Evolutionary game-based delegated proof of stake consensus for secure and efficient data storage in sensor networks

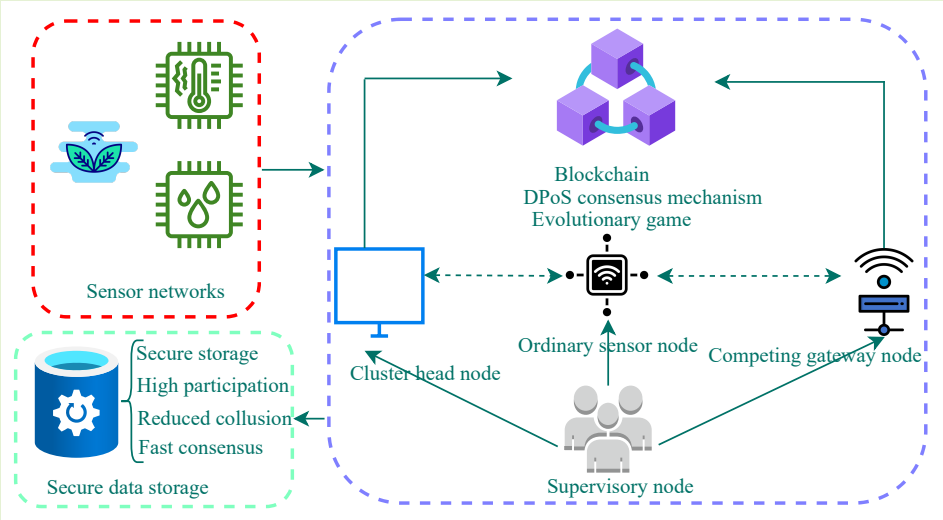
Article

Accepted Version

Evolutionary Game-Based Delegated Proof of Stake Consensus for Secure and Efficient Data Storage in Sensor Networks

Wencheng Chen, *Graduate Student Member, IEEE*, Jun Wang, *Senior Member, IEEE*, Jeng-Shyang Pan, *Senior Member, IEEE*, R. Simon Sherratt, *Fellow, IEEE*, and Jin Wang, *Senior Member, IEEE*

***Abstract*— With the rapid expansion of sensor networks across domains such as environmental monitoring, industrial automation, and smart healthcare, ensuring secure and reliable data storage in resource-constrained environments has become a critical challenge. Traditional centralized storage systems struggle with data tampering, privacy leakage, and vulnerability to collusion among nodes. Blockchain technology, characterized by decentralization, immutability, and traceability, provides a promising foundation for trustworthy sensor data management. Among various consensus mechanisms, Delegated Proof of Stake (DPoS) has been recognized for its efficiency and low energy consumption, yet it faces two critical issues: limited incentives for ordinary sensor nodes to participate in voting and the risk of collusion that undermines fairness and stability. To overcome these limitations, this study proposes a blockchain-enabled sensor data storage framework incorporating a four-party evolutionary game model. The model explicitly captures the strategic interactions among cluster head nodes, ordinary sensor nodes, competing gateway nodes, and supervisory nodes, while integrating reputation evaluation, penalty enforcement, and supervisory oversight. Through evolutionary game analysis, the proposed framework reveals the stability conditions of node behaviors and identifies strategies that promote fair and secure consensus. Simulation results verify that the mechanism enhances node participation, suppresses collusion, accelerates consensus convergence, and achieves superior throughput and fault tolerance compared with existing schemes. This research provides theoretical insights and practical guidance for designing secure, efficient, and scalable blockchain-enabled sensor network data storage systems.**



***Index Terms*— Sensor networks, Blockchain, Delegated proof of stake, Data storage, Evolutionary game.**

This work is supported in part by the Natural Science Foundation of China under Grants No. 62473146, the Industry-Academia Collaboration Program of Fujian Universities under Grant No. 2020H6006, the Fujian Province Special Funding Projects for Promoting High-Quality Development of Marine and Fishery Industry under Grant No. FJHYF ZH-2023-06, and the Key Project of Natural Science Foundation of Hunan Province under Grant No. 2024JJ3017. *(Corresponding author: Jin Wang)*

Wencheng Chen and Jun Wang are with the College of Electrical Engineering and Automation, Fuzhou University, Fuzhou 350116, China (e-mail: 220110006@fzu.edu.cn; wangjun_online@hotmail.com).

Jeng-Shyang Pan is with the School of Artificial Intelligence, Nanjing University of Information Science & Technology, Nanjing 210000, China (e-mail: jspan@ieee.org).

R. Simon Sherratt is with the School of Biomedical Engineering, the University of Reading, RG6 6AY, United Kingdom (e-mail: sherratt@ieee.org).

I. Introduction

With the accelerated convergence of digitalization and intelligence, sensor network technologies have been extensively deployed across critical domains such as environmental monitoring, industrial automation, healthcare, and smart cities [1]–[3]. According to recent forecasts, billions of sensors are expected to be connected worldwide by 2025, with the majority of data being generated and processed at the edge [1]. The continuous influx of massive heterogeneous sensing

Jin Wang is with the School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China (e-mail: jinwang@hnust.edu.cn).

devices and the generation of high-frequency sensor data impose severe challenges on traditional centralized storage architectures [4]. These centralized systems are prone to single points of failure, suffer from poor scalability and high latency, and struggle to meet the sensor network environment's multifaceted demands for real-time responsiveness, data integrity, privacy preservation, and trustworthy management [5].

Blockchain technology, with its intrinsic features of decentralization, immutability, traceability, and automated smart contract execution, offers a promising alternative for secure and reliable sensor data storage and management [6], [7]. By integrating data uploading, distributed ledger storage, and contract-driven automation, blockchain enhances data integrity and transparency while fostering trust and collaboration among multiple sensing nodes [8]. However, when applied to resource-constrained sensor networks characterized by limited energy and computational capabilities, blockchain systems face scalability bottlenecks, particularly regarding consensus mechanisms, which significantly hinder real-world deployment [9].

Among existing consensus algorithms, Delegated Proof of Stake (DPoS) has emerged as a widely adopted solution in blockchain–sensor network integration due to its rapid transaction confirmation, low energy consumption, and compatibility with lightweight infrastructures [10]. Nevertheless, when implemented in sensor network scenarios, DPoS exhibits two critical shortcomings. First, the voting participation rate of ordinary sensor nodes is generally low, as many remain idle or lack sufficient incentives to engage in elections due to energy constraints and limited computational ability. This leads to a concentration of voting power among a few cluster heads, undermining decentralization and fairness [11]. Second, restricted communication ranges and local information asymmetry among cluster head nodes can facilitate covert bribery, enabling malicious nodes to manipulate votes by colluding with ordinary sensors—an attack strategy known as "election collusion"—which compromises both the fairness of consensus and overall system stability [12]. In real-time sensor data applications, where supervisory mechanisms are often inadequate, the success rate of collusion attacks under DPoS may exceed 60% in certain cases, posing a significant threat to the security, reliability, and scalability of blockchain-enabled sensor networks.

Although various enhancements—such as the incorporation of reputation systems, dynamic elections, and randomized voting—have been proposed to mitigate DPoS vulnerabilities, these solutions largely remain at the algorithmic or procedural level. They often fail to provide a comprehensive framework for analyzing the strategic behavior and interactions among heterogeneous participants. In particular, conventional two-party or three-party game models are insufficient to capture the intricate dynamics inherent in blockchain-based sensor networks, which typically involve interactions among four key actors: cluster head (authorized) nodes, ordinary sensor nodes, competing gateway nodes, and supervisory nodes. This highlights the urgent need for a more expressive and adaptable modeling paradigm that can accommodate complex strategic behaviors and system evolution processes.

To address this gap, this paper focuses on the core issue of inadequate voting incentives and frequent collusion among nodes under the DPoS consensus mechanism in sensor networks. We propose an evolutionary game-theoretic model tailored for blockchain-enabled sensor data storage, incorporating four representative node types and systematically investigating how incentive, punishment, and supervision mechanisms influence the evolution of strategies and system-level stability. The proposed model integrates key characteristics of sensor network deployments and the operational rules of the DPoS consensus protocol. It establishes a multi-strategy evolutionary framework incorporating Nash equilibrium analysis, Jacobian matrix–based stability assessment, and replication dynamic equations. Simulation experiments are conducted to verify the model's adaptability and practical feasibility. The main contributions of this study are as follows:

i) We construct a blockchain-enabled sensor network storage framework and propose a four-party evolutionary game model involving cluster head nodes, ordinary sensor nodes, competing gateway nodes, and supervisory nodes. The model employs a strategic interaction matrix to capture the dynamic evolution and interrelations of node behaviors under the DPoS consensus mechanism.

ii) The game model integrates reputation, punishment, and supervisory mechanisms to systematically analyze the evolutionary paths and convergence characteristics of node strategies, while quantitatively evaluating their effectiveness in curbing irrational behaviors such as bribery and collusion in sensor networks.

iii) Simulation experiments and performance evaluations against existing two-party and three-party models demonstrate that the proposed method significantly improves sensor node participation rate, consensus convergence speed, and system fault tolerance, offering a practical solution for the secure and efficient implementation of blockchain-based sensor data storage.

The remainder of this paper is organized as follows. Section II reviews related work. Section III describes the problem and the proposed storage framework. Section IV details the construction of the evolutionary game model for the blockchain DPoS consensus mechanism. Section V presents the experimental results and analysis. Section VI provides the discussion, and Section VII concludes the paper.

II. Related work

A. Research on Blockchain in Sensor Networks

With the development of wireless sensor networks (WSNs), issues of secure storage, privacy protection, and reliable data management have become increasingly critical. Blockchain technology, with its decentralized and tamper-resistant nature, has been widely studied to address these challenges in WSNs.

Recent studies have primarily focused on lightweight authentication and privacy preservation. For example, Yu et al. [13] proposed a blockchain- and physically unclonable functions-based lightweight authentication protocol for WMSNs, demonstrating improved resistance to cyber and physical

security threats. Zhang et al. [14] introduced a blockchain-assisted biometric and password-based authentication and key agreement scheme for wireless body area networks, which preserves user privacy and reduces computational overhead. In addition, blockchain has been employed to improve secure data collection and storage efficiency. Li et al. [15] presented a blockchain-enhanced data collection framework for UAV-assisted WSNs, integrating spatiotemporal data aggregation and a Merkle-tree authentication mechanism to ensure secure data transmission. Pravija Raj et al. [16] designed a secure data collection model combining blockchain and machine learning for WSNs, effectively detecting malicious nodes and enhancing secure storage through blockchain-based registration and authentication. Hsiao et al. [17] proposed a blockchain-based encapsulation framework for wireless sensing data in smart agriculture, improving confidentiality, integrity, and tamper-resistance of environmental monitoring data. On the consensus side, researchers have also explored protocol-level innovations. For instance, Li et al. [18] developed a novel Proof-of-Channel consensus protocol for blockchain-enabled wireless networks, enhancing persistence, liveness, and resilience against jamming and Sybil attacks.

Although these studies have substantially advanced authentication, privacy, secure data collection, and consensus resilience in blockchain-enabled sensor networks, they fall short in resolving incentive misalignment among ordinary sensor nodes and collusion risks between cluster heads and gateway nodes. This gap underscores the need for a dynamic game-theoretic framework that integrates incentive, punishment, and supervision mechanisms to ensure both security and efficiency in blockchain-based sensor networks.

B. Research on Blockchain DPoS Consensus Mechanism

In blockchain technology, the DPoS consensus mechanism is extensively used in various blockchain systems owing to its high efficiency. In the context of resource-constrained sensor networks, DPoS has also received widespread attention because of its lightweight structure and low energy consumption. However, DPoS still faces challenges such as inactive node voting and collusion attacks, which directly threaten the stability and security of sensor network–based blockchain systems.

To address these challenges, scholars have proposed several optimization schemes. To enhance voting motivation, Zhu et al. [19] proposed a hierarchical reputation consensus mechanism that combined DPoS and Proof of Work to enhance the efficiency and security of certificate validation. Additionally, they introduced a rapid validation method based on block height and secure authentication. Ahmad et al. [20] proposed a reputation-delegated proof-of-interest consensus algorithm that selected agent nodes to participate in the consensus process by weighting both the number of votes and the reputation values of the nodes. However, such schemes remain vulnerable in sensor networks, as reputation values can be manipulated by a few highly reputable cluster head nodes, thereby creating new risks of collusion.

To address this limitation. Wang et al. [21] introduced a credit-weighted integrated election method that first calculated node activity using k-shell decomposition. It then determined the weighted vote value and selected the delegate by integrating both the node activity and the weighted vote. While this method encourages node participation, it is limited in handling malicious nodes because of a lack of continuous monitoring. To address this, researchers have proposed a node-lifting mechanism and dynamic election strategy for honest nodes. Feng et al. [22] introduced a dynamic strategy for honest nodes that effectively reduced the probability of selecting malicious nodes but did not significantly improve node voting activity. Additionally, to improve voting fairness and enhance the reliability and stability of the DPoS consensus mechanism, Xu et al. [23] proposed refining voting methods to include support, abstention, and opposition votes, thereby measuring the node's willingness to vote in three different ways.

Although these studies provide valuable insights, most of them remain static and fail to integrate incentive–punishment–supervision mechanisms into a unified framework. In particular, when applied to sensor networks characterized by high data real-time requirements and frequent topology changes, traditional optimization approaches cannot effectively balance efficiency and security. These limitations highlight the urgent need for a comprehensive consensus optimization framework that dynamically integrates incentive, punishment, and supervision mechanisms, which is precisely the gap addressed in this study through a four-party evolutionary game model tailored for sensor networks.

C. Game Theory in DPoS Consensus Mechanism

Game theory, as a mathematical tool for analyzing decision-making and strategy selection, has been extensively used in blockchain consensus mechanisms. In sensor network environments, where cluster head nodes, ordinary sensor nodes, and gateway nodes must frequently adjust strategies under resource and trust constraints, game-theoretic approaches provide a rigorous foundation for modeling strategic interactions. Pan et al. [24] investigated how dividends affected user decisions and welfare in DPoS consensus mechanisms and proposed using a theoretical framework to enhance resistance to unfair behavior. However, the two-party game model does not adequately reflect the complexity of the DPoS consensus mechanism or the dynamic influence of multiple subjects. Ren et al. [25] introduced a monitoring mechanism and a reward and punishment system and constructed a three-party evolutionary game model involving agent, voting, and supervisory nodes to analyze changes in node behavioral strategies before and after improvements to the consensus scheme, thereby providing a theoretical basis for optimizing network behavior. Therefore, Wang et al. [26] proposed a new DPoS consensus mechanism that verified nodes' votes based on reputation and optimized user costs and node utility through a three-stage Stackelberg game. These studies offer new perspectives for understanding interactions among different participants in the DPoS consensus mechanism and lay the foundation for optimizing network behavior through reward and punishment mechanisms.

Nevertheless, existing research is still confined to two-party or three-party models, which overlook the strategic roles of competing gateway nodes and supervisory nodes, and fail to capture collusive behaviors that frequently arise in sensor networks. In addition, the absence of feedback loops and temporal evolution analysis limits their ability to model real-world consensus dynamics in heterogeneous sensor networks. By extending beyond static two- or three-party models, this paper introduces a four-party evolutionary game model that explicitly incorporates cluster head nodes, ordinary sensor nodes, competing gateway nodes, and supervisory nodes. This approach enables a more accurate depiction of strategy evolution, consensus fairness, and system stability in blockchain-based sensor networks.

III. Problem Description and Storage Framework

With the rapid development of sensor network technology, the large-scale data generated by heterogeneous sensing devices challenges traditional centralized storage systems, which struggle to meet the sensor networks' security, reliability, and real-time requirements. Blockchain technology, with its decentralized, tamper-proof, and traceable features, offers a promising solution. This section defines the problem of applying the DPoS consensus mechanism in sensor networks, analyzes its security challenges, and presents an optimized data storage framework to improve both security and efficiency.

A. Game-Theoretic Characterization of the DPoS Consensus Mechanism in Sensor Networks

With the rapid proliferation of sensor networks, a vast number of distributed sensor nodes continuously generate high-frequency data streams. Traditional centralized storage architectures are increasingly inadequate to satisfy the multi-dimensional demands for security, reliability, and real-time responsiveness in such environments. In this context, blockchain technology—characterized by decentralization, immutability, and traceability—has emerged as a promising paradigm for secure and trustworthy sensor data storage. Among various blockchain consensus algorithms, DPoS has attracted considerable attention for its low energy consumption and high operational efficiency, making it particularly suitable for resource-constrained sensor networks. However, the integration of DPoS into sensor networks also introduces several prominent security challenges:

(1) Ordinary sensor nodes often lack sufficient incentive to actively participate in the voting process. Due to their limited computational resources and energy constraints, these devices are unable to execute complex encryption or validation algorithms, and therefore exhibit low participation rates. This leads to a prevalent issue of "voter absenteeism", whereby voting rights become concentrated among a small subset of cluster head nodes, undermining the fairness and dynamism of the consensus process.

(2) Cluster head nodes, owing to their limited communication ranges, possess only partial knowledge of the network state. This "local information asymmetry" provides fertile ground for electoral collusion. Competing gateway nodes may exploit this by bribing ordinary sensors or forming alliances with certain cluster heads, thereby manipulating voting outcomes. Once elected, these colluding nodes can monopolize block generation rights, significantly compromising system fairness and stability.

(3) Real-time sensor data applications, such as industrial monitoring or healthcare sensing, impose stringent latency constraints. Excessive consensus delays in blockchain systems directly degrade the timeliness of sensor data reporting, which may result in severe operational or safety risks. Thus, ensuring rapid consensus convergence while maintaining security is a critical challenge in blockchain-enabled sensor networks.

Although similar threats exist in traditional IT-based blockchain systems, they are further exacerbated in sensor networks due to constrained computation, intermittent connectivity, and the lack of persistent supervisory mechanisms. These challenges highlight the urgent need for incorporating dynamic supervision frameworks and game-theoretic modeling to systematically analyze and mitigate the evolution of collusive behaviors in resource-constrained, trust-deficient sensor network blockchain environments.

In the proposed model, four types of nodes are explicitly defined to capture the heterogeneity of blockchain-enabled sensor networks. Cluster head nodes act as authorized entities responsible for block validation and generation, leveraging their relatively higher computational and communication capabilities. Ordinary sensor nodes are widely distributed, resource-constrained devices that primarily generate sensing data and participate in voting. Competing gateway nodes possess partial computational resources and attempt to challenge cluster heads in elections for block-generation rights. Supervisory nodes function as trusted monitoring agents, detecting collusion and enforcing penalties through lightweight mechanisms. Notably, supervisory nodes themselves may also be subject to oversight to prevent abuse of authority. This categorization reflects the resource asymmetry and diverse roles within sensor networks, grounding the evolutionary game model in realistic deployment scenarios and reinforcing its practical relevance and adaptability.

B. DPoS-Based Sensor Network Blockchain Data Storage Framework

To effectively address critical challenges such as insufficient voting incentives, communication asymmetry, and node collusion in the DPoS consensus mechanism within sensor networks, this paper proposes an optimized blockchain data storage framework that tightly integrates the architectural characteristics of sensor networks with the operational logic of the DPoS protocol. The proposed framework is designed in accordance with the practical demands of sensor data applications and is structured into three functional layers: the sensor data collection layer, the consortium chain interaction layer, and the game-theoretic consensus layer, as illustrated in Fig. 1.

Sensor Data Collection Layer: This layer is responsible for the collection and preliminary processing of raw data

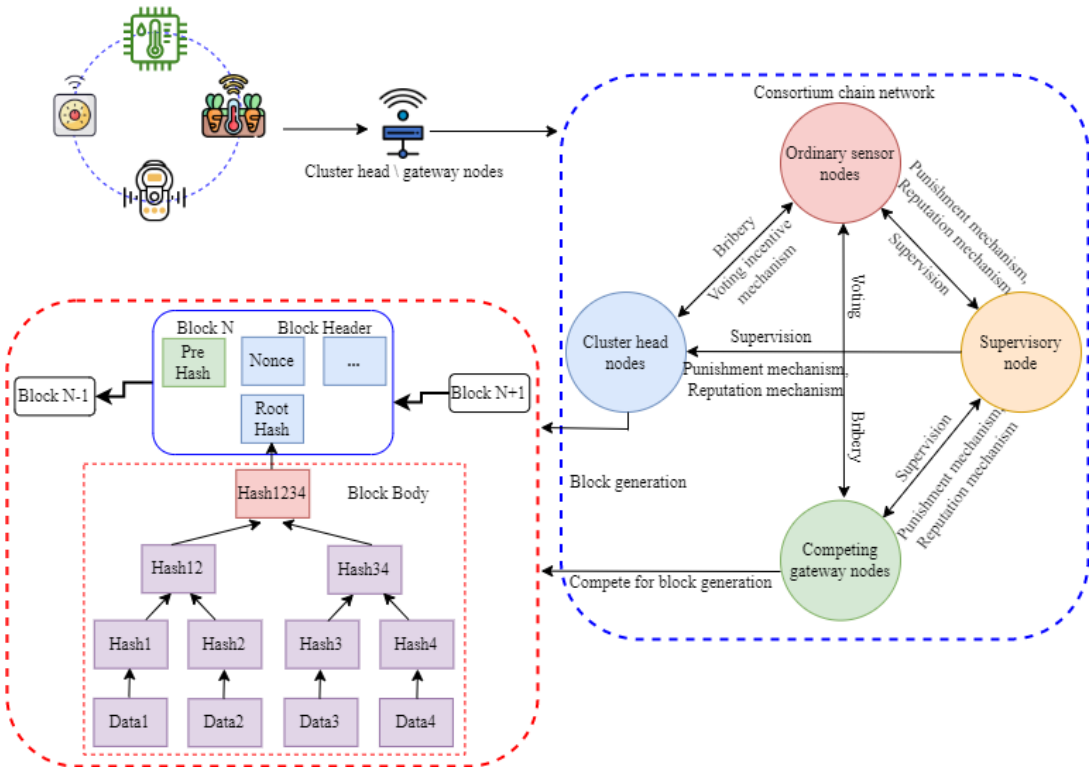


Fig. 1. Blockchain-based sensor network data storage framework

generated by distributed sensor nodes. These nodes—such as environmental sensors, wearable health monitors, and industrial detectors—typically operate with constrained energy and computational capacity. To mitigate these limitations, cluster head or gateway nodes are employed to perform local preprocessing tasks, including filtering, aggregation, compression, and initial validation. Such preprocessing reduces redundancy, enhances integrity, and improves transmission efficiency.

Consortium Blockchain Interaction Layer: Once preprocessed, the data is transmitted from cluster heads to a consortium blockchain network composed of multiple identified and trusted nodes. This layer employs a DPoS consensus mechanism to achieve efficient, low-latency, and energy-aware data consensus and on-chain storage. The system incorporates four categories of participants:

(1) Cluster head nodes: elected through voting by ordinary sensor nodes, responsible for validating sensor data and generating blocks.
(2) Ordinary sensor nodes: general sensor devices that generate data and participate in the voting process.
(3) Competing gateway nodes: alternative cluster head or gateway nodes that challenge incumbents in elections for block-generation rights.
(4) Supervisory nodes: trusted agents managed by authorities or operators to monitor network behavior, detect collusion, and enforce accountability through reputation evaluation and penalty mechanisms.

Game-Theoretic Consensus Layer: In the operation of the DPoS mechanism, the strategic interactions among the four node types fundamentally influence system security and consensus efficiency. To capture these dynamics, a game-theoretic framework is constructed to model the evolutionary behaviors of ordinary sensors, cluster heads, competing gateways, and supervisory nodes. The framework incorporates reputation differentiation, bribery penalties, supervisory rewards, and energy consumption constraints to guide the system's strategic evolution. Evolutionary game theory is employed to simulate and analyze strategy adaptation processes over time.

Within this multi-layered architecture, sensor nodes serve as ordinary participants responsible for data generation; cluster heads handle aggregation and block validation; competing gateways seek to challenge incumbents under rational constraints; and supervisory nodes ensure fair participation and detect collusion. The blockchain system, reinforced by game-theoretic mechanisms, incentivizes compliant behavior while penalizing misconduct, thereby enhancing the security, robustness, and trustworthiness of sensor data storage systems.

IV. Our Proposed Blockchain DPoS Consensus Mechanism Game Model Construction

In Section III, a blockchain-based data storage architecture tailored to the sensor network environment is constructed, and three core challenges inherent in applying the DPoS consensus mechanism to sensor networks are clearly identified: (1) the lack of incentive for ordinary sensor nodes to actively participate in voting, (2) the significant risk of collusion between cluster head nodes and competing gateway nodes during the election process, and (3) the stringent real-time requirements of sensor data that aggravate consensus latency issues. To systematically capture the evolutionary dynamics

of these misbehaviors and assess their impact on system stability, Section IV employs evolutionary game theory to model and analyze the strategic interactions among four key types of nodes in blockchain-enabled sensor networks: cluster head nodes, ordinary sensor nodes, competing gateway nodes, and supervisory nodes. Building upon the problem definition and architectural framework established in the previous section, this part focuses on modeling node behavior strategies, constructing corresponding payoff functions, analyzing the dynamic evolution trajectories, and determining the stability conditions. These efforts aim to provide a solid theoretical foundation and strategic insights for the optimization and robustness of the DPoS consensus mechanism in sensor network applications.

A. Modeling of Node Game Problems and Basic Assumptions

In sensor network environments, characteristics such as constrained node resources, limited communication ranges, and latency-sensitive data flows expose inherent limitations of the DPoS consensus mechanism. These include insufficient incentives for ordinary sensor nodes, frequent collusion among cluster head and competing nodes, and weaknesses in supervisory mechanisms. In response, this paper proposes a systematic modeling approach grounded in the behavioral evolution of node-level strategies, integrating both resource constraints and real-time sensing requirements into the design.

The four categories of nodes are redefined in the context of sensor networks:

(1) Cluster head nodes: Aggregation or sink nodes with higher computing and communication capacity. They can either follow legitimate voting results to produce blocks or attempt to manipulate elections by bribing ordinary sensors.
(2) Ordinary sensor nodes: Resource-constrained sensing devices responsible for generating raw data and voting. They can choose to vote normally or accept bribes, though their limited computation and energy directly affect their willingness to participate.
(3) Competing gateway nodes: Alternative cluster heads or gateways with partial resources, which compete to replace current authorized nodes. They may adopt legitimate competition strategies or collude with ordinary sensors to seize block production rights.
(4) Supervisory nodes: Trusted monitoring entities (e.g., operator-deployed agents or third-party verifiers) that oversee consensus fairness, detect collusion, and enforce penalties.

The four types of nodes modeled in this study—cluster head nodes, ordinary sensor nodes, competing gateway nodes, and supervisory nodes—are defined based on the practical characteristics of sensor network deployment. This node mapping framework ensures that the proposed model accurately captures the heterogeneity of device roles, energy constraints, communication limitations, and the dynamic nature of strategic interactions inherent in sensor networks.

Specifically, to capture the evolutionary dynamics of node behavior in a blockchain-enabled sensor data storage context, this study builds upon the foundational principles of the DPoS consensus mechanism [27] and the theoretical framework of evolutionary game theory [28], while integrating insights from relevant prior studies on blockchain–sensor network integration, incentive mechanisms, and collusion prevention [24]–[26]. It systematically considers the trade-offs among node interests and the behavioral feedback mechanisms influencing strategy selection across different types of sensor nodes. On this basis, the paper proposes a set of fundamental assumptions tailored to the constraints and characteristics of sensor networks. This assumption framework serves as both the theoretical underpinning and the modeling foundation for the subsequent analysis of node evolutionary trajectories and system stability.

(1) Bounded rationality of heterogeneous nodes. In line with evolutionary game theory [28], all four categories of participants—cluster head nodes, ordinary sensor nodes, competing gateways, and supervisory nodes—are assumed to exhibit bounded rationality in their decision-making due to energy, computational, and communication constraints. Each type of node selects strategies based on historical payoffs and behavioral feedback rather than perfect foresight. Let $M = \{supervisory M_1, non\text{-}supervisory M_2\}$, $B = \{collusive\, B_1,\ non\text{-}collusive\, B_2\}$, $G = \{normal\ voting G_1, abnormal\ voting G_2\}$, and $S = \{bribery A_1,\ non\text{-}bribery A_2\}$ denote the strategy sets available to supervisory nodes, competing nodes, ordinary sensor nodes, and cluster head nodes, respectively.
(2) Cluster head nodes may adopt bribery strategies. In sensor networks, cluster head or sink nodes are responsible for block production due to their higher computation and communication capacity [24]. Normally, they obtain block generation rights via legitimate voting and earn payoff P_1. However, due to local communication asymmetry and strong incentives for power retention, they may attempt to bribe ordinary sensor nodes, incurring a bribery cost C_1 but obtaining higher returns P_2 if successful. If detected, they face economic penalty F_1 and reputation loss L_1. This reflects the reality that cluster heads, with limited visibility beyond their own communication range, may exploit asymmetry to collude without being immediately exposed.
(3) Ordinary sensor nodes face trade-offs under resource constraints. As widely distributed, low-power devices, sensor nodes play a crucial role in voting but are severely constrained by energy consumption and computational limits [25].For ordinary sensor nodes, the payoff of normal voting is P_3, the payoff of bribery-induced abnormal voting is P_4, and the payoff of collusion-induced abnormal voting is P_5. All voting behaviors incur a participation cost C_2. Under supervision, bribery-based abnormal voting is penalized with a fine F_2 and and a reputation loss L_2, while collusion-based abnormal voting is penalized with a fine F_3 and a reputation loss L_3. However, in the absence of supervision, bribery strategies may yield higher immediate payoffs, particularly when the energy cost of

legitimate voting outweighs the perceived benefit, making short-term opportunism attractive.

(4) Competing gateway nodes can choose collusion or legitimate competition. Competing gateways (alternative cluster heads) seek to replace current authorized nodes. By colluding with ordinary sensors, they may gain block production rights and payoff P_6 but must bear collusion cost C_3. Alternatively, legitimate competition yields payoff P_7. Under active supervision, collusion incurs penalty F_4 and reputation loss L_4. Without supervision, however, collusion becomes a rational short-term strategy, particularly in resource-constrained and trust-deficient sensor networks [26].

(5) Supervisory nodes maintain fairness but are costly to operate. Supervisory nodes (e.g., trusted monitoring agents or operator-deployed verifiers) are responsible for detecting bribery, collusion, and abnormal voting. They incur cost C_4 but receive reward P_8 under normal monitoring. Upon violation detection, they additionally obtain penalties F_1, F_2, F_3, and F_4 from offenders. However, supervision in sensor networks is itself resource-intensive; failure to supervise or deliberate negligence may yield short-term payoff P_9 but risks severe penalty bF_5 under multi-layer oversight mechanisms (cross-verification, on-chain audits, or external audits). This reflects the high monitoring cost vs. incentive dilemma that supervisory entities face in practical deployments.

The game model presented in this paper focuses on the strategic interactions among the four types of nodes. By constructing the payoff function and penalty mechanism, and incorporating the specific roles and definitions of variables (P_1-P_9, C_1-C_4, F_1-F_5, L_1-L_4, b, etc.), we build the game matrix and derive the replication dynamics equations. Table I provides a detailed list of the variable symbols and their corresponding meanings, which are crucial for the subsequent analysis of the evolutionary process.

TABLE I

SYMBOL SETTING AND MEANING OF FOUR-PARTY GAME MODELS

Node type	symbol	Meaning
Cluster head nodes	A_1	Cluster head nodes adopt a bribe strategy
	A_2	Cluster head nodes adopt a non-bribery strategy
	P_1	Cluster head nodes gain block-generation rights through normal voting and profit from completing block-generation tasks
	P_2	Cluster head nodes successfully bribe ordinary sensor nodes for voting support
	C_1	Bribery cost for cluster head nodes to bribe ordinary sensor nodes
	F_1	Penalty cost for cluster head nodes when bribery is detected
	L_1	Reputation loss of cluster head nodes due to bribery behavior
Ordinary sensor nodes	G_1	Ordinary sensor nodes adopt normal voting strategy
	G_2	Ordinary sensor nodes abstain or adopt abnormal voting
	P_3	Ordinary sensor nodes' reward from normal voting
	P_4	Ordinary sensor nodes gain benefits by accepting bribes to participate in voting
	P_5	Ordinary sensor nodes collude with cluster head or competing nodes for profit
	C_2	Voting cost for ordinary sensor nodes
	F_2	Penalty cost for ordinary sensor nodes engaged in bribed or collusive voting
	L_2	Reputation loss of ordinary sensor nodes due to bribery or collusion
	F_3	Ordinary sensor node colluding in voting behavior fines
	L_3	Reputational loss from collusive voting behavior of Ordinary sensor node
Competing gateway nodes	B_1	Competing gateway nodes adopt collusive strategies
	B_2	Competing gateway nodes adopt a non-collusive strategy
	P_6	Competing gateway nodes successfully collude to profit from ordinary nodes gaining block bookkeeping rights
	P_7	Competing gateway nodes profit by attracting Ordinary sensor nodes to vote for block bookkeeping rights through normal channels
	C_3	Cost of collusion or bribery for competing gateway nodes
	F_4	Fines for collusive behavior and collusive intent at Competing gateway nodes
	L_4	Reputational loss from collusive behavior and collusive intent of Competing gateway nodes
Supervisory nodes	M_1	Supervisory nodes adopt supervisory strategies
	M_2	Supervisory nodes adopt a strategy of non-supervisory
	P_8	Supervisory node's supervisory profitability
	P_9	Supervisory node's non-supervised profiting
	C_4	Supervisory node's supervisory costs
	F_5	Supervisory nodes fail to supervise fines for bribery and collusive behavior
	bF_5	Fines for supervisory nodes turning a blind eye to bribery and collusive behavior

B. Benefits Matrix Construction

Building on the evolutionary game model of the DPoS system within the sensor network blockchain framework developed in the previous section, this section further analyzes the dynamic evolution of node behaviors under different strategy combinations, aiming to reveal the underlying patterns and distribution of stable strategies within the system's game structure.

In the four-party evolutionary game model, each participant corresponds to a distinct type of sensor network entity and makes strategic choices according to its preferences and resource constraints. To reflect the heterogeneity of sensor networks, the benefit matrix construction explicitly incorporates energy costs of sensor voting, communication range limitations of cluster heads, and latency penalties for real-time sensor applications.

(1) Let x represent the probability that a cluster head node chooses the bribery strategy, where $x \in [0,1]$, and $1-x$ denotes the probability of choosing the non-bribery strategy.

(2) Let y denote the probability that an ordinary sensor node adopts normal voting, where $y \in [0,1]$; accordingly, $1-y$ denotes the probability of abnormal voting. Here, energy consumption directly affects the cost of participation, so bribery strategies may appear more attractive to energy-constrained nodes.

(3) For a competing gateway node, let m denote the proba-

TABLE II

THE PAYOFF MATRIX FOR THE FOUR-PARTY EVOLUTIONARY GAME

			Cluster head node, Ordinary sensor node			
			Bribery x		Non-bribery $1-x$	
			Normal voting y	Abnormal voting $1-y$	Normal voting y	Abnormal voting $1-y$
Supervisory node, Competing gateway node	Supervisory z	Collusive m	$P_8 - C_4 + F_1 + F_4$ $P_7 - F_4 - L_4$ $P_1 - F_1 - L_1$ $P_3 - P_2$	$-C_4 + P_8 + F_1 + F_2 + F_3 + F_4$ $P_6 - C_3 - F_4 - L_4$ $P_2 - C_1 - F_1 - L_1$ $P_4 + P_5 - 2C_2 - F_2 - L_2 - F_3 - L_3$	$P_8 - C_4 + F_4$ $P_7 - F_4 - L_4$ P_1 $P_3 - C_2$	$P_8 - C_4 + F_3 + F_4$ $P_6 - C_3 - F_4 - L_4$ P_1 $P_5 - C_2 - F_3 - L_3$
		Non-collusive 1-m	$P_8 - C_4 + F_1$ P_7 $P_1 - F_1 - L_1$ $P_3 - C_2$	$P_8 - C_4 + F_1 + F_2$ P_7 $P_2 - C_1 - F_1 - L_1$ $P_4 - C_2 - F_2 - L_2$	$P_8 - C_4$ P_7 P_1 $P_3 - C_2$	$P_8 - C_4 + F_2 + F_3$ P_7 P_1 $P_3 - C_2 - F_2 - L_2 - F_3 - L_3$
	Non-supervisory $1-z$	Collusive m	$P_9 - bF_5$ P_7 P_1 $P_3 - C_2$	$P_9 - bF_5$ $P_6 - C_3$ $P_2 - C_1$ $P_4 + P_5 - 2C_2$	$P_9 - bF_5$ P_7 P_1 $P_3 - C_2$	$P_9 - bF_5$ $P_6 - C_3$ P_1 $P_5 - C_2$
		Non-collusive $1-m$	$P_9 - bF_5$ P_7 P_1 $P_3 - C_2$	$P_9 - bF_5$ P_7 $P_2 - P_1$ $P_4 - C_2$	$P_9 - bF_5$ P_7 P_1 $P_3 - C_2$	$P_9 - bF_5$ P_7 P_1 $P_3 - C_2$

bility of choosing a collusive strategy, where $m \in [0, 1]$, and $1 - m$ be the probability of choosing a non-collusive strategy. This models the trade-off between short-term collusive gains and the cost of building sustainable legitimacy.

(4) For a supervisory node, let z represent the probability of choosing the supervisory strategy, where $z \in [0, 1]$, and $1 - z$ be the probability of non-supervisory. Since supervision incurs monitoring cost but provides rewards from penalties, z reflects the supervision–cost dilemma in resource-limited sensor networks.

Based on these assumptions and analyses, the four-party game benefit matrix of the DPoS consensus mechanism in sensor networks is constructed, as presented in Table II. This matrix systematically incorporates not only the traditional payoffs and penalties, but also sensor-specific costs such as participation energy consumption, communication overhead, and real-time latency penalties, thereby capturing the unique characteristics of blockchain-enabled sensor data storage systems.

C. Four-Party Evolutionary Game Model Analysis

Building upon the game payoff matrix established in the previous section, this section introduces the concept of expected payoff to quantitatively model the returns of different sensor network nodes under varying strategy probability distributions. This modeling lays a theoretical foundation for the dynamic simulation of subsequent evolutionary paths and facilitates a deeper exploration of the behavioral evolution mechanisms of blockchain-enabled sensor nodes in distributed environments.

To characterize the variations in payoffs for different types of nodes under various strategic choices, this paper introduces the concept of expected return [29]. This metric reflects the weighted average payoff that a specific type of node can obtain by adopting a given strategy, considering the probabilistic distribution of strategies adopted by the other three types of nodes in the current game environment. In sensor networks, this expected return must explicitly incorporate the energy consumption of ordinary sensor nodes, the communication asymmetry of cluster head nodes, and the latency penalties associated with real-time sensing tasks.

For instance:

(1) E_{A1} denotes the expected payoff for a cluster head node when it selects the bribery strategy. This value is determined not only by the probabilities of ordinary sensors accepting bribery and competing gateways colluding, but also by the likelihood of supervisory detection and the additional communication overhead incurred in the bribery process.

(2) E_{G1} represents the expected payoff for an ordinary sensor node when it opts for the normal voting strategy, calculated by considering both the voting reward and its energy cost C_2, which plays a decisive role in the long-term willingness of resource-constrained sensors to participate.

(3) E_{M1} represents the expected payoff for a competing gateway node when it engages in collusion, factoring in both the collusion cost C3 and the risk of being penalized under supervision.

(4) E_{Z1} denotes the expected payoff of a supervisory node under active monitoring, combining supervisory cost C_4 with potential revenue from penalties (F_1, F_2, F_3, and F_4).

The computation of expected returns serves as the foundation for constructing the evolutionary replication dynamic equations. Since nodes are inclined to adopt strategies that yield higher payoffs, differences in expected returns—shaped by incentive mechanisms, energy-efficiency trade-offs, and supervision intensity—act as the driving force behind the continuous evolution of the system's strategic distribution. Consequently, a detailed analysis of the expected return functions for each node type is essential to uncover the stable evolutionary trajectories and equilibrium structures within the game system. This analysis also provides a theoretical basis

for guiding strategic adjustments and optimizing consensus performance in sensor networks with real-time data demands.

Based on the above definition, the expected payoff can be expressed as follows:

$$E_{s_k} = \sum_{a=1}^{2}\sum_{b=1}^{2}\sum_{c=1}^{2}(P_{abc} \times R_{s_k,abc}) \tag{1}$$

where, E_{s_k} denotes the expected payoff of the focal entity when adopting strategy s_k. The variables a, b, and c represent the strategies selected by the other three interacting entities, where a value of 1 or 2 corresponds to their choice of the first or second strategy, respectively. P_{abc} denotes the joint probability that these three entities adopt the specific strategy combination abc. $R_{s_k,abc}$represents the payoff received by the focal entity when it chooses strategy s_k while the other three entities simultaneously adopt the strategy profile abc.

The following presents the expected payoff calculation for the cluster head nodes when adopting the "bribery" strategy, based on the corresponding entries in the benefit matrix and incorporating bribery cost (C_1), supervision penalties (F_1, L_1), and communication overhead in sensor networks:

$$\begin{aligned} E_{A1} = {} & zmy(P_1 - F_1 - L_1) + zm(1-y)(P_2 - C_1 - \\ & F_1 - L_1) + z(1-m)y(P_1 - F_1 - L_1) + z(1- \\ & m)(1-y) + (P_2 - C_1 - F_1 - L_1) + (1-z)myP_1 \\ & + (1-z)m(1-y)y(P_2 - C_1) + (1-z)(1-m)yP_1 \\ & + (1-z)(1-m)(1-y)(P_2 - C_1). \end{aligned} \tag{2}$$

The expected payoff for cluster head nodes when selecting the non-bribery strategy is given by:

$$\begin{aligned} E_{A2} = {} & zmyP_1 - zm(1-y)P_1 + z(1-m)yP_1 \\ & + z(1-m)(1-y)P_1 + (1-z)myP_1 + (1- \\ & z)m(1-y)P_1 + (1-z)(1-m)yP_1 + (1- \\ & z)(1-m)(1-y)P_1. \end{aligned} \tag{3}$$

The average payoff for the authorized node across all strategy choices is:

$$\overline{E_A} = xE_{A1} + (1-x)E_{A2}. \tag{4}$$

Similar expected payoff functions for ordinary sensor nodes, competing gateway nodes, and supervisory nodes follow the same computational logic, with their respective strategy sets and cost structures reflecting energy consumption (C_2), collusion costs (C_3), and monitoring costs (C_4). To avoid redundancy, these derivations are omitted but can be analogized from the above.

D. Evolutionary Stable Strategy Solution

To further examine the evolutionary stability of the system as driven by the expected returns, this section formulates the replicator dynamic equations and investigates the evolutionary trends of the system under different strategy combinations, taking into account the behavioral characteristics of the game participants in the sensor network context. In evolutionary game theory, the long-term dynamic evolution of strategy selection among interacting agents can be effectively characterized using the replicator dynamic equation [30]. This equation captures the temporal change in the proportion of individuals adopting a specific strategy within a population, thereby reflecting the relative fitness or competitive advantage of that strategy compared to others.

The general form of the replicator dynamic equation is as follows:

$$F(P) = \frac{dP}{dt} = P\left(E_s - \bar{E}\right) \tag{5}$$

where P represents the probability that a subject selects a particular strategy, E_s denotes the expected return associated with that strategy given the current strategy profile, and $\bar{E}$ signifies the subject's average expected return across all possible strategy combinations.

(1) Based on the payoff matrix in Table II and the expected payoffs of each strategy, the replicator dynamic equation [30] for cluster head nodes is expressed as:

$$\begin{aligned} F(x) = \frac{\mathrm{d}x}{\mathrm{d}t} &= x(E_{A1} - \overline{E_A}) = x(1-x)(E_{A1} - E_{A2}) \\ &= x(x-1)(C_1 + P_1 - P_2 - yC_1 + zF_1 + zL_1 \\ &\quad - yP_1 + yP_2). \end{aligned} \tag{6}$$

In the sensor network setting, this difference is shaped not only by bribery cost C_1, payoff gap ($P_1 - P_2$), and supervision penalties (F_1, L_1), but also by the additional communication overhead that bribery entails when cluster heads attempt to influence geographically distributed sensors.

Let y_0 be defined as:

$$y_0 = \frac{C_1 + P_1 - P_2 + z(F_1 + L_1)}{C_1 + P_1 - P_2}. \tag{7}$$

1) When $y = y_0$, the function satisfies $F(x) \equiv 0$, indicating that any $x \in [0,1]$ constitutes a stable equilibrium point.
2) When $y \neq y_0$, solving $F(x) = 0$ yields two stable points at $x = 0$ and $x = 1$, indicating that both the "bribery" and "non-bribery" strategies adopted by authorized nodes can constitute evolutionarily stable strategy (ESS) under different conditions.

Lemma 1: When $0 < y < y_0$, the ESS for the cluster head nodes is $x = 1$; conversely, when $y_0 < y < 1$, the ESS shifts to $x = 0$, i.e., non-bribery dominates.

Proof: Taking the first-order partial derivative of $F(x)$ with respect to the variable x, we obtain: $\frac{\partial F(x)}{\partial x} = (2x - 1)(C_1 + P_1 - P_2 - yC_1 + zF_1 + zL_1 - yP_1 + yP_2)$. According to the stability theorem of differential equations, if $F(x) = 0$ and $\frac{\partial F(x)}{\partial x} < 0$, then x is a stable point for the strategy selection of cluster head nodes. Specifically, when $0 < y < y_0$, we have $F(x)\big|_{x=1} = 0$ and $\left.\frac{\partial F(x)}{\partial x}\right|_{x=1} < 0$, implying that $x = 1$ is an ESS. This indicates that when the probability of ordinary sensor nodes adopting the normal voting strategy is below y_0, cluster head nodes will ultimately favor the bribery strategy. Conversely, when $y_0 < y < 1$, since $F(x)\big|_{x=0} = 0$, $\left.\frac{\partial F(x)}{\partial x}\right|_{x=0} < 0$, it follows that $x = 0$ is an ESS. In this case, cluster head nodes will tend to adopt the non-bribery strategy, as the likelihood of ordinary sensor nodes voting normally exceeds the threshold y_0. ■

The phase diagram illustrating the strategic evolution of cluster head nodes is presented in Fig. 2. As shown, the plane $y = y_0$ divides the strategy space into two distinct regions, denoted as Region I and Region II. According to Lemma 1, when the initial state of the cluster head nodes lies within Region I, the system converges to the stable point $x = 1$, indicating that the cluster head nodes will ultimately adopt the bribery strategy. Conversely, if the initial state falls within Region II, the system converges to $x = 0$, meaning that the cluster head nodes will eventually adopt the non-bribery strategy.

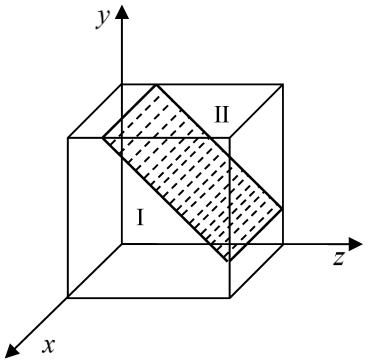


Fig. 2. Phase diagram of strategy selection for cluster head nodes

Following the detailed analysis of the strategic evolution of cluster head nodes, the evolutionary processes of ordinary sensor nodes, competing gateway nodes, and supervisory nodes can be derived using the same replicator dynamic equations and stability analysis framework. The critical conditions for their ESS, as well as the structural characteristics of their corresponding phase diagrams, follow analogous logical patterns. To avoid redundancy, only the key strategic behaviors of the remaining node types are briefly summarized below, with their respective phase diagrams presented separately.

(2) When the probability of cluster heads choosing bribery exceeds a threshold x_0, ordinary sensors tend to adopt normal voting to avoid penalties, provided that the supervisory intensity is strong enough. Otherwise, they are more likely to adopt abnormal voting or bribery-based voting, since energy-saving shortcuts yield immediate payoffs at the cost of long-term fairness. The phase diagram of this strategy evolution is shown in Fig. 3.

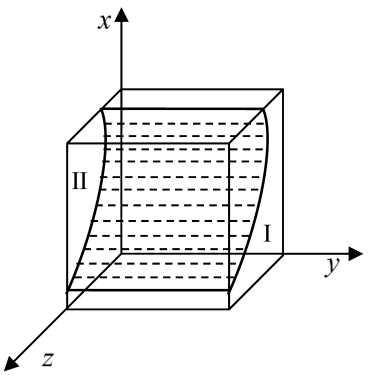


Fig. 3. Phase diagram of strategy selection for ordinary sensor nodes

(3) When the probability of supervisory nodes adopting active monitoring exceeds a critical threshold z_0, competing gateways tend to adopt non-collusive strategies. Otherwise, collusion dominates, as gateways can exploit local communication asymmetry and partial knowledge of cluster heads to form covert alliances. The corresponding phase diagram is shown in Fig. 4.

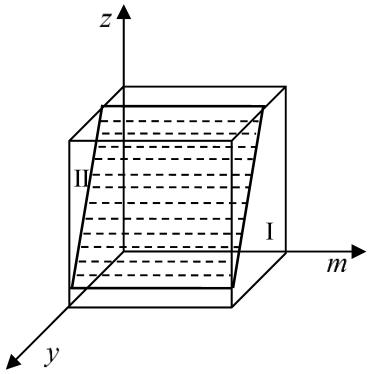


Fig. 4. Phase diagram of strategy selection for competing gateway nodes

(4) When the probability of competing gateways adopting collusion exceeds the threshold m_0, supervisory nodes converge toward active monitoring, since higher violation prevalence increases the expected returns from penalty rewards (F_1–F_4). Conversely, when collusion is rare, supervisors reduce monitoring efforts to save energy and cost (C_4), favoring non-supervision. The strategic phase diagram is shown in Fig. 5.

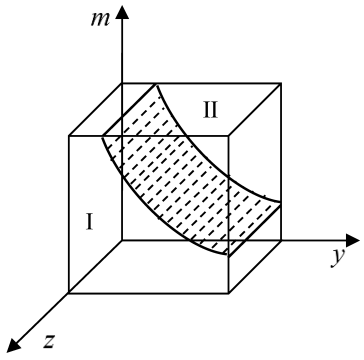


Fig. 5. Phase diagram of strategy selection for supervisory nodes

To analyze the stability of the four-party evolutionary game system, this study adopts two complementary approaches: Nash equilibrium [31] analysis and Jacobian matrix [32] eigenvalue analysis. As a fundamental concept in game theory, a Nash equilibrium refers to a strategy profile in which no participant has an incentive to unilaterally deviate, assuming that the strategies of others remain unchanged. In the context of evolutionary game theory, a pure-strategy Nash equilibrium can be regarded as an ESS under certain conditions [30]. To further determine the local stability of equilibrium points, we employ eigenvalue sign analysis of the Jacobian matrix. Specifically,

$$
J = \begin{bmatrix}
\frac{\partial F(x)}{\partial x} & \frac{\partial F(x)}{\partial y} & \frac{\partial F(x)}{\partial n} & \frac{\partial F(x)}{\partial z} \\
\frac{\partial F(y)}{\partial x} & \frac{\partial F(y)}{\partial y} & \frac{\partial F(y)}{\partial m} & \frac{\partial F(y)}{\partial z} \\
\frac{\partial F(m)}{\partial x} & \frac{\partial F(m)}{\partial y} & \frac{\partial F(m)}{\partial m} & \frac{\partial F(m)}{\partial z} \\
\frac{\partial F(z)}{\partial x} & \frac{\partial F(z)}{\partial y} & \frac{\partial F(z)}{\partial m} & \frac{\partial F(z)}{\partial z}
\end{bmatrix}
$$

$$
= \begin{bmatrix}
\begin{array}{l}(2x-1)(C_1+P_1-P_2\\ -yC_1+zF_1\\ +zL_1-yP_1+yP_2)\end{array} & \begin{array}{l}x(x-1)(-C_1\\ -P_1+P_2)\end{array} & 0 & x(x-1)F_1 \\
\begin{array}{l}-y(y-1)(P_3-P_4\\ +mC_2-mP_3\\ -zF_3-zL_3\\ +mzF_2+mzF_3\\ +mzL_2+mzL_3)\end{array} & \begin{array}{l}(-2y+1)(mP_3-mP_5\\ +zF_2+zF_3\\ +zL_2+zL_3\\ +xP_3-xP_4\\ +mxC_2-mzF_2\\ -mzL_2-mxP_3\\ -xzF_3-xzL_3\\ +mxzF_2+mxzF_3\\ +mxzL_2+mxzL_3)\end{array} & \begin{array}{l}-y(y-1)(P_3-P_5\\ +xC_2-zF_2\\ -zL_2-xP_3\\ +xzF_2+xzF_3\\ +xzL_2+xzL_3)\end{array} & \begin{array}{l}-y(y-1)(F_2+F_3\\ +L_2+L_3\\ -mF_2-mL_2\\ -xF_3-xL_3\\ +mxF_2+mxF_3\\ +mxL_2+mxL_3)\end{array} \\
0 & m(m-1)(C_3+P_6-P_7) & \begin{array}{l}(2m-1)(C_3-P_6+P_7\\ -yC_3+zF_4\\ +zL_4+yP_6-yP_7)\end{array} & m(m-1)(F_4+L_4) \\
\begin{array}{l}-z(z-1)(xF_1-xF_3\\ +mxF_2+mxF_3\\ +xyF_3-mxyF_2\\ -mxyF_3+bxyF_5\\ -bmxyF_5)\end{array} & \begin{array}{l}-z(z-1)(-F_2-F_3\\ -bF_5+mF_2\\ +xF_3-mxF_2\\ -mxF_3+bmF_5\\ +bxF_5-bmxF_5)\end{array} & \begin{array}{l}-z(z-1)(-F_2+F_4\\ +xF_2+xF_3\\ +yF_2-xyF_2\\ -xyF_3+byF_5\\ -bxyF_5)\end{array} & \begin{array}{l}(-2z+1)(F_2-C_4+F_3+P_8-P_9\\ +bF_5-mF_2+mF_4+xF_1\\ -xF_3-yF_2-yF_3-byF_5\\ +mxF_2+mxF_3+myF_2+xyF_3\\ -mxyF_2-mxyF_3+bmyF_5+bxyF_5\\ -bmxyF_5)\end{array}
\end{bmatrix}
$$

the system's replicator dynamic equations are formulated and differentiated to construct the corresponding Jacobian. According to the principle of differential equation stability theory, if all eigenvalues of the Jacobian matrix are negative, the corresponding equilibrium point is deemed locally asymptotically stable [31]. According to the stability principle of differential equations, when the system of replicator dynamics satisfies $F(x) = F(y) = F(m) = F(z) = 0$, the model admits 16 pure-strategy equilibrium solutions. In evolutionary game theory, any strategy combination that satisfies this equilibrium condition is considered a pure-strategy Nash equilibrium [31], implying that no participant has an incentive to unilaterally deviate from their strategy when the strategies of others remain unchanged. Based on Friedman's analytical framework [30], certain pure-strategy Nash equilibria can further qualify as ESS under specific conditions. Ritzberger [31] emphasizes that in asymmetric evolutionary games, an ESS typically corresponds to a strict Nash equilibrium. To further evaluate the local stability of these equilibrium points, this study applies Lyapunov's First Theorem [32], constructs the Jacobian matrix derived from the replicator dynamics, and computes its eigenvalues. If all eigenvalues exhibit negative real parts, the equilibrium point is locally asymptotically stable. This method is widely adopted for assessing local nonlinear stability in evolutionary game models. Accordingly, this paper analyzes all 16 pure-strategy combinations— $E_1(0,0,0,0)$, through $E_{16}(1,1,1,1)$—formed by the four types of game participants, and constructs their respective Jacobian matrices, as shown below:

In the asymmetric game, an evolutionary stable equilibrium must also be a strict Nash equilibrium, which subsequently must be a pure strategy equilibrium [31]. Thus, only the stability of the pure strategy equilibria is discussed. The eigenvalues and stability analysis of the equilibrium points $E_1 \sim E_{16}$ eigenvalues and the equilibrium points are shown in Table III.

E. Equilibrium Point Stability Analysis

Building upon the preceding game evolution analysis, this section introduces the methodologies for determining the Jacobian matrix and identifying Nash equilibria, in order to analyze the system's stable equilibrium structure under specific parameter settings. In the sensor network context, this stability analysis not only considers traditional payoff differences but also incorporates factors such as energy consumption of nodes, communication overhead between geographically distributed sensors, and the timeliness of supervisory actions.

According to Lyapunov's first method, a local equilibrium point qualifies as an ESS only if all the eigenvalues of its associated Jacobian matrix are negative. Based on the eigenvalue analysis presented in Table III, the Jacobian matrices corresponding to the 16 local equilibrium points are examined. The results indicate that only the following points exhibit potential stability:$E_2(0,0,1,0)$, $E_4(0,0,1,1)$, $E_6(0,1,0,1)$, $E_9(1,0,0,0)$, $E_{10}(1,0,0,1)$, $E_{11}(1,0,1,0)$, and $E_{12}(1,0,1,1)$.

However, based on the preceding assumptions and parameter constraints, the following inequality relationships hold:

$$
\begin{cases}
-(F_1+L_1) < 0 \\
-(F_2+F_3+L_2+L_3) < 0 \\
P_8 - C_4 - P_9 < 0
\end{cases} \tag{8}
$$

These constraints indicate that effective punishment mechanisms, combined with the supervisory cost–reward trade-

off (P_8-C_4-P_9), determine which equilibria remain evolutionarily stable in practice. Therefore, the equilibrium point $E_6(0,1,0,1)$ is identified as the ESS of the system.

Based on the eigenvalue analysis, equilibrium point $E_6(0,1,0,1)$ is identified as the ESS of the system. In the sensor network context, this equilibrium implies that cluster head nodes refrain from bribery, ordinary sensor nodes consistently participate in normal voting, competing gateways avoid collusion, and supervisory nodes remain active. Such a configuration balances energy efficiency, consensus fairness, and network trustworthiness. Although supervisory monitoring incurs computational and energy costs, the penalty-and-reward mechanism ensures that the supervisory role remains profitable, thereby preventing negligence. Overall, equilibrium point E_6 reflects the optimal trade-off between energy consumption, communication efficiency, and consensus security in resource-constrained sensor networks, confirming its role as the evolutionarily stable state of the proposed DPoS consensus game model.

V. Experimental Results and Analysis

A. Simulation Setup

Trade-offs and decisions are inherent in blockchain DPoS consensus mechanisms. Consequently, this section focuses on how the four parties—Cluster head nodes, Ordinary sensor nodes, Competing gateway nodes, and supervisory nodes—change their behavioral strategy preferences over time. According to the stability analysis in Section IV, the optimum state of the four-party evolutionary game is (non-bribery, normal voting, non-collusive, supervisory), corresponding to strategy combination $E_6(0,1,0,1)$.

To ensure reproducibility, the simulation incorporates both theoretical parameters and empirical data. We adopt the publicly available Intel Berkeley Research Lab (IBRL) sensor dataset, which contains time-series measurements (temperature, humidity, light, and voltage) collected from 54 Mica2Dot wireless sensor nodes deployed in a real-world indoor environment. This dataset provides representative characteristics of resource-constrained sensor networks and is widely used as a benchmark in IoT-related studies. By mapping sensor devices to ordinary nodes, cluster heads to authorized nodes, gateway devices to competing nodes, and monitoring agents to supervisory nodes, we effectively align the dataset with the four-node game-theoretic framework.

The simulations are conducted on a workstation configured with an Intel Core i7 processor, 32 GB of memory, and Windows 11 operating system, ensuring that the results can be reproduced under a standard computing environment. Numerical simulations are implemented using MATLAB R2017b, following the replicated dynamic equations and parameter constraints outlined in Section IV.

Based on the actual DPoS consensus mechanism [27], this study adopts assignment methods from existing research literature [24]–[26] to reasonably set the model parameters. The initial probabilities for the strategy selection of the four entities are set at $[0.5, 0.3, 0.2, 0.3]$. The horizontal axis represents time (t), while the vertical axis represents the probability (P) that the authorized node (x), ordinary node (y), competing node (m), and supervisory node (z) select their respective strategies. The combination of real-world sensor data with game-theoretic simulations allows the model to capture both theoretical dynamics and practical constraints, thereby enhancing its credibility and application relevance.

The specific parameter settings are summarized in Table IV.

TABLE III

Stability Analysis of Pure Strategy Equilibrium Points

Balance point	Eigenvalue	Positive or negative	Stability	Scene
(0,0,0,0)	$P_2-P_1-C_1$,0,$P_6-P_7-C_3$,$P_8-P_9-C_4+F_2+F_3+bF_5$	N,0,N,N	Saddle point	\
(0,0,0,1)	$P_2-P_1-C_1-F_1-L_1$,$F_2+F_3+L_2+L_3$, $P_6-C_3-P_7-F_4-L_4$,$P_9+C_4-P_8-F_2-F_3-bF_5$	N,+,N,N	Unstable	\
(0,0,1,0)	$P_2-P_1-C_1$,P_3-P_5,$P_7-P_6+C_3$, $P_8-P_9-C_4+F_3+F_4+bF_5$	N,N,N,N	ESS	(1)
(0,0,1,1)	$P_2-C_1-P_1-F_1-L_1$,$P_3+F_3+L_3-P_5$, $P_7+C_3+F_4+L_4-P_6$,$P_9+C_4-P_8-F_3-F_4-bF_5$	N,N,N,N	ESS	(2)
(0,1,0,0)	0,0,0,$P_8-P_9-C_4$	0,0,0,N	Saddle point	\
(0,1,0,1)	$-F_1-L_1,-F_2-F_3-L_2-L_3,-F_4-L_4$,$P_9+C_4-P_8$	-,-,-,N	ESS	(3)
(0,1,1,0)	0,P_5-P_3,0 ,$P_8+F_4+bF_5-C_4-P_9$	0,N,0,N	Saddle point	\
(0,1,1,1)	$-F_1-L_1$,$P_5-P_3-F_3-L_3$,F_4+L_4, $P_9+C_4+F_2-P_8-F_3-F_4-bF_5$	-,N,+,N	Unstable	\
(1,0,0,0)	$P_1+C_1-P_2$,P_3-P_4,$P_6-C_3-P_7$,$P_8-C_4-P_9+F_1+F_2+bF_5$	N,N,N,N	ESS	(4)
(1,0,0,1)	$P_1+C_1+F_1+L_1-P_2$,$P_3+F_2+L_2-P_4$,$P_6-C_3-F_4-L_4-P_7$, $P_9+C_4-P_8-F_1-F_2-bF_5$	N,N,N,N	ESS	(5)
(1,0,1,0)	$P_1+C_1-P_2$, $P_3+C_2-P_4-P_5$,$P_7+C_3-P_6$, $P_8+F_1+F_2+F_3+F_4+bF_5-P_9-C_4$	N,N,N,N	ESS	(6)
(1,0,1,1)	$P_1+C_1+F_1+L_1-P_2$,$P_3+C_2+F_2+L_2+F_3+L_3-P_4-P_5$, $P_7+C_3+F_4+L_4-P_6$,$P_9+C_4-P_8-F_1-F_2-F_3-F_4-bF_5$	N,N,N,N	ESS	(7)
(1,1,0,0)	0,P_4-P_3,0,$P_8+F_1+bF_5-P_9-C_4$	0,N,0,N	Saddle point	\
(1,1,0,1)	F_1+L_1,$P_4-P_3-F_2-L_2$,$-F_4-L_4$,$P_9+C_4-P_8-F_1-bF_5$	+,N,-,N	Unstable	\
(1,1,1,0)	0,$P_4+P_5-P_3-C_2$,0,$P_8+F_1+F_4+bF_5-P_9-C_4$	0,N,0,N	Saddle point	\
(1,1,1,1)	F_1+L_1,$P_4+P_5-P_3-C_2-F_2-F_3-L_2-L_3$, F_4+L_4, $P_9+C_4-P_8-F_1-F_4-bF_5$	+,N,+,N	Unstable	\

Note: N indicates that the positivity or negativity of the eigenvalue could not be determined; ESS indicates evolutionary stabilization strategy.

B. Influence of Competitive Gateway Nodes on the Evolution of Parties' Strategies

In sensor networks, competing gateway nodes typically represent gateway devices or edge servers with partial computing resources. Their strategic behavior directly influences the speed of consensus formation. Under the parameter conditions described in Section V-A, scenario (3) is satisfied.

When competing gateway nodes choose not to collude ($m = 0$), the system evolves rapidly toward stability. This benign behavior accelerates the convergence to the equilibrium strategy combination $E_6(0, 1, 0, 1)$, where bribery and collusion are suppressed, and supervisory monitoring remains active.

Conversely, when competing gateway nodes choose collusion ($m = 1$), malicious behaviors emerge. The evolution trend becomes slower, delaying the stabilization of strategies. This inhibitory effect arises because collusive gateways manipulate ordinary nodes' voting outcomes, thereby increasing instability. Fig. 6 shows that the system requires more iterations to converge when collusion occurs.

C. Impact of Supervision on the Reputation Value of Different Subjects

The reputation mechanism is critical in sensor networks, where lightweight nodes have limited computational capacity but rely on trust-based coordination. To evaluate its impact, the reputation losses were set as $L_2 = \{0, 5, 15, 60\}$ and $L_3 = \{0, 0.5, 26, 75\}$. The strategy evolution process and the results of the four-party game are shown in Fig. 7.

TABLE IV
PARAMETER SETTINGS

Parameter	Value	Parameter	Value
P_1	8	P_2	12
P_3	11	P_4	6
P_5	15	P_6	10
P_7	7	P_8	16
P_9	9	F_1	1
F_2	2	F_3	5
F_4	6	F_5	8
L_1	0.6	L_2	0.3
L_3	0.5	L_4	0.9
C_1	3	C_2	2
C_3	4	C_4	5
b	0.5		

As shown in Fig. 7, when the reputation penalty increases, ordinary sensor nodes gradually stabilize on normal voting, while the bribery behavior of cluster head nodes and the collusion of competing gateway nodes decline toward zero. Supervisory nodes' monitoring probability decreases slightly after achieving stability, reflecting an energy–security tradeoff.

This analysis indicates that reasonable reputation thresholds significantly improve node participation and reduce malicious behaviors. However, excessive penalties yield diminishing returns, suggesting that a calibrated reputation-loss threshold must be set to balance fairness and energy efficiency.

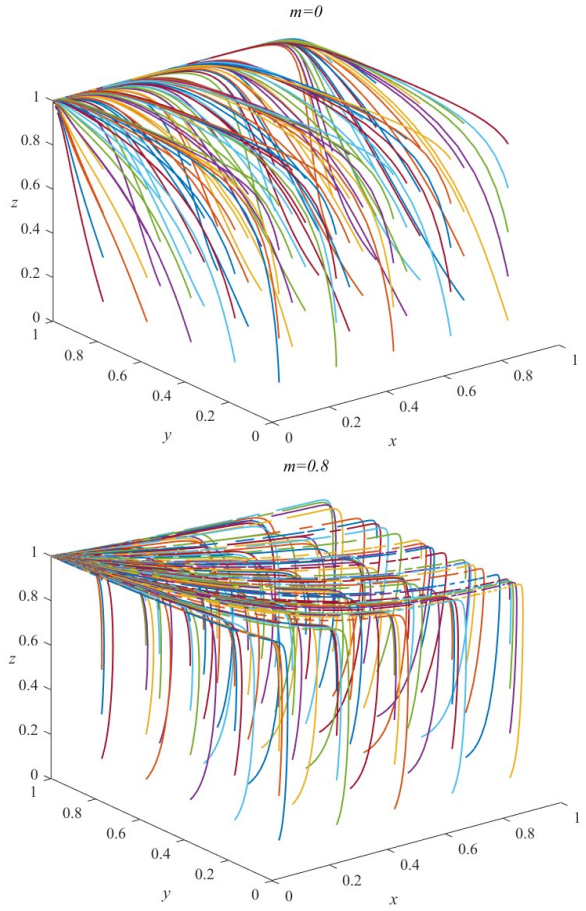


Fig. 6. Influence of competing gateway nodes on the evolution of parties' strategies

D. The Effect of Different Punishments on the Subject's Strategy Choice

The penalty mechanism deters misconduct in blockchain-based sensor networks. We tested penalty values $F_2 = \{0, 2, 10\}$ and $F_3 = \{0, 5, 16\}$. The strategy evolution process and the results of the four-party game are shown in Fig. 8.

As illustrated in Fig. 8, increasing penalties leads to higher probabilities of normal voting among ordinary sensor nodes and stronger supervisory participation, while bribery and collusion are nearly eliminated.

This shows that penalty mechanisms enhance both fairness and stability, provided penalty magnitudes are chosen carefully to avoid excessive energy consumption in supervisory monitoring.

E. The Effect of Different Punishment Levels on the Subject's Strategy Choice

In practice, supervisory nodes (e.g., cluster heads or sink nodes) incur energy costs when performing monitoring. To study the effect of punishment severity for supervisory negligence, the penalty strength was varied: $b = \{0, 0.5, 3\}$, and study its effect on the stable evolutionary trend of the four-party nodes, as shown in Fig. 9.

Fig. 9 reveals that as b increases, supervisory nodes are more motivated to remain active, while ordinary sensor nodes'

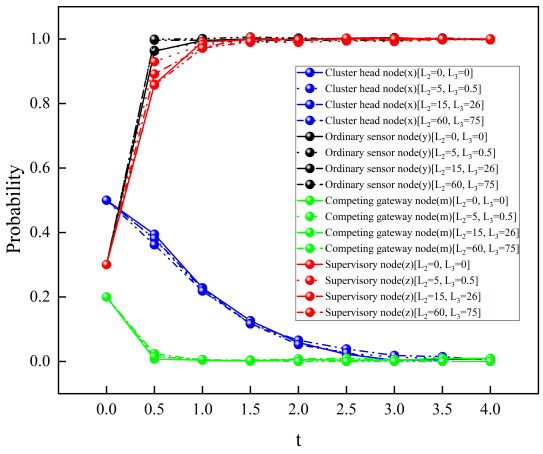


Fig. 7. Impact of supervision on the reputation of different subjects

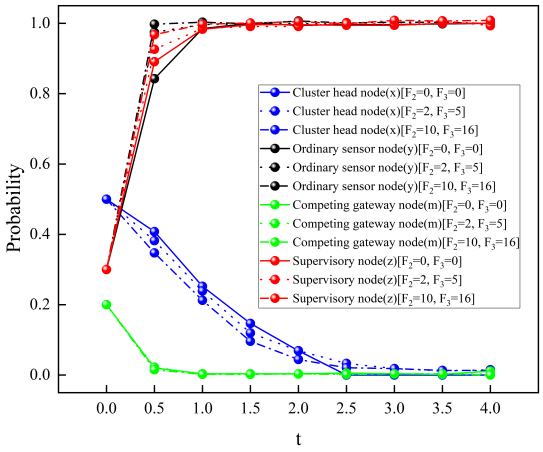


Fig. 8. Effect of different penalties on subject's strategy choice

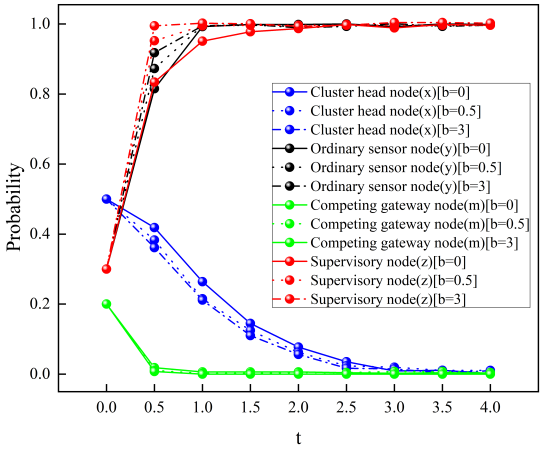


Fig. 9. Impact of different penalty levels on subject's strategy choice

voting enthusiasm improves. Cluster head nodes abandon bribery, and competing gateway nodes reduce collusion.

These results confirm that adaptive tuning of punishment severity is necessary during different stages of network evolution, enabling secure consensus while minimizing unnecessary monitoring overhead in energy-constrained sensor networks.

F. The Effect of Different Collision Costs at Competitive gateway Nodes on the Subject's Strategy Choice

To analyze the effect of collusion costs, we varied $C_3 = \{0, 4, 10\}$. The strategy evolution process and the results of the four-party game are shown in Fig. 10.

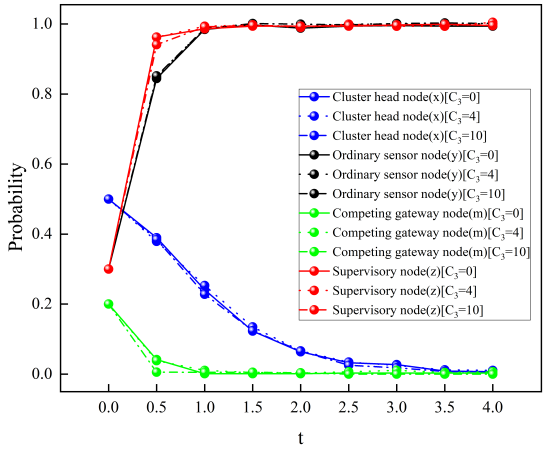


Fig. 10. Effect of different collision costs of competing gateway nodes on the subject's strategy choice

Fig. 10 demonstrates that as collusion costs increase, competing gateway nodes increasingly adopt non-collusive strategies, ordinary sensor nodes prefer normal voting, and authorized nodes stabilize at non-bribery behavior.

Thus, by setting reasonable collusion costs, the system can discourage malicious coordination, foster greater node participation, and reduce supervisory burdens, ultimately promoting efficient consensus in large-scale sensor deployments.

G. Game-Theoretic Model Comparison Experiments

To comprehensively validate the effectiveness and advantages of the proposed four-party evolutionary game model in sensor network blockchain environments, this section conducts a systematic comparison with existing two-party and three-party models commonly adopted in related literature. The analysis focuses on two critical dimensions: the stabilization paths of node strategies and the convergence speed of system dynamics.

(1) Comparative analysis of strategy stabilization paths. Fig. 11 presents the strategy stabilization trajectories of cluster head nodes, ordinary sensor nodes, and supervisory nodes under two-party, three-party, and four-party models. As shown, the four-party model stabilizes within approximately 1 second, which is significantly faster than the three-party (1.5 seconds) and two-party (3 seconds) cases. Compared with the two-party model, the four-party model reduces the stabilization time by about 66.7%, and compared with the three-party model, the convergence speed improves by about 33.3%. This improvement arises from the introduction of reputation supervision, supervisory incentives, and collusion cost adjustments, which jointly accelerate convergence and reinforce consensus fairness in sensor networks.

(2) Comparative analysis of behavioral strategy selection. Fig. 12 compares node behavioral strategies under the three-party and four-party models when supervisory nodes are

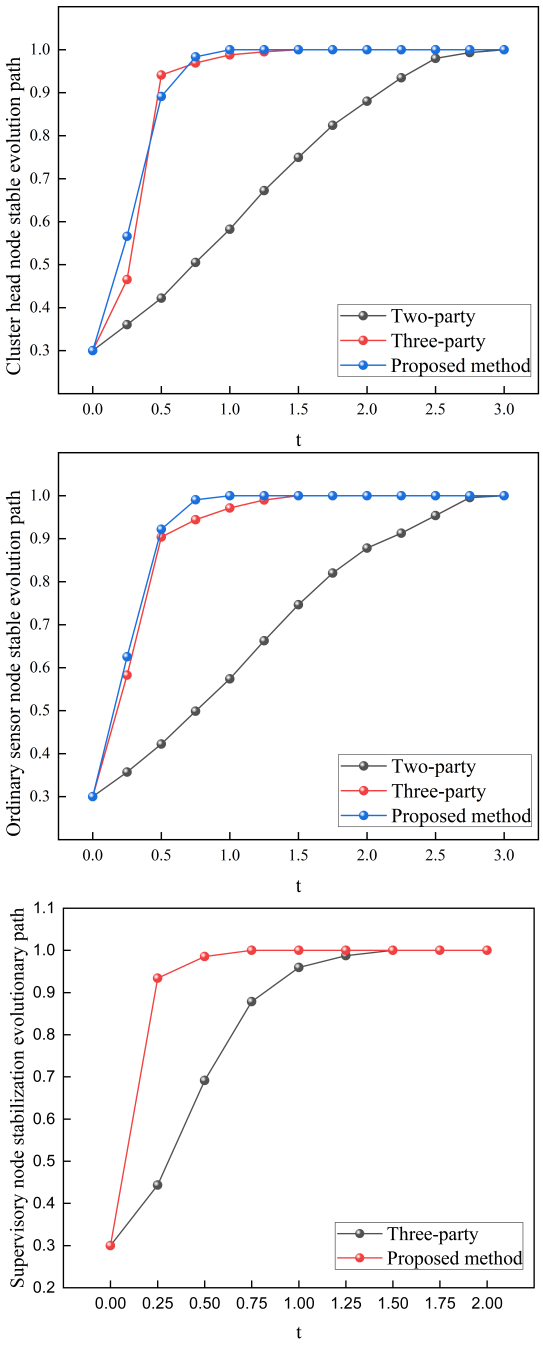


Fig. 11. Stable evolutionary paths of each node type

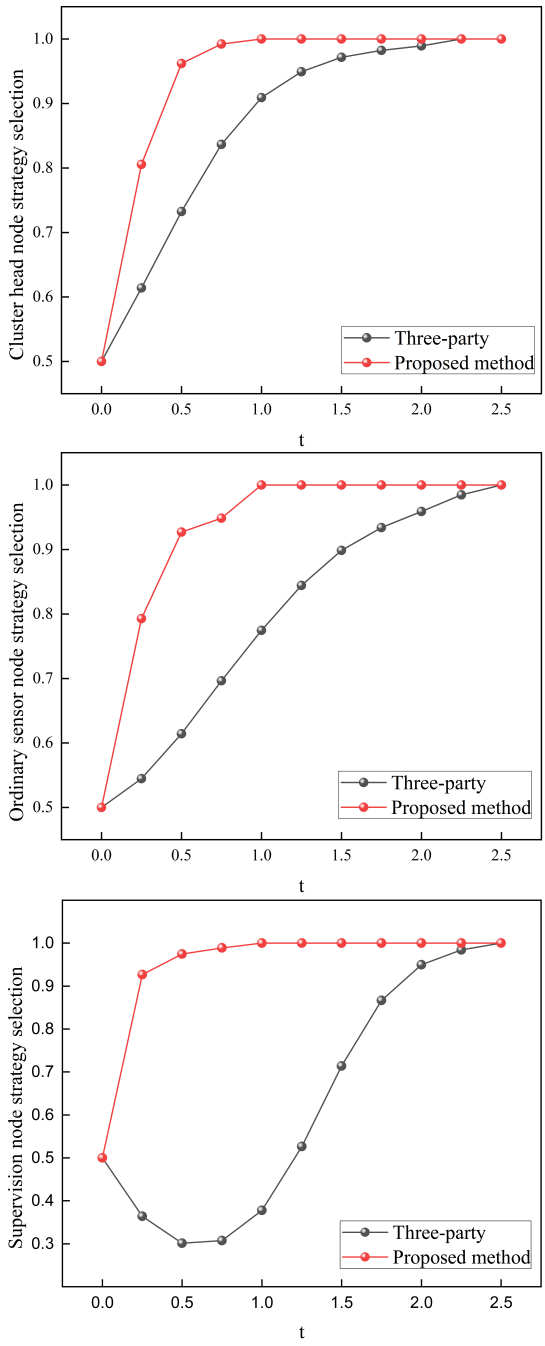


Fig. 12. Strategy selection of nodes

inactive and the penalty parameter is set to $b = 0.5$. The results show that the convergence time for both cluster head and ordinary sensor nodes is shortened from 2.5 seconds in the three-party model to 1 second in the four-party model—an improvement of about 60%. This highlights the critical role of competing gateway nodes in accelerating behavioral adaptation and improving collaborative responsiveness across heterogeneous sensor devices.

H. Simulation Experiments on Blockchain Performance

Building upon the analyses in Sections V-B to V-F, this study integrates reputation mechanisms, punishment strategies, supervisory incentives, and rational collusion costs into the DPoS framework to enhance the security and efficiency of sensor network blockchain systems. To validate performance improvements, simulation experiments were conducted and compared with the original DPoS mechanism and the methods in [21] and [19], focusing on throughput, participation incentives, and error node ratios. The simulations were implemented in Python, with 301 nodes (100 cluster head nodes and 201 ordinary sensor nodes, including competing gateway nodes), across 50 consensus rounds.

(1) Comparison of network throughput.

Network throughput. Throughput, measured in Transac-

tions Per Second (TPS), was evaluated under varying block generation settings. As shown in Fig. 13, the proposed method achieves an average TPS of 121.79, which is 61.6% higher than the original DPoS (75.36), 40.6% higher than [21] (86.63), and 5.9% higher than [19] (115.00). Moreover, the TPS remained relatively stable, demonstrating robustness against fluctuating sensor data loads.

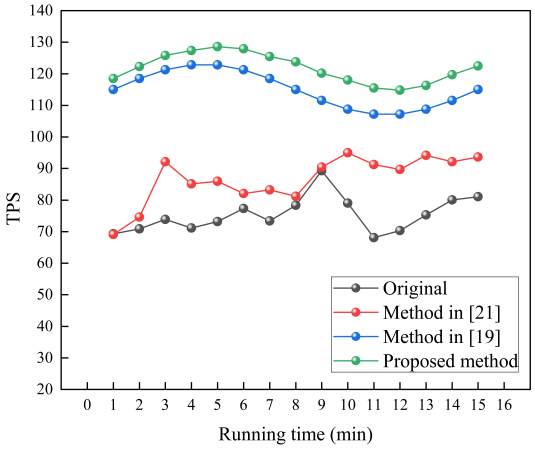


Fig. 13. Comparison of system throughput

(2) Node participation incentives

Fig. 14 shows the voting participation rate evolution. The proposed model achieved an average participation rate of 83.86% after 50 rounds, compared with 45.99% (original DPoS), 77.84% ([21]), and 70.00% ([19]). This improvement illustrates that ordinary sensor nodes are more effectively incentivized through reputation and supervisory mechanisms, addressing the issue of voter apathy in sensor networks.

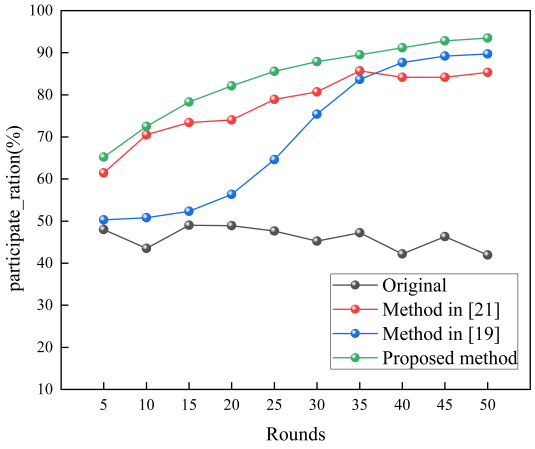


Fig. 14. Comparison of node participation incentives

(3) Faulty node ratio.

As shown in Fig. 15, the proportion of faulty nodes (e.g., misbehaving or collusive gateways) decreased to 0.263% under the proposed mechanism, compared with 47.91% (original DPoS), 1.12% ([21]), and 0.83% ([19]). This reduction highlights the effectiveness of penalty enforcement and supervisory oversight in suppressing malicious behaviors, thereby ensuring consensus reliability and secure data storage in large-scale sensor deployments.

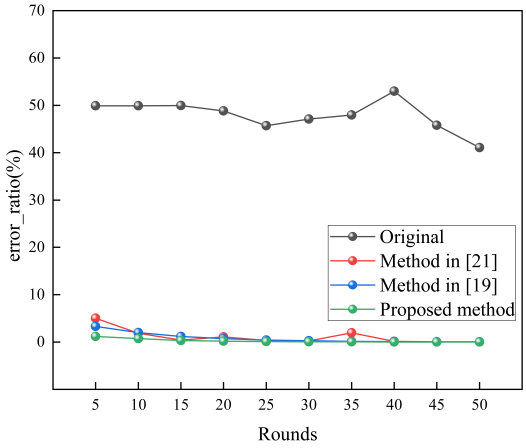


Fig. 15. Comparison of error node ratio

VI. Discussion

To comprehensively evaluate the effectiveness of the proposed optimization mechanism in sensor-network-oriented blockchain systems, this study discusses its contributions, limitations, and potential applications.

A. Comparative Analysis

Firstly, from the perspective of evolutionary stability, Table V shows that the four-party game model significantly accelerates convergence, with all nodes stabilizing within 1 second. This is faster than the three-party (1.5 seconds) and two-party (3 seconds) models. Even under partial regulatory inactivity, the proposed framework retains rapid convergence, reflecting strong resilience against strategic uncertainty. The improvements stem from the integration of reputation mechanisms, punishment constraints, and supervisory incentives, which jointly reinforce fairness and controllability.

TABLE V
Comparative Analysis of Key Performance Metrics

comparison scheme	System average TPS↑	Average node participation rate↑	Error node ratio↓
Original	75.36	45.99	47.91
Literature methods [21]	86.63	77.84	1.12
Literature methods [19]	115.00	70.00	0.83
Proposed method	121.79	83.86	0.263

Note: ↑ indicates a performance metric where higher values are better; ↓ indicates a metric where lower values are preferable.

Secondly, regarding blockchain performance, the results confirm that the proposed mechanism achieves substantial gains in throughput, node participation, and fault tolerance. As summarized in Table VI, the model achieves an average TPS of 121.79, a participation rate of 83.86%, and a fault ratio as low as 0.263%. Compared to the original DPoS, throughput improves by 61.6%, and the faulty node ratio decreases by over 99%. These enhancements are particularly relevant in large-scale sensor deployments, where high-frequency data generation demands both efficiency and reliability. Thirdly, in terms of practical implications for sensor networks, the results

TABLE VI
CONVERGENCE PERFORMANCE OF DIFFERENT GAME MODELS

Types of game models	Stabilization time of cluster head nodes (s) ↓	Stabilization time of Ordinary sensor nodes (s) ↓	Stabilization time of supervisory nodes (s) ↓	Strategy selection time of cluster head nodes (s) ↓	Strategy selection time of Ordinary sensor nodes (s) ↓
Two- party game model	3.0	3.0	—	—	—
Three- party game model	1.5	1.5	1.5	2.5	2.5
Four-party game modeling (this paper)	1.0	1.0	1.0	1.0	1.0

Note: "↓" indicates that lower values represent better performance; "–" denotes that the node type is not applicable in the corresponding game model.

highlight the importance of balancing energy cost, fairness, and trustworthiness. Ordinary sensor nodes—constrained by limited computing and battery capacity—benefit from reduced decision complexity, as their role is restricted to voting. Supervisory nodes, although incurring energy costs, are sustained through well-calibrated reward–penalty mechanisms. This ensures continuous monitoring without exhausting node resources.

B. Applications in Sensor Networks

The proposed blockchain-based DPoS consensus mechanism has strong applicability across multiple categories of sensor networks, where secure, fair, and efficient data storage is critical.

(1) In industrial environments, thousands of sensors continuously collect data on temperature, vibration, and energy consumption. The proposed mechanism ensures that this mission-critical data is securely stored, while the evolutionary game framework incentivizes cluster heads nodes to maintain fairness, thereby reducing the risk of bribery or collusion in automated manufacturing systems.

(2) Urban sensor deployments for traffic management, smart lighting, and environmental monitoring demand large-scale consensus with minimal latency. By incorporating supervisory nodes and reputation-driven penalties, the model enhances trust across heterogeneous city-wide sensor infrastructures. The rapid convergence demonstrated in Section V ensures timely consensus, supporting real-time decision-making in smart transportation and emergency response.

(3) Sensor nodes in agriculture or environmental ecosystems are energy-constrained and intermittently connected. The proposed mechanism minimizes the computational burden on ordinary sensor nodes, limiting their role to lightweight voting, while supervisory oversight preserves data integrity, making it highly suitable for long-term deployments in remote or harsh environments.

(4) In healthcare monitoring, where data confidentiality and reliability are paramount, the integration of punishment and reputation mechanisms mitigates data manipulation risks and fosters trust among distributed medical devices. This ensures that sensitive patient data recorded by wearable sensors can be securely aggregated and stored.

Collectively, these application scenarios highlight the adaptability of the proposed DPoS-based consensus mechanism across diverse sensor network deployments, demonstrating both theoretical significance and practical utility.

C. Scalability Considerations

While the proposed mechanism shows strong performance in small-to-medium sensor networks, scalability remains a critical concern for real-world large-scale deployments.

(1) To handle millions of sensor nodes in smart city or industrial contexts, a multi-layer structure can be introduced, where local sub-chains handle intra-cluster consensus, and a global chain coordinates inter-cluster data aggregation. This reduces communication overhead and accelerates consensus at scale.

(2) Ordinary sensor nodes often lack the computational resources for heavy blockchain operations. By restricting their role to voting and delegating block generation to more capable cluster heads, the mechanism ensures scalability without overburdening resource-constrained devices.

(3) Adaptive tuning of penalty factors (b), incentives (P_8), and reputation thresholds (L_2, L_3) is necessary to accommodate varying network sizes and workloads. For example, stricter penalties may be required in high-density urban deployments, while lighter settings suffice for agricultural monitoring networks.

(4) Supervisory nodes incur energy costs during monitoring. Future extensions may adopt energy-aware supervision scheduling, where supervisory intensity dynamically adjusts to current network trust levels, balancing system security with battery preservation.

These scalability considerations emphasize that while the proposed consensus mechanism is robust under current simulation conditions, real-world deployment will require architectural extensions, adaptive mechanisms, and energy-aware optimizations to fully meet the challenges of ultra-large-scale sensor networks.

D. Limitations

Despite these contributions, several limitations remain.

(1) The current model assumes simplified classifications of nodes (Ordinary sensor, Cluster head, Competing gateway, supervisory). In real deployments, sensor networks may include multiple tiers with highly diverse computational and energy profiles.

(2) Parameters such as penalties and incentives were assumed fixed during simulations. In practice, these may need to adapt dynamically to environmental fluctuations, traffic load, or malicious attack intensity.

(3) While simulation results are promising, the overhead of supervisory monitoring and cross-verification may increase under very large-scale sensor deployments (e.g., smart cities with millions of nodes).

E. Discussion on Simplified Node Strategies and Model Generalization

In this study, node behaviors were abstracted into binary strategies such as "bribery/non-bribery" and "collusion/non-collusion." This simplification was motivated by two primary considerations: (1) to maintain the analytical tractability of the evolutionary game equations and facilitate the derivation of stability conditions, and (2) to clearly interpret the strategic evolution of heterogeneous nodes under bounded rationality. This abstraction approach has been widely adopted in prior blockchain game-theoretic research [24]–[26] and is suitable for revealing essential behavioral dynamics in complex decentralized systems.

It is important to note that this simplification does not undermine the generalization capability of the proposed model. The evolutionary outcomes are primarily governed by payoff differentials, incentive and punishment mechanisms, and supervision strength, rather than by the discrete number of strategies. Therefore, the proposed four-party evolutionary game framework can be regarded as a primitive model for multi-dimensional strategy extensions. Future work may incorporate multi-level bribery intensities, partial collusion probabilities, or adaptive supervision mechanisms to better represent the heterogeneity of node behaviors and further enhance the model's applicability in real-world blockchain-enabled sensor networks.

F. Discussion on Homogeneous Assumption, Bounded Rationality, and Model Generalization

In this study, cluster head, ordinary sensor, competing gateway, and supervisory nodes are modeled as homogeneous sub-populations with identical rationality and adaptation rates to simplify analysis and reveal overall evolutionary dynamics. The bounded rationality assumption is adopted to reflect realistic decision-making, where nodes with limited energy, computation, and communication resources adjust strategies based on local information and historical feedback rather than global optimization. This assumption departs from perfect rationality in classical game theory and better captures adaptive behavior under incomplete information. Although the model assumes homogeneity, practical systems exhibit heterogeneity in resources and topology, leading to varied rationality and learning rates. Future work will extend the framework to a heterogeneous evolutionary game model with differentiated rationality parameters and multi-layer replicator dynamics to characterize asynchronous evolution and enhance generalization and applicability.

G. Discussion on Continuous Approximation and Discrete Consensus Epochs

Although the replicator dynamic equations adopted in this work are formulated in continuous time, they represent an analytical approximation of the discrete strategy updates that occur across DPoS consensus epochs. In practice, each DPoS epoch corresponds to a complete voting–block-generation cycle, where node strategies evolve through payoff-driven adjustments. The continuous-time formulation is thus an abstraction of this iterative learning process, allowing for closed-form stability and equilibrium analysis. This modeling approach has been extensively validated in prior evolutionary game-based blockchain studies [28], [31]. In addition, our simulation experiments employ discrete iterations and confirm that the resulting trajectories closely follow the theoretical continuous dynamics. Therefore, while the actual DPoS operates in discrete epochs, the continuous replicator dynamics remain an effective and accurate tool for capturing the macroscopic evolution of consensus behaviors in blockchain-enabled sensor networks.

VII. Conclusion and Future Work

This study tackles the challenges of insufficient voting incentives and collusion in DPoS consensus for sensor networks by mapping blockchain roles to cluster head nodes, ordinary sensor nodes, competing gateway nodes, and supervisory nodes. A four-party evolutionary game model integrating reputation, punishment, and supervisory mechanisms was developed and validated through theoretical analysis and simulations. Results show that the model enhances node participation, accelerates convergence, suppresses malicious behaviors, and improves throughput, security, and fairness. This work provides both a theoretical foundation and practical guidance for secure and efficient blockchain-based sensor networks, while future research will address node heterogeneity, dynamic environments, and adaptive incentive mechanisms to strengthen scalability and real-world applicability.

References

[1] F. Yang, Q. Sun, Z. Zhao, X. Wang, J. Xu, Y. Zheng, H. Zhang, and L. Wang, "Environment fusion routing protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 24, no. 8, pp. 13 418–13 430, 2023.

[2] J. Liu, L. Wang, and Y. Yu, "Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5256–5266, 2020.

[3] Y. Zhou, C. Xie, S. Sun, X. Zhang, and Y. Wang, "A self-supervised human activity recognition approach via body sensor networks in smart city," *IEEE Sensors Journal*, vol. 24, no. 5, pp. 5476–5485, 2023.

[4] C. Zhang, L. Zhu, and C. Xu, "Bsdp: Blockchain-based smart parking for digital-twin empowered vehicular sensing networks with privacy protection," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 7237–7246, 2022.

[5] J. Donnal, "Joule: A real-time framework for decentralized sensor networks," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3615–3623, 2018.

[6] C. Yang, S. Lan, Z. Zhao, M. Zhang, W. Wu, and G. Q. Huang, "Edge-cloud blockchain and ioe-enabled quality management platform for perishable supply chain logistics," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3264–3275, 2022.

[7] W. Li, P. Cheng, Y. Feng, N. Liu, M. Liu, and Y. Li, "A blockchain-assisted hierarchical data aggregation framework for iiot with computing first networks," *IEEE Transactions on Network and Service Management*, vol. 22, no. 4, pp. 3496–3512, 2025.

[8] J. Tan, J. Shi, J. Wan, H.-N. Dai, J. Jin, and R. Zhang, "Blockchain-based data security and sharing for resource-constrained devices in manufacturing iot," *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 25 558–25 567, 2024.

[9] C. C. Rawlins, S. Jagannathan, and V. S. S. Nadendla, "A reputation system for provably-robust decision making in iot blockchain networks," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14 088–14 099, 2023.
[10] D. Wang, Y. Jia, L. Liang, K. Ota, and M. Dong, "Resource allocation in blockchain integration of uav-enabled mec networks: A stackelberg differential game approach," *IEEE Transactions on Services Computing*, vol. 17, no. 6, pp. 4197–4210, 2024.
[11] Y. Z. Wei, Q. Xu, and H. Peng, "An enhanced consensus algorithm for blockchain," *Scientific Reports*, vol. 14, no. 1, p. 17701, 2024.
[12] Q. Zhu, A. Jing, C. Gan, X. Guan, and Y. Qin, "Hcsc: A hierarchical certificate service chain based on reputation for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 6, pp. 6123–6145, 2023.
[13] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 20 214–20 228, 2022.
[14] S. Zhang, Z. Yan, W. Liang, K.-C. Li, and C. Dobre, "Baka: Biometric authentication and key agreement scheme based on fuzzy extractor for wireless body area networks," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 5118–5128, 2023.
[15] G. Li, B. He, Z. Wang, X. Cheng, and J. Chen, "Blockchain-enhanced spatiotemporal data aggregation for uav-assisted wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4520–4530, 2021.
[16] P. P. Raj and A. M. Khedr, "Sdcbm: A secure data collection model with blockchain and machine learning integration for wireless sensor networks," *IEEE Sensors Journal*, vol. 25, no. 4, pp. 7457–7466, 2025.
[17] S.-J. Hsiao and W.-T. Sung, "Enhancing cybersecurity using blockchain technology based on iot data fusion," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 486–498, 2022.
[18] M. Xu, F. Zhao, Y. Zou, C. Liu, X. Cheng, and F. Dressler, "Blown: A blockchain protocol for single-hop wireless networks under adversarial sinr," *IEEE Transactions on Mobile computing*, vol. 22, no. 8, pp. 4530–4547, 2022.
[19] Q. Y. Zhu, A. K. Jing, C. Q. Gan, X. W. Guan, and Y. Z. Qin, "Hcsc: A hierarchical certificate service chain based on reputation for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 6, pp. 6123–6145, 2023.
[20] J. Ahmad, S. A. Shah, S. Latif, F. Ahmed, Z. Zou, and N. Pitropakis, "Drann_pso: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8112–8121, 2022.
[21] W. Bing, H.-l. Li, and P. Li, "Optimized dpos consensus strategy: Credit-weighted comprehensive election," *Ain Shams Engineering Journal*, vol. 14, no. 2, p. 101874, 2023.
[22] J. Y. Feng, X. Y. Zhao, K. X. Chen, F. Zhao, and G. H. Zhang, "Towards random-honest miners selection and multi-blocks creation: proof-of-negotiation consensus mechanism in blockchain networks," *Future Generation Computer Systems*, vol. 105, pp. 248–258, 2020.
[23] G. X. Xu, Y. Liu, and P. W. Khan, "Improvement of the dpos consensus mechanism in blockchain based on vague sets," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4252–4259, 2020.
[24] D. P. Pan, J. L. Zhao, S. K. Fan, and Z. Q. Zhang, "Dividend or no dividend in delegated blockchain governance: A game theoretic analysis," *Journal of Systems Science and Systems Engineering*, vol. 30, no. 3, pp. 288–306, 2021.
[25] N. Ren and Y. Y. Ma, "Research on evolutionary game and strategy of dpos consensus mechanism improvement," *Computer engineering and applications*, vol. 58, no. 12, pp. 102–111, 2022.
[26] D. Wang, Y. J. Jia, L. Liang, M. X. Dong, and K. Ota, "A game for task offloading in reputation-based consortium blockchain networks," *IEEE Wireless Communications Letters*, vol. 11, no. 7, 2022.
[27] J. Mišić, V. B. Mišić, and X. Chang, "Toward decentralization in dpos systems: Election, voting, and leader selection using virtual stake," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 1777–1790, 2024.
[28] J. x. Sun, R. Zhao, H. r. Yin, and W. Cai, "Incentive mechanism for redactable blockchain governance: An evolutionary game approach," *IEEE Transactions on Computational Social Systems*, vol. 11, pp. 6953–6965, 2024.
[29] Y. R. Chen, Y. Y. Zhang, S. W. Wang, F. Wang, Y. Li, Y. M. Jiang, L. Y. Chen, and B. Guo, "Dim-ds: Dynamic incentive model for data sharing in federated learning based on smart contracts and evolutionary game theory," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 24 572–24 584, 2022.
[30] P. f. Wan, X. m. Wang, G. y. Min, L. Wang, Y. g. Lin, W. y. Yu, and X. j. Wu, "Optimal control for positive and negative information diffusion based on game theory in online social networks," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 1, pp. 426–440, 1998.
[31] Y. w. Cheng, Z. y. Zhen, and L. d. Wen, "Evolutionary selection in normal-form games," *IEEE Transactions on Control of Network Systems*, vol. 11, no. 2, pp. 1056–1066, 2024.
[32] B. Nortmann, A. Monti, M. Sassano, and T. Mylvaganam, "Nash equilibria for linear quadratic discrete-time dynamic games via iterative and data-driven algorithms," *IEEE Transactions on Automatic Control*, vol. 69, no. 10, pp. 6561–6575, 2024.

Wencheng Chen (Graduate Student Member, IEEE) received the M.S. degree from Fujian University of Technology, China. He is pursuing the Ph.D. degree in the College of Electrical Engineering and Automation, Fuzhou University, China. His research interests include blockchain, Internet of Things, edge computing, and game theory.

Jun Wang (Senior Member, IEEE) received the B.S. and M.S. degrees in communication and information systems from Hohai University, Nanjing, China, in 2003 and 2006, respectively, and the Ph.D. degree in communication and information systems from Southeast University, Nanjing, in 2012. He is currently a Faculty Member with the College of Electrical Engineering and Automation, Fuzhou University, Fuzhou, China. He is also a member of Fujian Integrated Circuits Design Center. His current research interests include statistical signal processing, cyclostationary signal analysis, ultra-wide band wireless communication, and cognitive radios.

Jeng-Shyang Pan (Senior Member, IEEE) received the B.S. degree in electronic engineering from the National Taiwan University of Science and Technology in 1986, the M.S. degree in communication engineering from National Chiao Tung University, Taiwan, in 1988, and the Ph.D. degree in electrical engineering from the University of Edinburgh, U.K., in 1996. He is currently the Director of the Fujian Provincial Key Lab of Big Data Mining and Applications, and an Assistant President with the Fujian University of Technology. He is also the Professor with the Harbin Institute of Technology. He is the IET Fellow, U.K., and has been the Vice Chair of the IEEE Tainan Section. He was offered Thousand Talent Program in China in 2010.

R. Simon Sherratt (Fellow, IEEE) is currently a Professor of Biomedical Engineering at the University of Reading, UK. Professor Simon Sherratt received the B.Eng. From Sheffield City Polytechnic (now Sheffield Hallam University), M.Sc. from The University of Salford, and Ph.D. from The University of Salford; he was elected as Fellow of the IEEE in 2012, Fellow of the IET in 2009; Senior Fellow of the Higher Education Academy in 2014. He is a Chartered Engineer (C.Eng.) and registered European Engineer (Eur Ing). Professor Simon Sherratt was awarded the IEEE International Symposium on Consumer Electronics (ISCE) 2006 1st Place Best Paper Award: IEEE Chester Sall Award for best papers in the IEEE Transactions on Consumer Electronics in 2006, 2016, 2017, 2018. He has published over 200 articles in peer review journals and international conferences. His research area is wearable devices, mainly for healthcare and emotion detection.

Jin Wang (Senior Member, IEEE) received the B.S. and M.S. degree from Nanjing University of Posts and Telecom., China in 2002, 2005 respectively. He received Ph.D. degree from Kyung Hee University Korea in 2010. Now, He is a professor at Hunan University of Science and Technology. He has published more than 400 international journal and conference papers. His research interests mainly include wireless sensor network, network performance analysis and optimization. He is an IET Fellow, and senior member of IEEE.