomputing, 2022, 506 146-157.

[17] Gevorgyan Z. SIoU loss: More powerful learning for bounding box regression[J]. arXiv preprint arXiv:2205.12740, 2022.

[18] Yang L, Zhang R Y, Li L, et al. Simam: A simple, parameter-free attention module for convolutional neural networks[C]//International conference on machine learning. PMLR, 2021: 11863-11874.

[19] Hu J, Shen L, Sun G. Squeeze-and-excitation networks[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2018: 7132-7141.

[20] Zhang Q L, Yang Y B. Sa-net: Shuffle attention for deep convolutional neural networks[C]//ICASSP

2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2021: 2235-2239.

[21] Han K, Wang Y, Tian Q, et al. Ghostnet: More features from cheap operations[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2020: 1580-1589.

[作者简介]

张俊杰（2002-），男，学位：学士，职称：无，主要研究方向：智能制造。

沈震（1982-），男，学位：博士，职称：正高级，主要研究方向：智能制造，三维深度学习，无人系统。

方启航（1997-），男，学位：博士，职称：无，主要研究方向：智能制造。

董西松（1978-）男，学位：博士，职称：副高级，主要研究方向：复杂系统的建模与分析，以及智能交通系统(ITS)和社会化制造。

王迪（1986-），男，学位：博士，职称：教授，主要研究方向：金属增材制造，装备金属增材制造，工艺金属增材制造，医学和工业应用激光加工。

熊刚（1969-），男，学位：博士，职称：正高级，主要研究方向：并行控制与管理、复杂系统的建模与优化、云计算和大数据、智能制造以及智能交通系统。

Data-Driven Raw Material Dynamic Procurement Optimization Method Based on Industrial Internet of Things and Application

LUO Jiang, WANG Yalin, LIU Chenliang

***Abstract*—The Industrial Internet of Things is pivotal in modern smart manufacturing. Raw material procurement planning is a critical component of industrial processes, directly impacting production plan execution, cost control, and product quality. However, due to the dynamic characteristics of market prices and enterprise production demands, existing optimization methods are challenging to effectively adapt to the complex fluctuations in market conditions and production needs. To address this, this paper proposes a dynamic replay reinforcement learning (DRRL) method to cope with the dynamic changes in raw material prices and production demands. Initially, this method utilizes a long short-term memory (LSTM) network to capture short-term variations in raw material prices and production demands. Subsequently, a dynamic raw material procurement framework is established based on the actual procurement processes in process industries. Finally, a deep Q-Network (DQN) method with a dynamic time alignment experience replay mechanism is employed for sequential decision-making in raw material procurement planning, determining the procurement quantity for each cycle. The effectiveness of the proposed method is validated using coal procurement data from a salt lake chemical enterprise.**

***Keywords* — Industrial Internet of Things, Procurement Plan Optimization, Reinforcement Learning, Price Prediction, Demand Prediction.**

School of Automation, Central South University, Changsha 410083, China.

This work is supported in part by the National Natural Science Foundation of China (NSFC) under Grant 92267205 and in part by the Science and Technology Innovation Program of Hunan Province in China under Grant 2021RC4054

I. INTRODUCTION

Procurement planning for raw materials is an indispensable component of supply chain management and one of the key factors in achieving efficient supply chain operations and strategic goals for enterprises[1, 2]. With meticulous procurement planning for raw materials, enterprises can mitigate inventory backlogs and prevent financial and risk issues caused by excessive inventory. Additionally, they can avoid production delays resulting from insufficient inventory. Nevertheless, developing a procurement plan for raw materials is a challenging task. Frequent fluctuations in the prices of raw materials and seasonal changes in production demand make it difficult for manually-based procurement plans to adapt to market changes and ensure continuous stable production, thereby affecting the economic efficiency and market competitiveness of

enterprises. Hence, an optimization method that can dynamically adjust raw material procurement plans based on market conditions and production demand can provide relevant information and assist decision-making for related practitioners, playing a vital role[3, 4].

Price prediction and production demand forecasting play a critical role in raw material procurement planning[5, 6]. Accurate predictions serve as a foundation for formulating effective and reasonable procurement plans, which is a key factor in ensuring successful implementation of the procurement process and maximizing economic benefits for enterprises. Currently, researchers have conducted extensive studies in the field of price prediction and production demand prediction. Typically, the methods for price and production demand forecasting are mainly based on time series forecasting models. Some scholars use traditional statistical models for prediction, such as linear regression models, autoregressive integrated moving average (ARIMA)[7], and generalized autoregressive conditional heteroskedasticity (GARCH)[8]. However, these simple linear models often struggle to capture the temporal features of complex time series. With the development of computer technology, machine learning methods such as Support Vector Regression (SVR)[9] and Decision Trees[10] have been applied in the fields of price prediction and production demand forecasting. Furthermore, to better capture temporal features, deep learning models have also received extensive attention from researchers, such as multilayer perceptron neural network (MLP)[11], long short-term memory network (LSTM)[12, 13], etc. Extensive experimental results show that deep learning methods have obvious advantages due to their excellent feature extraction capabilities.

The supply of raw materials directly affects the continuity and production cost of enterprises, especially in the continuous production and stable supply of raw materials required by the process of industrial production mode[14]. Therefore, optimizing the raw material procurement plan plays an important role. In terms of purchase volume decision-making, experts and scholars have conducted a lot of research. For example, Harris proposed the economic order quantity model (EOQ), which formulates purchasing strategies from an economic perspective to minimize costs[15]. It mainly focuses on the changes in the internal inventory of the enterprise, so that the purchasing volume is independent of the market price. On this basis, some extensions of the EOQ model have been gradually studied and formed into a systematic theory. For example, Tang et al.[16] studied the raw material inventory problem of steel enterprises, established an inventory model based on EOQ to determine the appropriate purchasing quantity and opportunity. Gao et al.[17] studied the problem of raw material procurement batch size, and determined the purchase quantity under the premise of meeting production demand so that the sum of procurement cost and inventory cost is minimized. However, these methods often assume that the price and demand of raw materials remain unchanged, which is difficult to cope with the frequent fluctuations in raw material supply market prices and production demand. Therefore, subsequent purchasing decision-making models have considered the changes in market prices and production demand in the model. For example, Chen et al.[18] used a geometric Brownian process to describe the changes in raw material prices and established a multi-period crude oil procurement model for a refinery. Zhai et al.[19] considered changes in demand and proposed a robust optimization method to solve the vendor selection problem. Andreas et al.[20] established a robust optimization-based inventory control method for uncertain demand and delivery times. These methods consider raw material prices and production demand as an uncertain distribution, and related research is relatively comprehensive, but there is a significant gap between the assumptions and their application, making accurate descriptions difficult.

To this end, this paper proposes a reinforcement-guided optimization of raw material procurement plan under dynamic price and demand, utilizing the powerful nonlinear extraction ability of LSTM model for short-term prediction of raw material market prices and production demand. It also implements sequential decision-making of raw material procurement quantity using reinforcement learning methods with dynamic

temporal alignment experience replay mechanism. The contributions of this paper are as follows:

1.The multi-cycle dynamic raw material procurement framework is established based on an in-depth analysis of the dynamic procurement processes within the process industry.

2.An LSTM model, utilizing historical data from the process industry, is employed to accurately predict raw material market prices and production demands.

3.A dynamic replay reinforcement learning method for raw material procurement planning under variable pricing and demand is proposed. This method adaptively selects the optimal strategy according to the current state, thereby better accommodating the dynamic fluctuations in raw material supply market prices and production demands.

The rest of the article is structured as follows: Section II briefly introduces the basic models used in the proposed method. In Section III, the proposed model method is described in detail. Then, in Section IV, the problem description and dataset are presented, and the proposed method is validated in the process industry coal procurement process. Finally, the conclusions are summarized in Section V.

II. THE PROPOSED METHOD

In this section, a brief overview is provided for two main techniques utilized in the proposed models: dynamic time warping (DTW) algorithm and Deep Q-Network (DQN).

A. Dynamic time warping algorithm

DTW algorithm is a method used to compute the similarity between two time series, particularly useful for handling cases where there are time shifts or variations in speed between the time series. This method dynamically adjusts the length and time scale of the time series to align them along the time axis, allowing for stretching and compressing of sequences in time and magnitude, thus enabling a more accurate comparison of similarity between time series.

The core concept of DTW involves computing a distance matrix between the elements of two sequences, followed by finding the optimal alignment path that minimizes the total distance. This alignment path represents the best matching between corresponding elements of the sequences, with its total distance effectively indicating the correlation between the time series.

Given two time series $A=\{a_1,a_2,\cdots,a_n\}$ and $B=\{b_1,b_2,\cdots,b_m\}$ with lengths n and m respectively, where a_i and b_j represent elements in sequences A and B, define a distance matrix D, where $D(i,j)$ represents the distance between element a_i in sequence A and element b_j in sequence B. Typically, the Euclidean distance is used for measurement, which can be expressed as follows

$$D(i,j)=\sqrt{(a_i-b_j)^2}=\left|a_i-b_j\right| \tag{1}$$

Dynamic programming matrix DTW can be calculated as the minimum distance ending with elements a_i and b_j. The dynamic programming process is as follows:

$$DTW(i,j)=D(i,j)+\min\begin{cases} DTW(i-1,j) \\ DTW(i,j-1) \\ DTW(i-1,j-1) \end{cases} \tag{2}$$

Through this recursive dynamic programming process, the optimal alignment path that minimizes the total distance can be found, thereby measuring the degree of match between two sequences and capturing time shifts and magnitude changes between time series.

B. Deep Q-Network

Reinforcement learning is a type of machine learning that enables an agent to make decisions by interacting with its environment. In this process, the agent chooses an action based on its current state, and receives feedback in the form of rewards or penalties from the environment. These signals help the agent determine which actions to take n the future. The concept diagram of reinforcement learning as shown is translated in Fig.1.

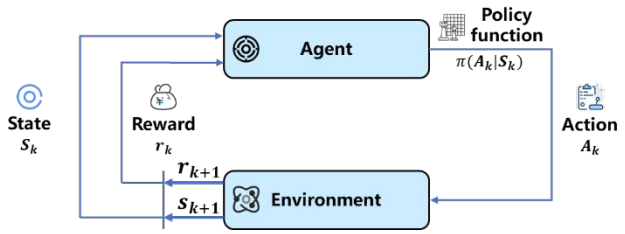


Fig.1.　The concept map of reinforcement learning

DQN is a reinforcement learning algorithm based on deep learning. It approximates the value function in Q-learning using a neural network, which the update rule of Q-learning can be represented as follows

$$Q(s,a) \leftarrow Q(s,a) + \alpha(r + \gamma \max_{a'} Q(s',a') - Q(s,a)) \quad (3)$$

Where $Q(s,a)$ represents the estimated value function for taking action a in state s. r represents the immediate reward obtained after taking action a. s' represents the next state after taking action a. a' represents the next action chosen in state s'. α represents the learning rate, controlling the update step size. γ represents the discount factor, representing the importance of future rewards.

To ensure stable training, DQN adopts the mechanisms of experience replay and target networks. Specifically, the experience replay mechanism mainly stores the experiences generated during the interaction between the agent and the environment. These experiences are then randomly sampled during the training process to update the Q-network. Experiences consist of tuples generated during the agent-environment interaction and can be represented as (s,a,r,s'). These experiences are stored in an experience replay buffer. During each network update, a small batch of experience samples is randomly extracted from the experience replay buffer to update the parameters of the Q-network. This approach enhances training stability and increases data utilization by utilizing the sampled experiences.

The main purpose of the target network is to stabilize the updates of Q-values and avoid their oscillation. The target network is a copy of the main network (i.e., the Q-network being trained), but its parameters are updated less frequently. Assuming the parameters of the main network are denoted as θ and the parameters of the target network are denoted as θ', the update formula for Q-values can be expressed as:

$$y = r + \gamma \max_{a'} Q_{target}(s',a';\theta') \quad (4)$$

Where, $Q_{target}(\cdot)$ is the Q-value function of the target network. The parameters of the target network θ' are copied from the parameters of the main network θ, periodically instead of being updated at each Q-value update. This avoids instability caused by frequent changes in target values. By combining experience replay and target networks, DQN can effectively handle high-dimensional state spaces, significantly improving training stability and efficiency, thereby effectively dealing with complex environments.

III. The Reinforcement-guided Optimization of Raw Material Procurement Plan

A. Problem statement

The research subject of this paper is the coal procurement process of a salt lake chemical company. This task requires, in the context of the actual production and operation environment of the enterprise, to develop a reasonable raw material procurement plan for the next procurement decision point while ensuring the continuous and stable operation of production. This is to minimize the total acquisition cost, which includes procurement costs, inventory costs, and production penalty costs, under the dynamic changes in raw material market prices and production demand. Specifically, the parameters and symbols involved in this task can be defined as shown in Table 1.

Table 1 Parameters and symbol representations

symbol	Description
Related sets and parameters	
P	The set of raw material prices
D	The set of raw material production demand
I	The set of raw material inventory levels
$\tilde{P}$	The set of raw material price prediction
$\tilde{D}$	The set of raw material production demand prediction

p_k	Raw material price for k-th procurement decision point
d_k	Raw material production demand for k-th procurement decision point
i_k	Raw material inventory level for k-th procurement decision point
$\tilde{p}_k$	Raw material price prediction for k-th procurement decision point
$\tilde{d}_k$	Raw material production demand prediction for k-th procurement decision point
C_{transp}	Unit transportation cost of raw materials
C_{inv}	Unit inventory holding cost of raw materials
C_{prod}	Unit production penalty cost of raw materials
ss	Safety stock level
sc	Warehouse storage capacity upper limit
$q_{\max}$	Supplier supply capacity upper limit
Decision variables	
Q	The set of procurement quantities of raw materials
q_k	Procurement quantity of raw materials for k-th procurement decision point

Since the coal procurement problem involves the actual production process of the salt lake chemical company, certain practical requirements need to be considered. These mainly include production continuity constraints, inventory balance constraints, initial inventory constraints, final inventory constraints, storage capacity constraints, procurement quantity upper limit constraints, and non-negativity constraints on procurement quantity. According to the parameters and symbols defined in Table 1, these constraints can be described as follows:

Production Continuity Constraint: Since the salt lake chemical company operates in the process industry, continuous supply of raw materials must be ensured. To prevent raw material shortages caused by unforeseen events, a safety stock is usually set, ensuring that the sum of the current procurement quantity and inventory quantity is greater than or equal to the safety stock. This constraint can be expressed as follows:

$$q_k + i_k - d_k \geq 0 \tag{5}$$

Inventory Balance Constraint: The inventory balance constraint represents the relationship between procurement, inventory, and production demand. It states that the inventory level for the current period equals the inventory level of the previous period plus the current procurement quantity minus the current demand quantity. This constraint can be expressed as follows:

$$i_k = i_{k-1} + q_k - d_k \tag{6}$$

Initial Inventory Constraint: The initial inventory must be greater than or equal to 0. This constraint can be expressed as follows:

$$i_0 \geq 0 \tag{7}$$

Final Inventory Constraint: The final inventory must be greater than or equal to 0. This constraint can be expressed as follows:

$$i_T \geq 0 \tag{8}$$

Storage Capacity Constraint: The inventory level must be less than or equal to the storage capacity of the warehouse. This constraint can be expressed as follows:

$$i_k \leq sc \tag{9}$$

Procurement Quantity Upper Limit Constraint: The procurement quantity must be less than or equal to the maximum quantity provided by the supplier. This constraint can be expressed as follows:

$$q_k \leq q_{\max} \tag{10}$$

Non-negativity Constraint on Procurement Quantity: The procurement quantity must be greater than or equal to 0. This constraint can be expressed as follows:

$$q_k \geq 0 \tag{11}$$

Through the aforementioned constraints, an environment for describing the coal procurement process of the salt lake chemical company can be constructed. However, this environment is based on the

premise of known and deterministic raw material market prices and production demands. Since the prices and production demands of coal are dynamic and difficult to determine in advance, there is a need for a coal procurement optimization decision framework based on forecasts of coal prices and production demands.

B. Optimization framework for procurement planning based on reinforcement learning

To address the problem at hand and the relevant constraints, a dynamic framework for raw material procurement planning is established shown in Fig. 3. The procurement period is divided into T cycles, with each cycle ending at a procurement decision point. At these decision points, information is updated based on the forecasted results of raw material market prices and production demand. Through the use of reinforcement learning methods, optimal procurement decisions for each cycle are made, while minimizing procurement and inventory costs and ensuring continuous and stable production.

Based on the raw material procurement framework in Fig.3, a reinforcement learning model is constructed using RL to make iterative decisions on the appropriate procurement quantity at each procurement decision point. Hence, it is necessary to define the state, action, and reward functions. The following is a detailed description of the state variables, action variables, and reward function.

State Variables: The system's state directly affects the decision-making of the agent. In this paper, the state variables are set as S, and the current raw material price p_k, demand d_k, and inventory i_k at the current time point are used as state variables to reflect the system characteristics at the current time. In order to perceive market prices and production demand, the next procurement decision point's raw material price $\tilde{p}_{k+1}$ and production demand $\tilde{d}_{k+1}$ are also included as part of the state variables. In order to minimize the size of the state space as much as possible, the difference between the predicted value of the next procurement decision point and the observed value of this procurement decision point is used as part of the state variables, as follows:

$$\Delta\tilde{p}_{k+1} = \tilde{p}_{k+1} - p_k \tag{12}$$

$$\Delta\tilde{d}_{k+1} = \tilde{d}_{k+1} - d_k \tag{13}$$

In summary, the state S_k of the k-th procurement decision point can be represented as follows:

$$S_k = [p_k, d_k, i_k, \Delta\tilde{p}_{k+1}, \Delta\tilde{d}_{k+1}] \tag{14}$$

Action variable: The action variable is the decision made by the agent after observing the system state. In this paper, the action is set as A, and the agent's action variable is set as q_{k+1}, which represents the amount of raw materials to be purchased for the next procurement decision point. Thus, the agent's action for the k-th procurement decision point can be represented as:

$$A_k = [q_{k+1}] \tag{15}$$

Reward Function: The reward function evaluates the action taken by the agent in the current state and is a key metric for the agent to choose the best action. In this paper, the reward function of the model is obtained by taking the negative value of the sum of the procurement cost, inventory holding cost, and production penalty cost as follows:

$$r_k = -\left\{(p_k + C_{transp})q_k + C_{inv} i_k + C_{prod}\left[ss - \min\left(ss, q_k + i_{k-1} - d_k\right)\right]\right\} \tag{16}$$

As the market price and production demand of purchased raw materials tend to change dynamically over time, the purchasing optimization decision cases in different periods do not necessarily have reference value for the optimization decision at the current purchasing decision point. The traditional experience replay mechanism adopts the principle of random extraction to

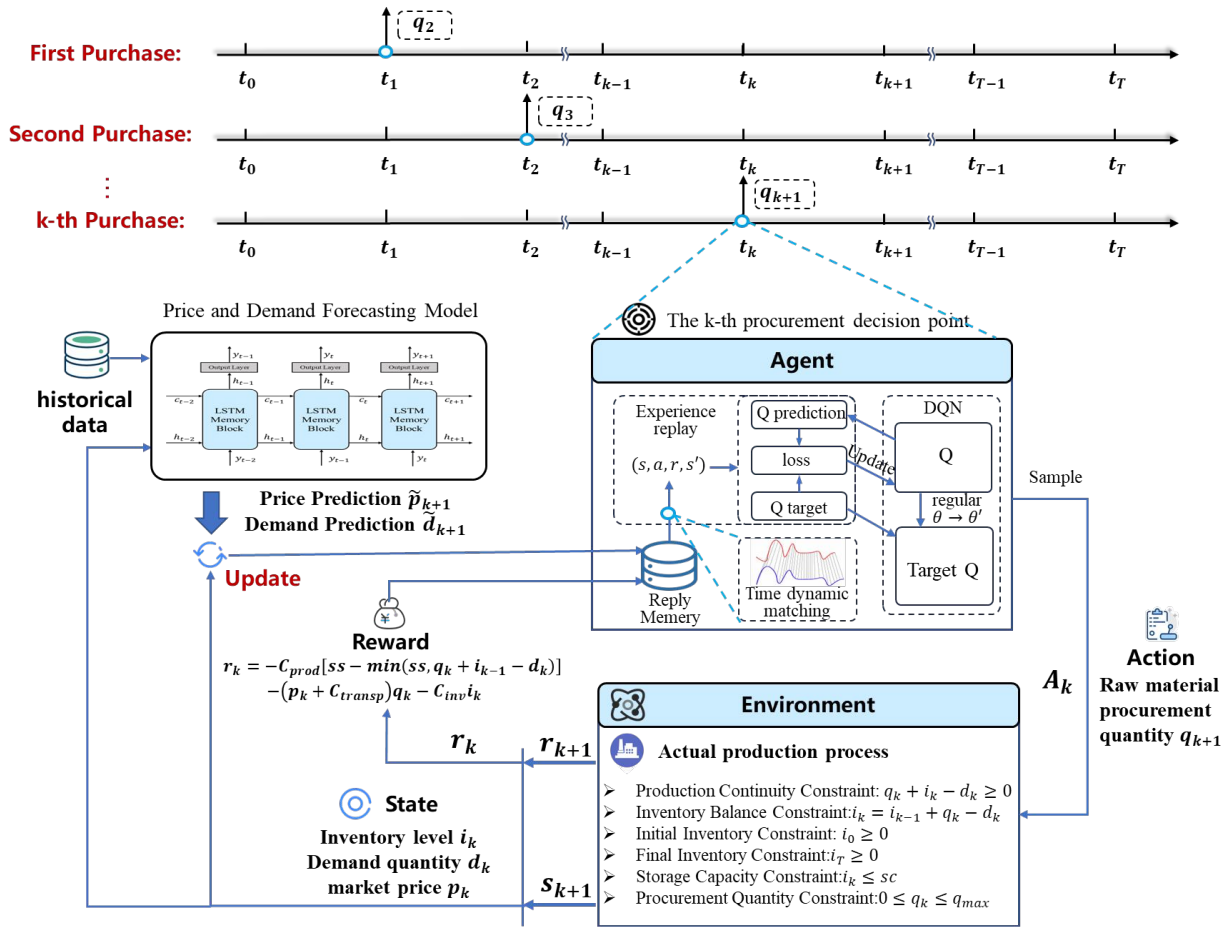


Fig.2. The framework for raw material procurement plan

extract the experience stored in the experience replay unit with equal probability, which makes it difficult to selectively replay experience data with more reference value. To this end, this paper adopts a reinforcement learning algorithm based on the dynamic experience replay mechanism to train the coal procurement plan optimization problem based on the set state, action and reward functions. The method mainly adopts the DTW algorithm on the basis of the experience replay mechanism, and selects N procurement optimization cases in the experience replay unit that are most similar to the market and production environment at the current procurement time point for the updating of network parameters. Hence, the method is able to focus on more important data samples in the process of experience replay, and relatively unimportant data samples do not need to be learnt too much. The basic structure of the DQN based on the dynamic experience replay mechanism is demonstrated in the agent section of Fig.2, and the detailed training process is shown is as follows:

Step 1: Assume that at time k, sample $S_k = [p_k, d_k, i_k, \Delta\tilde{p}_{k+1}, \Delta\tilde{d}_{k+1}]$ is input. A sliding window of length L is set, and the last sample within the window is used to replace all the samples within the window. The sliding window is moved sequentially, and based on formula (2), the time similarity $DTW_{p_k}(m,k)$, $DTW_{d_k}(m,k)$, and $DTW_{i_k}(m,k)$ of the raw material price, production demand, and inventory level between the sequence of each window and the sequence of the window where the input sample is located are calculated.

Step 2: The weights of raw material price, production demand, and inventory level are comprehensively measured using formula (17).

$$DTW_k(m,k) = \alpha DTW_{p_k} + \beta DTW_{d_k} + \gamma DTW_{i_k} \quad (17)$$

Step 3: Sort $\{DTW_k(m,k)\}_{m=1}^{M_1}$ in descending order. The larger the value of $DTW_k(m,k)$, the higher the relevance of the m-th sample to the given sample. Select the top N samples to form the set of experience samples

of S_k, which are then added to the training of the DQN.

Based on this, the DQN algorithm process with a dynamic experience replay mechanism is shown in Algorithm 1.。

Algorithm 1: Training process of DQN based on the Dynamic Experience Replay Mechanism

Initialize replay memory M;
Initialize action-value network Q with random weight θ;
Initialize target action-value network $\hat{Q}$ with random weight θ^-;
for $episode \leftarrow 1$ **to** M **do**
  Initialize sequence s_1;
  for $k \leftarrow 1$ **to** T **do**
    With probability ε select a random action a_k;
    Otherwise select $a_k = argmax_a Q(s_k, a; \theta)$;
    Excute action a_k and observe reward r_k via (16);
    Store transition (s_k, a_k, r_k, s_{k+1}) in M;
    Sample minibatch of tansitions (s_k, a_k, r_k, s_{k+1}) from M by dynamic experience replay mechanism;
    Set $y_j = \begin{cases} r_j & if\, espisodeterminatesatstepj+1 \\ r_j + \gamma max_{a'} \hat{Q}(s_{k+1}, a_{k+1}; \theta^-) & otherwise \end{cases}$
    Perform a gradient descent step on $(y_j - Q(s_k, a; \theta))^2$ with respect to the network parameters θ;
    Every C steps reset $\theta^- = \theta$;
  end
end

As shown in Fig.3, the training process of the model at the kth purchasing decision point is as follows:

Step 1: Update the current state variable based on the feedback provided by the actual environment, including the current raw material price p_k, production demand d_k, and inventory level i_k. The raw material price and production demand are obtained through interaction between the actual market price and the enterprise production process, while the inventory level can be updated using equation (9).

Step 2: Combine historical data. Use the LSTM model to predict the raw material price $\tilde{p}_{k+1}$ and production demand $\tilde{d}_{k+1}$ for the next procurement decision point, and calculate their predicted increments based on equations (15)-(16). Update the state variable accordingly.

Step 3: Calculate the reward function r_k based on equation (19) and input it into the agent. The agent evaluates the raw material procurement decision made at the previous purchasing decision point based on the reward function and updates the network parameters accordingly.

Step 4: Based on the updated state S_k, the agent provides the decision variable, i.e., the amount of raw material to be purchased for the next procurement decision point.

Step 5: Input the decision variable q_{k+1} into the environment for interaction, and the feedback result of the interaction can only be obtained at the next purchasing decision point. Set k=k+1 and return to Step 1 until the end of the procurement execution period.

IV. CASE STUDY

A. Description of dataset

In this paper, the effectiveness of the proposed method is verified in the coal procurement process of Salt Lake chemical enterprises. A total of 455 weekly raw material demand and weekly prices from January 2014 to March 2023 were collected as data samples. In addition, weekly raw material procurement data for manual decision-making from January 2014 to March 2023 was collected for comparison. The actual parameters involved in the procurement optimization problem are shown in Table 2.

TABLE 2 Parameter settings of optimization problem

Parameter	Unit	Parameter value
C_{transp}	CNY/ton	70
C_{inv}	CNY/(ton•day)	30
C_{prod}	CNY/ton	100
ss	ton	3000
sc	ton	10000
$q_{\max}$	ton	60000
$q_{\max}$	ton	60000

Based on the above data set and procurement process

parameter settings, the experimental simulation of prediction task and optimization task is carried out respectively.

B. Results and discussion of prediction task

Two statistical indicators, root mean square error, RMSE and absolute mean error (MAE), are used to evaluate the prediction performance of each model, as follows:

$$RMSE = \sqrt{\sum_{n=1}^{N}(y_n - \tilde{y}_n)^2 / (N-1)} \tag{18}$$

$$MAE = \sum_{n=1}^{N} | y_n - \tilde{y}_n | / N \tag{19}$$

where y_n and $\tilde{y}_n$ n are the actual and predicted values of raw material prices and production demand, respectively. The smaller these two metrics represent better prediction performance.

TABLE 3 The prediction performance of the three methods on the market prices

Method	RMSE	MAE
ARIMA	108.94	80.66
GARCH	50.06	27.67
SVR	46.65	26.62
LSTM	**31.49**	**18.51**

In this study, ARIMA, GARCH, and SVR methods were constructed to compare with the LSTM model to verify their effectiveness. The prediction results of these four models are shown in Table 3. Since ARMA is a traditional linear model, it is difficult to capture the complex timing features of the price series, so the worst forecast effect is achieved. Due to the volatility of the time series, the GARCH method has lower RMSE and MAE compared to the ARIMA model. The SVR model can extract the nonlinear features of the time series, so it can achieve better prediction preference than the ARIMA and GARCH model. Since LSTM is able to extract the complex dynamic features of time series, the smallest RMSE and MAE are obtained.

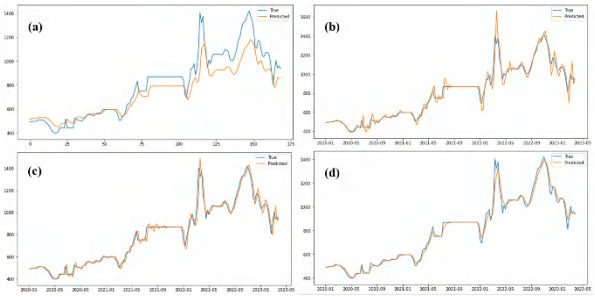


Fig. 3. Prediction results of four methods for predicting the market prices: (a) ARIMA; (b) GARCH; (c) SVR; (d) LSTM

Intuitively, the prediction details of these four methods are shown in Fig.3. Fig.3 (a), Fig.3 (b), Fig.3 (c), Fig.3 (d) denotes the raw material price predicted curve and true value of ARIMA, GARCH, SVR and LSTM, respectively. It can be seen that the prediction curve of LSTM has the best fitting effect.

TABLE 4 The prediction performance of the three methods on the production demand

Method	RMSE	MAE
ARIMA	2890.05	2299.12
GARCH	1891.48	1477.74
SVR	1466.31	1129.37
LSTM	**1072.37**	**811.95**

Similarly, ARIMA, GARCH and SVR models were built against the production demand dataset and compared with the LSTM model. The prediction results are shown in Table 4. It can be seen that the LSTM achieves the best predictive performance with the smallest RMSE and MAE. Fig.4 (a), Fig.4 (b), Fig.4 (c), Fig.4 (d) show the predicted results and true values of raw material production demand of ARIMA, GARCH, SVR models and LSTM, respectively, where LSTM has the best fitting performance.

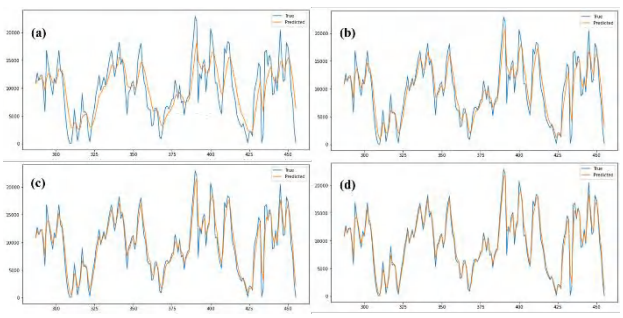


Fig. 4. Prediction results of four methods for predicting the market prices: (a) ARIMA; (b) GARCH; (c) SVR; (d) LSTM

C. Results and discussion of procurement optimization task

Based on the actual operational data of a salt lake chemical enterprise in 2022, the proposed method was compared with the Real Manually-determined Procurement Strategy (RMP), Safety Stock Procurement Strategy (SSP), and the reinforcement learning-based raw material procurement strategy (RL-MPS). The RMP strategy is a procurement quantity determined manually by the enterprise manager. SSP (Supply, Schedule, Production) refers to the consideration of predicted production demand in making decisions, so that the inventory at the next purchasing decision point corresponds exactly to the safety stock, which is the action variable at the current purchasing decision point $q_{k+1} = ss + \tilde{d}_{k+1}$.

TABLE 5 The performance metrics of different purchasing strategies on actual operational data

Methods	Total procurement quantity	Total procurement cost	Unit procurement cost
RMP	513841.77	292645188.2	569.52
SSP	531405.27	301645016.5	567.64
RL-MPS	527635.25	287635873.4	545.14
DRRL-MPS	**514732.19**	**276543736.5**	**537.25**

The performances of three different purchasing strategies on real enterprise operation data are shown in Table 5. It can be seen that due to the need to ensure sustained and stable production of the enterprise, SSP has the highest total procurement quantity to meet safety production needs. Compared with the RMP method, SSP has a higher total procurement volume and total procurement cost and a lower unit procurement cost. The RL-MPS has lower unit procurement costs compared to two traditional procurement methods. The method proposed in this paper focuses on market prices and enterprise production demand, therefore achieving the best performance with the lowest total procurement cost and unit procurement cost among all purchasing strategies.

V. CONCLUSION AND FUTURE WORK

In this paper, a reinforcement-guided optimization method for raw material procurement plan under dynamic supply and demand is proposed. To cope with the dynamic changes in raw material market prices and production demand, an LSTM model is utilized for short-term prediction. Based on this, a sequential decision-making for raw material procurement plan is achieved using the DQN method with a dynamic temporal alignment experience replay mechanism. The effectiveness and superiority of the proposed method, named DRRL-MPS, were verified on real operational data from a coal procurement process, achieving the lowest total procurement cost and unit procurement cost. In the future, more research in the field of deep learning is needed to improve the prediction accuracy of the forecasting method and reduce the computational cost of the reinforcement learning method.

References

[1] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, “A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Internet of Things Journal,* vol. 8, no. 8, pp. 6222-6246, 2021.

[2] J. D. Nel, and H. Simon, “Introducing a process for radical supply chain risk management,” *INTERNATIONAL JOURNAL OF BUSINESS PERFORMANCE MANAGEMENT,* vol. 21, no. 1-2, pp. 149-165, 2020.

[3] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and Privacy-Enhanced Federated Learning for Industrial Artificial Intelligence."

[4] D. Singh, and A. Verma, “Inventory Management in Supply Chain,” *Materials Today: Proceedings,* vol. 5, no. 2, Part 1, pp. 3867-3872, 2018/01/01/, 2018.

[5] W. K. R., and E. H. P. J. E. S. W. Applications, "Volatility of main metals forecasted by a hybrid ANN-GARCH model with regressors," 2017.

[6] L. M. Sheng, J. Zhou, X. Li, Y. F. Pan, and L. F. Liu, "Water quality prediction method based on preferred classification," *IET CYBER-PHYSICAL SYSTEMS: THEORY & APPLICATIONS,* vol. 5, no. 2, pp. 176-180, JUN, 2020.

[7] J. Wu, Y. Chen, T. Zhou, and T. L. J. Energies, "An Adaptive Hybrid Learning Paradigm Integrating CEEMD, ARIMA and SBL for Crude Oil Price Forecasting," 2019.

[8] O. Bustos, and A. Pomares-Quimbaya, "Stock market movement forecast: A Systematic review," *Expert Systems with Applications,* vol. 156, pp. 113464, 2020/10/15/, 2020.

[9] J. Zhang, Y.-F. Teng, and W. Chen, "Support vector regression with modified firefly algorithm for stock price forecasting," *Applied Intelligence,* vol. 49, no. 5, pp. 1658-1674, 2019/05/01, 2019.

[10] C. Liu, Z. Hu, Y. Li, and S. Liu, "Forecasting copper prices by decision tree learning," *Resources Policy,* vol. 52, pp. 427-434, 2017/06/01/, 2017.

[11] C. Wang, X. Zhang, M. Wang, M. K. Lim, and P. Ghadimi, "Predictive analytics of the copper spot price by utilizing complex network and artificial neural network techniques."

[12] Y. Hu, J. Ni, and L. Wen, "A hybrid deep learning approach by integrating LSTM-ANN networks with GARCH model for copper price volatility prediction."

[13] L. Ji, Y. Zou, K. He, and B. Z. J. P. C. Science, "Carbon futures price forecasting based with ARIMA-CNN-LSTM model," 2019.

[14] L. de Boer, E. Labro, and P. Morlacchi, "A review of methods supporting supplier selection," *European Journal of Purchasing & Supply Management,* vol. 7, no. 2, pp. 75-89, 2001/06/01/, 2001.

[15] F. W. Harris, "How Many Parts to Make at Once."

[16] L. Tang, G. Liu, and J. Liu, "Raw material inventory solution in iron and steel industry using Lagrangian relaxation."

[17] Z. Gao, and L. X. Tang, "Combine column generation with GUB to solve the steel-iron raw materials purchasing lot-sizing problem," *Zidonghua Xuebao/Acta Automatica Sinica,* vol. 30, pp. 20-25, 01/01, 2004.

[18] R. Chen, T. Deng, S. Huang, and R. Qin, "Optimal crude oil procurement under fluctuating price in an oil refinery."

[19] J. Zhai, H. Yu, and C. Sun, "Robust Optimization for the Newsvendor Problem with Discrete Demand," *Mathematical Problems in Engineering,* vol. 2018, pp. 5358219, 2018/08/26, 2018.

[20] A. Thorsen, and T. Yao, "Robust inventory control under demand and lead time uncertainty."

About the authors

Yalin Wang received the B.Eng. degree in automation and the Ph.D. degree in control science and engineering from the Department of Control Science and Engineering, Central South University, Changsha, China, in 1995 and 2001, respectively. She is currently a Professor with the School of Automation, Central South University, Changsha, China

Her research interests include the modeling, optimization and control for complex industrial processes, intelligent control, and process simulation. (Email: ylwang@csu.edu.cn)

Jiang Luo received the B.Eng. degree in School of Automation from the Central South University of Science and Technology, Changsha, China, in 2020. He is currently pursuing the Ph.D degree with the School of Automation, Central South University, Changsha, China.

His research interests include deep learning, soft sensor modeling, and supply chain management. (Email: ljiang@csu.edu.cn)

Chenliang Liu received the Ph.D. degree in control science and engineering from the School of Automation, Central South University, Changsha, China, in 2024. He is currently a lecturer with the School of Automation, Central South University, Changsha, China.

From 2023 to 2024, he was a joint training Ph.D. student with the School of Chemistry, Chemical Engineering and Biotechnology at Nanyang Technological University, Singapore. His research interests include deep learning, modeling and optimal control of complex industrial process. (Email: lcliang@csu.edu.cn)

基于 ZOA-ShareSpace 的多模态数据共享子空间方法

许云晋 ，周灿

（中南大学 自动化学院，长沙 410000）

摘　要：随着工业互联网时代的到来，对我国工业体系的自动化和智能化水平提出了新的要求。作为我过工业体系的重要一环，锌冶炼在我国工业和经济发展中占据重要地位。而锌电解作为锌冶炼的关键环节，保持锌电解的稳定运行和析出锌的质量稳定是保证生产效率和产品质量的重要因素。而目前的研究多为单模态研究，难以满足自动化和智能化需求。为了解决这个问题，提出了一个基于多模态数据共享子空间方法，ZOA-Sharespace。该方法以日志文本和红外图像为输入，通过潜在共享编码器提取出不同模态信息的潜在共享信息，并利用共享激活函数将潜在共享信息映射到共享空间中。实验结果表明，该方法具有较高的准确率，能够有效地实现对锌析出工况的分类，为生产实践提供了有力支持。

关键词：ZOA-ShareSpace；多模态共享子空间；工况分类；锌电解

Multimodal Data Shared Subspace Method Based on ZOA-ShareSpace

Yunjin Xu[1], Can Zhou[1]

（School of Automation，Central South University，Changsha 410000）

Abstract: With the advent of the industrial internet era, new demands have been placed on the automation and intelligence levels of China's industrial system. As an important part of China's industrial system, zinc smelting occupies a significant position in the country's industrial and economic development. Zinc electrolysis, as a key process in zinc smelting, is crucial for ensuring stable operation and consistent quality of zinc deposition, which are essential for maintaining production efficiency and product quality. However, current research predominantly focuses on unimodal approaches, which are insufficient to meet the needs for automation and intelligence. To address this issue, a multimodal data shared subspace method, ZOA-ShareSpace, has been proposed. This method uses log text and infrared images as inputs and extracts latent shared information from different modalities through a latent shared encoder. A shared activation function is then used to map the latent shared information into a shared space. Experimental results show that this method achieves high accuracy and effectively classifies zinc deposition conditions, providing strong support for production practices.

Key words: ZOA-ShareSpace, multimodal shared subspace, condition classification, zinc electrolysis

1　引言

锌电解是锌冶炼的关键工序之一，占世界锌产量的 90%以上[1]。随着工业互联网时代的到来，对锌电

解过程的自动化与智能化发展提出了新的要求和挑战。锌电解过程工艺不断完善，流程日益复杂，其生产过程中产生并存储了海量数据。这些数据来源广泛，形态各异，既包括设备监测数据、 产品质量检测数据、能耗数据等结构化数据，日志文本等半结构数据，还包括生产监控系统产生的大量图片、视频等非结构化数据，可以提供不同角度和维度的信息，具有更丰富的信息和潜在的价值[2-4]。如何处理这些多源异构数据，是推动锌电解过程自动化和智能化水平发展的关键。

目前，针对多源异构数据，通过对其进行有效融合，进行多层次特征提取，获得比单一来源数据更准确有用的信息，从而解决多源异构数据结构不一致、数据维度高的问题。根据融合阶段的不同，多模态数据融合的方法包括数据级融合、特征级融合和决策级融合[5-6],而更为常见的分类方法则是基于概率的数据融合、基于证据的数据融合以及基于人工智能的数据融合[7-8]。

传统的数据融合算法大多以概率为核心，其中又以贝叶斯理论、马尔可夫链和蒙特卡罗方法研究最多、应用最为广泛。贝叶斯理论依据概率原则有效地整合来自不同传感器信息，并以概率的形式明确表达其中的不确定性。在此基础上，通过给定的多模态数据条件，进一步计算出某个假设为真的后验概率。证据理论是处理不确定性和融合多模态信息的有效方法，区别于传统概率论，它不依赖于先验或条件概率，并能明确区分“不确定”和“不知道”的差异。但传统的数据融合方法多应用于结构化数据中，面对非结构化数据，其效果往往无法令人满意。

伴随人工智能技术的发展，基于人工智能的多模态融合方法正逐渐成为被广泛采用的主流方法。这些方法利用机器学习和深度学习等技术，能够更加智能地整合来自不同模态的数据，从而提高数据的综合利用率和准确性。基于深度学习的方法不用考虑不同模态间的先验概率与后验概率，只需要相对应的数据，便可对实现多模态数据的融合。并且，得益于在机器视觉领域和自然语言处理领域技术的发展，基于深度学习的多模态数据融合模型对非结构化数据的处理性能是基于概率的数据融合方法和基于证据的数据融合方法所不能比拟的。因此，在面对需要对图像模态和文本模态的数据融合时，学者们往往倾向于采用基于深度学习的多模态数据融合方法。

受 Gabriele[9]等人的工作的启发，我们提出了多模态共享子空间模型 - ZOA-ShareSpace 模型。具体来说，为增加模型的可解释性和透明性，先对各个模态的数据进行特征提取，再利用编码的方式提取各个模态的潜在共享空间，再将各模态的潜在共享空间映射到一个特征共享子空间中。由于共享子空间的存在，它可以描述不同模态信息在同一任务上的共同特征，从而更为精确地实现下游任务。

本文以锌电解极板析出工况分类为下游任务，通过将图像信息（红外图像）和文本信息（日志文本）两种模态的信息结合起来，充分挖掘不同模态数据的内在特征，将不同模态的共享信息映射到同一共享子空间中，从而提高分类任务的准确性。

我们的工作如下：

（1）提出了一种统一图像和文本信息的多模态共享子空间模型。

（2）利用图像和数据信息训练了提出的多模态共享子空间模型，并实现了对锌电解极板析出情况的工况分类。

（3）利用现实世界上的数据集评估模型的性能，并且证明了我们的模型可以学习到多模态特征，并且在多个评估指标上优于其他模型。

2 相关工作

2.1 传统数据融合方法

传统的数据融合方法包括基于概率的数据融合方法和基于证据的数据融合方法。传统数据融合方法其可解释性强，模型更为简单，目前的研究趋势是将传统数据融合方法与特定方法融合，来完成数据融合任务。

文献[10]提出了一个用于鲁棒贝叶斯视觉跟踪的机架级融合框架，用于在线测量各个跟踪器的性能，以指导融合决策。文献[11]针对工业领域中高卢面料检测中多传感器难以直接应用的问题，将面料理论和多源数据贝叶斯理论融合，使得检测更为精确。文献[12]提出了一种基于贝叶斯方法的传感器融合决策融合策略，可以识别传感器数据中的不一致性，使杂乱的数据从传感器融合过程中消除。在基于证据的融合方法中，以 D-S 理论体系研究最为广泛。文献 13]采用极限学习机（ELM）和 D-S 理论结合的方式，对质子交换膜燃料电池进行故障诊断；文献[14]将神经网络与 D-S 理论共同应用特征级的数据融合，实现轴承故障检测。文献[15]提出了一种基于数据驱动证据理论的多传感器数据融合方法，用于土地覆盖特征提取，对地表覆盖类型进行分类，其中 D-S 证据理论的实现主要利用了多传感器数据和多光谱卫星图像两种类型的数据。

上述数据融合方法在处理大数据融合时，常常会面临一些挑战。基于概率的融合方法在处理高维度数据时面临困难，并且存在证据理论上的缺陷；而基于证据理论的融合方法则面临计算量大、证据融合悖论以及概率指派等问题，无法适应当下数据结构复杂，数据维度高的情况。

2.2 基于深度学习的数据融合方法

深度学习方法能够利用海量数据提升模型性能，并且面对高维和非线性数据上，基于深度学习的方法能够通过多层非线性变换捕捉复杂的非线性关系，在大规模数据上表现出色，因而被学者们广泛研究。

文献[l6]提出了 GregNets 的通用框架，用于联合学习预测模型和利用知识图谱中的图联通性的关联结构，利用基于知识图谱关系的新正则化器，以指导关联结构的估计。文献[17]提出了一种多模态图神经网络(MAGNN)来从多模态输入中学习金融时序预测序列，并利用两阶段注意力机制进行联合优化，允许终端用户调查模态间来源的重要性。文献[18]针对合成孔径雷达（SAR）目标识别问题，提出了一种深度学习融合识别方法，通过 PCA 和 SAE 提取 SAR 图像的深层特征，结合卷积神经网络（CNN）的特征提取，完成融合。

上述深度学习方法在多模态数据融合处理上具有显著的优势，但也存在其本身的问题。由于多模态深度学习模型往往是“黑盒”模型，缺乏可解释性，并且当某一模态的信息不完整时，其效果可能会无法令人满意。

2.3　数据共享子空间方法

数据共享子空间能够将不同模态间的信息映射到一个共享的空间中。利用共享子空间，可以知道哪些信息需要“共享”，哪些信息是“独有”的，因而增强了模型的可解释性。同时，伴随特征的融合提取，数据维度也进一步降低，因此，可以有效降低数据的维度。

传统的数据共享子空间方法按不完整信息补充分为两类：一类是通过挖掘多模态数据信息的互补性和一致性来学习一个一致的表示；第二类是通过核技巧填补缺失的模态信息，然后对填充后的多模态信息进行共享表示。文献[19]利用核典型相关分析技术迭代补全各个缺失数据的核矩阵，挖掘不同模态信息间的互补性，实现对不完整模态数据的共享表示。文献[20]采用生产对抗网络来生成缺失的多模态信息，提出一个对齐聚类损失函数以促进多模态统一表示的学习效率。文献[21]在挖掘局部子结构的同时补全缺失的关联度信息，并采用图约束来指导共享子空间的学习，从而获得完整的共享子空间结构。以上方法虽然在不完整模态表示上取得了不错的效果，但在面对不同模态时，认为每个模态的贡献是一致的，并且多模态数据填充算法都是基于核方法，而核函数的设计具有很大的经验性。因此，本文针对旧有共享子空间方法的缺陷与不足，利用深度学习的方法，结合两者的优势，无需依赖于经验，实现对多模态数据共享子空间的提取，从而提高模型的可解释性，并对数据实现降维，提高模型泛化能力。

3　基于 ZOA-ShareSpace 的多模态共享子空间方法

3.1　ZOA-ShareSpace 方法

方法结构图如 1 所示，分为三个部分，潜在共享信息提取模块，共享空间分析模块和检测层。潜在共享信息模块针对不同模态，利用不同的编码器和潜在信息激活函数提取不同模态的潜在共享信息。在共享空间分析模块中，利用共享模态编码层和共享激活函数将各模态潜在共享信息映射到共享空间中。之后通过计算不同模态信息特征的欧式距离，提取出更为相似的特征，减少冗余信息，提升数据融合的效果。最后，检测层根据共享子空间结果执行分类任务。

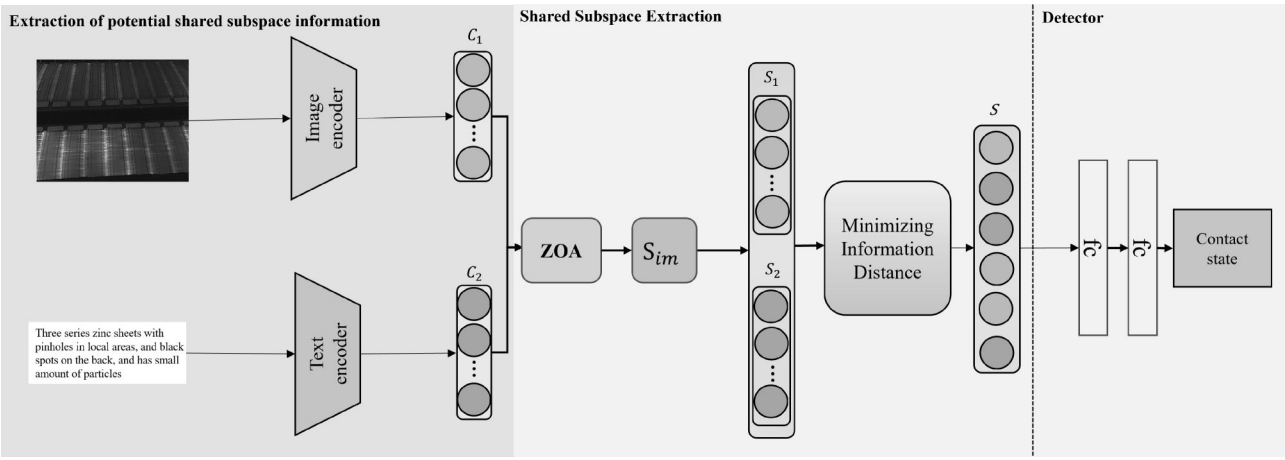


图 1. ZOA-ShareSpace 模型结构，包含三个部分，潜在共享信息提取，共享子空间提取和检测层。

3.2 潜在共享信息编码

对于不同的模态信息，在构建不同模态信息的共享子空间之前，需要提取出不同模态中的潜在共享信息。潜在信息提取部分由不同的编码器层组成。对于不同模态，采用不同的编码器对其潜在共享信息进行提取。

针对文本信息，采用 BERT 模型对文本信息进行编码。BERT 是一种基于 Transformer 编码架构的高级预训练单词嵌入模型，可以针对特定的自然语言处理任务进行微调利用，将 BERT 作为句子编码器，可以准确地获取句子的上下文表示。在预训练阶段，BERT 模型通过两个任务来学习通用的文本表示：掩码语言建模（MLM）和下一句预测任务（NSP）。在 MLM 任务中，BERT 模型会随机地掩盖序列中的一些单词，然后模型尝试预测这些屏蔽的单词，这使模型能够学习到丰富的词语上下文关系；在 NSP 中，BERT 模型会尝试预测给定两个句子是否在语义上相邻。预训练完后，给定文本输入，可以利用训练好的 BERT 模型生成文本表征。

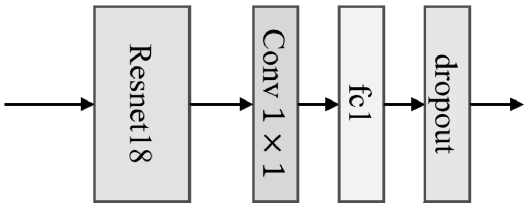


图 2. 文本编码器

在各种图像任务中，卷积神经网络（CNN）表现良好。因此，我们采用 CNN 模型作为图像的编码器。其结构如图 2 所示。Resnet 在图像特征提取任务中具有十分优秀的性能，因此，采用预训练的 ResNet18，降低训练成本，提高模型效率，取得良好的效果。在 Resnet18 之后，采用1×1卷积来实现信道间的信息流，然后通过一层全连接层实现信道信息流，并加入一层 dropout 层防止过拟合现象发生。

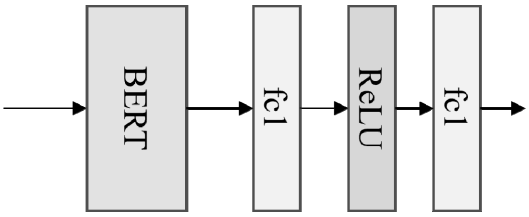


图 3. 图像编码器

在对多模态信息进行编码之后，需要将编码信息，、映射到潜在共享信息空间中。具体而言，采用潜在共享信息激活函数将编码后的信息映射为潜在共享信息。潜在共享激活信息其计算如下：

$$c_{im} = (1 + \exp(-(\phi_i(x_{im}) \underset{j \in B_{im}}{\Theta} \phi_i(x_{ij}))))^{-1} \tag{1}$$

$$\Theta = \gamma^{(i)} \frac{x_{ij} - \mu_i}{\sqrt{(\sigma_i)^2 + \varsigma}} + \beta^{(i)} \tag{2}$$

其中，$B_{im} \subseteq \mathbb{N}$ 属于包含 m 个样本的批次样本的指数；x_{im} 为第 m 个模态的特征空间；x_{ij} 为其他模态

的特征空间；ϕ_i 为第 i 个模态的编码方式；Θ 表示批次标准化函数；$\gamma^{(i)}$ 表示第 i 个模态的缩放参数；β 表示平移参数；μ_i 表示平均值；σ_i 表示标准差；ς 为小参数，防止分母为 0；C_{im} 表示模态潜在共享空间。

3.3　共享子空间激活函数

对于每个模态的潜在共享信息，需将其映射到共享子空间中。我们利用共享激活函数来实现这一目标。其结构与潜在信息激活函数结构类似，也由 sigmod 函数和批次标准化函数组成，但与潜在信息激活函数不同的地方在于，采用一组参数作为各个模态映射到共享子空间的权重，使得提取到共享子空间中的信息能够更为集中于下游任务的特征中。共享激活函数的结构如下：

$$s_{im} = (1 + \exp(-(\psi_i(c_{im}) \underset{i=1,\ldots,n \wedge j \in B_{im}}{\Theta} \psi_i(c_{ij}))))^{-1} \tag{3}$$

其中，$\psi_i(x)$ 表示参数优化函数，s_{im} 表示映射的共享子空间，c_{ij} 表示模态潜在共享空间。

3.4　斑马寻优算法

在批量归一化函数中，有两个关键参数需要进行参数优化，缩放参数 和平移参数 。这两个参数会改变归一化后的范围和大小，对实验结果产生深刻影响，因此，需对这两个参数进行寻优处理。我们发现，斑马寻优算法（ZOA）在参数上具有优异的性能，因此，我们采用斑马优化架构作为我们的 。

斑马优化算法分为两个阶段，觅食阶段和防御阶段。在第一阶段，根据斑马的觅食行为来更新种族成员。斑马的主要食物是草和莎草，对应高价值参数，而当主要食物缺乏时，则会食用芽、水果、树皮和叶子，对应次优参数。在斑马中，有一种斑马会作为先驱，食取上层和营养较少的草和树冠。因此，在 ZOA 中，种群个体最好的被认为为先锋斑马，并引导其他种群成员走向其在搜索空间中的位置。在觅食阶段的位置更新建模如下：

$$x_{i,j}^{new,P1} = x_{i,j} + r \cdot (PZ_j - I \cdot x_{ij}), \tag{4}$$

$$X_i = \begin{cases} X_{i,j}^{new,P1}, F_i^{new,P1} < F_i \\ X_i, else \end{cases} \tag{5}$$

其中 r 为 $[0,1]$ 之间的随机数，I 为属于集合 $\{1,2\}$ 的随机数，PZ 表示先锋斑马的位置。

在第二阶段，模拟斑马对捕食者攻击的防御策略，以更新 ZOA 种群成员在搜索空间中的位置。斑马的捕食者包括狮子、猎豹、鳄鱼等，面对不同的捕食者采用不同的防御策略。在面对狮子时，会采用 Z 字形和随机转弯动作逃跑，而面对较小的捕食者，可能会采用较具攻击性的方式进行防御。在 ZOA 算法中，假设两种进攻策略以相同概率发生：

（1）　面对狮子，采取逃跑策略；

（2）　面对其他捕食者，采取攻击策略。

在第一种策略中，当受到狮子攻击时，斑马会在其他位置附近躲避狮子的攻击。而在第二种策略中，

当其他捕食者攻击其中一只斑马时，群中的其他斑马会向被攻击的斑马靠近，采取攻击策略。这两种策略的数学模型如（5）式所示。在更新斑马位置时，如果斑马在新位置中的目标函数具有更好的值，则接受该新位置，其更新条件如（5）式所示。

$$x_{i,j}^{new,P2}=\begin{cases}S_1: x_{i,j}+R\cdot(2r-1)\cdot(1-\dfrac{t}{T})\cdot x_{ij}, P_s\le 0.5\\ S_2: x_{i,j}+r\cdot(AZ_j-I\cdot x_{i,j}), else\end{cases} \tag{6}$$

$$X_i=\begin{cases}X_i^{new,P2}, F_i^{new,P2}<F_i\\ X_i, else\end{cases} \tag{7}$$

其中 t 是迭代次数，T 为最大迭代次数，R 为 0.01 的常数，P_s 为两种策略的切换概率，其值为[0,1]之间的随机数，AZ 为攻击斑马的状态。其算法流程图如图 4 所示。

3.5 损失函数

ZOA-ShareSpace 方法能够将潜在的不同模态的信息集成到统一的向量空间中。然而，在潜在共享信息编码器在学习过程中，可能会将一些模态特有信息映射到共享空间的同一位置，导致共享信息空间的信息被污染。为避免这种现象的发生。需要在损失函数 L 上引入一个额外的模块来实现一个共享信息语义上一致的空间。这样，可以使得模型能够学习不同模态的共享信息，并防止共享信息被污染。损失函数计算如下：

$$\mathcal{L}(y,\hat{y},s)=\mathcal{T}(y,\hat{y})+\frac{\lambda}{|M|}\sum_{(i,q)\in M\subseteq(\{1,\cdots,n\}_2)}\|s_i-s_q\|_2 \tag{8}$$

其中 $\lambda\in\mathbb{R}$ 是控制语义正则化强度的超参数，q 是任务特定损失函数，M 是所有模态对 $(\{1,\cdots,n\}_2)$ 的子集，并且 $\|s_i-s_q\|_2$ 表示两种不同模态 i 和 q 中相同样本映射到共享子空间后不同特征之间的欧几里得范数。

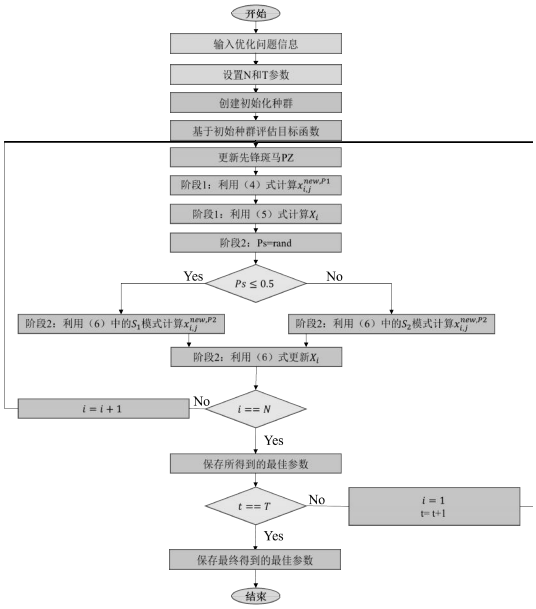


图 4. ZOA 算法流程

4 实验结果

我们使用从锌冶炼厂收集的实际数据训练和测试了我们提出的ZOA-ShareSpace方法，其中包括匹配的文本数据和带有故障的极板红外图像。首先，利用训练集数据对各个潜在编码器进行训练，其中，冻结ResNet18模型的最后一层外的所有参数。然后将各模态提取的潜在共享信息通过共享激活函数提取出共享子空间。然后，利用提取的共享子空间实现分类。如下表所示，ZOA-ShareSpare在所有指标上都优于最先进的单模态检测方法，并在复杂的分类任务中活得更好的性能。

表 1：实验结果对比

	LSTM	GRU	Resnet	ZOA-ShareSpace
Accuracy	0.6818	0.7273	0.6364	0.8636
Precision	0.7407	0.7833	0.7667	0.8783
Recall	0.6786	0.7262	0.6250	0.8690
F1-Score	0.6861	0.7277	0.6343	0.8660

5、结论

我们提出了一种基于ZOA-ShareSpace的共享子空间构建方法。该方法通过提取锌电解过程的红外图像和日志文本的共享信息，在一个共同的语义空间中实现了两种模态的统一表示。实验结果表明，该方法具有较高的准确性和稳定性，能够准确地实现对锌析出工况的分类。此外，我们还比较了与其他单模态模型的性能，结果表明多模态信息的融合有助于提高模型性能。综上所述，本研究为锌电解析出工况的分类提供了一种新思路和新方法，为实际工业生产具有一定的应用价值和推广意义，也为工业互联网的发展提供了新的道路。

参考文献：

[1] 桂卫华，阳春华，陈晓方，等. 有色冶金过程建模与优化的若干问题及挑战[J]. 自动化学报，2013，39(3)：197-207.

[2] 陈世超，崔春雨，张华，等. 制造业生产过程中多源异构数据处理方法综述[J]. 大数据，2020，6(05)：55-81.

[3] Zhang P，Li T，Wang G，et al. Multi-source information fusion based on rough set theory：A review[J]. Information Fusion，2021，68(4)：85-117.

[4] Chai L，Yi W，Hoseinnezhad R，et al. Heterogeneous multi-sensor fusion for PHD filter in decentralized sensor networks[J]. Information Fusion，2023，100(12)：101956.

[5] Li X，Fir D，Jean D. Multi-source information fusion：Progress and future[J]. Chinese Journal of Aeronautics，2024，44(12)，1-35.

[6] Zhou J，Hong X，Jin P. Information fusion for multi-source material data：progress and challenges[J]. Applied Sciences，2019，9(17)：3473.

[7] Alam F，Mehmood R，Katib I，et al. Data fusion and IoT for smart ubiquitous environments：A survey[J].

IEEE Access, 2017, 5(4): 9533-9554.
[8] 张红，程传祺，徐志刚，等. 基于深度学习的数据融合方法研究综述[J]. 计算机工程与应用，2020, 56(24): 1-11.
[9] Dominici, Gabriele, Pietro Barbiero, Lucie Charlotte Magister, Pietro Liò and Nikola Simidjievski. SHARCS: Shared Concept Space for Explainable Multimodal Learning. arXiv, 2023. http://arxiv.org/abs/2307.00316
[10] Biresaw T A, Cavallaro A, Regazzoni C S. Tracker-level fusion for robust Bayesian visual tracking[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2014, 25(5): 776-789.
[11] 苗亮亮, 陈先中, 侯庆文, 等. 高炉料面检测中的多源数据融合[J]. 光学精密工程, 2014,22(09):2407-2415
[12] MANISH K, DEVENDRAG，RANDY A Z. A generalized approach for inconsistency detection in data fusion from multiple sensors［J］. 2006 IEEE American Control Conference，2006(1) : 2078－2081.
[13] Ohadi B, Sun X, Esmaieli K, et al. Predicting blast-induced outcomes using random forest models of multi-year blasting data from an open pit mine[J]. Bulletin of Engineering Geology and the Environment: The official journal of the IAEG, 2020, 79(6):329-343.
[14] 姬文焱, 梁全东, 李科志, 等. 基于神经网络和 DS 证据理论的多传感器数据融合目标识别方法[J]. 网络安全与数据治理, 2023, 42(S2):193-201. DOI:10. 19358/j. issn. 2097-1788. 2023. S1. 076.
[15] Saeidi V, Pradhan B, Idrees M O, et al. Fusion of airborne LiDAR with multispectral SPOT 5 image for enhancement of feature extraction using Dempster–Shafer theory[J]. IEEE Transactions on Geoscience and Remote Sensing, 2014, 52(10): 6017-6025.
[16] Ibrahim S, Chen W, Zhu Y, et al. Knowledge graph guided simultaneous forecasting and network learning for multivariate financial time series[C]. Proceedings of the Third ACM International Conference on AI in Finance, 2022: 480-488.
[17] Cheng D, Yang F, Xiang S, et al. Financial time series forecasting with multi-modality graph neural network[J]. Pattern Recognition, 2022, 121(1): 108218.
[18] Jia Z, Guangchang D, Feng C, et al. A deep learning fusion recognition method based on SAR image data[J]. Procedia Computer Science, 2019, 147(2): 533-541.
[19] Liu X, Zhu X, Li M, et al. Multiple Kernel k-Means with Incomplete Kernels[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020, 42(5):1191-1204.
[20] Xu C, Guan Z, Zhao W, et al. Adversarial Incomplete Multi-view Clustering[C]//IJCAI. 2019: 3933-3939.
[21] Meng L, Tan A, Xu D. Semi-Supervised Heterogeneous Fusion for Multimedia Data Co-Clustering[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(9): 2293-2306.

作者简介：

周灿（1984-），男，博士，教授，研究领域为工业建模与模拟和自动化设备

许云晋（2000-），男，硕士研究生，研究方向为工业参数测量

面向工业的数据空间构建

王晨

大数据系统软件国家工程研究中心（清华大学）　北京　100084

清华大学软件学院　北京　100084

摘　要：数据空间构建是数据科学领域中一个关键的挑战，它不仅要解决技术问题，还要满足实际应用中的多样化需求。传统上，数据空间技术主要集中于分析数据在不同系统或存储介质中关联关系。传统数据空间技术只关注 IT 语义环境下的数据关联，而工业界更需要的是能够从业务角度解释数据关联的技术。本文介绍了一项新型面向工业的数据空间构建技术，它旨在满足工业界的实际需求，并具备解释业务语义的能力。这项技术将产品构成的 BOM（Bill of Materials）作为研究对象，采用业务流程模型来分析数据间的关联关系。此外，该方法还定义了一种链表结构，以支持自由的操作需求。文章提供了实现链表结构和数据空间构建过程的具体算法。

关键词：数据空间；业务过程模型；BOM

Data Space Construction for Industrial Applications

Chen Wang

National Engineering Research Center for Big Data Software, Tsinghua University, Beijing, 100084

School of Software, Tsinghua University, Beijing, 100084

Abstract: The construction of data space poses a critical challenge in the field of data science, encompassing not only technical issues but also the need to address diverse practical applications. Traditionally, data space technologies have primarily focused on establishing relationships between data across different systems or storage media. However, these approaches solely consider data relationships from an IT semantic perspective, while industries require technologies capable of interpreting business semantics. This paper presents a novel industry-oriented data space construction technology that aims to meet practical needs and interpret business semantics effectively. Specifically, this technology focuses on analyzing the correlation between data using a business process model with the BOM (Bill of Materials) of product composition as its research object. Moreover, it defines a linked list structure to support flexible operational requirements. The paper also provides specific algorithms for implementing both the linked list structure and the data space construction process.

Key words: data space, business process model, BOM

1　导言

在工业领域，构建一个面向数据的空间是至关重要的。数据一致性协议（DCP）能够保证数据连续空

间的形成，确保数据的关联关系相互依存。但在实际的工业生产过程中，产品从原材料到成品的转变涉及到多个生产阶段，每个阶段都会改变产品的具体属性。当产品完成所有生产阶段后，其数据空间也就被确定了。然而，DCP 在设计上存在一些局限性，它可能无法充分满足工业生产中对数据空间构建的特定需求，因为状态变化是由生产活动本身驱动的，而非靠人工标注所驱动的。

2 问题概述

DCP 在应用与工业领域时存在局限，它不能提供对产品或部件整个工业生产活动过程中数据的连贯性支持，这是获取所需信息的关键。在实际的工业生产中，生产流程可能会因各种因素而发生变动，这就要求数据空间能够灵活适应这些变化。基于这一逻辑，本文提出了一种新的工业数据空间构建方法，旨在克服 DCP 在满足工业生产数据空间构建能力方面的不足。通过这种方法，可以更有效地描述产品或部件在生产过程中的各个阶段的状态，确保数据的完整性和准确性，从而支持生产过程的监控、优化和管理。

工业企业普遍的数据现状和特点，决定了已有的数据空间技术与工业应用还存在不匹配不适应的情况。工业企业现有的以在用信息系统为主体所构成数据体系中，大量生产过程中上下文相关的有用信息在设计期就未被纳入相应的信息系之中。这些信息不是现有的数据空间技术能够恢复的，因为这些技术的目标和对象是对数据库中已有数据，在数据在不同的数据库之间传输和转换过程中的加工处理信息分析出来。两种场景从基于的目标和对象开始就完全不同，其过程中所用到的计算和分析技术也有很大区别。工业企业强调其数据体系在反映生产过程上下文时的严格性、准确性和完备性，而现有数据空间技术只能对数据库中已经存在的数据开展分析，但是很多数据库中不存在的数据并不代表其在生产过程中不发生不存在，并且很多时候这些数据对工业企业甚至可能更重要。

3 定义与符号

3.1 定义

本节将需要用到的概念和定义进行介绍。在介绍 APDP 之前，首先参考[6]中的内容，引入业务过程模型、过程实例和产品的物料清单 BOM 的形式化定义。

定义一：业务过程模型

业务过程模型（Business Process Model, BPM）是一种抽象化的表示方法，旨在捕捉、分析和优化组织中的业务流程。它通过定义流程中的活动、任务、决策点、输入输出以及这些元素之间的顺序和条件关系，提供了一个全面的业务视图。业务过程模型通常使用特定的符号和图形表示法，如业务流程模型和符号（Business Process Model and Notation, BPMN）标准，来确保模型的标准化和可读性。业务过程模型用于描述和分析组织内部业务流程的系统化方法。它通过图形化或文本化的方式，将业务流程中的各个环节、活动、决策点以及它们之间的逻辑关系清晰地展现出来。业务过程模型的核心价值在于其能够支持业务流

程的可视化、沟通、分析和改进。它允许组织识别流程瓶颈、冗余步骤和潜在的改进机会。此外，业务过程模型也是实现业务流程自动化和集成的关键工具，有助于提高效率、降低成本和增强客户满意度。业务过程模型可以作为工业描述生产过程的手段，支持用户深入理解特定业务流程的运作机制，评估不同管理策略的影响，或者开发新的业务流程设计原则。通过将业务过程模型与定量分析、模拟或其他研究方法相结合，可以更全面地探索业务流程的复杂性和动态性。

定义二：BOM

物料清单（Bill of Materials，简称 BOM）是一份详细列出制造产品所需的所有原材料、部件、组件和它们之间数量关系的文档。它是生产计划和库存管理的关键组成部分，对于确保生产过程的顺利进行至关重要。以下是 BOM 定义：

物料清单（BOM）是一种结构化的列表，它详细记录了制造特定产品所需的所有物料项，包括原材料、半成品、成品以及它们之间的层级和数量关系。BOM 不仅包括物料的类型和规格，还可能包含有关物料来源、供应商信息、替代物料以及生产过程中的特定要求等附加信息。BOM 通常以层次化的方式组织，显示了产品组件的分解结构，从而允许用户理解从原材料到最终产品的转换过程。这种层次化视图有助于识别产品结构的复杂性，评估物料需求，以及优化物料采购和库存管理策略。在实际工业生产中，BOM 可以作为统一语言，用于分析产品设计、生产效率、供应链管理以及成本控制等方面。通过研究 BOM 的结构和内容，设计者、制造者、用户都可以评估不同物料管理策略对生产成本和效率的影响，或者探索如何通过优化 BOM 来提高产品的市场竞争力和用户使用性。

BOM 在工业中的重要性不容忽视，它不仅关系到产品的质量和交货时间，还直接影响到企业的运营效率和成本控制。因此，深入理解和有效管理 BOM 对于任何从事产品制造的组织都是至关重要的。

3.2 符号与术语

本节介绍后续需要使用的各种符号。

设产品 A 的生产流程服从某业务过程模型描述的序列，我们用来 m 标记这一特定模型。对于产品 A 的生产过程中的任何特定时间点 t，对产品 A 的物料清单结构 b，我们用 b.A 来表示。

对于产品 A 中的任何一个零部件 A.c，用 m.A.c 来记录其生产过程。工业企业的价值和存在目的是制造产品，它们所追踪的关键指标均与产品及其各个部分（例如零部件）的物理化学属性紧密相关。在业务流程的每一步，业务活动的执行都扮演着“因”的角色，引发产品或零部件在某些指标上的变动，形成“果”。这些活动按顺序串联起来，就构成了一组数据空间的组成构建。同时，零部件的生产过程所对应的数据变化情况，构成了数据空间。数据空间是一种全面而量化的方法，用以详细记录产品或其零部件的生产过程。

4　数据空间的构建算法

在本节中，首先对数据空间的构建算法的核心理念和实现方式进行阐释。该算法分为两个关键部分：

预处理和数据体系关联算法。预处理阶段主要对产品的 BOM 进行遍历，以识别每个零部件所关联的数据变化与内在关系，然后计算出这些零部件生产过程中的完整数据空间。

在设计数据空间的数据结构时，应当兼顾两个方面：一是能够体现活动之间的先后关系；二是可以方便地进行向前和向后遍历。为此，可以将数据空间的元数据设计为链表，该链表的结点包括首结点（FN）和数据空间结点（DSN）。

Algorithm 1 产品 A 的数据空间 $D.A$

Require: 产品 A

Ensure: 产品 A 的生产业务过程 $A.m$

创建一个数据空间首头指针 fn

$fn.data = A.b$;

$fn.next = Null$;

return fn;

Algorithm 2 CreateDataSpaceNode

// 创建下一个数据空间结点

Require: 产品的 BOM 信息 $A.b$

Ensure: 指向生成的数据结点

if **then**

  构建一个数据空间结点 rn;

  $fn.nxt = pre$;

  $fn.ID = MID(j)$;

  $fn.nxt = Suctsk(iam_{c_f}[j][id])$;

  $fn.nxt = CreateDataSpaceNode(c_f, i_d, k, rn)$;// 递归地构建数据空间节点链表

else

  return $Null$;

end if

首结点，用来存储一个数据空间链表的指针，同时还需要指向因为业务过程的发生而产生的数据空间链表。数据空间链表由一系列结点串联，每个节点代表一个活动对应的数据。以上内容就是基于业务过程的工业数据空间的构建方法。

5 相关文献

本论文的主要贡献：

业务过程模型用作构建数据空间的工具。业务流程是实现生产和加工任务的有序活动序列，其能够解释数据和信息的因果关系。通过将业务过程模型作为数据空间构建的记录框架，能够确保数据空间的完整性和可解释性，每个活动都成为构建数据空间过程中的关键节点。

BOM结构数据直接反映工业生产活动中数据的存在载体：产品BOM结构明确了产品的所有组成部分，为数据空间的构建设定了具体目标。通过专注于产品变化及其对环境数据的反映，可以保证数据空间内容的集中性和实用性，防止技术方向的偏离，确保始终以产品的生产活动为中心。BOM结构支持数据空间的

结构完整性，BOM结构提供了在产品各个构成单元上定义和数据空间各组成片段间关系的能力。这些特性可以通过指标的向量化或矩阵化描述，赋予工业生产过程以高度的灵活性和分析能力，以适应不同的查询和分析需求。

6　总结

以往对数据空间的研究，主要集中在计算机科学领域数据库专业的科研人员，其视角主要局限于信息系统之间的互联互通。这样的方法的本质是“基于数据孤岛”的连接。这样的方法第一会依然是碎片化的数据体系，第二会同样无法反映面向生产过程的数据关联关系。本文立足于工业制造的实际需求，以产品生产流程为出发点，聚焦于产品的物料清单（BOM）。目标是跟踪产品在工业生产过程中数据关联关系的演变。通过开发合适的关联算法，实现一种数据空间的构建方法，它不仅易于理解，而且具有较低的存储和计算需求。

基金项目：国家自然科学基金委“未来工业互联网基础理论与关键技术”重大研究计划项目（92267203）

参考文献：（参考文献格式参照 2015 年新标准 GBT 7714-2015）

[1] Abadi D, Ailamaki A, Andersen D, et al. The seattle report on database research[J]. ACM SIGMOD Record, 2020, 48(4): 44-53.

[2] Simmhan, Y. L., Plale, B., & Gannon, D. (2005). A survey of data provenance. Computer techniques Science Department, Indiana University, Bloomington IN, 47405, 69.

[3] Wang Y R , Madnick S E .A Polygen Model for Heterogeneous Database Systems: The Source Tagging Perspective[C]//16th International Conference on Very Large Data Bases, August 13-16, 1990, Brisbane, Queensland, Australia, Proceedings.1990.

[4] Green T J, Karvounarakis G, Tannen V. Provenance semirings[C]//Proceedings of the twenty-sixth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. 2007: 31-40.

[5] Hartig O, Zhao J. Publishing and consuming provenance metadata on the web of linked data[C]//International Provenance and Annotation Workshop. Springer, Berlin, Heidelberg, 2010: 78-90.

[6] Kulkarni D. A provenance model for key-value systems[C]//5th USENIX Workshop on the Theory and Practice of Provenance (TaPP 13). 2013.

[7] N. Zheng, A. Alawini and Z. G. Ives, Fine-Grained Provenance for Matching & ETL[C]//2019 IEEE 35th International Conference on Data Engineering (ICDE), Macao, China, 2019, pp:184-195.

[8] Bourhis P , Deutch D , Moskovitch Y. Equivalence-Invariant Algebraic Provenance for Hyperplane Update Queries[C]//Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data, 2020.415-429.

[9] Jahanzeb, K.M., Ruoyu, W., Daniel, S., & Guoqiang, L. (2020). Data Provenance Based System for Classification and Linear Regression in Distributed Machine Learning[J]. Lecture Notes in Computer Science, 12028, 279-295..

[10] Yazici I M, Aktas M S. A novel visualization approach for data provenance[J]. Concurrency and Computation: Practice and Experience, 2022, 34(9): e6523.

[11] Aalst, Wil. (1999). On the automatic generation of workflow processes based on product structures. Computers in Industry. 39. 97-111.

[12] Peter Buneman and Wang-Chiew Tan. Data Provenance: What next?[J].ACM SIGMOD Record. 47, 3 (September 2018), 5-16.

[13] P. Buneman, A. Chapman, and J. Cheney.Provenance management in curated databases[C]//In Proceedings of the 2006 ACM SIGMOD international conference on Management of data (SIGMOD '06). Association for Computing Machinery, New York, NY, USA, 539–550..

[14] Cheney, James, Laura Chiticariu and Wang Chiew Tan.Provenance in Databases: Why, How, and Where[J]. Found. Trends Databases,2009, 1(4):379–474.

[15] Herschel M , Diestelkmper R , Lahmar H B . A survey on provenance: What for? What form? [C]//Very Large Data Bases.Springer Berlin Heidelberg, 26(6):881–906, 2017.

[16] G. Karvounarakis and T. J. Green. Semiring-annotated data: queries and provenance? [J].SIGMOD Record, 2012, 41(3):5–14.

[17] Y. R. Wang and S. E. Madnick. A polygen model for heterogeneous database systems: The source tagging perspective[C]//16th International Conference on Very Large Data Bases, August 13-16, 1990.

[作者简介]

王晨，1981 年生，副研究员，主要研究方向为数据库、工业大数据。

A High-Performance Data Collaborative Analysis Chain with Privacy Protection

Haonan Yan[1], Bin Wang[2]

Abstract—Collective perception and swarm intelligence collaborative learning have emerged as innovative paradigms in sensing and computation, pivotal for enhancing the efficacy of the industrial internet. However, these advancements have also brought to light a plethora of cybersecurity issues within industrial control systems, with the leakage of industrial data and user privacy information becoming a prominent concern. Traditional security measures are ill-equipped to address the novel security and privacy risks posed by the extensive interconnectivity of the future industrial internet. Consequently, this work introduces a high-performance collaborative data analysis chain with privacy protection. It achieves this through the optimization of distributed deep learning performance for consortium blockchains and the implementation of efficient swarm intelligence perception based on Bayesian differential privacy, thereby ensuring the privacy protection and high-performance analysis of data within the industrial internet.

Keywords— Future Industrial Internet, Consortium Blockchains, Differential Privacy, Swarm Intelligence Perception, Performance Optimization

1 Introduction

In recent years, with the increasing prominence of trends towards mobility, broadband, and intelligence in the information and communication industry, the integration and permeation of traditional industries with the internet and the Internet of Things have ushered in a new round of intelligent manufacturing transformation. As the scale of factory production continues to expand, the demand for industrial automation and information technology has surged dramatically. How to harmonize the use of the vast array of devices connected by the Industrial Internet of Things, analyze the vast amount of data in the production process, continuously optimize various business application processes, enhance the efficiency of production, material, and logistics automation systems, improve production management methods, and achieve labor cost reduction is a challenge facing every industry user. Collective perception and swarm intelligence collaborative learning are emerging as a new type of perception and computation model, which has become a hot topic of common concern in academia and industry. This model leverages the participatory and collaborative nature of groups to accomplish complex perception and computation tasks, characterized by high scalability, flexibility, and controllable data quality, making it an important technology for enhancing the efficiency of the industrial internet.

However, as the future industrial internet propels the current internet, which is centered on ”human-to-human” connections, towards a comprehensive ”human-machine-thing” interconnection, it significantly expands the boundaries and functionalities of cyberspace. This expansion also disrupts the traditional closed and highly reliable structure of industrial control systems, thereby exposing a plethora of cybersecurity issues. The interlacing and amplification of online and offline security risks have complicated the security landscape, posing a significant threat to the safety of industrial enterprises, public welfare, the national economy, and even the security of national development. The industrial internet, encompassing numerous critical manufacturing sectors, necessitates the concurrent advancement of a security safeguard

The part of Bin Wang’s work was supported by the Major Research Plan of the National Natural Science Foundation of China under Grant 92167203.

Haonan Yan. Xidian University, Xian 710126, China (e-mail: yanhaonan.sec@gmail.com).

Bin Wang. Zhejiang Key Laboratory of Artificial Intelligence of Things (AIoT) Network and Data Security, Hangzhou 310053, China (Corresponding Author, e-mail: wangbin02@xidian.edu.cn).

system to effectively avert safety production accidents and the loss of people's lives and property. Furthermore, the issue of industrial data and user privacy information leakage is becoming increasingly prominent. The industrial internet carries vital industrial data that is crucial to enterprise production, the lifeblood of the social economy, and even national security. Should this data be compromised or diverted overseas, it could threaten national security. Additionally, demands for personalized customization and service extension involve a vast amount of personal privacy, such as individual preferences and geographic locations, which are highly susceptible to theft and misuse in an open environment.

Furthermore, the core of future industrial internet construction lies in the "interconnection" of industrial control networks with other networks, with a focus on the "interoperability" of production data with other data types. As the industrial internet continues to deepen and advance, the traditional swarm intelligence collaborative systems within individual workshops or manufacturers can no longer meet the interconnected and interoperable requirements of future business scenarios. This has led to traditional security technologies being inadequate to address the new security and privacy risks brought about by the extensive interconnectivity of the future industrial internet. The key issues currently facing industrial internet security and privacy protection are: as traditional industrial control networks transition to the industrial internet, shifting from machine interconnection to extensive collaboration among humans, machines, and things, user privacy and corporate trade secrets have become inescapable security concerns. Therefore, this work, guided by the future network and data security needs of the industrial internet, explores collaborative learning schemes supported from the perspectives of data security and privacy protection, constructing an energy-efficient and highly secure edge intelligent computing architecture, it investigates methods for optimizing the performance of distributed deep learning for consortium blockchains and efficient swarm intelligence perception algorithms based on Bayesian differential privacy, ultimately achieving a high-performance collaborative data analysis chain with privacy protection.

The main contributions of this paper are as follows:

1. An optimization method for distributed deep learning performance oriented towards consortium blockchains. Leveraging hierarchical chaincode-based distributed analysis and fusion techniques to reduce the data transmission costs for users and enhance the data analysis and processing capabilities of the consortium blockchain.
2. A swarm intelligence perception algorithm based on Bayesian differential privacy. Utilizing Bayesian differential privacy to precisely add noise during the neighborhood perception information exchange phase among devices within a cluster, addressing the issue of traditional differential privacy methods having too significant an impact on the quality of service of business models.
3. Experimental validation of the proposed data analysis scheme. Extensive experimental results demonstrate that the proposed scheme has achieved effective improvements in terms of security and privacy while keeping costs within controllable limits.

2 Related Works

2.1 The High-Performance Collaborative Data Analysis Chain

Blockchain technology, serving as an effective decentralized trustworthy architecture solution, can effectively address the trust issues among participants in the future industrial internet. Researchers have proposed a series of blockchain-based schemes for the protection of industrial sensitive data and privacy. In the field of industrial internet applications, to counter the security and privacy challenges faced by applications, Lu et al. [1] designed a novel blockchain-authorized federated learning collaborative architecture. This architecture facilitates data sharing among distributed parties and further safeguards data privacy through differential privacy techniques. Industrial internet manufacturers typically collect user data and establish analytical models. Consequently, Zhao et al. [2] designed a blockchain-based federated learning system that employs a novel normalization technique to enhance model accuracy while protecting user privacy with differential privacy techniques. In the power industry, to address the tracking of energy usage without leaking user identities, Gai et al. [3] proposed a licensed blockchain edge model, PBEM-SGN. Furthermore, Gai et al. [4] designed a blockchain-enabled transaction model, PBT, which prevents attacks and conceals user privacy in energy transaction systems by generating noise. To reduce communication costs in the industrial internet, Fang et al. [5] introduced a new scheme, HFWP, which designed a lightweight encryption protocol aimed at providing provable privacy protection while maintaining the practicality of the model. In the scenario based on mobile edge computing, Kang et al. [6] designed a scheme based on reputation as a criterion for selecting trustworthy edge nodes for federated learning.

To ensure the confidentiality of industrial sensitive data and privacy information in the industrial internet, researchers have proposed cryptographic blockchain privacy protection schemes. Awan et al. [7] proposed a blockchain-based privacy-preserving federated learning framework. This framework performs gradient aggregation on private data based on a variant of the Paillier cryptosystem and uses a distributed ledger to record the information flow regarding gradient aggregation. Zhang et al. [8] combined the Chinese Remainder Theorem with Paillier homomorphic encryption to handle shared gradients, thereby achieving cost-effective and privacy-preserving federated learning. At the same time, Hao et al. [9] used homomorphic encryption and Laplace mechanism-based differential privacy technology to address threats arising from collusion between cloud servers and multiple users. To achieve secure aggregation, Zhou et al. [10] combined blinding algorithms with Paillier homomorphic encryption on the basis of ε-differential privacy to counter model attacks, realizing the secure aggregation of model parameters.

Although the aforementioned methods have resolved the trust issues among users in the industrial internet to some extent, due to the inherent overhead of blockchain, there are still aspects that merit further improvement in secure aggregation, service quality trade-offs, and efficiency optimization.

2.2 Data Analysis Chains with Privacy Protection

The modern industrial landscape necessitates an abundance of intelligent devices capable of swiftly recording diverse industrial data to provide real-time industrial services. Bi et al. [11] explored a novel model of swarm intelligence perception in the Internet of Things, known as Mobile Crowd-Sensing, which, due to its low cost and extensive coverage, can be applied to various environmental sensing industrial applications. In the industrial internet of things, industrial sensing tasks are delegated to workers for data collection and sharing; requesters can obtain sensing status by aggregating data from mobile workers.

The research on mobile crowd-sensing primarily encompasses five aspects: task allocation, worker selection, quality control, incentive mechanisms, and privacy protection. In the realm of task allocation, Cai et al. [12] proposed a two-stage sampling method with bounded variance, which includes an unbiased estimator based on sampling data and a perturbation mechanism designed for optimal differential privacy, to establish a pricing mechanism for task allocation. In terms of worker selection, Chen et al. [13] devised a greedy algorithm to select workers that cover the maximum number of sample points, yet this method did not consider the cost constraints of worker selection. Li et al. [14] utilized Lyapunov optimization to decompose long-term optimization problems into a series of real-time optimization problems, selecting the optimal workers for long-term environmental monitoring to maximize the utility of time-averaged data. In the domain of quality control, R. Alabduljabbar et al. [15] introduced a dynamic method that selects the most suitable quality control approach for a given task based on its type. Although these methods enhance the efficiency and quality of tasks in mobile crowd-sensing, they do not address the privacy concerns of users within the crowd-sensing context.

In the realm of crowd-sensing and user privacy, Ge et al. [16] proposed a privacy-preserving data processing method that optimizes the integration of effective information in data through genetic algorithms, balancing data privacy with data utility. Hussein et al. [17] put forward a blockchain-based privacy supervision method and employed genetic algorithms to optimize the data exchange process, maximizing the privacy protection effect. Xu et al. [18] suggested a joint optimization method for device utility, weighing the execution performance in the data transmission process against the privacy protection effect, enabling devices to transcend reliance on singular protection strategies. Sun et al. [19] utilized genetic algorithms to optimize the image perception structure based on convolutional neural networks, endowing the target network with greater plasticity and optimization outcomes compared to other networks.

Although the aforementioned methods contribute to resolving privacy issues in mobile crowd-sensing within the industrial internet, most do not comprehensively consider how to determine privacy protection thresholds and achieve maximum data usability, nor do they address how to perform efficient data reliability verification to mitigate the impact of data tampering. Therefore, it is imperative to devise novel privacy protection methods in the swarm intelligence perception of the industrial internet.

3 Method

3.1 Distributed Deep Learning Performance Optimization for Consortium Blockchains

Data vendors engaged in large-scale data analysis transactions may require the capability to upload data from remote locations. For instance, enterprises like power grids that are deployed and collect data across

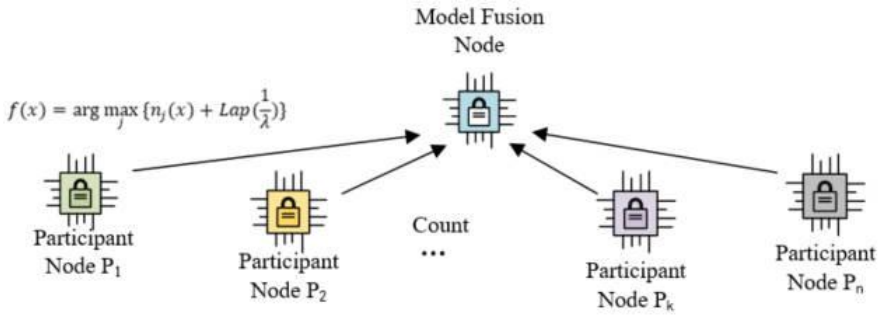


Figure 1 Performance optimization of distributed deep learning for alliance chains.

different geographical regions can benefit from uploading data locally to consortium blockchain nodes, thereby reducing data transmission costs. To protect privacy in the analysis of data stored remotely for big data analytics, this work proposes a distributed analysis and fusion technique based on tiered chaincodes, which diminishes the data transmission costs for users and enhances the data analysis and processing capabilities of the consortium blockchain.diag

Tiered chaincodes primarily consist of analysis chaincodes and fusion chaincodes, shown in Figure 1. The analysis chaincode is tailored for vendor data and performs an analysis of the vendor's data under supervision at the endorsing node, returning the transaction results to the fusion chaincode. The fusion chaincode aggregates all results from the analysis tasks of the same data analysis transaction, integrating the outcomes of the analysis chaincodes using distributed learning methods to analyze the vendor's data stored remotely. Specifically, the dataset on the endorsing node is divided into N equally sized, mutually exclusive data subsets (X_N, Y_N), which are independently trained to yield N preliminary learning models $f_{primary_i}$. The predictive results $f_{primary_i}(x)$ from each of these preliminary models are then used as inputs. A fused preliminary training model votes on and tallies the predictions for M categories, i.e., $n_j(x) = |\{i : i \in N, f_{primary_i}(x) = j\}|, j \in M$. By incorporating Laplace noise that satisfies ε-differential privacy, a senior learning model is trained

$$f(x) = \arg\max\{n_j(x) + Lap(\frac{1}{\lambda})\} \tag{1}$$

Here, ε represents the privacy budget for differential privacy, and the senior learning model is submitted as a secure sandbox output to the data user. This method not only prevents the impact on transmission and computational resources when dealing with large volumes of data but also reduces the number of noise additions, thereby maximizing the classification performance of the final model as much as possible.

The task allocation of the analysis chaincode and the selection of endorsing nodes can be regarded as a combinatorial optimization problem, shown in Figure 2. Given the distributed storage of the vendor's dataset, the buyer's analysis model, the consortium blockchain node data storage situation, and the cost of data distribution, the optimization goal is to minimize both the data distribution cost and the length of analysis time. By adjusting the deployment of the analysis chaincode tasks and the settings of the chaincode endorsing nodes, the task allocation and endorsing node selection of the analysis chaincode are achieved to meet the optimization objectives.

3.2 Bayesian Differential Privacy in Swarm Intelligence Perception Algorithms

To address the issue that traditional differential privacy methods significantly impact the service quality of business models, Bayesian differential privacy is proposed to apply precise noise during the neighborhood perception information exchange phase among devices within a cluster. This approach ensures the privacy of the perception data while striving to obtain higher-quality perceptual data characteristics. The distribution of perceptual data characteristics is extracted, and the Bayesian differential privacy loss calculation method is utilized, employing the Rényi divergence to continuously compute the privacy loss in each round of perceptual interaction. Under the condition of satisfying (ε, δ)-differential privacy, the amount of noise added is reduced. This encourages devices within the cluster to submit higher-quality perceptual data characteristics during the swarm intelligence information interaction process, thereby enhancing the service quality of the swarm intelligence business model.

The concept of Bayesian differential privacy is closely related to classical differential privacy. The difference lies in its consideration of the randomness of x' and the fulfillment of two assumptions: (1) All data in the per-

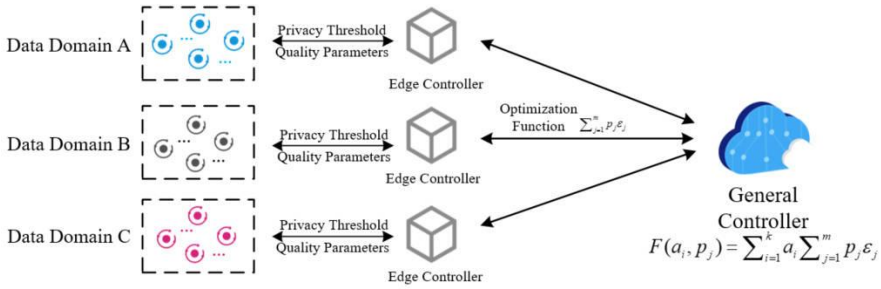


Figure 2　A multi-domain three-dimensional collaborative secure computing architecture underpinned by swarm intelligence.

ceptual information adhere to the same distribution $\mu(x)$. (2) All data points are exchangeable, meaning that any permutation of data points has the same joint probability. Its expression is as follows:

$$\Pr\left[L(w,D,D') \geq \varepsilon_\mu\right] \leq \delta_\mu,$$

where the probability $\Pr[L(w,D,D') \geq \varepsilon]$ depends on the randomness of the output result w and data x'. Applying differential privacy to swarm intelligence information interaction requires tracking privacy loss in each round of interaction. Calculating the privacy loss involves determining the R nyi divergence $D_\lambda(P\|Q)$ between model distributions through the probability density function of the business model distribution. Its expression is as follows:

$$D_\lambda(P\|Q) = \frac{1}{\lambda-1}\log\int\left[\frac{p(x)}{q(x)}\right]^{\lambda-1} p(x)\,dx,$$

where P and Q represent two different data distributions, and $p(x)$ and $q(x)$ represent the density functions of P and Q, respectively. Based on the calculated R nyi divergence $D_\lambda(P\|Q)$, the privacy loss during the t-th iteration can be computed. Its calculation expression is as follows:

$$c_t(\lambda) = \log \mathbb{E}_x\left[e^{(\lambda D_{(\lambda+1)}(p_t\|q_t))}\right],$$

where $p_t = p(w^{(t)}|w^{(t-1)},D)$ and $q_t = p(w^{(t)}|w^{(t-1)},D')$ represent the distribution of the model before and after noise addition, respectively.

According to the properties of Bayesian differential privacy and the advanced composition theorem, accumulating the privacy loss in each round of interaction yields the overall privacy loss of the neighborhood perception information interaction process within the entire cluster. As long as the privacy loss during the information interaction process does not exceed a specific threshold, privacy protection for business models in industrial internet scenarios can be achieved with a minimal amount of noise. The process is shown in Figure 3.

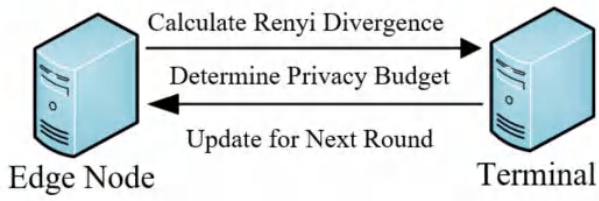


Figure 3　A swarm intelligence perception algorithm predicated on Bayesian differential privacy.

4　Experiments

4.1　Setting

4.1.1　Datasets

The widely utilized datasets MNIST, CIFAR-10, and FEMNIST are employed in this study. MNIST is a handwritten digit dataset comprising 60,000 training samples and 10,000 test samples, with each sample being a 28x28 grayscale image labeled from 0 to 9. CIFAR-10 is a collection of color images, encompassing 50,000 training samples and 10,000 test samples, where each instance is a 32x32 color image with three channels, categorized into ten classes such as ”airplane,” ”bird,” ”truck,” and so on. FEMNIST is a specialized dataset for heterogeneous handwritten digits and letters, containing 805,263 samples, each a 28x28 grayscale image, with labels encompassing the digits 0 to 9, lowercase letters a to z, and uppercase letters A to Z, totaling 62 classes. The dataset is partitioned using a 9:1 training-to-test ratio, allocating 90% for training samples and 10% for test samples.

4.1.2　Baselines

In this context, we compare our approach with the conventional consortium blockchain analysis and fusion (CCB) and the naive Gaussian differential privacy (NGDP).

4.1.3 Environments

This experiment is conducted on a server operating Ubuntu 22.04.4 LTS, equipped with two NVIDIA GeForce RTX 3090 graphics cards and CUDA version 12.1. The underlying blockchain-related components are managed using the Go programming language, while the model training aspects are implemented with the PyTorch framework, version 2.1.0. Interactions between Python and Go are facilitated by the Go-Python library.

4.2 Performance

4.2.1 Accuracy

We initially present the accuracy of the three methods across various datasets in Figure 4, demonstrating that while our approach exhibits a marginally lower precision compared to CCB, the NGDP experiences a significant decline under the same privacy budget. This observation underscores the enhanced utility of our proposed Bayesian Differential Privacy in Swarm Intelligence Perception Algorithms, which indeed maintains a higher level of performance under an equivalent degree of privacy protection.

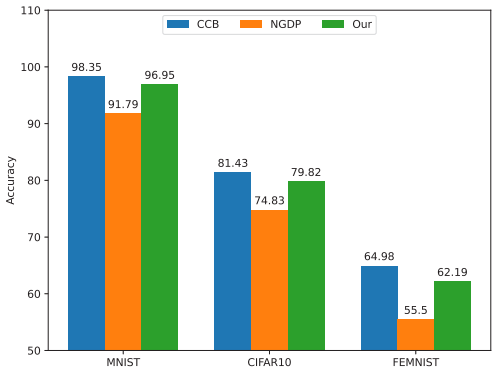


Figure 4 The accuracy of the three methods across various datasets.

To further substantiate this interpretation, we conducted an analysis of the two privacy protection methods under an identical privacy budget. Examination of the experimental results depicted in Figure 5 reveals that as the privacy budget expands, both schemes exhibit varying degrees of accuracy enhancement on the CIFAR-10 dataset. Notably, our proposed method consistently achieves higher model analytical precision than NGDP. This indicates that our approach indeed minimizes the addition of noise while ensuring compliance with (ε, δ)-differential privacy constraints, thereby enhancing the service quality of the swarm intelligence business model.

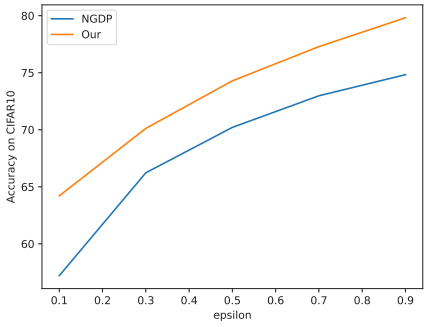


Figure 5 The accuracy comparison on the CIFAR-10 dataset.

4.2.2 Cost

Here, we also conducted experiments regarding cost. Conventional blockchains, without performance optimization, incur substantial data transmission and communication overhead. Our proposed scheme partitions the dataset on the endorsing nodes into N equally sized, mutually exclusive data subsets and trains preliminary learning models, with 62 subsets for the FEMNIST dataset and 10 for others, thereby reducing the overall expenditure to $\frac{1}{62}$ and $\frac{1}{10}$, respectively, as illustrated in Table 1.

Table 1 The cost comparison across various datasets.

Dataset	CCB	Our
MNIST	1	$\frac{1}{10}$
CIFAR10	1	$\frac{1}{10}$
FEMNIST	1	$\frac{1}{62}$

5 Conclusion

This work introduces an energy-efficient and secure edge intelligence computing architecture, culminating in a trusted computing platform that encompasses data security, privacy protection, and swarm intelligence collaborative learning functionalities. Utilizing the blockchain-based privacy protection technologies proposed in this work, we assess the secure interconnectivity and the trustworthiness of cross-domain data within the future industrial internet. Additionally, we validate the usability of the edge-side trusted security system in real-world, computation-aware industrial scenarios and its defensive capabilities against malicious attacks.

References

[1] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. Blockchain and federated learning for privacy-preserved data sharing in industrial iot. IEEE Transactions on Industrial Informatics, 16(6):4177–4186, 2019.

[2] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. Privacy-preserving blockchain-based federated learning for iot devices. IEEE Internet of Things Journal, 8(3):1817–1829, 2020.

[3] Keke Gai, Yulu Wu, Liehuang Zhu, Lei Xu, and Yan Zhang. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet of Things Journal, 6(5):7992–8004, 2019.

[4] Keke Gai, Yulu Wu, Liehuang Zhu, Meikang Qiu, and Meng Shen. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Transactions on Industrial Informatics, 15(6):3548–3558, 2019.

[5] Chen Fang, Yuanbo Guo, Na Wang, and Ankang Ju. Highly efficient federated learning with strong privacy preservation in cloud computing. Computers & Security, 96:101889, 2020.

[6] Jiawen Kang, Zehui Xiong, Dusit Niyato, Yuze Zou, Yang Zhang, and Mohsen Guizani. Reliable federated learning for mobile networks. IEEE Wireless Communications, 27(2):72–80, 2020.

[7] Sana Awan, Fengjun Li, Bo Luo, and Mei Liu. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, pages 2561–2563, 2019.

[8] Xianglong Zhang, Anmin Fu, Huaqun Wang, Chunyi Zhou, and Zhenzhu Chen. A privacy-preserving and verifiable federated learning scheme. In ICC 2020-2020 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2020.

[9] Meng Hao, Hongwei Li, Guowen Xu, Sen Liu, and Haomiao Yang. Towards efficient and privacy-preserving federated deep learning. In ICC 2019-2019 IEEE international conference on communications (ICC), pages 1–6. IEEE, 2019.

[10] Chunyi Zhou, Anmin Fu, Shui Yu, Wei Yang, Huaqun Wang, and Yuqing Zhang. Privacy-preserving federated learning in fog computing. IEEE Internet of Things Journal, 7(11):10782–10793, 2020.

[11] Mengnan Bi, Yingjie Wang, Zhipeng Cai, and Xiangrong Tong. A privacy-preserving mechanism based on local differential privacy in edge computing. China Communications, 17(9):50–65, 2020.

[12] Zhipeng Cai and Zaobo He. Trading private range counting over big iot data. In 2019 IEEE 39th international conference on distributed computing systems (ICDCS), pages 144–153. IEEE, 2019.

[13] Jiaoyan Chen and Jingsen Yang. Maximizing coverage quality with budget constrained in mobile crowd-sensing network for environmental monitoring applications. Sensors, 19(10):2399, 2019.

[14] Juan Li, Jie Wu, and Yanmin Zhu. Selecting optimal mobile users for long-term environmental monitoring by crowdsourcing. In Proceedings of the International Symposium on Quality of Service, pages 1–10, 2019.

[15] Reham Alabduljabbar and Hmood Al-Dossari. A dynamic selection approach for quality control mechanisms in crowdsourcing. IEEE Access, 7:38644–38656, 2019.

[16] Yong-Feng Ge, Jinli Cao, Hua Wang, Jiao Yin, Wei-Jie Yu, Zhi-Hui Zhan, and Jun Zhang. A benefit-driven genetic algorithm for balancing privacy and utility in database fragmentation. In Proceedings of the Genetic and Evolutionary Computation Conference, pages 771–776, 2019.

[17] Ahmed F Hussein, N ArunKumar, Gustavo Ramirez-Gonzalez, Enas Abdulhay, João Manuel RS Tavares, and Victor Hugo C de Albuquerque. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cognitive Systems Research, 52:1–11, 2018.

[18] Xiaolong Xu, Chengxun He, Zhanyang Xu, Lianyong Qi, Shaohua Wan, and Md Zakirul Alam Bhuiyan. Joint optimization of offloading utility and privacy for edge computing enabled iot. IEEE Internet of Things Journal, 7(4):2622–2629, 2019.

[19] Yanan Sun, Bing Xue, Mengjie Zhang, Gary G Yen, and Jiancheng Lv. Automatically designing cnn architectures using the genetic algorithm for image

classification. IEEE transactions on cybernetics, 50(9):3840–3854, 2020.

About the Authors

Haonan Yan, Ph.D. student at the School of Cyber Engineering, Xidian University, Xi'an, China. He received his bachelor's degree from Xidian University. His current research interests focus on trustworthy AI.

Bin Wang [corresponding author], Ph.D., professor of Zhejiang Key Laboratory of Multi-dimensional Perception Technology, Application and Cybersecurity and Xidian University. He received the Ph.D. degree from the China National Digital Switching System Engineering & Technological R&D Center. His research interests mainly include Internet of Things security, cryptography, artificial intelligence security, new network security architecture and so on.

Image semantic transmission method for downstream tasks of industrial Internet

LU Yanpeng[1], YAO Shengshi[1], NIU Kai[1,2], DONG Chao[1]

***Abstract*—With the expansion of the industrial Internet, an increasing array of devices such as industrial cameras and monitors are being integrated into industrial networks, leading to substantial demands for image transmission. Current industrial networks, however, are struggling to keep up with these demands, highlighting the urgent need for innovative solutions. In this paper, we introduce a novel image transmission system designed specifically for the downstream tasks of the industrial Internet. Our system leverages cutting-edge semantic communication and joint source-channel coding technologies to optimize the unique characteristics of industrial networks. This approach not only improves communication performance and resource utilization but also supports the downstream tasks of the industrial sector without disruption. We have extensively tested this method in actual industrial environments to verify its practicality and effectiveness.**

***Keywords*—semantic communications, industrial Internet, image transmission**

Manuscript received XX. XX, 2024; accepted XX. XX, 2024.

1. The Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications , Beijing 100876, China;

2. Department of Broadband Communication, Peng Cheng Laboratory, Shenzhen 518000.

This work is in part by the National Natural Science Foundation of China under Grant 92067202.

I. INTRODUCTION

The industrial internet, as the cornerstone of the fourth industrial revolution, has rapidly garnered widespread attention from the industrial sector since its inception. With the empowerment of the industrial internet, enterprises are able to construct more intelligent and efficient production management frameworks, which can not only significantly reduce production costs but also enhance the utilization efficiency of resources and the overall effectiveness of production.[1][2] The interconnection of all things is the foundation of the construction of the industrial internet. As the industrial internet evolves, more industrial production equipment is being networked to enhance automation and intelligence in production processes.[3] For example, integrating sensors for temperature and humidity can monitor equipment status and provide fault warnings. Additionally, industrial cameras enable continuous monitoring of production and quality inspections of products. Within the industrial internet framework, these devices generate real-time data and transmit it to the cloud for analysis.

However, with the increasing number of devices connected to the network, existing communication systems are struggle to meet the communication demands of the industrial internet for the real-time transmission of massive amounts of data. Therefore, in order to adapt to the development of

the industrial internet, there is an urgent need to develop more efficient transmission technologies to enhance the communication performance of industrial networks and meet their growing communication needs. This is not only related to the productivity improvement of individual enterprises but also to the healthy development of the entire industrial internet ecosystem.

Given that image sources have become the main transmission objects in modern industrial communication systems, this study is dedicated to designing a semantic communication network suitable for the transmission of image sources in industrial production scenarios. To this end, we choose the defect detection scenario in the industrial pharmaceutical production process to verify the performance of the designed network. In the industrial pharmaceutical production process, various defects such as missing pills, damaged or soiled drug bags may occur due to machine operation errors or equipment aging. These defective products need to be detected and removed in a timely manner during the production process to ensure the quality. Modern defect detection is mainly automated through various defect detection algorithms, which is more efficient and accurate than manual detection. To achieve cost reduction and centralized management, a widely adopted strategy is to deploy image acquisition devices at the production end and transmit the captured pharmaceutical images to the cloud for centralized detection.

However, with the expansion of production scale and the increase in production speed, the increase in image acquisition devices and the demand for image transmission make the industrial network gradually unable to support the transmission of massive product images, having to sacrifice image quality to meet communication requirements. The decline in image quality will directly affect the accuracy of defect detection. To address this challenge, this study applies the industrial semantic communication system based on semantic coding technology as the image transmission system, to optimize the communication performance of the industrial network and enhance the support capability of the industrial transmission network for related tasks.

The structure of this paper is arranged as follows: Section 2 will introduce related work. Section 3 will provide a detailed introduction to the design philosophy and overall architecture of the proposed semantic communication system. Section 3 will present the specific simulation results, a comparative analysis with traditional communication schemes, and verify the impact of the designed communication system on downstream tasks; finally, there will be a summary of the entire paper.

II. RELATED WORK

Current communication systems struggle to meet the demands of massive data volume and low-delay transmission in the industrial network. A critical observation is that the primary objective of machine-type communication diverges from the traditional goal of exact underlying message reconstruction. Instead, the emphasis is on enabling machines to make accurate inferences and timely, context-appropriate decisions and actions, which typically require only a subset of the information contained in original videos to complete their tasks. In other words, full-resolution videos, reconstructed for human vision, often have low practical value density for machine processing tasks[7]. This mismatch between existing communication methods and the need for machine-type communication has inspired the pursuit of more efficient transport methods. One

of the most promising developments in this field is the semantic communications.

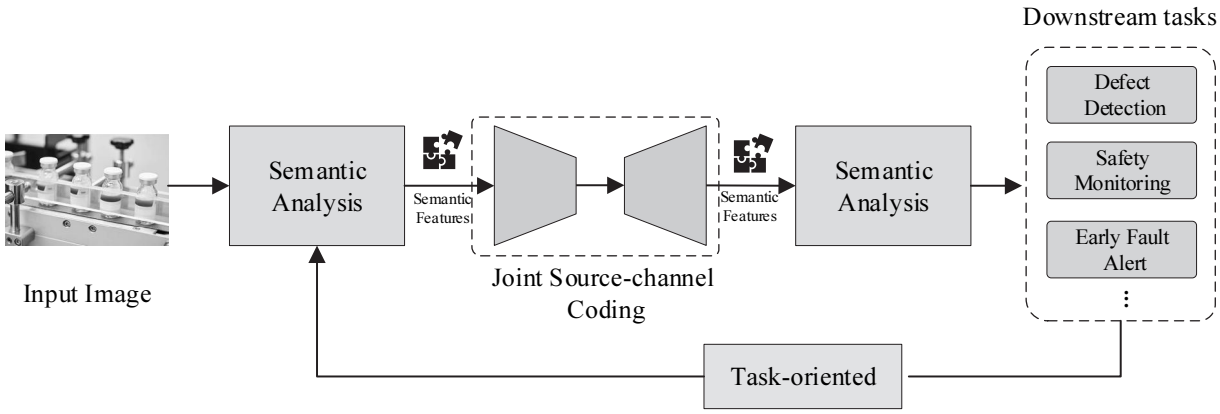


Figure 1 The overall architecture of proposed industrial semantic communication system.

Semantic communication technology, which diverges from traditional symbol-based communication, focuses on extracting and transmitting semantic information from the source through a constructed semantic encoder. Unlike conventional systems that require error-free transmission of source symbols, semantic communication prioritizes the accurate conveyance of semantic content, thereby enhancing error tolerance and overall system performance[8][11]. The integration of feature extraction and transmission processes aligns well with current industrial network requirements, suggesting a promising future for semantic communication systems.

III. SYSTEM ARCHITECTURE

In this section, we detail the architecture of the designed semantic communication system, outlining the image transmission process and discussing system implementation and optimization strategies.

A. ARCHITECTURE

The framework structure of the proposed industrial semantic communication system is shown in the Fig. 1. It demonstrates the overall process of semantically assisted industrial data acquisition, processing, transmission and final decision making. The scheme has the characteristics of multi-task compatibility and semantic interoperation. As shown in the figure, intelligent tasks such as fault warning and defect detection can be realized through semantic information processing to reduce human intervention in the manufacturing process. The framework first processes the massive data collected by multiple sensors and converts it into semantic features to reduce the amount of data. After the semantic information is extracted from the source, the extracted semantic information will be codec, that is, the symbol representing the semantic information will be converted into the symbol that can be transmitted directly in the channel. This process will further improve the utilization of communication resources.

When transmitting an image, the raw input image x is fed into a semantic encoder $g(\cdot)$, which transforms the raw data into low-level feature y. This feature extraction process is tailored to specific downstream tasks by incorporating task-specific losses into the loss function, ensuring that the features retain critical information for these tasks.

These features are then input into a joint source-channel coding module $h(\cdot)$, which converts them into symbols s which is suitable for transmission through noisy channels. At the receiving end, the inverse operation reconstructs the image from these symbols. The reconstructed image $\hat{x}$ is then processed by downstream task model $T(\cdot)$ to perform various functions. Thus, the diagram of the framework can be formulated as:

$$x \xrightarrow{g(\cdot)} y \xrightarrow{h(\cdot)} s \xrightarrow{channel} \hat{s} \xrightarrow{h'(\cdot),g'(\cdot)} \hat{x} \longrightarrow T(\cdot) \quad (1)$$

As mentioned above, thanks to the fit between semantic communication and machine-task oriented communication, features required for downstream tasks can be obtained only by filtering and fine-tuning features at the receiving end[5][9]. It supports multitasking compatibility well by inserting different feature filters based on task requirements. Semantics from sensors, log files, and other sources are aggregated to enable collaborative work between humans and machines.

B. SYSTEM IMPLEMENTATION AND OPTIMIZATION

In theory, the semantic communication system designed for industrial networks can handle any type of information source data transmission by implementing different neural networks for various modules within the framework. For instance, RNNs or Transformers can be used for processing text and voice data in industrial contexts, while CNNs or Transformer networks are suitable for image-like data. This paper specifically focuses on the transmission of image information sources, which constitute a significant portion of data in industrial networks. We primarily utilize CNNs and Transformers to implement the system, highlighting their effectiveness in this domain.

When optimizing the network, in order to make the system more scalable and support as many downstream tasks as possible, we want the network to retain the ability to reconstruct the underlying information of the source. Therefore, we take the reconstruction quality of the source image as one of the optimization goals of the system. Specifically, we use MSE to measure the similarity between the original image and the reconstructed image. However, when the channel conditions are poor, it is difficult to retain all the information of the source. However, the accuracy of several tasks can be guaranteed by adding the loss of these tasks to the optimization objective. In essence, this operation is equivalent to instructing the semantic communication system to preferentially retain the part of the original data when the channel conditions are limited. To sum up, the optimization function of the system can be written as follows:

$$L = \mathbb{E}_{x \sim p_x(x)}[\lambda R + d(x, \hat{x}) + (\alpha_1 l_1 + \alpha_2 l_2 + ...)] \quad (2)$$

Where x denotes original image, $\hat{x}$ denotes the reconstructed image, R denotes the coding rate, denote the task losses, λ and $(\alpha_1, \alpha_2, ...)$ are hyperparameters. Denotes the distortion between the original image and the reconstructed image. In this paper, we use MSE as the distortion loss:

$$d(\mathbf{x}, \tilde{\mathbf{x}}) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \tilde{x}_i)^2 \quad (3)$$

VI. EXPERIMENTAL

In order to verify the performance of the proposed semantic communication system in the industrial network, we deployed and verified the system in the actual industrial drug defect detection scenario. In this section, we will introduce the verification process and results in detail.

A. EXPERIMENTAL CONFIGURATION

The verification of the semantic communication system is carried out in the actual drug production scenario. The operation flow of the entire industrial drug defect detection system is shown in Fig. 2. The industrial drug production line includes a conveyor belt and an industrial camera mounted above it. As drugs move along the conveyor belt, the camera captures images of them. These images are then encoded by a semantic communication network and transmitted to a cloud server, where a defect detection algorithm analyzes the images to identify any discrepancies.

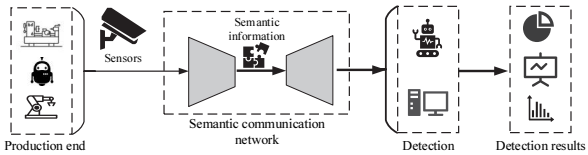
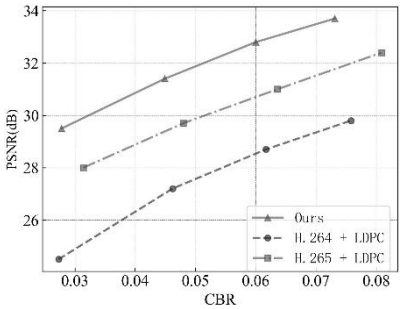


Figure 2 The operation flow of the defect detection system.

During implementation, to mimic the low-cost constraints typical in industrial settings, the semantic communication network's inference process operates on a single GTX 3060 GPU. The system's signal-to-noise ratio (SNR) is set at 10dB to align with the real-world demands of the industrial environment. For training data, approximately 10,000 images of drugs collected during production are used.

B. EXPERIMENTAL RESULTS

Fig. 3 and Fig.4 compare the image reconstruction quality of the industrial semantic communication system with two traditional communication schemes, "H.264 + LDPC" and "H.265 + LDPC," at the same compression rate. Image quality is evaluated using the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM). PSNR gauges the pixel-level similarity between the reconstructed and original images, while SSIM assesses their structural similarity. Considering that the proposed method is source channel joint coding, channel bandwidth ratio (CBR) and channel bandwidth radio (CBR) are used as the measurement



index of image compression. CBR represents the ratio of the number of symbols the source transmits in the channel to the number of symbols the source originally had. For image source, $CBR = k / m$, where k is the symbol number of the original image output after the source channel joint coding, and m is the number of pixels of the original image.

Figure 3 PSNR performance across three transmission methods.

In these figures, the solid line with a triangle icon represents the image reconstruction quality of our proposed semantic communication system, while the dashed lines with square and round icons correspond to the two traditional industrial network communication methods. The results demonstrate that our semantic communication system consistently outperforms the traditional methods in terms of

both pixel value (PSNR) and structural quality (SSIM) of the reconstructed images. Specifically, the semantic communication method achieves a PSNR improvement of about 4dB and an SSIM increase of 0.15 compared to the 'H.264 + LDPC' method. This performance gap widens under lower Constant Bit Rates (CBR), with differences reaching approximately 5dB in PSNR and 0.2 in SSIM. When compared with the 'H.265 + LDPC' method, the reconstructed image shows a PSNR improvement of about 2dB and an SSIM increase of 0.05.

In the industrial product defect detection scenario, the communication system not only needs to have powerful image compression coding and reconstruction capabilities, but also should have a fast image transmission speed to match the real-time needs of industrial production scenes. Therefore, we also calculated the average transmission processing time of the three methods for the images with three resolutions, as shown in Fig. 5.

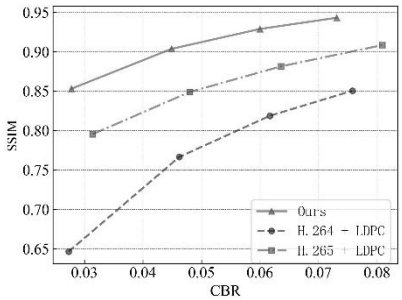


Figure 4 SSIM performance across three transmission methods.

It can be seen that compared with the traditional “H.264 + LDPC” communication method, the semantic communication method has a rate increase of more than 50%. Compared with the traditional “H.265 + LDPC” communication method, which has a slower transmission processing speed, the transmission rate is increased by dozens of times. The results show that the proposed industrial semantic communication network has excellent image processing speed, and can well meet the needs of high real-time in industrial data transmission scenarios.

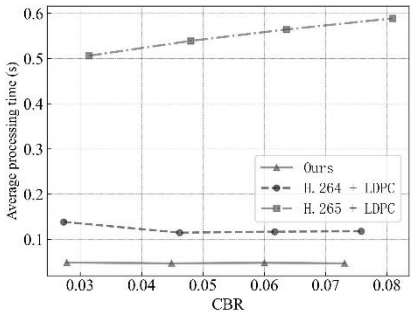


Figure 5 The average processing time of the three methods.

Data transmission in industrial scenarios is ultimately to complete downstream tasks in industrial production scenarios, so the accuracy rate of downstream tasks is also an important indicator to measure the applicability of the transmission system in industrial scenarios. We tested the impact of industrial semantic coding transmission system on downstream tasks in the actual drug production process. We tested 500 drugs on the computer, including about 100 damaged drugs.

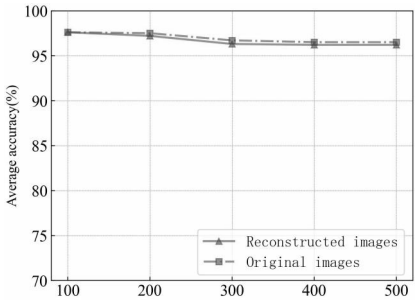
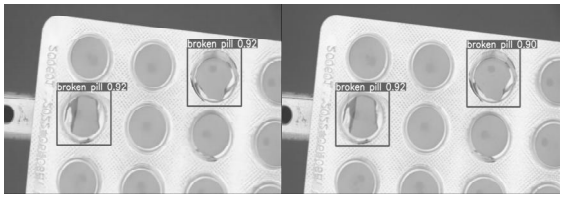


Figure 6 Comparison of detection accuracy based on original image and image reconstructed by proposed system.

The final test results are shown in Fig. 6. It can be seen that for each type of defect and all defects, the detection accuracy rate of semantic communication method is basically no different from that of original

image-based detection under the average accuracy index, which fully indicates that our method has powerful image compression and transmission capability, but will not affect the performance of downstream tasks in industrial network. It has a wide application prospect in the industrial data transmission scenario.



Detection results based on the original images　　Detection results based on reconstructed images

Figure 7 The actual drug test results.

Fig. 7 shows the results of actual drug image reconstruction and drug defect detection results. It can be seen that the reconstructed drug image has high clarity, and the defect detection results on the reconstructed image are basically consistent with those on the original image.

V. CONCLUSION AND FUTURE WORK

This paper addresses the growing data transmission demands of the industrial Internet by proposing an innovative semantic coding transmission system to enhance data compression and transmission performance in industrial networks. Initially, we analyze the communication challenges of the industrial Internet. Then, we introduce the basic principles and benefits of semantic communication technology and provide a detailed description of the architecture of our proposed industrial semantic communication system.

During the deployment verification phase, we tested the system in a real industrial drug defect detection scenario. The results demonstrate significant advantages of the designed system over traditional communication schemes in terms of image reconstruction quality, transmission speed, and downstream task performance, without negatively impacting task accuracy. These findings suggest that semantic communication technology has considerable potential to advance the industrial Internet, offering a promising avenue for future communication technology advancements.

References

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial internet of things: Challenges, opportunities, and directions,” IEEE transactions on industrial informatics, vol. 14, no. 11, pp. 4724–4734, 2018.

[2] U. Cisco, “Cisco annual internet report (2018–2023) white paper,” Cisco: San Jose, CA, USA, vol. 10, no. 1, pp. 1–35, 2020.

[3] W. Qin, S. Chen, and M. Peng, “Recent advances in industrial internet: insights and challenges,” Digital Communications and Networks, vol. 6, no. 1, pp. 1–13, 2020.

[4] C. E. Shannon and W. Weaver, The Mathematical Theory of Communication. The University of Illinois Press, 1949.

[5] K. Niu, J. Dai, S. Yao, S.Wang, Z. Si, X. Qin, and P. Zhang, “A paradigm shift toward semantic communications,” IEEE Communications Magazine, vol. 60, no. 11, pp. 113–119, 2022.

[6] S. Yao, Y. Lu, K. Niu, J. Dai, C. Dong, and P. Zhang, “Semantic information processing for interoperability in the industrial internet of things,” Fundamental Research, vol. 4, no. 1, pp. 8–12, 2024.

[7] D. G¨und¨uz, Z. Qin, I. E. Aguerri, H. S. Dhillon, Z. Yang, A. Yener, K. K. Wong, and C.-B. Chae, “Beyond transmitting bits: Context, semantics, and task-

oriented communications," IEEE Journal on Selected Areas in Communications, vol. 41, no. 1, pp. 5–41, 2022.

[8] Z. Chen, K. Fan, S. Wang, L. Duan, W. Lin, and A. C. Kot, "Intermediate deep feature compression: Toward intelligent sensing.," IEEE transactions on image processing: a publication of the IEEE Signal Processing Society, 2019.

[9] K. Fischer, F. Brand, and A. Kaup, "Boosting neural image compression for machines using latent space masking," arXiv preprint arXiv:2112.08168, 2021.

[10] X. Luo, H.-H. Chen, and Q. Guo, "Semantic communications: Overview, open issues, and future research directions," IEEE Wireless Communications, vol. 29, no. 1, pp. 210–219, 2022.

[11] J. Dai, S. Wang, K. Tan, Z. Si, X. Qin, K. Niu, and P. Zhang, "Nonlinear transform source-channel coding for semantic communications," IEEEJournal on Selected Areas in Communications, vol. 40, no. 8, pp. 2300–2316, 2022.

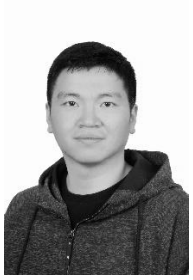
[12] E. Bourtsoulatze, D. B. Kurka, and D. G¨und¨uz, "Deep joint sourcechannelcoding for wireless image transmission," IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 3, pp. 567–579, 2019.

[13] W. Thomas, et al. "Overview of the H. 264/AVC video coding standard." IEEE Transactions on circuits and systems for video technology 13.7 (2003): 560-576.

[14] P., Christine, et al. "BPG: Seamless, automated and interactive visualization of scientific data." BMC bioinformatics 20 (2019): 1-5.

[15] J.-Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial internet: A survey on the enabling technologies, applications, and challenges," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1504–1526, 2017.

About the authors



LU Yanpeng received the B.S. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2022. He is currently pursuing the Master degree with Beijing University of Posts and Telecommunications. His research focuses on semantic communications and source and channel coding.

YAO Shengshi received the B.S. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2019. He is currently pursuing the Ph.D. degree with Beijing University of Posts and Telecommunications. His research focuses on semantic communications and source and channel coding.

Kai Niu received the B.S. degree in information engineering and the Ph.D. degree in signal and information processing from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 1998 in 2003, respectively. He is currently a Professor with the School of Artificial Intelligence, BUPT. Since 2008, he has been a Senior Member with the Chinese Institute of Electronics (CIE) and a committee member of the Information Theory Chapter of CIE. He currently serves as an Associate Editor with the IEEE Communications Letters. His research interests include coding theory and its applications, space-time codes and broadband wireless communication. (Email: niukai@bupt.edu.cn)

Modeling and Collaborative Control for Networked Heterogeneous Re-Entrant Manufacturing Systems

Chenguang Liu, Qing Gao, and Jinhu Lü

***Abstract*—This paper concentrates on the modeling and collaborative control problem for a class of networked heterogeneous re-entrant manufacturing systems (ReMSs). The framework for the networked manufacturing system encompasses the isolated production line, the manufacturing network and the networked workshop. In light of the principle of mass conservation, the linear hyperbolic partial differential equations are first given to describe the isolated production lines, based on which the dynamics of the workshop coupled by several different production lines are then established by the semilinear hyperbolic equations. An appropriate cooperative controller is designed to facilitate inter-workshop communication and fulfill the objective of market demand tracking. Computational simulations corroborate the efficacy of the proposed networked architecture and control scheme.**

***Index Terms*—Re-entrant manufacturing systems (ReMSs), networked heterogeneous system, intelligent manufacturing, industrial internet, coordinated regulation.**

I. Introduction

The importance of manufacturing systems in the future of industrial development is paramount, serving as the foundation for advancements in production technology and operational efficiency. As the demand for more sophisticated and efficient manufacturing processes grows, the re-entrant manufacturing systems (ReMSs) have gained substantial importance in diverse industrial sectors, such as the chemical material processing [1], the circuit board fabrication [2], and the semiconductor manufacturing [3]–[5], where work-in-progress (WIP) revisits the same workstation multiple times during production.

Up to now, extensive studies on ReMSs utilizing discrete event models like queuing networks [6], [7] and Petri nets [8], [9] have been documented. Nevertheless, as manufacturing systems expand in complexity and scale, the Petri net models often become excessively complex, complicating the analysis and control of ReMSs. Additionally, the queuing network modeling might fail when system dynamics are not adequately captured by queuing sequences [10]. To address these challenges, a full-continuum model using hyperbolic equations that is based on the conservative law has been employed to characterize RMSs [11]–[14]. In [10], the author used a nonlinear and nonlocal hyperbolic conservation law to model the continuous production flow of a high-volume, multistage re-entrant factory, proving the stability of the low-volume state while controlling output by adjusting the start rate to adapt to changing demand rates. In [12], the author first proposed the basic partial differential equation (PDE) model for single-product re-entrant manufacturing systems, and established the continuous model for multi-product ReMSs with different priorities by introducing a new state equation that considers the re-entrant degree of the product. In [13], the author applied the event-triggered controller to a continuous highly ReMSs, and derived the boundary controller and its feasible event generator through a Lyapunov argument to avoid the occurrence of Zeno behavior in the closed-loop system.

Collaborative intelligent manufacturing is increasingly emerging as a key trend and central aspect in the future evolution of the manufacturing sector. This advanced manufacturing framework typically includes a supply chain network comprising numerous manufacturing workshops spread across various regions, each featuring multiple production lines. Coordinating the production activities of these lines in real-time according to market demand is crucial for production capacity control, which can be addressed by networked modeling and control for ReMSs [15]–[21]. In [15], a cooperative state feedback control scheme based on a backstepping approach was presented to guarantee both the leaderless and the leader-follower output synchronization for a class of networked parabolic PDE systems. In [16], the synchronization gain problem for networked distributed parameter systems was investigated where both the constant and the time-varying synchronization gains were designed for regulation. In [17], the leader-follower synchronization for a class of networked unknown nonlinear systems was studied and distributed adaptive cooperative controllers were devised to address the robust synchronization. The above-mentioned approaches all focused on general networked PDE systems and indicate the potential of utilizing distributed cooperative regulation to achieve synchronous production activities in ReMSs. Although some control methods such as the event-triggered control [13] and the fuzzy control [22], [23], have been preliminarily used to explore ReMSs, the networked modeling of ReMSs and the collaborative control of systems based on networked ReMSs remain an open topic.

In this work, the modeling and collaborative control problem for the networked heterogeneous ReMSs is investigated. Unlike the existing ReMSs, which consist of either a single isolated production line [13] or simple parallel architectures with multiple lines [22], the heterogeneous networked ReMSs are established in this paper. The manufacturing systems fea-

This work was supported by the National Key Research and Development Program of China under Grant 2022YFF0902800. *(Corresponding author: Qing Gao.)*

Chenguang Liu is with the Institute of Artificial Intelligence, Beihang University, Beijing 100191, China (e-mail: chenguangliu@buaa.edu.cn).

Qing Gao and Jinhu Lü are with the School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, P. R. China and also with the Zhongguancun Laboratory, Beijing, P. R. China (e-mails: gaoqing@buaa.edu.cn; jhlu@iss.ac.cn.)

ture complex coupling relationships, encompassing production lines with different functionalities, manufacturing networks formed by the coupling of these varied functional lines, and networked workshops capable of information exchange. The appropriate cooperative controllers are designed to guarantee the product density can track the market demand. Simulations from a numerical example validate the effectiveness of the networked structure and the cooperative controllers.

Notations: $\eta_1(\cdot)$ and $\eta_2(\cdot)$, respectively, denote the smallest and the largest eigenvalues. $\otimes$ is the Kronecker product. For any $\theta(t,\omega) = (\theta_1(t,\omega), \theta_2(t,\omega), \ldots, \theta_n(t,\omega))^T \in \mathbb{R}^n$ with $(t,\omega) \in \mathbb{R}^+ \times [0,l]$ where $0 < l \leqslant 1$ and n is a positive integer, one has $\|\theta(t,\cdot)\|_2^2 = \sum_{p=1}^{n} \int_0^l \theta_p^2(t,\omega)d\omega$.

II. System Modeling and Problem Formulation

A. System Modeling

In this work, the networked architecture for the heterogeneous ReMSs is showed in the Fig. 1, including the isolated production line, the manufacturing network and the networked workshop.

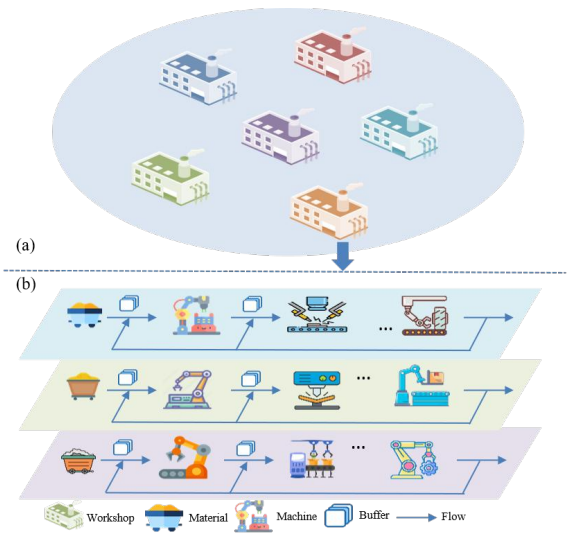


Fig. 1. Networked architecture of ReMSs.

1) Production Line: In an isolated re-entrant manufacturing line with numerous workstations consisting of manufacturing machines and buffer pools, as displayed in Fig. 1. (b), the WIP cycles through the different workstations for processing or assembly at different manufacturing machines until the products that meet the requirements are finished. According to the conservation law, the following hyperbolic equation describes an isolated re-entrant manufacturing line [10]:

$$\frac{\partial \mu(t,\omega)}{\partial t} + \delta \frac{\partial \mu(t,\omega)}{\partial \omega} = 0,$$

where $t \in [0,+\infty)$ is the time variable, $\omega \in [0,1]$ denotes the completion of WIP; $\mu(t,\omega) \in \mathbb{R}$ indicates the density of WIP at $\omega \in [0,1]$ and $t \in [0,+\infty)$; $0 \leqslant \delta \in \mathbb{R}$ describes the running velocity of production line.

2) Manufacturing Network: To increase the diversification of production and meet the customized market demand, a workshop tend to form a manufacturing network that coupled by many production lines with different functionalities. Thereby, the dynamics of manufacturing network can be further established as follows:

$$\frac{\partial \mu^i(t,\omega)}{\partial t} = -\delta^i \frac{\partial \mu^i(t,\varphi)}{\partial \omega} + \sum_{j=1}^{m} c^{ij} y^j(\mu^j(t,\omega)), \quad (1)$$

in which $i,j = 1,2,...,m$, m denotes the number of production lines in a workshop; $\mu^i(t,\omega) \in \mathbb{R}$ is the density of WIP in the ith production line; $0 \leqslant \delta^i \in \mathbb{R}$ is the running velocity of the ith production line; $y^j(\cdot)$ is the material flow from the production line j to the production line i, and $c^{ij} \in \mathbb{R}$ is the coupling strength between the production i and the production j; $y^j(\cdot)$ is Lipschitz continuous with the constant $\vartheta^j \in \mathbb{R}$.

3) Networked Workshop: To accomplish large-scale customized production tasks, an intelligent manufacturing plant typically consists of numerous workshops with different manufacturing tasks. These workshops are located in various regions, forming a complex networked system with upstream and downstream structures. By acquiring production information from neighboring workshops, these workshops can adjust their own production to prevent severe overproduction or underproduction. Thus, the nominal system for the ith production line of the pth workshop can be established as follows:

$$\frac{\partial \mu_p^i(t,\omega)}{\partial t} = -\delta_p^i \frac{\partial \mu_p^i(t,\omega)}{\partial \omega} + \sum_{j=1}^{m} c_p^{ij} y_p^j(\mu_p^j(t,\omega)), \quad (2)$$

where $p = 1,2,\ldots,n$, n is the number of workshops in the networked ReMSs; $\mu_p^i(t,\omega) \in \mathbb{R}$ and δ_p^i represent the density of WIP and the running velocity of the ith production line of the pth workshop, respectively. $y_p^j(\cdot)$ and $c_p^{ij} \in \mathbb{R}$ denote the material flow and the coupling strength between the production i and the production j in the the pth workshop.

Further, to enable information transfer among workshops, define the triple $\mathcal{W} = \{\mathcal{X}, \mathcal{Y}, Z\}$ as the communication topology where $\mathcal{X} = \{1,2,\ldots,n\}$ is the node set, $\mathcal{Y} \subset \mathcal{X} \times \mathcal{X}$ is the edge set and $Z \in \mathbb{R}^{n\times n}$ is the weighted adjacency matrix. The set of neighbors of the qth workshop is denoted by $\mathcal{U}_q = \{p \in \mathcal{X} : (q,p) \in \mathcal{Y}\}$. The element z_{pq} of Z satisfies the following condition: if $q \in \mathcal{U}_p$, $z_{pq} = z_{qp} > 0$, otherwise, $z_{pq} = z_{qp} = 0 (p \neq q)$, and $z_{pp} = -\sum_{\substack{q=1 \\ q\neq p}}^{n} z_{pq}$. Define

$$\begin{aligned}
&y_p(\mu_p(t,\omega)) = (y_p^1(\mu_p^1(t,\omega)), \ldots, y_p^m(\mu_p^m(t,\omega)))^T \in \mathbb{R}^m,\\
&\mu_p(t,\omega) = (\mu_p^1(t,\omega), \mu_p^2(t,\omega), \ldots, \mu_p^m(t,\omega))^T \in \mathbb{R}^m,\\
&0 \leqslant \Xi_p = \mathrm{diag}((\vartheta_p^1)^2, (\vartheta_p^2)^2, \ldots, (\vartheta_p^m)^2) \in \mathbb{R}^{m\times m},\\
&0 \leqslant U_p = \mathrm{diag}(\delta_p^1, \delta_p^2, \ldots, \delta_p^m) \in \mathbb{R}^{m\times m},\\
&C_p = (c_p^{ij})_{m\times m} \in \mathbb{R}^{m\times m},
\end{aligned}$$

then the dynamics of the pth workshop under the control input $\varphi_p(t,\omega) \in \mathbb{R}^m$ can be reformulated as the following compact form:

$$\frac{\partial \mu_p(t,\omega)}{\partial t} = -U_p \frac{\partial \mu_p(t,\omega)}{\partial \omega} + C_p y_p(\mu_p(t,\omega)) + \varphi_p(t,\omega), \quad (3)$$

subject to the initial and Dirichlet boundary conditions:

$$\mu_p(0,\omega)=\mu_p^*(\omega),\ \omega\in[0,l],$$
$$\mu_p(t,0)=\mu_e,\ t\in[0,+\infty),$$

where $0\leqslant\mu_p^*(\omega)$ is a continuous function and $0\leqslant\mu_e\in\mathbb{R}$.

B. Problem Formulation

Generally, manufacturing systems aim to minimize inventory costs and production waste by aligning product density in workshops with real-time market demand. This ensures that the dynamic evolution of all workshops ultimately synchronizes with market demand. Consequently, for a given market demand $\mu_e(t,\omega)=(\mu_e^1(t,\omega),\mu_e^2(t,\omega),\ldots,\mu_e^3(t,\omega))^T\in\mathbb{R}^m$, it must represent one of the evolutionary states of the workshop dynamics (3), satisfying the following equation:

$$\frac{\partial\mu_e(t,\omega)}{\partial t}=-U_p\frac{\partial\mu_e(t,\omega)}{\partial\omega}+C_py_p(\mu_e(t,\omega)).$$

This study aims to design a cooperative control strategy ensuring that the solution $\mu_p(t,\omega)$ of the re-entrant manufacturing system (3) synchronizes with the market demand $\mu_e(t,\omega)$, satisfying the following condition:

$$\lim_{t\to+\infty}\|\mu_p(t,\cdot)-\mu_e(t,\cdot)\|_2=0,p=1,2,\ldots,n. \tag{4}$$

III. Main Results

For simplicity, let the difference between $\mu_p(t,\omega)$ and $\mu_q(t,\omega)$ be represented as $\mu_{pq}(t,\omega)\triangleq\mu_p(t,\omega)-\mu_q(t,\omega)$. To accomplish the control objective of tracking market demand, the following synchronization controller, comprising an error feedback component and a networked component, is proposed:

$$\varphi_p(t,\omega)=-B[\mu_p(t,\omega)-\mu_e(t,\omega)]-D\sum_{q\in\mathcal{U}_p}z_{pq}\mu_{pq}(t,\omega), \tag{5}$$

where $p,q=1,2,\ldots,n$; $B=\mathrm{diag}(b_1,b_2,\ldots,b_m)\in\mathbb{R}^{m\times m}$ and $D=\mathrm{diag}(d_1,d_2,\ldots,d_m)\in\mathbb{R}^{m\times m}$ are both the feedback gain matrix to be determined.

Theorem 3.1. The solution $\mu_p(t,\omega)$ of the re-entrant manufacturing system (3) is able to converge to the market demand $\mu_e(t,\omega)$ by leveraging the state feedback controller (5) if the matrices B and D satisfying the following inequality:

$$\frac{1}{2}(CC^T+\Xi)-(I_n\otimes B)+(Z\otimes D)\leqslant 0, \tag{6}$$

where $C=\mathrm{diag}(C_1,C_2,\ldots,C_n)\in\mathbb{R}^{mn\times mn}$ and $\Xi=\mathrm{diag}(\Xi_1,\Xi_2,\ldots,\Xi_n)\in\mathbb{R}^{mn\times mn}$.

Proof. Define error vector $\theta_p(t,\omega)=\mu_p(t,\omega)-\mu_e(t,\omega)$, then the closed-loop control system formed by (3) and (5) can be obtained such that:

$$\begin{aligned}\frac{\partial\theta_p(t,\omega)}{\partial t}&=-U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}+C_py_p(\mu_p(t,\omega))-C_py_p(\mu_e(t,\omega))\\&\quad-B[\mu_p(t,\omega)-\mu_e(t,\omega)]-D\sum_{q\in\mathcal{U}_p}z_{pq}\mu_{pq}(t,\omega)\\&=-U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}+C_p[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))]\\&\quad-B\theta_p(t,\omega)-D\sum_{\substack{q=1\\q\neq p}}^{n}z_{pq}[\mu_p(t,\omega)-\mu_q(t,\omega)]\\&=-U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}+C_p[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))]\\&\quad-B\theta_p(t,\omega)-D\sum_{q=1}^{n}z_{pq}\mu_q(t,\omega)\\&=-U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}+C_p[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))]\\&\quad-B\theta_p(t,\omega)+D\sum_{q=1}^{n}z_{pq}[\theta_q(t,\omega)+\mu_e(t,\omega)]\\&=-U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}+C_p[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))]\\&\quad-B\theta_p(t,\omega)+D\sum_{q=1}^{n}z_{pq}\theta_q(t,\omega).\end{aligned} \tag{7}$$

Taking $\theta(t,\omega)=(\theta_1^T(t,\omega),\theta_2^T(t,\omega),\ldots,\theta_n^T(t,\omega))^T\in\mathbb{R}^{nm}$, one can design the following Lyapunov energy function:

$$\begin{aligned}S(t)&=\frac{1}{2}\int_0^l\theta^T(t,\omega)\theta(t,\omega)d\omega\\&=\frac{1}{2}\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)\theta_p(t,\omega)d\omega.\end{aligned} \tag{8}$$

Taking the derivative of (8), one deduces

$$\begin{aligned}\dot{S}(t)&=\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)\frac{\partial\theta_p(t,\omega)}{\partial t}d\omega\\&=\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)\Big[C_p[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))]\\&\quad-U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}-B\theta_p(t,\omega)+D\sum_{q=1}^{n}z_{pq}\theta_q(t,\omega)\Big]d\omega\\&=\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)C_p[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))]d\omega\\&\quad-\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}d\omega\\&\quad-\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)B\theta_p(t,\omega)d\omega\\&\quad+\sum_{p=1}^{n}\sum_{q=1}^{n}\int_0^l z_{pq}\theta_p^T(t,\omega)D\theta_q(t,\omega)d\omega.\end{aligned} \tag{9}$$

Since $y^j(\cdot)$ are the Lipschitz continuous with constant ϑ^j, one can infer that

$$\begin{aligned}&\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)C_p\left[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))\right]d\omega\\&\leqslant\frac{1}{2}\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)C_pC_p^T\theta_p(t,\omega)d\omega\\&\quad+\frac{1}{2}\sum_{p=1}^{n}\int_0^l\left[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))\right]^T\\&\quad\times\left[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))\right]d\omega\\&\leqslant\frac{1}{2}\sum_{p=1}^{n}\int_0^l\theta_p^T(t,\omega)C_pC_p^T\theta_p(t,\omega)d\omega\end{aligned}$$

$$+\frac{1}{2}\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)\Xi_p\theta_p(t,\omega)d\omega. \tag{10}$$

By the integral operation and the boundary condition, one can obtain that

$$\begin{aligned}
&-\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}d\omega\\
&=\sum_{p=1}^{n}\int_0^l \frac{\partial\theta_p^T(t,\omega)}{\partial\omega}U_p\theta_p(t,\omega)d\omega\\
&\quad-\sum_{p=1}^{n}\theta_p^T(t,\omega)U_p\theta_p(t,\omega)|_{w=0}^{w=l}\\
&=\sum_{p=1}^{n}\int_0^l \frac{\partial\theta_p^T(t,\omega)}{\partial\omega}U_p\theta_p(t,\omega)d\omega\\
&\quad-\sum_{p=1}^{n}\theta_p^T(t,l)U_p\theta_p(t,l)\\
&\leqslant\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}d\omega.
\end{aligned} \tag{11}$$

Further, it can be acquired from (9)-(11) that

$$\begin{aligned}
\dot{S}(t)&=\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)C_p[y_p(\mu_p(t,\omega))-y_p(\mu_e(t,\omega))]d\omega\\
&\quad-\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)U_p\frac{\partial\theta_p(t,\omega)}{\partial\omega}d\omega\\
&\quad-\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)B\theta_p(t,\omega)d\omega\\
&\quad+\sum_{p=1}^{n}\sum_{q=1}^{n}\int_0^l z_{pq}\theta_p^T(t,\omega)D\theta_q(t,\omega)d\omega\\
&\leqslant\frac{1}{2}\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)C_pC_p^T\theta_p(t,\omega)d\omega\\
&\quad+\frac{1}{2}\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)\Xi_p\theta_p(t,\omega)d\omega\\
&\quad-\sum_{p=1}^{n}\int_0^l \theta_p^T(t,\omega)B\theta_p(t,\omega)d\omega\\
&\quad+\sum_{p=1}^{n}\sum_{q=1}^{n}\int_0^l z_{pq}\theta_p^T(t,\omega)D\theta_q(t,\omega)d\omega\\
&=\frac{1}{2}\int_0^l \theta^T(t,\omega)CC^T\theta(t,\omega)d\omega\\
&\quad+\frac{1}{2}\int_0^l \theta^T(t,\omega)\Xi\theta(t,\omega)d\omega\\
&\quad-\int_0^l \theta^T(t,\omega)(I_n\otimes B)\theta(t,\omega)d\omega\\
&\quad+\int_0^l \theta^T(t,\omega)(Z\otimes D)\theta(t,\omega)d\omega\\
&=\int_0^l \theta^T(t,\omega)\Big[\frac{1}{2}(CC^T+\Xi)-(I_n\otimes B)\\
&\quad+(Z\otimes D)\Big]\theta(t,\omega)d\omega.
\end{aligned} \tag{12}$$

Then it follows from (6) and (12) that

$$\begin{aligned}
\dot{S}(t)&\leqslant\eta_2(\Gamma)\int_0^l \theta^T(t,\omega)\theta(t,\omega)d\omega\\
&=\eta_2(\Gamma)\|\theta(t,\cdot)\|_2^2,
\end{aligned} \tag{13}$$

where $\Gamma=\frac{1}{2}(CC^T+\Xi)-(I_n\otimes B)+(Z\otimes D)$.

Further, on the basis of (8) and (13), one can infer that

$$\dot{S}(t)-2\eta_2(\Gamma)S(t)\leqslant 0. \tag{14}$$

Then, it can be deduced from (14) that

$$\begin{aligned}
&\int_0^t[\mathrm{e}^{-2\eta_2(\Gamma)\beta}\dot{S}(\beta)-2\eta_2(\Gamma)\mathrm{e}^{-2\eta_2(\Gamma)\beta}S(\beta)]d\beta\\
&=\int_0^t[\mathrm{e}^{-2\eta_2(\Gamma)\beta}S(\beta)]'d\beta\\
&\leqslant 0,
\end{aligned}$$

which further yields

$$S(t)\leqslant S(0)\mathrm{e}^{2\eta_2(\Gamma)t}. \tag{15}$$

In light of (8) and (15), one yields

$$\|\theta(t,\cdot)\|_2\leqslant\sqrt{2S(0)}\mathrm{e}^{\eta_2(\Gamma)t},$$

which implies that

$$\lim_{t\to+\infty}\|\theta(t,\cdot)\|_2=0.$$

As a result, the proof of Theorem 3.1 is finished.

IV. Simulations

This section presents simulation results to illustrate the networked architecture proposed in Section II and the cooperative control strategy from Section III. A networked ReMS consisting of five distinct workshops, each equipped with three production lines, is considered. The corresponding parameter settings are as follows:

$$C_1=\begin{pmatrix}0.24&0.34&0\\0.34&0.85&0.22\\0&0.22&0.45\end{pmatrix},\ U_1=\begin{pmatrix}0.3&0&0\\0&0.8&0\\0&0&0.2\end{pmatrix},$$

$$C_2=\begin{pmatrix}0.15&0.25&0.7\\0.25&0.55&0.32\\0.7&0.32&0.85\end{pmatrix},\ U_2=\begin{pmatrix}0.2&0&0\\0&0.4&0\\0&0&0.7\end{pmatrix},$$

$$C_3=\begin{pmatrix}0.03&0&0.2\\0&0.45&0.22\\0.2&0.22&0.55\end{pmatrix},\ U_3=\begin{pmatrix}0.5&0&0\\0&0.4&0\\0&0&0.3\end{pmatrix},$$

$$C_4=\begin{pmatrix}0.25&0&0\\0&0.35&0\\0&0&0.45\end{pmatrix},\ U_4=\begin{pmatrix}0.1&0&0\\0&0.3&0\\0&0&0.2\end{pmatrix},$$

$$C_5=\begin{pmatrix}0.1&0.35&0.15\\0.35&0.45&0\\0.15&0&0.45\end{pmatrix},\ U_5=\begin{pmatrix}0.6&0&0\\0&0.9&0\\0&0&0.4\end{pmatrix},$$

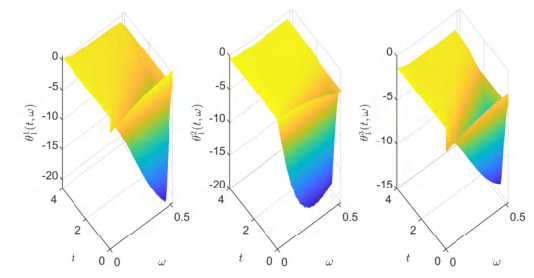


Fig. 2. Evolution curves of $\theta_1^i(t,\omega), i=1,2,3$.

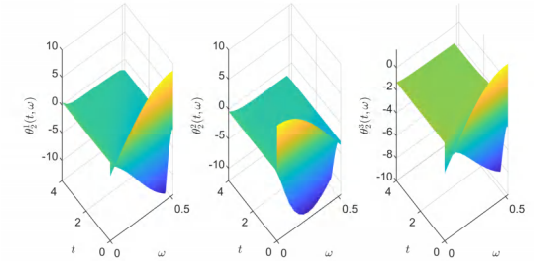


Fig. 3. Evolution curves of $\theta_2^i(t,\omega), i=1,2,3$.

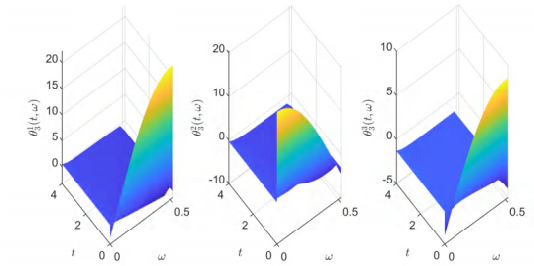


Fig. 4. Evolution curves of $\theta_3^i(t,\omega), i=1,2,3$.

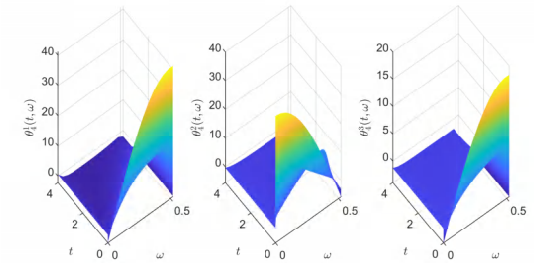


Fig. 5. Evolution curves of $\theta_4^i(t,\omega), i=1,2,3$.

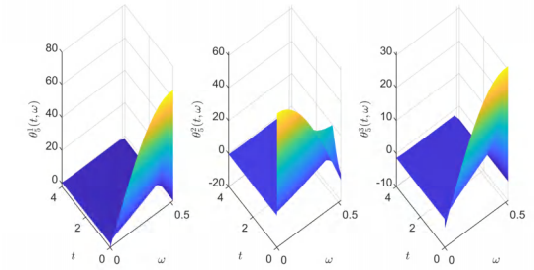


Fig. 6. Evolution curves of $\theta_5^i(t,\omega), i=1,2,3$.

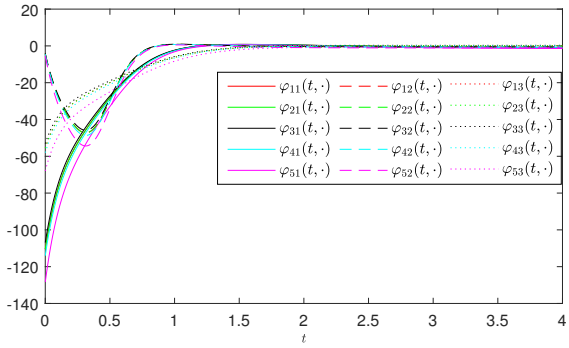


Fig. 7. Control inputs $\varphi_p^1(t,\cdot), \varphi_p^2(t,\cdot)$ and $\varphi_p^3(t,\cdot), p=1,2,\ldots,5$.

$$Z=\begin{pmatrix} -2 & 1 & 0 & 0.5 & 0.5 \\ 1 & -4.2 & 1.2 & 1.5 & 0.5 \\ 0 & 1.2 & -2.2 & 0 & 1 \\ 0.5 & 1.5 & 0 & -2 & 0 \\ 0.5 & 0.5 & 1 & 0 & -2 \end{pmatrix},$$

$$\begin{aligned} y_1(\mu_1) &= (0.42\tanh(\mu_1^1), 0.33\tanh(\mu_1^2), 0.25\tanh(\mu_1^3))^T, \\ y_2(\mu_2) &= (0.15\tanh(\mu_2^1), 0.16\tanh(\mu_2^2), 0.17\tanh(\mu_2^3))^T, \\ y_3(\mu_3) &= (0.24\tanh(\mu_3^1), 0.25\tanh(\mu_3^2), 0.26\tanh(\mu_3^3))^T, \\ y_4(\mu_4) &= (0.34\tanh(\mu_4^1), 0.36\tanh(\mu_4^2), 0.35\tanh(\mu_4^3))^T, \\ y_5(\mu_5) &= (0.05\tanh(\mu_5^1), 0.06\tanh(\mu_5^2), 0.07\tanh(\mu_5^3))^T. \end{aligned}$$

The elements of the functions $y_1(\cdot), y_2(\cdot), y_3(\cdot), y_4(\cdot), y_5(\cdot)$ are confirmed to be Lipschitz continuous. Subsequently, the feedback gain matrices satisfying (6) can be computed using the MATLAB toolbox YALMIP as follows:

$$B=\begin{pmatrix} 1.5615 & 0 & 0 \\ 0 & 1.6565 & 0 \\ 0 & 0 & 1.5950 \end{pmatrix},$$

$$D=\begin{pmatrix} 0.1000 & 0 & 0 \\ 0 & 0.0945 & 0 \\ 0 & 0 & 0.1358 \end{pmatrix}.$$

In virtue of Theorem 3.1, the solution $\mu_p(t,\omega)$ of the re-entrant manufacturing system (3) can converge to the market demand $\mu_e(t,\omega)$ using the state feedback controller (5). The simulation results are shown in Figs. 2-7, where Figs. 2-6 display the evolution curves of $\theta_p^i(t,\varphi), p=1,2,\ldots,5, i=1,2,3$ for the system using the state feedback controller (5); Fig. 7 shows the evolving processes of the control inputs $\varphi_p(t,\cdot), p=1,2,\ldots,5$.

V. Conclusion

Regulation of manufacturing processes has become increasingly vital in contemporary industry. This study delves into the modeling and coordinated regulation of a category of interconnected heterogeneous re-entrant manufacturing systems (ReMSs). The framework of the networked manufacturing system encompasses solitary production lines, manufacturing networks, and networked workshops. Considering the principle of mass conservation, linear hyperbolic partial differential

equations are initially introduced to characterize the solitary production lines. Subsequently, the workshop dynamics, intertwined with various production lines, are formulated using semilinear hyperbolic equations. A bespoke cooperative controller is developed to facilitate inter-workshop communication and fulfill the objective of market demand tracking. Computational simulations corroborate the efficacy of the proposed regulatory framework.

References

[1] J. Han, M. Cai, Y. Lin, W. Liu, X. Luo, H. Zhang, and M. Zhong, "3D re-entrant nanograss on microcones for durable superamphiphobic surfaces via laser-chemical hybrid method," *Applied Surface Science*, vol. 456, pp. 726–736. 2018.

[2] M. Ibrahim and S. Reveliotis, "Throughput maximization of capacitated re-entrant lines through fluid relaxation," *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 2, pp. 792–810, Apr. 2019.

[3] S. Arima, A. Kobayashi, Y.-F. Wang, K. Sakurai, and Y. Monma, "Optimization of re-entrant hybrid flows with multiple queue time constraints in batch processes of semiconductor manufacturing," *IEEE Transactions on Semiconductor Manufacturing*, vol. 28, no. 4, pp. 528–544, Nov. 2015.

[4] F. Zhang, J. Song, Y. Dai, and J. Xu, "Semiconductor wafer fabrication production planning using multi-fidelity simulation optimisation," *International Journal of Production Research*, vol. 58, no. 21, pp. 6585–6600, Jan. 2020.

[5] R. G. Askin and G. J. Hanumantha, "Queueing network models for analysis of nonstationary manufacturing systems," *International Journal of Production Research*, vol. 56, nos. 1-2, pp. 22–42, Nov. 2017.

[6] S. Kumar and P. R. Kumar, "Queueing network models in the design and analysis of semiconductor wafer fabs," *IEEE Transactions on Robotics and Automation*, vol. 17, no. 5, pp. 548–561, Oct. 2001.

[7] J. M. Harrison and L. M. Wein, "Scheduling networks of queues: Heavy traffic analysis of a two-station closed network," *Operations Research*, 1990, 38(6): 1052–1064.

[8] C. Lin, M. Xu, D. C. Marinescu, F. Ren, and Z. Shan, "A sufficient condition for instability of buffer priority policies in re-entrant lines," *IEEE Transactions on Automatic Control*, vol. 48, no. 7, pp. 1235–1238, Jul. 2003.

[9] N. G. Odrey, J. D. Green, and A. Appello, "A generalized Petri net modeling approach for the control of re-entrant flow semiconductor wafer fabrication," *Robotics and Computer-Integrated Manufacturing*, 2001, 17: 5–11.

[10] D. Armbruster, D. E. Marthaler, C. Ringhofer, K. Kempf, and T. Jo, "A continuum model for a re-entrant factory," *Operations Research*, vol. 54, pp. 933–950, 2006.

[11] C. D'Apice and R. Manzo, "A fluid dynamic model for supply chains," *Networks and Heterogeneous Media*, vol. 1, no. 3, pp. 379–398, 2006.

[12] M. Dong and F. He "A new continuous model for multiple re-entrant manufacturing systems," *European Journal of Operational Research*, vol. 223, no. 3, pp. 659–668, 2012.

[13] M. Diagne and I. Karafyllis, "Event-triggered boundary control of a continuum model of highly re-entrant manufacturing systems," *Automatica*, vol. 134, 2021, Art. no. 109902.

[14] J. Chu, P. Shang, and Z. Wang, "Controllability and stabilization of a conservation law modeling a highly re-entrant manufacturing system," *Nonlinear Analysis*, vol. 189, 2019, Art. no. 111577.

[15] J. Deutscher, "Robust cooperative output regulation for a network of parabolic PDE systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 1, pp. 451–459, Jan. 2022.

[16] M. A. Demetriou, "Adaptation and optimization of synchronization gains in the regulation control of networked distributed parameter systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 8, pp. 2219–2224, Aug. 2015.

[17] A. Das and F. L. Lewis, "Distributed adaptive control for synchronization of unknown nonlinear networked systems," *Automatica*, vol. 46, no. 12, pp. 2014–2021, 2010.

[18] Y. Wan, G. Wen, X. Yu, and T. Huang, "Distributed consensus tracking of networked agent systems under denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 10, pp. 6183–6196, Oct. 2021.

[19] E. Panteley and A. Loría, "Synchronization and dynamic consensus of heterogeneous networked systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3758–3773, Aug. 2017.

[20] S. Phillips and R. G. Sanfelice, "Robust distributed synchronization of networked linear systems with intermittent information," *Automatica*, vol. 105, pp. 323–333, 2019.

[21] H. Yu and P. J. Antsaklis, "Output synchronization of networked passive systems with event-driven communication," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 750–756, Mar. 2014.

[22] C. Zhang, Q. Gao, M. V. Basin, J. Lü, and H. Liu, "Robust control of multi-line re-entrant manufacturing plants via stochastic continuum models," *IEEE Transactions on Automation Science and Engineering*, early access, Aug. 23, 2023, doi: 10.1109/TASE.2023.3305308.

[23] K. Zhang, M. V. Basin, Q. Gao, Y. Deng, and X. Song, "Robust stability and fuzzy controller synthesis for a class of hybrid re-entrant manufacturing systems," *Discrete and Continuous Dynamical Systems-S*, vol. 16, pp. 1909–1928, 2023.

Chenguang Liu received the B.E. degree in computer science and technology from the Pingdingshan University, Pingdingshan, China, in 2019. He received the M.E. degree in Computer Science and Technology with the School of Computer Science and Technology, Tiangong University, Tianjin, China. He is currently the pursuing the Ph.D. degree in electronic information with the Institute of Artificial Intelligence, Beihang University, Beijing, China.

His current research interests include partial differential systems, fractional-order systems, and intelligent manufacturing.

Qing Gao received the B.Eng. and Ph.D. degrees in mechanical and electrical engineering from the University of Science and Technology of China, Hefei, China, in 2008 and 2013, respectively, and the Ph.D. degree in mechatronics engineering from the City University of Hong Kong, Hong Kong, in 2014.

From 2014 to 2016, he was a Post-Doctoral Research Associate with the School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy, Canberra, ACT, Australia. Since 2018, he has been a Full Professor with the School of Automation Science and Electrical Engineering, Beihang University. His current research interests include intelligent control and quantum control.

Dr. Gao was a recipient of the Outstanding Research Thesis Award from the City University of Hong Kong, in 2013, and the Outstanding Doctoral Dissertation Award from the Chinese Academy of Sciences in 2015, the Alexander von Humboldt Fellowship of Germany, and the 21st Guan Zhao-Zhi Award.

Jinhu Lü (M'03–SM'06–F'13) received the Ph.D. degree in applied mathematics from the Academy of Mathematics and Systems Science (AMSS), Chinese Academy of Sciences, Beijing, China, in 2002.

Currently, he is the Dean with the School of Automation Science and Electrical Engineering, Beihang University, Beijing, China. He is also an Adjunct Professor with the AMSS, Chinese Academy of Sciences. He was a Professor with RMIT University, Melbourne, VIC, Australia, and a Visiting Fellow with Princeton University, Princeton, NJ, USA. He is a Chief Scientist of National Key Research and Development Program of China and a Leading Scientist of Innovative Research Groups of National Natural Science Foundation of China. His current research interests include cooperation control, industrial Internet, complex networks, and Big Data. He is the author of four research monographs and more than 200 international journal papers (>110 IEEE Trans. Papers), with more than 21000 citations and h-index 70 from Web of Science. He also has 82 authorized patents.

Dr. Lü was a recipient of the prestigious Ho Leung Ho Lee Foundation Award in 2015, the National Innovation Competition Award in 2020, the State Natural Science Award three times from the Chinese Government in 2008, 2012, and 2016, respectively, the Australian Research Council Future Fellowships Award in 2009, the National Natural Science Fund for Distinguished Young Scholars Award, and the Highly Cited Researcher Award. He is/was an Editor in various ranks for 16 SCI journals, including the Co-Editor-in-Chief of IEEE TII. He served as a member in the Fellows Evaluating Committee of the IEEE CASS, the IEEE CIS, and the IEEE IES. He was the General Co-Chair of IECON 2017, and Program Co-Chair of the 9th Asian Control Conference. He is the Fellow of IEEE/CAA/ORSC/CICC.

基于多源特征融合的飞机翼身交点孔精密镗削刀具磨损状态监测

杨展鹏[1]，华丰[2]，付白斗[1]，胡笑楠[1]，程骋[1]，袁烨[1]

（1. 华中科技大学 人工智能与自动化学院，湖北武汉 430074；2. 华中科技大学 机械科学与工程学院，湖北武汉 430074）

摘　要：装配是航空装备制造的最后一个环节，直接决定最终交付质量。在飞机的装配过程中，翼身交点孔作为连接机身与机翼的关键交点孔，影响着最终飞机产品的机翼平衡能力、飞机机动性能、外形准确性等，对加工精度的要求达到了 0.001mm 量级。目前通用的加工方法普遍采样少量多次的保守试切策略，加工占比时间长，是飞机装配过程中极为重要的一环。基于此，本文提出了一种属于数据驱动型的整机超大尺寸交点孔精密镗削刀具磨损状态监测方案，基于仿翼身交孔的实机精密卧式镗削加工实验收集到的时序与图像数据，实现了对刀具前后刀面磨损状态的准确预测。实验结果表明，该方法在均方根误差、平均绝对误差与R^2上的表现均优于经典机器学习与深度学习模型，同时该方法也在公开数据集上表现出良好的泛化性能。

关键词：翼身交点孔；刀具磨损状态预测；深度学习

Precision Wear Monitoring of Large-Sized Hole-Making Tools for Complete Machines Based on Multi-Source Feature Fusion

YANG Zhanpeng, HUA feng, FU Baidou, HU xiaonan, CHENG cheng,YUAN Ye

Abstract: Assembly is the last part of aviation equipment manufacturing, which directly determines the final quality. In the assembly process of aircraft, the wing-body intersection hole, as a critical juncture connecting the fuselage and wings, affects the wing balance, aircraft maneuverability, and shape accuracy of the final aircraft product， which calls for a roughly 0.001mm precision for the machining process. At present, the general processing method generally adopts a small number of multiple conservative trial cutting strategy, which takes a long time and therefore plays a very important part role in the aircraft assembly process. Based on this, this paper presents a data-driven monitoring scheme for the tool wear status during the precision rough machining of ultra-large size intersection holes, using time-series and image data collected from real precision horizontal boring experiments simulating wing-body intersection holes. This method has demonstrated superior performance in terms of root mean square error and mean absolute error compared to traditional machine learning and deep learning models and has also shown good generalization performance on public datasets.

Key words: wing-body intersection hole; tool wear state prediction; deep learning;

1　引言

制造业是国民经济的支柱，是国家综合国力的重要体现，而航空工业作为制造业的前沿，更是对国家经济建设和国防安全起着领头与导向作用，具有极其重要的战略地位，综合反应着国家制造业的实力和科技现代化的水平。作为航空工业的主要产品之一，飞机制造水平以其质量要求高、技术难度大等特点，成为衡量航空工业水准的重要指标。飞机的制作过程大致可分为毛胚制造、零件加工、部件装配和试验四个阶段。作为直接决定飞机产品最终质量与使用性能的关键环节，部件装配因其协调关系复杂、涉及零件与连接件数量众多、工作量巨大等特点，成为了飞机生产过程中效率及质量的核心瓶颈。因此，飞机装配技术的提高，对于全面提升飞机制造的质量与效率具有举足轻重的意义。

翼身交点孔位于飞机机身主体两侧，用于连接飞机机身与机翼，是飞行器装配连接的关键高附加值部位，其加工质量的好坏，直接影响着飞机产品外形的准确度、机翼的平衡性以及飞机的机动能力。翼身交点孔的加工一般要求采用精密镗削、加工环境为部件弱刚性夹持状态且无切削液，这对生产单位的加工设备能力与工艺能力提出了极高的要求[1]，若相关工艺参数（如主轴转速、进给、加工前孔径、进刀量等）设置过大，会导致表面质量不达标、刀具磨损甚至机床主轴损坏等问题，造成巨大的经济以及时间损失。因而，对于交点孔精密镗削刀具磨损状态的监测至关重要。

在目前的实际工业加工场景中，刀具磨损状态检测问题的解决方案通常分为两个大类，即物理模型方法和数据驱动方法[2]。在物理建模方面，Atabey 等人[3]通过对钻孔过程的基本原理与工艺参数入手，通过考量切削面、刀具形状以及切屑等因素，确定了镗削加工中造成刀具磨损的一些物理量；Li 等人[4]通过考量切削机理以及切削力对切削边缘的贡献，提出了一种解析性的螺旋铣削动态切削力模型，准确描述了螺旋铣削过程中刀具的退化过程。而一般来说，随着刀具的磨损，包括机床产生的振动、切削时发出的声音、切屑的形状、机床的功率等在内的许多因素都会发生变化[5]，这往往导致基于物理模型的方法泛用性不高，针对具体场景难以优化；同时，过高的代价惩罚，经验判断往往采取过保护策略，增加企业的生产成本，这种问题在航空航天领域格外突出，严重影响企业的生产效率和经济效益[6]。

随着传感器技术的发展、机器学习、信号处理技术的进步，数据驱动分析方法越来越多的被应用于监测刀具磨损状态[7]。Rao 等人[8]利用人工神经网络(artificial neural network, ANN)对刀具磨损进行评估，并将其用于刀具磨损状态预测和刀具寿命预测。Benkedjouh 等人[9]利用 SVR 对多传感器信号提取的健康指标进行建模，用于刀具寿命预测。近年来，随着工业智能化与工业大数据的不断推进发展，基于深度学习的方法也得到了人们的重视[10]。文献

[11][12][13][14][15][16][17]提出了基于卷积神经网络(Convolutional Neural Network，CNN)的不同框架，汪海晋等人[18]通过搭建一维卷积神经网络，实现了对铣刀磨损状态的监测。除此之外，长短期记忆网络(Long Short-Term Memory，LSTM)作为时序数据预测方面性能极好的模型，也得到了相关的研究与实地应用。例如，Xia 等人[19]引入了另一种混合模型，其中构建了被称为卷积双向长短期记忆网络(Convolutional Bidirectional Long Short-Term Memory Network，CBLSTM) 的深度神经网络来解决工具磨损预测任务。出于 Transformer 在自然语言处理领域以及长序列数据处理方面的优异表现，注意力机制也得到了越来越多研究者的重视，开始被应用于关键部件的剩余寿命的预测当中[20]。除此之外，为快速构建新工艺条件下的刀具磨损状态预测模型，迁移学习也有所研究。例如，蔡伟立等人[21]通过对抗域适应训练的方法，利用新工艺条件下的少量目标域样本，成功实现了对源域预训练得到的预测模型的调整，并通过具体的加工实验验证了方法的有效性。

由此可见，在翼身交点孔精密镗削、刀具磨损状态监测领域，通过使用数字化、智能化的方法进行相应工艺的改进，已被证明具有广阔的发展前景和优秀的应用效果。但在涉及到翼身交点孔精密镗削刀具磨损状态监测时，仍缺少成熟的数字化、智能化解决方案，难以应对本文所面对的加工场景。

本文以面向未来工业互联网的航空柔性装配机理建模与智能调控为应用场景，针对翼身交点孔加工中精密镗削这一流程，以提高加工效率与加工质量为目标，通过融合多传感器数据，借助深度学习方法，提出了一种结合语义分割模型模型与带注意力的基于 MCNN-BiGRU 网络的解决方案。对于时序数据，它通过多分支的 CNN 网络提取输入不同尺度的特征，再将自注意力机制应用于特征提取层与特征融合之后的输出，实现对不同通道间时空关系的学习，最后利用 BiGRU 网络实现对于磨损值的预测；对于图像数据，它借助 SAM 网络模型进行语义分割，计算已磨损的区域面积作为是否磨损的判据。该方案为实际翼身交点孔精密镗削生产活动中刀具磨损以及刀具更换提供支持策略。

本文的组织如下：第二章描述了本文模型的背景，第三章对刀具磨损状态监测问题进行了具体的定义并描述了针对航空航天工业翼身交点孔精密镗削加工刀具磨损状态在线监测的方法，第四章介绍了所用数据来源、模型的评价指标、与现有方法的比较结果以及模型在公开数据集上的泛化能力表现，第五章对文章进行了总结。

2 原理介绍

2.1 卷积神经网络

卷积神经网络是深度学习的代表算法之一，其具有局部感知与权值共享的特点，被广泛

的运用于特征的学习与提取。卷积神经网络一般由多个卷积层与池化层堆叠而成。如图 1 所示，在卷积层中，卷积核会以滑窗的方式与输入进行卷积操作，以此获得局部感受视野，提取数据特征信息。

二维卷积操作的公式为：

$$f_j^{(l)} = f\left(\sum_{i\in M_j} \omega_{i,j}^{(l)} \cdot f_i^{(l-1)} + b_j^{(l)}\right) \tag{1}$$

其中，l 表示第 l 层卷积网络，$f_i^{(l-1)}$表示将第$l-1$ 层卷积网络的输出结果作为第 l 层网络的输出，i 表示该特征向量的第 i 个分量，M_j表示该特征向量共有M_j个特征分量，j 表示输出特征向量的第j 个分量。

池化层（Pooling Layer）常用于卷积层后，能够有效降低特征维度、减少参数数量，以提高模型的鲁棒性，防止模型过拟合。池化函数一般分为平均池化、最大池化两种，在处理时间序列数据时，由于相邻时间序列采样数据少有突变，故采用平均池化方法，平均池化的公式如下：

$$p_{t,i}^{(l)} = pool\left\{f_{t,i}^{(l)}, p\right\}, p \in S_p \tag{2}$$

其中，p为池化窗口的大小，$p_{t,i}^{(l)}$表示第 l 层时间步长 t 的特征向量的第 i 个分量，$pool(\cdot)$为子采样函数，在这里为均值函数，S_p为输入数据的大小。

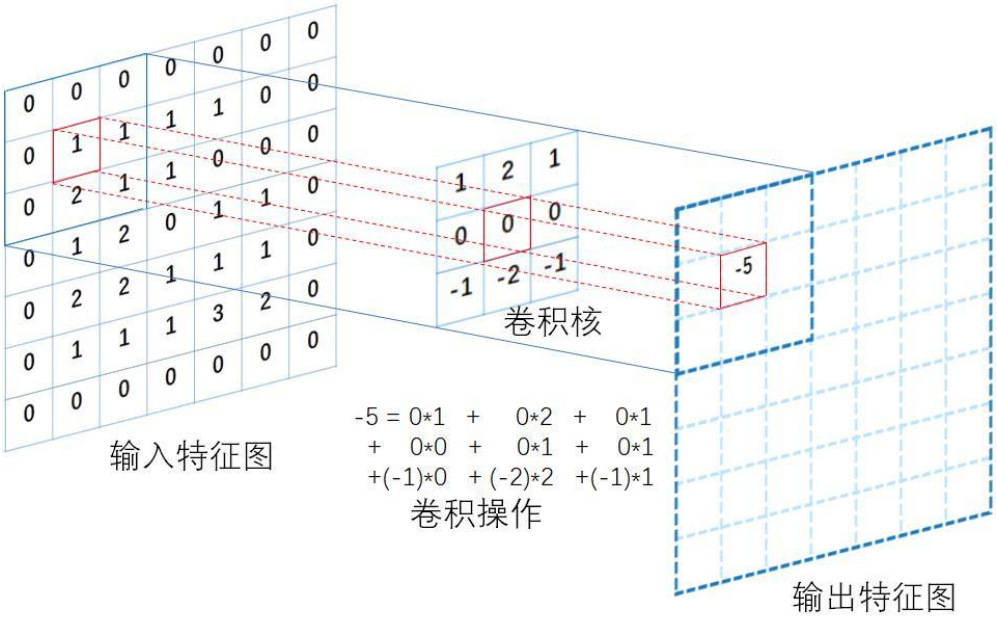


图 1 二维卷积计算过程示意图

2.2 自注意力机制

并非所有的特征都为刀具磨损预测带来了相同的贡献，为了给预测模型提供有效的特征，因此本文使用 Vaswani A 等人[22]等提出的自注意力机制对特征进行加权。图 2 为自注意力机

制的简单图解，$\{a^1, a^2, \dots, a^n\}$为向量化的输入向量，q、k、v 分别为查询（Query）、键（Key）、值（Value）向量。Query 即自主提示，是主观意识的特征向量；Key 即非自主提示，指物体的突出特征信息向量；Value 则是代表物体本身的特征向量。注意力机制是就通过 Query 与 Key 的注意力汇聚，实现对 Value 的注意力权重分配，生成最终的输出结果。特征注意力权重可以用公式描述为：

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{3}$$

其中，Q、K、V 即上述各输入向量的 q、k、v 的矩阵表示，d_k为缩放因子。

在此基础上，还需要对各个输入向量进行位置编码，使得网络可以学习到输入之间的位置关系。本文使用 transformer 原文中经典的 sin、cos 编码方式，其公式如下：

$$PE_{pos,2i} = sin\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \tag{4}$$

$$PE_{pos,2i+1} = cos\left(\frac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \tag{5}$$

其中，PE 表示位置编码，pos 表示待求的输入向量（即 token）在整个输入向量中的位置，位置编码即为一个向量（embedding），i 表示向量中每个元素的索引，d_{model}表示位置编码的向量维度。

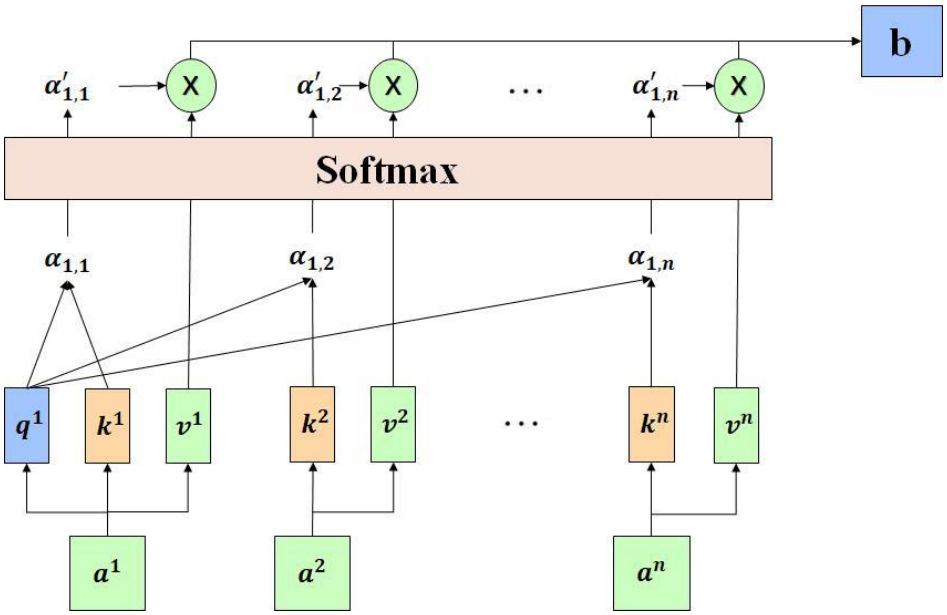


图 2 自注意力机制图解

2.3 门控循环单元（Gate Recurrent Unit, GRU）

GRU 已被证明可用于学习序列建模中的长期依赖关系，它与长短期记忆神经网络（Long short-term Memory， LSTM）解决了循环神经网络梯度消失、梯度爆炸的问题。与 LSTM 相比，GRU 在结构上更为简单，其只具有重置门与更新门两个门控逻辑单元，因此也更加容易训练。一个典型的 GRU 网络如下图所示：

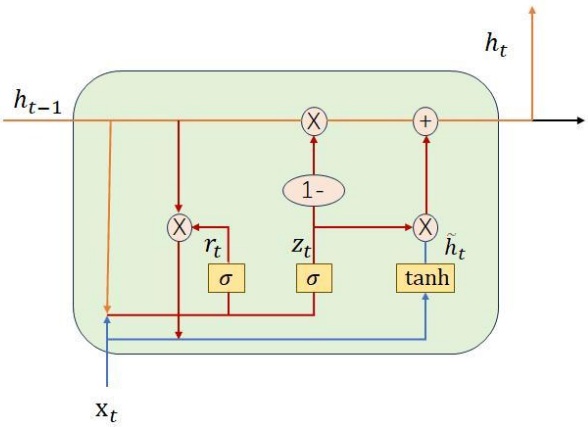


图 3 GRU 门控单元结构示意图 GRU 门控单元结构示意图

其中，x_t为当前 t 时刻输出，h_t为 t 时刻网络输出，$\tilde{h}_t$表示当前网络的候选隐藏状态，r_t为重置门，z_t为更新门，σ为 sigmoid 激活函数。重置门通过结合当前输入与前一时刻 GRU 的输出，来决定上一时刻信息有多少得到保留，其公式如下：

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t]) \tag{6}$$

其中，W_r为权重矩阵，r_t将会用于候选隐藏状态$\tilde{h}_t$ 计算的过程中，公式如下：

$$\tilde{h}_t = tanh\,(W \cdot [r_t * h_{t-1}, x_t]) \tag{7}$$

其中，W 为权重矩阵。

更新门用于决定有多少信息传递给下一时刻，整个过程由更新门、更新记忆两个模块组成，更新门的公式如下：

$$z_t = \sigma(W_z \cdot [x_t, h_{t-1}]) \tag{8}$$

更新记忆公式如下：

$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t \tag{9}$$

其中，W_z为权重矩阵。

由此可见，GRU 网络通过对上一时刻状态信息h_{t-1} 和当前时刻 t 的输入信息x_t 的选择性保留与利用，在实际应用中能够有效获取数据中的刀具状态退化信息。

2.4 Segment Anything 网络模型

分段任何模型（Segment Anything，SAM）是由 Meta AI 的 FAIR 实验室于 2023 年提出的一个图像分割大模型[23]，其可以在使用提示工程的前提下适应各种下游分割问题，并且在各种分割任务中实现最先进的性能。

SAM 模型的架构如下图所示，其包含三个组件，即图像编码器（image encoder）、提示编码器（prompt encoder）、结合了提示和图像编码器的嵌入的轻量级掩码解码器（lightweight mask decoder），三个组件协同工作以获取有效的掩码。其中，图像编码器是基于视觉注意力

（Vision Transformer，Vit）预训练的视觉变换器，用于将图像编码为图嵌入向量；提示编码器将背景点、遮罩、边界框或文本实时编码到嵌入向量中，用于生成提示（即位置、文本等）的嵌入向量，并与图像嵌入向量一起送入掩码解码器中；轻量级掩码解码器根据来自图像和提示编码器的嵌入预测分割掩码，其将图像嵌入、提示嵌入和输出标记映射到掩码并将其输出。

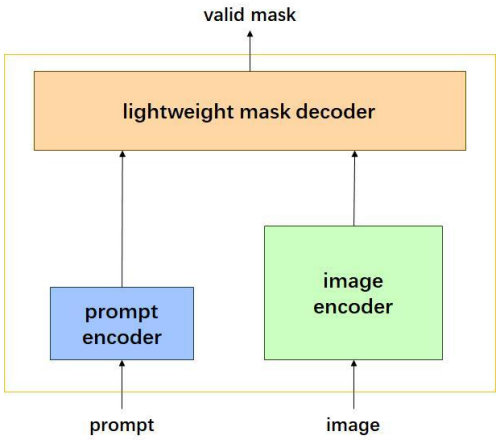


图 4 SAM 模型架构

基于上述 SAM 模型具备的优秀性能，本文提出的方法使用其作为图像数据处理的通道，用来分出刀具磨损区域并计算其面积，预测前刀面刀具磨损的状态。

3 基于多源特征融合的精密镗削刀具磨损状态监测方法

3.1 问题描述

在精密镗削的加工过程中，刀具的磨损失效具有多种失效形式。经实验验证，在当前工况下的主要磨损形式为：前刀面磨损、后刀面磨损以及崩刃。而出于实际使用情况，本文主要针对前、后刀面磨损两种失效形式进行监测。

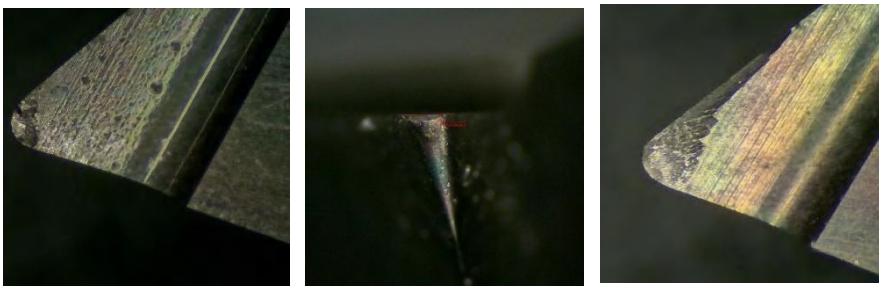


图 5 前刀面磨损（左）、后刀面磨损（中）、崩刃（右）

从输入输出的角度来讲，前刀面磨损的监测属于分类问题，即通过选择合适的网络模型，判断输入前刀面图像数据的类别是否属于已磨损类；而后刀面磨损的监测属于多通道的时序预测问题，后刀面磨损值是指加工前后后刀面与工件接触部分的直径的差距，其公式为

$$Y_{\Delta}^{i} = Y_{T}^{i} - Y_{0}^{i} \tag{10}$$

其中，i 表示第 i 个样本，Y_0、Y_T分别表示加工前后后刀面与工件接触部分的直径，Y_Δ则表示其变化大小，上述物理量单位均为微米。

时序数据集包括$X_{dataset} = \{X_{train}, X_{test}\}$，其中，$X_{dataset}$为刀具加工过程中所采集到的时序数据，将其按照 7：3 的比例划分为训练集X_{train}和测试集X_{test}。该问题可以被描述为通过分析训练集数据，以建立时序数据与后刀面磨损值的非线性映射$f_\omega(\cdot)$，可用公式表述如下：

$$\widehat{Y}_\Delta = f_\omega(X_{train}) \tag{11}$$

具体而言，$X_{\text{train}} \epsilon \mathbb{R}^{l \times c}$，$l$ 为每段训练数据的时间长度，c 为每段时序数据的通道数，每个通道的数据由不同的传感器获取。由于每条时序数据的长度不同，还需要通过滑窗提取特征以获取等长的输入序列。经滑窗处理后的数据可表示为：

$$X_i = \begin{bmatrix} x_1^1 & x_2^1 & x_3^1 & \cdots & x_T^1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^c & x_2^c & x_2^c & \cdots & x_T^c \end{bmatrix}, i = 1,2,\cdots,N \tag{12}$$

其中，T 为处理后的时序数据长度，c 为通道数量，N 为样本数量，i 表示第 i 个样本。

在训练阶段，模型需要最小化损失函数以提高模型的预测精度，这可以用公式描述如下：

$$\omega^* = \underset{\omega}{argmin}[\frac{1}{N}\sum_{i=1}^{N}(Y_\Delta^i - \widehat{Y}_\Delta)^2] \tag{13}$$

其中，ω即为模型待优化的参数。

3.2 模型框架

按照数据的格式，本文提出的刀具磨损状态监测方法主要分为两个部分：前刀面磨损监测模型、后刀面磨损监测模型，分别对应图像数据支路和时序数据支路。框架可视化如下：

后刀面磨损监测模型基于带注意力的 MCNN-BiGRU 模型进行预测，如图所示，其主要分为三个部分：输入层、平行特征提取层与预测回归层。

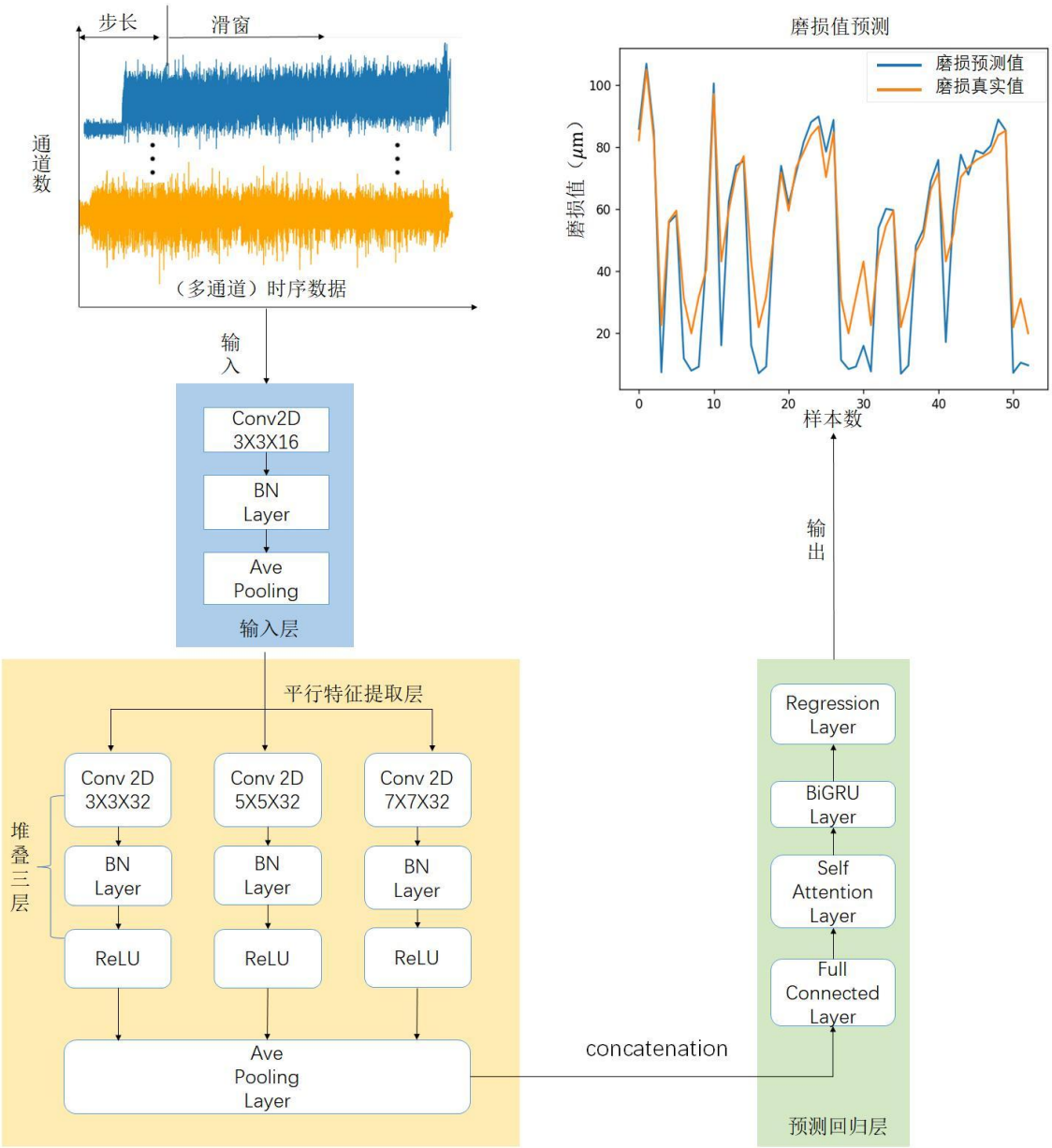


图 6 基于带注意力的 MCNN-BiGRU 网络刀具后刀面磨损状态预测模型

原始数据信号首先送入由卷积层、批归一化层和池化层组成的输入层中进行初步的特征提取，之后送入到平行特征提取层，通过设置三个不同大小的卷积核以提取输入数据不同尺度的特征，提取过程如图所示。由于输入数据是一个多通道的长时序列，其表征为一个长矩形，因此在卷积过程中需要进行适当的边缘补充。同时，在每一个并行分支中，在卷积层后设置一个批归一化层(batch normalization layer, BN)以解决网络在训练过程中的过拟合问题，提高网络的泛化能力、加快网络训练速度。BN 层计算涉及的数学表达式为：

$$\begin{cases} \mu_B = \frac{1}{m}\sum_{i=1}^{m} x_i \\ \sigma_B^2 = \frac{1}{m}\sum_{i=1}^{m} (x_i - \mu_B)^2 \\ \hat{x}_i = \frac{x_i - \mu_B}{\sqrt{\sigma_B^2 + \epsilon}} \\ y_i = \gamma \hat{x}_i + \beta \end{cases} \tag{14}$$

其中，x_i、y_i 分别为 BN 层的输入、输出，m 表示批的总数，μ_B、σ_B^2 分别为批数据的均值和方差，γ、β 为网络训练过程中需要学习的参数。之后，将三个并联的 CNN 网络提取出来的特征向量拼接，得到一系列$\{f_1, f_2, f_3, ..., f_m\}$作为融合后的特征向量，送入由堆叠双向 GRU 网络、自注意力机层和全连接层组成的预测回归层中进行时序方面的特征提取与磨损量预测。

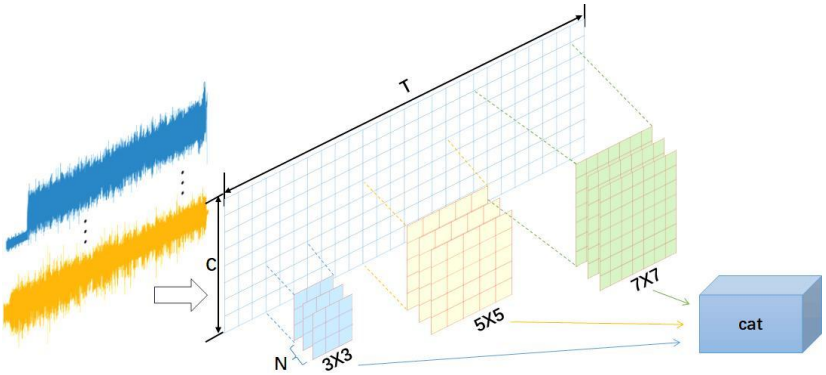


图 7 特征提取过程

由于时序数据具有多个通道，在经过特征提取层与特征融合之后，其训练的特征向量仍具有很大的尺度；并且，为了使得网络进一步学习不同通道间的时空关系，考虑在平行特征提取层和 BiGRU 层之间加入自注意力层，以增强网络的学习能力。

后刀面磨损是一个渐进的过程，在当前时刻 t，其磨损状态与刀具之前的状态、t 时刻后的操作有着密切的关系，因此，选用 BiGRU 网络进行时间层面的预测，如图所示。输入$\{f_1, f_2, f_3, ..., f_t, ..., f_m\}$为前文提到的融合后的特征向量，每个 GRU 的隐藏层数设置为 64，在 BiGRU 网络后，连接一个回归层以进行磨损值的预测。

回归层由三层全连接层组成，神经元个数分别为 512、256、1。全连接层对输入特征向量进行加权计算，最后得到后刀面磨损值的预测值。

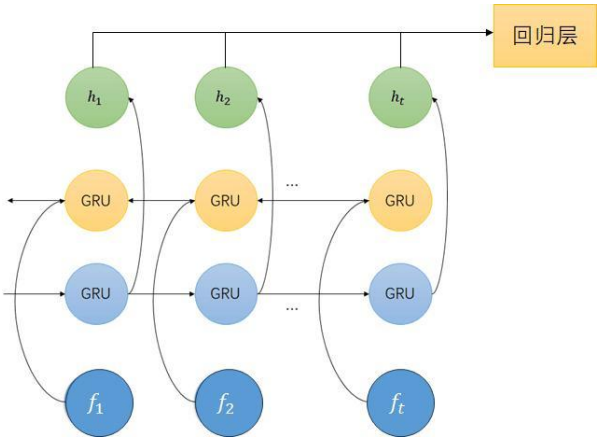


图 8 双向 GRU 网络结构示意图

前刀面磨损的监测借助 SAM 模型完成。从输入输出的角度来看，该通道输入采集到的图像数据，送到训练好的 SAM 网络模型中进行语义分割，计算已磨损的区域面积，以此来作为

刀具是否磨损的判据。输入、输出的样图如图所示。

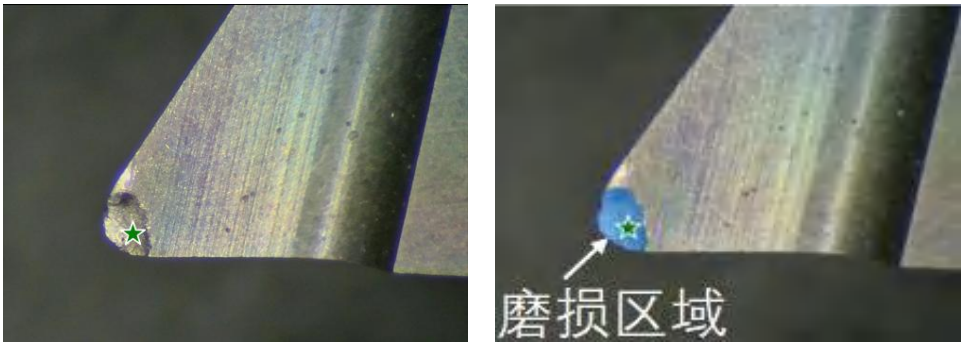


图 9 图像通道输入输出样图

4 实验

4.1 数据集介绍

本文采用的数据集由仿翼整机超大尺寸交点孔加工精密镗削平台模拟加工并采集前后刀面刀具磨损状况数据构建。使用 Kisler 平台采集得到后刀面的.mf4 格式时序数据，采样频率为 100kHz，包含三个方向的切削力、三个方向的振动量以及三相电流的值，共计 9 个通道。部分加工刀数的各个通道的时序数据可视化如下：

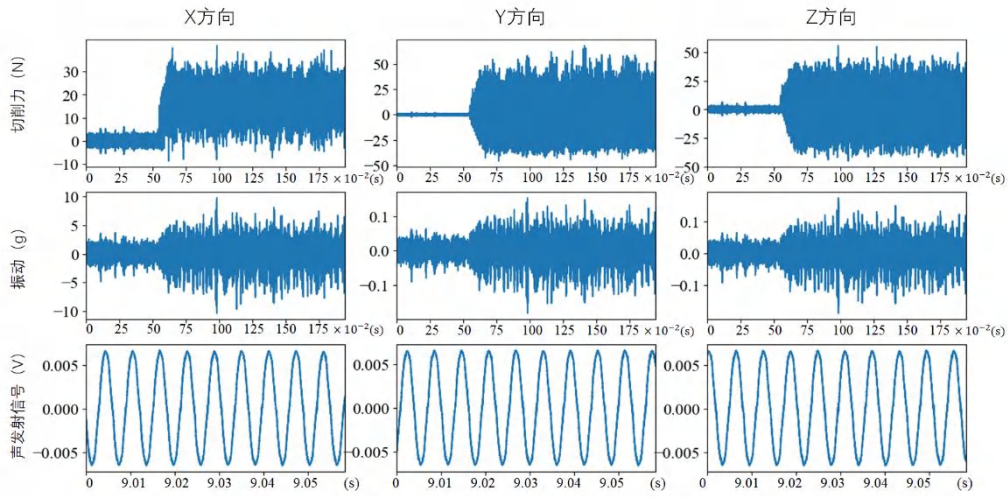


图 10 时序数据可视化

由于采样频率过高，为兼顾表示的美观与准确，图示中，X、Y、Z 方向切削力与振动信号截取的为 0-2 秒，X、Y、Z 方向电流截取的是 9.00-9.06 秒。

此外，时序数据的标签则通过工业显微镜获取。在每刀加工前后测量刀具直径，并计算刀具磨损值作为训练用标签，并根据具体场景定义：当前刀面磨损面积比达 0.037，或后刀面磨损值达阈值 0.075mm，即判定为刀具失效。部分标签数据如下表所示。

表 1 部分数据标签

5-1	7	600	20	24.5
5-1	8	600	24	44.9
5-1	9	600	16	54.5
5-1	10	400	20	21.8

对于前刀面的图像数据，使用海康 MV-CA013-20GC 工业相机进行采集，由于刀具失效的情况中，前刀面磨损与后刀面磨损的发生是各自独立的，因此图像的数量与加工刀数并不对应，共采集 45 张作为方法的验证。部分图像数据如下图所示。

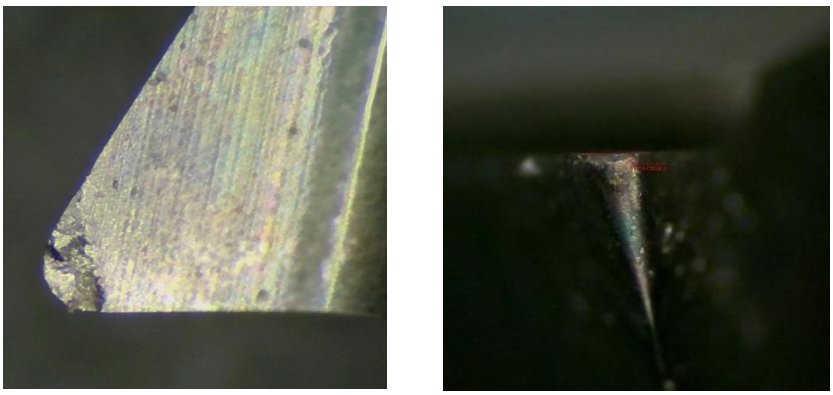


图 11 前刀面磨损图像（左）、后刀面磨损图像（右）数据实例

4.2 数据预处理

对于时序数据而言，由于不同传感器采集到的原始数据具有不同的长度与量纲，这会对刀具磨损的预测带来干扰，因此需要对采集到的原始数据做如下步骤的处理：

第一步，清洗数据集，除去其中无用以及不适合用来训练部分。由于数据是逐刀加工获取的，在每一段数据的开始与结尾，刀具的加工状态并不稳定，故除去开头、结尾各 2.5%的数据量；此外，为最大限度消除噪声影响，对数据进行了均值滤波处理。

第二步，对原始数据进行标准化处理，以消除量纲影响、提高网络的计算性能。数据标准化处理的公式如下：

$$x_i^{'} = \frac{x_i - \mu_i}{\sigma_i} \tag{15}$$

其中，x_i为第 i 个样本数据，μ_i为该行数据的平均值，σ_i为该行数据的标准差。标准化处理后，各通道数据均满足均值为 0，标准差为 1。

第三步，解决单条样本长度不一的问题。对数据进行滑窗处理，使之转变为$X_{train} = \{X_{train}\}_{i=1}^{N}$，其中样本量 N 的大小与当前段时序数据长度和滑窗长度有关。可将其表现为二维矩阵的形式：

$$X_i = \begin{bmatrix} x_1^1 & x_2^1 & x_3^1 & \cdots & x_T^1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^c & x_2^c & x_2^c & \cdots & x_T^c \end{bmatrix}, i = 1,2,\cdots,N \tag{16}$$

其中，T 为滑窗长度，c 为通道数量，N 为样本数量，i 表示第 i 个样本。在实际操作中，以 2000 为时间步长对各个信道进行切片，最后共得到 58 条序列长度相同的时序数据，并按照 7：3 的比例划分训练集、测试集。

4.3 评价指标

本文使用三个表征来评估模型的性能，第一个是均方根误差（Root Mean Square Error，RMSE），它对时间序列中较高的值更为敏感，第二个是平均绝对误差（Mean Absolute Error，MAE），它使用于测量预测值与实际值之间的偏差，第三个是决定系数（R^2），它能够衡量模型的预测能力、评估回归模型的拟合能力。

因此 $RMAE$ 和 MSE 越低，R^2越高，意味着模型性能越好。这三个评价指标的计算公式如下：

$$RMSE = \sqrt{\frac{1}{n}\sum_{t=1}^{n}(\hat{y}_t - y_t)^2} \tag{17}$$

$$\mathrm{MAE} = \frac{1}{n}\sum_{t=1}^{n}|\hat{y}_t - y_t| \tag{18}$$

$$R^2 = 1 - \frac{\sum_{t=1}^{n}(y_t - \hat{y}_t)^2}{\sum_{t=1}^{n}(y_t - \bar{y})^2} \tag{19}$$

上式中，$\hat{y}_t$、y_t、$\bar{y}$ 分别为 t 时刻刀具后刀面的预测磨损值、实际磨损值、实际磨损值的均值, n 为样本总量。

4.4 实验流程设计与模型参数

4.3.1 时序数据支路

为了更好的训练带注意力机制的 CNN-BiGRU 模型，通过一系列的实验确定了表现最优的超参数，具体的，设置 BiGRU 隐藏状态为 64、堆叠层数为 2，自注意力机制 encoder 层输入向量长度为 512，堆叠 4 层，多头注意力设置为 4，并设置 Adam 优化器用以更新网络权重，初始学习率、批大小以及最大训练轮数分别设置为 0.001、16、400。

为了防止网络过拟合，在上述深度学习模型的训练过程中，引入 L2 正则化以提高模型的泛化性能。加入 L2 正则化后的损失函数定义为

$$L(\omega) = \frac{1}{n}\sum_{t=1}^{n}(\hat{y}_t - y_t)^2 + \frac{\lambda}{2}||\omega||_2^2 \tag{20}$$

其中，ω 是待优化的权重参数，n 是时间序列的长度，$\hat{y}_t$、y_t 分别是 t 时刻的磨损预测值和磨损实际值，λ 是正则化因数，在这里选择 0.005，$||\omega||_2^2$ 为权重ω 的 L2 范数。

此外，设置损失函数阈值为 0.001 作为早停参数，进一步防止模型过拟合。

4.3.2　图像数据支路

在前刀面磨损监测过程中，采用 SAM 模型对加工过程中采集到的前刀面模型进行像素级的语义分割，从而识别出前刀面已磨损的区域并计算其面积。该支路的处理流程如下：

首先，搜集加工过程中采集到的前刀面图像并将其导入到 SAM 模型的输入接口中，如图 12 所示；

其次，模型依据输入图像自动计算出所有可分割的区域。在本实验条件下，限定其进行三次语义分割，按照返回掩码从大到小的顺序排列为前景、刀具前刀面整体区域、磨损区域；

最后，计算各 mask 掩码总和，并将磨损区域掩码与刀具前刀面整体区域掩码做商，根据实验结果，定义该比值大于 0.037 为前刀面磨损严重。最终输出结果如图 13 所示

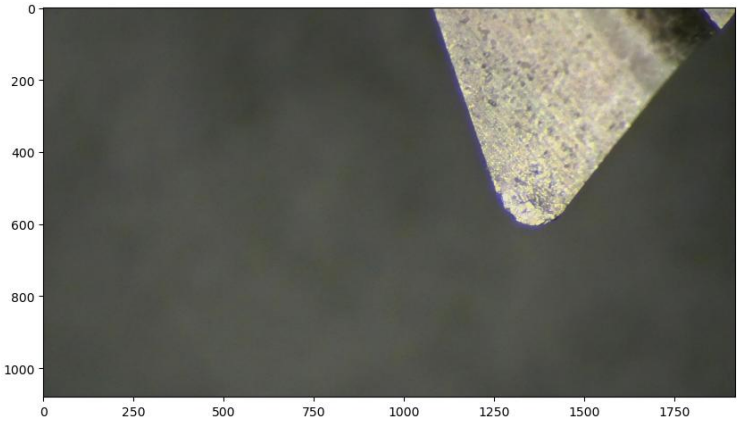


图 12 图像数据支路输入（坐标：像素）

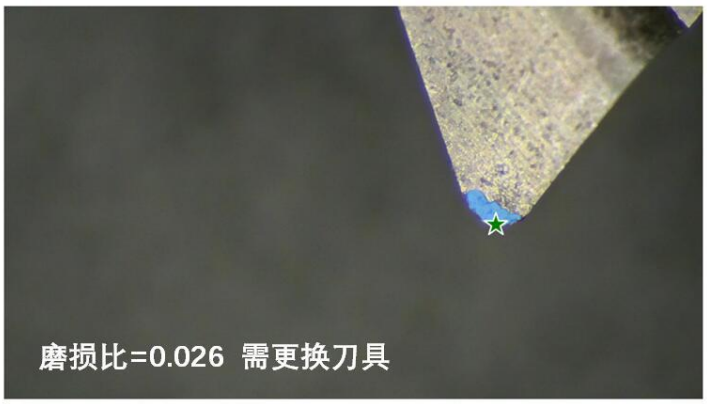


图 13 图像数据支路输出

4.5 模型结果

4.5.1　模型比较

为了更好的评估本文提出的用于时序数据预测的带注意力的 MCNN-BiGRU 模型在搜集到的数据集上的表现，设置了一些传统机器学习与流行深度学习的方法，在同样的数据集上进行训练并与本文提出的方法进行了比较。所用模型分别为线性回归网络（Liner Regression

LR）、支持向量机（Supporting Vector Machine SVR）、由卷积神经网络与堆叠长短期记忆网络组成的混合模型（CNN-LSTM）以及时间卷积网络（Time Convolution Network TCN）。其结果如表 2 所示：

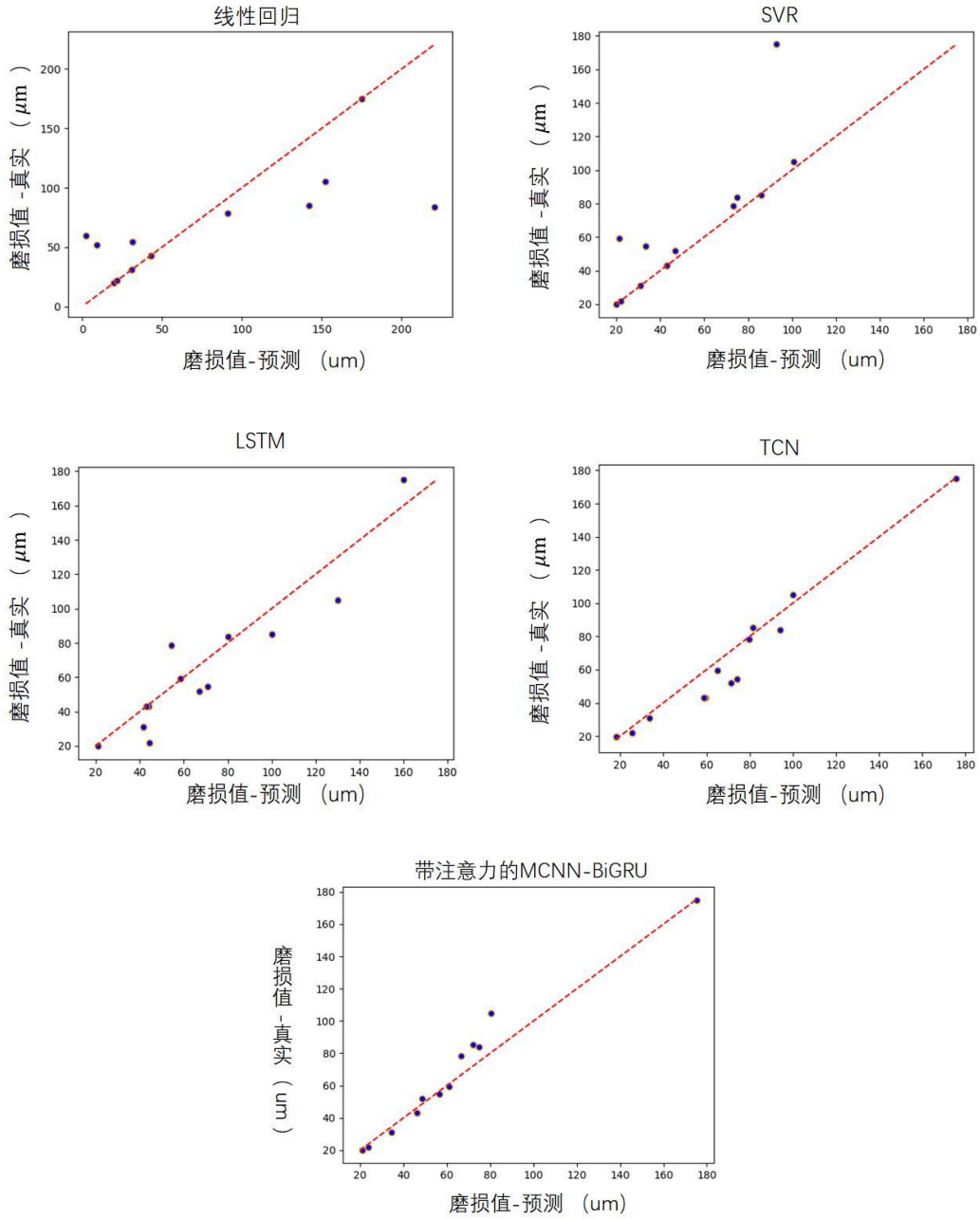


图 12 上述五种方法在测试集上的预测表现散点图

可以发现深度学习对比机器学习有着极大的优势，这主要是因为机器学习模型难以学习数据间的非线性关系，并且在属于深度学习的三种方法中，相比经典的 CNN-LSTM 时序预测模型和功能强大的 TCN 模型，本文提出的模型在 MAE、RMSE 两个指标上均做到了好于 TCN，R^2则略逊于 TCN。这可能是因为，一方面，刀具在给定时刻的磨损值预测需要考虑刀具当前状态和未来可能的操作，这使得 BiGRU 网络对比 CNN-LSTM 来说可以挖掘到更多有用的特

征，用于回归预测。

表 2 不同模型在数据集上的表现情况

模型	MAE	RMSE	R^2
LR	27.86	52.02	-0.68
SVR	12.74	25.96	0.58
CNN-LSTM	11.4	18.4	0.85
TCN	8.84	9.79	0.92
带注意力的 MCNN-BiGRU	6.03	9.01	0.94

而从训练过程角度分析，本文提出的带注意力的 CNN-BiGRU 方法虽然在训练时间上耗时最长，但相比于 CNN-LSTM 与 TCN 收敛的速度最快，仅需训练 200 个左右的轮次便可达到收敛；而 CNN-LSTM、TCN 模型虽然训练速度快，但需要训练接近 1,000 个轮次才逐渐收敛，每次梯度更新对于模型参数更新的影响都不是很大。这可能是因为本文提出的网络结构中卷积操作包含有零填充，并且引入了自注意力机制，使得网络可以选择性的舍弃不那么重要的信息、关注更为重要的信息，从而使得模型更快收敛。

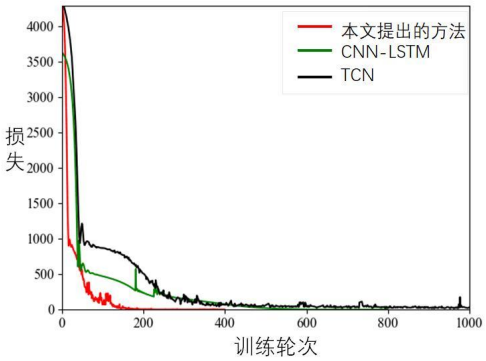


图 13 三种深度学习方法的训练过程损失

除此之外，本文提出的带注意力的 CNN-BiGRU 网络使用了三种不同尺度的卷积核，并通过引入注意力机制，使得网络在不同尺度上、同通道间都有能力实现更全面的特征挖掘与融合能力。

综上所述，通过实验的验证，发现所提出模型的精度较高，证明该模型具有较强的特征挖掘与融合能力。该模型的 RMSE、MAE 值均优于其他四种方法，R^2值略逊于 TCN，证明了该模型在处理多通道时序数据上的优越性。

4.5.2 模型泛化性能验证

为了进一步验证模型的泛化性能，本文在 IEEE PHM2010 挑战数据集[24]上对本文提出的带注意力的 CNN-BiGRU 模型、TCN 模型的表现进行了进一步的验证。由于该数据集中只有 C1, C4 和 C6 数据集有相应的刀具磨损值，因此本实验使用 C1, C4 和 C6 数据集来验证模型并规定 C1、C4 为训练集，C6 为验证集。图 14 为三组数据中铣刀各切削刃的磨损曲线：

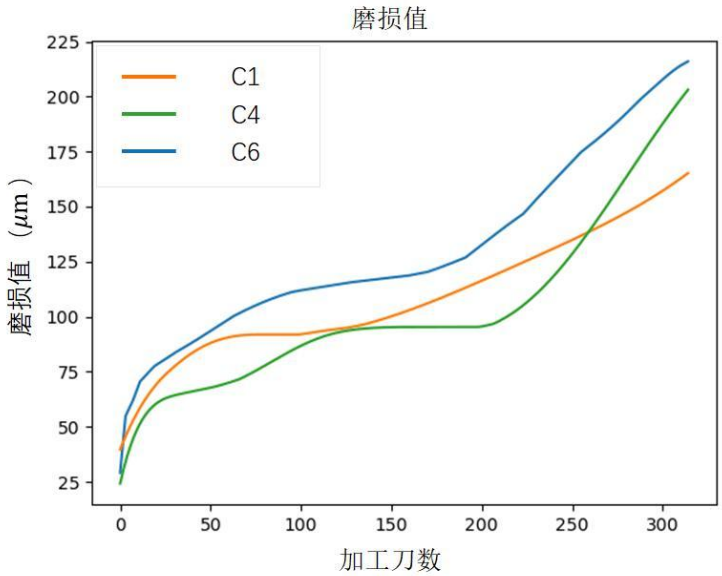


图 14 数据集标签展示

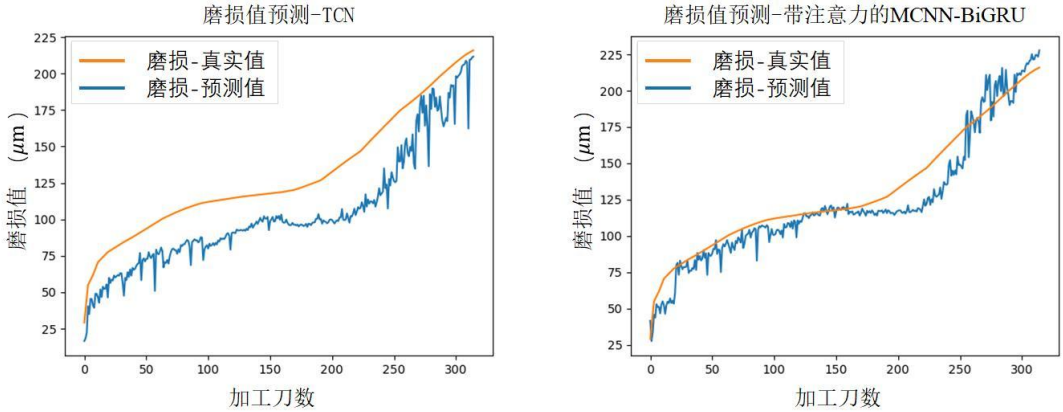


图 15 测试集预测结果

图 15 分别展示了本文提出的模型和 TCN 模型在 PHM2010 数据集上的测试结果。可以看到，本文提出的模型基本上学习到了刀具的退化过程，磨损值的预测值曲线和真实值曲线大体呈现相同的上升趋势，这证明本文提出的模型具有一定的可迁移性。

表 3 测试集评价指标

方法	MAE	RMSE	R^2
TCN	9.96	12.85	0.89
带注意力的 MCNN-BiGRU	10.95	12.67	0.89

表 3 展示了这两种模型在该数据集上的性能指标可以看出，在 PHM 2010 公开数据集上，成熟的 TCN 模型与本文所提出的带注意力机制的 MCNN-BiGRU 模型在 MAE、RMSE 和R^2三个指标上的表现大致相同，其中 MAE 略逊于本文提出的模型，RMSE 略优，而R^2基本没有区别，这也从反面验证了带注意力的 MCNN-BiGRU 模型之所以在卧式镗削加工实验中的表现优于使用了膨胀卷积的 TCN，很大程度上是因为 MCNN-BiGRU 提取通道间信息对预测精度

的贡献，超过了使用更好的卷积结构对预测精度做出的贡献。

5　结论

针对航空工业整机镗削加工工况和多通道时序数据的处理，本文提出了一种带注意力的基于 CNN-BiGRU 的深度学习模型，并通过了一系列的实验验证，模型可以自动的提取多通道时序数据的时间、空间特征，实现了对刀具磨损值的回归预测。并且通过实机实验与公开数据集的验证，证明了本文提出的带注意力的 CNN-BiGRU 模型在多通道时序数据的处理上获得了优于对照组模型的表现。另外，提出了一种基于多源数据的、结合了 SAM 模型和带注意力的 CNN-BiGRU 模型的对刀具进行在线的磨损状态监测的方法，可以应用到实际的生产加工过程中，为加工过程中的相关决策提供帮助。

实验结果表明，数据驱动方法在刀具磨损状态的预测领域有着不错的效果，在未来，我们将尝试对方法进行改进，以达到更好的效果和创新性。

参考文献：（参考文献格式参照 2015 年新标准 GBT 7714-2015）

[1] 袁立.航空制造工程手册（第 2 版）［M］．北京航空工业出版社，2010.

[2] 邱立军,吴明辉.PHM 技术框架及其关键技术综述[J].国外电子测量技术,2018,37(02):10-15.

[3] Atabey F, Lazoglu I, Altintas Y. Mechanics of boring processes—Part I[J]. International Journal of Machine Tools and Manufacture, 2003, 43(5): 463-476.

[4] Li Z, Liu Q, Ming X, et al. Cutting force prediction and analytical solution of regenerative chatter stability for helical milling operation[J]. The International Journal of Advanced Manufacturing Technology, 2014, 73: 433-442.

[5] Olortegui-Yume J A, Kwon P Y. Tool wear mechanisms in machining[J]. International Journal of Machining and Machinability of Materials, 2007, 2(3-4): 316-334.

[6] 曾六生.飞机部件装配精加工[J].航空制造技术,2002,(10):63-66.

[7] 王子豪. 大数据环境下的刀具剩余寿命智能预测研究[D].哈尔滨工业大学,2022

[8] Benkedjouh T, Medjaher K, Zerhouni N, et al. Health assessment and life prediction of cutting tools based on support vector regression[J]. Journal of Intelligent Manufacturing, 2015, 26: 213-223.

[9] Sawant V, Deshmukh R, Awati C. Machine learning techniques for prediction of capacitance and remaining useful life of supercapacitors: A comprehensive review[J]. Journal of Energy Chemistry, 2023, 77: 438-451.

[10] Wang Y, Zhao Y, Addepalli S. Remaining useful life prediction using deep learning approaches: A review[J]. Procedia Manufacturing, 2020, 49: 81-88.

[11] Wang B, Lei Y, Yan T, et al. Recurrent convolutional neural network: A new framework for remaining useful life prediction of machinery[J]. Neurocomputing, 2020, 379: 117-129.

[12] Li H, Zhao W, Zhang Y, et al. Remaining useful life prediction using multi-scale deep convolutional neural network[J]. Applied Soft Computing, 2020, 89: 106113.

[13] Zhang X, Lu X, Li W, et al. Prediction of the remaining useful life of cutting tool using the Hurst exponent and CNN-LSTM[J]. The International Journal of Advanced Manufacturing Technology, 2021, 112: 2277-2299.

[14] Wang H, Peng M, Miao Z, et al. Remaining useful life prediction techniques for electric valves based on convolution auto encoder and long short term memory[J]. ISA transactions, 2021, 108: 333-342.

[15] Li T, Zhao Z, Sun C, et al. Hierarchical attention graph convolutional network to fuse multi-sensor signals for remaining useful life prediction[J]. Reliability Engineering & System Safety,2021, 215: 107878.

for remaining useful life estimation under variable failure behaviors[J]. Reliability Engineering & System Safety, 2021, 216: 107946.

[17] 汪海晋，尹宗宇，柯臻铮，等.基于一维卷积神经网络的螺旋铣刀具磨损监测[J].浙江大学学报:工学版，2020, 54(5):931-939.

[18] 李亚平,李素杰,马波,等.基于 TCN 的滚动轴承振动趋势与剩余寿命预测研究[J].现代制造工程,2021(09):124-131.

[19] 刘耕鑫，董辛旻，张瑞博，等. 基于特征选择与 Transformer 的涡扇发动机剩余使用寿命预测[J]. Machine Tool & Hydraulics, 2024, 52(7).

[20] 蔡伟立,胡小锋,刘梦湘.基于迁移学习的刀具剩余寿命预测方法[J].计算机集成制造系统,2021,27(06):1541-1549.

[21] 刘战强,艾兴.高速切削刀具磨损表面形态研究[J].摩擦学学报,2002(06):468-471.

[22] 张蕊,李锦涛.基于深度学习的场景分割算法研究综述[J].计算机研究与发展,2020,57(04):859-875.

[23] Kingma D P, Ba J. Adam: A method for stochastic optimization[J]. arXiv preprint arXiv:1412.6980, 2014.

[24] PHM Society. PHM society conference data challenge. https://www.phmsociety. org/competition/phm/10

[作者简介]

杨展鹏(2001-)，男，硕士，在读，主要从事数据驱动建模理论及其工业应用的研究；

华丰(1995-)，男，博士，在读，主要从事数据驱动建模理论及其在工业应用的研究；

付白斗(2003-)，男，学士，在读，主要从事自然语言处理与多源异构数据融合的研究；

胡笑楠(2001-)，男，硕士，在读，主要从事计算机视觉稠密预测相关任务研究；

程骋(1990-)，女，博士，讲师，主要从事工业大数据和智能制造等方面的理论和应用研究；

袁烨(1986-)，男，博士，教授，主要从事辨识、控制及优化理论，人工智能等方面的科研工作。

基于多源特征融合的飞机翼身交点孔精密镗削刀具磨损状态监测

杨展鹏[1]，华丰[2]，付白斗[1]，胡笑楠[1]，程骋[1]，袁烨[1]

（1. 华中科技大学 人工智能与自动化学院，湖北武汉 430074；2. 华中科技大学 机械科学与工程学院，湖北武汉 430074）

摘　要：装配是航空装备制造的最后一个环节，直接决定最终交付质量。在飞机的装配过程中，翼身交点孔作为连接机身与机翼的关键交点孔，影响着最终飞机产品的机翼平衡能力、飞机机动性能、外形准确性等，对加工精度的要求达到了 0.001mm 量级。目前通用的加工方法普遍采样少量多次的保守试切策略，加工占比时间长，是飞机装配过程中极为重要的一环。基于此，本文提出了一种属于数据驱动型的整机超大尺寸交点孔精密镗削刀具磨损状态监测方案，基于仿翼身交孔的实机精密卧式镗削加工实验收集到的时序与图像数据，实现了对刀具前后刀面磨损状态的准确预测。实验结果表明，该方法在均方根误差、平均绝对误差与R^2上的表现均优于经典机器学习与深度学习模型，同时该方法也在公开数据集上表现出良好的泛化性能。

关键词：翼身交点孔；刀具磨损状态预测；深度学习

Improvement of Visual Sensing System via Dual Attention YOLOv5 in Calcium Carbide Factory

ZHU Haijiang[1], LIU Yutong[1], WANG Yan[2], ZHAO Lina[3]

Abstract—**In the early days, visual sensors were highly applied to supervise the wearing of fire-resistant clothing to ensure safe production in calcium carbide factories. However, artificial intelligence is difficult to apply to these visual sensing systems with the rapid development of information technology. Considering this, an improved approach is established that allows for the operation of old visual sensing system without adding too much financial expenditure in this paper. Herein, we first improve Efficient Channel Attention (ECA) and Pyramid Split Attention (PSA) module. Two attention modules are also integrated into bottleneck module of the YOLOv5 network, which is named as Dual Attention based on YOLOv5 (DA-YOLOv5). Public dataset and self-made dataset are utilized to validate the effectiveness of the proposed approach. At the same time, the impact of data augmentation and annotation quality on performance was studied to guide the application of the algorithm in practical engineering. The results show that the improvement of old visual sensing system is successful in calcium carbide factories.**

Keywords — **artificial intelligence, image sensors, industrial internet, object detection, safety measurement**

Manuscript received June. 28, 2024; accepted August. 10, 2024.

ZHU Haijiang, LIU Yutong. The College of Information and Technology, Beijing University of Chemical Technology, Beijing 100029, China (e-mail: 2007500037@buct.edu.cn; 2021400211@buct.edu.cn).

WANG Yan. China CACS Engineering Corporation, Beijing, 100026 China (e-mail: 1261983114@qq.com).

ZHAO Lina. The College of Mathematics and Physics, Beijing University of Chemical Technology, Beijing, 100029 China (e-mail: zhaoln@buct.edu.cn).

This work is supported by the National Natural Science Foundation of China under grant No. 92367111.

I. INTRODUCTION

Industrial Internet is a new type of infrastructure, application mode and industrial ecology that is deeply integrated with the new generation of information and communication technology and industrial economy. The purpose is to promote the digital, networked, and intelligent development of industry. Visual sensing systems in the calcium carbide production workshop were widely utilize to monitor the wearing of safety protective clothing and helmets. This is an important application scenario of industrial Internet, which can guarantee the safety of life and property. The visual sensing system consists of cameras, image acquisition cards, computers, visual processing software, etc. At present, visual sensing systems have achieved productization and practicality in many fields. The functions of related equipment such as image sensors, image acquisition cards, and visual processors are

becoming increasingly sophisticated with the rapid development of artificial intelligence technology[1,2].

Most calcium carbide factories had installed many image sensors to supervise the wearing of fire-resistant clothing in China. However, these early visual sensing systems had high labor costs and were prone to misjudgment due to human eye fatigue, which required manual interpretation. Can we transform the existing visual sensing systems in the calcium carbide factory into an automatic or semi-automatic fire clothing monitoring system. This itself is a challenge.

Considering this, a principle has been established that allows for the operation of old visual sensing systems without additional financial expenditure. These old visual sensing systems in the calcium carbide plants are transformed into applications of deep learning. The image sensors are manufactured by a company in Hangzhou, China in our case. The function of the visual sensing systems is to be supplemented by deep learning.

In the visual sensing systems, object detection is a very important task. Traditional object detection methods are susceptible to interference from image sensor imaging quality, which affects real-time performance and detection accuracy.

Since Hinton has reported a paper on the Deep Belief Network in 2006[3], deep learning has been extensively applied in many fields. YOLOv1[4] network broke the dominance of RCNN algorithm in the target detection in 2015, and only one convolution neural network can achieve the goal of end-to-end target detection. He[5] proposed the Spatial Pyramid Pooling (SPP) layer, which allows input images with different sizes to get the same feature map after passing through the SPP layer, making multi-scale network training more efficient. YOLOv3 algorithm[6] improved the detection accuracy of small targets by introducing feature pyramid module to fuse feature maps of different scales. Subsequently, YOLO networks attracted widespread attention from researchers[7,8,9,10].

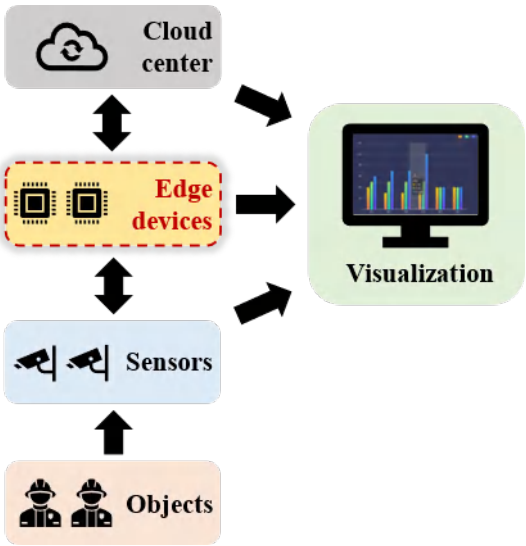


Figure 1 The overall structure of the improved system.

Although YOLO networks are applied for object detection, there is very little reported literature on their application in calcium carbide factory. Because there are overexposure, darkness, smoke or occlusion in calcium carbide production, the data quality obtained by image sensors is low. This is a significant challenge for improving visual sensing systems.

In this article, we propose an improved YOLOv5 for fireproof clothing detection in calcium carbide production. Herein, two improved attention modules are integrated into the backbone network of the YOLOv5 and we call it DA-YOLOv5. The experimental results show that the improved YOLOv5 algorithm has higher detection average accuracy (mAP @ [0.5:0.95]) at different intersection and union ratio thresholds. The main contributions of this paper are summarized below:

- We propose a dual attention module based on YOLOv5 network (DA-YOLOv5) for fireproof clothing real-time detection.
- An improved Pyramid Split Attention (PSA) module is presented to establish information dependencies between spatial attention and remote areas.
- The improvement of visual sensing system in calcium carbide factories is implemented through integrating our designed ECA-SPP module into the DA-YOLOv5.

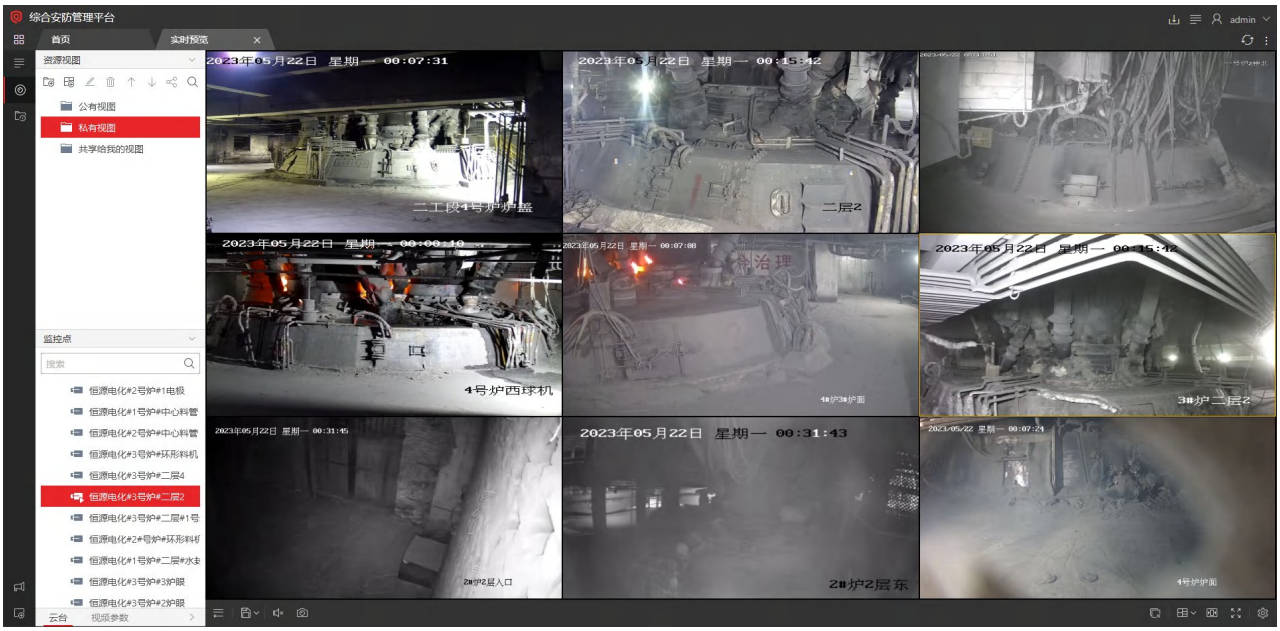


Figure 2 Multi-sensors visual system in the calcium carbide factory.

II. MULTI-CAMERAS VISUAL SENSING SYSTEM

The calcium carbide production workshop often requires workers to carry out production operations on the production site, but the working environment at the operation site is complex. Some areas have dim lighting, many stones on the ground, high temperatures and smoke in some areas, and some areas need to prevent the danger of falling objects from high altitude. The production environment is complex and there are numerous hazardous elements, so it is necessary to protect the personal safety of on-site operators in real time.

Multi-cameras visual sensing system in calcium carbide enterprises are established by HIKVISION company. The old visual sensing system is divided into three parts: video acquisition module, video transmission and processing module, and video display module.

In video surveillance systems, the camera is the most front-end, basic, and largest investment sensor. Its main function is to image and transmit the target area, and its quality directly affects the overall application of the video surveillance system, while also affecting the engineering cost. The camera sensor is connected to a Digital Video Recorder (DVR), and there is a certain limit to the number of DVR channels. After the DVR is fully connected, adding a camera will also increase the hardware cost. The video in DVR can be uploaded to the monitoring center through the local area network. However, there are long image transmission delay, inability to achieve multi-channel simultaneous monitoring, and poor integration in the system.

There are many applications of artificial intelligence detection methods based on edge computing in the field of video surveillance. This technology combines edge computing and artificial intelligence technology. By running AI algorithm on the gateway device, video data can be processed and analyzed in real time on site, thus realizing intelligent identification and analysis. We improve the old visual sensing system through adding some edge devices, and the overall structure is shown in the Fig.1.

The image data can be acquired from this visual sensing system at the different calcium carbide factories, and these image data are displayed in Fig.2.

To reduce the risk of high-temperature burns, falling objects, and other injuries to on-site workers, they need to wear protective clothing and safety helmets to protect

Figure 3 Example of protective clothing and helmet from sensor.

their own safety. According to the different operating environments, the protective clothing for on-site workers is divided into two types: the first type is a full body silver protective clothing, including protective helmets and fire-resistant clothing; The second type is fireproof clothing and safety helmets. The two types of protective clothing in Fig.3 will serve as instance objects for the dataset in this article.

III. ARCHITECTURE OF THE PROPOSED DEEP LEARNING ALGORITHM

In this section, we describe the structure of our proposed deep learning algorithm, which is called DA-YOLOv5.The overall framework of the DA-YOLOv5 is illustrated in Fig.4.

In DA-YOLOv5, three improvements are presented. First, SENet (squeeze excitation) weight module is replaced by ECA (efficient channel attention) weight module[11]. Second, the ECA attention module[11] is inserted after each pooling core in the SPP (spatial pyramid pooling) module. Finally, the YOLOv5network is improved through inserting PSA and ECA attention modules. The DA-YOLOv5 network may enhance feature extraction, learn more multi-scale information, and compensate for the lack of global convolution. And the proposed network may also obtain more global contextual information, increase receptive fields, and thus improve the detection performance of the network.

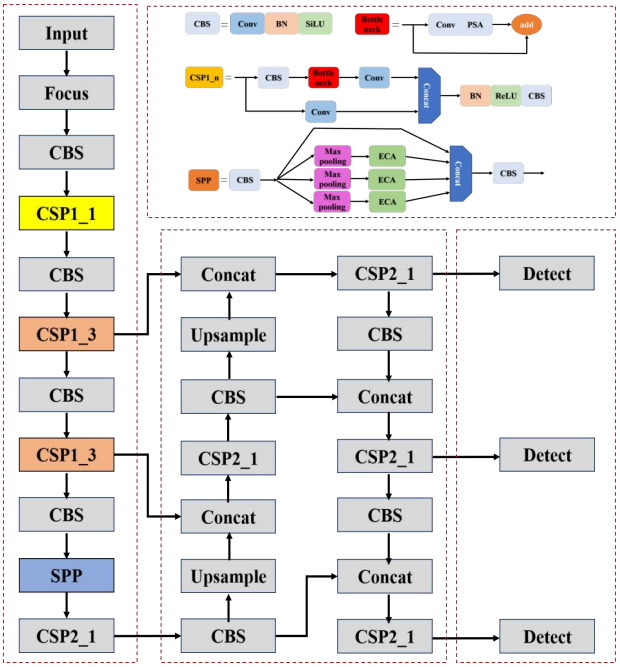


Figure 4 The framework of the DA-YOLOv5.

A. IMPROVED PSA MODULE

The detailed framework of the improved PSA module[5] is shown in Fig.5. First, the feature map is input to the SPC module and divided into s groups at the channel level. Then, multi-scale feature maps can be obtained by performing convolution operations on the feature maps in each group. Next, the weight values of channels in each group are estimated through inputting the multi-scale feature maps into the ECA attention module. The ECA module[11] is substituted for the SENet channel attention module in the improved PSA module. Finally, a softmax function is normalized the weights , and the normalized weights and their corresponding values are summed to obtain the final attention.

The improved PSA module compensates for the shortcomings of attention modules such as SE, BAM(Bottleneck Attention Module) and CBAM(convolution block attention module). It can capture spatial information at multiple scales to enrich the feature space, and establish information dependencies between spatial attention and remote areas. The improved PSA module can reduce the workload of algorithm.

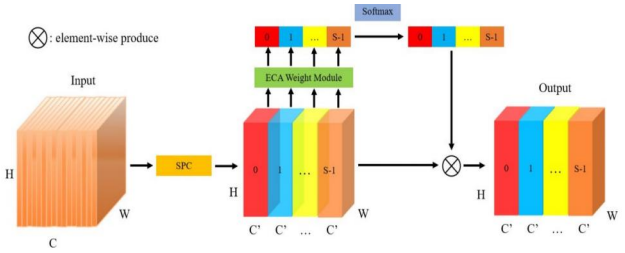


Figure 5 The framework of the improved PSA module.

Subsequently, the improved PSA(IPSA) module is substituted for the 3×3 convolution of the Bottleneck in Darknet-53, which is the backbone network of YOLOv5. We combine IPSA-Bottleneck with CSP (Cross Stage Partial) and acquire an improved CSP module. The improved CSP module may reduce the calculation amount of the network and remove the repeated gradient information. It may also enhance the learning ability of the whole network. In comparison with the third row and the forth one in Tab.7, we can see that the improved model has a 2.08% increase in mAP @ [0.5:0.95] based on original Yolov5 network.

B. ECA-SPP MODULE

The ECA channel attention module is an improved version of the SENet attention module. This module is a local cross channel interaction without dimension reduction, and can lower the influence on channel attention learning without reducing dimensions.

The full connection layer in the SENet was discarded in the ECA module, and the 1D convolution of shared weights is adopted directly. The size of kernel in 1D convolution can be adaptive determined through the mapping of channel dimensions. The ECA module not only reduces the number of network parameters, but also effectively obtains cross channel interaction information. And then The ECA module is helping to improve the network performance.

In the backbone network of YOLOv5, the ECA module is integrated into the SPP module. We call it ECA-SPP module, which its structure is illustrated in Fig.6. After each pooled core in the SPP module, the ECA attention module is inserted. Thus, the feature

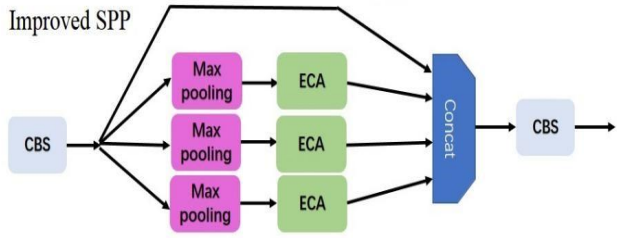


Figure 6 The improved SPP module.

information with different scales is acquired through the ECA attention module.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The operating system in this experiment is Linux Ubuntu 20.04.4 LTS, and the processor is 12th Gen Intel ® CoreTM i9-12900K×24. The GPU is a 24GB GeForce RTX 3090Ti video memory. The algorithm is a Python framework, and CUDA11.1 parallel computing architecture is used. The YOLOv5s with the smallest model is adopted. In this experiment, the number of iterations is set to 1200, and the initial learning rate is 0.01. The parameter of the maximum training batch is 16, Adam optimizer and the loss function CIoU are selected.

A. DATASETS

The datasets of object detection on calcium carbide industry are rarely reported, and a dataset that represents safety helmet and protective clothing wearing in calcium carbide plants is created. A public dataset on safety helmet wearing detection is named as SHWD[12].

Our dataset has a total of 11952 images, of which 8963 are training sets and 2989 are validation sets. The labels of the dataset are divided into three categories according to the standard, people are labeled as person category, wearing safety helmets are labeled as helmet category, and wearing protective clothing are labeled as cloth category. According to statistics, there are a total of 31522 labeled labels, of which person category labels have 12881, helmet category labels have 9434, and cloth category labels have 9207. According to the general dataset COCO, the objects in the dataset images

Table 1 Comparison of the DA-YOLOv5 combined with one data enhancement method.

No data augmentation	Geometric transformation	Mosaic	HSV	Mixup	Precision	mAP
√					0.6952	0.3432
	√				0.9518	0.5502
		√			**0.9551**	**0.6468**
			√		0.9242	0.3695
				√	0.6894	0.3420

Table 2 Comparison of the DA-YOLOv5 combined with various data enhancement methods.

No.	Geometric transformation	Mosaic	HSV	Mixup	Precision	mAP
1					0.6952	0.3432
2	√	√			0.9452	0.6695
3	√		√		0.9519	0.5579
4	√			√	0.9536	0.5455
5		√	√		0.9531	0.6449
6		√		√	0.9537	0.6490
7			√	√	0.9341	0.3635
8	√	√	√		0.9447	0.6678
9	√	√		√	0.9506	0.6698
10	√		√	√	0.9542	0.5558
11		√	√	√	**0.9546**	0.6475
12	√	√	√	√	0.9481	**0.6719**

are divided into small objects, medium objects, and large objects. Among them, small objects are smaller than 32 * 32 pixels, medium objects are between 32 * 32 pixels and 96 * 96 pixels, and large objects are larger than 96 * 96 pixels. According to this standard, there are 5328 small object labels, 19481 medium object labels, and 6713 large object labels in this dataset.

SHWD[12] provides the dataset used for both safety helmet wearing and human head detection. It includes 7581 images with 9044 human safety helmet wearing objects(positive) and 111514 normal head objects (not wearing or negative). A total of 5457 training set images and 607 verification set images are selected. This dataset is simple of scenario and easy to classify.

B. EXPERIMENTS ON THE IMPACT OF DATA AUGMENTATION ON NETWORK MODEL

In this experiment, different data augmentation methods are combined to compare the improvement effect of improved YOLOv5 network indicators. Here, data augmentation methods include geometric transformation, Mosaic, HSV and Mixup. Tab.1 compares the experimental results of one augmentation method combined with the improved YOLOv5 network. From Tab.1, the network metrics with data augmentation methods are higher than those without data augmentation methods. Among them, the mAP value of the mosaic method has increased by 30.36%, and the improvement effect is very significant. Then HSV and Mixup have little effect on improving network model metrics. By analyzing the loss curve, we found that the network combining HSV and Mixup experienced overfitting, while the network combining mosaic effectively suppressed the overfitting. The experimental results indicate that appropriate data augmentation methods can effectively improve the richness of the dataset and enhance the generalization of network.

In addition, we perform experiments by combining

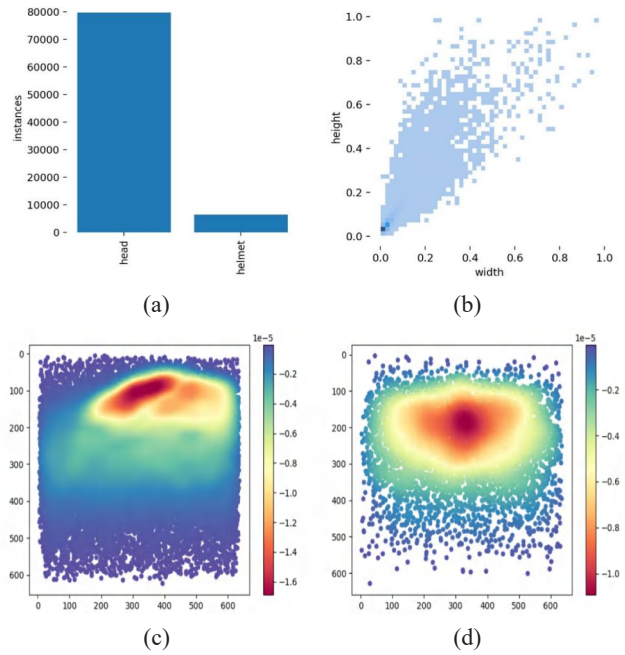


Figure 7 Data information statistics in SHWD [12].

two or three data augmentation methods with the DA-YOLOv5 network. The experimental results are listed by Tab.2. We can see that the combination of four data augmentation methods lead to the greatest improvement in network model performance, with a 32.87% increase. Data augmentations effectively decrease overfitting of network models, enhances their generalization, and improves their detection performance.

C. EXPERIMENT ON THE IMPACT OF OBJECT LABEL MISLABELING

In this section, we conduct experiments on the impact of missing labels and large annotation boxes on the DA-YOLOv5 network. The dataset used in this experiment is SHWD[12], which provides data for helmet wearing and human head detection. Fig.7 is data information statistics of the dataset SHWD[12]. Fig.7(a) shows the quantity distribution of each category in the dataset label. Fig.7 (b) shows the aspect ratio of the annotation boxes for each instance object in the dataset, with the horizontal and vertical coordinates of each pixel being the normalized result. Fig.7 (c) is the density distribution of the center points of the annotation boxes for head class labels. The red part in the figure indicates a high density of the center points of the annotation boxes in that area, while the blue part indicates a low distribution of the center points of the annotation boxes in that area. Fig.7 (d) is the density distribution of the center points of the annotation boxes for helmet class labels. The red part indicates a high density of the center points of the annotation boxes in this area, while the blue part indicates a low distribution.

Table 3 The impact of different labels missing rates on evaluation results in SHWD [20].

No.	The proportion of deleted data	mAP@[0.5:0.95]
1	**0**	**0.5319**
2	0.1	0.5108
3	0.2	0.5087
4	0.3	0.4671
5	0.4	0.4351
6	0.5	0.4166
7	0.6	0.3695
8	0.7	0.3492
9	0.8	0.2893
10	0.9	0.1921

For all instance objects in the dataset, this experiment randomly removes labels from each category at a certain ratio. Images without any labels are deleted to avoid networks using instances in the images as backgrounds, which may have a negative impact on network training. We will evenly distribute the deleted label instances to each image, while protecting images with fewer labels. And images with more labels are first deleted to avoid reducing the number of the dataset.

In the experiment, the label instances in the corresponding files of each image were deleted by reducing the total number of labels by 10% each time, and the remaining dataset was trained. The experimental results are shown in Tab.3. The DA-YOLOv5 indicators gradually decrease with the deletion ratio increasing. When the deletion ratio is 0.3, the network model indicators decrease significantly. Therefore, when there is a missed label, the training network will consider the unlabeled object as the background and provide incorrect information during training.

Table 4 The experimental results with the expanded annotated boxes dataset.

No.	Adding pixels	mAP@[0.5:0.95]
1	**0**	**0.5319**
2	2	0.4799
3	4	0.4203
4	6	0.3422
5	8	0.2602
6	10	0.2281

D. EXPERIMENTS ON THE INFLUENCE OF OBJECT ANNOTATION BOX SIZE

This section discusses the impact of expanding the annotation box on the training metrics of the DA-YOLOv5 network. We only employ a helmet wearing detection dataset in this experiment. and expands the instance object labels in the label file corresponding to each image by 2 pixels each time according to the width and height of the annotation box. The width and height of the annotation box for instance objects are expanded by 2 pixels at a time. The experimental results using the expanded dataset with annotated boxes for training are listed in Tab.4.

We can see that the evaluation index of the DA-YOLOv5 network gradually decreases with the annotation box expands. When the annotation box is expanded by 8 pixels, the indices decrease the fastest. When the annotation box expands, the training network mistakes the background in the annotation box for an instance object. This lead to have a negative impact on the localization loss function and classification loss function, and a decrease in the network's evaluation metrics. In addition, we also present loss function curves with different expanded annotation boxes. The loss function of the original dataset converges the fastest and has the smallest loss value. Therefore, we not only ensure that there are no missing labels on the instance object, but also the annotation box is tightly aligned with the edge of the target object. This can avoid unnecessary background in the annotation box and reduce the impact of background on network training.

Table 5 The experimental results when ECA module is set at the different location.

No.	Model	mAP@[0.5:0.95]
1	**ECA-YOLOv5-Backbone**	**0.8710**
2	ECA-YOLOv5-Neck	0.7795
3	ECA-YOLOv5-Head	0.8560

E. EXPERIMENT ON TESTING ECA ATTENTION MODULES AT DIFFERENT POSITIONS

In this experiment, the detection accuracy of the network is validated when the ECA module is placed at the backbone network, the neck, and the prediction head of the improved YOLOv5.

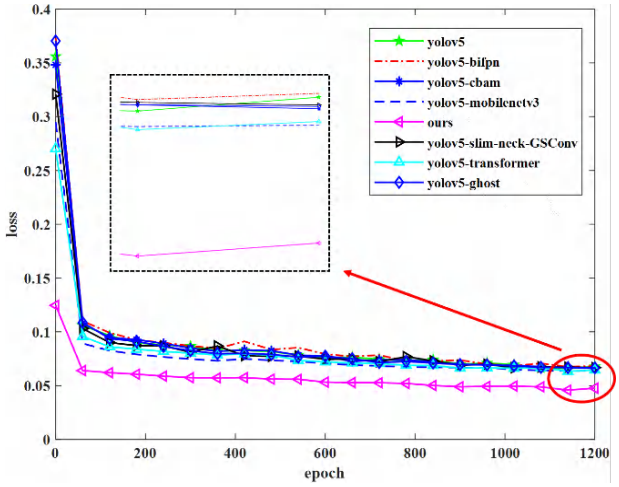
Tab.5 presents the experimental comparison results of ECA attention module integration into three different locations of the YOLOv5 network. We can see that the mAP of the ECA attention module integrated in YOLOv5 backbone network is the highest among the three cases. This is because more undiscovered contour, texture and other information can be extracted in the backbone network. When the ECA attention module is added to the neck and prediction head, the image feature map size is smaller, there is more redundant semantic information, and the channel is too large. These are easy to cause the problem of over fitting in network. The attention module is close to the classification layer, and its effectiveness will have a greater impact on classification. Thus, this leads to lower prediction accuracy.

F. PERFORMANCE TEST EXPERIMENT OF THE PROPOSED DA-YOLOV5

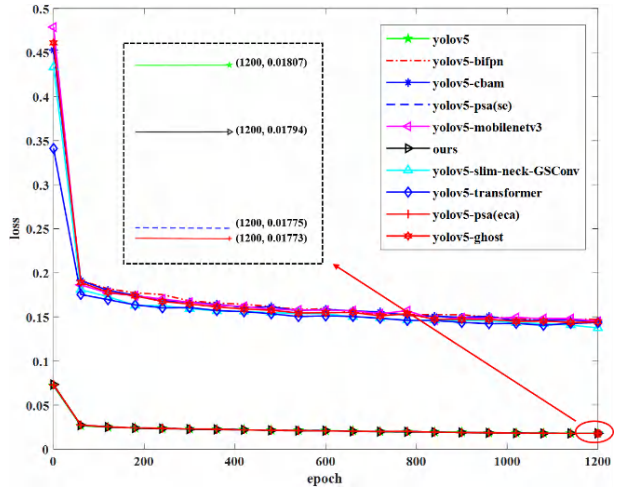
The evaluation indicators in this experiment include precision(P), recall(R), mean average precision (mAP), etc.[13]. And the loss function in YOLOv5 network is also utilized to assess the improved method. The loss function is written by equation (1).

$$\boldsymbol{L} = \sum_{i}^{N}\left(\lambda_1 \boldsymbol{L}_{box} + \lambda_2 \boldsymbol{L}_{obj} + \lambda_3 \boldsymbol{L}_{cls}\right) \quad (1)$$

where λ_1, λ_2 and λ_3 are weight coefficients, $\boldsymbol{L}_{box}$ is the bounding box regression loss, $\boldsymbol{L}_{obj}$ is the

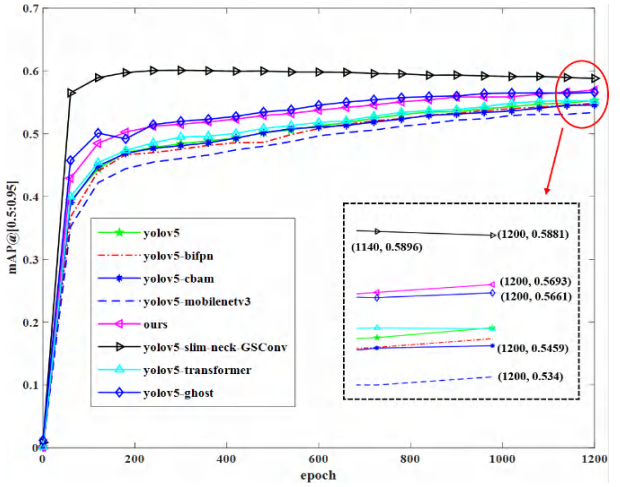


(a)

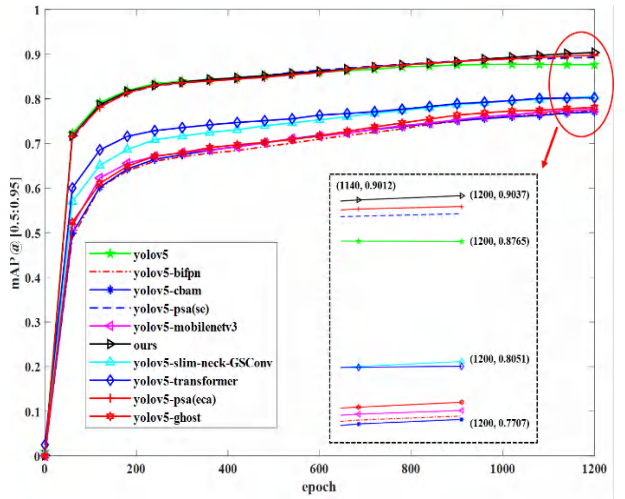


(b)

Figure 8 The loss curves of our network and other YOLOv5 networks: (a)SHWD, and (b)Our dataset.



(a)



(b)

Figure 9 The mAP curves of our network and other YOLOv5 networks: (a)SHWD, and (b)Our dataset. The abscissa represents the number of network training times, and the ordinate is the value of mAP@[0.5:0.95].

confidence loss, and L_{cls} is the classification loss. Fig.8 shows the loss curves of this method and other methods based on YOLOv5 on the SHWD[12] and our dataset. The smaller the loss value, the smaller the error between the predicted value and the true value of the method. Fig.9 displays the mAP curves of this method and other methods based on YOLOv5 on the SHWD[12] and our dataset. The higher the mAP value, the better the model performance.

From the loss curves, our improved method converges faster, with a lower loss value and a higher mAP value for the SHWD[12] dataset. In our dataset, the loss value of the improved DA-YOLOv5 is slightly higher than that of the YOOv5-PSA (ECA) and YOOv5-PSA (SE) methods, with a difference of 2.1×10^(-4). The improved DA-YOLOv5 in this paper has higher mAP value. Because YOLOv5-PSA (ECA) and YOLOv5-PSA (SE) methods produce over fitting in training, the mAP values of them have no further raising.

G. COMPARATIVE EXPERIMENTS

In this section, a comparative experiment between the proposed DA-YOLOv5 and the existing object detection methods for our dataset and SHWD[12] are firstly presented. And then the visualization results of DA-YOLOv5 and YOLOv5 in the calcium carbide plant are illustrated in Fig.10 and Fig.11.

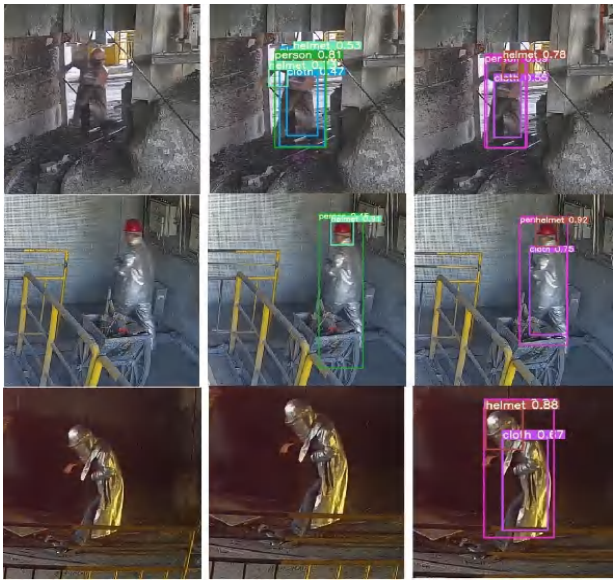


Figure 10 Comparison of detected results. The mislabeled and missed detection are presented in second column using the original YOLOv5, and the third one is correct. The box in the figures is the prediction box. The helmet, person, and cloth on the prediction box are the predicted results, and the number after the category is the confidence.

Figure 11 Comparison of detected results. The second column is false detection using the original YOLOv5, and the third one is correct detection. The box in the figures is the prediction box. The helmet, person, and cloth on the prediction box are the predicted results, and the number after the category is the confidence.

First, the proposed DA-YOLOv5 is compared with other YOLOv5 detection algorithms. The experimental results are listed in Tab.6. The second column in Tab.6 is different network models, and the third column is the mAP@[0.5:0.95] value obtained after training. We can see that the other improved YOLOv5 methods have a few increases in the detection effect of safety helmet compared with the original YOLOv5 algorithms. The proposed DA-YOLOv5 in this paper has a 3.53% increase in comparison with the original YOLOv5. This indicates that our improved method has a good effect on safety helmet detection.

Table 6 The comparison of experimental results of helmet wearing detection in SHWD[20] dataset.

No.	Models	mAP@ [0.5:0.95]
1	YOLOv5[15]	0.5528
2	YOLO-transformer[15]	0.5662
3	YOLO-BiFPN[15]	0.5486
4	YOLO-Ghost[15]	0.5341
5	YOLO-CBAM[17]	0.5455
6	YOLO-slim-neck-GSConv[16]	0.5522
7	YOLO5-mobileNet[13]	0.5694
8	**DA-YOLOv5(Ours)**	**0.5881**

In our calcium carbide plant dataset experiments, the same experimental conditions are adopted. The comparison experiments are also implemented using the same dataset, and the mAP indicators are used for evaluation. The experimental results are presented in Tab.7. In Tab.7, the second column in the table is different network models, the third column is the mAP@[0.5:0.95] value obtained after training, and the fourth column is the parameter amount of the network. The proposed DA-YOLOv5 has the best mAP.

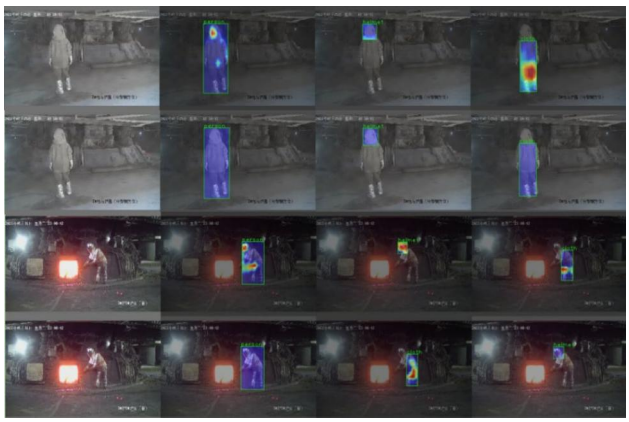
Second, the visual results of the proposed DA-YOLOv5 and the original YOLOv5 are illustrated in Fig.10 and Fig.11. In these experiments, the first column is original images of the calcium carbide plant, the second column is the detected results by the original YOLOv5, and the last column is the results using the proposed DA-YOLOv5.

Fig.10 shows the comparison results of the mislabeled and missed detection in the low contrast and complex background images. There are mislabeled and missed detection in the results by the original YOLOv5. And the proposed method presents the accurate detection.

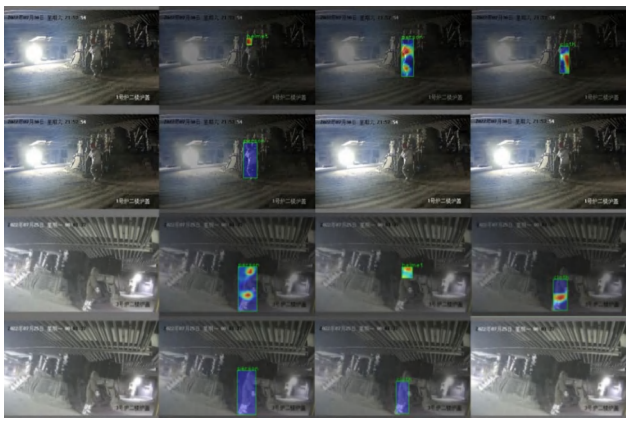
Fig.11 shows the comparison results of the false or true detection using two methods. These detected results by the original YOLOv5 are false detection, and the proposed DA-YOLOv5 presents the true detection.

Table 7 The comparison of experimental results in our dataset.

No.	Model	mAP@ [0.5:0.95]	Parameters
1	SSD300[18]	0.6550	-
2	SSD512[18]	0.7301	-
3	YOLOv5s[15]	0.8765	6129704
4	YOLO5s -PSA(ECA)	0.8973	6238463
5	YOLO5s-PSA(SE)	0.8936	6242429
6	YOLOv5-Transformer[15]	0.8020	7069192
7	YOLOv5-BiFPN[15]	0.7727	6025916
8	YOLOv5-Ghost[15]	0.7723	3693376
9	YOLOv5-CBAM[17]	0.7707	6158640
10	YOLOv5-slim-neck-GSConv[16]	0.8050	7410696
11	YOLOv5-mobileNet[13]	0.7760	4140168
12	**DA-YOLOv5(Ours)**	**0.9037**	6238463



(a)



(b)

Figure 12 The heat map of DA-YOLOv5 and original YOLOv5 network detection in our dataset. The first and third row in (a) and (b) are the results of DA-YOLOv5, and the second and forth row are the results of original YOLOv5.

From the experimental results, we can see that the proposed DA-YOLOv5 has a lower rate of missed or false detection.

In addition, we compared the heat maps of the DA-YOLOv5 network with the original YOLOv5 network through Grad-CAM (Gradient-weighted Class Activation Mapping)[14].

Fig.12 presents the heat map of DA-YOLOv5 and original YOLOv5 network detection in our dataset. The red areas in the heat map represent the parts that the network model is concerned about. The darker the color, the greater the contribution of that part to the target classification.

From Fig.12(a), the DA-YOLOv5 focuses the texture and shape information of the object comparison with original YOLOv5. There are also more focus points in the DA-YOLOv5 network. In Fig.12(b), the DA-YOLOv5 has fewer missed objects compared with original YOLOv5, and the focuses on the target is more significant. For example, the category “person” is paid attention to both head and leg information, and to determine whether the category belongs to “person”.

We can see from these heat maps that the DA-YOLOv5 network has more concentrated features in determining target categories, which indicates the feasibility of the DA-YOLOv5 network.

V. CONCLUSION AND FUTURE WORK

This paper has described the improved YOLOv5

network for the detection of helmet and fireproof clothing in calcium carbide plants. Through integrating the Pyramid Segmentation Attention (PSA) module into the feature extraction network, the receptive field and feature extraction ability were increased. And the Efficient Channel Attention (ECA) module was introduced into the SPP module to obtain more multi-scale information and global context information. The experimental results on the public dataset and our dataset shown that the improved method had obtained the best detection results on both datasets. Meanwhile, the effective combination of data augmentation and the impact of annotation quality on performance were explored. The next work will explore how to reduce the reasoning time and improve the real-time efficiency, and strengthen the detection effect of the algorithm in the over-exposure scene.

References

[1] Sanoob A.H., Roselin J., Latha P. Smartphone Enabled Intelligent Surveillance System,IEEE Sensors Journal,2016,16(5):1361-1367.

[2] Armenta J.S.,Andrade A.G., Rodriguez M.D. An Intelligent Multi-Sourced Sensing System to Study Driver's Visual Behaviors. IEEE Sensors Journal, 2021,21(10):12295-12305.

[3] Hinton,G.E.,Osindero, S. and Teh, Y., A fast learning algorithm for deep belief nets. Neural Computation, 2006, 18:1527-1554.

[4] Redmon, Joseph et al. You Only Look Once: Unified, Real-Time Object Detection, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016: 779-788.

[5] He K, Zhang X, Ren S, et al.Spatial Pyramid Pooling in Deep Convolutional Networks for Visual Recognition, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2015, 37(9):1904-1916.

[6] Redmon J , Farhadi A .YOLOv3: An Incremental Improvement[J].arXive-prints, 2018.DOI:10.48550/arXiv.1804.02767.

[7] Song Y., Xie Z., Wang X., Zou Y. MS-YOLO: Object Detection Based on YOLOv5 Optimized Fusion Millimeter-Wave Radar and Machine Vision,IEEE Sensors Journal, 2022,22 (15):15435-15447.

[8] Yan W., Liu W., Bi H.,et al.YOLO-PD: Abnormal Signal Detection in Gas Pipelines Based on Improved YOLOv7,IEEE Sensors Journal, 2023, 23(17) :19737-19746.

[9] Wang Y., Bochkovskiy A., Liao M. YOLOv7: Trainable bagof-freebies sets new state-of-the-art for real-time object detectors, in Proceeding of the IEEE Conference on Computer Vision and Pattern Recognition, 2023: 7464–7473.

[10] Tong X., Li Z. Substation helmet detection based on improved YOLOX-S algorithm, in Proceeding of the IEEE 12th Data Driven Control and Learning Systems Conference, 2023: 129-134.

[11] Wang, Qilong et al. “ECA-Net: Efficient Channel Attention for Deep Convolutional Neural Networks. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) ,2020: 11531-11539.

[12] https://github.com/njvisionpower/Safety-Helmet-Wearing-Dataset.

[13] https://github.com /RedHandLM /MobileNet-YOLOv5.

[14] R.R. Selvaraju,M.Cogswell, A.Das, et.al. Grad-CAM: Visual Explanations from Deep Networks via Gradient-based Localization, Proceedings of the IEEE International Conference on Computer Vision, 2017: 618-626.

[15] Glenn Jocher, Ayush Chaurasia, Alex Stoken et al. (2022). ultralytics/yolov5: v6.2 - YOLOv5 Classification Models, Apple M1, Reproducibility, ClearML and Deci.ai integrations(v6.2). Zenodo. https://doi.org/10. 5281/zenodo.7002879.

[16] Li H., Li J., Wei H., et al. Slim-neck by GSConv: A better design paradigm of detector architectures for autonomous vehicles, 2022, ArXiv abs/2206.02424.

[17] Hao S., Zhang X., Ma X., el al. Foreign object detection in coal mine conveyor belt based on CBAM-YOLOv5. Journal of China Coal Society, 2022,47(11):4147-4156.

[18] Berg A C, Fu C Y, Szegedy C, et al.SSD: Single Shot MultiBox Detector.2015,DOI:10.1007/978-3-319-46448-0_2.

About the authors

ZHU Haijiang received the Ph.D. degree in pattern recognition and intelligent system from the National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 2004. From 2006 to 2007, he was a Visiting Scholar with the Faculty of Engineering, Iwate University, Japan. He is currently a Professor with the College of Information Science and Technology, Beijing University of Chemical Technology. He is interested in image processing and computer vision.

WANG Yan. obtained a bachelor's degree from Beijing University of Chemical Technology in 2020 and a master's degree from Beijing University of Chemical Technology in 2023. He currently works at China CACS Engineering Corporation. He is engaged in research on object detection.

LIU Yutong. received the master's degree from North China University of Technology in 2021 and is currently a doctoral student at Beijing University of Chemical Technology in China. His research interests include machine learning and image processing.

ZHAO Lina [corresponding author] received the Ph.D. degree in applied mathematics from the Chinese Academy of Sciences, Beijing, China, in 2004. She is currently a Professor with the Beijing University of Chemical Technology, Beijing, China. Her research interests include computational and applied mathematics, which includes geometric problems in computer vision, image processing, and information mining from 3-D Big Data.

Resource-Efficient Consensus for Large-Scale Industrial Multi-Agent Systems: An Event-Triggered Approach*

Ruchao Su, Xianwei Li and Shaoyuan Li

***Abstract*— Cooperative tasks of large-scale industrial multi-agent systems are often subject to inevitable high cost and constrains induced by inter-agent communications. To address this important issue, in this paper, we propose a novel event-triggered method for the fundamental problem—output-feedback consensus of multi-agent systems. The proposed method relies on fully distributed control and edge-based event-triggered communications. By utilizing the idea of edge-based nonmonotonic clock variables, the proposed method guarantees the existence of strictly positive inter-event times between events further than achieving Zeno-freeness, and the number of required communications is reduced. Theoretical results are verified via a numerical example.**

I. Introduction

In the last two decades, cooperative control of multi-agent systems (MASs) has drawn much attention due to its broad applications on various fields. A fundamental problem in MASs termed output-feedback consensus, which aims at designing control protocols to achieve an agreement among agents using output measurements, has been widely studied [1]–[3]. Note that, however, the limited energy/channels have restricted the practicality of protocols with continuous communications among agents as in aforementioned earlier results. Event-triggered (ET) strategies, as an effective tool to save more power/resources, are utilized and reported in various fields, whose basic idea is to trigger an activity (e.g, an update of information) only when certain conditions are satisfied. In particular, event-triggered strategies for consensus of MASs are developed in [4], [5], achieving consensus protocols with intermittent communications.

To further address the issues in ET-based output-feedback consensus, the following properties are crucial:

1) Fully Distributed ET Design: In the context of consensus of general linear MASs, the global information of the communication network is required to be known as a prior in earlier results. Instead, the fully distributed design removes the dependence on the global information and facilitates the network scalability.

2) Edge-Based Communications: Node-based ET schemes require each agent to broadcast signals to all of its neighbors simultaneously, while an edge-based scheme allows an agent to transmit information to each neighbor independently, and thus is more flexible and practical.

3) Strictly Positive Minimum Inter-Event Times (MIETs): It is well-known that Zeno-behavior may arise in ET-based protocols. Further than excluding that, a critical and more challenging property is to guarantee the existence of strictly and uniformly positive inter-event times, i.e., the lower bound of MIET would not reach zero (even as time goes to infinity).

Achieving these properties simultaneously in the context of output-feedback consensus is particularly challenging. Fully distributed ET protocols in [6], [7] use time-dependent functions or dynamic ET strategies to relax triggering conditions, but fail to derive the existence of strictly positive MIETs. Related results [8], [9] following the clock variable technique developed in [10] provide fully distributed node/edge-based ET designs with guarantees on strictly positive MIETs, however, their protocols can only tackle state-feedback case. To the best of our knowledege, there are very few results on fully distributed ET design for output-feedback consensus with edge-based communications.

In view of the aforementioned results and discussions, the main contributions of this paper are stated as follows:

i) An observer-based adaptive event-triggered (OB-AET) strategy with asynchronous edge-based communications among agents for output-feedback consensus problem of linear MASs on undirected graphs. Compared with the recent advance [7], a distinctive feature is that the existence of strictly positive MIETs is guaranteed.

ii) A novel edge-based *nonmonotonic* clock variable is introduced for designing triggering conditions. Compared with [8], [9] that utilize similar clock-variable-based techniques on related problems, nonmonotonic clock variables lead to an improved triggering process that helps enlarge the average inter-event time, since the non-monotonicity property delays the time clock variables take to evolve from a positive value to zero (also see remark 1).

A. Graph Theory

Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be an undirected graph, where $\mathcal{V}$ is the node set and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the edge set. Node j is said to be a neighbor of node i if $(j, i) \in \mathcal{E}$. For undirected graphs, $(j, i) \in \mathcal{E}$ if and only if $(i, j) \in \mathcal{E}$. The set of all neighbors of node i is denoted by $\mathcal{N}_i$. The cardinality of the set $\mathcal{N}_i$ is denoted by $|\mathcal{N}_i|$. Each edge is associated with a weight a_{ij} such that $a_{ij} > 0$ if $(i, j) \in \mathcal{E}$ and $a_{ij} = 0$ otherwise. Then Laplacian matrix of the graph is denoted by $\mathcal{L} = [l_{ij}]_{N \times N}$, respectively, where $l_{ii} = \sum_{k \in \mathcal{N}_i} a_{ik}$ and $l_{ij} = -a_{ij}$ for $1 \leq i, j \leq N$. An undirected graph is said to be connected if there exists a path, i.e., an ordered sequence of edges, between any two nodes.

Lemma 1: For an undirected, connected graph $\mathcal{G}$, $\lambda_1 = 0$ is a simple eigenvalue of the Laplacian matrix $\mathcal{L}$ with $\mathbf{1}_N$ as a right eigenvector and other eigenvalues of $\mathcal{L}$ are positive real numbers, and the smallest positive eigenvalue $\lambda_2(\mathcal{L})$ of $\mathcal{L}$ satisfies $\lambda_2(\mathcal{L}) = \min_{\mathbf{1}^{\mathrm{T}} x = 0, \|x\| = 1} \frac{x^{\mathrm{T}} \mathcal{L} x}{x^{\mathrm{T}} x}$.

*This work was supported in part by the Natural Science Foundation of China under Grants 62273227 and 92367203, and in part by the Natural Science Foundation of Shanghai under Grant 21ZR1430500.

The authors are with the Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China, with the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China, and with the Shanghai Engineering Research Center of Intelligent Control and Management, Shanghai 200240, China. {srcatsjtu,xianwei.li,syli}@sjtu.edu.cn

B. Notations

Let $\mathbb{N}$ and $\mathbb{C}$ be the set of non-negative integers and complex numbers, respectively, and $\mathbb{R}^{m\times n}$ denotes the set of $m\times n$ real matrices. For a symmetric matrix $A\in\mathbb{R}^{n\times n}$, $\lambda_{\rm m}(A)$ and $\lambda_{\rm M}(A)$ denote its maximum and minimum eigenvalues, respectively. For a vector $x\in\mathbb{R}^n$, $\|x\|$ denotes its Euclidean norm. For a matrix $X\in\mathbb{R}^{n\times n}$, $\|X\|$ stands for its induced 2-norm, and $\det(X)$ is the determinant of X. The $N\times N$ identity matrix is denoted by I_N. Symbol $\mathbf{1}_N$ denotes the $\mathbb{R}^N$ vector with all elements equal to 1. Symbol $\otimes$ denotes the Kronecker product.

Lemma 2: Given two matrices $A\in\mathbb{R}^{m\times n}$ and $B\in\mathbb{R}^{n\times m}$ with $m\geq n$, then for all $\lambda\in\mathbb{C}$, we have

$$\det\left(\lambda I_m - AB\right) = \lambda^{m-n}\det\left(\lambda I_n - BA\right),$$

II. Problem Formulation

A multi-agent system with N linear agents is considered, whose dynamics are

$$\begin{aligned}\dot{x}_i(t) &= Ax_i(t) + Bu_i(t)\\ y_i(t) &= Cx_i(t),\end{aligned} \tag{1}$$

where $x_i(t)\in\mathbb{R}^n$, $u_i(t)\in\mathbb{R}^m$ and $y_i(t)\in\mathbb{R}^q$ are the state, the control input and the output measurement of agent i, respectively, and A, B and C are constant matrices.

Assumption 1: The matrix pair (A,B) is stablizable, and (C,A) is detectable.

Assumption 2: The communication topology is described by an undirected, connected graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$.

The considered problem is: given the undirected, connected graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$, design a fully distributed edge-based ET protocol based on output measurements such that the resulting closed-loop system satisfies $\lim_{t\to\infty}\|x_i(t)-x_j(t)\|=0$, $\forall(i,j)\in\mathcal{E}$, and the existence of strictly positive MIETs is guaranteed between any two consecutive events.

III. Edge-Based AET Protocol Design

In this section, we propose the designed edge-based adaptive event-triggered control protocol along with the triggering mechanism based on nonmonotonic clock variables.

A. Control Protocol Design

The Luenberger observer is constructed for each agent:

$$\dot{v}_i = Av_i + Bu_i + F(Cv_i - y_i), \tag{2}$$

in which, $v_i\in\mathbb{R}^n$ is the observer state and F is the gain matrix to be determined with an appropriate dimension. Within each event interval, the estimated observer state $\hat{v}_{i,j}$ is utilized to formulate the OB-AET control protocol satisfying

$$\begin{cases}\dot{\hat{v}}_{i,j}(t) = A\hat{v}_{i,j}(t), & t\in[t_k^{i,j},t_{k+1}^{i,j}),\\ \hat{v}_{i,j}(t) = v_i(t), & t=t_k^{i,j+},\end{cases} \tag{3}$$

where $\{t_k^{i,j}|(i,j)\in\mathcal{E},k\in\mathbb{N}\}$ is the time sequence (with $t_0^{i,j}=0$) that denotes time instants when the real observer state $v_i(t)$ is sampled by agent i and transmitted to its neighbor j. Note that $\hat{v}_{i,j}$ is an estimation of v_i shared by agent i and j, and the transmission between agents is asynchronous and edge-based, i.e., in general, $t_k^{i,j}\neq t_k^{j,i}$ and $t_k^{i,j}\neq t_k^{i,q}$ if $q\neq j$. Then, the control input u_i is designed as

$$u_i = K\sum_{j\in\mathcal{N}_i} a_{ij}c_{ij}(\hat{v}_{j,i}-\hat{v}_{i,j}), \tag{4}$$

in the above, c_{ij} is the adaptive parameter for $(i,j)\in\mathcal{E}$, satisfying

$$\dot{c}_{ij} = \kappa_{ij}a_{ij}||K(\hat{v}_{i,j}-\hat{v}_{j,i})||^2, \tag{5}$$

where $\kappa_{ij}=\kappa_{ji}>0$, K is the gain matrix to be determined with an appropriate dimension, and $c_{ij}(0)=c_{ji}(0)>0$, which further implies that $c_{ij}(t)=c_{ji}(t)$ for all $t\geq 0$. By solving the algebraic Riccati equations (ARE):

$$A^{\rm T}P + PA - PBB^{\rm T}P = -2I, \tag{6}$$

$$QA^{\rm T} + AQ - QC^{\rm T}CQ = -I, \tag{7}$$

where $P>0$ and $Q>0$, the gain matrices K and F can determined by $K=B^{\rm T}P$ and $F=-QC^{\rm T}$.

B. Asynchronous Edge-Based AET mechanism

We use $e_{i,j}$ to characterize the estimation error of $\hat{v}_{i,j}(t)$:

$$e_{i,j}(t) = \hat{v}_i^{i,j}(t) - v_i(t),$$

whose dynamics can be given according to (2) and (3):

$$\begin{cases}\dot{e}_{i,j} = Ae_{i,j} - Bu_i + F(Cv_i - y_i), & t\in[t_k^{i,j},t_{k+1}^{i,j}),\\ e_{i,j} = 0, & t=t_k^{i,j+},\end{cases}$$

for $(i,j)\in\mathcal{E}$ and $k\in\mathbb{N}$.

Now we introduce the nonmonotonic clock variable $\xi_{i,j}(t)$ each edge $(i,j)\in\mathcal{E}$, to determine triggering instants. The dynamic of $\xi_{i,j}$ is designed to satisfy

$$\dot{\xi}_{i,j} = \begin{cases}\bar{f}, & \text{if } f_{i,j}>\bar{f} \text{ or } \|e_{i,j}\|=0,\\ f_{i,j}, & \text{otherwise},\end{cases} \tag{8}$$

for $t\in[t_k^{i,j},t_{k+1}^{i,j})$ and

$$\xi_{i,j}(t_k^{i,j+}) = \bar{\xi}_{i,j},$$

where $\bar{\xi}_{i,j}>0$ and $\bar{f}>0$ are any two positive constants. Obviously, the clock variable satisfies $\xi_{i,j}^{\rm a}\geq 0$ for all $t\geq 0$. The time derivative of $\xi_{i,j}$ as in (8) is determined by the function $f_{i,j}(t)$ defined by

$$\begin{aligned}f_{i,j} \triangleq \frac{1}{||P^{\frac{1}{2}}e_{i,j}||^2}\Big[&\sum_{k\in\mathcal{N}_i}\phi_{i,k}a_{ik}c_{ik}||K(\hat{v}_{i,k}-\hat{v}_{k,i})||^2\\ &-2a_{ij}c_{ij}e_{i,j}^{\rm T}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i}) - \xi_{i,j}e_{i,j}^{\rm T}(A^{\rm T}P+PA)e_{i,j}\\ &+2\xi_{i,j}e_{i,j}^{\rm T}PBu_i - \mu_{i,j}||Ke_{i,j}||^2\Big] - \epsilon_{i,j}(\xi_{i,j})^2,\end{aligned} \tag{9}$$

where $\Theta\triangleq K^{\rm T}K$, $\epsilon_{i,j}>0$ and $\phi_{i,j}$ are positive constants that $\phi_{i,j}\in(0,\frac{1}{|\mathcal{N}_i|})$, and $\mu_{i,j}$ is an adaptive parameter for $(i,j)\in\mathcal{E}$, satisfying

$$\dot{\mu}_{i,j} = \pi_{i,j}||Ke_{i,j}||^2, \tag{10}$$

with $\mu_{i,j}(0)>0$ and $\pi_{i,j}>0$ being any two positive constants. Obviously, $\mu_{i,j}(t)>0$ for all $t\geq 0$. The triggering condition for determining event instants $t_k^{i,j}$ is given by:

$$t_{k+1}^{i,j} = \inf\{t>t_k^{i,j}|\xi_{i,j}(t)=0\}, \tag{11}$$

for $(i,j)\in\mathcal{E}$, $k\in\mathbb{N}$ and $t_0^{i,j}=0$.

It should be emphasized that the designed ET mechanism is a recursive real-time verification procedure within each inter-event interval $[t_k^{i,j},t_{k+1}^{i,j})$ and each edge (i,j): $\xi_{i,j}$ is first reset to the positive constant $\bar{\xi}_{i,j}$ at $t=t_k^{i,j+}$, then $\xi_{i,j}$ evolves according to

until it reaches zero, triggering the $(k+1)$th event at $t_{k+1}^{i,j}$. At $t = t_{k+1}^{i,j}$, agent i samples its observer state $v_i(t_{k+1}^{i,j})$ and transmits the newly sampled observer state to neighbor j, entering the next interval $[t_{k+1}^{i,j}, t_{k+2}^{i,j})$.

The setup $\xi_{i,j}^{\mathrm{a}} = \bar{f}$ when $f_{i,j}^{\mathrm{a}} > \bar{f}$ in (8) is a technical treatment for numerical reliability. It can be seen that right after the event instant $t_k^{i,j+}$, the sampling error $e_{i,j}$ varies from zero, which, if the condition $0 < ||e_{i,j}|| << ||K(\hat{v}_{i,j} - \hat{v}_{j,i})||$ holds without the constraint $f_{i,j}^{\mathrm{a}} \leq \bar{f}$, would result in a quite large $f_{i,j}^{\mathrm{a}}$ that causes potential numerical errors.

Remark 1: The clock variable was proposed in the seminal work [10] for ET consensus. On the one hand, compared with the recent advance [7] on fully distributed output-feedback ET consensus, the proposed method guarantees strictly positive MIETs between any two consecutive events. On the other hand, results in related literature [8]–[10] with a similar technique follow a typical paradigm that $\dot{\xi}_{i,j} \leq -\sigma$ for a positive constant $\sigma > 0$, which, compared with (8) in this article, did not take the possible degree of freedom that $\dot{\xi}_{i,j} > 0$, into consideration, resulting in more transmission events between agents. In contrast, our design approach allows a nonmonotonic $\xi_{i,j}$ which slows down the decline of clock variables while providing potentials for $\xi_{i,j}$ to rise, leading to larger inter-event times in general.

IV. Consensus and Inter-Event Analysis

In this section, the consensus result and the existence of strictly positive MIETs is proved.

A. Analysis on Consensus

Theorem 1: Consider the MAS (1) under the OB-AET control protocol (4). If the event-triggering mechanism (8)–(11) are satisfied, the resulting closed-loop system can reach consensus, while the adaptive parameters c_{ij} and $\mu_{i,j}$, $(i,j) \in \mathcal{E}$, ultimately converge to some positive constants.

Proof: For convenience, we first define

$$\begin{cases} \eta_i = x_i - \frac{1}{N}\sum_{j=1}^{N} x_j, \\ \zeta_i = v_i - \frac{1}{N}\sum_{j=1}^{N} v_j, \\ \chi_i = \zeta_i - \eta_i, \end{cases}$$

for $i \in \mathcal{V}$. From (2) and (4), we have

$$\begin{cases} \dot{\eta}_i = A\eta_i + BK\sum_{j\in\mathcal{N}_i}(\hat{v}_{j,i} - \hat{v}_{i,j}), \\ \dot{\zeta}_i = A\zeta_i + BK\sum_{j\in\mathcal{N}_i}(\hat{v}_{j,i} - \hat{v}_{i,j}) + FC\chi_i, \\ \dot{\chi}_i = (A+FC)\chi_i, \end{cases} \tag{12}$$

By the observer design (2) and that $(A+FC)$ is designed to be Hurwitz, it is not difficult to show that

$$||v_i(t) - x_i(t)||^2 \leq \varepsilon_{i,1}e^{-\delta t} \tag{13}$$

for some positive constants $\delta > 0$ and $\varepsilon_{i,1} > 0$. Moreover,

$$||\chi_i||^2 \leq \varepsilon_{i,2}e^{-\delta t} \tag{14}$$

holds for some positive constant $\varepsilon_{i,2} > 0$. Now consider a candidate Lyapunov function as

$$V = V_1 + V_2 + V_3 + V_4, \tag{15}$$

where

$$V_1 = \frac{1}{2}\sum_{i=1}^{N}\zeta_i^{\mathrm{T}}P\zeta_i, \qquad V_2 = \sum_{(i,j)\in\mathcal{E}}\frac{\gamma_{i,j}}{8\kappa_{ij}}\left(c_{ij} - \frac{\alpha}{\gamma_{i,j}}\right)^2,$$

$$V_3 = \frac{1}{2}\sum_{(i,j)\in\mathcal{E}}\xi_{i,j}e_{i,j}^{\mathrm{T}}Pe_{i,j}, \quad V_4 = \sum_{(i,j)\in\mathcal{E}}\frac{1}{4\pi_{i,j}}(\mu_{i,j} - \beta)^2.$$

Constant parameters are designed to satisfy $\alpha > 0$, $\beta > 0$ (will be specified later) and $\gamma_{ij} = 2(\frac{1}{|\mathcal{N}_i|} - \phi_{i,j})$. Since $P > 0$ and $\xi_{i,j} \geq 0$ for all $t \geq 0$, the function V is non-negative, while equals to zero only if all $\eta_i = 0$. Now define the set $\{t_l : l \in \mathbb{N}\}$ as time instants when at least one event is triggered at any edge $(i,j) \in \mathcal{E}$, and it is easy to verify that $V(t_l^-) = V(t_l^+)$ holds at any triggering instant t_l for all $l \in \mathbb{N}$ since $e_{i,j}(t_k^{i,j+}) = 0$ and $\xi_{i,j}(t_k^{i,j-}) = 0$ hold for all $(i,j) \in \mathcal{E}$ and $k \in \mathbb{N}$.

Taking the time derivative of V_1 for $t \in (t_l, t_{l+1})$ along the trajectory of ζ_i in (12) yields

$$\begin{aligned}\dot{V}_1 = &\frac{1}{2}\sum_{i=1}^{N}\zeta_i^{\mathrm{T}}(A^{\mathrm{T}}P + PA)\zeta_i + \sum_{i=1}^{N}\zeta_i^{\mathrm{T}}PFC\chi_i \\ &+ \sum_{(i,j)\in\mathcal{E}}a_{ij}c_{ij}\zeta_i^{\mathrm{T}}\Theta(\hat{v}_{j,i} - \hat{v}_{i,j}),\end{aligned}$$

in which, using $a_{ij} = a_{ji}$, $c_{ij} = c_{ji}$ and $\zeta_i - \zeta_j = (\hat{v}_{i,j} - \hat{v}_{j,i}) - (e_{i,j} - e_{j,i})$ gives

$$\begin{aligned}&\sum_{(i,j)\in\mathcal{E}}a_{ij}c_{ij}\zeta_i^{\mathrm{T}}\Theta(\hat{v}_{j,i} - \hat{v}_{i,j}) \\ &= -\frac{1}{2}\sum_{(i,j)\in\mathcal{E}}a_{ij}c_{ij}(\zeta_i - \zeta_j)^{\mathrm{T}}\Theta(\hat{v}_{i,j} - \hat{v}_{j,i}) \\ &= -\frac{1}{2}\sum_{(i,j)\in\mathcal{E}}a_{ij}c_{ij}||K(\hat{v}_{i,j} - \hat{v}_{j,i})||^2 \\ &\quad + \sum_{(i,j)\in\mathcal{E}}a_{ij}c_{ij}e_{i,j}^{\mathrm{T}}\Theta(\hat{v}_{i,j} - \hat{v}_{j,i}).\end{aligned}$$

In addition, we apply the dynamics of χ_i in (12) to get

$$\begin{aligned}\sum_{i=1}^{N}\zeta_i^{\mathrm{T}}PFC\chi_i &\leq \frac{1}{2}\sum_{i=1}^{N}||\zeta_i||^2 + \frac{1}{2}||PFC||^2\sum_{i=1}^{N}||\chi_i||^2 \\ &\leq \frac{1}{2}\sum_{i=1}^{N}||\zeta_i||^2 + \frac{1}{2}||PFC||^2\sum_{i=1}^{N}\varepsilon_{i,2}e^{-\delta t}\end{aligned}$$

Therefore, $\dot{V}_1$ can be bounded by

$$\begin{aligned}\dot{V}_1 \leq &\frac{1}{2}\sum_{i=1}^{N}\zeta_i^{\mathrm{T}}(A^{\mathrm{T}}P + PA + I_n)\zeta_i + \frac{1}{2}||PFC||^2\sum_{i=1}^{N}\varepsilon_{i,2}e^{-\delta t} \\ &- \frac{1}{2}\sum_{(i,j)\in\mathcal{E}}a_{ij}c_{ij}||K(\hat{v}_{i,j} - \hat{v}_{j,i})||^2, \\ &+ \sum_{(i,j)\in\mathcal{E}}a_{ij}c_{ij}e_{i,j}^{\mathrm{T}}\Theta(\hat{v}_{i,j} - \hat{v}_{j,i}).\end{aligned} \tag{16}$$

Taking the time derivative of V_2 for $t \in (t_l, t_{l+1})$ yields

$$\begin{aligned}\dot{V}_2 = &\sum_{(i,j)\in\mathcal{E}}\frac{\gamma_{ij}a_{ij}c_{ij}}{4}||K(\hat{v}_{i,j} - \hat{v}_{j,i})||^2 \\ &- 2\times\frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}}a_{ij}||K(\hat{v}_{i,j} - \hat{v}_{j,i})||^2.\end{aligned} \tag{17}$$

It follows from $\zeta_i - \zeta_j = (\hat{v}_{i,j} - \hat{v}_{j,i}) - (e_{i,j} - e_{j,i})$ that

$$\frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}}a_{ij}||K(\zeta_i - \zeta_j)||^2$$

$$= \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}||K(\hat{v}_{i,j}-\hat{v}_{j,i})||^2 + \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}||K(e_{i,j}-e_{j,i})||^2 - \frac{\alpha}{4}\sum_{(i,j)\in\mathcal{E}} a_{ij}(e_{i,j}-e_{j,i})^{\mathrm{T}}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i}). \tag{18}$$

In the above, $a_{ij}=a_{ji}$ indicates that

$$\begin{aligned}
&\frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}||K(\zeta_i-\zeta_j)||^2\\
&= \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}\zeta_i^{\mathrm{T}}\Theta(\zeta_i-\zeta_j) - \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}\zeta_j^{\mathrm{T}}\Theta(\zeta_i-\zeta_j)\\
&= \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}\zeta_i^{\mathrm{T}}\Theta(\zeta_i-\zeta_j) + \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ji}\zeta_j^{\mathrm{T}}\Theta(\zeta_j-\zeta_i)\\
&= \frac{\alpha}{4}\sum_{(i,j)\in\mathcal{E}} a_{ij}\zeta_j^{\mathrm{T}}\Theta(\zeta_j-\zeta_i),
\end{aligned} \tag{19}$$

$$\begin{aligned}
&-\frac{\alpha}{4}\sum_{(i,j)\in\mathcal{E}} a_{ij}(\hat{v}_{i,j}-\hat{v}_{j,i})^{\mathrm{T}}\Theta(e_{i,j}-e_{j,i})\\
&= -\frac{\alpha}{4}\sum_{(i,j)\in\mathcal{E}} \left[a_{ij}e_{i,j}^{\mathrm{T}}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i}) - a_{ij}e_{j,i}^{\mathrm{T}}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i})\right]\\
&= -\frac{\alpha}{2}\sum_{(i,j)\in\mathcal{E}} a_{ij}e_{i,j}^{\mathrm{T}}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i}).
\end{aligned} \tag{20}$$

As for the second item in (18), using $a_{ij}=a_{ji}$ gives

$$\begin{aligned}
&\frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}||K(e_{i,j}-e_{j,i})||^2\\
&= \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}(e_{i,j}^{\mathrm{T}}\Theta e_{i,j} - 2e_{i,j}^{\mathrm{T}}\Theta e_{j,i} + e_{j,i}^{\mathrm{T}}\Theta e_{j,i})\\
&\le \frac{\alpha}{4}\sum_{(i,j)\in\mathcal{E}} a_{ij}(e_{i,j}^{\mathrm{T}}\Theta e_{i,j} + e_{j,i}^{\mathrm{T}}\Theta e_{j,i})\\
&= \frac{\alpha}{2}\sum_{(i,j)\in\mathcal{E}} a_{ij}||Ke_{i,j}||^2.
\end{aligned} \tag{21}$$

Combining (17)–(21) yields an upper bound of $\dot{V}_2$ as

$$\begin{aligned}
&\dot{V}_2\\
&\le \frac{1}{4}\sum_{(i,j)\in\mathcal{E}} \gamma_{ij}a_{ij}c_{ij}||K(\hat{v}_{i,j}-\hat{v}_{j,i})||^2\\
&\quad -\frac{\alpha}{4}\sum_{(i,j)\in\mathcal{E}} a_{ij}\zeta_i^{\mathrm{T}}\Theta(\zeta_i-\zeta_j) - \frac{\alpha}{8}\sum_{(i,j)\in\mathcal{E}} a_{ij}||K(\hat{v}_{i,j}-\hat{v}_{j,i})||^2\\
&\quad -\frac{\alpha}{2}\sum_{(i,j)\in\mathcal{E}} a_{ij}e_{i,j}^{\mathrm{T}}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i}) + \frac{\alpha}{2}\sum_{(i,j)\in\mathcal{E}} a_{ij}||Ke_{i,j}||^2.
\end{aligned}$$

Taking the time derivative of V_3 for $t\in(t_l,t_{l+1})$ yields

$$\begin{aligned}
\dot{V}_3 = &\frac{1}{2}\sum_{(i,j)\in\mathcal{E}} \xi_{i,j}e_{i,j}^{\mathrm{T}}(A^{\mathrm{T}}P+PA)e_{i,j} - \sum_{(i,j)\in\mathcal{E}} \xi_{i,j}e_{i,j}^{\mathrm{T}}PBu_i\\
&+\sum_{(i,j)\in\mathcal{E}} \xi_{i,j}e_{i,j}^{\mathrm{T}}PF(Cv_i-y_i) + \frac{1}{2}\sum_{(i,j)\in\mathcal{E}} \dot{\xi}_{i,j}||P^{\frac{1}{2}}e_{i,j}||^2.
\end{aligned}$$

Bounding the third term above by (13) as

$$\begin{aligned}
&\sum_{(i,j)\in\mathcal{E}} \xi_{i,j}e_{i,j}^{\mathrm{T}}PF(Cv_i-y_i)\\
&\le \sum_{(i,j)\in\mathcal{E}} \frac{\epsilon_{i,j}}{2}(\xi_{i,j})^2||P^{\frac{1}{2}}e_{i,j}||^2\\
&\quad + \sum_{(i,j)\in\mathcal{E}} \frac{1}{2\epsilon_{i,j}}||P^{\frac{1}{2}}F||^2||Cv_i-y_i||^2\\
&\le \sum_{(i,j)\in\mathcal{E}} \frac{\epsilon_{i,j}}{2}(\xi_{i,j})^2||P^{\frac{1}{2}}e_{i,j}||^2 + \sum_{i=1}^{N}\varepsilon_{i,3}e^{-\delta t}
\end{aligned}$$

for sufficiently large constants $\varepsilon_{i,3}>0$, $i\in\mathcal{V}$. Recall that $\epsilon_{i,j}>0$ is a given positive parameter for $(i,j)\in\mathcal{E}$. Therefore, $\dot{V}_3$ can be bounded by

$$\begin{aligned}
\dot{V}_3 \le &\frac{1}{2}\sum_{(i,j)\in\mathcal{E}} \dot{\xi}_{i,j}||P^{\frac{1}{2}}e_{i,j}||^2 + \sum_{i=1}^{N}\varepsilon_{i,3}e^{-\delta t}\\
&+\frac{1}{2}\sum_{(i,j)\in\mathcal{E}} \xi_{i,j}e_{i,j}^{\mathrm{T}}(A^{\mathrm{T}}P+PA)e_{i,j}\\
&-\sum_{(i,j)\in\mathcal{E}} \xi_{i,j}e_{i,j}^{\mathrm{T}}PBu_i + \frac{1}{2}\sum_{(i,j)\in\mathcal{E}} \epsilon_{i,j}(\xi_{i,j})^2||P^{\frac{1}{2}}e_{i,j}||^2.
\end{aligned}$$

Moreover, $\dot{V}_4$ for $t\in(t_l,t_{l+1})$ can be calculated as

$$\dot{V}_4 = \sum_{(i,j)\in\mathcal{E}} \frac{\mu_{i,j}-\beta}{2}||Ke_{i,j}||^2.$$

Combine the bounds of $\dot{V}_1$, $\dot{V}_2$, $\dot{V}_3$ and $\dot{V}_4$, together with the relation $\gamma_{i,j}=2(\frac{1}{|\mathcal{N}_i|}-\phi_{i,j})$, we further upper bound $\dot{V}$ as

$$\begin{aligned}
\dot{V} \le &\frac{1}{2}\zeta^{\mathrm{T}}\left[I_N\otimes(A^{\mathrm{T}}P+PA+I_n) - \frac{1}{2}\alpha(\mathcal{L}\otimes\Theta)\right]\zeta\\
&+\sum_{(i,j)\in\mathcal{E}} R_{i,j} + \sum_{(i,j)\in\mathcal{E}} R_{i,j}^{\alpha} + \varepsilon e^{-\delta t},
\end{aligned} \tag{22}$$

where $\zeta=[\zeta_1^{\mathrm{T}},\zeta_2^{\mathrm{T}},\ldots,\zeta_N^{\mathrm{T}}]^{\mathrm{T}}$, $\varepsilon := \sum_{i=1}^{N}(\frac{1}{2}||PFC||^2\varepsilon_{i,2}+\varepsilon_{i,3})>0$, and

$$\begin{aligned}
R_{i,j} = &-\sum_{k\in\mathcal{N}_i} \frac{\phi_{i,k}}{2}a_{ik}c_{ik}||K(\hat{v}_{i,k}-\hat{v}_{k,i})||^2 + \frac{1}{2}\dot{\xi}_{i,j}||P^{\frac{1}{2}}e_{i,j}||^2\\
&+\frac{\xi_{i,j}}{2}e_{i,j}^{\mathrm{T}}(A^{\mathrm{T}}P+PA)e_{i,j} + \frac{\epsilon_{i,j}}{2}||P^{\frac{1}{2}}e_{i,j}||^2\\
&+a_{ij}c_{ij}e_{i,j}^{\mathrm{T}}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i})\\
&-\xi_{i,j}e_{i,j}^{\mathrm{T}}PBu_i + \frac{\mu_{i,j}}{2}||Ke_{i,j}||^2,\\
R_{i,j}^{\alpha} = &-\frac{\alpha}{8}a_{ij}||K(\hat{v}_{i,j}-\hat{v}_{j,i})||^2 - \frac{\beta}{2}||Ke_{i,j}||^2\\
&-\frac{\alpha}{2}a_{ij}e_{i,j}^{\mathrm{T}}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i}) + \frac{\alpha}{2}a_{ij}||Ke_{i,j}||^2.
\end{aligned}$$

Note that $(\mathbf{1}^{\mathrm{T}}\otimes I_n)\eta=0$ and Lemma 1 imply that $-\frac{1}{2}\alpha\zeta^{\mathrm{T}}(\mathcal{L}\otimes\Theta)\zeta \le -\frac{1}{2}\alpha\lambda_2(\mathcal{L})\zeta^{\mathrm{T}}(I_N\otimes\Theta)\zeta$. Moreover, Lemma 1 and Assumption 2 imply that $\lambda_2(\mathcal{L})>0$. Choosing a finite positive constant α such that $\alpha\ge\frac{2}{\lambda_2(\mathcal{L})}$ with the ARE (6) yields

$$\begin{aligned}
&\frac{1}{2}\zeta^{\mathrm{T}}\left[I_N\otimes(A^{\mathrm{T}}P+PA+I_n) - \frac{1}{2}\alpha(\mathcal{L}\otimes\Theta)\right]\zeta\\
&\le \frac{1}{2}\zeta^{\mathrm{T}}[I_N\otimes(A^{\mathrm{T}}P+PA+I_n-PBB^{\mathrm{T}}P)]\zeta = -\frac{1}{2}\|\zeta\|^2,
\end{aligned}$$

which, substituted into (22), gives

$$\dot{V}_1 \le -\frac{1}{2}\|\zeta\|^2 + \sum_{(i,j)\in\mathcal{E}} R_{i,j} + \sum_{(i,j)\in\mathcal{E}} R_{i,j}^{\alpha} + \varepsilon e^{-\delta t}. \tag{23}$$

For $R_{i,j}$, if $||e_{i,j}||=0$, then obviously $R_{i,j}\le 0$ according to its definition. If $||e_{i,j}||\neq 0$, it follows from (9) and the definition of $R_{i,j}$ that

$$R_{i,j}=\frac{1}{2}(\dot{\xi}_{i,j}-f_{i,j})||P^{\frac{1}{2}}e_{i,j}||^2,$$

which, by the clock driving function (8), yields that $R_{i,j}=0$ if $f^{\mathrm{a}}_{i,j}\le\bar{f}$ and $R_{i,j}<0$ otherwise. Overall, we have $R_{i,j}\le 0$ holds for all $t\ge 0$. Moreover, in the definition of $R^{\alpha}_{i,j}$,

$$\begin{aligned}&-\frac{\alpha}{2}a_{ij}e^{\mathrm{T}}_{i,j}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i})\\ \le&\frac{\alpha}{8}a_{ij}||K(\hat{v}_{i,j}-\hat{v}_{j,i})||^2+2\alpha a_{ij}||Ke_{i,j}||^2,\end{aligned}\tag{24}$$

hence that

$$R^{\alpha}_{i,j}\le(\frac{5\alpha}{2}-\frac{\beta}{2})a_{ij}||Ke_{i,j}||^2.\tag{25}$$

Thus, $R^{\alpha}_{i,j}\le 0$, can be guaranteed for a sufficiently large β. Therefore, by using the designed $\dot{\xi}_{i,j}$ in (8) and (9) and choosing a sufficiently large β, we have $R_{i,j}\le 0$ and $R^{\alpha}_{i,j}\le 0$ for all $t\ge 0$. Therefore, it follows from (23) that $\dot{V}_{\mathrm{a}}\le-\frac{1}{2}\|\zeta\|^2+\varepsilon e^{-\delta t}$ for $(i,j)\in\mathcal{E}$ and all $t\in(t_l,t_{l+1})$, $l\in\mathbb{N}$.

As a result, for all $t\ge 0$, we have

$$V(t)\le V(0)+\int_0^t(\varepsilon e^{-\delta\tau})d\tau=V(0)+\frac{\varepsilon(1-e^{-\delta t})}{\delta}.$$

Note that the inequality above together with $V_{\mathrm{a}}(t_l^-)=V_{\mathrm{a}}(t_l^+)$, $l\in\mathbb{N}$, implies the boundness of V_{a} for all $t\ge 0$, which further implies that ζ_i, c_{ij}, $\mu_{i,j}$ and $e_{i,j}$ are all bounded for all $t\ge 0$. Furthermore, we have

$$\begin{aligned}\lim_{t\to\infty}\int_0^t\frac{1}{2}||\zeta(\tau)||^2d\tau\le&\lim_{t\to\infty}\int_0^t\left[\varepsilon e^{-\delta\tau}-\dot{V}(\tau)\right]d\tau\\ \le&\frac{\varepsilon}{\delta}+V(0)-V(\infty)<\infty.\end{aligned}$$

The boundedness of ζ_i, c_{ij}, $\mu_{i,j}$ $e_{i,j}$ and χ_i implies the boundedness of the time-derivative of ζ_i, therefore, $||\zeta||^2$ is uniformly continuous. Then we conclude that $||\zeta||^2$ will eventually converge to zero as $t\to\infty$, or equivalently, $v_1=v_2=\cdots=v_N$. Since (v_i-x_i) also converges to zero exponentially according to (13), consensus is asymptotically reached. The adaptive parameters c_{ij} and $\mu_{i,j}$ will converge to some positive constants as $t\to\infty$ since they have been shown to be bounded and are monotonically non-decreasing as in (5) and (10), respectively. ■

B. Analysis on Strictly Positive Inter-Event Times

Theorem 2: Consider the MAS (1) under the control protocol (4). If the event-triggering mechanism (8)–(11) is satisfied, then $\inf_{(i,j)\in\mathcal{E},k\in\mathbb{N}}\{t^{i,j}_{k+1}-t^{i,j}_k\}\ge\tau$ for some positive constant $\tau>0$, i.e., there exists a strictly positive minimum inter-event time between two consecutive events.

Proof: We first recall the triggering mechanism in (11). The proof is completed by demonstrating the uniform lower bound of $\dot{\xi}_{i,j}$. By the definition of $f_{i,j}$ in (9) and Young's inequality, it is not difficult to show that

$$\begin{aligned}&2a_{ij}c_{ij}e^{\mathrm{T}}_{i,j}\Theta(\hat{v}_{i,j}-\hat{v}_{j,i})-2\xi_{i,j}e^{\mathrm{T}}_{i,j}PBu_i\\ =&2(\xi_{i,j}+1)a_{ij}c_{ij}e^{\mathrm{T}}_{i,j}\Theta(\hat{v}_{i,j}-\hat{x}_{j,i})\\ &+2\xi_{i,j}e^{\mathrm{T}}_{i,j}\Theta\sum_{q\in\mathcal{N}_i\setminus\{j\}}a_{iq}c_{iq}(\hat{v}_{i,q}-\hat{v}_{q,i})\\ \le&\frac{a_{ij}c_{ij}}{\phi_{i,j}}(\xi_{i,j}+1)^2||Ke_{i,j}||^2+\phi_{i,j}a_{ij}c_{ij}||K(\hat{v}_{i,j}-\hat{v}_{j,i})||^2\\ &+\sum_{q\in\mathcal{N}_i\setminus\{j\}}\frac{a_{iq}c_{iq}}{\phi_{i,q}}(\xi_{i,j})^2||Ke_{i,j}||^2\\ &+\sum_{q\in\mathcal{N}_i\setminus\{j\}}\phi_{i,q}a_{iq}c_{iq}||K(\hat{v}_{i,q}-\hat{v}_{q,i})||^2.\end{aligned}\tag{26}$$

Meanwhile, in (9), the ARE (6) implies

$$\xi_{i,j}e^{\mathrm{T}}_{i,j}(A^{\mathrm{T}}P+PA)e_{i,j}\le\xi_{i,j}||Ke_{i,j}||^2.\tag{27}$$

Then, by substituting (26) and (27) into (9), we have

$$\begin{aligned}f_{i,j}\ge-\Big[&\xi_{i,j}+\mu_{i,j}+\frac{a_{ij}c_{ij}}{\phi_{i,j}}(\xi_{i,j}+1)^2\\ &+\sum_{q\in\mathcal{N}_i\setminus j}\frac{a_{iq}c_{iq}}{\phi_{iq}}(\xi_{i,j})^2\Big]\frac{||Ke_{i,j}||^2}{||P^{\frac{1}{2}}e_{i,j}||^2}-\epsilon_{i,j}(\xi_{i,j})^2.\end{aligned}\tag{28}$$

If $||e_{i,j}||\neq 0$, the well-known property for product of matrix norms and Lemma 2 imply that

$$\begin{aligned}\frac{||Ke_{i,j}||^2}{||P^{\frac{1}{2}}e_{i,j}||^2}=&\frac{e^{\mathrm{T}}_{i,j}P^{\frac{1}{2}}P^{-\frac{1}{2}}\Theta P^{-\frac{1}{2}}P^{\frac{1}{2}}e_{i,j}}{||P^{\frac{1}{2}}e_{i,j}||^2}\\ \le&\lambda_{\mathrm{M}}(P^{-\frac{1}{2}}\Theta P^{-\frac{1}{2}})=\lambda_{\mathrm{M}}(P^{-1}\Theta),\end{aligned}$$

which, together with (28), further implies that

$$\begin{aligned}f_{i,j}\ge-\lambda_{\mathrm{M}}(P^{-1}\Theta)\Big[&\xi_{i,j}+\mu_{i,j}+\frac{a_{ij}c_{ij}}{\phi_{i,j}}(\xi_{i,j}+1)^2\\ &+\sum_{q\in\mathcal{N}_i\setminus j}\frac{a_{iq}c_{iq}}{\phi_{iq}}(\xi_{i,j})^2\Big]-\epsilon_{i,j}(\xi_{i,j})^2.\end{aligned}$$

According to (8), if $\|e_{i,j}\|=0$ or $f_{i,j}>\bar{f}$, then $\dot{\xi}_{i,j}=\bar{f}>0$ and $\dot{\xi}_{i,j}=f_{i,j}$ otherwise. Consequently, for $[t^{i,j}_k,t^{i,j}_{k+1})$,

$$\begin{aligned}\dot{\xi}_{i,j}\ge-\lambda_{\mathrm{M}}(P^{-1}\Theta)\Big[&\xi_{i,j}+\mu_{i,j}+\frac{a_{ij}c_{ij}}{\phi_{i,j}}(\xi_{i,j}+1)^2\\ &+\sum_{q\in\mathcal{N}_i\setminus j}\frac{a_{iq}c_{iq}}{\phi_{i,q}}(\xi_{i,j})^2\Big]-\epsilon_{i,j}(\xi_{i,j})^2.\end{aligned}\tag{29}$$

By the comparison lemma [11, Lemma 3.4], we obtain $\xi_{i,j}(t)\ge\varphi_{i,j}(t)$ for $t\in[t^{i,j}_k,t^{i,j}_{k+1})$, where $\varphi_{i,j}(t)$ is the solution to the ODE

$$\begin{aligned}\dot{\varphi}_{i,j}=-\lambda_{\mathrm{M}}(P^{-1}\Theta)\Big[&\varphi_{i,j}+\bar{\mu}_{i,j}+(\varphi_{i,j}+1)^2\frac{a_{ij}\bar{c}_{ij}}{\phi_{i,j}}\\ &+\sum_{q\in\mathcal{N}_i\setminus j}\frac{a_{iq}\bar{c}_{iq}}{\phi_{i,q}}(\varphi_{i,j})^2\Big]-\epsilon_{i,j}(\varphi_{i,j})^2,\end{aligned}$$

where $\varphi_{i,j}(t^{i,j+}_k)=\bar{\xi}_{i,j}$, $\bar{\mu}_{i,j}=\sup_{t\ge 0}\mu_{i,j}(t)$ and $\bar{c}_{ij}=\sup_{t\ge 0}c_{ij}(t)$, $(i,j)\in\mathcal{E}$. It is easy to see that the time it takes for $\varphi_{i,j}$ evolving from $\bar{\xi}_{i,j}$ to 0 can be derived analytically and proved to be strictly larger than zero according to [12].

Therefore, $\tau=\min_{(i,j)\in\mathcal{E}}\{\tau_{i,j}\}$ is a strictly positive lower bound of MIET for the proposed event-triggering mechanism, i.e., $t^{i,j}_{k+1}-t^{i,j}_k\ge\tau$, $(i,j)\in\mathcal{E}$, $k\in\mathbb{N}$. ■

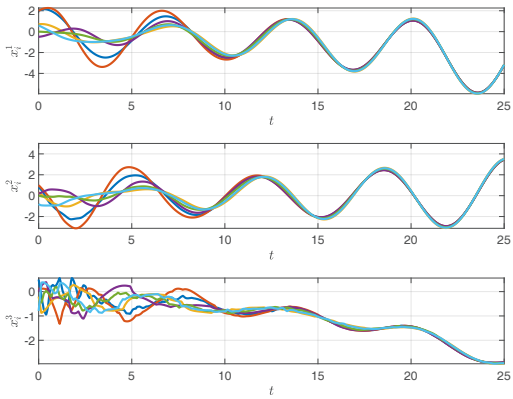


Fig. 1. States of agents

V. Numerical Examples

In this section, we provide a numerical example to verify the effectiveness of our method.

Consider the MAS (1) with 6 agents under a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where the edge set is $\mathcal{E} = \{(1,2),(2,1),(1,4),(4,1),(1,5),(5,1),(3,6),(6,3),(5,6),(6,5)\}$. The system matrices are given by $A = \begin{bmatrix} 0 & 1 & 0.1 \\ -1 & 0.1 & 1 \\ 0 & 0.1 & 0.1 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$. Solving the ARE (6) and (7) to get $K = [-0.357, 2.345, 2.675]$ and $F = [-2.241, -1.863, -1.476]^{\mathrm{T}}$. The initial states of all agents/observers, $c_{ij}(0)$ and $\mu_{i,j}(0)$ are selected randomly under the constraint: $c_{ij}(0) = c_{ji}(0)$, $c_{ij}(0) > 0$ and $\mu_{i,j}(0) > 0$. Set $\bar{\xi}_{i,j} = 5$, $\pi_{i,j} = 1$, $\kappa_{ij} = \kappa_{ji} = 0.1$, $\phi_{i,j} = \frac{1}{2|\mathcal{N}_i|}$, $\bar{f} = 100$, and $\epsilon_{i,j} = 1$. It can be seen from Fig. 1 and Fig. 2 that consensus is reached, while $\mu_{i,j}(t)$ and $c_{ij}(t)$ converge to some positive constants. Fig. 3 shows $\xi_{1,2}$ and the time interval of two consecutive events of edge $(1,2)$, where the cyan filled points denote the time instants when $\xi_{1,2}$ reaches zero, and it is clear that the evolution of $\xi_{1,2}$ is nonmonotonic.

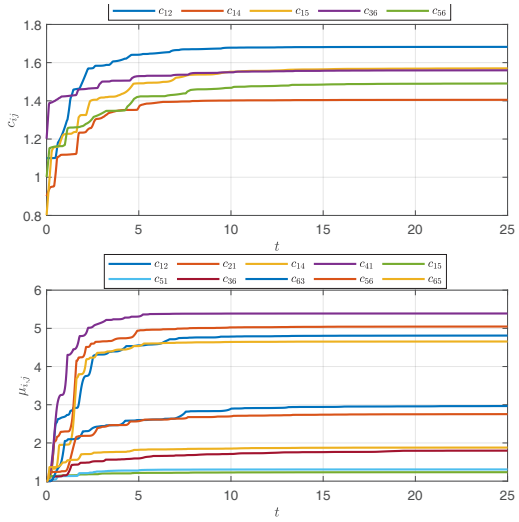


Fig. 2. Evolution of $\mu_{i,j}, c_{ij}$

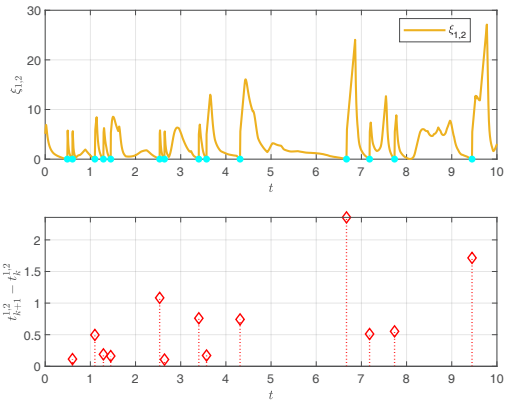


Fig. 3. Clock variable $\xi_{1,2}$ and event intervals of edge $(1,2)$

VI. Conclusion

This paper studies output-feedback consensus problem for linear MASs on undirected graphs. We propose a fully distributed edge-based ET protocol which provides guarantees on strictly positive MIETs. The novel nonmonotonic clock variable is introduced for determining triggering conditions, leading to larger inter-event times. We expect to extend our method to general directed graphs in our future works.

References

[1] C. L. P. Chen, G.-X. Wen, Y.-J. Liu, and Z. Liu, "Observer-based adaptive backstepping consensus tracking control for high-order nonlinear semi-strict-feedback multiagent systems," *IEEE Transactions on Cybernetics*, vol. 46, no. 7, pp. 1591–1601, 2016.

[2] H. Su, M. Z. Q. Chen, X. Wang, and J. Lam, "Semiglobal observer-based leader-following consensus with input saturation," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 6, pp. 2842–2850, 2014.

[3] B. Tian, H. Lu, Z. Zuo, and W. Yang, "Fixed-time leader–follower output feedback consensus for second-order multiagent systems," *IEEE Transactions on Cybernetics*, vol. 49, no. 4, pp. 1545–1550, 2019.

[4] D. V. Dimarogonas and K. H. Johansson, "Event-triggered control for multi-agent systems," in *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, 2009, pp. 7131–7136.

[5] G. S. Seyboth, D. V. Dimarogonas, and K. H. Johansson, "Event-based broadcasting for multi-agent average consensus," *Automatica*, vol. 49, no. 1, pp. 245–252, 2013.

[6] X. Li, Z. Sun, Y. Tang, and H. R. Karimi, "Adaptive event-triggered consensus of multiagent systems on directed graphs," *IEEE Transactions on Automatic Control*, vol. 66, no. 4, pp. 1670–1685, 2021.

[7] W. Xu, W. He, D. W. Ho, and J. Kurths, "Fully distributed observer-based consensus protocol: Adaptive dynamic event-triggered schemes," *Automatica*, vol. 139, p. 110188, 2022.

[8] Y.-Y. Qian and Y. Wan, "Design of distributed adaptive event-triggered consensus control strategies with positive minimum inter-event times," *Automatica*, vol. 133, p. 109837, 2021.

[9] S. Guo and X. Meng, "Fully distributed control of multiagent networks with edge-based event-triggered communication," *IEEE Transactions on Automatic Control*, vol. 68, no. 9, pp. 5630–5637, 2023.

[10] J. Berneburg and C. Nowzari, "Distributed dynamic event-triggered coordination with a designable minimum inter-event time," in *2019 American Control Conference (ACC)*, 2019, pp. 1424–1429.

[11] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.

[12] X. Sun and X. Meng, "A robust control approach to event-triggered networked control systems with time-varying delays," *IEEE Access*, vol. 9, pp. 64 653–64 664, 2021.

基于随流检测的确定性网络混合时敏流量调度技术研究

王圣恺 蔡岳平* 陈晨 韩笑

重庆大学微电子与通信工程学院

摘　要：工业 4.0 和智能工厂的发展对于网络传输的确定性低时延和低抖动提出了更高的要求。为解决大规模确定性网络中事件触发流和时间触发流混合传输的有界时延保证问题，提出了一种面向混合时敏流量的基于随流检测的最早截止时间优先调度技术（IFEDS）。利用随流检测技术实现网络测量和数据包染色。设计了一种基于截止时间的数据包概率染色算法和一种基于染色的半抢占式最早截止时间优先调度算法。最后用 OMNeT++仿真验证了 IFEDS 方案的有效性。结果表明，在高负载情况下 IFEDS 平均端到端时延比 Deadline-TSN 降低了 6.84%。在 ET 占比为 40%的情况下比 Deadline-TSN 减少了 0.37%的丢包率。

关键词：确定性网络；时间敏感网络；调度；随流检测；循环指定排队和转发

Research on hybrid scheduling of time-sensitive flow in deterministic networking based on in-situ flow information telemetry

WANG Sheng-kai, CAI Yue-ping, CHEN Chen, HAN Xiao

School of Microelectronics and Communication Engineering, Chongqing University

Abstract: The development of Industry 4.0 and smart factories places higher demands on deterministic low latency and low jitter for network transmission. To address the issue of hybrid transmission of Event-Triggered (ET) flows and Time-Triggered (TT) flows in Large-scale Deterministic Network. Proposed an Earliest Deadline First Scheduling Based on In-situ Flow Information Telemetry for Hybrid Time-Sensitive Flows (IFEDS). Networking telemetry and packet coloring based on In-situ Flow Information Telemetry. Designed a probabilistic deadline-based packet coloring algorithm and a coloring based semi-preemptive earliest deadline first scheduling algorithm. Simulation based on OMNET++. Results show that the average end-to-end latency of IFEDS under high load is 6.84% lower than Deadline-TSN, and reduce the packet loss rate by 0.37% when the ET flow ratio is 40%.

Key words: Deterministic Network, Time-sensitive Networking, Scheduling, In-situ Flow Information Telemetry,Cyclic Queuing and Forwarding

1　引言

工业 4.0 和智能工厂的发展对工业通信网络提出了保证确定性时延和抖动的挑战。不可预测的时延和抖动限制了工厂的制造能力，甚至可能导致事故发生。因此工厂自动化、运动控制等产业都不再满足于传

*通信作者：蔡岳平 caiyueping@cqu.edu.cn

统分组交换网络通常采用的“尽力而为”（Best Effort，BE）的传输服务[1, 2]，而是开始寻求能提供高服务质量（Quality of Service，QoS）的技术。确定性网络（Deterministic Networking，DetNet）通过控制流量转发、帧复制与消除等方法，提供确定性时延、抖动、丢包率、带宽和可靠性等 QoS 保障，为工业 4.0 提供了“准时、准确”的数据传输能力[3, 4]。

DetNet 的流量调度技术分隔了时敏流量和非时敏流量的带宽资源，保障了时敏流量的可靠性传输。例如循环排队转发（Cyclic Queuing and Forwarding，CQF）[5]及其演进的循环指定排队转发（Cyclic Queuing and Forwarding，CSQF）[6]都利用队列的循环实现了对时间触发（Time-Triggered，TT）时敏流量时延和抖动的确定性控制[7]，确保 TT 流不被低优先级流量阻塞。但如表 1 所示，实际的工业互联网中包含了周期性和非周期性的多种流量。例如在智能变电站中，GOOSE 报文会周期性地测试发送以确保系统的完整性和通信链路的可靠性。但当监测的数据或系统状态发生变化时，比如保护装置检测到故障，GOOSE 报文会被触发并以非周期发送。这是一种事件触发（Event-Triggered，ET）的时敏流量。智能电网是典型的需要低时延、低抖动、低丢包可靠通信的大规模网络。因此忽视 ET 流的调度会极大影响实际场景下流量的确定性传输。

表 1 工业互联网流量分类与 QoS 需求

类型	优先级	周期性	典型周期	流量到达率（包/s）	数据大小（Byte）	流量比例
网络控制（TT）	7	周期	50ms~1s	50	50-500	2%
同步（TT）	6	周期	<2ms	500	30-100	6%
循环（TT）	5	周期	2~20ms	50	50-1000	6%
控制（ET）	4	非周期		50	100-200	5%
警报、命令（ET）	3	非周期		50	100-1500	2%
配置、诊断	2	非周期		50	500-1500	8%
视频	1	周期	帧速率	50-150	1000-1500	15%
音频	1	周期	采样速率	50-150	1000-1500	15%
BE	0	非周期		50-150	30-1500	41%

ET 流的存在对 DetNet 的确定性通信目标带来了挑战。此外，对可预知流量的调度技术计算是 NP 难问题，需要复杂的离线运算，但对于不可预知流量，在线调度则更加困难。在大规模确定性网络（Large-scale Deterministic Network，LDN）中，由于网络规模的扩大和网络拓扑变化，例如设备入网、设备故障等情况，需要研究 ET 和 TT 的混合时敏流量在线调度。

本文的贡献是：

（1）在 LDN 引入随流检测（In-situ Flow Information Telemetry，IFIT）以监测网络状态与数据包信息。

（2）设计了一种基于截止时间的数据包概率染色算法。

（3）设计了一种基于染色的半抢占式最早截止时间优先（Earliest Deadline First，EDF）调度算法。

所提出的方案称之为随流最早截止时间调度（In-situ Flow Earliest Deadline Scheduling，IFEDS）。

本文的其余部分组织如下。第二部分介绍了相关工作，第三部分介绍了 IFEDS 的方案设计。第四部分通过 OMNeT++仿真评估了提出的方案并做出分析。最后，第五部分总结了本文。

2　相关工作

提供确定的低时延和时延抖动是 DetNet 的主要目标之一，实现这一目标的核心原则是流在每个节点的抖动是确定的，不能因跳数的增加而累积。微突发是抖动累积的直接原因，现象主要发生在多个输入端口同时到达的数据包需要被同一输出端口发送的情况。

CSQF[8]可以根据时间单位进行资源预留，从而规划流量，减少微突发的发生。其核心是引入了周期调度和显式路由的概念，利用控制器计算整个网络的流量状态。控制器为每个流计算一条满足时延需求的路径，以及流在每个路径节点的发送时间。通过配置分段路由扩展头（Segment Routing Header，SRH）安排好路径、各节点的调度周期和发送时间，从而实现确定性时延。文献[9]针对 TT 流量实现了 CSQF 的全网调度。文献[10]提出了基于可用队列信息的大规模网络演算路径规划方法，文献[11]提出了一种基于称为 PB-HOA 的路径手册的启发式在线算法，该算法预先计算路径，并在路径级别使用流速率的指标来选择路由。然而，上述研究大多聚焦于对 TT 流的调度，对 ET 流的研究较少，不能解决 ET 流带来的微突发问题。

文献[12]针对车载通信系统提出了一种名为 EDSched 的流量管理方案，以 IEEE 802.1Q-2018 标准中定义的机制为基础，实现了对事件驱动实时流的明确支持。文献[13]提出了 Deadline-TSN（D-TSN）机制，在 TSN 中引入了基于 EDF 的在线调度，为事件驱动的实时流量提供支持，能够统一处理实时周期性和事件驱动的流量。然而，上述研究都没有将应用场景扩展到 LDN 中。

当需要在 LDN 中调度 TT 和 ET 的混合时敏流量时，如图 1(a)所示，当 ET 流数据包和 TT 流数据包同时到达，且安排其在同一周期内输出，会导致该周期后续所有数据包被延迟，可能会进一步导致有 TT 数据包无法在调度安排的时隙内被转发，打乱调度，若后续节点出现同样的现象，这样的抖动会随跳数增多而累积，且在此之后到达的其他 TT 包均会受此影响。如图 1(b)所示，当 ET 流数据包和 TT 流数据包同时到达，且安排 ET 流缓存一周期再输出，则这一过程在每一跳内都会导致 ET 数据包被时延一个循环周期 T_C，该 ET 数据包很可能因为无法满足端到端（End to End，E2E）截止时间要求而被丢弃。由此可见，ET 流带来的不确定性会随着网络规模的增大而累积。

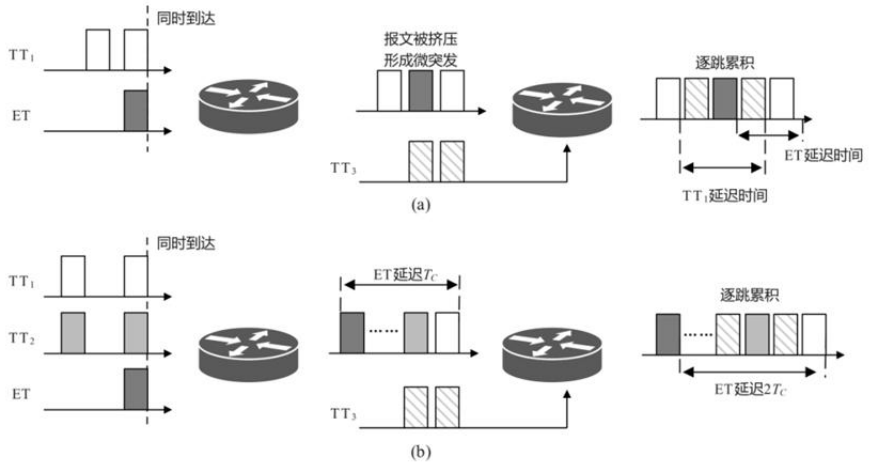


图 1 ET 流传输的微突发问题

3 方案设计

IFEDS 包含三个部分，分别是 IFIT 报文头扩展、基于截止时间的数据包概率染色算法以及基于染色的半抢占式 EDF 调度算法。总体架构如图 2 所示。

CSQF 工作在三层网络，不再使用门控队列来管理队列、调度流量。因此为实现流量调度，需要对不同流进行区分，此外在线调度还需实时监测网络信息。我们提出使用基于 IFIT 的染色技术用以标记流量。

IFIT 是一种随流检测技术，可以通过在真实数据包中插入 IFIT 数据包头对数据包进行标记或在数据包中嵌入检测信息实现带内检测[14]。并且 IFIT 可以直接测量到具体流量的时延、丢包、抖动等指性能，并上报给控制器，无需外部监控设备即可实现实时、准确的数据收集和分析。这种方法大大提高了网络管理的粒度和响应速度，有利于快速发现和解决问题，并支持基于实时流状况的动态网络优化。

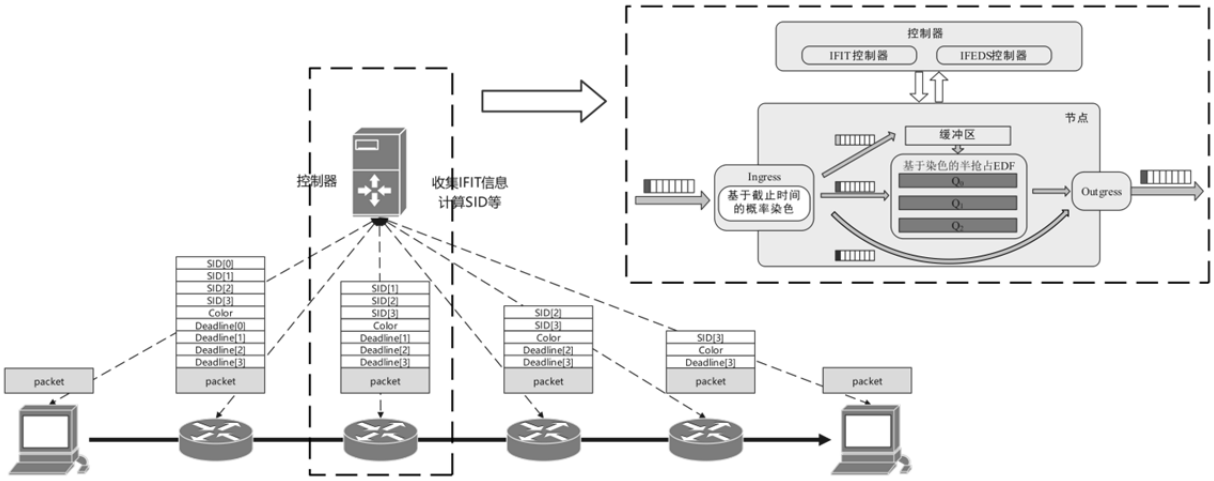


图 2 IFEDS 整体架构

3.1　IFIT 报文头扩展

可扩展性是构建大规模确定性网络的关键性能要求之一。分段路由（Segment Routing，SR）技术支持利用 SRH 承载的信息实现网络编程，满足定制化的业务需求。CSQF 利用 SRH 的段标识符（Segment Identifier，SID）维护流量每一跳的转发路径和出端口时间。为专注于调度技术的研究，我们在源节点采用了基于 Dijkstra 的最短路径算法规划流量的传输路径，同样写入 SR 头部。IFIT 能够在不同的网络规模和复杂度中实现对实际业务数据的实时监控和分析。它同样利用 SRH 封装其头部，标识诸如数据包长度、流指令头、流指令扩展头等信息。IFEDS 将 IFIT 和 CSQF 相结合。因此，IFEDS 也可以在 IFIT 的基础上实现进一步扩展。

每个数据包的染色信息和各节点的截止时间信息将被存储到 SRH 中 IFIT 头的染色相关扩展位内，如图 3 所示。Color 段表示当前数据包的染色信息。Time slot 段用于收集各个节点各队列的时隙利用情况，利用这一信息在前序节点获知后续节点的信息，以便制定调度方案。Deadline 保存了当前数据包在每个路径节点上的截止时间要求。

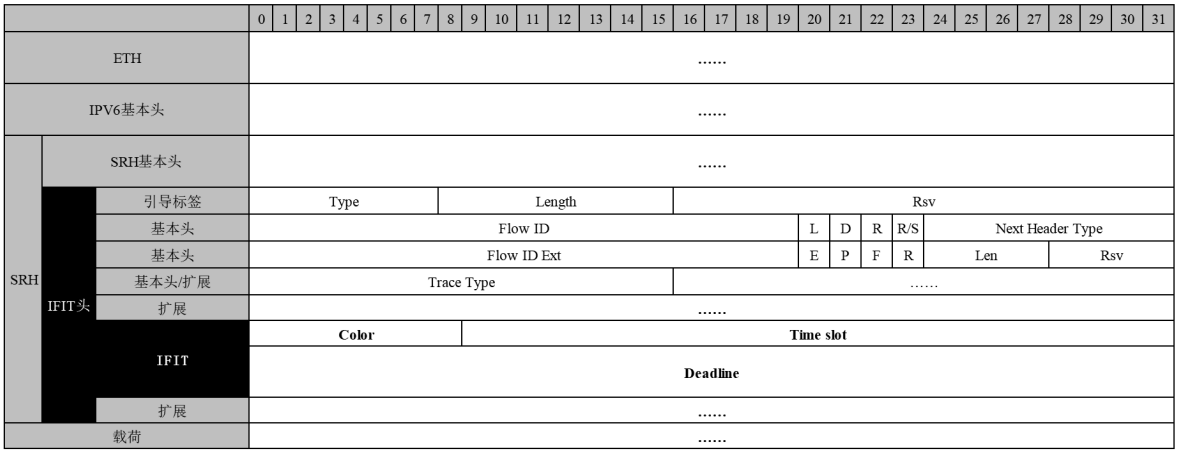


图 3 SRH 封装结构示意图

基于对 SR 和 IFIT 扩展，我们定义流量的集合为 F，对于任意的流 f_i，可以表示为：

$$\begin{aligned} &\forall f_i \in F, i \in \{1,2,\cdots,k\} \\ &f_i = \{C, v_s, v_d, T, S, N, D\} \end{aligned} \tag{1}$$

其中，C 表示数据包的颜色；s_v、s_d 分别为流的源节点和目的节点。T 表示流的生成周期，若该流为 ET 流，则置 0。S 是该流路径信息的集合，N 是该流量到每个节点时所经历的周期数的集合，D 是该流量到每个路径节点的截止时间集合，单位为 μs。例如，若 f_i={1, 3, 40, {(1, 2, 3}, {0, 1, 4}, {50, 100, 200}}，说明该流从节点 1 被发送；目的节点是节点 3；该流每 40 μs 生成一次；所经过的路径是节点 1→节点 2→节点 3；在 1 个 T_c 周期内到达节点 2，在第 4 个周期内到达节点 3，在节点 1、2、3 内的截止时间分别为 50 μs、100 μs 和 200 μs。

3.2 基于截止时间的数据包概率染色算法

基于 IFIT 技术，我们可以对数据包染色。且因为染色标记是随流的，所以可以被保留到后续节点被继续使用，而非仅在当前交换机内有意义。

相较于只调度 TT 流的系统，包含 ET 流的混合时敏流量在到达时存在一定的不确定性。传统的严格时间划分的染色算法虽然简单易于部署，但灵活性较低，并不能很好保证时间边界附近到达的数据包的调度。因此基于这一点我们考虑了令 DetNet 流量在排队前会基于截止时间进行概率染色。

如图 4 所示，t_0 是一个周期的开始时间，t_d 表示该数据包在该节点的截止时间。t_1 到 t_5 是从周期开始到截止这一时段内时间的六等分点，以便兼容传统优先级配置。t_f 表示最晚可接受的数据包到达时间。

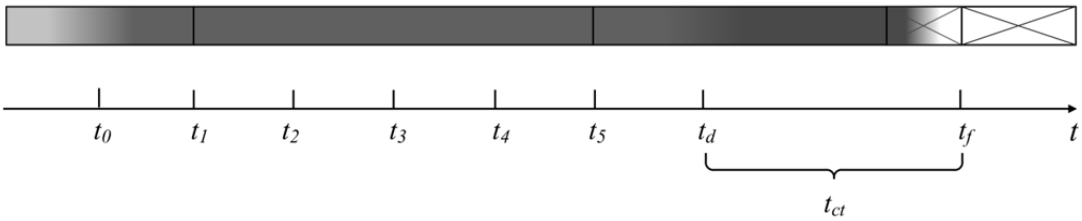


图 4 基于截止时间的数据包概率染色算法

其中 t_d 到 t_f 的时段我们称其为可直通期，用变量 t_{ct} 描述，其定义如下：

$$t_{ct} = D^n{}_i - (\sum_{n}^{k} D_l) \tag{2}$$

其中 $D^n{}_i$ 表示数据包 i 在节点 n 处的剩余截止时间，n 为当前节点号，k 表示目的节点号。该公式表示 t_{ct} 等于数据包的剩余截止时间减去从该节点到数据包的目的节点之间所有链路时延的和。对上式的解释为：对于一个被染色为红色的数据包来说，如果其后续节点都不再将其缓存并排队，而是能将其直通转发，则从染色的这一节点起到目的节点的这段传输路径的总时延就等于这段路径上每跳链路时延的和。

具体的染色方案如下：

- 在 t_1 之前到达的数据包：按照概率 P_g 染为绿色，其余染为黄色。

$$P_g = \frac{2t_1}{2t_1 - t} - 1 \tag{3}$$

- 在 t_1 到 t_5 之间到达的数据包染为绿色，且根据其具体的剩余截止时间对数据包做出标记，例如果一数据包被标记为 f_{g2}，说明其被染为绿色，且在时段 t_2 到 t_3 内到达。
- t_5 到 $1/2t_{ct}$ 之间到达的数据包：按照概率 P_r 染为红色，其余染为绿色。

$$P_r = \frac{t - t_5}{t_d + \frac{1}{2}t_{ct} - t_5} \tag{4}$$

- 到达时间晚于 $1/2t_{ct}$ 但早于 t_f 的数据包按照概率 P_d 丢弃，未丢弃的染为红色。

$$P_d = \frac{t-(t_d+\frac{1}{2}t_{ct})}{t_f-(t_d+\frac{1}{2}t_{ct})} \tag{5}$$

- 晚于 t_f 到达则直接被丢弃。

算法 1 是上述染色算法的伪代码。染色在实质上将所有数据包分为了 8 个优先级，其中红色数据包优先级最高，黄色数据包优先级最低，绿色数据包按照其到截止时间的距离排序，离截止时间越近的数据包优先级越高。

算法所有操作均在循环内部执行，因此总的时间复杂度主要由循环决定。其他操作（包括条件判断和集合操作）都是常数时间操作 O(1)。因此算法总的时间复杂度为 O(|F|)，其中|F|表示流集合大小。算法的空间复杂度则主要取决于 F_{buf}、F_{sch} 和 F_{ct} 这三个集合的大小。在最坏情况下，这三个集合可能会包含所有输入的流，因此算法的空间复杂度同样是 O(|F|)。

算法的计算开销在不同网络规模下主要受流集合大小|F|的影响。在小规模网络中流的数量往往较少，因此计算开销较低。并随着网络规模的增大，时间和空间开销也随之增加。但由于该算法具有线性的时间复杂度，其计算开销随着网络规模的增大仅线性增长，因此在大规模网络中的应用是合理且可行的。这种线性增长模式不仅在计算时间上更具优势，而且更容易扩展，适合在实际的大规模网络环境中应用。

算法 1：基于截止时间的数据包概率染色算法

输入：流集合 F;
　　当前时间 t
输出：缓存流集合 F_{buf};
　　调度流集合 F_{sch};
　　直通流集合 F_{ct}

```
for f_i ∈ F
  if t ≤ t_1
    if P_g > 0.5
      f_i.C ← green
      F_temp ← f_i
    else
      f_i.C ← yellow
      F_buf.F ← f_i
      F_buf.T ← t
  else if t_1 < t ≤ t_5
    f_i.C ← green
    F_temp ← f_i
  else if t_5 < t ≤ (t_5+0.5t_ct)
    if P_r > 0.5
```

```
        f_i.C ← red
        F_ct ← f_i
      else
        f_i.C ← green
        F_temp ← f_i
    else if (t_5+0.5t_ct) < t ≤ (t_5+0.5t_ct)
      if P_d > 0.5
        drop ← f_i
      else
        f_i.C ← red
        F_ct ← f_i
    else
      drop ← f_i
  return F_buf, F_sch, F_ct
```

3.3 基于染色的半抢占式 EDF 调度算法

生成流量的源节点内。首先需要将 ET 数据包周期化，这是为了能以一个确定的粒度规划调度。例如，若系统中可能存在 n 种 ET 流，其最坏可容忍端到端时延分别是 D_1、D_2、⋯、D_n。路径有 m 跳，第 i 跳的链路时延共计 D_{li} ，则每跳的最坏可容忍处理时延即 ET 周期为：

$$T_e = \frac{\min(D_1, D_2, \cdots, D_n) - \sum_{1}^{m} D_{li}}{m} \tag{6}$$

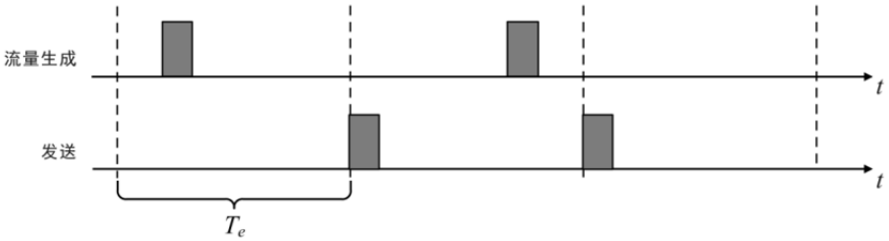


图 5 基于截止时间周期化 ET 数据包

如图 5 所示，这样就完成了 ET 流的周期化处理，可以将任意 ET 流其看做以 T_e 为生成周期的 TT 流进行调度计算。

在交换机节点内，针对不同染色的流量，我们对其使用不同的调度方案。

- 红色数据包将被直通转发，这将显著缩短其到达目的节点的时延。尽管数据包可能已经错过了在某个中间节点的截止时间，但仍有可能在最终的绝对截止时间前到达目的节点。不过，在数据包被染色并进行直通转发之前，需要先评估后续路径上交换机的可用时隙，确保能够发送该数据包。这一过程需要借助 IFIT 机制来获取后续节点的队列状态。

- 黄色数据包将在到达节点时被缓存一个周期（T_C）并被更新为绿色。因为其到达时间早于 t_0，所以即使等待一个 T_C，数据包也不会在 t_d 之后被调度发送。
- 绿色数据包将根据染色标记进行调度。距离截止时间越近的数据包将获得越高的优先级，实现 EDF 调度。

但要注意的是，传统抢占式 EDF 要求调度的任务相互无关、无次序约束，且所有任务均可抢占。但在 DetNet 中，不同时敏流量的重要性并不相同，因此在传统 EDF 算法的基础上，还需要额外考虑到信息的重要性，这往往由流量的优先级表征，如表 1 所示。另外对于同一染色标记的流量，流的到达时间同样需要被考虑，否则会导致调度冲突以及抖动的大幅增加。因此，将流量的优先级和到达时间纳入考虑，调度顺序可以综合为式(7)所示，我们将这种 EDF 称为基于染色的半抢占式 EDF 调度。

$$\text{调度顺序} = \frac{\text{优先级}}{\text{染色标记} \times \text{到达顺序}} \tag{7}$$

图 6 展示了基于染色的半抢占式 EDF 调度算法流程图。在该算法中，新到的流按染色标记和到达顺序插入队列，优先处理截止时间最早的数据包，这一过程不发生抢占，类似于非抢占式 EDF 算法。如果处理某流量时，又有新流量到来，则比较两者染色标记。若新流截止时间更早，再根据双方的优先级进行比较，决定是否抢占。若新流优先级更高，则发生抢占；否则排队等待，这与传统抢占式 EDF 的即刻抢占不同。

图 7 是一个使用 IFEDS 方案进行流量调度的实例，且将 IFEDS 与固定优先级的调度方案做出对比。案例展示了一个节点接收到 6 个 TT 数据包和 2 个 ET 数据包的情况，其中 TT0 到达时晚于其在这一节点的截止时间。

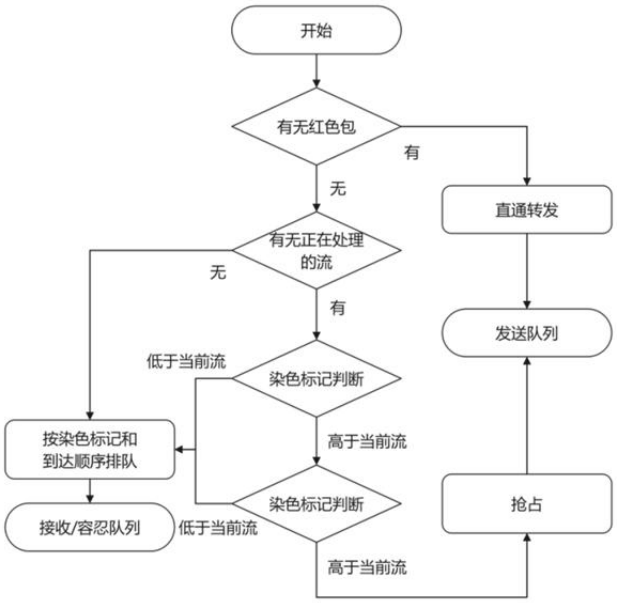


图 6 基于染色的半抢占式 EDF 算法流程图

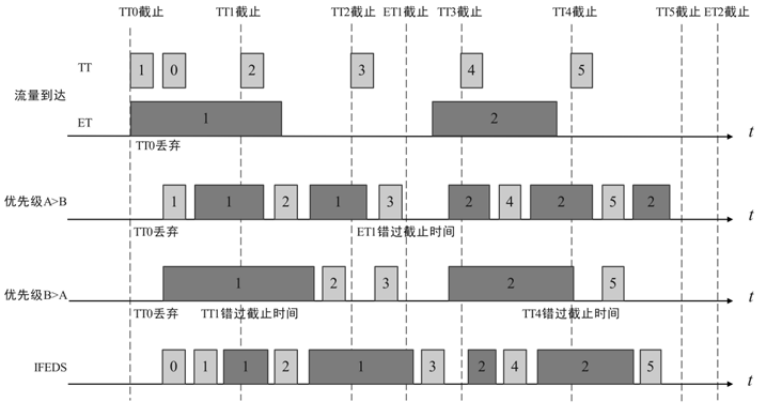


图 7 IFEDS 调度示例

在这个案例中，数据包 TT0 在本应因无法在截止时间到达之前完成传输而被直接丢弃，但由于 IFEDS 的染色与调度技术，在判断其可以直通转发后将其染为红色，并直接转发。而其他数据包按照原定计划到达，染为绿色。但此时因流量汇聚产生了微突发，流量强度已经接近交换机负载，不论 A 与 B 哪种流量的优先级更高，按照固定优先级的传统方法排队时都会存在因错过截止时间而被丢弃的情况。但使用 IFEDS，则可以实现所有数据包都在截止时间前完成转发。

与传统的基于优先级的调度方案不同的是，传统调度方法对同一优先级流量的处理是相同的，而染色能对每个数据包实现差异化的调度。特别是针对优先级相同但截止时间不同的多种流量时，优先级调度策略是一致的，而 IFEDS 调度策略是不同的。且因为染色是仅针对时敏流量的，因此在同样确保非时敏流不影响时敏流的前提下，染色为时敏流提供了更细致的分类方法，且颜色是可以随流在路径节点中根据实际情况改变。

此外，IFEDS 还有着良好的网络兼容性。在当前的网络设备中直接实现数据包的染色和相应的调度策略是非常困难的，因为需要依托于支持 IFIT 功能的交换机和路由器等硬件设备。因此硬件的升级或定制是必要的。但不支持 IFEDS 的设备可以将 IFEDS 流透明传输，即在不支持 IFIT 的节点处仍使用传统调度方案，不对染色信息进行处理。这样虽然会损失一定的性能，但确保了对大规模网络的适用性。使得网络设备可以逐渐升级替换，降低了部署成本。

4 评估

4.1 最坏端到端时延评估

在 IFEDS 中，对于采用存储转发模式传输的数据包，只有当数据包处于正确的周期时间内时才会被写入传输队列。因此黄色数据包会先被缓存等待 T_C。下式中 b_i 表示数据包需要被缓存的时间。

$$b_i = \begin{cases} T_c, & f_i.C = yellow \\ 0, & f_i.C = green \end{cases} \tag{8}$$

对任意非红色包，其端到端时延 W_i 数据包从源节点生成到传送到目的节点所需的时间，可以由下式计算得到：

$$W_i = b_i + num(f_i.S)\cdot(D_t + Q_i) + \sum_{j=0}^{num(f_i.S)}(f_i.N_j - f_i.N_{j-1})\cdot T_C \tag{9}$$

其中 D_t 表示数据包的传输时延，Q_i 表示排队时延，这与数据包在染色时标记的时段编号有关。上式的第二项表示数据包在传输路径中每个节点排队和发送时延的和。第三项表示数据包所在队列由接收转换为发送所需经历的周期时间。

对于数据包的最坏端到端时延，由于红色数据包在截止时间前都有可能通过紧急直通转发的方式到达目的节点。因此任意可调度数据包的最坏端到端时延等于数据包的截止时间。这是由具体业务需求定义的。

4.2 仿真评估

为评估提出的机制的性能，我们选择将 IFEDS 与 CSQF[8]、D-TSN[10]方案相对比，比较它们的的时延抖动丢包率等指标。我们基于 OMNeT++仿真平台[15]和开源框架 NeSting[16]，构建了生成确定性流量并部署调度方案的验证环境。首先使用严格时间划分染色和概率染色分别进行仿真，将得到的结果中时延抖动丢包表现好的一部分数据作为训练集，训练完成决策树的构建。

4.2.1 构建仿真模型

1) 网络模型

仿真网络模型是基于现实的 NSFNet 拓扑构建的真实结构，包含了 14 个节点和 21 个链路，如图 8 所示，图中的单位为 μ s。这些节点是全双工的，并有多个输入输出端口。节点之间的连接全部为全双工链路，由两条单向链路组成。链路以固定数据速率传输数据。每台交换机都部署了流量调度和整形方案，以实现对流的控制。同时，利用 IFIT 对节点和路径状态进行测量、监控和感知，用于规划调度方案。该仿真框架将验证真实拓扑结构下各机制的的确定性流量调度性能。网络资源包括链路带宽、队列长度、T_C 大小等。链路带宽设置为 1 Gbps，将每个队列的长度设置为 10，并且 T_C 大小为 125 μ s。

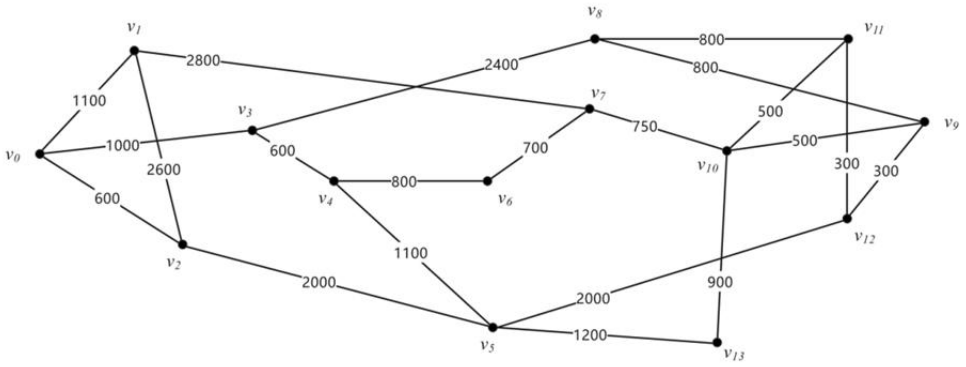


图 8 基于 NSFNet 的网络拓扑结构

2) 流量模型

按照表 1 中工业场景下流量分类及 QoS 要求设置流量的产生。按照公式(3)定义流量携带的信息。通过调整到达率模拟工业场景下产生流量，并在规定范围内随机生成数据包大小。对于每个流，源节点和目标节点都是从所有顶点集中随机选取而创建的。

4.2.1 仿真结果与分析

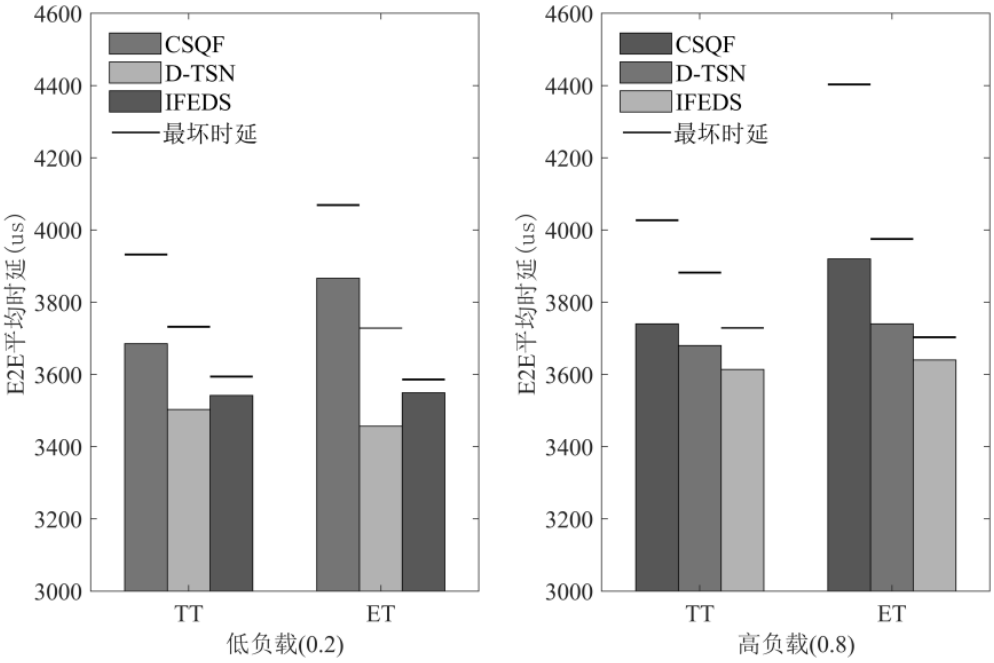


图 9 端到端平均时延和最坏时延比较

图 9 显示了 CSQF、D-TSN、和 IFEDS 机制分别在低负载（0.2）和高负载（0.8）情况下的 TT 流和 ET 流的平均端到端时延性能。可以观察到，DTSN 和 IFEDS 都能以相对一致的性能处理 TT 流和 ET 流，而 CSQF 则对 ET 流支持较差。低负载情况，D-TSN 能提供最小的端到端平均时延，但最坏时延要大于 IFEDS。这是因为 D-TSN 仅在源节点将截止时间映射到优先级，这减少了中间节点的处理时间，而 IFEDS 可随流动态调整。在高负载情况下，IFEDS 表现出了最好的平均时延和最坏时延，IFEDS 技术对 ET 包的 E2E 平均时延相较于传统 CSQF 降低了 7.14%，最大 E2E 时延相较于 D-TSN 降低了 6.84%。这是因为 IFEDS 能处理相当一部分晚于截止时间到达的数据包，这在高负载情况下保障确定性传输是更有利的。

图 10 显示了在固定 ET 帧占比为 20%，不同网络负载下 CSQF、D-TSN 和 IFEDS 的 TT 流抖动变化趋势。结果表明，随着网路负载的增加，三种机制的 TT 流抖动均逐渐增加。这是因为随着流数目的增加，会造成流排队的延迟增加。其中 CSQF 的抖动增加最为显著，这是因为随负载增加会导致微突发出现的频率增加，并导致抖动的累积。D-TSN 和 IFEDS 均能抑制抖动的增加，但 IFEDS 动态的染色机制带来了更好的灵活性，而 D-TSN 需要根据网络和流量的特性调整流门和周期的参数，若选取不当，则会推迟数据包的发送。

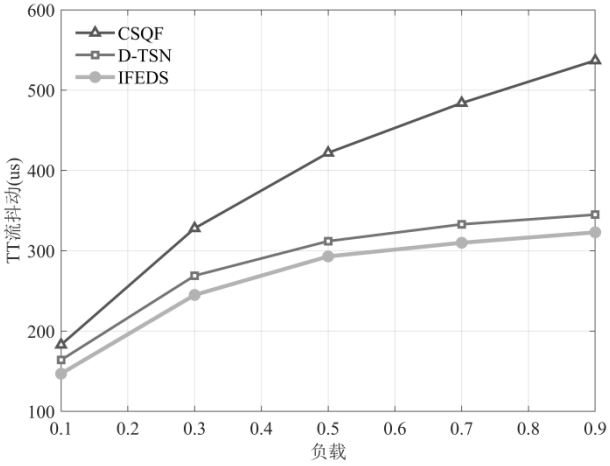


图 10 TT 流抖动表现

图 11 给出了固定负载为 0.6，在不同的 ET 数据包占比情况下，三种机制的丢包率对比。可以看到不论 ET 数据包占比，IFEDS 都能表现出最低的的丢包率。这是由 IFEDS 的紧急数据包直通转发机制实现的，这一机制令原本应被丢弃的数据包有了传输的机会。在 ET 数据包占比为 40%的情况下，IFEDS 的丢包率比 CSQF 降低了 1.26%，比 D-TSN 降低了 0.37%。

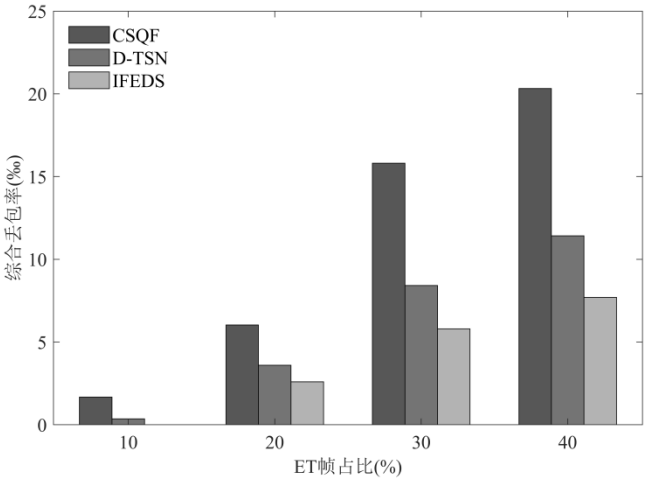


图 11 随 ET 数据包增多，各机制丢包率对比

5 结束语

本文提出了一种面向大规模确定性网络的新型流量调度技术——随流最早截止时间调度，以应对工业4.0和智能工厂对非周期的事件触发流量的确定性传输需求。该方案通过引入基于随流检测和最早截止时间优先技术，有效改善了传统方法在处理混合时敏流量时遇到的时延和抖动问题。通过OMNeT++仿真验证了IFEDS方案的有效性，结果表明该方案能够在高负载情况下最大E2E平均时延相较于CSQF降低了7.14%，最大E2E时延相较于D-TSN降低了6.84%。在ET数据包占比为40%的情况下，比CSQF的丢包率降低了1.26%，比D-TSN降低了0.37%。证明该机制在不同网络条件和流量模式下保持较低的时延和抖动，显著提高了网络的服务质量。

尽管IFEDS展示了在混合时敏流量调度场景中有效的网络状态监测与调度能力，但在实际应用中，随着网络规模的进一步扩大和流量类型的多样化，如何在保持高效性能的同时确保IFEDS的可扩展性和适应性仍需深入研究。特别是在超大规模网络中，数据包的数量和种类大幅增加，将对现有的染色和调度算法的性能产生影响。基于机器学习或自适应控制的增强方法值得进一步探索。另外，IFIT收集的网络状态信息是瞬态的，因此当网络快速变化时，并不能保证据此计算的策略满足流量通过时的要求。决策过程中需要考虑测量信息和当前状态的权衡。可以引入联合路由调度或增量调度等方案以便灵活调整策略。

参考文献：

[1] 蔡岳平, 姚宗辰, 李天驰. 时间敏感网络标准与研究综述[J]. 计算机学报, 2021, 44(07): 1378-1397.

[2] 黄韬, 汪硕, 黄玉栋, 等. 确定性网络研究综述[J]. 通信学报, 2019, 40(06): 160-176.

[3] ADDANKI V, Iannone L. Moving a step forward in the quest for Deterministic Networks (DetNet)[C]. 2020 IFIP Networking Conference (Networking), 2020, Paris, France: 458-466.

[4] MISEREZ J, SHARMA G P, TAVERNIER W. Routing protocols exploiting queue information for deterministic networks[C]. 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), 2023, Vilanova i la Geltru, Spain: 1-8.

[5] IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks – Amendment 29: Cyclic Queuing and Forwarding[S]. IEEE std. IEEE 802.1Qch-2017, 2017: 1-30.

[6] HUANG Y, WANG S, FENG T, et al. Towards Network-Wide Scheduling for Cyclic Traffic in IP-based Deterministic Networks[C]. 2021 4th International Conference on Hot Information-Centric Networking (HotICN), 2021, Nanjing, China: 117-122.

[7] WANG X, Yao, H, Mai T, et al. Joint Routing and Scheduling With Cyclic Queuing and Forwarding for Time-Sensitive Networks[C]. IEEE Transactions on Vehicular Technology, 2022, 72(3): 3793-3804.

[8] IETF. Segment routing (SR) based bounded latency[S/OL]. May 2019.

[9] HUANG Y, WANG S, PENG G. Traffic Shaping at the Edge: Enabling Bounded Latency for Large-scale Deterministic Networks[C]. 2021 IEEE International Conference on Communications Workshops (ICC Workshops), 2021, Montreal, QC, Canada: 1-6.

[10] MISEREZ J, SHARMA G P, TAVERNIER W. Routing protocols exploiting queue information for deterministic networks[C]. 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), 2023, Vilanova i la Geltru, Spain:1-8.

[11] WANG M, ZHU S, ZHANG Y. A Heuristic Online Algorithm for Routing in Large-Scale Deterministic Networks[C]. 2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS), 2023, Sejong, Korea: 189-194.

[12] BELLO L L, PATTI G, VASTA G. Assessments of real-time communications over TSN automotive networks[J]. Electronics, 2021, 10(5): 556.

[13] PATTI G, BELLO L L, LEONARDI L. Deadline-Aware Online Scheduling of TSN Flows for Automotive Applications[J]. 2023, IEEE Transactions on Industrial Informatics, 19(4):5774-5784.

[14] 华为技术有限公司. IFIT 技术白皮书[R]. 深圳: 华为技术有限公司, 2021.

[15] ADDANKI V, Iannone L. Moving a step forward in the quest for Deterministic Networks (DetNet)[C]. 2020 IFIP Networking Conference (Networking), 2020, Paris, France: 458-466.

[16] FAKL J, HELLMANNS D, CARABELLI B, et al. Nesting: Simulating ieee time-sensitive networking (tsn) in omnet++[C] International Conference on Networked Systems (NetSys). 2019, Munich, Germany: 1-8.

[作者简介]

王圣恺（1999_ ），男，硕士生，重庆大学微电子与通信工程学院在读，主要研究方向为时间敏感网络。

蔡岳平（1980_ ），男，博士，重庆大学微电子与通信工程学院副教授，主要研究方向为工业互联网、确定性网络、5G/6G 网络、数据中心网络、算力网络等。

陈晨（1988_ ），男，博士，重庆大学微电子与通信工程学院研究员，主要研究方向为面向 6G 和物联网的智能无线光通信技术。

韩笑（2001_ ），男，硕士生，重庆大学微电子与通信工程学院在读，主要研究方向为时间敏感网络。

YOLO_LSK: A Sintered Surface Defect Detection Model Based on Large Selective Kernel Network

YANG Yi[1,2], CEN Hanyu[1], CHEN Tengtuo[1,*],LI Yanjing[1],WANG Minghao[1]

***Abstract*—In the steel metallurgy industry, with the advancement of digitalization, networking, and intelligence, a large amount of image data from the sintering process remains underutilized. This paper proposes a sintering surface defect detection model, YOLO_LSK, based on a large selective kernel network (LSK), which utilizes computer vision technology for real-time detection of surface defects. The model uses an improved YOLOv7 for defect detection, incorporating the LSK feature extraction module to dynamically adjust the receptive field, allowing for the accurate identification of both moderately severe and severe cracks. With the iteration of training epochs, the recognition accuracy for these two types of cracks reached 100%, and the model's mAP achieved 63.17%. This study constructed a dataset of 1,000 real sintering process images, and through manual annotation and expert experience, established a qualitative and quantitative defect evaluation model to ensure the accuracy and reliability of the detection results. Experimental results show that the YOLO_LSK model excels in real-time crack length and direction identification, significantly improving the quality and efficiency of steel production.** ***Keywords*—Sintered Surface Defect Detection, Large Selective Kernel Network (LSK), YOLO_LSK, Computer Vision**

I. INTRODUCTION

With the rapid development of technologies such as 5G, artificial intelligence, and big data, a new wave of technological revolution is sweeping across the globe. As the foundational industry of the real economy, industrial manufacturing is undergoing profound transformation. In this context, General Electric first introduced the concept of the Industrial Internet[1], which integrates industrial, informational, network, and human-machine interaction technologies centered around industrial systems. The industrial manufacturing sector leverages intelligent means within the Industrial Internet to monitor production processes in real-time, using physical sensors at various stages to track production status and collect data, thereby enabling timely detection and management of system anomalies.

The steel metallurgy industry is a typical example of traditional process industries, where the iron ore sintering process is a crucial preparatory step in steel production. The sintering process provides the necessary raw materials for blast furnace ironmaking, and is essential for achieving high-quality, high-output, and low-energy steel production. The quality of sintered ore directly affects smelting efficiency and output. Consequently, steel companies install physical sensors at key stages of the sintering production line for real-time monitoring, gathering vast amounts of time-series data rich in information, including real-time signal data from traditional sensors and video image data captured by industrial cameras and thermal imagers. However, the massive image data collected has not been fully utilized during monitoring.

This study employs object detection methods from computer vision to analyze the massive image data collected, detecting surface defects in the sintering process to monitor the quality of the sintered surface in real-time, thereby enhancing the quality and efficiency

of steel production. Through the qualitative and quantitative surface defect evaluation model developed by our research group, the YOLO_LSK model can accurately identify two types of cracks—generally severe and very severe—on the sintered surface, providing a reference in the field of surface crack detection. Beyond the sintering surface in this industrial context, the model can also be applied to defect detection in other scenarios, such as road surface monitoring, dam crack detection, and bridge crack detection. The underutilized massive image data offers an alternative solution for addressing product quality issues in manufacturing.

Manuscript received XX. XX, 2018; accepted XX. XX, 2018.

1.School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China;

2. Peng Cheng Laboratory, Shenzhen 518000, China.

This work is supported by National Science Foundation of China (Grant Number 92167110) and Innovation Project of Qiyuan Laboratory (Grant Number 11300LB2023114001).

II. RELATED WORK

The research on soft measurement models for the sintering process focuses on combining instrument data and exploring patterns and rules from industrial data through sintering mechanisms to predict key indicators. Key parameters include the Basic Temperature Point (BTP), moisture content in the mix, and FeO content. BTP prediction mainly uses mechanism modeling methods, such as the waste temperature fitting method and the BRP forecasting method[3]. Data-driven methods[4], like neural networks, are also used for nonlinear system identification. Moisture content in the mix is directly measured using methods like thermal drying and conductivity moisture detection to ensure optimal balling rate and sintering layer permeability. FeO content detection methods include direct detection, mechanism model prediction, process data-driven detection, and machine vision detection. These methods aim to improve the strength and reducibility of sintered ore, reduce the blast furnace coke ratio, and decrease fuel consumption. However, they have limitations such as data misalignment and erroneous data, necessitating multi-source data supplementation to enhance fault prediction.

With the rise of machine vision technology, some researchers use image processing methods to determine whether the sintering process has achieved the desired effect. For example, Li et al[5]. utilized feature image decomposition technology to extract the combustion state of sintering flames, Nellros et al[6]. determined the sintering degree by calculating the geometric properties and curvature of particles in microscopic sintering images, and Donskoi et al[7]. used Mineral4/Recognition4 software and structural texture methods to analyze common sintering phases for judgment. Although these methods have achieved certain results, in actual production, factories still rely on workers to subjectively judge and adjust sintering machine parameters by observing the sintered ore surface for defects or using instrument measurement data. Moreover, the complex texture details of sintered surface images, along with parameters like particle density and reflectance, cannot accurately represent the severity of sintering defects. Therefore, it is necessary to thoroughly study how to use the collected sintered ore surface images to assist machine learning judgments to improve the reliability of quality inspection.

YOLOv7[2] is a fast object detection algorithm using convolutional neural networks, advantageous in real-time applications. YOLOv7 achieves a superior balance between accuracy and speed compared to other object detection algorithms. Its novel network architecture and optimized loss function enhance detection accuracy, particularly excelling in small object detection. Additionally,YOLOv7 demonstrates stronger generalization capabilities and scalability, enabling efficient operation across various computing environments, making it well-suited for real-time object detection tasks. Deep learning models based on YOLOv7 have been widely used in surface defect detection and recognition. For instance, Chen W H et al.[8] used an improved YOLOv7 model for target detection of ships in SAR images; Gao S et al.[9] employed an improved YOLOv7 model for detecting small defects on metal surfaces; Yang Z et al.[10] used a YOLOv7 model for detecting diseases on asphalt pavements. These studies have achieved significant

results, indicating that YOLO models have great potential in surface defect detection.

In our preliminary study, we utilized DeepLabV3+ [11]for semantic segmentation of the collected images, segmenting the sintered material surface to reduce background interference. Subsequently, quality evaluation criteria were determined based on expert experience, and a dataset was constructed for YOLOv7 target detection. This study aims to utilize these image data and achieve real-time detection of sintering surface defects using an improved YOLOv7 model based on LSKNet[12] to enhance the quality and efficiency of steel production.

III. PROPOSED MODEL - YOLO_LSK

This study addresses product quality issues during the sintering process and aims to achieve high-precision sintering defect detection by combining YOLO v7 and LSKNet to design a deep CNN model named YOLO_LSK, as shown in the **Fig 1.** In terms of data preprocessing, this study employs the semantic segmentation module of DeepLabV3+ to separate the background from the sintered surface in the images and constructs evaluation labels for target monitoring and identification based on expert consultation methods. Since data preprocessing and label establishment are not the main focus of this paper, they will not be detailed here.

The YOLO_LSK network can be divided into three main components: Input, Backbone, Head. The input data first undergoes feature extraction through four convolution modules, followed by connection to the ELAN module. Then, it passes through three sets of ELAN modules and the MP-1 module to obtain feature map outputs of different sizes, denoted as C3, C4, and C5. After producing these feature maps, two LSKNet modules and the SPPCSPC module are introduced to enhance feature extraction and multi-scale information processing. By performing operations such as downsampling, feature extraction, and shallow-deep feature fusion on the feature maps output by the backbone network, outputs P3, P4, and P5 are obtained. After adjusting the number of channels through the REP module, a convolution is used for the final prediction of objects, classes, and bounding boxes. The detailed modules in the YOLO_LSK model are introduced as **Fig 1**.

A. BACKBONE NETWORK MODULES

The backbone structure of YOLO_LSK primarily consists of CBS, ELAN, and MP-1 modules. The LSKNet module is introduced after the ELAN module to enhance the extraction of relevant features, suppress irrelevant feature extraction, and improve network performance. CBS is a convolution module composed of a convolution layer, batch normalization layer, and Silu activation function, as shown in **Fig 2 (a)**.The structure of the CBM module is similar to that of CBS, except that the last layer is replaced with a Sigmoid activation function, as shown in **Fig 2 (b)**. CBS modules are subdivided into three types based on convolution kernel size and stride: k=1, s=1 for changing data channels; k=3, s=1 for feature extraction; and k=3, s=2 for downsampling. The combination of CBS and CBM enables YOLO_LSK to achieve an excellent balance between speed and accuracy. ELAN uses different numbers of convolution modules for feature extraction, achieving shallow and deep feature fusion through concatenation. The structure is shown in **Fig 2 (c)**.The MP module performs downsampling through two branches: one branch first applies max pooling, then uses a 1×1 convolution to change the number of channels; the other branch goes through two different CBS modules to obtain the downsampling output. The final feature map of "super" downsampling is obtained through a merge operation.The structure is shown in **Fig 2 (d)**. The ELAN module effectively enhances feature representation through multi-level feature aggregation, allowing the model to retain input feature information while achieving richer feature representation, thereby improving detection accuracy. The MP module reduces dimensionality through max pooling, preserving important information while reducing computational load and memory requirements, further increasing the model's computational efficiency.

In the YOLO_LSK model, multi-scale feature fusion improves the training accuracy of the neural network model. The SPPCSPC module's SPP uses max pooling operations to obtain different receptive fields, adapting to images of different resolutions. The first branch goes

through max pooling operations with convolution kernels of sizes 1×1, 5×5, 9×9, and 13×13, distinguishing large and small targets. The CSP module divides the features into two parts: one part undergoes regular processing, while the other part undergoes SPP structure processing. Finally, the two parts are merged, reducing computational load and improving computational speed and model accuracy. The structure is shown in **Fig 2 (e)**.

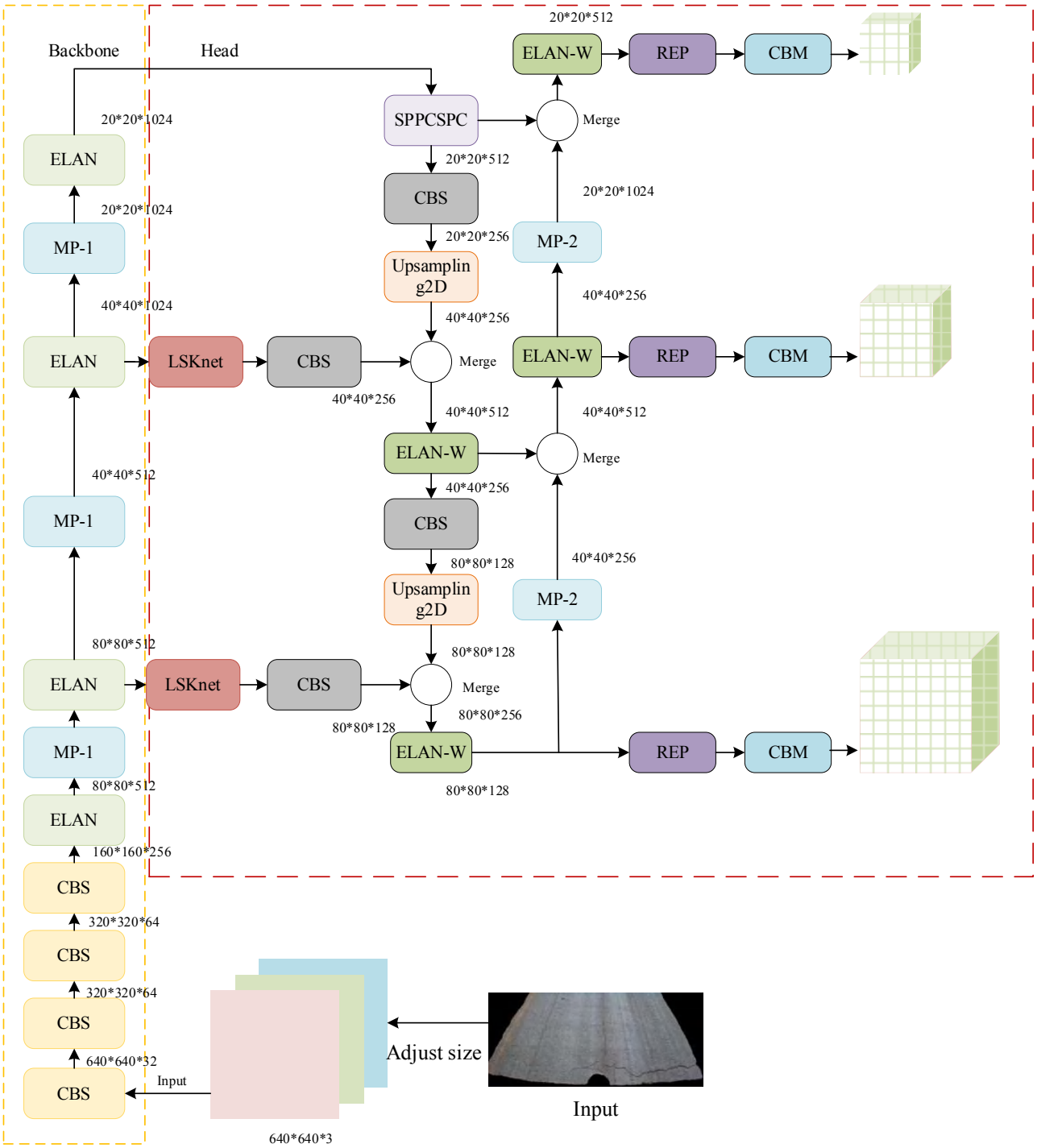


Figure 1 YOLO_LSK Network Structure

B. Large Selective Kernel Network

The attention mechanism was discovered in the 1990s by scientists studying human vision and has since been widely introduced into artificial intelligence neural network models to improve performance. Currently, the attention mechanism has become one of the most widely used key components in the field of deep learning. This mechanism is typically divided into channel attention mechanisms and spatial attention mechanisms. In addition, kernel selection technology is an adaptive and effective dynamic context modeling technique.

The Large Selective Kernel Network (LSKNet) proposed by Yuxuan Li et al.[12]. is designed for remote sensing target detection tasks, aiming to fully exploit the inherent characteristics of remote sensing images, which require broader and more adaptive contextual understanding. LSKNet, by adapting its large spatial receptive field, effectively models the subtle contextual differences between different object types. The LSKNet used in this study comprises multiple LSKNet blocks, each consisting of two residual sub-blocks: the Large Kernel Selection (LK Selection) sub-block and the Feed-Forward Network (FFN) sub-block. The core LSK module is embedded in the LK Selection sub-block and consists of a series of large kernel convolutions and spatial kernel selection mechanisms. The core LSK module's large kernel convolution consists of two or three depth convolution modules designed to construct larger convolution kernels through depth convolutions with large growth kernels and increased dilation, obtaining various features with large receptive fields. The spatial kernel selection mechanism involves spatial selection from different scales of large convolution kernels and effectively extracts spatial relationships through channel-based average kernel maximization.

This model incorporates the LSKNet module to dynamically acquire different receptive fields and contextual information, enhancing target feature extraction in conjunction with the SPPCSPC module.

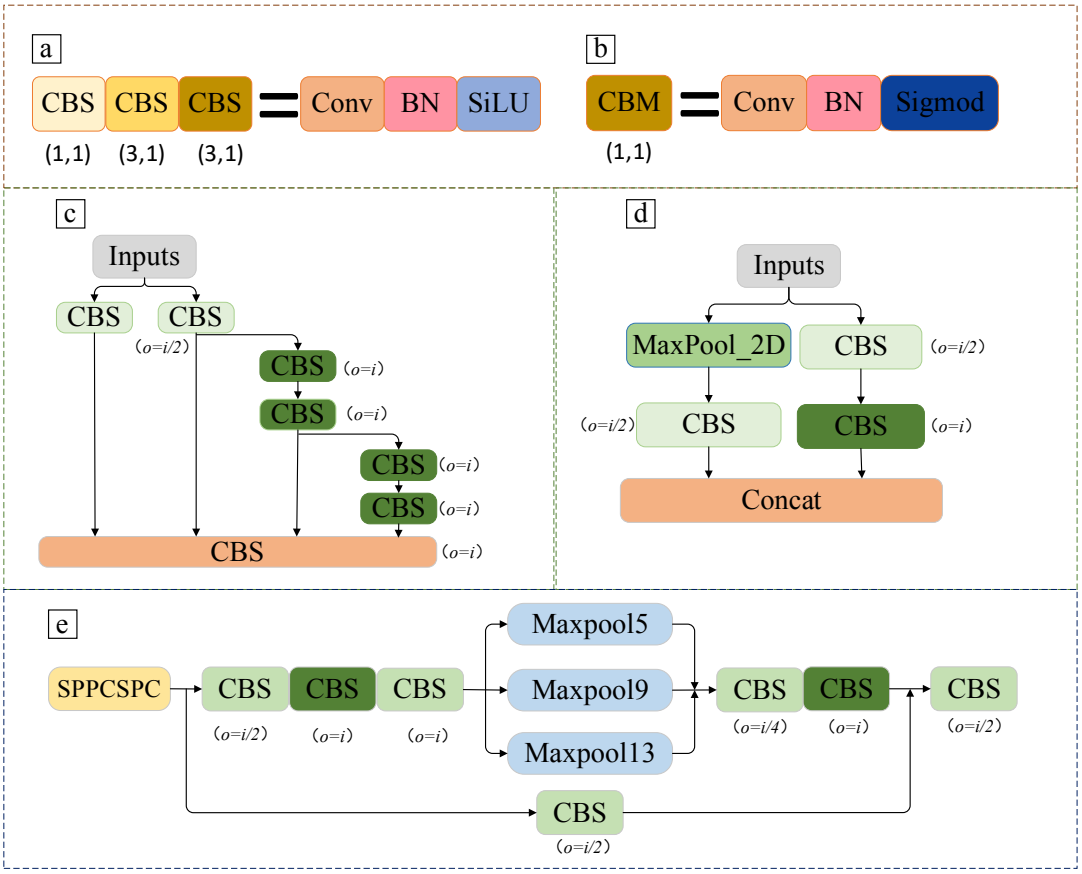


Figure 2 (a)the structure of CBS (b)the structure of CBS (c) the structure of ELAN (d) the structure of MP-1 (e) the structure of SPPCSPC

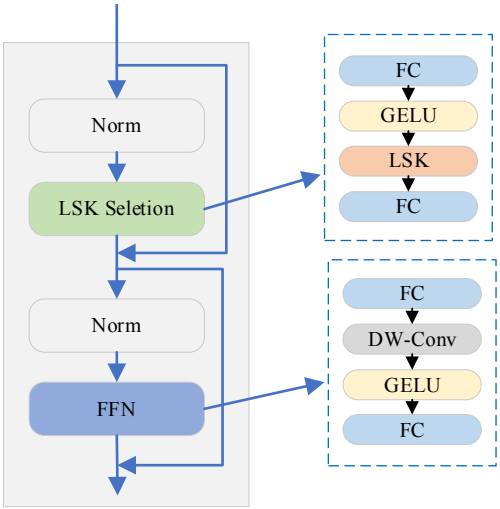


Figure 3 A block of LSKNet

Table 1: Training parameter setting

Hyperparameter	Meaning	Value
fp16	Half-precision floating point	True
anchors_mask	Index array of anchor boxes	Default
pretrained	Pretrained	False
mosaic_prob	Probability of applying mosaic augmentation	0.5
mixup_prob	Probability of applying mixup augmentation	0.5
special_aug_ratio	Range within which mosaic augmentation is applied	0.7
freeze_epoch	Number of iterations in the frozen stage	50
freeze_batch_size	Batch size during the frozen stage	8
unfreeze_epoch	Number of iterations in the unfrozen stage	300
unfreeze_batch_size	Batch size during the unfrozen stage	4

IV. EXPERIMENT

A.EXPERIMENT SETTINGUP

The YOLO_LSK network model developed in this study is built using the PyTorch 1.11 deep learning framework, with the program code written in Python. The model runs on a computing platform comprising a 12th Gen Intel(R) Core(TM) i7-12700K 3.60GHz CPU, NVIDIA GPU, and GeForce RTX 3080. The operating system used is 64-bit Ubuntu 20.04. The **Tab 1** are the parameter settings for the model.

B. EALUATION METRICS

This study uses Precision, Recall, and Average Precision (AP) as evaluation metrics to assess the performance of the network model. AP is an important evaluation metric for object detection algorithms. It represents the average precision across different recall levels and can be seen as the area under the precision-recall curve. The higher the AP value, the better the object detection model performs on the current dataset.

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

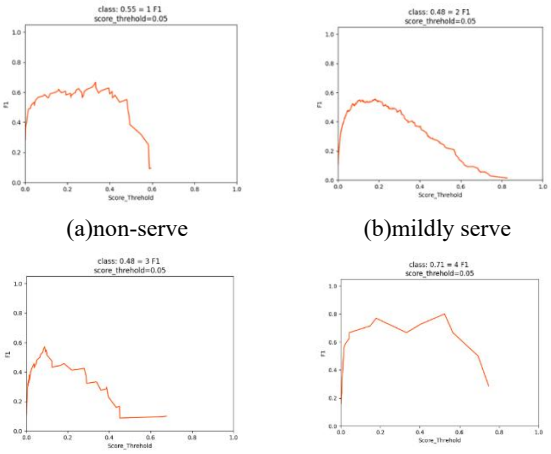
$$AP = \sum \int_0^1 P(R)dR \tag{3}$$

C. PERFORMANCE MEASURES

The YOLO_LSK network model is trained for 300 epochs, with each epoch undergoing 49 iterations, and 64 images are input to the network per iteration. The network is trained a total of 14,700 times. Considering that the assessment of the overall severity of the sintered ore surface focuses more on identifying all cracks, especially the relatively critical categories of general

severity and very severe cracks, this experiment pays more attention to the Recall performance indicator. It can be observed that detection performance meets expectations better when the confidence interval is within (0, 0.2].

The F1-score considers both Precision and Recall, allowing for an overall evaluation of the model's classification performance. Its curve is shown in the **Fig 4**. In object detection tasks, the F1-score can be used to assess the model's accuracy and completeness in detecting all targets. By observing the F1 curve, we can understand how the F1 value changes with the confidence Score_Threshold during training. Comprehensive analysis of various F1 values reveals that the model's training performance is relatively better when the confidence interval is within (0, 0.2].



(a)non-serve (b)mildly serve

(c)generally serve (d)very serve

Figure 4 F1 curve of YOLO_LSK training model

This study uses Average Precision (AP) and mean Average Precision (mAP) as overall evaluation criteria. The closer the AP and mAP values are to 1, the better the model quality. Average Precision is calculated based on Precision and Recall, essentially averaging the Precision in the PR curve. Mean Average Precision is the mean of the Average Precision for all labels, used to measure the overall recognition accuracy of the model. Based on the previous analysis, the training results of the model with a confidence level of 0.05 are shown below. The AP for each label and the mAP for all labels are shown in the table. The AP values are 0.8438 for non-severe, 0.4667 for mildly severe, 0.4306 for generally severe, and 0.7857 for very severe. The mean Average Precision (mAP) for all labels is 0.6317. Other data are shown in the **Tab 2**.

D.ABLATION STUDY

In this study, through experimentation, the insertion points of the LSKNet module in the YOLOv7 model were determined to be at the positions of the backbone network output, named stage1 and stage2, respectively. Multiple ablation and control experiments were conducted. To verify the performance of the LSKNet attention mechanism, the MLCA attention mechanism was also added for comparison.

The study was designed by adding the attention mechanisms separately at one stage and at two stages, as well as mixing the two mechanisms at two stages, resulting in the following experimental groups, as shown in **Tab 3**.In addition, the models with added attention mechanisms were also compared with the original YOLOv7 model.

Table 3 YOLO models at different locations

Stage1	Stage2	Name
LSK	LSK	YOLO_LSK
LSK	/	YOLO_LSK1
/	LSK	YOLO_LSK2
MLCA	MLCA	YOLO_MLCA
MLCA	/	YOLO_MLCA1
/	MLCA	YOLO_MLCA2
LSK	MLCA	YOLO_LSK_MLCA

To verify the performance of the YOLO_LSK network model proposed in this study, ablation experiments were conducted. The compared component is the MLCA attention mechanism. The performance of the generated neural network model was analyzed using different components and tested on a pre-prepared dataset for status detection. The ablation experiments compared the YOLO v7 model with the YOLO_LSK model. The hyperparameters and operating environment of the models were kept consistent to ensure the accuracy of the ablation experiments. Different components added at different stages constituted different models, which were trained multiple times.

The experimental results are shown in the table. As shown in **Tab 4**, the YOLO_LSK model demonstrates improvements over YOLOv7 in the three metrics (AP, Precision, and Recall) with the addition of the LSKNet.

There is almost no difference in model size and training time, but there is a difference in processing speed. To more clearly illustrate the effectiveness of the improved model, the prediction results of different models are visualized in the images, as shown in the **Fig 5**.

V. CONCLUSION AND FUTURE WORK

This study developed both qualitative and quantitative evaluation models for surface defects on sintering pages, providing a reference for other surface crack products. A convolutional neural network model named YOLO_LSK, based on YOLOv7 and LSKNet, was designed for defect detection in the sintering process. This model employs multiple feature extraction methods and integrates LSKNet modules to capture contextual information and accurately identify features. Multi-scale training was used to enhance information extraction from images, and experiments demonstrated that this approach significantly improves network performance and effectiveness. Using a dataset of sintering images provided by the factory, the model achieved excellent defect prediction results. The experimental results indicate that the model reached a mean Average Precision (mAP) of 63.17% in detecting defects on sintering pages, with accuracies of 100% for both moderately severe and extremely severe cracks as the number of training iterations increased. This has proven crucial for assessing the quality of sintering products. Compared to the original YOLOv7 model, the YOLO_LSK model's accuracy improved by 4%.

Despite preprocessing of the image data, variations in workshop lighting conditions may lead to inconsistent image quality, with some images containing noise. Additionally, the model's feature extraction methods remain relatively coarse. Future work could explore more precise texture and edge feature extraction methods to filter noise and extract relevant image features. Moreover, expanding the data samples using deep learning techniques could enhance data representation and model accuracy. This model not only aids in the evaluation of crack quality on sintering pages but also provides a reference for evaluating crack quality in transportation roads and bridges.

Table 2 YOLO_LSK identification results on the test set

Defect class	Score Threhold	AP (%)	F1	Recall (%)	Precision (%)	mAP (%)
1(non-severe)	0.05	84.38	0.54	95.00	37.25	63.17
2(mildly severe)		46.67	0.45	78.42	31.59	
3(generally severe)		43.06	0.48	68.42	37.14	
4(very severe)		78.57	0.62	83.33	50.00	

Table 4 Ablation test results

Models	mAP（%）	Precision（%）	Recall（%）	F1	AP
YOLOv7	59.86	39.58	95.00	0.56	73.75
		30.86	74.82	0.44	46.73
		41.94	68.42	0.52	41.88
YOLO_LSK (ours)	63.17	55.56	83.33	0.67	77.08
		37.25	95.00	0.54	84.38
		31.59	78.42	0.45	46.67
		37.14	68.42	0.48	43.06
		50.00	83.33	0.62	78.57
YOLO_LSK1	60.59	38.78	95.00	0.55	70.95
		34.75	76.26	0.48	50.67
		38.71	63.16	0.48	42.19
		62.50	83.33	0.71	78.57

		33.93	95.00	0.5	77.79
YOLO_LSK2	60.74	29.65	73.38	0.42	46.27
		31.58	63.16	0.42	40.34
		50.00	83.33	0.62	78.57
		37.04	100.00	0.54	66.15
YOLO_MLCA	58.87	31.60	74.10	0.44	46.44
		36.11	68.42	0.47	47.67
		41.67	83.33	0.56	75.24
		32.20	95.00	0.48	79.05
YOLO_MLCA1	62.81	31.14	74.82	0.44	49.23
		33.33	63.16	0.44	44.38
		50.00	83.33	0.62	78.57
		36.54	95.00	0.53	72.71
YOLO_MLCA2	61.10	31.85	76.98	0.45	47.54
		41.67	52.63	0.47	46.56
		55.56	83.33	0.67	78.57
		36.54	95.00	0.53	78.64
YOLO_LSK_MLCA	62.55	31.86	77.70	0.54	49.02
		43.75	73.68	0.55	43.99
		62.50	83.33	0.71	78.57

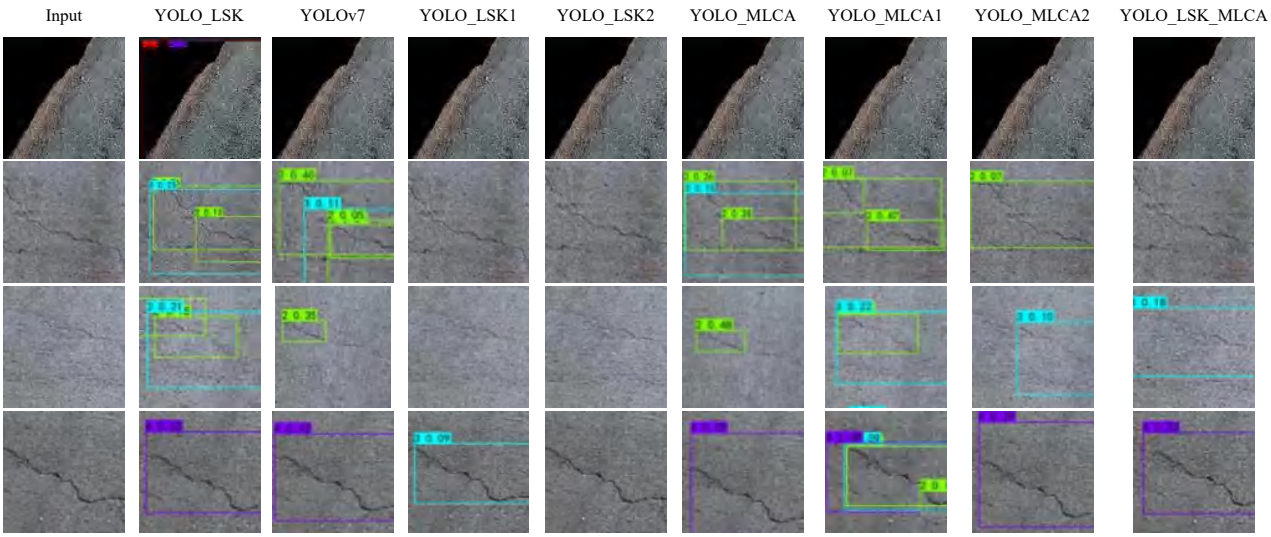


Figure 5 Comparison of prediction effect of different models

References

[1]Evans P, Annunziata M. Industrial Internet: Pushing the Boundaries of Minds and Machines[J]. General Electric Reports, 2012, 1:488-508.

[2]Wang C-Y, Bochkovskiy A, Liao H-Y M. YOLOv7: Trainable Bag-of-Freebies Sets New State-of-the-Art for Real-Time Object Detectors[A]. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)[C]. Vancouver, Canada: IEEE, 2023:7464-7475.

[3]LiuY Q，Pan D，Jiang Z H，Yu H Y，Gui W H, et al. A review of detection methods of key parameters in sintering process of iron and steel manufacturing.(in Chinese) Sintering and Pelletizing.2023.06.080

[4]Yan F, Zhang X, Yang C, et al. Data - driven modelling methods in sintering process: Current research status and

perspectives[J]. The Canadian Journal of Chemical Engineering, 2023, 101(8): 4506-4522.

[5]Li W, Wang D, Chai T. Flame image-based burning state recognition for sintering process of rotary kiln using heterogeneous features and fuzzy integral[J]. IEEE Transactions on Industrial Informatics, 2012, 8(4): 780-790.

[6]Nellros F, Thurley M J, Jonsson H, et al. Automated measurement of sintering degree in optical microscopy through image analysis of particle joins[J]. Pattern Recognition, 2015, 48(11): 3451-3465.

[7]Donskoi E, Poliakov A, Manuel J R. Automated optical image analysis of natural and sintered iron ore[M]//Iron Ore. Woodhead Publishing, 2015: 101-159.

[8]Chen Z, Liu C, Filaretov V F, et al. Multi-scale ship detection algorithm based on YOLOv7 for complex scene SAR images[J]. Remote Sensing, 2023, 15(8): 2071.

[9]Gao S, Chu M, Zhang L. A detection network for small defects of steel surface based on YOLOv7[J]. Digital Signal Processing, 2024, 149: 104484.

[10]Yang Z, Ni C, Li L, et al. Three-stage pavement crack localization and segmentation algorithm based on digital image processing and deep learning techniques[J]. Sensors, 2022, 22(21): 8459.

[11]Yang Y, Chen T, Zhao L. From Segmentation to Classification: A Deep Learning Scheme for Sintered Surface Images Processing[J]. Processes, 2023, 12(1): 53.

[12]Li Y, Hou Q, Zheng Z, et al. Large Selective Kernel Network for Remote Sensing Object Detection. arXiv 2023[J]. arXiv preprint arXiv:2303.09030.

About the authors

YANG Yi was born in 1978. She received the Ph.D. degree from the Nanjing University of Science and Technology,in 2008. She was engaged in postdoctoral research with the School of Reliability and Systems Engineer-ing, Beihang University, where she has been a Professor, since2024.Her main research focuses on reliability engineering ,multimodal data fusion , and AI and the Industrial Internet of Things.(Email:yang_cissy@163.com)

CHEN Tengtuo received his bachelor's degree in Automation from the Ocean University of China, China, in 2022. He is currently a postgraduate student with the School of Reliability and Systems Engineering, Beihang University, China. His focus lies on control systems, reliability engineering, AI and the Industrial Internet of Things.

CEN Hanyu was born in 2000. She received the B.E. degree in safety engineering from the Central South University of China, in 2023 She is now a postgraduate student with the School of Reliability and Systems Engineering, Beihang University, China. Her research focuses on multimodal data fusion and the Industrial Internet of Things.(Email :hycen@buaa.edu.cn)

LI Yanjing received his bachelor's degree in Safety Engineering from the China University of Geosciences Beijing in 2023. He is a postgraduate of School of Reliability and Systems Engineering, Beihang University. His research direction is mainly in Reliability Analysis and Industrial Internet.

WANG Minghao received his bachelor's degree in Network Engineering from Dalian University of Technology, China, in 2024. He is currently pursuing a master's degree at the School of Reliability and Systems Engineering, Beihang University, China. His research focuses on pattern recognition and the Industrial Internet of Things.

A Review of Steelmaking and Continuous Casting Scheduling Based on Intelligent Optimization Methods

SONG Xinbo[1], YU Yang[1,*], SUN Liangliang[2], JIANG Shenglong[3]

Abstract **— Steelmaking and continuous casting (SCC) is one of the crucial links in steel production, and its scheduling process involves multiple parameters and complex production environments. The application of intelligent optimization methods in the SCC scheduling can improve production efficiency, reduce energy consumption, optimize production plans, and provide more accurate and reliable decision support for steel enterprises. Regarding the production scheduling problem of the SCC process. Firstly, we introduce some applications of intelligent optimization methods in the SCC scheduling systems, and summarize their characteristics. Secondly, we divide the SCC scheduling problem into static scheduling and dynamic scheduling, and discuss the solving methods under different constraints. Finally, we point out the future research direction and significant contents to promote the research .**

Keywords **— Steelmaking and continuous casting; Production scheduling system; Static scheduling, Dynamic scheduling; Intelligent optimization methods**

Manuscript received XX. XX, 2018; accepted XX. XX, 2018.

[1]School of Automation, Shenyang Aerospace University, Shenyang 110136, China;

[2]School of Control Engineering, Northeastern University, Qinhuangdao, 066004, China;

[3]College of Materials Science and Engineering, Chongqing University, Chongqing 400044, China.

[*] Corresponding author. E-mail: ergejiayu@126.com

This work is partly supported by the National Natural Science Foundation of China (92367106, 62273221), the “Chunhui Plan” of Ministry of Education (HZKY20220431), Department of Education of Liaoning Province (CN) (20240066), the Natural Science Foundation of Hebei Province under Grant (F2023501006), Special Fund for Basic Scientific Research Business Expenses of Undergraduate Universities in Liaoning Province (CN) (20240206).

I. INTRODUCTION

The steel industry is one of the important indicators of national economic development [1-2]. The steel industry is not only a pillar of economic development, but also closely related to society, technology, national security, and other aspects. It plays an irreplaceable role in maintaining and promoting national prosperity and global stability.

Steelmaking and continuous casting (SCC), as an indispensable part of steel manufacturing, is an important factor in reducing energy loss, reducing operating costs, and improving production efficiency. The classification of SCC problem can be divided into two categories: dynamic scheduling and static scheduling [3].

Static scheduling for SCC refers to a scheduling method in which the sequence of operation execution and resource allocation plan for the continuous casting process are determined in advance in steelmaking production, and no modifications are made throughout the entire continuous casting process. In the process of SCC, a series of operations and adjustments need to be carried out on the continuously cast molten steel, such as replacing the crystallizer, cleaning the gate, replacing refractory materials, etc. These operations require a reasonable arrangement of time and resources to ensure the continuity and stability of production, while maximizing production efficiency and product quality. Therefore, the static scheduling of SCC manages the continuous casting process through a fixed scheduling plan on the basis of predetermined job execution sequence and resource allocation scheme, in order to meet production needs and optimize production efficiency.

Dynamic scheduling of SCC refers to a scheduling method in which the execution sequence and resource allocation plan of the continuous casting process can be dynamically adjusted according to the actual situation in steelmaking production. Unlike static scheduling, dynamic scheduling allows for flexible adjustment of job execution sequence and resource allocation based on changes in the production process [4], such as equipment failures, production plan adjustments, or changes in production demand, in order to maximize production needs and optimize production efficiency. However, when static SCC scheduling encounters uncertain factors, it can lead to the failure of plan [5]. The dynamic disturbances are caused by the uncertain factors [6], and the concept of dynamic scheduling was first proposed by [7], which involved the formulation and adjustment of production scheduling plans under dynamic disturbances.

At present, many steel enterprises rely on the experience of scheduling personnel, which may result in insufficient accuracy and non-standard situations [8]. With the increasingly prominent contradiction between multi variety, small batch contract orders and large-scale production organization processes [9-10], steel enterprises are constantly increasing their requirements for intelligence, especially in the face of multiple uncertain disturbances in the production process. The scheduling mode relying on manual

experience can no longer meet the dynamic scheduling needs of steel enterprises. Therefore, the dynamic scheduling problem in the steel production process is still a difficult problem that needs to be jointly studied and urgently solved by the academic and industrial communities. This paper surveys the intelligent optimization methods to solve the SCC scheduling problem. By retrieving in ScienceDirect with "intelligent optimization method" and "Steelmaking and continuous casting (SCC) scheduling" as the subject terms, it finds 134 articles. Figure 1 shows the statistics of these articles. In the past two years, the number of papers for the intelligent optimization algorithms in SCC scheduling problem has significantly increased, and become an emerging topic in the related fields.

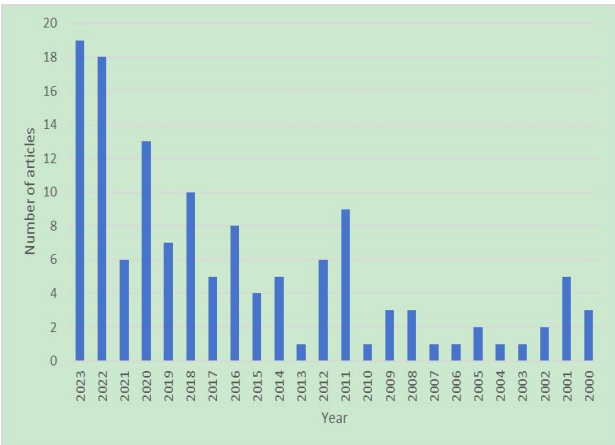


Figure 1 Scheduling statistics based on intelligent optimization methods in ScienceDirect.

II. Production scheduling problem and intelligent optimization method of SCC process

The solution of SCC optimization scheduling problem can be divided into two categories, one is intelligent optimization; One type is precise algorithms. This article mainly provides an overview of intelligent optimization algorithms for solving SCC scheduling problems, as shown in Figure 2. The algorithm mainly includes: heuristic algorithms, evolutionary computation algorithm, system optimization and reinforcement learning.

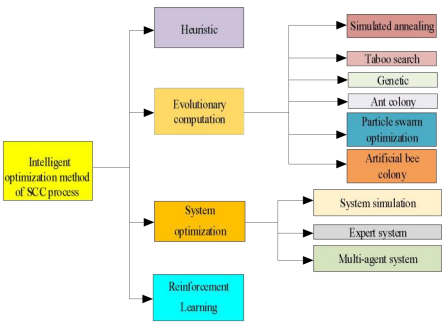


Figure 2 Intelligent optimization method of SCC

II-I. Characteristics of production scheduling problems in SCC processes

The production process of SCC is very complex, including complex physical and chemical reactions, with the characteristics of high pressure, high temperature, and high speed, and there are many uncertain factors. The manufacturing process of steel includes ironmaking, steelmaking, refining, and continuous casting stages. During the steelmaking process, the temperature and pressure inside the furnace are quite high. High temperature helps to melt and remove harmful impurities from raw materials, ensuring the quality of the final product. One of the key steps in steelmaking is to reduce iron ore to iron. This process is usually carried out in a high-temperature environment, by reacting with a reducing agent (usually coke) to reduce oxygen in iron ore to iron. In the steelmaking stage, it is necessary to strictly control the carbon content in the furnace and the addition of alloying elements. This is to ensure that the final steel has the required mechanical properties, corrosion resistance, and other characteristics. During the refining process, it is necessary to carry out desulfurization and dephosphorization treatment on the steel liquid to reduce the content of these harmful elements. This is usually achieved by adding desulfurizers and dephosphorizers. The main process of steel production is shown in Figure 3, including main processes such as ironmaking, SCC, hot rolling, etc. In the ironmaking process, raw materials such as coke, pellets, sintered ore, and limestone are added to the blast furnace through a rotary feeder, while coal powder is sprayed and hot air is blown to obtain high-temperature molten iron in the blast furnace. In the steelmaking process, high-temperature molten iron, scrap steel, slag-making agent, etc. are added to the converter, while oxygen is blown in. Elements such as carbon, silicon, and manganese are removed through oxidation-reduction reactions to obtain preliminarily qualified molten steel. The steel obtained from the converter sometimes needs to be refined in the refining furnace to further improve the quality of the steel. In the continuous casting process, the intermediate ladle containing molten steel continuously injects molten steel into the crystallizer. The water-cooled copper tube continuously carries away the heat in the crystallizer, causing the surface of the molten steel to solidify into a shell. The solidified shell is continuously pulled out at a certain speed, and after being water-cooled and straightened, it is cut into a specified length to obtain the continuous casting billet. The hot rolling process uses pressure processing to cause plastic deformation of the casting billet, resulting in the formation of products with customized specifications. In the traditional hot rolling process mode, continuous casting billets are stored in the slab warehouse. When there is a need for hot rolling tasks, they are heated by a heating furnace and then enter the

rolling mill; In the hot direct rolling and direct hot charging rolling modes of continuous casting billets, high-temperature continuous casting billets enter the rolling mill directly or through compensatory heating. After rolling, the billet is cooled and curled to form hot-rolled steel coils. After the hot rolling process, the product is formed and delivered to the order after a series of subsequent processes such as finishing, quality inspection, packaging, and warehousing.

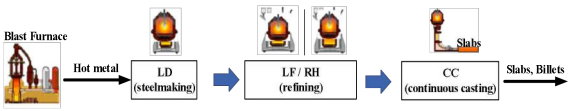


Figure 3 Steel production process

II-II. Intelligent optimization method of production scheduling problem of SCC process

The existing steel scheduling methods include intelligent optimization methods. Intelligent optimization methods include heuristic algorithms, genetic algorithms, ant colony algorithms, particle swarm optimization algorithms, artificial bee colony algorithms, taboo search, simulated annealing, system simulation, expert systems, and multi-agent systems. Table 1 is a summary of the author's research methods on steel production scheduling.

Table 1 Research methods of iron and steel production scheduling

Algorithm	Characteristic	Case
Heuristic	(1) The operation is relatively easy, with a fast solving speed, and the obtained solution is relatively good; (2) If the scale of the solution is large, there are few ways to judge the quality of the solution; (3) No requirement for an exact solution, only need to approach the optimal solution.	Heuristic algorithms with multiple rules [11-13]
Genetic [14]	(1) The required calculation time is short, the convergence is good, and it has strong robustness; (2) If there are many individuals, the search space can be large and the required search time can be long; (3) The algorithm lacks the ability to search for new spaces and is prone to obtaining local optimal solutions; (4) Due to the randomness of the evolutionary process of algorithms, the obtained solutions may not be reliable and have poor stability; There are high requirements for the initial population selection, and poor initial population selection can directly affect the reliability of the solution and the efficiency of the algorithm.	Hybrid genetic algorithm [15-16] Improving Genetic Algorithm [17-18]
Ant colony [19]	(1) Strong robustness and high quality of searched solutions; (2) It does not rely on the initial route selection, has lower requirements for the initial route selection, and does not require manual adjustment during the search process; (3) In large-scale optimization problems, there may be a contradiction between time performance and search space, which can lead to excessively long computation time or rapid convergence to local optimal solutions.	Combining other algorithms with ant colony algorithm [20-21]
Particle swarm optimizatio-n [22-23]	(1) The composition of the algorithm is relatively easy, without adjusting a large number of parameters, and the implementation is relatively simple; (2) The effectiveness of dealing with discrete optimization problems is not good, and it is easy to obtain local optimal solutions; (3) Mainly used for multi-objective optimization, function optimization, signal processing, and neural network training.	Other algorithms can also be combined with particle swarm optimization [24]
Artificial bee colony	(1) Few parameters need to be controlled, convergence is fast, stability is good, and efficiency is high; (2) Slow convergence in the later stage, low search accuracy, and easy obtaining of local optimal solutions are common issues in optimization algorithms.	Artificial bee colony algorithm needs to be improved according to specific problems [25-26]
Taboo search [27]	(1) It can move quickly and with a high probability in a positive direction, and has good convergence; (2) The requirement for parameter selection is high, and parameter selection has a significant impact on the final solution obtained, with poor robustness; (3) A too long taboo length can lead to cyclic search, and a long taboo table can easily lead to local optimal solutions.	Taboo search can solve the optimal furnace schedule [28] Taboo search can be combined with other algorithms [29]
Simulated annealing [30]	(1) The solution is only a random approximation, and the quality of the solution depends heavily on a large number of experiments; (2) Not only local search, but also global search; The selection of parameters is very important. If inappropriate parameters are selected, the calculation time is very long, and even unsatisfactory results may not be obtained.	Combining Simulated Annealing with Genetic Algorithm [31] Mixed sorting immune simulated annealing [32]
System simulation	(1) It simulates the actual production situation and analyzes the global nature of the system; (2) Conducting system simulation requires a significant amount of time and is expensive; (3) The accuracy of simulation is limited by human judgment, and even high-precision simulation models cannot guarantee that the optimal solution or suboptimal scheduling can be found.	Simulation optimization [33] Petri network module [34]
Expert system	(1) It requires a lot of expert knowledge and analytical methods to solve complex problems; (2) Expert systems can handle specific scheduling problems and establish production scheduling systems in the SCC process.	Expert system [35-36]
Multi-agent system	(1) It solves difficult problems with many interactions; (2) Decompose complex large-scale systems into multiple simple intelligent agents that coordinate, communicate	The combination of multi-agent systems and other algorithms

	with each other, and are easy to manage.	[37-38]
Reinforcem-ent learning	(1) It can adaptively adjust strategies to cope with uncertainty and dynamic changes in production. (2) It can learn in real-time from the production process and adjust strategies based on real-time feedback, allowing the model to adapt to changes in the production process. (3) The trained reinforcement learning model can generalize in different production conditions and environments, which means that the model can be applied to various complex scenarios.	Reinforcement learning [77-81]

II-III.The usage of scheduling systems in some typical steel mills at home and abroad

Scheduling systems play a crucial role in the operation of steel mills, ensuring efficient production and optimal utilization of resources. The integration of scheduling systems in steel mills has led to significant improvements in productivity, cost reduction, and overall operational efficiency. Application of Scheduling System in Some Typical Steel Plants in Table 2.

Table 2 The usage of scheduling systems in some typical steel mills at home and abroad

Steelworks	Name	Characteristic
Shanghai Baosteel	SCC scheduling system	Establish a scheduling model through expert reasoning, combined with human-computer interaction, to quickly respond to complex events.
Hebei Iron and Steel Tangshan	Tangshan Iron and Steel APSS (advanced planning and scheduling) System	The intelligent optimization algorithm combines manual planning and scheduling knowledge and experience to achieve resource integration, unified management, and improve scheduling efficiency and flexibility.
Fangda Special Steel	SCC production scheduling system	It applies scheduling rules to calculate the initial scheduling plan, and then adjusts the scheduling plan based on real-time data feedback.
Nippon Steel Corporation of Japan	Production planning and scheduling system	By using constraint based rule-based operations and optimization algorithms, production operation planning and scheduling capabilities from steelmaking to hot rolling are provided.
NKK Keihin Steel Plant in Japan	Scheplan system	It uses artificial intelligence and human-computer interaction technology to generate scheduling plans, and the system includes scheduling for blast furnace converter, converter continuous casting, and continuous casting rolling mill.

III. Classification of SCC scheduling with different constraint conditions

III-I. Static scheduling of SCC

III-I-I. Static scheduling problem

Static scheduling of SCC refers to the process of allocating machines and determining the start and end processing times for each process of each furnace based on the known start pouring time, given the raw data such as casting number, furnace number, and refining method, before the processing operation is carried out, to form a scheduling plan table.

The static scheduling of SCC is an ideal state of scheduling, where the processing equipment is always in a processable state without any equipment malfunctions; No urgent order insertion or cancellation during the processing; The raw materials required for the processing process are also in sufficient supply. Given the known processing time and the transportation time between equipment, based on the pouring schedule, reasonable allocation is made with similar equipment as shared resources to ensure timely pouring at the given pouring time and continuous pouring during the pouring process. A reasonable scheduling schedule is obtained, and this set of furnaces is processed according to the scheduling schedule until the end.

III-I-II. The Current Status of Static Scheduling Research

The research on static scheduling of SCC has a long history. Jackson [7] began researching the two-machine scheduling problem as early as 1957 and has a history of nearly 70 years. After more than 60 years of development, the research methods of static scheduling have shifted from a single operations research method to computational intelligence and artificial intelligence optimization methods. In 1996, Lee HS, et al.[56] discussed scheduling problems in the steelmaking industry and various solutions in different scheduling fields, dividing research methods into three categories: operations research methods, artificial intelligence, and hybrid methods. Tang Lixin, et al.[57] further divided the static scheduling methods for SCC into four categories in 2001: operations research methods, computational intelligence, human-machine interaction, and multi-agent systems. The research method for static scheduling of SCC is shown in Figure 3.

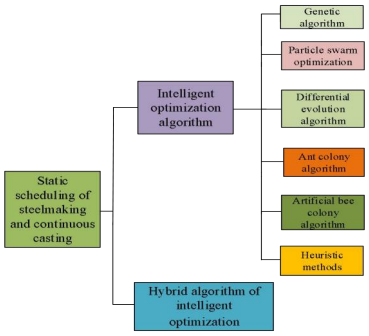


Figure 3 Research method for static scheduling of SCC

A research method combining rules and algorithms has been proposed to address the static scheduling problem, based on extensive investigation and practical application. The so-called "rules" refer to the general rules for commanding production scheduling based on the experience of scheduling personnel and actual production situations, such as rules for controlling time, rules for equipment matching, rules for adjusting operation, and rules for process constraints, forming a rule library about production scheduling. The so-called "algorithm" refers to the calculation method for solving the scheduling problem of SCC, such as using the artificial bee colony algorithm and the heuristic algorithm to solve the production scheduling problem and obtain the method of static scheduling. Based on different production plans and situations, determine accurate constraints and the best production organization mode according to rules, then establish a production scheduling model, and use appropriate algorithms to solve the model.

III-II. Dynamic scheduling of SCC

In practical production processes, dynamic scheduling research is more in line with actual production requirements and can better ensure the feasibility of scheduling. Dynamic scheduling refers to an adjustment method adopted when a specific furnace batch cannot be carried out as originally planned due to the influence of certain random events. In the event of a random occurrence in the production site that prevents the original plan from being implemented, a dynamic scheduling system will analyze the type of disturbance based on the disturbance information and actual production data collected on-site. Subsequently, the produced furnace batches are manually adjusted to ensure the smooth progress of the ongoing furnace batches, and this adjustment of the produced furnace batches is referred to as real-time online scheduling. Rescheduling involves the compilation of furnace batches that have not been produced (or combined with new plans).

III-II-I. The disturbance factor of the dynamic scheduling of SCC

There are many complex problems in the actual SCC production process, such as equipment failures, order insertion, and incidents of unqualified steel composition. Once these disturbance events occur, the original scheduling plan (i.e. static scheduling) often cannot be executed smoothly in the production process. At this time, there is an urgent need for a new scheduling scheme to dynamically adjust the disturbance problems that occur in the actual production process to ensure the smooth completion of the production process. Therefore, dynamic scheduling has become the main research direction of SCC production scheduling at present.

The disturbance factors that occur in the SCC production scheduling process can be classified into the following categories: time, equipment, order, process, and quality. Process disturbance events include quality disturbances and temperature disturbances, as shown in Table 3.

Table 3 Classification of disturbance factors in dynamic scheduling of SCC

Type	Classification	Brief introduction	Common disturbance events
Time	Internal disturbance	Time type disturbances are the most common types of disturbances in the steel production process, and many dynamic time disturbances can ultimately be transformed into time type disturbances.	Processing time is uncertain [39] Delayed start time [40] Delay in converter steelmaking [41] Converter [42-43]
Equip-ment	Internal disturbance	Equipment disturbance mainly refers to the reduction in the number of available machines and equipment caused by equipment failures. It is necessary to reassign the number of unprocessed furnaces on the faulty machine and assign equipment accordingly.	Refining furnace [42] Continuous casting machine [44-45] Heating furnace [46] Hot rolling mill [46]
Order form	External disturbance	Order disturbance events refer to the modification, addition, or cancellation of order information (such as molten steel composition) required by users or producers during the steelmaking continuous casting production process.	Urgent order addition [47] Order cancellation [48-49] Order Change Return and diversion of molten steel [50]
Procs-s	Internal disturbance	Process disturbances refer to changes in production process routes or deviations in process parameters.	Fluctuations in molten iron supply [51] Abnormal weight/compositio-n [52-53] Temperature too high/too low [47]
Quali-ty	Internal disturbance	Quality disturbances are mainly reflected in the need to reorganize production or dynamically adjust the matching relationship between materials and orders by re refining furnaces that do not meet the casting requirements and steel composition of the manufacturer.	Product quality is unqualified [48] Unqualified intermediate product quality [49]

In the actual production process of SCC, there are often many unexpected situations. In addition to the common single types mentioned above, there are also many disturbances [54-55] that include two or more types of disturbance events.

III.II.II. Research status of intelligent optimization methods in dynamic scheduling of SCC

Intelligent optimization methods are widely used to solve dynamic steel scheduling problems due to their efficiency and ease of implementation. In existing research, Pang Xinfu, et al.[58] reduced the SCC rescheduling problem to a mixed flow shop scheduling problem[59], established a rescheduling model to minimize the maximum completion time, and designed a solution algorithm combining heuristic rules and genetic algorithms. Zheng Zhong, et al.[60] proposed a hybrid algorithm combining genetic algorithm and time-lapse strategy, as well as a hybrid algorithm combining genetic algorithm and generalized variable neighborhood search algorithm[61]. Xiong Wei, et al. [62-63] designed a dynamic scheduling method based on an immune multi-agent system algorithm. Tang Lixin, et al.[64] drew an improved differential evolution algorithm. Ning Shushi et al.[48] proposed a dynamic scheduling method for SCC based on the just-in-time concept and designed an evolutionary iterative local search algorithm based on multiple neighborhood structures and population evolution strategies. Peng Kunkun [65] presented an improved imperial competition algorithm. Ding Shuai, et al.[66] designed an adaptive genetic algorithm for the dynamic scheduling problem of steelmaking continuous casting under equipment failure. Li Junqing, et al.[67] designed a hybrid fruit fly optimization algorithm with an embedded iterative greedy algorithm. Peng Kunkun, et al.[74] proposed an improved artificial bee colony algorithm. Liu Wentao, et al.[68] designed a heuristic algorithm for the dynamic scheduling problem of production performance deviating from the planned time, which is aimed at rescheduling the production of whole and half castings due to obstruction. Qian Qiangfei, et al.[69] established conflict elimination rules and broken casting repair rules for the delay disturbance of electric arc furnace SCC process in the remanufacturing of scrap steel, and designed rule-based time passage strategies and furnace redistribution strategies. Wang Chuang, et al.[70] designed a heuristic rule-based operation time adjustment method for the dynamic scheduling problem of SCC stage in special steel production. Jiang Shenglong, et al.[71] decomposed the dynamic scheduling problem of SCC into a global scheduling problem and local scheduling problem and proposed a dynamic multi-objective differential evolution algorithm based on decomposition. Zhou Tao, et al.[75] proposed a rescheduling algorithm consisting of two parts: an equipment assignment algorithm based on the "furnace machine correspondence" scheduling strategy and a time adjustment algorithm based on the process flexible buffer control strategy. Wang Jiayang, et al.[76] established the Basic Resource Task Network (RTN) model and Flex RTN model for SRCC scheduling considering the flexibility of the refining process.

The actual advantages and limitations of dynamic scheduling in steel production are shown in Table 4.

Table 4 The actual advantages and limitations in dynamic scheduling of SCC

Advant-ages	Characteristic	Limitations	Characteristic
Strong adaptail-ity	The dynamic scheduling system can respond in real-time to changes in the production process, such as equipment failures, raw material supply delays, etc. By adjusting the production plan in a timely manner, it ensures the continuity and stability of the production process.	Complexity	The implementation and maintenance of dynamic scheduling systems require high technical support, and the complexity of the system will increase the difficulty of management.
Increase efficiec-y	By optimizing resource allocation, dynamic scheduling can reduce waiting time and resource waste in the production process, improve production efficiency and output.	Cost	Building and maintaining an efficient dynamic scheduling system may require significant initial investment, including hardware infrastructure and software development costs.
Flexibil-ity	Dynamic scheduling allows production plans to be quickly adjusted based on actual conditions to adapt to market changes and changes in production demand.	Data processing	Dynamic scheduling relies on accurate and real-time data, and the collection, processing, and analysis of data require reliable IT infrastructure and professional data analysts.
Reduce downti-me	In the event of an emergency, dynamic scheduling helps minimize downtime on the production line and quickly restore production.	Human resources	Implementing dynamic scheduling may require retraining employees to adapt to the new scheduling process, which may involve additional human resource costs.

Improv-e product quality	Through real-time monitoring and adjustment, dynamic scheduling helps ensure product quality and reduce the occurrence of defective products.	System stability	The dynamic scheduling system requires stable operation, and any system failure may lead to production chaos.

III-III. The scheduling problem of SCC under different constraints

III-III-I. A scheduling optimization method for SCC considering energy constraints

In the steelmaking process, there are characteristics of high emissions and high energy consumption, among which carbon emissions are closely related to energy consumption and energy consumption. It is one of the key focuses of the country under the "dual carbon background". Therefore, the optimization method of steelmaking continuous casting scheduling considering energy constraints is particularly important. Jiang Shenglong [72] proposed a SCC scheduling optimization method considering energy constraints, combining the characteristics of energy flow and material flow coupling in steel production, based on process energy load constraints, a multi-objective production scheduling optimization model was established that simultaneously pursues maximum completion time and total waiting time minimization.
This scheduling method mainly converts the optimization objective of reducing energy consumption into considering the upper limit of energy load, which serves as a hard constraint for modeling SCC scheduling. At the same time, an improved multi-objective optimization algorithm with individual fitness hierarchical evolution and a predictive population strategy is designed to solve the model.

III-III-II. A scheduling optimization method for SCC considering the malfunction of the casters

The most common interference in the SCC production process is the malfunction of the casters. The existing redistribution mode for caster failures lacks consideration for the uncertainty of molten steel. Song Yuqin [73] established a scheduling model for this problem that considers the grade and temperature of molten steel, as well as the lifespan limitation of the intermediate ladle caused by the uncertainty of molten steel. To obtain a more efficient solution within a tolerable computing time, the NSGA-II algorithm was designed and optimized based on the characteristics of the problem. A multi-layer encoding was designed based on the furnace state, and feasible solutions were obtained by introducing furnace reassignment rules. Finally, calculate based on actual production data. The experiment shows that the proposed furnace redistribution rule is effective for SCC dynamic scheduling considering the uncertainty of molten steel in caster faults.

VI. Discussion and Conclusion

SCC scheduling is a special hybrid flow shop scheduling problem that requires strong time continuity. It is a hybrid flow shop (HFS)/flexible job shop (FJSP) scheduling problem, and it is difficult to achieve good results with only one research method. The combination of reinforcement learning methods, evolutionary computation algorithms, heuristic algorithms, and other algorithms is an effective way to solve such scheduling problems. Reinforcement learning is a method of learning optimal behavioral strategies through the interaction between agents and their environment. In SCC scheduling, reinforcement learning can be used to optimize production sequence and resource allocation. The advantage of reinforcement learning methods is that they can adapt to complex and changing environments, and improve scheduling efficiency by continuously learning and adjusting strategies. However, the training process of reinforcement learning algorithms typically requires a large amount of data and computational resources, and their results are limited by the representativeness of the training data. Evolutionary computation algorithm is an optimization method based on the theory of biological evolution, including genetic algorithm, genetic programming, ant colony algorithm, etc. In SCC scheduling, evolutionary computation algorithms can search for optimal solutions by simulating natural evolutionary processes. The advantage of evolutionary computing algorithms is that they do not require complex mathematical models and can handle complex optimization problems. However, evolutionary computation algorithms typically require a large number of iterations and computational resources, and their convergence speed and quality are limited by the design and parameter settings of the algorithm. Heuristic algorithm is an algorithm based on problem specific knowledge and experience, which guides the search process through heuristic rules. In steelmaking and continuous casting scheduling, heuristic algorithms can generate feasible scheduling plans based on experience and expert knowledge. The advantage of heuristic algorithms is that they have high computational efficiency and can quickly generate feasible scheduling solutions. However, the performance of heuristic algorithms is limited by the quality and coverage of heuristic rules, and may not be able to find the global optimal solution. In summary, reinforcement learning methods, evolutionary computing algorithms, and heuristic algorithms all have their unique advantages and limitations in steelmaking and continuous casting scheduling. In order to achieve better scheduling results, it is possible to consider combining these methods to leverage their respective advantages and form a comprehensive scheduling optimization method. For example, a heuristic algorithm can be used to generate an initial

scheduling plan, then an evolutionary computation algorithm can be used to optimize the plan, and finally reinforcement learning methods can be used to further adjust and optimize the scheduling strategy.

Based on previous research methods, this article provides a detailed introduction to the application of intelligent algorithms in SCC scheduling. Next, the research ideas of "rule+algorithm" and artificial intelligence algorithms are proposed for static scheduling and dynamic scheduling, respectively. Static scheduling should consider the constraints of overhead cranes and steel ladles, refine the scheduling model, combine rule and algorithm solving, determine the production mode by rules, and then use algorithms to solve; For dynamic scheduling, a single process operation or regulation research is no longer able to cope with complex production processes. Therefore, in the future, it is necessary to strengthen the collaboration between product quality and multiple processes and production processes, which can be of great significance for achieving the intelligence, efficiency, and coordination of the SCC scheduling process.

References

[1] Yin R Y. Metallurgical Process Engineering [M]. Beijing: Metallurgical Industry Press, 2009.

[2] Xue Y, Li J, Xue S R, et al. Analysis of development situation and discussion of transformation for iron and steel industry in China [J]. Research on Iron and Steel, 2016, 44(3): 53-56.

[3] Ding J L, Yang C E, Chen Y D, et al. Research progress and prospects of intelligent optimization decision making in complex industrial process [J]. Acta Automatica Sinica, 2018, 44(11): 1931-1943.

[4] Sabuncuoglu I, Goren S. Hedging production schedules against uncertainty in manufacturing environment with a review of robustness and stability research [J]. International Journal of Computer Integrated Manufacturing, 2009, 22(2): 138-157.

[5] Ouelhadj D, Petrovic S. A survey of dynamic scheduling in manufacturing systems [J]. Journal of Scheduling, 2009, 12(4): 417-431.

[6] Aytug H, Lawley M A, Mckay K, et al. Executing production schedules in the face of uncertainties: A review and some future directions [J]. European Journal of Operational Research, 2005, 161(1): 86-110.

[7] Jackson J R. Simulation research on job shop production [J]. Naval Research Logistics Quarterly, 1957, 4(4): 287-291.

[8] Gui W H, Wang C H, Xie Y F, et al. The necessary way to realize great-leap-forward development of process industries [J]. Bulletin of National Natural Science Foundation of China, 2015(5): 337-342.

[9] Zhao Z, Liu S, Zhou M, et al. Heuristic scheduling of batch production processes based on Petri nets and iterated greedy algorithms [J]. IEEE Transactions on Automation Science and Engineering, 2020, PP(99): 1-11.

[10] Zhao Z, Liu S, Zhou M, et al. Dual-objective mixed integer linear program and memetic algorithm for an industrial group scheduling problem [J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(6): 1199-1209.

[11] Liu G, Li T K. A steelmaking-continuous casting production scheduling model and its heuristic algorithm. Systems Engineering, 2002, 20(6): 44-48.

[12] Feng Z J, Yang G K, Du B, et al. Two stage optimization algorithms based on heuristic and linear programming in continuous casting scheduling [J]. Metallurgical Industry Automation, 2005(4): 18-22.

[13] Yu S P, Chai T Y. Heuristic scheduling method for Steelmaking continuous casting production process [J]. Control Theory and Applications, 2016, 33(11): 1413-1421.

[14] Sampson J R. Adaptation in natural and artificial systems (John H. Holland), 1976, Bulletin of Mathematical Biology, 1976, 38(2): 211–214.

[15] Fujii S, Tanimoto S, Tomiyama S, et al. Genetic algorithm with reduction of search space using operational constraints and its application to scheduling system for steelmaking process. Tetsu-to-Hagane, 2003, 89(12): 1220-1226.

[16] Xu Z J, Zheng Z, Gao X Q. HGA combined with priority strategy for production planning of steelmaking-continuous casting [J]. Control Decision, 2016, 31(8): 1394-1400.

[17] Yuan S P, Li T K, Wang B L. Improved fast elitist non-dominated sorting genetic algorithm for multi-objective steelmaking continuous casting production scheduling [J]. Computer Integrated Manufacturing Systems, 2019, 25(1): 115-124.

[18] Li T K, Su Z X. Two-stage genetic algorithm for SM-CC production scheduling [J]. Frontiers of Chinese Management Sciences, 2009, 17(5): 68-74.

[19] Dorigo M, Maniezzo V, Colorni A. Ant system: optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man and Cybernetics. Part B, 1996, 26(1): 29-41.

[20] Zhu D F, Zheng Z, Gao X Q. Hybrid genetic algorithm optimization-based production planning and simulation analysis for Steelmaking continuous casting [J]. Computer Engineering and Applications, 2010, 46(1): 241-245.

[21] Fang Y D, Wang F, Wang H. Research of multi-objective optimization study for job shop scheduling problem based on grey ant colony algorithm [J]. International Conference on Advanced Design and Manufacturing Engineering, 2011, 308-311: 1033.

[22] Xue Y C, Zheng D L, Yang Q W. Optimum charge plan of steelmaking continuous casting based on the modified discrete particle swarm optimization algorithm [J]. Computer integrated manufacturing system, 2011, 17(7): 1509-1517.

[23] Zheng P, Tang Q H, Zhang Q M, et al. Discrete particle swarm optimization for steelmaking and continuous casting production [J]. Mechanical Design and Manufacture, 2016(7): 49-51.

[24] Zarandi M H F, Dorry F. A hybrid fuzzy PSO algorithm for solving steelmaking-continuous casting scheduling problem [J]. International Journal Of Fuzzy Systems, 2017, 20(15): 1-17.

[25] Pan Q K. An effective co-evolutionary artificial bee colony algorithm for steelmaking-continuous casting scheduling [J]. European Journal of Operational Research, 2016, 250(3): 702-714.

[26] Peng K K, Pan Q K, Zhang B. An improved artificial bee colony algorithm for steelmaking-refining-continuous casting scheduling problem [J]. Chinese Journal Of Chemical Engineering, 2018, 26(8): 1727-1735.

[27] Glover F, Greenberg H. New approaches for heuristic search: a bilateral linkage with artificial intelligence [J]. European Journal of Operational Research, 1989, 39(2): 119-130.

[28] Yu G, Tian N Y, Xu A J. Computer-aided simulation of steelmaking-continuous casting production scheduling [J].

Journal of University of Science and Technology Beijing, 2009, 31(9): 1183-1188.
[29] Zhang Q, Manier H, Manier M A. A genetic algorithm with tabu search procedure for flexible job shop scheduling with transportation constraints and bounded processing times [J]. Computers & Operations Research, 2012, 39(7): 1713-1723.
[30] Kirkpatrick S, Gellatt C D, Vecchi M P. Optimisation by simulated annealing. Science, 1983, 220(4598): 671-679.
[31] Zhao W. Job-shop scheduling based on genetic algorithm and simulated annealing algorithm [J]. Computer Simulation, 2011, 28(7): 361-364.
[32] Shivasankaran N, Kumar P, Raja K V. Hybrid sorting immune simulated annealing algorithm for flexible job shop scheduling [J]. Computer Integrated Manufacturing Systems, 2015, 8(3): 455.
[33] Yang Z, Qiu H L, Luo X W, et al. Simulating schedule optimization problem in steelmaking continuous casting process [J]. International Journal of Simulation Modelling, 2015, 14(4): 710-718.
[34] Wu Y L, Zeng J C, Wei J H, et al. Dynamic scheduling algorithm for batch process systems based on hybrid Petri nets [J]. Journal of Xi'an Jiaotong University, 2002, 36(2): 147-151.
[35] Liao S H. Expert system methodologies and applications-a decade review from 1995 to 2004. Expert Systems with Applications, 2005, 28(1): 93-103.
[36] Sun F Q, Tang L X, Zheng B L. The steelmaking-continuous casting production scheduling based on expert system [J]. Metallurgical Industry Automation, 1998(6): 31-33.
[37] Ma C B. Research on the Simulation Methods of Crane Scheduling in Steel Plants Based on Multi-Agent [D]. Kunming: Kunming University of Science and Technology, 2011.
[38] Gu X J, Zhu Z Y, Zhang J, et al. Multi agent ant colony optimization for dynamic scheduling of Steelmaking continuous casting [J]. Science Technology and Engineering, 2016, 16(27): 50-57.
[39] Yu S P, Pang X F, Chai T Y, et al. Research on production scheduling for Steelmaking continuous casting with processing time uncertainty [J]. Control and Decision, 2009, 24(10): 1467-1472.
[40] Yu S P, Chai T Y. Rescheduling method for starting time delay in Steelmaking continuous casting production processes [J]. Acta Automatica Sinica, 2016, 42(3): 358-374.
[41] Liu L J, Wen Z, Su F Y, et al. Research and application of hybrid integrated scheduling management system of steelmaking-casting-rolling [J]. Metallurgical Industry Automation, 2014, 38(1): 28-34.
[42] Pang X F, Gao L, Pan Q K, et al. Rescheduling method of Steelmaking continuous casting with break down of converter or refining furnace [J]. Control and Decision, 2015, 30(11): 1921-1929.
[43] Yu S P, Chai T Y, et al. Dynamic Optimal Scheduling Method and Its Application for Converter Fault in Steelmaking continuous casting Production Process [J]. IFAC ProceedingsVolumes, 2011, 44(1): 9506-9511.
[44] Wang B L, Li T K, Zhang C S, et al. Dynamic CSP based scheduling algorithm for Steelmaking continuous casting with conticaster breakdown [J]. Computer Integrated Manufacturing Systems, 2011, 17(10): 2185-2194.
[45] Long J Y, Zheng Z, Gao X Q. Dynamic scheduling in steelmaking-continuous casting production for continuous caster breakdown [J]. International Journal of Production Research, 2017, 55(11): 3197-3216.
[46] Pan R L, Hu B G, Cao J H, Liu D L, et al. Heating furnace and hot rollinginterval rescheduling based on simulation optimization [J]. Computer Integrated Manufacturing Systems, 2014, 20(6): 1405-1415.
[47] Pang X F, Jiang Y C, Yu S P, et al. Flexible job shop rescheduling method of steelmaking-continuous casting base on human-computer cooperation [J]. Computer Itegrated Manufacturing Systems, 2018, 24(10): 2415-2427.
[48] Ning S S, Wang W, Pan X J. A dynamic scheduling algorithm based on just-in-time principle for steelmaking-continuous casting process [J]. Information and Control, 2007(1): 56-62.
[49] Guo Y X, Li T K, Zhang W X. Dy-namic scheduling of hot rolling based on human-com-puter interaction [J]. Computer Engineering and Design, 2012, 33(1): 367-371.
[50] Zhang C S, Li T K. Study on the dynamic coordination between steelmaking-continuous casting scheduling and hot rolling scheduling [J]. Metallurgical Industry Automation, 2016, 40(5): 19-25.
[51] Lu Y M, He D F, Xu A J, et al. Dynamic scheduling simulation system based on integrated production of SM-CC-HR [J]. Metallurgical Industry Automation, 2010, 34(6): 33-38.
[52] Shan D, Lu Y M, Xu A J. Study on strategies and methods of dynamic scheduling based on SM-CC-HR integrated production [J]. Control Engineering of China, 2012, 19(1): 20-24.
[53] Huang H, Chai T Y, Zheng B L, et al. Design and development of molten iron scheduling simulation system [J]. Journal of System Simulation, 2012, 24(6): 1192-1199.
[54] Wang C, Liu Q, Wang B, et al. Scheduling model of steelmaking continuous casting processes in special steel plants [J]. Journal of University of Science and Technology Beijing, 2013, 35(3): 371-378.
[55] Wang G, Wang B, Wang B, et al. Scheduling model for steelmaking-continuous casting process based on "furnace-caster matching" principle [J]. Journal of University of Science and Technology Beijing, 2013, 35(8): 1080-1092.
[56] Lee HS, et al. Primary production scheduling at steelmaking Industries [J]. Ibm Journal of Research & Development, 1996, 40(2): 231-252.
[57] Tang L X, Liu J Y, Rong A Y, et al. A review of planning and scheduling systems and methods for integrated steel production [J]. European Journal of Operational Research, 2001, 133(1): 1-20.
[58] Pang X F, Yu S P, Zhang Z Y, et al. Optimal rescheduling method for steelmaking-continuous casting, Journal of Systems Engineering, 2010, 25(1): 98-103+144.
[59] Zhao Z Y, Zhou M C, Liu S X. Iterated greedy algorithms for flow-shop scheduling problems: A tutorial [J]. IEEE Transactions on Automation Science and Engineering, 2021, PP(99): 1-19.
[60] Long J Y, Zheng Z, Gao X Q, et al. Production re-planning based on genetic algorithm for steelmaking-continuous casting [J]. Journal of University of Science and Technology Beijing, 2014, 36(1): 115-122.
[61] Long J Y, Zheng Z, Gao X Q. Dynamic scheduling in steelmaking-continuous casting production for continuous caster breakdown [J]. International Journal of Production Research, 2017, 55(11): 3197.
[62] Xiong W, Fu D M, Gu X J, et al. Based on immune multi-agent system to resolve dynamic scheduling problem of Steelmaking continuous casting (to be continued) [J]. Metallurgical Industry Automation, 2014, 38 (3): 24-28.

[63] Xiong W, Fu D M, Gu X J, et al. Based on immune multi-agent system to resolve dynamic scheduling problem of Steelmaking continuous casting (end) [J]. Metallurgical Industry Automation, 2014, 38(4): 7-10.

[64] Tang L, Zhao Y, Liu J. An improved differential evolution algorithm for practical dynamic scheduling in steelmaking-continuous casting production [J]. IEEE Transactions on Evolutionary Computation, 2014, 18(2): 209-225.

[65] Peng K K, Deng X, Zhang C, et al. An improved imperialist competitive algorithm for hybrid flowshop rescheduling in steelmaking-refining-continuous casting process, Measurement & Control, 2020, 53 (9/10): 1920-1928.

[66] Ding S, Li T K, Shi C T. Study of hybrid flow shop rescheduling with consideration of machine breakdown [J]. Computer Engineering and Applications, 2012, 48(23): 234-238.

[67] Li J Q, Pan Q K, Mao K. A hybrid fruit fly optimization algorithm for the realistic hybrid flowshop rescheduling problem in steelmaking systems [J]. IEEE Transactions on Automation Science and Engineering, 2016, 13(2): 932-949.

[68] Liu W T, Zhang Q, Sun S Q. Research on rescheduling problem of steel factory [J]. Metallurgical Industry Automation, 2004, 28(6): 5-8.

[69] Qian Q F, Chen W D. Research on rescheduling model and algorithm in the iron and steel scrap remanufacturing taking the EAF's steel delay into considerations [J]. Industrial Engineering and Management, 2016, 21(5): 28-34+41.

[70] Wang C, Liu Q, Wang B, et al. Scheduling model of steelmaking-continuous casting processes in special steel plants [J]. Journal of University of Science and Technology Beijing, 2013, 35 (3): 371-378.

[71] Jiang S L, Zheng Z, Liu M. A multistage dynamic soft scheduling algorithm for the uncertain steelmaking-continuous casting scheduling problem [J]. Applied Soft Computing, 2017, 60: 722-736.

[72] Jiang S L, Wen Y M, Tang W, Peng G Z. A scheduling optimization method for Steelmaking continuous casting considering energy constraints [J]. Journal of Huazhong University of Science and Technology.(Natural Science Edition), 2022, 50(06): 118-123+132.

[73] Song Y Q. Steelmaking and Continuous Casting Dynamic Scheduling of Continuous Caster Faults with Molten Steel Uncertainty Constraints [J]. Value Engineering, 2023, 42 (04): 138-141.

[74] Peng K K, Pan Q K, Gao L, et al. An improved artificial bee colony algorithm for real-world hybrid flowshop rescheduling in steelmaking-refining-continuous casting process [J]. Compute& Industrial Engineering, 2018, 122: 235-250.

[75] Zhou T, Shao X, Gao S, et al. Steel making continuous casting rescheduling based on smelting equipment failures [J]. Metallurgical Industry Automation, 2023, 47(06): 45-46.

[76] Wang J Y, Wang Q, Sun W Q. Optimal power system flexibility-based scheduling in iron and steel production: A case of steelmaking–refining–continuous casting process [J]. Journal of cleaner production, 2023, 414(Aug.15): 137619.1-137619.9.

[77] Pan R L, Wang Q, Cao J H. Zhou C L. Deep reinforcement learning for solving steelmaking-continuous casting scheduling proble ms under time-of-use tariffs [J]. International Journal of Production Research, 2024, 62(1/2): 404-420.

[78] Liu R K, et al. Deep reinforcement learning for dynamic scheduling of a flexible job shop [J]. International Journal of Production Research, 2022, 60(13): 4049-4069.

[79] Cai J C, et al. A novel shuffled frog-leaping algorithm with reinforcement learning for distributed assembly hybrid flow shop scheduling [J]. International Journal of Production Research, 2023, 61(4): 1233-1251.

[80] Sabri A, et al. Reinforcement learning and stochastic dynamic programming for jointly scheduling jobs and preventive maintenance on a single machine to minimise earliness-tardiness [J]. International Journal of Production Research, 2024, 62(3): 705-719.

[81] Lee J H, Kim, H J. Reinforcement learning for robotic flow shop scheduling with processing time variations [J]. International Journal of Production Research, 2022, 60(7): 2346-2368.

Xinbo Song was born in Shenyang. He is currently pursuing a Master's degree in Electronic Information at Shenyang University of Aeronautics and Astronautics. His research interests include scheduling optimization. (Email: 2104599274@ qq.com)

Yang Yu received the the Ph.D. degree in control science and engineering from North-eastern University, Shenyang, China, in 2018. He is currently a Lecturer with School of Automation, Shenyang Aerospace University, Shenyang, China. His research interests include process control in complex industrial system.(Email: 20180029@sau.edu.cn)

Liangliang Sun received PhD degrees in control theory and control engineering from Northeastern University, China in 2015. He is currently serving as Professor and Associate Dean at the School of Control Engineering, Northeastern University at Qinhuangdao, China. His current research interests include management decision optimization and intelligent production manufacturing. (Email:sun liangliang@neuq.edu.cn)

Sheng-Long Jiang received a Ph.D. degree in control science and engineering from the Department of Automation, Tsinghua University, Beijing, China. His current research interests mainly include mathematical modelling, data-driven optimization approaches. (Email: jiang_shl@cqu.edu.cn)

TD3-based Stochastic Workload Offloading for 5G-based Cloud Control System

LI Sha[1], SUN Lei[2], WANG Jianquan[3], MA Zhangchao[4], FU Meixia[5], ZHANG Lifang[6], HUANG Rong[7]

***Abstract*—With the intelligent transformation of Industry 4.0, the limitation of programmable logic controller (PLC) as the core equipment of industrial control has become an obstacle to the development of industrial automation. Cloud PLC is a key technology which supports virtualization deployment of multiple PLCs in a central cloud server and interacts with remote actuators through 5G communication networks. However, it's an issue about how to make full use of communication and computation resources to bear as many control workloads as possible in this scenario. To this end, this paper proposes a cloud control system for control workloads. Each control workload can be partially processed locally and remotely in parallel. Then, this paper considers the deadline of control workload and the limited resources as constraint boundaries, and proposes a stochastic workload offloading scheme based on the deep reinforcement learning (DRL). The scheme utilizes the twin delayed deep deterministic policy (TD3) scheme to optimize the workload distribution and network resource allocation to guarantee workload execution success rate. The simulation results demonstrate that the proposed algorithm in terms of average system energy consumption outperforms other benchmark ones.**

***Keywords*—5G, central PLC, cloud control system, deep reinforcement learning, stochastic workload offloading**

I. INTRODUCTION

The industrial internet of things (IIoT) is a new networked paradigm to motivate modern industrial control production moving toward Industry 4.0[1,2]. A typical characteristic of Industry 4.0 is intelligent manufacturing. Programmable logic controller (PLC) is the core equipment of industrial control, serving as the heart of industrial automation and playing a crucial role in Industry 4.0. Traditional industrial control workloads have a small amount of computational data, only simple functions can be implemented. With the advent of Industry 4.0, new applications have emerged in industrial production, such as image recognition, object detection, and other high-volume computing workloads [3-5]. However, traditional PLCs have limited computation capabilities, making it difficult to run complex control algorithms and intelligent models. This limitation hinders the integration of artificial intelligence (AI) models with traditional PLCs, which has become a bottleneck in improving the intelligent level of industrial control [6,7]. Furthermore, PLCs are typically connected to devices through specialized industrial fieldbus technologies. The communication standards of the industrial field create information exchange barriers for collaborative interaction among

traditional PLC devices. Cloud control system achieves software-based control on a general computing platform, enabling partial decisions to be computed on a centralized cloud platform. The decision results are transmitted to remote actuators through wireless networks. The cloud control system can dynamically allocate computing resources according to workloads, which makes industrial control more flexible and scalable [8]. However, the network performance is essential for the stability and reliability of cloud control system. Recently, with development of deterministic such as 5G ultra–reliable low latency communication (uRLLC), the cloud control system is starting to be applied in practice to shorten transmission delay [9].

In recent years, computation offloading has been extensively investigated in IIoT systems. In [10-13], these literatures mainly focused on offloading decision-making with a deterministic task arrival model. In [14], the authors considered a stochastic task arrival model and proposed a stochastic computing offloading algorithm to minimize the long-term energy consumption. However, the authors neglect the deadline constraints of all tasks. In actual industrial automation system, the control workloads need processing within a strict deadline. This is because the control workloads have a strict logical relationship with each other, and have a significant impact on production safety. Unexpected delays or workload interruptions can cause huge production losses [15,16]. The authors constructed a virtual queue using Lyapunov optimization techniques to ensure task deadline in [17], the virtual queues are used to assist actual task queues reduce the average traffic delay. The authors assume that the mobile edge cloud (MEC) server has sufficient computing resources, the execution delay of the server is ignored. However, the computation resources of the server are finite, task offloading delay should take into account both the traffic delay and the execution delay.

A critical challenge in industrial control system research is the development of efficient computing offloading schemes that effectively distribute workloads of multiple industrial control devices. Deep reinforcement learning (DRL) is an emerging technique that showed high performance when applied on solving the task offloading problem [18,19]. DRL differs from traditional optimization solutions because it leverages the knowledge learned in past optimizations, which is beneficial in highly dynamic and time-varying scenarios. Some existing articles have used DRL to optimize task offloading in IIoT networks, medical networks and vehicle networks. For example, the authors in [14] proposed an asynchronous actor-critic (AAC) algorithm to minimize the long-term energy efficiency. The authors in [20] proposed a deep Q-learning network (DQN) based frame aggregation and task offloading scheme to reduce average delay and system energy consumption. The authors in [21] proposed a deep deterministic policy gradient (DDPG) based computation offloading and power allocation scheme to minimize latency in a mobile edge computing system. In [22], the authors utilized dual-critic deep deterministic policy gradient (DC-DDPG) to tackle computation offloading and resource allocation problems aimed at minimizing the computational cost. In [23], the authors proposed a proximal policy optimization (PPO) to select the edge node for task execution to obtain long-term benefits. For the field of intelligent logistics, the authors in [24] investigated a federated edge collaborative computation (FECC) offloading framework to guarantee the delay tolerance of the tasks. However, few literatures pay attention on resource allocation and

offloading of industrial control workloads through deep reinforcement learning.

To cover this unexplored area in the research, an adaptive workload offloading scheme in a 5G-based cloud control system with a deep reinforcement learning model is investigated. The main contributions of this paper are listed as:

1). A two-level cloud control system based on 5G is proposed. It enables controllers at 5G MEC and local computing nodes to collaborate, efficiently processing massive control workloads.

2). A service model is the first to attempt to characterize the control workload arrival feature. The high randomness, computationally intensive, and strict millisecond level deadline of control workloads are considered by the service model. The workload offloading problem in the 5G-based control system is formulated as a consecutive non-convex optimization problem of minimizing average system energy consumption.

3). To solve the formulated optimization problem, a twin delayed deep deterministic policy (TD3) model is utilized to effectively explore the environment and action space. Subsequently, the model is trained to optimize offloading decisions, including the determination of transmission power allocation and offloading ratios, guided by a strategically designed reward function.

This work is supported by the National Key Research and Development Program of China with Grant No. 2020YFB1708800; the Guangdong Provincial Key R&D Program with Grant No. 2020B0101130007; the National Foreign experts Project with Grant No. G2023105035L.

II. THE PROPOSED METHOD

In this section, the system model and optimization problem are formulated. Firstly, a 5G-based two-level cloud control system model is proposed. Based on this system model, the workload model, local-PLC (L-PLC) computing model, and central-PLC (C-PLC) computing model are designed, respectively. Then, the workload offloading problem in the 5G-based control system is formulated as a consecutive non-convex optimization problem of minimizing average system energy consumption. To tackle the formulated problem, the optimization problem is converted to a Markov decision process. Furthermore, the state space, action space, and reward function are well-designed. Finally, the detailed process of using the TD3 algorithm to optimize the workload offloading ratio and transmission power allocation is described.

A. SYSTEM MODEL

A 5G-based cloud control system is shown in Fig.1, it usually designs two-level controller to balance efficiency and reliability, C-PLC is deployed in 5G MEC to process large volumes of control workloads, and L-PLCs are deployed in local computing nodes nearing actuators to process control workloads with time-critical requirements. The C-PLC communicates with multiple L-PLCs via 5G, enabling collaborative processing of control workloads between the C-PLC and L-PLCs. Therefore, offloading some control workloads to the C-PLC may be necessary for L-PLCs to work efficiently and prolong their battery life.

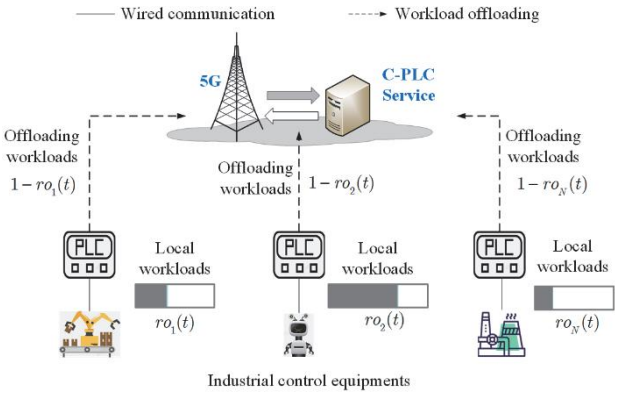


Figure 1 A 5G-based cloud control system

A 5G-based cloud control system consists of one 5G base station, one C-PLC and N L-PLCs, where $\mathcal{N}=\{1,2,\ldots,N\}$. We assume that each L-PLC has the same computation capacity, meanwhile, the whole working time of cloud control system is separated into several computing period with same duration τ, where $t\in\mathcal{T}=\{1,2,\ldots,T\}$. To facilitate modeling, the mini-slot for resource allocation in 5G is 1 ms, the system maintains static updates based on the resources allocated in the first millisecond within each computing period.

B. WORKLOAD MODEL

At the beginning of computing period t, each industrial control equipment generates a workload, and each workload is represented by $d_{j,t}$ and $ddl_{j,t}$, which denotes the data volume of workload and deadline of workload. Without loss of generality, we assume that the generation of workload follows the Poisson distribution with mean $E(d_{j,t})=d$ (bits\period) and the workload can be arbitrarily partitioned into two independent parts. $d_j^{\mathrm{la}}(t)$ is the data volume of workload processed locally for the jth L-PLC, which is computed as

$$d_j^{\mathrm{la}}(t)=ro_j(t)\cdot d_{j,t} \tag{1}$$

Where $ro_j(t)\in[0,1]$ is a stochastic workload offloading ratio. Therefore, the data volume of workload $d_j^{\mathrm{eg}}(t)$ offload to C-PLC is defined as:

$$d_j^{\mathrm{eg}}(t)=(1-ro_j(t))\cdot d_{j,t} \tag{2}$$

C. L-PLC COMPUTING MODEL

During the computing period t, the local computation resource used to process the workload of the jth L-PLC processes one bit of workload. $T_j^{\mathrm{la}}(t)$ is the processing time of local workload, which can be defined as

$$T_j^{\mathrm{la}}(t)=\frac{d_j^{\mathrm{la}}(t)\cdot c}{f_{j,t}}=\frac{ro_j(t)\cdot d_{j,t}\cdot c}{f_{j,t}} \tag{3}$$

The corresponding energy consumption is calculated as:

$$E_j^{\mathrm{la}}=\kappa(f_{j,t})^2\cdot d_j^{\mathrm{la}}(t)\cdot c \tag{4}$$

Where $\kappa(f_{j,t})^2$ denotes the energy consumption of unit CPU cycle, which depends on the chip architecture of L-PLC[14].

D. C-PLC COMPUTING MODEL

The offloading workload d_j^{eg} of the jth L-PLC is offloaded to the C-PLC server via 5G. We assume the 5G allocates the equal communication bandwidth W to each L-PLC. According to Shannon's formula, the uplink transmission rate of the jth L-PLC during the computing period t can be defined as:

$$rt_j(t)=W\log_2\left(1+\frac{p_j(t)\cdot h_{j,t}\cdot D_j^{-\beta}}{\sigma^2}\right) \tag{5}$$

Where $p_j(t)$ represents the transmission power of

L-PLC, $h_{j,t}$ is the radio channel gain, D_j represents the distance from L-PLC to 5G, β denotes path loss coefficient, σ^2 is the noise power. The corresponding transmission delay is expressed as:

$$T_j^{\text{tran}}(t) = \frac{d_j^{\text{eg}}(t)}{rt_j(t)} \tag{6}$$

The energy consumption related to workload transmission is calculated as:

$$E_j^{\text{of,tran}}(t) = p_j(t) \cdot T_j^{\text{tran}}(t) \tag{7}$$

In the C-PLC, the maximum processing delay of the offloading workload $d_j^{\text{eg}}(t)$ during computing period t is computed as:

$$T_j^{\text{cmp,max}}(t) = ddl_{j,t} - T_j^{\text{tran}}(t) \tag{8}$$

According to the processing delay $T_j^{\text{cmp,max}}$ and the computation capacity of C-PLC f_t^{e}, the computation resource of C-PLC allocated for workload $d_j^{\text{eg}}(t)$ is defined as:

$$f_j^{\text{cmp}}(t) = \max\left\{\frac{d_j^{\text{eg}}(t)\cdot c}{T_j^{\text{cmp,max}}}, \frac{d_j^{\text{eg}}(t)}{\sum_{j=1}^{N} d_j^{\text{eg}}(t)} \cdot f_t^{e}\right\} \tag{9}$$

The energy consumption to process workload $d_j^{\text{eg}}(t)$ is expressed as [25]

$$E_j^{\text{of,cmp}}(t) = \xi(f_j^{\text{cmp}}(t))^2 \cdot d_j^{\text{eg}}(t) \cdot c \tag{10}$$

Where $\xi(f_j^{\text{cmp}}(t))^2$ denotes the energy consumption for unit CPU cycle on C-PLC server. Thus, the energy consumption for processing the offloading workload $d_j^{\text{eg}}(t)$ is expressed as:

$$E_j^{\text{off}}(t) = E_j^{of,tran}(t) + E_j^{\text{of,cmp}}(t) \tag{11}$$

In this work, the energy consumption of transmission computation results to the L-PLC are ignored.

E. PROBLEM FORMULATION

A cost function $C(t)$ is defined to describe the whole system energy consumption:

$$C(t) = \sum_{j\in\mathcal{N}} C_j(t) \tag{12}$$

$$C_j(t) = E_j^{\text{la}}(t) + E_j^{\text{of,tran}}(t) + E_j^{\text{of,cmp}}(t) \tag{13}$$

The optimization problem of this work is to minimize average system energy consumption in a 5G-based cloud control system, which can be formulated as:

$$\text{P1}: \min_{ro(t),p(t)} C_{\text{avg}} = \frac{1}{|\mathcal{T}|}\sum_{t\in\mathcal{T}} C(t) \tag{14}$$

Subject to:

$$\text{C1}: ro_j(t) \in [0,1]$$
$$C2: 0 \le p_j(t) \le p_{j,t}^{\max}$$
$$\text{C3}: \sum_{j\in\mathcal{N}} f_j^{\text{cmp}}(t) \le f_t^{\text{e}}$$
$$\text{C4}: \max\left\{T_j^{\text{la}}(t), T_j^{\text{tran}}(t) + \frac{d_j^{\text{eg}}(t)\cdot c}{f_j^{\text{cmp}}(t)}\right\} \le ddl_{j,t}$$

Constraints C1 and C2 mean the workload offloading ratio and transmission power constraints, respectively. Constraint C3 means that the required computation resources of all offloading workloads should not exceed the computation capacity of C-PLC. Constraint C4 means that the processing delay of workload cannot exceed its deadline.

F. TD3-BASED STOCHASTIC OFFLOADING

As aforementioned, the formulated consecutive non-convex optimization problem P1 is difficult to solve. The TD3 algorithm introduces new techniques such as twin Q-networks, delayed updates, and target policy noise to enhance the stability and convergence of the algorithm, as well as its exploration capabilities in the environment. It is a powerful tool for solving optimization problems in an environment with continuous action spaces. To tackle the optimization

problem P1, it is formulated as a Markov decision process problem, and the TD3 algorithm is utilized to optimize the workload offloading ratio and transmission power allocation solutions. In this work, the TD3 algorithm is considered as an agent. The agent interacts in real-time with the 5G-based cloud control system, as illustrated in Fig.2. The agent is a logical function entity, it may be deployed at the base station physically.

1)State Space: at the computing period t, we can construct system state $\mathbf{s}_t$ as:

$$\mathbf{s}_t = \{\mathbf{d}_t, \mathbf{dt}_t, \mathbf{h}_t, \mathbf{p}_t^{\max}, \mathbf{f}_t^{\mathrm{lo}}, f_t^{\mathrm{e}}\} \tag{15}$$

Where $\mathbf{d}_t = \{d_{j,t} \mid j \in \mathcal{N}\}$ is the workloads vector, $\mathbf{dt}_t = \{ddl_{j,t} \mid j \in \mathcal{N}\}$ denotes as the deadline of workloads vector, $\mathbf{h}_t = \{h_{j,t} \mid j \in \mathcal{N}\}$ represents the radio channel gain for each L-PLC, $\mathbf{p}_t^{\max} = \{p_{j,t}^{\max} \mid j \in \mathcal{N}\}$ is the maximum transmission power for each L-PLC, the allocated computation resource for each L-PLC is denoted as $\mathbf{f}_t^{\mathrm{lo}} = \{f_{j,t} \mid j \in \mathcal{N}\}$, f_t^{e} denotes the allocated computation resources of C-PLC server at computing period t.

2)**Action**: Based on the system state $\mathbf{s}_t$, the agent will output an action $\mathbf{a}_t$ at computing period t:

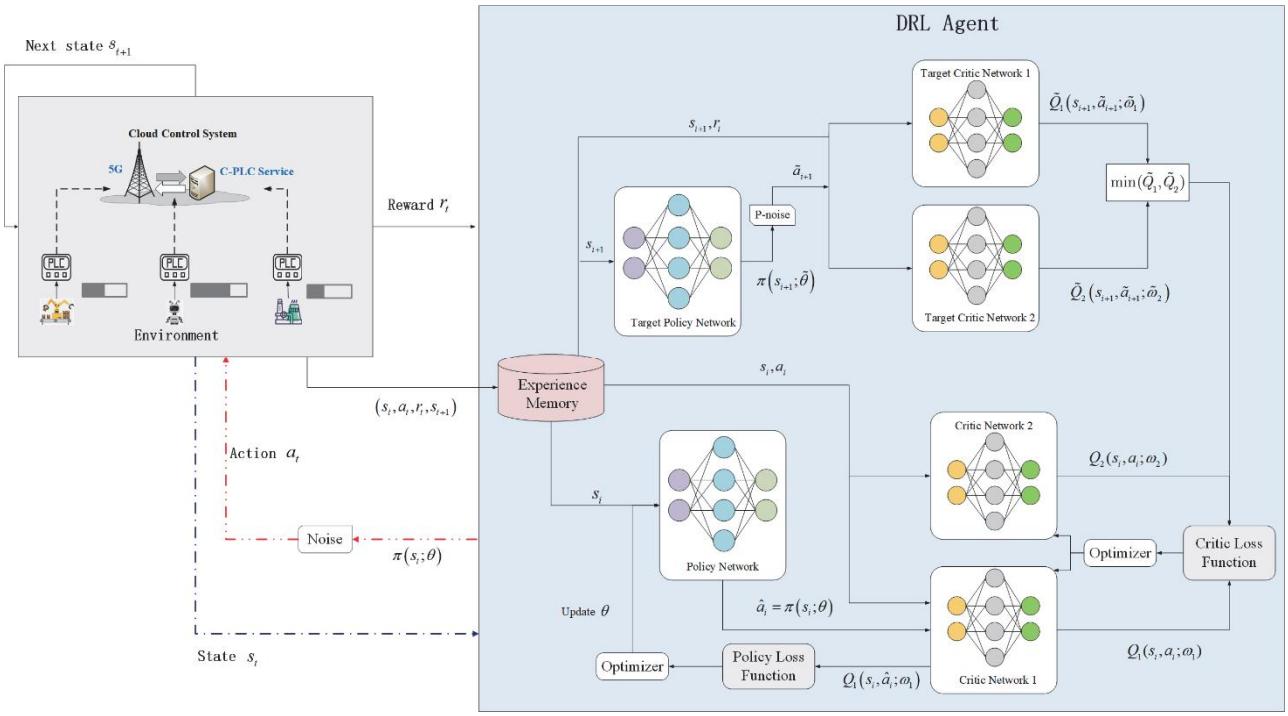


Figure 2 The illustration of the TD3 framework

$$\mathbf{a}_t = \{\mathbf{ro}_t, \mathbf{p}_t\} \tag{16}$$

According to choosing action $\mathbf{a}_t$, the environment can calculate the data transmission rate for each L-PLC at computing period t, and obtain the computation resources that C-PLC server allocates for each L-PLC, i.e., $\mathbf{f}_t = \{f_{j,t}^{\mathrm{cmp}} \mid j \in \mathcal{N}\}$.

3)**Reward**: after executing action $\mathbf{a}_t$, the environment update system state from $\mathbf{s}_t$ to $\mathbf{s}_{t+1}$, and the agent receives a scaler reward r_t from the environment. This reward r_t can be defined as the goal of P1 problem,

$$r_t = \sum_{j\in\mathcal{N}} \begin{cases} -C_j(t), & d_{j,t} \text{ successfully processed} \\ -100, & \text{otherwise} \end{cases} \tag{17}$$

In this work, the purpose of the agent is to maximize the long-time cumulative reward, which can be expressed as:

$$R(\mathbf{s},\mathbf{a}) = \max\left[\sum_{t=k}^{T} \gamma^{(t-k)} r_t\right] \tag{18}$$

Where $\gamma \in [0,1]$ is the discount factor which determines the balance of current and future rewards[21].

4)**TD3 Algorithm**: TD3 is a policy gradient-based DRL algorithm that can effectively solve continuous action space problems. As shown in Fig.2, the TD3 network employs the actor-critic framework, which consists of a policy network and twin critic networks, meanwhile, the TD3 network includes three target networks. Moreover, the TD3 network includes an experience memory $\mathcal{B}$, which disrupts the correlation between experiences to avoid inefficient learning[26]. The training process for the TD3 algorithm is shown in Algorithm 1.

For TD3 algorithm, the state $\mathbf{s}_i$ is inputted to the policy network, and then the policy network outputs an action $\mathbf{a}_i$, defined as:

$$\mathbf{a}_i = \hat{\mathbf{a}}_i + \chi \tag{19}$$

Where i is the random sample index, χ is the

Algorithm 1 TD3 Stochastic Workload Offloading

Input: Environment state $\mathbf{s}_t$ at each time slot *t*, and the structure of TD3 network.

Output: $\mathbf{ro}_t$, $\mathbf{p}_t$.

Initialize: experience memory $\mathcal{B}$, discount factor γ, std of gaussian exploration noise χ, frequency of delayed policy update fd, soft update coefficient ϑ;
Set iteration number *M*, max step *T*, and training interval *TR*;
for *episode*=1, 2, …, *M* **do**
    Initialize: environment parameters
    for *step*=1, 2, …, *T* **do**
        Generate state $\mathbf{s}_t$ from environment;
        Input $\mathbf{s}_t$ into policy network and obtain action $\mathbf{a}_t$;
        Execute $\mathbf{a}_t$ and observe r_t, $\mathbf{s}_{t+1}$;
        Store 4-tuple $(\mathbf{s}_t, \mathbf{a}_t, r_t, \mathbf{s}_{t+1})$ into $\mathcal{B}$;
        if *step* mod *TR* **then:**
            Randomly sample a batch size of data set from $\mathcal{B}$ and input TD3 network;
            Train twin critic networks and update the weights ω_1, ω_2 based on (23);
            if *step* mod fd **then:**
                Update the weight θ of policy network based on (20);
                Update the weights $\tilde{\theta}$, $\tilde{\omega}_1$, $\tilde{\omega}_2$ of target networks: $\tilde{\theta} \leftarrow \vartheta\theta + (1-\vartheta)\tilde{\theta}$, $\tilde{\omega}_1 \leftarrow \vartheta\omega_1 + (1-\vartheta)\tilde{\omega}_1$, $\tilde{\omega}_2 \leftarrow \vartheta\omega_2 + (1-\vartheta)\tilde{\omega}_2$
            end if
        end if
    end for
end for

Gaussian exploration noise, where $\hat{\mathbf{a}}_i = \pi(\mathbf{s}_i;\theta)$ is the explored workload offloading ratio and power allocation policy based on the policy network, θ denotes as the weight parameter of policy network and it is trained through the Eq.20:

$$\nabla_\theta J(\theta) = \mathrm{E}_\pi[\sum \nabla_\theta \pi(\mathbf{s}_i;\theta)\cdot \nabla_{\hat{\mathbf{a}}_i} Q_1(\mathbf{s}_i,\mathbf{a}_i;\omega_1)] \quad (20)$$

TD3 introduces twin target critic networks to estimate the target Q-value and chooses the minimum of their outputs as the target Q-value y_i, the target Q-value is estimated based on the experience 4-tuple $(\mathbf{s}_i,\mathbf{a}_i,r_i,\mathbf{s}_{i+1})$, which can be obtained through Eq.21and Eq.22:

$$\tilde{\mathbf{a}}_{i+1} = \pi(\mathbf{s}_{i+1};\tilde{\theta}) + \zeta, \zeta \leftarrow clip(N(0,\tilde{\sigma}),-e,e) \quad (21)$$

$$y_i = r_i + \gamma \min\{\tilde{Q}_1(\mathbf{s}_{i+1},\mathbf{a}_{i+1};\tilde{\omega}_1),\tilde{Q}_2(\mathbf{s}_{i+1},\mathbf{a}_{i+1};\tilde{\omega}_2)\} \quad (22)$$

Where $\tilde{\mathbf{a}}_{i+1}$ is estimated based on $\mathbf{s}_{i+1}$ by the target policy network, $\pi(\mathbf{s}_{i+1};\tilde{\theta})$ is the target policy network, $\tilde{\theta}$ is the weight parameters of the target policy network, ζ is the target policy noise, ζ follows a truncated normal distribution $clip(N(0,\tilde{\sigma}),-e,e)$, and $\zeta \in [-e,e]$. $Q_1(\tilde{\mathbf{s}}_{i+1},\tilde{\mathbf{a}}_{i+1};\tilde{\omega}_1)$ and $\tilde{Q}_2(\mathbf{s}_{i+1},\tilde{\mathbf{a}}_{i+1};\tilde{\omega}_2)$ are twin target critic networks, $\tilde{\omega}_1$ and $\tilde{\omega}_2$ are the weight parameters of twin target critic networks, respectively.

The state $\mathbf{s}_i$ and action $\mathbf{a}_i$ are outputted to twin critic networks for evaluation, two separate critic networks output the estimated Q-values $Q_1(\mathbf{s}_i,\mathbf{a}_i;\omega_1)$ with the weight ω_1 and $Q_2(\mathbf{s}_i,\mathbf{a}_i;\omega_2)$ with the weight ω_2, respectively. Twin critic networks are trained by minimizing the loss function, the loss function of twin critic networks can be expressed as:

$$L(\omega_1,\omega_2) = (Q_1(\mathbf{s}_i,\mathbf{a}_i;\omega_1) - y_i)^2 + (Q_2(\mathbf{s}_i,\mathbf{a}_i;\omega_2) - y_i)^2 \quad (23)$$

III. Results and Discussion

In this section, several simulations are proposed to verify the performance of the proposed stochastic workload offloading scheme. The simulation parameters are provided in Table.1.

Table 1 Simulation Parameters

parameter	value	parameter	value
d	40000bits/period	ξ	10^{-28}
τ	0.05s	f^{lo}	1GHz
c	100cycles/bit	f^{e}	10GHz
κ	10^{-11}	$p_{\max}$	1W
D	50m	γ	0.95
β	3	χ	0.1
σ^2	10^{-11}	$\tilde{\sigma}$	0.2
W	5MHz	e	0.5

The policy network of TD3 has three fully-connected layers with 256, 518, 518 neurons, respectively. And one output layer adopts activation function tanh. TD3 has two critic networks, each critic network has two fully-connected hidden layers with 518 neurons in each and one output layer with a neuron. The deadline of each workload is randomly chosen from $\{0.02,0.04,0.05,0.06,0.08\}(s)$. We set 1500 episodes and 1000 steps in the training stage. The capacity of the replay buffer is 10^8, and the batch size is 64.

TD3 introduces a delayed update mechanism, which updates the policy network and three target networks

after a certain period. This avoids overfitting of the policy network and reduces the error propagation to the target Q-value. Fig.3 shows that impact of delayed policy update frequency on the performance of TD3. We can see, when the delayed policy update frequency (fd) is 4, the reward of the TD3 algorithm converges to the highest value. Therefore, the best policy updates frequency is 4 for the proposed scheme.

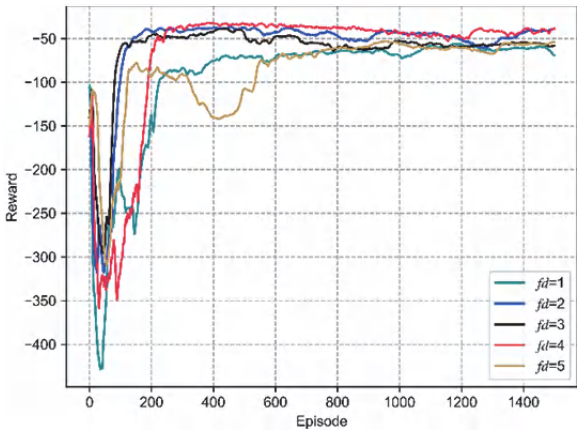


Figure 3 Impact of various updates frequency

The negative correlation between system computation cost and training episodes is depicted in Fig.4 with the different number of L-PLCs. The computation cost of a system rises as the number of L-PLCs becomes large, meanwhile, the convergence speed of TD3 becomes slower with the growth of L-PLC numbers. The reason is that the more L-PLCs require more communication and computation resources, which may increase the computational complexity of TD3 algorithm.

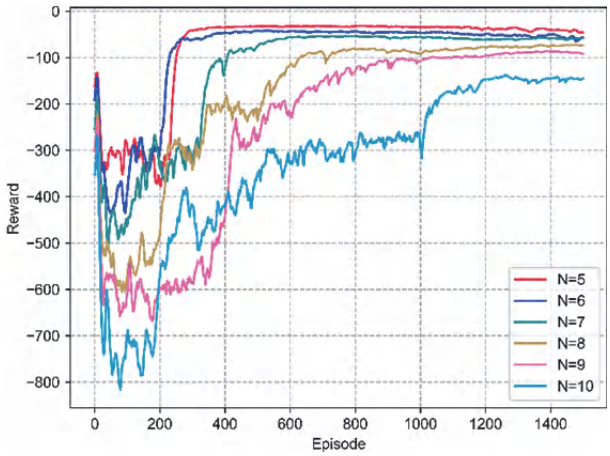


Figure 4 TD3's reward under different the number of L-PLCs

To evaluate the performance of the proposed scheme, three traditional offloading schemes are selected for comparison: (1) all L-PLC computing; (2) all C-PLC computing; (3) 0-1 offloading computing, the workload can be randomly processed on the L-PLC or C-PLC. Fig.5 and Fig.6 show the comparison of average computation cost and workloads execution success rate under different offloading schemes, respectively. It can be seen that under the condition of same workload arrival model, the average computation cost of the proposed offloading scheme is very small, and its performance is much better than other offloading schemes. As shown in Fig.6, the workloads execution success rate of the proposed and all L-PLC computing schemes can reach about 100%, however, the average computation cost of all L-PLC computing scheme is very large. By optimizing workload offloading ratio and transmission power allocation, the proposed offloading scheme can achieve the highest workload execution success rate with the lowest average computation cost.

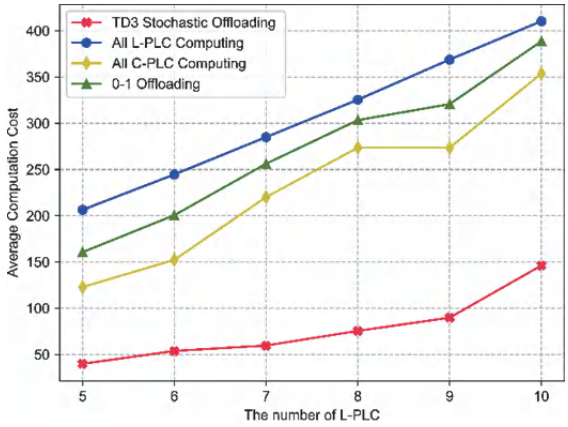


Figure 5 System average computation cost comparison

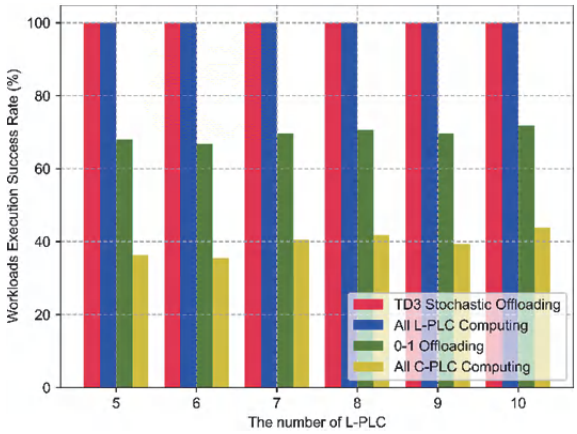


Figure 6 Workloads execution success rate comparison

VI. CONCLUSION

5G deterministic network can provide low latency and high reliable communication guarantee for industrial services, which enables central PLC in practice. In this work, we utilize a C-PLC and L-PLC collaborative computing model, which can decrease the whole cloud control system operational cost.

Moreover, to make the proposed 5G-based cloud control system processing control workloads more efficiently, we construct a stochastic model for the arrival of control workloads and propose a TD3-based stochastic workload offloading scheme to minimize the average system energy consumption by jointly optimizing the workload offloading ratio and transmission power allocation strategies. Simulation results indicates that the proposed deep reinforcement learning mode can achieve the highest workloads execution success rate while minimizing the average energy consumption.

References

[1] DENG X, YIN J, GUAN P, et al. Intelligent delay-aware partial computing task offloading for multiuser industrial internet of things through edge computing [J]. IEEE internet of things journal, 2023, 10(4): 2954-2966.

[2] XU S Y, LI Y M, GUO S Y, et al. Cloud–edge collaborative SFC mapping for industrial IoT using deep reinforcement learning [J]. IEEE transactions on industrial informatics, 2022, 18(6): 4158-4168.

[3] XU X L, SHEN B W, YIN X C, et al. Edge server quantification and placement for offloading social media services in industrial cognitive IoV [J]. IEEE transactions on industrial informatics, 2021, 17(4), 2910-2918.

[4] REN J, LIU J, ZHANG Y M, et al. An efficient two-layer task offloading scheme for MEC system with multiple services providers [C]. // IEEE INFOCOM 2022 - IEEE Conference on Computer Communications in United Kingdom, London, 2022: 1519-1528.

[5] KE H C, WANG H, SUN H B, et al. Deep reinforcement learning-based task offloading and service migrating policies in service caching-assisted mobile edge computing [J]. China communications, 2024, 21(4): 88-103.

[6] WANG J Q, MA Z C, SUN L, et al. Evolution, key technology, prospects, and applications of industrial network architecture [J]. Chinese journal of engineering, 2023, 45(8): 1376-1389.

[7] LIAO Y Z, SHOU L Q, YU Q, et al. An intelligent computation demand response framework for IIoT-MEC interactive networks [J]. IEEE networking letters, 2020, 2(3): 154-158.

[8] ANA L, CARMEN L M, IMANOL M, et al. Analysis of 5G-TSN Integration to Support Industry 4.0 [C]. // 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) in Austria, Vienna, 2020: 1111-1114.

[9] HUANG H, YE Q, ZHOU Y T. 6G-Empowered Offloading for Realtime Applications in Multi-Access Edge Computing [J]. IEEE transactions on network scienc

e and engineering, 2023, 10(3): 1311-1325.

[10] LV X C, TIAN H, NI W, et al. Energy-Efficient Ad mission of Delay-Sensitive Tasks for Mobile Edge Co mputing [J]. IEEE transactions on communications, 20 18, 66(6):2603-2616.

[11] TANG H J, WU H M, ZHAO Y B, et al. Joint com putation offloading and resource allocation under task-overflowed situations in mobile-edge computing [J]. I EEE transactions on network and service management, 2022, 19(2): 1539-1553.

[12] HUANG L, BI S Z, ZHANG Y A. Deep reinforceme nt learning for online computation offloading in wirel ess powered mobile-edge computing networks [J]. IEE E transactions on mobile computing, 2020, 19(11): 25 81-2593.

[13] ZHANG Z, ZENG F. Efficient task allocation for co mputation offloading in vehicular edge computing [J]. IEEE internet of things journal, 2023, 10(6): 5595-5 606.

[14] DAI Y, ZHANG K, MAHARJAN S, et al. Deep rein forcement learning for stochastic computation offloadi ng in digital twin networks [J]. IEEE transactions on industrial informatics, 2021, 17(7): 4968-4977.

[15] SUN Z J, YANG H, LI C, et al. Cloud-edge collabo ration in industrial internet of things: a joint offloadin g scheme based on resource prediction [J]. IEEE inter net of things journal, 2022, 9(18): 17014-17025.

[16] YANG H, LIANG Y S, YUAN J Q, et al. Distribute d blockchain-based trusted multidomain collaboration f or mobile edge computing in 5G and beyond [J]. IEE E transactions on industrial informatics, 2020, 16(11): 7094-7104.

[17] WU H M, CHEN J Q, TANG H J, et al. Lyapunov-guided delay-aware energy efficient offloading in IIoT -MEC systems [J]. IEEE transactions on industrial inf ormatics, 2023, 19(2): 2117-2128.

[18] FENG C, ZHANG X, HAN P C, et al. Policy netwo rk-based dual-agent deep reinforcement learning for m ulti-resource task offloading in multi-access edge clou d networks [J]. China communications, 2024, 21(4): 5 3-73.

[19] CHEN J, XING H L, XIAO Z W, et al. A DRL age nt for jointly optimizing computation offloading and r esource allocation in MEC [J]. 2021, 8(24): 17508-17 524.

[20] YUAN X M, ZHANG Z D, FENG C J, et al. A D QN-based frame aggregation and task offloading appr oach for edge-enabled IoMT [J]. IEEE transactions on network science and engineering, 2023, 10(3): 1339-1351.

[21] WANG K D, LI H D, DING Z G, et al. Reinforcem ent learning based latency minimization in secure NO MA-MEC systems with hybrid SIC [J]. IEEE transact ions on wireless communications, 2023, 22(1): 408-42 2.

[22] LU S F, LIU S, ZHU Y J, et al. A DRL-based dece ntralized computation offloading method: an example of an intelligent manufacturing scenario [J]. IEEE tran sactions on industrial informatics, 2023, 19(9): 9631-9 641.

[23] LV P, XU W B, NIE J T, et al. Edge computing tas k offloading for environmental perception of autonom ous vehicles in 6G networks [J]. IEEE transactions o n network science and engineering, 2023, 10(3): 1228 -1245.

[24] LI Q, CUI Y P, SONG T, et al. Federated multiagen t actor–critic learning task offloading in intelligent log istics [J]. 2023, 10(13): 11696-11707.

[25] GUO M. Research on computation task offloading me thods of mobile edge computing for industrial internet [D]. Sichuan: Sichuan University, 2021.

[26] FUJIMOTO S, HOOF H V, MEGER D. Addressing Function Approximation Error in Actor-Critic Methods [C]. //Proceedings of the 35th International Conferen ce on Machine Learning in Stockholm SWEDEN, Sto ckholmsmässan, 2018: 1587-1596.

About the authors

LI Sha was born in 1996. He received the M.E. degree in software engineering from Taiyuan University of Technology. She is now a Ph.D. at University of Science and Technology Beijing. Her research interests include Industrial Internet of Thing and Mobile Edge Computing. (Email: lisha@xs.ustb.edu.cn)

WANG Jianquan was born in 1974. He received the Ph.D. degree in telecommunications engineering from Beijing University of Posts and Telecommunications. He is now an professor. His research interests include Industrial Internet of Thing and Network Security. (Email: wangjianquan@ustb.edu.cn)

FU Meixia was born in 1990. She received the Ph.D. degree in information and communication engineering from Beijing University of Posts and Telecommunications. She is now a lecturer. Her research interests include Industrial Intelligence and Computer Vision. (Email: mxfu1205@ustb.edu.cn)

HUANG Rong received the Ph.D. degree in communication and information systems from Beijing University of Posts and Telecommunications. She is now a senior engineer. Her research interests include 5G network communication. (Email: huangr27@chinaunicom.cn)

SUN Lei [corresponding author] was born in 1984. He received the Ph.D. degree in communication and information systems from Beijing University of Posts and Telecommunications. He is now an associate professor. His research interests include Industrial Internet of Thing and Time Sensitive Network. (Email: sun_lei@ustb.edu.cn)

MA Zhangchao was born in 1984. He received the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications. He is now an associate professor. His research interests include Industrial Time Sensitive Network and Network Security. (Email: mazhangchao@ustb.edu.cn)

ZHANG Lifang received the Ph.D. degree in communication and information systems from Beijing University of Posts and Telecommunications. She is now a senior engineer. Her research interests include 5G network communication. (Email: zhanglf49@chinaunicom.cn)