Blockchain-based 5G Wireless Access Network Resource Sharing Framework and Secure Resource Allocation Method

Deqiang Fei and Xu Wei*

Department of Basic Medical Education, Dazhou Vocational College of Chinese Medicine, Dazhou, 635000, China
E-mail: FfDdQIang52458@163.com; weixu186@163.com
**Correspondence Author*

Received 20 January 2026; Accepted 27 February 2026

Abstract

In response to problems such as a lack of trust, low resource utilization rates, conflicts due to multiple constraints, and security risks associated with sharing 5G wireless access network resources, this study proposes an efficient, trustworthy, and secure distributed resource sharing system and optimizes the resource allocation strategy. First, it performs virtual decoupling and atomic modeling for the three core computing resources: spectrum, security, and computing power. It also designs a five-layer distributed resource-sharing framework that integrates blockchain and software-defined networks. Additionally, it proposes an improved delegated proof-of-stake consensus mechanism, as well as an asymmetric encryption transaction authentication and resource status traceability mechanism. Second, for the multi-constraint conflict issue, it designs a multi-agent deep deterministic strategy gradient secure resource allocation algorithm integrating long-term and short-term memory state prediction. The verification experiments were carried out based on the

Journal of Cyber Security and Mobility, Vol. 15_3, 577–602.
doi: 10.13052/jcsm2245-1439.1533

5G-RAN public resource scheduling dataset in accordance with the 3GPP TR38.901 protocol specification. The experimental hardware was equipped with Intel Core i9-13900K processor, NVIDIA RTX 4090 graphics card, etc. The simulation platform was built on the Ubuntu 22.04 LTS system using the PyTorch 2.1.0 deep learning framework and the NS-3 3.36 simulation tool. The comparison benchmarks were mainstream centralized resource allocation schemes, blockchain, federated deep reinforcement learning schemes, and consortium chain hierarchical cross-slice schemes. The experimental results showed that the resource utilization rate of this framework reached 89.3%, the transaction delay was only 21.8 ms, the service quality satisfaction and security compliance rate were 96.7% and 98.2% respectively, the double-spend attack resistance rate and resource status traceability accuracy rate both reached 99.9%, and all related indicators were significantly superior to the existing comparison schemes. This study provided technical support for 5G resource collaboration in scenarios such as industrial internet and vehicle networking, effectively solving the trust bottleneck and scheduling problems in distributed environments. However, the research has not fully considered the adaptability of resource scheduling in extreme network environments. The computational power consumption of the algorithm in large-scale node deployment scenarios must be optimized further. The computational cost of the blockchain and multi-agent deep reinforcement learning components is high. Additionally, the system's scalability in ultra-dense 5G scenarios must be improved. To a certain extent, this framework's immediate large-scale practical application in complex 5G network environments is limited.

Keywords: 5G wireless access network, block chain, resource sharing, secure resource allocation, multi-agent deep reinforcement learning.

1 Introduction

With the rapid evolution of 5G technology, wireless access networks, as the key hub connecting terminals and core networks, bear the important mission of supporting diversified services such as industrial Internet and high-definition video transmission for Internet of Vehicles. Its resource sharing efficiency and security assurance capabilities directly determine the service quality and application expansion potential of the 5G network [1–3]. Resource sharing has become the core approach for improving network utilization and reducing infrastructure construction costs during the deployment

and operation of 5G wireless access networks. However, current industry practices and technical research face multiple urgent challenges that need to be overcome. The actual impacts of these problems are clearly quantifiable [4–6]. Under the traditional centralized resource allocation scheme, the average resource utilization rate in the industry is only about 70% and the transaction delay of core services is generally over 40 ms. In the distributed sharing scenario, the occurrence rate of security threats such as double-spending attacks remains high. For example, in the 5G deployment scenario of connected vehicles, the failure rate of resource scheduling due to trust loss is over 15%. The unwillingness of edge clouds and mobile virtual operators to share resources further exacerbates the imbalance between the supply and demand of network resources. These quantitative data and actual deployment pain points fully confirm the urgency and practical relevance of optimizing resource sharing in 5G wireless access networks [7–9]. Based on the above issues, the core direction of this research lies in constructing an efficient, reliable and secure distributed resource sharing system for 5G wireless access networks. The core research questions focus on solving the bottlenecks of distributed resource sharing in a trusted environment, optimizing resource scheduling under multiple constraints and conflicts, ensuring full traceability of resource status, and achieving a balance between efficiency and security. The specific research goals are to efficiently match and schedule the three core resources (computing, spectrum, and security) in 5G wireless access networks. This will improve resource utilization and transaction processing efficiency while enhancing the security of resource sharing and the ability to resist attacks.

To eliminate the above difficulties, academia and industry have carried out a large amount of related research. In response to the problem of real-time and secure resource allocation in 5G wireless access networks in shared infrastructure, Seid et al. integrated blockchain and multi-agent deep reinforcement learning to propose a dynamic framework for multi-drone assistance scenarios. This framework modeled resource allocation as a hierarchical Stackelberg game, which was then transformed into a stochastic game and solved using the multi-agent deep deterministic policy gradient (MADDPG) algorithm. Simulation showed that this method was superior to existing solutions in terms of utility optimization and service quality satisfaction [10]. Aiming at the problem of slicing tenants falsely reporting resource requirements in 5G wireless access networks, leading to resource waste and shortage and slowing down the response of centralized controllers, Ayepah-Mensah et al. proposed a peer-to-peer resource trading framework. This research

combined blockchain with federated deep reinforcement learning (FDRL) to achieve decentralized and trusted cross-slice sharing. The results showed that this mechanism was significantly better than the existing centralized solution in terms of resource utilization, delay and service quality [11]. Edge clouds are unwilling to share service images due to resource constraints. Zhou et al. proposed an incentive sharing mechanism based on blockchain. This study modeled service-oriented edge resource allocation as mixed integer nonlinear programming. Moreover, this research decoupled user assignments through Gibbs sampling, and combined Lyapunov and convex optimization to reduce long-term energy consumption and budget. Experiments showed that this solution was superior to existing methods in terms of delay, energy consumption, and resource utilization [12]. Aiming at the problems of large differences in computing resource utilization in multi-access edge network slices, waste or shortage of idle virtual machine quotas, and the reluctance of mobile virtual operators to share due to security concerns, Kwantwi et al. proposed a hierarchical cross-slice computing resource trading framework based on the alliance chain. This research used Hyperledger smart contracts to ensure the security of peer-to-peer transactions. Research results showed that this algorithm was better than the baseline scheme in terms of slice satisfaction, resource utilization, and resistance to double payment attacks [13].

In summary, these studies provide useful ideas for 5G wireless access network resource sharing, but there are still obvious shortcomings; it is difficult to balance the efficiency and security of the consensus mechanism, and the interference of malicious nodes in the consensus process is not effectively suppressed. The resource allocation algorithm fails to fully consider the dynamic changes of the network and has limited ability to balance multi-constraint conflicts. Moreover, it lacks a full-process traceability mechanism for resource status, making it difficult to ensure the credibility and auditability of transactions. The research targets the shortcomings of existing studies and constructs an atomic description model for three core resources: computing, spectrum, and security. By virtualizing and decoupling physical resources and standardizing their packaging, it achieves refined characterization and management of resources. At the same time, a five-layer distributed resource sharing framework integrating blockchain and software-defined network (SDN) is designed. To realize distributed scheduling and trusted management of resources, a hierarchical architecture consisting of the resource access layer, atomic resource adaptation layer, blockchain consensus layer, SDN control layer, and application service layer is established. The

improved delegated proof-of-stake (DPoS) consensus mechanism proposed in this study is based on the model and framework. It introduces node reputation values to optimize the logic of account node election. This mechanism incorporates historical reputation, resource contribution, and online duration into the election priority calculation. Compared with the traditional DPoS consensus mechanism, it effectively filters malicious nodes and improves consensus efficiency and stability. The MADDPG security resource allocation algorithm integrates long-term and short-term memory (LSTM) state prediction. It uses historical state data stored on the blockchain through the LSTM module to predict the future availability of resources. The algorithm then integrates these prediction results into its state space. At the same time, the research establishes a transaction authentication mechanism based on asymmetric encryption and a blockchain log storage structure. This mechanism secures the authentication of resource transactions and enables the full-process traceability of resource states.

The key elements of this research's innovation are reflected in four aspects. First, it creates atomic description models for three types of core resources – computing, spectrum, and security – to achieve virtual decoupling and standardized encapsulation of physical resources. The methods in existing studies that use single-resource dimensions are compared with this method. The method can achieve refined characterization and unified management of multi-dimensional resources. This lays the foundation for efficient resource matching. It also solves the problems of rough resource characterization and poor adaptability in existing models. Second, it designs a five-layer distributed resource sharing framework that integrates blockchain and SDN, breaking the insufficient integration of blockchain and network scheduling technology in existing research. Through collaborative implementation of the hierarchical architecture, distributed scheduling and trusted resource management are realized, making it more suitable for the scheduling requirements of 5G wireless access networks. This improves scheduling flexibility and efficiency. Third, it proposes an improved DPoS consensus mechanism that introduces node reputation values. Compared with traditional DPoS and proof-of-work (PoW) consensus mechanisms, it realizes the selection of superior nodes through multi-dimensional election priorities. This effectively suppresses the interference of malicious nodes. At the same time, it improves the consensus efficiency while ensuring the security of the consensus. This solves the core problem of the inability to balance efficiency and security in existing consensus mechanisms. Fourth, it designs a MADDPG security resource allocation algorithm that integrates LSTM state

prediction. The LSTM module realizes the dynamic prediction of network resource states and integrates the results into the state space and decision-making process of the algorithm. This significantly enhances the algorithm's adaptability to dynamic changes in the network. At the same time, the ability to balance multiple constraints, such as delay, energy consumption, and security, is strengthened by introducing a penalty function with constraints. This results in global optimization of resource allocation. The research work holds significant reference value in areas such as communication network optimization, industrial digital transformation, and intelligent transportation development. At the theoretical level, the 5G core resource atomization model and the five-layer distributed framework integrated with blockchain-SDN proposed in this study enriches the theoretical system of 5G wireless access network resource virtualization and distributed scheduling. This study proposes an improved DPoS consensus mechanism and an LSTM-enhanced MADDPG algorithm. These new theoretical ideas provide a foundation for optimizing blockchain consensus mechanisms and applying deep reinforcement learning to network resource scheduling. At the engineering practice level, the solutions proposed in this study effectively address trust bottlenecks and multi-constraint scheduling problems in 5G resource sharing within a distributed environment. These solutions significantly improve resource utilization and transaction efficiency while enhancing the security and anti-attack capabilities of resource sharing. They can also provide direct technical support for typical scenarios, such as the deployment of 5G private networks in the industrial internet, low-latency and high-reliability communication in vehicle networking, and the large-bandwidth resources necessary for high-definition video transmission. It can also directly reduce the construction and operation costs of 5G networks and accelerate the integration and application of 5G technology with various industries.

2 Methods and Materials

This research first conducts virtual decoupling and atomization modeling of the three core resources of the 5G wireless access network, computing, spectrum, and security, builds a standardized atomic resource description model, and then designs a distributed resource sharing framework integrating blockchain and SDN. It proposes a cross-node consensus mechanism based on improved DPoS and designs an intelligent allocation algorithm for security resources based on MADDPG to achieve global optimization of resource allocation.

2.1 Design of a Distributed Resource Sharing Framework for a 5G Wireless Access Network Empowered by Blockchain

This study first implements virtualization decoupling and atomization modeling of 5G wireless access network resources. For the three core resources of computing, spectrum, and security, a standardized atomic resource description model is constructed, as shown in Equation (1) [14].

$$RA_k = R^k_{type}, C^k_{comp}, B^k_{data}, S^k_{level}, A^k_{status}, T^k_{valid} \tag{1}$$

In Equation (1), RA_k represents the kth resource atomic unit, $R^k_{type} \in \{1, 2, 3\}$ is the resource type identifier (1 corresponds to computing resources, 2 corresponds to spectrum resources, and 3 corresponds to security resources), and C^k_{comp} represents the computing overhead of the resource atom. The computing resource is taken as its own computing power value, and the spectrum and security resources are taken as the amount of computing resources required in the scheduling process. B^k_{data} is the data size of the resource atom and $S^k_{level} \in [1, 5]$ is the security protection level. Computing and spectrum resources are based on the security requirement level of the business they carry, and security resources are based on their own protection capability level. $A^k_{status} \in \{0, 1\}$ is the real-time availability status (1 is available, 0 is occupied). T^k_{valid} is the effective duration of resource atoms. Based on the above atomization model, a distributed resource scheduling architecture integrating blockchain and SDN is researched and designed. The architecture includes the resource access layer, the atomic resource adaptation layer, the blockchain consensus layer, and the SDN control layer, as shown in Figure 1.

In Figure 1, the resource access layer deploys macro base stations, micro base stations, edge computing nodes and other equipment. Each device maps physical resources into atomic resources through a hardware abstraction interface. The atomic resource adaptation layer is responsible for standardized encapsulation of atomic resources, generating resource metadata, and uploading it to the consensus layer through a lightweight blockchain client. The blockchain consensus layer consists of verification nodes and accounting nodes. The verification node verifies the legality of resource metadata, and the accounting node packages the verified metadata into blocks. The SDN control layer obtains the atomic resource status by calling the blockchain smart contract, generating a resource scheduling flow table and sending it to the access layer device to realize distributed scheduling of resources. To ensure the consensus efficiency and security of the architecture, this research

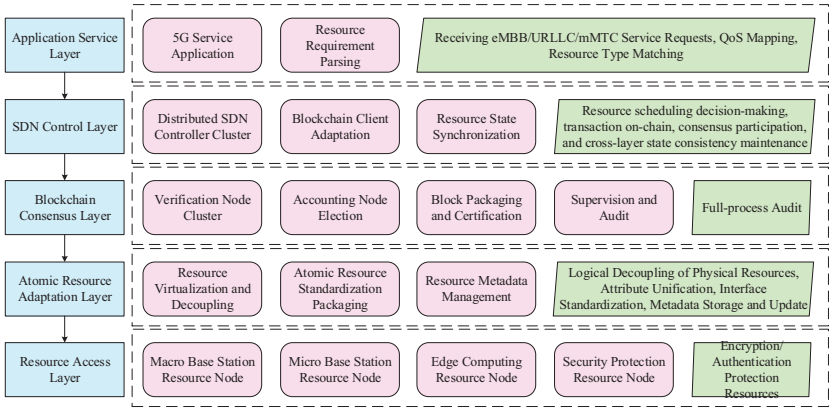

Figure 1 Distributed resource scheduling architecture integrating blockchain and SDN.

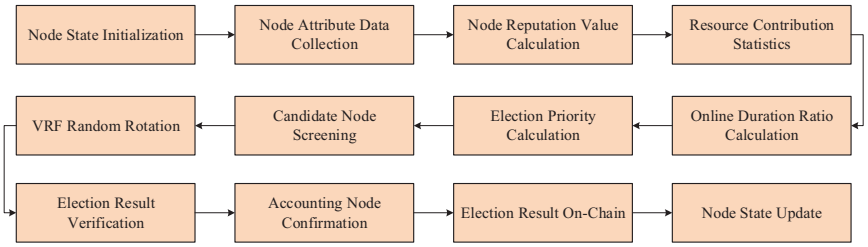

Figure 2 Priority-based accounting node election process.

proposes a cross-node consensus mechanism based on improved DPoS and introduces node reputation value to optimize the accounting node election logic. The calculation of its election priority is shown in Equation (2) [15].

$$P_{node} = \omega_1 \cdot Rep_{node} + \omega_2 \cdot Res_{contrib} + \omega_3 \cdot Uptime_{ratio} \tag{2}$$

In Equation (2), P_{node} is the election priority of the node, $Rep_{node} \in [0, 100]$ is the historical reputation value of the node (5 points are added for successful performance and 20 points are deducted for breach of contract), $Res_{contrib}$ is the total number of resource atoms contributed by the node, $Uptime_{ratio}$ is the proportion of the node's online time, and ω_1, ω_2, and ω_3 are weight coefficients (default values are 0.4, 0.3, and 0.3). The accounting node election process based on this priority is shown in Figure 2.

In Figure 2, the system first counts the reputation value, resource contribution and online time of all nodes, calculates and sorts the priority of each node, and selects the top 10% nodes as candidate accounting nodes.

The candidate node generates a rotating random value through a verifiable random function (VRF) to determine the final accounting node sequence. After the accounting node completes the block packaging, the results will be synchronized to the entire network. Meanwhile, the node reputation value is updated to complete a consensus cycle. To achieve secure authentication of resource sharing transactions, this research designs a transaction signature and verification mechanism based on asymmetric encryption. The signature of the transaction initiator is generated as shown in Equation (3) [16].

$$Sig_{tx} = E_{SK_{sender}}(Hash(RA_k \| Tx_{info} \| Timestamp)) \tag{3}$$

In Equation (3), Sig_{tx} is the transaction signature, SK_{sender} is the initiator's private key, $Hash(\cdot)$ is the SHA-256 hash function, Tx_{info} is transaction information, $Timestamp$ is the transaction timestamp, and $E_{SK_{sender}}$ is the private key encryption. The transaction initiator generates a transaction request containing a signature, and the verification node decrypts the signature through the initiator's public key and verifies the hash consistency. Transactions that pass verification are broadcast to the accounting node, which integrates the transaction and resource metadata into transaction records and packages them into new blocks. New blocks are uploaded to the chain through the consensus mechanism, and the SDN control layer updates the available status of resource atoms based on the transaction results. In order to realize the full-process traceability of resource status, this research designs a resource status log storage structure based on blockchain. Its log entry format is shown in Equation (4) [17].

$$Log_{ra} = \{RA_k, Op_{type}, Node_{addr}, Timestamp, Sig_{node}\} \tag{4}$$

In Equation (4), Log_{ra} is the status log of resource atoms, Op_{type} is the operation type, $Node_{addr}$ is the node address where the operation is performed, and Sig_{node} is the node's signature on the log. The state change operation of each resource atom generates corresponding log entries, which are stored in blockchain blocks in chronological order. When it is necessary to trace the resource status, all relevant logs are retrieved through the resource atomic identifier. After verifying the validity of the log signature, the resource occupation, release, and update processes are restored in order of timestamps to implement full-link auditing of resource usage. Finally, the blockchain-enabled 5G wireless access network distributed resource sharing framework designed in this study is shown in Figure 3.

In Figure 3, the blockchain-enabled 5G wireless access network distributed resource sharing framework achieves virtualized decoupling and

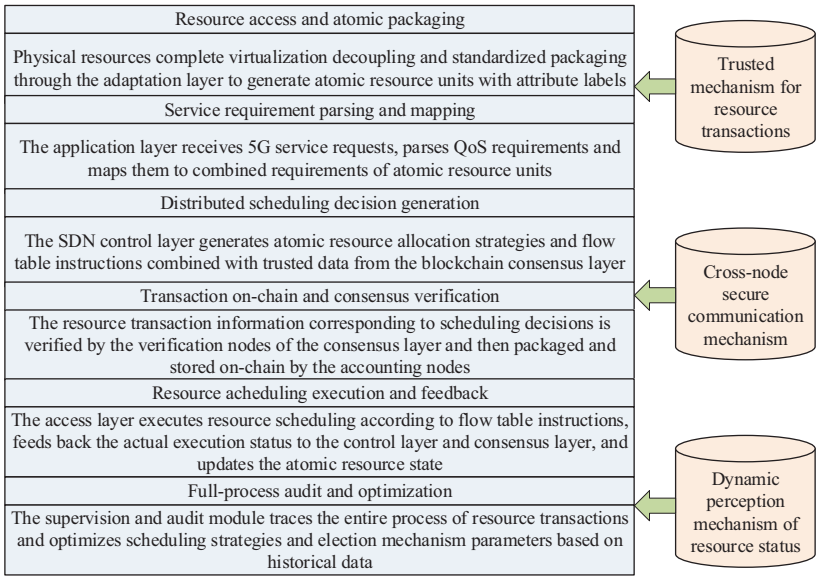

Figure 3 Blockchain-enabled 5G wireless access network distributed resource sharing framework.

standardized encapsulation of physical resources through a five-layer architecture. It relies on the improved DPoS consensus mechanism to ensure trusted collaboration between nodes and uses SDN's flexible scheduling capabilities to match the diverse QoS requirements of 5G services. Moreover, it integrates smart contracts, asymmetric encryption and dynamic sensing mechanisms to achieve automated execution of resource transactions, data cannot be tampered with and the entire process is traceable. This not only breaks the trust bottleneck of resource sharing in a distributed environment, but also takes into account scheduling efficiency, security, and service continuity through multi-constraint adaptive optimization. It adapts to the resource collaboration needs of multiple scenarios such as the Industrial Internet and Internet of Vehicles. A five-layer distributed resource sharing framework integrating blockchain and SDNing is designed for the deployment scenarios of medium-scale 5G wireless access networks consisting of 10 to 100 nodes. It uses a distributed trust model based on node reputation values. It also has protection mechanisms against typical network threats, such as double-spending attacks, malicious node consensus interference, and forged resource information. It can seamlessly adapt to public, private, and hybrid deployment modes of 5G wireless access networks. It enables trusted resource sharing

and intelligent scheduling in various 5G deployment scenarios, including industrial internet private networks, public vehicle networks, and government and enterprise mixed networks.

2.2 Optimization Method for Intelligent Allocation of Security Resources in a 5G Wireless Access Network Under Multiple Constraints

This study designs a secure resource intelligent allocation algorithm based on MADDPG, using the constructed blockchain-enabled distributed resource sharing framework. This algorithm addresses the multi-constraint conflict issues of delay, energy consumption, and security in 5G wireless access network resource allocation. It achieves global optimization of resource allocation by clarifying the core elements of the algorithm and integrating the state prediction mechanism and security filtering logic. First, it defines the state space of the algorithm, which comprehensively covers resource status, business requirements and network dynamic characteristics, as shown in Equation (5) [18].

$$S = \{RA_k, QoS_{req}, \rho_{net}, \tau_{consensus}\} \tag{5}$$

In Equation (5), S is the global state space of the agent, RA_k is a collection of resource atomic units, QoS_{req} is the multi-dimensional demand parameter of the business, ρ_{net} is the network load fluctuation coefficient, and $\tau_{consensus}$ is the blockchain consensus delay. The action space of the algorithm is defined as the allocation decision matrix of resource atomic units, which directly maps resource scheduling execution instructions, as shown in Equation (6) [19].

$$A = [a_{ij}]_{M \times N} \tag{6}$$

In Equation (6), A is the action space, M is the number of concurrent services, N is the total number of resource atomic units, and a_{ij} is the allocation decision of the ith service to the jth resource atom. To guide the agent to converge in the direction of multi-objective optimization, a reward function incorporating constraint penalties is studied and designed, as shown in Equation (7) [20].

$$R = \lambda_1 \cdot U_{delay} + \lambda_2 \cdot U_{energy} + \lambda_3 \cdot U_{sec} - \gamma \cdot (P_{delay} + P_{sec}) \tag{7}$$

In Equation (7), R is the reward value obtained by the agent in a single interaction, U_{delay} is the delay effect, U_{energy} is energy consumption utility,

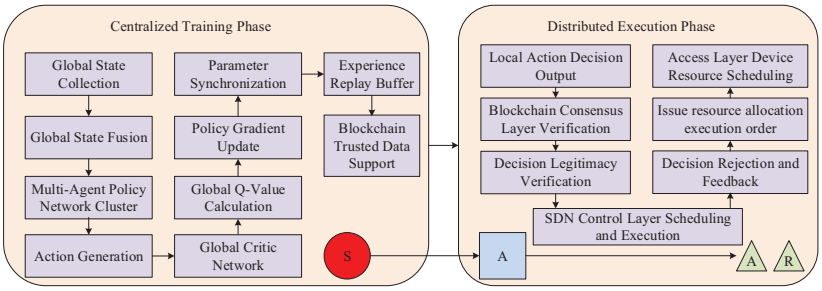

Figure 4 Schematic diagram of the MADDPG algorithm.

U_{sec} is the safety utility, P_{delay} is the penalty for delay constraint violation, P_{sec} is the penalty for security constraint violation, λ_1, λ_2, and λ_3 are utility weights, and γ is the constraint penalty coefficient. Based on the above definitions of status, action and reward, this study designs the core process of the MADDPG algorithm, including two stages: centralized training and distributed execution. The algorithm diagram is shown in Figure 4.

In Figure 4, the centralized training stage integrates the status and actions of all agents through the global critic network and calculates the global Q value to evaluate the quality of decisions. The policy network of each agent updates parameters through policy gradient descent. The update formula is shown in Equation (8) [21].

$$\nabla_{\theta_{\mu_i}} J(\theta_{\mu_i}) = \mathbb{E}_{\substack{s\sim\mathcal{D} \\ *a_i\sim\mu_i}} \nabla_{a_i} Q_i(s, a_1, \ldots, a_N)|_{a_i=\mu_i(s_i)} \nabla_{\theta_{\mu_i}} \mu_i(s_i) \tag{8}$$

In Equation (8), θ_{μ_i} is the parameter of the ith agent's policy network, $J(\theta_{\mu_i})$ is the policy objective function, $\mathcal{D}$ is the experience replay pool, Q_i outputs the Q value for the critic network of the ith agent, and $\mu_i(s_i)$ is the action of the agent based on the local observation s_i output. The experience replay pool stores samples generated by the interaction between the agent and the environment and is used for batch training to avoid the impact of data correlation. The blockchain module synchronizes resource allocation records and constraint satisfaction during the training process, providing credible data support for reward calculations. In the distributed execution stage, each agent outputs an allocation decision based on the local policy network and verifies the legitimacy of the decision through the blockchain consensus layer. After passing the verification, the SDN control layer executes resource scheduling. Meanwhile, it uploads feedback data such as actual delay and energy consumption to the training module. This research

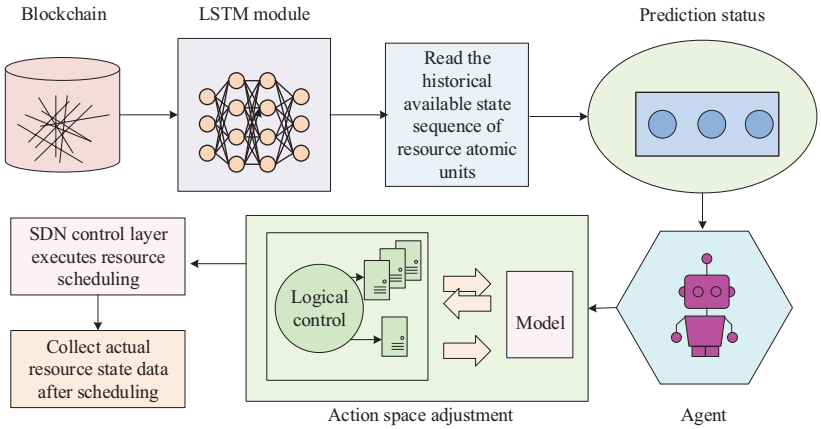

Figure 5 Fusion process of state prediction module and resource allocation algorithm.

integrates an LSTM status prediction module into the algorithm to solve the problem of allocation failure caused by sudden changes in resource status in dynamic networks. The module predicts the future availability of resource atoms based on historical status data stored in the blockchain. Its prediction formula is shown in Equation (9) [22].

$$\hat{A}^k_{status}(t+T) = LSTMA^k_{status}(t), A^k_{status}(t-\Delta t), \ldots, A^k_{status}(t-(L-1)\Delta t) \tag{9}$$

In Equation (9), $\hat{A}^k_{status}(t+T)$ is the predicted available state of the kth resource atom at time $t+T$, L is the time window length of LSTM, Δt is the status sampling interval, and $A^k_{status}(t)$ is the actual available state at time t. The integration process of the state prediction module and the resource allocation algorithm is shown in Figure 5.

In Figure 5, the state prediction module reads the historic available state sequence of resource atoms from the blockchain. The agent incorporates the predicted state into the current state space, adjusts the allocation decision in the action space, and gives priority to resource atoms that are continuously available during the prediction period. After the allocation is executed, the actual state is compared with the predicted state, the prediction error is calculated, and the error is fed back to the LSTM module to update parameters. Meanwhile, it writes the error data into the blockchain as a certificate to ensure the traceability of the prediction model optimization [23, 24]. The intelligent allocation optimization method of 5G wireless access network security resources under multiple constraints is shown in Figure 6.

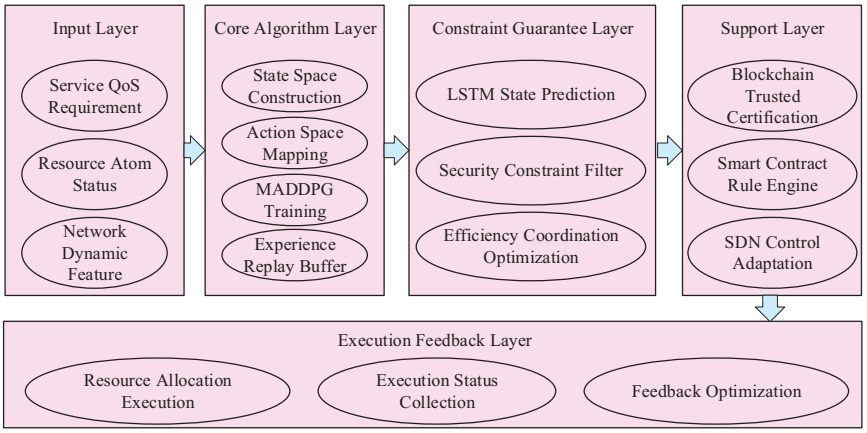

Figure 6 Optimization method for intelligent allocation of security resources in 5G wireless access network under multiple constraints.

In Figure 6, the blockchain support layer provides resource atomic status data, consensus delay data and trusted certificate storage services, providing data input and security guarantee for the algorithm. The core layer of the algorithm includes the MADDPG training module, the LSTM prediction module and the security filtering module. The constraint adaptation layer translates business QoS requirements into quantitative indicators that the algorithm can identify. At the same time, it converts the allocation decisions that the algorithm produces into scheduling instructions that the SDN control layer can execute. The execution feedback layer collects delay, energy consumption, and security level data after resource scheduling for algorithm parameter optimization and ultimately achieves global optimal resource allocation under multiple constraints.

3 Results

This research builds a 5G wireless access network simulation platform based on specific hardware, software environments and data sets. It selects mainstream resource allocation algorithms and different consensus mechanisms as comparison benchmarks, and conducts tests from the dimensions of algorithm performance, consensus efficiency, and comprehensive resource allocation performance. It evaluates the performance of the proposed MADDPG security resource intelligent allocation algorithm and blockchain-enabled 5G wireless access network distributed resource sharing framework.

3.1 Performance Analysis of the Security Resource Intelligent Allocation Algorithm Based on MADDPG

The dataset adopts the public 5G-RAN resource scheduling data set, which includes three types of typical business scenario data: industrial Internet, Internet of Vehicles, and high-definition video transmission. It covers 1000 resource atomic units, 5000 business request records, and 100,000 resource status history logs. The data sampling interval is 100 ms and complies with the 3GPPTR38.901 protocol specification. The experimental configuration parameters are shown in Table 1.

In Table 1, all hardware configurations are selected based on the high computing power and high concurrency requirements of 5G network simulation, blockchain node deployment, and multi-agent deep reinforcement learning algorithm training. Among them, the Intel Core i9-13900K processor (3.0GHz, 24 cores) provides multi-core parallel computing capabilities, supporting the distributed training of algorithms and large-scale data processing. The NVIDIA RTX 4090 graphics card, which has 24 GB of GDDR6X memory, provides professional-grade GPU acceleration for calculating gradients and updating parameters of deep learning models. This significantly improves the efficiency of model training. The 64 GB DDR5 55600 MHz memory ensures high-speed reading and writing of massive experimental data and simulation processes, avoiding memory bottlenecks. The 1 TB NVMe SSD storage is used to store 5G-RAN resource scheduling data sets, blockchain node operation data, and the entire algorithm training log,

Table 1 Experimental configuration parameter table

Configuration Category	Specific Configuration	Specific Parameters
Hardware configuration	CPU	IntelCore i9-13900K (3.0 GHz, 24 cores)
	GPU	NVIDIA RTX 4090 (24 GB GDDR 6X memory)
	Memory	64 GB DDR 55600 MHz
	Storage	1TB NVMe SSD
Software environment	Operating system	Ubuntu 22.04 LTS
	Programming language	Python 3.9
	Deep learning framework	PyTorch 2.1.0
	Network simulation tool	NS-33.36 (5G network simulation module)
	Blockchain platform	Hyperledger Fabric2.5 (blockchain node deployment)

ensuring low latency in data access. The software environment all selects mainstream and compatible tools and systems that are adapted to 5G communication, blockchain, and deep learning fields. The Ubuntu 22.04 LTS operating system provides a stable, open-source foundation for deploying various tools. Python 3.9 has been adopted as the primary programming language, ensuring compatibility with most deep learning and network simulation development libraries. The PyTorch 2.1.0 deep learning framework is used for model construction, training, and parameter optimization of the MADDPG+LSTM secure resource allocation algorithm, supporting dynamic computation graphs and GPU acceleration adaptation. The NS-3 3.36 5G network simulation module provides an experimental environment that closely resembles the operation of actual 5G wireless access networks. It can accurately simulate the network traffic and resource demand characteristics of businesses such as the industrial internet, vehicle networking, and high-definition video transmission. The Hyperledger Fabric 2.5 blockchain platform is used for deploying blockchain nodes, developing and operating smart contracts, and supporting the experimental verification of the improved DPoS consensus mechanism, as well as for authenticating transactions with asymmetric encryption and tracking the status of resources. This experiment selects three types of mainstream resource allocation algorithms as comparison benchmarks, namely deep Q-Network (DQN), deep deterministic policy gradient (DDPG), and FDRL. The accuracy comparison results of different algorithms on the value function and policy function are shown in Figure 7.

In Figure 7(a), when the number of iterations reaches 200, the accuracy of MADDPG rises to above 0.8. Moreover, when the number of iterations

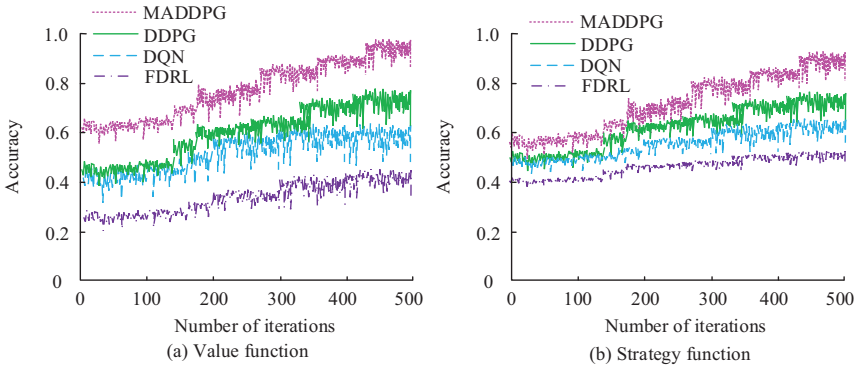

Figure 7 Accuracy comparison results of different algorithms on value function and strategy function.

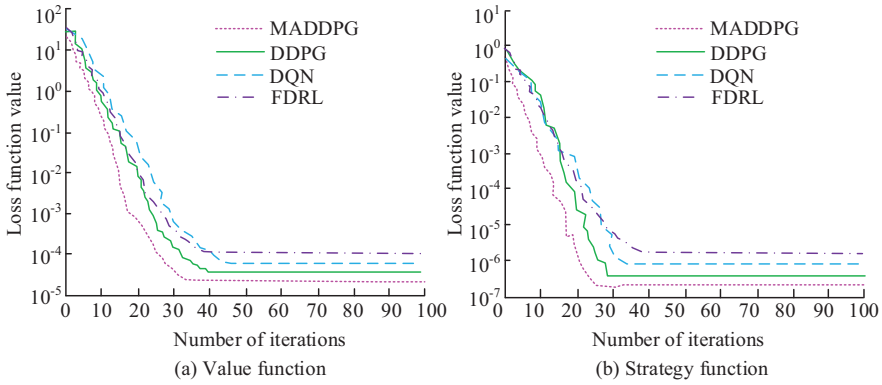

Figure 8 The convergence of different algorithms on the value function and policy function.

reaches 500, the accuracy of MADDPG stabilizes at around 0.95. In Figure 7(b), after 500 iterations, the accuracy of MADDPG remains around 0.93. This shows that MADDPG's multi-agent collaboration and centralized evaluation mechanism can more accurately optimize value and strategy functions and improve the accuracy and stability of resource allocation decisions. The convergence of different algorithms on the value function and policy function is shown in Figure 8.

In Figure 8(a), in the initial iteration stage, the loss values of MADDPG, DDPG, DQN, and FDRL decrease rapidly. When the number of iterations reaches 30, the loss value of MADDPG drops below 10^{-4}. In Figure 8(b), after 50 iterations, the loss value of MADDPG stabilizes below 10^{-6}. MADDPG's value function and policy function loss value converge significantly faster than other algorithms, and the final convergence accuracy is higher. MADDPG's centralized training and multi-agent collaboration mechanism can optimize value and strategy functions more efficiently and improve the convergence efficiency and stability of the algorithm. The ROC curves of different algorithms are shown in Figure 9.

Figure 9(a) shows the ROC curve of the MADDPG algorithm, and its area under the curve (AUC) reaches 0.92. When the false positive rate is 0.2, the true positive rate has risen to 0.85. When the false positive rate increases to 0.4, the true positive rate is close to 0.95. This reflects that the algorithm has higher accuracy in identifying malicious requests in secure resource allocation scenarios. Figures 9(b), 9(c), and 9(d) correspond to the ROC curves of the DDPG, DQN, and FDRL algorithms respectively. The AUCs of the three are 0.81, 0.75, and 0.78 respectively. The comparison

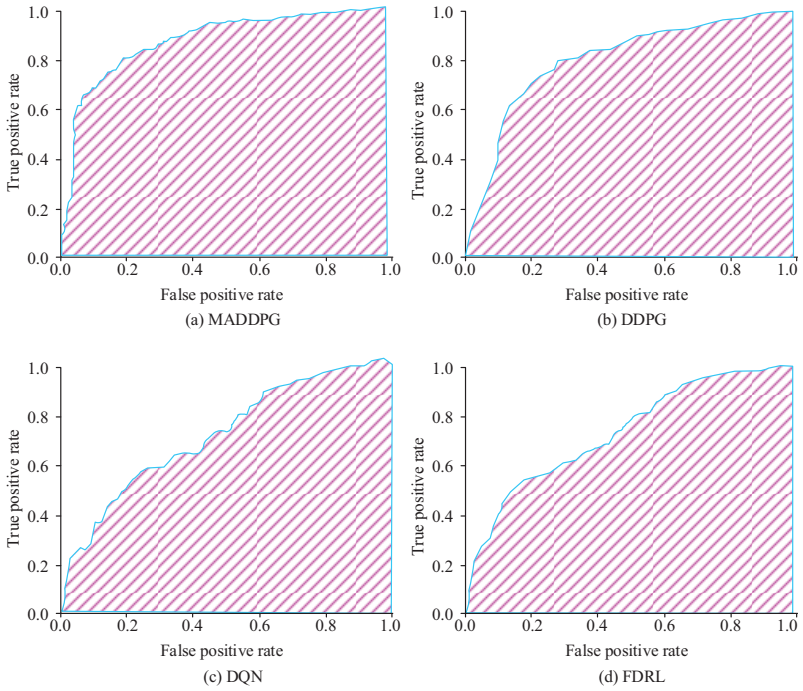

Figure 9 ROC curves of different algorithms.

results show that the ROC curve of MADDPG is always above the other three algorithms. This shows that MADDPG can achieve a higher true positive rate at a lower false positive rate in security threat detection tasks. Its ability to identify malicious behaviors in 5G wireless access network resource sharing scenarios is better.

3.2 5G Radio Access Network Resource Sharing Framework Verification

To verify the consensus efficiency of the proposed blockchain-enabled 5G wireless access network distributed resource sharing framework, this study tests the block packing latency and consensus success rate of the improved DPoS consensus mechanism under different node scale scenarios and selects the traditional DPoS consensus mechanism and PoW consensus mechanism as comparison benchmarks. The test results are shown in Figure 10.

In Figure 10(a), as the node scale expands, the block packing latency of the three mechanisms gradually increases, but the latency growth rate of the

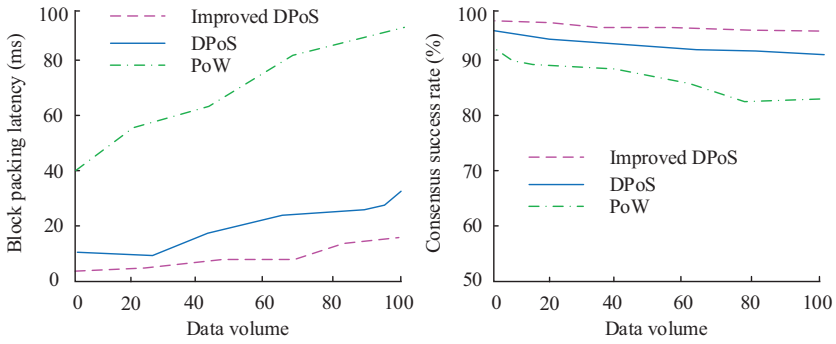

Figure 10 Performance comparison of different consensus mechanisms under different node sizes.

proposed improved DPoS mechanism is significantly lower. When the node size is 100, its block packing latency is only 18.6 ms, which is 31.9% lower than the 27.3 ms of traditional DPoS and 79.2% lower than the 89.5 ms of PoW. Even in the 20 scenarios with the smallest node size, the 8.32 ms delay of the improved DPoS is far better than the traditional DPoS (11.5 ms) and the PoW (42.8 ms). This fully reflects the effect of the improved DPoS on consensus efficiency after optimizing the node election logic. In Figure 10(b), the proposed improved DPoS mechanism maintains a very high consensus success rate at each node scale, reaching 99.8% when the node scale is 20. Even if the node size increases to 100, the success rate remains at 99.6%, with a fluctuation of only 0.2%. The consensus success rate of traditional DPoS decreases more obviously as the node scale increases. It drops from 99.1% for 20 nodes to 97.8% for 100 nodes, a decrease of 1.3%. PoW's consensus success rate is the worst, only 88.3% when there are 100 nodes, which is 11.3 percentage points lower than the improved DPoS. This is due to the improved DPoS that introduces node reputation value to filter accounting nodes, which effectively reduces the interference of malicious nodes on the consensus process and ensures the stability of the consensus in a distributed environment.

3.3 5G Wireless Access Network Security Resource Allocation Performance Evaluation

To comprehensively evaluate the comprehensive performance of the framework's security resource allocation, the existing centralized resource

Table 2 Comparison table of security resource allocation performance of different resource sharing schemes

Evaluation Index	Proposed Framework (Blockchain+ SDN+ MADDPG)	Centralized Resource Allocation Scheme	Blockchain+ FDRL Solution	Hierarchical Cross-slice Solution for Consortium Chains
Resource utilization rate (%)	89.3	72.5	78.6	81.2
Transaction delay (ms)	21.8	47.6	30.5	29.2
QoS satisfaction degree (%)	96.7	83.4	88.9	90.3
Safety level compliance rate (%)	98.2	79.6	86.8	89.5
Constraint violation rate (%)	1.80	8.70	5.30	4.60
Double payment attack defense rate (%)	99.9	75.3	92.6	94.8
Accuracy rate of resource status traceability (%)	99.9	82.4	93.1	95.2

allocation scheme, the blockchain+FDRL scheme (FDRL), and the consortium chain hierarchical cross-slicing scheme are selected as comparison benchmarks. The results are shown in Table 2.

Table 2 presents a comparison table of the security resource allocation performance of the blockchain+SDN+MADDPG distributed resource sharing framework and the existing mainstream 5G wireless access network resource sharing schemes. The multi-scheme comparison tests are conducted under the same 5G-RAN simulation data set and experimental environment. All data are the averaged results of multiple experiments. The resource utilization rate reflects the accuracy and efficiency of resource scheduling. It is calculated by dividing the actual usage of the three types of core resources by the total available resources and expressing the result as a percentage. The transaction delay is the total time consumed from the initiation of the resource transaction request to the update of the status (ms), reflecting the processing efficiency of transactions. The QoS satisfaction rate is the proportion of requests that meet the preset quality of service requirements. The compliance rate of the security level is the proportion of the number of services that meet the preset security protection level. The violation rate of constraints is the proportion of the number of services that violate the multi-dimensional preset constraints. The rate of resisting double spending attacks is the proportion of successful resistance to the attack, reflecting the core security protection capability. The accuracy rate of resource status traceability reflects the accuracy and

credibility of status traceability by measuring the percentage match between the results of blockchain log tracing and the actual status of the resources. The framework proposed in the study performs best in all indicators, with a resource utilization rate of 89.3%. Compared with the centralized solution (72.5%), the FDRL solution (78.6%), and the alliance chain solution (81.2%), it increases by 23.2%, 13.6%, and 10.0%, respectively. This is due to the synergy between atomized resource modeling and SDN dynamic scheduling, achieving precise resource matching. The transaction delay is only 21.8 ms, which is 28.7–62.3% lower than other solutions, reflecting the efficiency of the improved DPoS consensus mechanism and lightweight blockchain client. The QoS satisfaction and security level compliance rates reach 96.7% and 98.2% respectively, and the constraint violation rate is as low as 1.8%. This shows that the framework effectively balances the multi-constraint conflicts of delay, energy consumption and security. In terms of security protection, the double payment attack resistance rate and resource status tracing accuracy rate both reach 99.9%, which is significantly higher than the comparison solution. This verifies the security protection effect of asymmetric encryption and the blockchain log storage mechanism, ensuring the credibility and traceability of resource sharing transactions.

4 Conclusion

The research constructed an atomic description model for three core resources. These resources were computing, spectrum, and security. The model achieved virtual decoupling and standardized encapsulation of physical resources. This laid the foundation for precise multi-dimensional resource matching. It designed a five-layer, distributed resource-sharing framework that integrated blockchain and SDNing. It proposed an improved, DPoS consensus mechanism that introduced node reputation values to achieve dual optimization of consensus efficiency and security. It established a transaction authentication mechanism based on asymmetric encryption and a blockchain log storage structure, to achieve secure authentication throughout the resource transaction process and traceability of the resource status throughout the entire life cycle. It proposed a multi-agent, deep, deterministic strategy gradient algorithm that integrated dynamic predictions of resource status into its decision-making process. It also designed a reward function with constraint penalties, which significantly enhanced the algorithm's ability to adapt to dynamic network changes and resolve conflicts under multiple constraints.

The research was based on the assumption of a medium-scale 5G wireless access network deployment scenario with 10 to 100 nodes. It adopted a distributed trust model centered on node reputation values and designed protection mechanisms against double spending attacks, malicious node consensus interference, and resource information forgery. The framework could be adapted to public, private, and hybrid 5G deployment modes. Experimental verification showed that under this assumption, the proposed technical solution had good applicability and feasibility.

The experimental results showed that the resource utilization rate of this framework was 89.3%, the transaction delay was only 21.8 ms, and the service quality satisfaction rate and security compliance rate were 96.7% and 98.2%, respectively. The double spending attack resistance rate and resource status traceability accuracy rate both reached 99.9%, and compared with existing solutions, significant performance improvements were achieved. The improved DPoS consensus mechanism had a block packaging delay of only 18.6 ms and a consensus success rate of 99.6% at a scale of 100 nodes. After 500 iterations of the multi-agent deep deterministic strategy gradient algorithm, the accuracy of the value and strategy functions stabilized at around 0.95 and 0.93, respectively. This fully verified the comprehensive advantages of the proposed framework and algorithm in terms of resource scheduling efficiency, security, and stability. It effectively broke through the trust bottleneck and multi-constraint scheduling problem in distributed environments for 5G resource sharing.

The research achieved performance improvement in 5G wireless access network resource sharing. However, it has not fully considered the adaptability of resource scheduling in extreme network environments. The computational power consumption of the algorithm in large-scale node deployment scenarios still needs to be optimized. The system scalability in ultra-dense 5G scenarios needs to be further improved. In the future, the scope of the research will expand to include resource scheduling requirements in extreme network environments and ultra-dense deployment scenarios. The algorithm model will be optimized to reduce computational costs, and the integration path of the framework with 6G network resource management technology will be explored.

References

[1] Hu Z, Liu B, Shen A, Luo J. Blockchain-based resource allocation mechanism for the internet of vehicles: balancing efficiency and

security. IEEE Transactions on Network and Service Management, 2024, 21(4): 3971–3987. DOI:10.1109/TNSM.2024.3387931.

[2] Dubey M, Singh A K, Mishra R. AI based resource management for 5G network slicing: history, use cases, and research directions. Concurrency and Computation: Practice and Experience, 2025, 37(2): e8327.1–e8327.23. DOI:10.1002/cpe.8327.

[3] Wang J. Identification of SQL Injection Security Vulnerabilities in Web applications Based on Binary Code Similarity. Journal of Cyber Security and Mobility, 2024, 13(6): 1239–1262. DOI:10.13052/jcsm2245-1439.1361.

[4] Rajasekar A, Ramamoorthi R, Ramya M, Arunachalam V. A novel method to increase the security in 5G networks using deep learning. International Journal of Electronic Security and Digital Forensics, 2025, 17(3): 419–431. DOI:10.1504/IJESDF.2025.145879.

[5] Spanos T, Papageorgiou N, Paliouras V. Enhancing 5G downlink positioning security: embedding a novel authentication scheme into empty PRS resource elements. IEEE Communications Letters, 2025, 29(9): 2188–2192. DOI:10.1109/LCOMM.2025.3590481.

[6] Zhang H, Meng F, Wang Q. Computer Network Security System Optimization Based on Improved Neural Network Algorithm and Data Search. Journal of Cyber Security and Mobility, 2025, 14(1): 75–100. DOI:10.13052/jcsm2245-1439.1414.

[7] Pawana I W A J, Abella V, Lastre J K, Ko Y, You I. Enhancing roaming security in cloud-native 5G core network through deep learning-based intrusion detection system. Computer Modeling in Engineering and Sciences, 2025, 145(11): 2733–2760. DOI:10.32604/cmes.2025.072611.

[8] Garg T, Gupta S, Obaidat M S, Raj M. Drones as a service (DaaS) for 5G networks and blockchain-assisted IoT-based smart city infrastructure. Cluster Computing, 2024, 27(7): 8725–8788. DOI:10.1007/s10586-024-04354-1.

[9] Li X, Zhang J. Multi-source Data Fusion for Real-time Cybersecurity Situational Awareness and Visualization. Journal of Cyber Security and Mobility, 2025, 14(4): 955–980. DOI:10.13052/jcsm2245-1439.1448.

[10] Seid A M, Erbad A, Abishu H N, Albaseer A, Abdallah M, Guizani M. Blockchain-empowered resource allocation in multi-UAV-enabled 5G-RAN: a multi-agent deep reinforcement learning approach. IEEE Transactions on Cognitive Communications and Networking, 2023, 9(4): 991–1011. DOI:10.1109/TCCN.2023.3262242.

[11] Ayepah-Mensah D, Sun G, Boateng G O, Anokye S, Liu G. Blockchain-enabled federated learning-based resource allocation and trading for network slicing in 5G. IEEE/ACM Transactions on Networking, 2023, 32(1): 654–669. DOI:10.1109/TNET.2023.3297390.

[12] Zhou A, Li S, Ma X, Wang S. Service-oriented resource allocation for blockchain-empowered mobile edge computing. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3391–3404. DOI:10.1109/JSAC.2022.3213343.

[13] Kwantwi T, Sun G, Kuadey N A E, Maale G T, Liu G. Blockchain-based computing resource trading in autonomous multi-access edge network slicing: a dueling double deep Q-learning approach. IEEE Transactions on Network and Service Management, 2023, 20(3): 2912–2928. DOI:10.1109/TNSM.2023.3240301.

[14] Wang D, Jia Y, Liang L, Ota K, Dong M. Resource allocation in blockchain integration of UAV-enabled MEC networks: a Stackelberg differential game approach. IEEE Transactions on Services Computing, 2024, 17(6): 4197–4210. DOI:10.1109/TSC.2024.3418330.

[15] Yang J. Development strategy of rural e-commerce in the context of new media: construction of traceability system based on improved DPoS algorithm. International Journal of Web Engineering and Technology, 2025, 20(1): 4–21. DOI:10.1504/IJWET.2025.145517.

[16] Hewa T, Braeken A, Liyanage M, Ylianttila M. Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing. IEEE Transactions on Industrial Informatics, 2022, 18(10): 7174–7185. DOI:10.1109/TII.2022.3140792.

[17] Taskou S K, Rasti M, Nardelli P H. Blockchain function virtualization: a new approach for mobile networks beyond 5G. IEEE Network, 2022, 36(6): 134–141. DOI:10.1109/MNET.009.2100473.

[18] Hewa T, Porambage P, Kovacevic I, Weerasinghe N, Harjula E, Liyanage M, et al. Blockchain-based network slice broker to facilitate factory-as-a-service. IEEE Transactions on Industrial Informatics, 2022, 19(1): 519–530. DOI:10.1109/TII.2022.3173928.

[19] Zhao D, Huanshi X, Xun Z. Active exploration deep reinforcement learning for continuous action space with forward prediction. International Journal of Computational Intelligence Systems, 2024, 17(1): 1–8. DOI:10.1007/s44196-023-00389-1.

[20] Hu J, Paliwal Y, Kim H W Y X Z. Reinforcement learning with predefined and inferred reward machines in stochastic games.

Neurocomputing, 2024, 599(Sep.28): 1.1–1.19. DOI:10.1016/j.neucom .2024.128170.

[21] Deng X, Li J, Ma C, Wei K, Shi L, Ding M, et al. Blockchain assisted federated learning over wireless channels: dynamic resource allocation and client scheduling. IEEE Transactions on Wireless Communications, 2022, 22(5): 3537–3553. DOI:10.1109/TWC.2022.3219501.

[22] Liu M, Zhang M, Zhang P, Wang G, Chen X, Zhang H. Water level prediction model based on blockchain and LSTM. Journal of Intelligent and Fuzzy Systems, 2024, 46(1): 1–10. DOI:10.3233/JIFS-231411.

[23] Hao X, Yeoh P L, She C, Vucetic B, Li Y. Secure deep reinforcement learning for dynamic resource allocation in wireless MEC networks. IEEE Transactions on Communications, 2023, 72(3): 1414–1427. DOI:10.1109/TCOMM.2023.3337376.

[24] Adekunle T S, Alabi O O, Lawrence M O, Adeleke T A, Afolabi O S, Ebong G N, et al. An intrusion system for Internet of Things security breaches using machine learning techniques. Artificial Intelligence and Applications. 2024, 2(3): 165–171. DOI:10.47852/bonviewAIA420 21780.

Biographies

Deqiang Fei is currently a teacher at Dazhou Vocational College of Chinese Medicine. He graduated from the University of Electronic Science and Technology of China, majoring in Computer Network. He has published two monographs on computer applications and numerous academic papers in China. His main research interests include network information security and virtualization technology.

Xu Wei graduated from the Institute of Disaster Prevention in 2012, majoring in computer science and technology. She currently works at Dazhou Vocational College of Chinese Medicine. As a member, she participated in the curriculum development of the Basic Computer Application course at the college. Her research interests include network security, information security, and artificial intelligence.