International Journal of Mobile Computing and Multimedia Communications
Volume 15 • Issue 1 • January-December 2024

Multi-Dimensional Consensus Node Trust Evaluation and Selection for Blockchain-Empowered Electric Measurement Data Traceability

Xianbo Du
State Grid Jiangsu Electric Power Co., Ltd., China

Shuyun Wang
State Grid Jiangsu Electric Power Co., Ltd., China

Chunyang Li
State Grid Information and Telecommunication Group Co., Ltd., China

Mingtao Cui
State Grid Information and Telecommunication Group Co., Ltd., China

Zheng Xiong
State Grid Jiangsu Electric Power Co., Ltd., China

Haodong Liu
North China Electric Power University, China

ABSTRACT

With the deployment of internet of things-based monitoring terminals, massive electric measurement data are transmitted and shared among different grid company sectors. Consortium blockchain based consensus process has been adopted to enhance data traceability. However, previous studies face challenges including single-dimensional indication and lack of dynamic trustworthy degree update mechanism. Therefore, this paper proposes a node trust evaluation and selection algorithm based on improved fuzzy Petri network (IFPN). Firstly, the multi-dimensional node trust evaluation and selection framework for practical Byzantine fault tolerance (PBFT)-empowered electric measurement data sharing is constructed. On this basis, IFPN is proposed to dynamically evaluate measurement data node trust, and nodes participating in the PBFT consensus process are selected based on the Top-N algorithm. Further, the trustworthy degree of IFPN is dynamically updated based on the fuzzy deviation to improve the accuracy. Finally, the superiority of the proposed algorithm has been verified through simulation.

KEYWORDS

Electric Measurement Data, IoT, Blockchain, Improved Fuzzy Petri Network, Multi-Dimensional Node Trust Evaluation

MULTIDIMENSIONAL CONSENSUS NODE TRUST EVALUATION AND SELECTION FOR BLOCKCHAIN-EMPOWERED ELECTRIC MEASUREMENT DATA TRACEABILITY

With the widespread deployment of various Internet of Things (IoT)–based measurement devices, existing measurement data exhibit characteristics such as a large scale, diverse types, and an exponential growth in volume (Bai et al., 2021; Bedi et al., 2018; Hayashikoshi et al., 2018). Measurement data permeate multiple professional sectors, including grid company marketing, trading, development, dispatching, operation inspection, and the internet, facilitating business

DOI: 10.4018/IJMCMC.354068

applications such as the monitoring and dispatching of distribution grid operational status, energy management decision, load monitoring, and power trading markets. However, issues such as high real-time requirements of measurement data, difficulty in unifying communication specifications, and challenges in implementing encryption measures result in potential risks of data tampering, attacking, and theft during the data sharing process (Pan et al., 2018; Shi et al., 2020). Moreover, the accumulation of a large volume of electric measurement data interactions can lead to system overload. Therefore, the adoption of a consortium blockchain for the right confirmation of data that is trustworthy during electric measurement data sharing and interaction is necessary to establish a trusted network (Liao et al., 2021; Sun et al., 2023; Zhou et al., 2020). A consortium blockchain consists of multiple departments with joint control and management, featuring dedicated identity and privilege management system, and it uses encryption technology for data verification and storage (Bai et al., 2021). The consensus process is controlled by the master node, requiring all participating nodes to undergo verification and faithfully execute the consensus. Such arrangements enhance the security and efficiency of measurement data sharing and interaction while enhancing the transparency and traceability of data sharing.

The core part of a consortium blockchain ensures the integrity and consistency of nodes in the network through the consensus mechanism, which prevents the attack of malicious nodes and promotes the stability and security of network. There exist numerous algorithms to implement the consensus mechanism, among which practical Byzantine fault tolerance (PBFT) has been widely used. The core of PBFT is node trust evaluation and node selection. PBFT evaluates the trust of each node and classifies the nodes into master nodes, common slave nodes, and candidate nodes according to the level of trust from high to low. The master nodes construct the quorum certificate (QC) and lead slave nodes to carry out the consensus process. When the nodes fail to pass the QC verification in the consensus process, they are regarded as malicious nodes and removed from the consensus. At this time, the candidate nodes with higher trust will be transformed into common slave nodes. PBFT uses the trust mechanism to achieve lower communication overhead and significantly improves its performance in average consensus delay and throughput while effectively punishing malicious nodes (Fu et al., 2023; Liao et al., 2022). Many researchers have studied and applied the PBFT algorithm. Specifically, Luo et al. (2021) adopted blockchain to deal with the problem that the power generation system tends to be distributed and decentralized, and they proposed a multi-node data aggregation method based on PBFT. This method uses homomorphic encryption to assist trust evaluation and consensus node selection and safely realizes multi-node data aggregation of the microgrid without a trusted third party to assist automatic power dispatching. Sun et al. (2020) considered the security and privacy protection issues brought by vehicle-to-vehicle (V2V) energy trading framework. They combined a consortium blockchain with an improved PBFT algorithm in the design of an energy trading framework. This greatly reduces resource consumption in the node selection process and improves consensus efficiency. Lee et al. (2022) addressed the trust issue in data sharing in intelligent transportation systems. They proposed a two-tier trust system based on a blockchain, comprising a local blockchain and a global trust blockchain. They also introduced a location-based PBFT algorithm to reduce consensus convergence time by node selection. This algorithm evaluates the trust of vehicles on the basis of their activities, which is stored in the global trust blockchain to enhance data sharing security.

A fuzzy Petri net (FPN) is commonly used in modeling and fault diagnosis. It quantifies the strength of support or opposition between nodes by using modal values to construct node trust (Kait et al., 2024). The algorithm defines the parallel computation method in FPN and the rules for transferring node trust, which provides a method to calculate the consensus value of any node. It determines group preferences and consensus opinions on the basis of the consensus value to complete the consensus process (Ding et al., 2013; Zhou et al., 2021). Many studies have applied FPN in fault localization, node trust evaluation, and node selection. Specifically, Liu et al. (2021) addressed the issue of massive nodes and vast amount of data in the production field by proposing the Pythagorean FPN model.

They introduced Pythagorean fuzzy sets to capture imprecise and fuzzy inputs for determining node trust. Kiaei et al. (2020) adopted an intelligent power distribution system based on a fault localization method. They constructed an FPN-based fault location system and used discrete evidence such as protection device status and the results of fault indicators to locate faults in nodes. By introducing node trust and quantifying the similarity between measurement values, they determined the node with the smallest mismatch as the actual fault location, which accurately locates faults with multiple main and sublines. Chen et al. (2015) studied the load management issue in microgrids. To effectively detect fraud and abnormal consumption, they proposed the fractional order self-synchronization error-based FPN. This technology can detect nontechnical losses and interruption events, locate anomalies using multiple decision systems based on FPNs, track differences between professional and irregular load usage based on feature extractors, determine node trust, and improve fault localization accuracy.

THE CHALLENGE

Despite some progress made in the above-mentioned research, the key technical challenges still need to be addressed in the node trust evaluation for electric measurement data. First, the existing indicator system for node trust evaluation considers only the single-dimensional indicator, which fails to reflect the comprehensive performance and behavioral characteristics of nodes. It potentially conceals other node deficiencies and results in latent threats. Moreover, in measurement data sharing across various departmental services, each service type has different requirements, making it difficult for a single node trust evaluation to accurately rank and differentiate trust, leading to potential omissions or biases. Second, a traditional FPN lacks a dynamic trustworthy degree update mechanism, making it difficult to effectively capture rapid changes of node trust in the electric measurement network. The inability to make dynamic adjustment in real time leads to poor flexibility in measurement data sharing and interaction, which negatively affects the efficiency and security of the electric measurement data consensus. Therefore, how to establish a dynamic and fast trustworthy degree update mechanism to evaluate node trust through a multidimensional indicator system to enhance the efficiency and security of electric measurement data sharing and interaction is still an open issue.

CONTRIBUTION

We propose the improved fuzzy Petri network (IFPN)–based node trust evaluation and selection algorithm to address the aforementioned challenges. First, the multidimensional node trust evaluation and selection framework for PBFT-empowered electric measurement data sharing is constructed. Next, the IFPN-based node trust evaluation algorithm is proposed to dynamically evaluate each measurement data node trust by transforming the multidimensional indicator system for dynamic trust evaluation into the input for the IFPN. Then, the measurement data nodes participating in the PBFT consensus process are selected on the basis of the Top-N algorithm as well as node trust. Furthermore, the degree of trustworthiness of the IFPN is dynamically updated on the basis of the fuzzy deviation, which improves the accuracy of the trust evaluation and selection as well as the efficiency of electric measurement data interaction. The principle innovative points and contributions are introduced as follows.

Multidimensional Indicator System for Dynamic Trust Evaluation

We propose a multidimensional indicator system for dynamic trust evaluation that comprises two dimensions: computing capability and honesty. The computing capability encompasses metrics such as average delay, average delay fluctuation, and the percentage of average delay fluctuation. Honesty is assessed through criteria including the honest behavior ratio, honest behavior ratio fluctuations, and the percentage of honest behavior ratio fluctuations. It provides a comprehensive and accurate indicator system for dynamic trust evaluation in electric measurement data sharing and interaction.

Accurate Node Trust Evaluation and Selection for Consensus Implementation

We propose an IFPN–based node trust evaluation and selection algorithm. It involves inputting the computing capability and honesty indicators from a multidimensional indicator system into the IFPN. Next, the nodes involved in the PBFT consensus process are selected using the Top-N algorithm. The node with the highest trust rating is designated as the master node and is responsible for leading the entire consensus process. The trustworthiness level of the IFPN is continually updated through fuzzy deviation within the trust evaluation network, thereby enhancing the efficiency and accuracy of node trust evaluation and selection.

The remainder of this article is organized as follows. We first present the system model. Next, we introduce the proposed IFPN-based node trust evaluation and selection algorithm. We then conduct a simulation verification and then conclude the article.

SYSTEM MODEL

As shown in Figure 1, the multidimensional node trust evaluation and selection framework for a PBFT-empowered electric measurement data sharing is constructed, which consists of the perception layer, multidimensional indicator layer, decision layer, and PBFT layer.

The perception layer contains an IoT-based electric energy meter, ammeter, electric data acquisition, and other devices in the electric measurement system, which are responsible for acquiring data on the operation status of electric equipment and include a switchboard, charging pile, air conditioning unit, and distributed photovoltaic. Then, the sharing transactions of electric measurement data are uploaded to the PBFT layer for data deposit, block construction, and consensus, to enhance the security and traceability of data interaction and sharing.

The multidimensional indicator layer contains two dimensions: computing capability and honesty. The computing capability covers the average delay, average delay fluctuations, and percentage of average delay fluctuations. Honesty covers the honest behavior ratio, honest behavior ratio fluctuations, and percentage of honest behavior ratio fluctuations. The multidimensional indicator values of each node in the PBFT layer are calculated and uploaded to the decision layer for node trust calculation.

The decision layer contains the IFPN and Top-N algorithm. First, on the basis of the IFPN, the trust of each node is dynamically evaluated according to the indicator values of computing capability and honesty obtained from the multidimensional indicator layer. During the consensus process, the top N nodes are selected to participate on the basis of the Top-N; these are also known as *master nodes* (Liao et al., 2023). Finally, the decision information of the consensus nodes is uploaded to the PBFT layer.

The PBFT layer contains I servers, with each server representing a node in the blockchain, which is defined as $I = \{1, \cdots, i, \cdots, I\}$.On the basis of the decision information uploaded by the decision layer, the master node leads the whole consensus process.

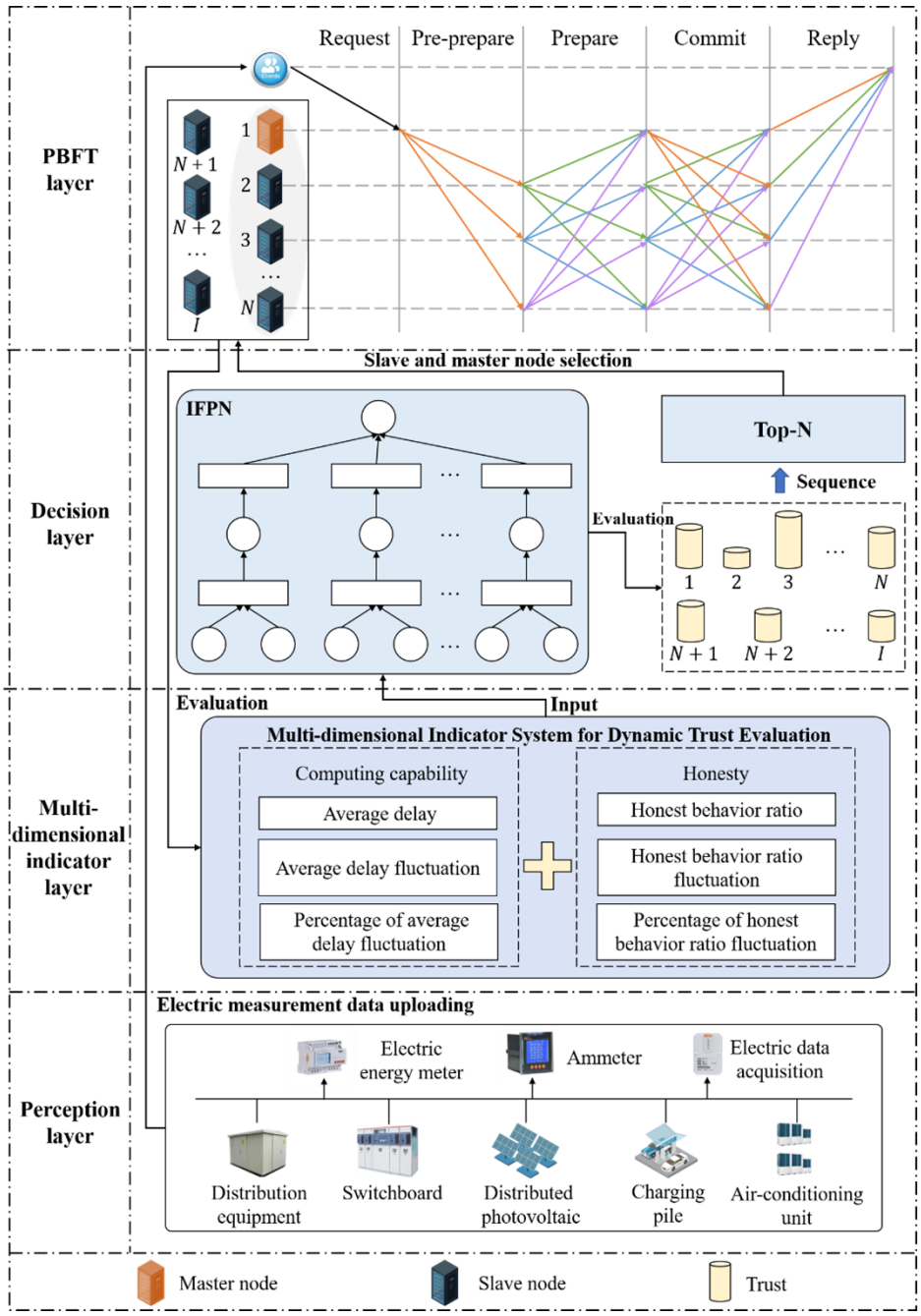
Multidimensional Indicator System for Dynamic Trust Evaluation

Computing Capability

We define the set of time slots for electric measurement data to be deposited and consensus as $\mathcal{T} = \{1, 2, \cdots, t\}$. The average delay of node i in the t time slot is defined as the average value of time spent in participating in the consensus of electric measurement data by node i through the consortium blockchain for the most recent T time slots, which can be expressed as in Equation 1.

$$\overline{\tau}_i(t) = \frac{1}{T} \sum_{a=t-T}^{t-1} \tau_i(a), \tag{1}$$

Figure 1. The multidimensional node trust evaluation and selection framework for PBFT-empowered electric measurement data sharing



Note. PBFT = practical Byzantine fault tolerance.

where $\bar{\tau}_i(t)$ is the average delay of the node i in the tth time slot and $\tau_i(t)$ is the time taken by the node i in the tth slot to participate in the consensus of electric measurement data through the consortium blockchain.

The average delay fluctuation of node i in the tth slot refers to the standard deviation of the consensus delay for the most recent Ttime slots, which can be expressed as in Equation 2.

$$\phi_i^{cal}(t)=\sqrt{\frac{1}{T}\left(\sum_{a=t-T}^{t-1}\left(\tau_i(a)-\overline{\tau}_i(t)\right)^2\right)}. \tag{2}$$

The percentage of average delay fluctuation of node i in the tth slot refers to the ratio of the average delay fluctuation to the consensus delay, which can be expressed as in Equation 3.

$$\varepsilon_i^{cal}(t)=\frac{\phi_i^{cal}(t)}{\tau_i(t)}. \tag{3}$$

Honesty

We consider the honest behavior ratio of node i in the tth slot as the honest interactions to the total number of interactions rate in which node i participates in the consensus of electric measurement data through the consortium blockchain for the most recent T time slots; the honest behavior ratio can be calculated as in Equation 4.

$$\omega_i(t)=\frac{\sum_{a=t-T}^{t-1}N_i^{legal}(a)}{\sum_{a=t-T}^{t-1}\left(N_i^{legal}(a)+N_i^{illegal}(a)\right)}, \tag{4}$$

where $N_i^{legal}(t)$ represents the number of honest interactions of node i in the tth time slot and $N_i^{illegal}(t)$ represents the number of non-honest interactions of node i in the tth slot.

The honest behavior ratio fluctuation of node i in the tth slot refers to the standard deviation of the honest behavior ratio in the most recent Ttime slot, which can be calculated as in Equation 5.

$$\phi_i^{tru}(t)=\sqrt{\frac{1}{T}\left(\sum_{a=t-T}^{t-1}\left(\omega_i(a)-\frac{1}{T}\sum_{b=t-T}^{t-1}\omega_i(b)\right)^2\right)}. \tag{5}$$

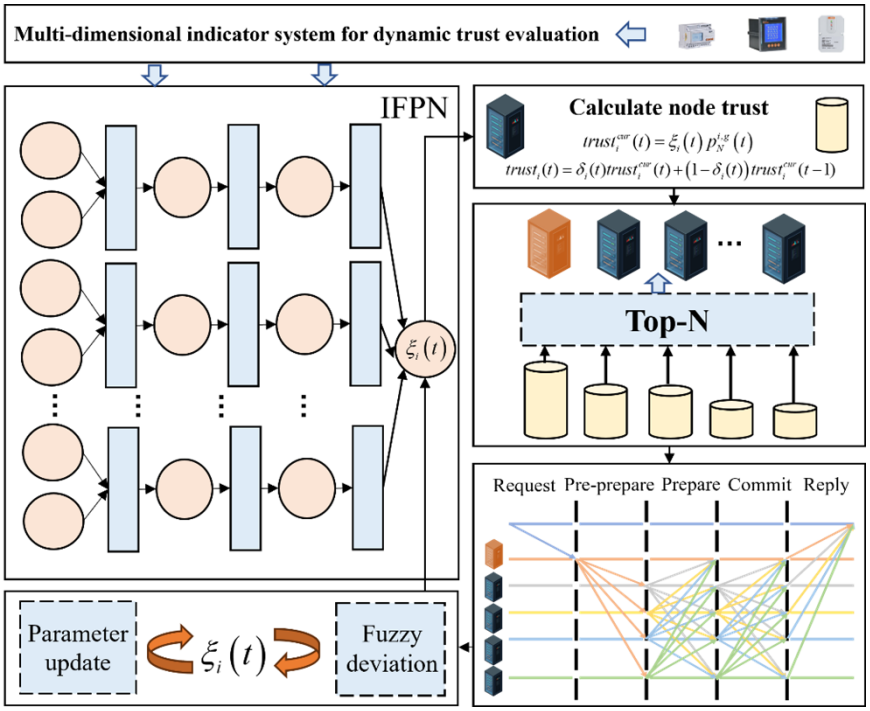
The percentage of honest behavior ratio fluctuation of node i in the tth time slot refers to the ratio of the honest behavior ratio fluctuation to the honest behavior ratio, which can be defined as in Equation 6.

$$\varepsilon_i^{tru}(t)=\frac{\phi_i^{tru}(t)}{\omega_i(t)}. \tag{6}$$

Node Trust Evaluation and Selection Algorithm Based on Improved Fuzzy Petri Network

In this section, we propose an IFPN-based node trust evaluation and selection algorithm. To start, building on the multidimensional indicator trust dynamic measurement system we have just established, we construct an IFPN to dynamically evaluate node trust, that is, a candidate edge server. Then, during the consensus process, on the basis of the Top-N algorithm and the trust of nodes, both master and slave nodes are selected to participate. Finally, we use fuzzy deviation to update the IFPN,

Figure 2. Principle diagram of the proposed algorithm



Note. IFPN = improved fuzzy Petri network.

which enhances the accuracy of node trust evaluation. The principal diagram is illustrated in Figure 2. The proposed IFPN-based node trust evaluation and selection algorithm is elaborated in Table 1.

IFPN-Based Node Trust Evaluation

A FPN has the significant advantages of distributed processing, high flexibility, and scalability. It effectively handles data indicators with low accuracy or fuzziness by simulating the inference process of fuzzy logic, and it has been widely applied in the consensus nodes trust evaluation for measurement data. However, existing evaluation methods for consensus nodes based on FPN typically focus on only a single dimension of indicators, limiting the accuracy and comprehensiveness of the evaluation. In addition, a traditional FPN lacks a dynamic trustworthy degree update mechanism, making it difficult to effectively capture and adapt to the rapid changes in node trust in the electric measurement data, which negatively affects the efficiency and security of electric measurement data consensus. To address these challenges, in this section we propose the IFPN-based node trust evaluation method, which transforms the multidimensional indicator system for dynamic trust evaluation into the input of an IFPN to comprehensively evaluate the trust of measurement data nodes. Furthermore, on the basis of the fuzzy deviation of node trust, dynamic trustworthy degree updates are implemented to improve the accuracy of trust evaluation and selection, enhancing the efficiency of electric measurement data sharing and interaction. The dynamic trustworthy degree update is specifically discussed in the section titled "IFPN Trustworthy Degree Update Based on Fuzzy Deviation of Trust."

An IFPN introduces fuzzy sets and fuzzy logic concepts, establishing a structured inference mechanism for fuzzy inference. Key components of an IFPN encompass places, transitions, arcs, initial states, and fuzzy inference rules. Places denote sets of states or resources within the system, and transitions depict potential events or operations. Arcs serve to link places and transitions, illustrating

Table 1. Node trust evaluation and selection algorithm based on the IFPN

Algorithm 1 Node trust evaluation and selection algorithm based on IFPN
1: **for:** $t = 1,2,...T$ **do**
2: **Input:** $U_i(t)$, $H_i(t)$, $W_i(t)$, input matrix $IN_i(t)$, output matrix $OUT_i(t)$, M-dimensional initial state matrix $K_0^i(t)$.
3: **Output:** $trust_i(t)$.
4: Phase 1: Node trust evaluation
5: Transform the multi-dimensional indicator system for dynamic trust evaluation into IFPN.
6: **for:** $i = 1,2,...I$ **do**
7: **for:** $g = 1,2,...G$ **do**
8: Calculate the equivalent input trustworthy degree of nodes i based on (9).
9: Calculate node trust based on (14).
10: **while** $K_{g+1}^i(t) \neq K_g^i(t)$ **do**
11: $g = g + 1$
12: Recalculate the next state after the transition occurs according to (9)-(14).
13: **end while**
14: **end for**
15: **end for**
16: Phase 2: Node selection
17: Select the top N node as the participating node for consensus based on (17).
18: Consensus based on selected top N nodes.
19: Phase 3: Updating
20: **end for**

Note. IFPN = improved fuzzy Petri network.

relationships between them or transitions to places. The weights assigned to arcs are fuzzy numbers, signifying the likelihood that a transition will occur. Initial states delineate the system's startup condition, reflecting the initial occupancy levels of each place. Fuzzy inference rules play a pivotal role in determining the credibility of target propositions within an IFPN.

In an IFPN, $\mathcal{X}_i = \{x_1^i, x_2^i, ..., x_M^i\}$ represents finite set of places, where M represents the number of places in $\mathcal{X}_i$; $\mathcal{R}_i = \{r_1^i, r_2^i, ..., r_J^i\}$ represents finite set of transitions, where J represents the number of transitions in $\mathcal{R}_i$, and $IN_i(t) = \{\beta_{m,j}^i\}(t), \beta_{m,j}^i(t) \in \{0,1\}$ represents input matrix of node i. When there is a directed arc from x_m^i to r_j^i, $\beta_{m,j}^i(t) = 1$, and otherwise, $\beta_{m,j}^i(t) = 0$, $OUT_i(t) = \{\varphi_{m,j}^i(t)\}, \varphi_{m,j}^i(t) \in \{0,1\}$ represents output matrix of node i. If the directed arc is from r_j^i to x_m^i, $\varphi_{m,j}^i(t) = 1$, and otherwise, $\phi_{m,j}(t) = 0$, $U_i(t) = \{u_{m,j}^i(t)\}, u_{m,j}^i(t) \in \{0,1\}$ represents trustworthy degree matrix of $M \times J$, which reflects the degree of support of transition for the corresponding output place, and $H_i(t) = \{h_{m,j}^i(t)\}$ represents the output threshold matrix of the places. If the directed arc is from r_j^i to x_m^i, $h_{m,j}^i(t) \in [0,1]$, and otherwise $h_{m,j}^i(t) = +\infty$, $W_i(t) = \{w_{m,j}^i(t)\}$ represents weight matrix of $M \times J$, which reflects the degree of influence of the input place on the corresponding transitions, and $K_0^i(t)$ is the initial state vector, which represents the degree to which the place is true.

The fuzzy inference rules of IFPN are expressed in Equation 7.

$$\xi_i(t) = \max\left(h_{1,1}^i(t)\, w_{1,1}^i(t), h_{1,2}^i(t)\, w_{1,2}^i(t), ..., h_{M,J}^i(t)\, w_{M,J}^i(t)\right), \tag{7}$$

where $\xi_i(t)$ represents the degree of trustworthiness of the target repository for node i. The specific execution process of IFPN is introduced in the following steps.

Step 1. Input the node consensus computing capability index and node honesty index in the multidimensional indicator system for dynamic trust evaluation into the IFPN and determine the initial state vector, $K_0^i(t)$, through expert evaluation and an analytic hierarchy process.

Step 2. Input $U_i(t)$, $H_i(t)$, $W_i(t)$, $IN_i(t)$, $OUT_i(t)$, the M-dimensional initial state matrix $K_0^i(t)$, and define $g = 1$, where g represents the iteration.

Step 3. Calculate the equivalent input degree of trustworthiness for each transition of node i, which is denoted in Equation 8.

$$F_g^i(t) = \left(W_i(t) \odot IN_i(t)\right)^T \bullet K_{g-1}^i(t), \tag{8}$$

where $F_g^i(t) = \left\{f_j^{i,g}(t)\right\}$ is the J-dimensional equivalent input degree of trustworthiness vector for each transition of node i in the tth time slot and the gth iteration, $f_j^{i,g}(t)$ is the jth element in $F_g^i(t)$, and $K_{g-1}^i(t)$ is the state vector of node i in the tth time slot during the $(g-1)$th iteration. Thus, $\odot$represents the direct multiplication operator: $A_{M\times J} \odot B_{M\times J} = C_{M\times J}$, so $c_{mj} = a_{mj}b_{mj}$. "$\bullet$" represents matrix multiplication.

Step 4. Calculate the next state after the transition occurs.

4.1. Calculate the $M \times J$ output enable matrix $E_g^i(t) = \left\{e_{m,j}^{i,g}(t)\right\}$ for node i in the gth iteration of the tth time slot, which is given in Equation 9.

4.2. Define $Y_g^i(t) = \left\{y_{m,j}^{i,g}(t)\right\}$ as the $M \times N$ threshold result comparison matrix for the gth iteration of node i in the tth time slot, while $y_{m,j}^{i,g}(t)$ is the element in row m and column j of $Y_g^i(t)$. Compare the equivalent trustworthy degree of $Y_g^i(t)$ storage with the threshold of the output library, which is given in Equation 10.

4.3. Calculate the new state vector $K_{g+1}^i(t)$, which is given in Equation 11.

$$E_g^i(t) = \left(e_{m,j}^{i,g}\right)_{M\times N}, e_{m,j}^{i,g} = \begin{cases} 1, & y_{m,j}^{i,g} \geq 0 \\ 0, & y_{m,j}^{i,g} < 0 \end{cases}, \tag{9}$$

where $e_{m,j}^{i,g}(t)$ represents the element at the intersection of the mth row and jth column in $E_g^i(t)$.

$$Y_g^i(t) = \left[\left(F_g^i(t)\right)^T, \left(F_g^i(t)\right)^T, ..., \left(F_g^i(t)\right)^T\right]_{M\times N}^T - H_i(t). \tag{10}$$

$$K_{g+1}^i(t) = K_g^i(t) \oplus \left(E_g^i(t) \odot U_i(t) \otimes F_g^i(t)\right), \tag{11}$$

where $\oplus$ is the addition operator, $A_{M\times J} \oplus B_{M\times J} = C_{M\times J}$, so $c_{mj} = \max\left\{a_{mj}, b_{mj}\right\}$, and $\otimes$ represents the multiplication operator, $A_{M\times L} \otimes B_{L\times J} = C_{M\times J}$, so $c_{mj} = \underset{1\leq l\leq L}{\max}\left\{a_{ml}, b_{lj}\right\}$.

Step 5. Determine whether the iteration has ended.

If $K_{g+1}^{i}(t) \neq K_{g}^{i}(t)$, make $g = g + 1$, and go back to Step 4.
If $K_{g+1}^{i}(t) = K_{g}^{i}(t)$, stop the calculation.

Step 6. Calculate the evaluation indicators for each place, which is calculated as in Equation 12.

$$P_{g}^{i}(t) = K_{g}^{i}(t)\, Q_{i}^{T}(t), \tag{12}$$

where $P_{g}^{i}(t) = \left\{ p_{m}^{i,g}(t) \right\}$ is the M-dimensional vector for each transition of node i in the tth time slot and the gth iteration; $p_{m}^{i,g}(t)$ is the mth element in $P_{g}^{i}(t)$, and the last element of this vector corresponds to the evaluation index of node trust that can be expressed as $p_{M}^{i,g}(t)$; and $Q_{i}(t)$ is the trust evaluation matrix of $M \times J$ nodes determined through expert evaluation and analytic hierarchy process.

Step 7. Calculate node trust $trust_{i}^{cur}(t)$, which is calculated as in Equation 13.

$$trust_{i}^{cur}(t) = \xi_{i}(t)\, p_{M}^{i,g}(t). \tag{13}$$

Because of the significant increase in the growth rate of trust, it is not conducive to the reasonable and effective evaluation of node trust. Therefore, this article improves the dynamic measurement method of node trust, which is given in Equation 14.

$$trust_{i}(t) = \delta_{i}(t)\, trust_{i}^{cur}(t) + \left(1 - \delta_{i}(t)\right) trust_{i}^{cur}(t-1), \tag{14}$$

where $trust_{i}(t)$ is the node trust calculated after considering the growth rate of trust, and $\delta_{i}(t)$ is the decentralized adjustment factor. By adjusting $\delta_{i}(t)$, the system avoids centralized nodes, which is updated as in Equation 15.

$$\delta_{i}(t) = trust_{thr} + \sigma \left(trust_{i}^{cur}(t) - trust_{i}^{cur}(t-1) \right)^{2}, \tag{15}$$

where $trust_{thr}$ represents node trust threshold, and σ represents node trust adjustment parameters, which is used to control the impact of node behavior on node trust.

IFPN-Based Node Trust Evaluation

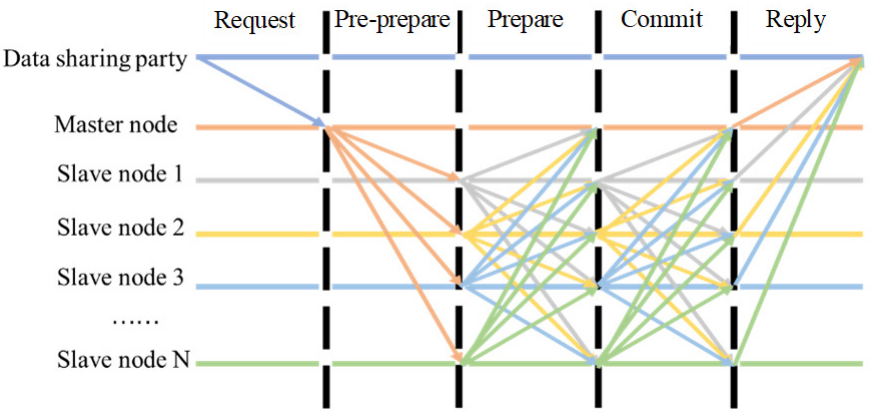
In this section, we first use the Top-N algorithm in the consensus process to select measurement data nodes to participated. Second, we introduce the node data consensus process based on PBFT.

Top-N–Based Node Selection

To ensure the security and trustworthy degree of blockchain consensus results and improve the consensus efficiency of nodes, we select the Top-N nodes with the highest degree of trustworthiness to participate in a consensus based on Top-N. The set of participating nodes in the consensus at the tth time slot as $\mathscr{C}(t)$is defined in Equation 16.

$$\mathscr{C}(t) = \underset{i \in \mathcal{F}}{\arg} Top_{N}\left(N, trust_{i}(t), \text{descent}\right), \tag{16}$$

Figure 3. PBFT consensus principle diagram



where $Top_N(\cdot)$ represents Top-N function. Equation 16 means to arrange the $trust_i(t)$ of each measurement data node in set $\mathcal{I}$ in descending order and select the Top-N nodes with the highest trust to join set $\mathcal{C}(t)$.

PBFT Consensus Process for Electric Measurement Data Sharing

The PBFT consensus is a state machine that replicates a based fault-tolerant algorithm, which can provide up to $(N-1)/3$ fault tolerance guarantees. The role of the server includes master nodes and slave nodes in the consensus process. In the tth time slot, all nodes in $\mathcal{C}(t)$ participate in the consensus. Among them, the master node has the highest degree of trustworthiness, and the other $N-1$ nodes are slave nodes. The PBFT consensus principle is illustrated in Figure 3, and the PBFT consensus process diagram for electric measurement data sharing is illustrated in Figure 4. The detailed introduction is as follows.

Step 1. **Request.** The data sharing party generates request messages for trading information sharing and interaction and sends them to the master node.

Step 2. **Pre-prepare.** The master node responds to the request from the data sharing party and assigns a number to the request messages, generates pre-prepared messages, and broadcasts them to the slave nodes.

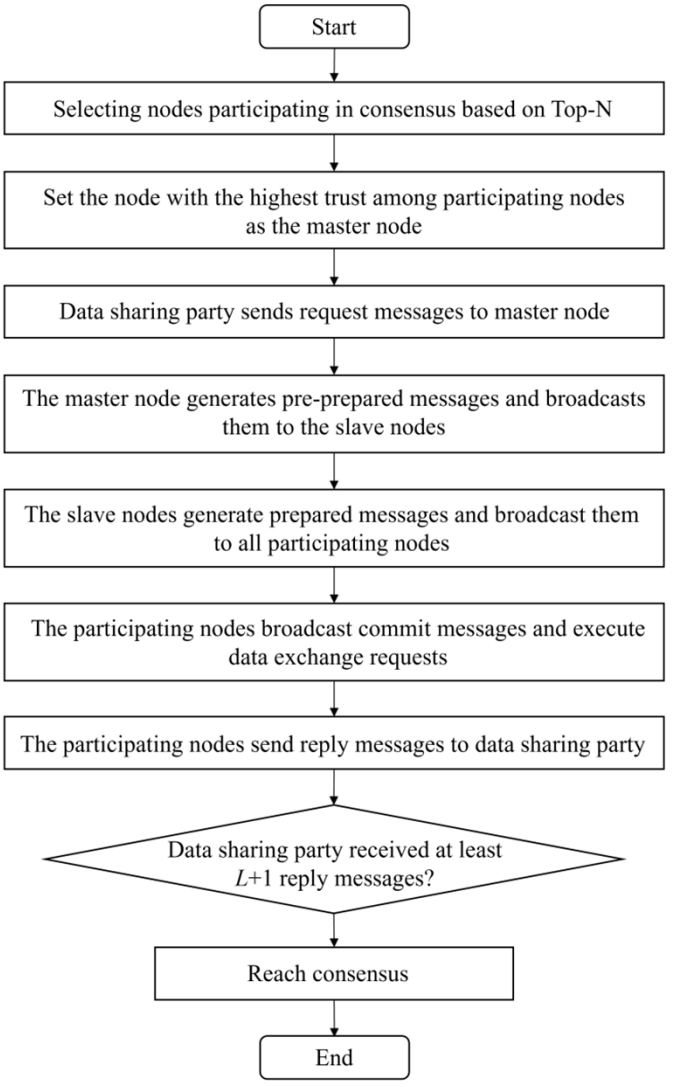
Step 3. **Prepare.** The slave nodes check the pre-prepared message and, if it passes the verification, the prepared messages are generated and broadcasted to all participating nodes.

Step 4. **Commit.** After receiving at least $\lceil 2L \rceil$ preparation messages and verifying them, the node broadcasts a commit message and executes the sharing and interaction requests of transaction information i from the data sharing party, where $L = (N-1)/3$, and $\lceil 2L \rceil$ represents round up $2L$. When a node receives $\lceil 2L+1 \rceil$ consistent prepared messages, it enters into the commit step.

Step 5. **Reply.** After the participating nodes complete the preceding operations, a reply message is sent to the data sharing party. When the data sharing party receives $L+1$ independent reply results, a consensus is reached and the algorithm ends.

The complexity analysis of the proposed algorithm is as follows. The multidimensional indicator system exhibits a constant complexity, $O(1)$, because it involves only the definition of the computation formulas for the indicators. The IFPN–based node trust evaluation algorithm has a complexity of $O(Ik)$, where I is the number of nodes and k is the number of iterations, because it requires multiple

Figure 4. PBFT consensus process diagram for electric measurement data sharing



Note. PBFT = practical Byzantine fault tolerance.

iterations of calculations for each indicator of each node. The Top-N based node selection has a complexity of $O(I \log N)$, because it involves sorting the trust degrees of all nodes and selecting the Top-N. The IFPN trustworthiness degree update based on fuzzy deviation has a complexity of $O(I)$, because it necessitates calculating the fuzzy deviation for each node and updating the target repository trustworthiness degree. Last, the PBFT consensus process has a complexity of $O(N)$, because it involves all nodes participating in the consensus process. In summary, the overall time complexity of the algorithm is $O(Ik + I \log N + I + N)$, where N is the number of nodes participating in the consensus. The complexity of the algorithm primarily depends on the number of nodes, the number of iterations, and the number of nodes participating in the consensus.

Table 2. Parameter table

Parameters	Value	Parameters	Value
Maximum number of iterations G	50	Threshold of node trust $trust_{thr}$	0.65
Number of nodes	50	Regulating parameters of node trust σ	0.3
Number of nodes involved in the consensus	35	Upper threshold of fuzzy deviation $trust^{e}_{\max}$	0.25
Maximum number of time slots T	150	Lower threshold of fuzzy deviation $trust^{e}_{\min}$	0.02

IFPN Trustworthy Degree Update Based on Fuzzy Deviation of Trust

In dynamic network environments, the trust of nodes may undergo frequent changes, making it difficult for the IFPN to effectively capture and adapt to the rapid changes in node trust in the network. Therefore, on the basis of the PBFT consensus results presented in Section titled IFPN-Based Node Trust Evaluation, the degree of trustworthiness of the fuzzy evaluation network is updated to achieve a more accurate evaluation and node selection. Updating the parameters of the fuzzy evaluation network by calculating the fuzzy deviation of the IFPN, the fuzzy deviation of the node's trust can be expressed in Equation 17.

$$trust_i^e(t) = \left[trust_i(t) - trust_i^{con}(t)\right]^2, \tag{17}$$

where $trust_i^{con}(t)$ represents the actual trust of node i obtained on the basis of consensus results.

In this article we dynamically adjust the degree of trustworthiness of the IFPN's target place on the basis of fuzzy deviation. When the fuzzy deviation is too large, it indicates that the fuzzy evaluation network has fluctuations, and the evaluation performance is unstable. The degree of trustworthiness of the target database should be appropriately reduced, and vice versa. The formula for the degree of trustworthiness of the target repository can be updated as in Equation 18.

$$\xi_i(t+1) = \begin{cases} \left(1 + V_i \dfrac{trust_i^e(t)}{trust_i(t)}\right)\xi_i(t), & trust_i^e(t) > trust^e_{\max} \\ \left(1 - V_i \dfrac{trust_i^e(t)}{trust_i(t)}\right)\xi_i(t), & trust_i^e(t) < trust^e_{\min} \end{cases}, \tag{18}$$

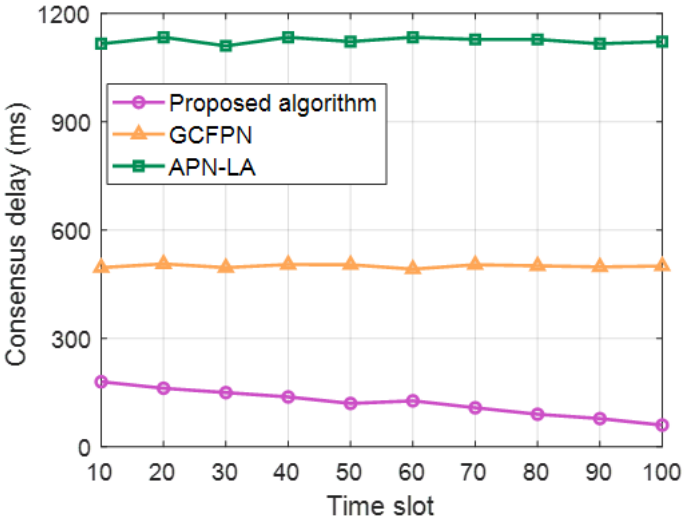
where $trust^e_{\max}$ and $trust^e_{\min}$ represent the upper and lower thresholds of fuzzy deviation, respectively, and V_i represents the adjustment weight of the degree of trustworthiness of the target place for node i.

SIMULATION RESULTS

In this section, we build a simulation platform based on MATLAB R2022b. The granular computing–fuzzy Petri net (GCFPN) and the learning automata-based adaptive Petri net (APN-LA) are used as comparison algorithms (Vahidipour et al., 2015; Zhou et al., 2023). The specific simulation parameters are given in Table 2 (Luo et al., 2024).

Figure 5 demonstrates the variation of consensus delay performance with time slots. One can see that the consensus delay of APN-LA becomes stable at about 1,100 ms within 10 to 100 time slots, which is because the algorithm needs adaptive learning. Compared with APN-LA, the consensus delay of the GCFPN algorithm is reduced by 51.37%. The proposed algorithm performs the best, and the consensus delay is reduced by 48.72% compared with the GCFPN algorithm. The proposed algorithm significantly reduces the consensus delay by selecting high-trust nodes to participate in the

Figure 5. Comparison of consensus delay performance



Note. GCPFN = granular computing–fuzzy Petri net; APN–LA = learning automata-based adaptive Petri net.

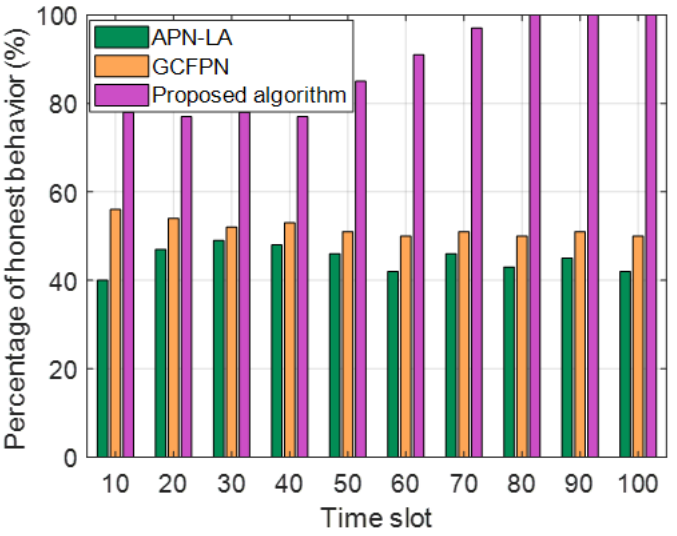
consensus through Top-N, as compared with other algorithms, demonstrating improved consensus convergence speed.

Figure 6 show the comparison of the proportions of honest behavior in different time slots. Of all the algorithms, the proportion of honest behaviors of the proposed algorithm is the highest, which is about 52.32% and 45.81% higher than APN-LA and GCFPN, respectively. The measurement data nodes are selected to participate in the consensus process on the basis of the Top-N algorithm and the node trust and updates the IFPN based on the fuzzy deviation. The proposed algorithm notably increases the proportion of honest behavior by selecting nodes on the basis of the Top-N algorithm and node trust, resulting in enhanced consensus security.

Figure 7 demonstrates the average delay fluctuating percentages of participating nodes in a certain time slot, and Figure 8 demonstrates the fluctuating percentages of honest behavior proportions of participating nodes. The mean of average delay fluctuation are 4%, 16%, and 31%, respectively, and the fluctuation ranges are 1%–7%, 6%–26%, and 22%–39%, respectively. The mean fluctuations of honest behavior proportion are 3.5%, 17%, and 30.5%, respectively, and the fluctuation ranges are 1%–8%, 7%–26%, and 21.5%–39.5%, respectively. The proposed algorithm has reached a small fluctuation percentage and fluctuation range in both average delay fluctuations and fluctuations in honest behavior proportion. This is because the proposed algorithm adopts a multidimensional indicator system for dynamic trust evaluation, and the results are more accurate and less fluctuant.

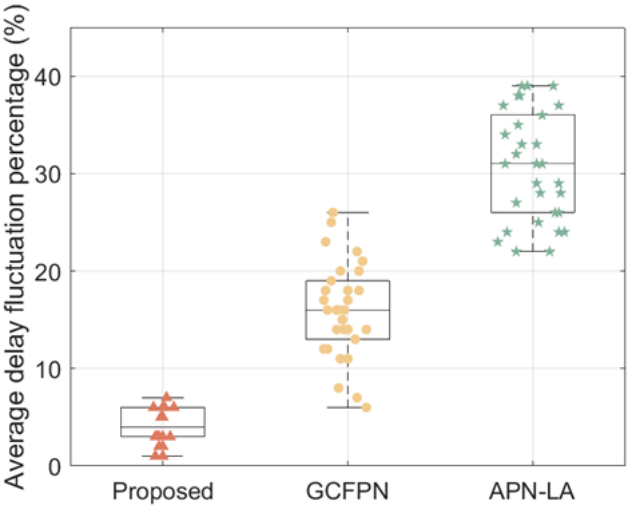
Figure 9 shows the evaluation errors of different trust evaluation algorithms under different evaluation indicators. The simulation uses the standard mean absolute error (MAE), mean absolute percentage error (MAPE), and root-mean-square error (RMSE) to compare the trust evaluation of different algorithms. The calculation method of each standard is shown in Equation 19.

Figure 6. Comparison of the proportion of honest behavior in different time slots



Note. GCPFN = granular computing–fuzzy Petri net; APN–LA = learning automata-based adaptive Petri net.

Figure 7. Average delay fluctuating percentages of participating nodes in a certain time slot



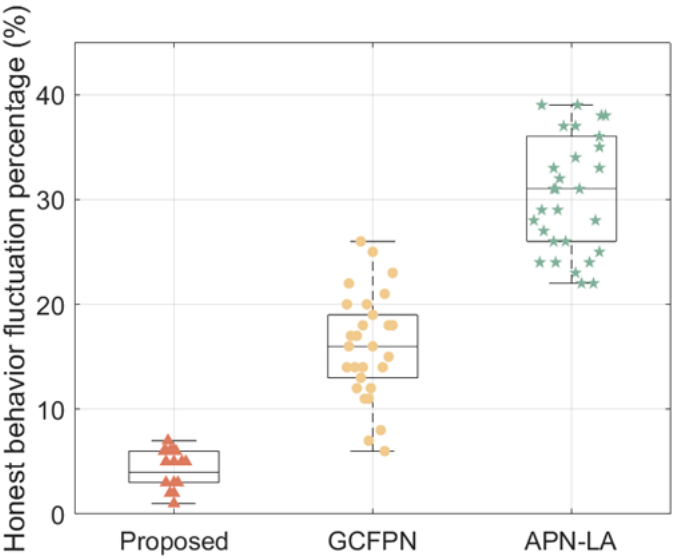
Note. GCPFN = granular computing–fuzzy Petri net; APN–LA = learning automata-based adaptive Petri net.

$$MAPE = \frac{1}{I}\sum_{i=1}^{I}\left|\frac{trust_i(t)-trust_i^{con}(t)}{trust_i^{con}(t)}\right|$$

$$MAE = \frac{1}{I}\sum_{i=1}^{I}\left|trust_i(t)-trust_i^{con}(t)\right| \quad (19)$$

$$RMSE = \sqrt{\frac{1}{I}\sum_{i=1}^{I}\left(trust_i(t)-trust_i^{con}(t)\right)^2}$$

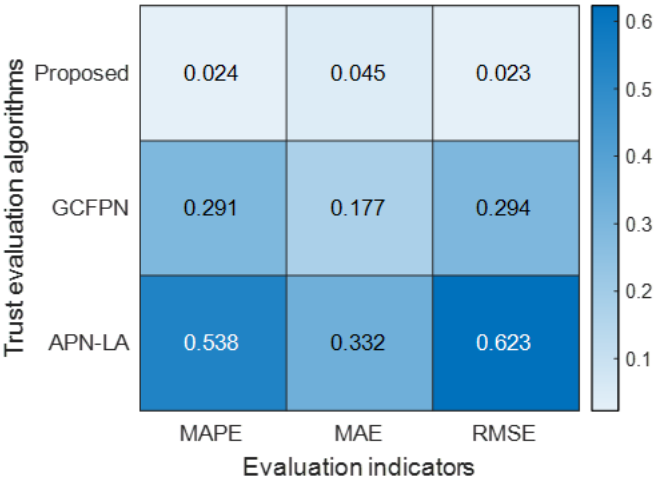
Figure 8. The fluctuating percentages of honest behavior proportions of participating nodes in a certain time slot



Note. GCPFN = granular computing–fuzzy Petri net; APN–LA = learning automata-based adaptive Petri net.

The evaluation error of the APN-LA algorithm is above 0.3 or even 0.6, the evaluation error of GCFPN is between 0.1 and 0.3, and the evaluation error of the proposed algorithm is below 0.02. The proposed algorithm exhibits the smallest evaluation error, indicating more accurate trust evaluation, which aids in selecting appropriate consensus nodes and improving data sharing efficiency.

Figure 9. Evaluation error of different trust evaluation algorithms under different evaluation indicators



Note. GCPFN = granular computing–fuzzy Petri net; APN–LA = learning automata-based adaptive Petri net; MAPE = mean absolute percentage error; MAE = mean absolute error; RMSE = root-mean-square error.

CONCLUSION

In this article, we have proposed an IFPN-based node trust evaluation and selection algorithm. We developed a multidimensional indicator system for dynamic trust evaluation that comprises two dimensions: computing capability and honesty. It provides a comprehensive and accurate indicator system for dynamic trust evaluation in electric measurement data sharing and interaction. Moreover, we proposed an IFPN–based node trust evaluation and selection algorithm. The degree of trustworthiness of the IFPN is dynamically updated by fuzzy deviation to enhance the efficiency and accuracy of node trust evaluation and selection. The simulation results indicated that, compared with the GCFPN and APN-LA, the proposed algorithm can reduce consensus delay by 48.72% and 75.13%, respectively, enhancing the consensus convergence speed. The honest behavior ratio is also notably higher, by 45.81% and 52.32%, respectively. In addition, the proposed algorithm demonstrates smaller fluctuations in average delays and honest behavior ratios, with an evaluation error <0.02, ensuring greater accuracy and minimal fluctuations.

Although our simulation results are promising, we recognize that the model's assumption of instantaneous communication between entities might not be fully representative of real world complexities. Future research will address this limitation by incorporating a more realistic communication framework and investigating its impact on the system's performance and robustness.

AUTHOR NOTE

This work was supported by the Science and Technology Project of State Grid Corporation of China under Grant 5700-202318300A-1-1-ZN.

The authors declare no competing interests.

PROCESS DATES

Received: March 8, 2024, Revision: May 22, 2024 Accepted: June 10, 2024

CORRESPONDING AUTHOR

Correspondence should be addressed to Xianbo Du; xianbo_du@163.com

REFERENCES

Bai, L., Fan, K., Bai, Y., Cheng, X., Li, H., & Yang, Y. (2021). Cross-domain access control based on trusted third-party and attribute mapping center. *Journal of Systems Architecture*, *101*, 101957. DOI:10.1016/j.sysarc.2020.101957

Bai, L., Fan, K., Zhang, K., Cheng, X., Li, H., & Yang, Y. (2021). Blockchain-based trust management for agricultural green supply: A game theoretic approach. *Journal of Cleaner Production*, *310*, 127407. DOI:10.1016/j.jclepro.2021.127407

Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. (2018). Review of internet of things (IoT) in electric power and energy systems. *IEEE Internet of Things Journal*, *5*(2), 847–870. DOI:10.1109/JIOT.2018.2802704

Chen, S.-J., Zhan, T.-S., Huang, C.-H., Chen, J.-L., & Lin, C.-H. (2015). Nontechnical loss and outage detection using fractional-order self-synchronization error-based fuzzy Petri nets in micro-distribution systems. *IEEE Transactions on Smart Grid*, *6*(1), 411–420. DOI:10.1109/TSG.2014.2345780

Ding, Z., Ma, J., & Kandel, A. (2013). Petri net representation of switched fuzzy systems. *IEEE Transactions on Fuzzy Systems*, *21*(1), 16–29. DOI:10.1109/TFUZZ.2012.2197755

Fu, J., Zhou, W., & Xu, J. (2023). Design of improved PBFT algorithm based on aggregate signature and node reputation. *Intelligent and Converged Networks, 4*(2), 158–167. https://www.doi.org/10.23919/ICN.2023.0016

Hayashikoshi, M., Noda, H., Kawai, H., Murai, Y., Otani, S., Nii, K., Matsuda, Y., & Kondo, H. (2018). Low-power multi-sensor system with power management and nonvolatile memory access control for IoT applications. *IEEE Transactions on Multi-Scale Computing Systems*, *4*(4), 784–792. DOI:10.1109/TMSCS.2018.2827388

Kait, R., Kaur, S., Sharma, P., Ankita, C., Kumar, T., & Cheng, X. (2024). Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities. *Expert Systems: International Journal of Knowledge Engineering and Neural Networks*, e13561. Advance online publication. DOI:10.1111/exsy.13561

Kiaei, I., & Lotfifard, S. (2020). Fault section identification in smart distribution systems using multi-source data based on fuzzy Petri nets. *IEEE Transactions on Smart Grid*, *11*(1), 74–83. DOI:10.1109/TSG.2019.2917506

Lee, S., & Seo, S. (2022). Design of a two layered blockchain-based reputation system in vehicular networks. *IEEE Transactions on Vehicular Technology*, *71*(2), 1209–1223. DOI:10.1109/TVT.2021.3131388

Li, W., Feng, C., Zhang, L., Xu, H., Cao, B., & Imran, M. I. (2021). A scalable multi-layer PBFT consensus for blockchain. *IEEE Transactions on Parallel and Distributed Systems*, *32*(5), 1146–1160. DOI:10.1109/TPDS.2020.3042392

Liao, H., Mu, Y., Zhou, Z., Sun, M., Wang, Z., & Pan, C. (2021). Blockchain and learning-based secure and intelligent task offloading for vehicular fog computing. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4051–4063. DOI:10.1109/TITS.2020.3007770

Liao, H., Wang, Z., Zhou, Z., Wang, Y., Zhang, H., Mumtaz, S., & Guisami, M. (2022). Blockchain and semi-distributed learning-based secure and low-latency computation offloading in space–air–ground-integrated power IoT. *IEEE Journal of Selected Topics in Signal Processing*, *16*(3), 381–394. DOI:10.1109/JSTSP.2021.3135751

Liao, H., Zhou, Z., Liu, N., Zhang, Y., Xu, G., Wang, Z., & Mumtaz, S. (2023). Cloud-edge-device collaborative reliable and communication-efficient digital twin for low-carbon electrical equipment management. *IEEE Transactions on Industrial Informatics*, *19*(2), 1715–1724. DOI:10.1109/TII.2022.3194840

Liu, H., Xu, D., Duan, C., & Xiong, Y. (2021). Pythagorean fuzzy Petri nets for knowledge representation and reasoning in large group context. *IEEE Transactions on Systems, Man, and Cybernetics. Systems*, *51*(8), 5261–5271. DOI:10.1109/TSMC.2019.2949342

Luo, H., Sun, G., Yu, H., Lei, B., & Guizani, M. (2024). An energy-efficient wireless blockchain sharding scheme for PBFT consensus. *IEEE Transactions on Network Science and Engineering*, *11*(3), 3015–3027. DOI:10.1109/TNSE.2024.3357770

Luo, X., Xue, K., Xu, J., Sun, Q., & Zhang, Y. (2021). Blockchain based secure data aggregation and distributed power dispatching for microgrids. *IEEE Transactions on Smart Grid*, *12*(6), 5268–5279. DOI:10.1109/TSG.2021.3099347

Pan, K., Teixeira, A., Cvetkovic, M., & Palensky, P. (2019). Cyber risk analysis of combined data attacks against power system state estimation. *IEEE Transactions on Smart Grid*, *10*(3), 3044–3056. DOI:10.1109/TSG.2018.2817387

Shi, X., Qiu, R., Mi, T., He, X., & Zhu, Y. (2020). Adversarial feature learning of online monitoring data for operational risk assessment in distribution networks. *IEEE Transactions on Power Systems*, *35*(2), 975–985. DOI:10.1109/TPWRS.2019.2941162

Sun, G., Dai, M., Zhang, F., & Hongfang, Y. (2020). Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles. *IEEE Internet of Things Journal*, *7*(9), 7868–7882. DOI:10.1109/JIOT.2020.2992994

Sun, Z., Zhao, P., Wang, C., Zhang, X., & Cheng, H. (2023). An efficient and secure trading framework for shared charging service based on multiple consortium blockchains. *IEEE Transactions on Services Computing*, *16*(4), 2437–2450. DOI:10.1109/TSC.2022.3216659

Vahidipour, S. M., Meybodi, M. R., & Esnaashari, M. (2015). Learning automata-based adaptive Petri net and its application to priority assignment in queuing systems with unknown parameters. *IEEE Transactions on Systems, Man, and Cybernetics. Systems*, *45*(10), 1373–1384. DOI:10.1109/TSMC.2015.2406764

Wang, H., Jiang, C., & Liao, S. (2001). Concurrent reasoning of fuzzy logical Petri nets based on multi-task schedule. *IEEE Transactions on Fuzzy Systems*, *9*(3), 444–449. DOI:10.1109/91.928740

Zhou, R., Chang, H., Zhou, Y., Xu, J., Lu, Y., & Feng, J. (2023). Constructing Cognitive Reasoning and Decision Making Under Attribute Granular Computing Using Fuzzy Petri Nets. *IEEE Transactions on Cognitive and Developmental Systems*, *15*(3), 1170–1182. DOI:10.1109/TCDS.2022.3197616

Zhou, Z., Jia, Z., Liao, H., Lu, W., Mumtaz, S., Guizani, M., & Tariq, M. (2021). Secure and latency-aware digital twin assisted resource scheduling for 5G edge computing-empowered distribution grids. *IEEE Transactions on Industrial Informatics*, *18*(7), 4933–4943. DOI:10.1109/TII.2021.3137349

Zhou, Z., Wang, B., Dong, M., & Ota, K. (2020). Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. *IEEE Transactions on Systems, Man, and Cybernetics. Systems*, *50*(1), 43–57. DOI:10.1109/TSMC.2019.2896323