

A Terminal Trust Assessment Method Based on Consensus Trust Aggregation

Shixin Cheng*, Jinzhe Zhang*, Liping Han*

*State Grid Qinghai Information & Telecommunication Company, Xining, China
1713147519@qq.com, rubymelloroad@gmail.com, 2690618708@qq.com

Abstract— Due to the numerous terminal devices in a power network environment, it is difficult to defend against the attack of malicious nodes, like deception and data tampering in common trust models. A terminal trust assessment method based on consensus trust aggregation is proposed in this paper. Aimed at the direct trust of a goal node, standard quantitative trust value is predicted based on records of historical access nodes after filtering great trust factors. Trustworthy consensus nodes are selected to participate in the feedback trust consensus module. The consensus trust verification module is designed to ensure the security of the consensus, including consensus verification and malicious node replacement. The simulation results demonstrate the proposed method can reflect the trust level of terminal nodes more effectively, which has a better constraint on suspicious nodes.

Keywords— trust assessment; consensus; power mobile network; terminal node

I. INTRODUCTION

With the in-depth development of the Internet and the widespread application of new technologies such as IoT in the power industry, the types and numbers of mobile terminal devices accessed in power networks have increased sharply. It poses a serious challenge to power network security in [1]. In terms of power network security defense, internal system attacks are far more serious than external attacks, and these malicious terminals existing within the system can be faked into legitimate terminals to invade the system. The security of the accessed terminal can be judged by whether it is authenticated and authorized. It can also be assessed by collecting data generated by a series of actions of the terminal in [2]. As a "soft technology" that effectively protects against malicious terminal attacks, trust management is highly scalable and applicable. Researchers have proposed many preliminary trust models in this field, such as a trust model based on game theory and a trust model based on fuzzy logic in [3]-[4].

II. RELATED WORK

Most trust evaluation models integrate direct trust and indirect trust to evaluate the final trust of terminal nodes and judge the reliability and accuracy of a trust evaluation model by a series of index parameters. Fang [5] proposed a trust evaluation method based on information entropy, where the direct trust is calculated based on the credibility model under

exponential distribution and updated through a sliding window. The indirect trust is expressed as a weighted sum of the direct trust values on the trust links connected by the endpoints. However, different research scholars have their ideas about it. Wu [6] argued indirect trust can be obtained through link recommendation, and propose a network trust model BLTM based on Beta and Link Quality Indicator (LQI), which can better guarantee the accuracy and stability of low-quality link trust values. Also, higher system energy consumption is required to screen an optimal link in this model. For this reason, some scholars have designed recommendation rules and introduced them into network security assessment. Shabut [7] filtered reasonable feedback information by calculating confidence, deviation, and closeness parameters of recommendation suggestions. Feng [8] proposed a Bayesian theory-based trust model BTMS, which sets third-party intermediate nodes as trustworthy nodes to calculate recommendation trust. Anuoluwapo [9] set a new recommendation rule to evaluate the recommendation trust value. Once direct interaction occurs between the source and target nodes, the recommendation trust cannot be contained in the integrated trust value. Although these models above solve the fraudulent behavior of malicious nodes. They only take one single trust dimension into consideration, resulting in poor accuracy of the integrated trust calculation.

As a decentralized distributed database, blockchain [10] can store data in block form and transmit it according to the chained data structure. Based on the great characteristics of blockchain, scholars have successively introduced the consensus idea into the field of trust evaluation to reduce the participation of malicious nodes. S. Besfort [11] proposed a tampering consensus method for IoT nodes based on a trust assessment model, which uses the similarity between nodes to select recommended nodes to complete tampering consensus and reduce trust evaluation bias. In order to improve nodes' enthusiasm to participate in consensus and avoid centralization, Kong [12] assigned nodes' reputations according to consensus completion and reduced the consensus participation rate of low-reputation nodes. Wang [13] divided nodes according to credit level and selected nodes with reputation value higher than the threshold to participate in consensus.

To solve the problems mentioned above, a terminal trust assessment method based on consensus trust aggregation CMTA is designed. Considering the decreasing time, energy,

interaction, and location trust factors are introduced to obtain historical trust value. The master node is selected by reputation, and nodes with high credibility are more likely to participate in consensus. Finally, the integrated trust value is calculated by combining direct trust value and consensus trust value.

III. TRUST ASSESSMENT MODEL

3.1 Model framework

Trust assessment in distributed network can be defined as the analysis of the future trust situation of a terminal node based on its historical access behaviour. As shown in Figure 1, each terminal node has a relationship with the edge server. Nodes with interaction records with the target node will be selected from the historical access behaviour database to form the set of historical access nodes. Based on the historical trust assessment value, the direct trust value will be predicted. In the consensus process, consensus nodes are selected from the set of historical access nodes based on the reputation voting mechanism. Consensus nodes and master nodes cooperate with each other to obtain consensus trust values, which is sent to the edge server for final trust aggregation. Among them, target node denotes the terminal device that is accepted for evaluation in the network, noted as A. The history access node denotes the node that has historical interaction with target node, and is the subject of the evaluation of target node, noted as r_i . The set of history access nodes is defined as R. The consensus node denotes the node that participates in the feedback trust consensus, and is a subset of the history access nodes, noted as Q.

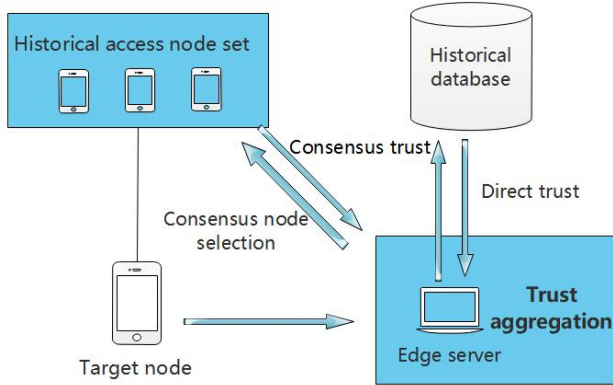


Figure 1. Framework of trust assessment

3.2 Direct trust model

The direct trust values in traditional trust models [14-15] are obtained based on Bayesian theory. In this paper, the direct trust calculation includes two modules: acquiring the node history data module and calculating direct trust value module. The server obtains the historical access record data associated with the target node from the database, such as access duration, access frequency, and energy consumption. The main trust factors will be determined to participate in the final direct trust evaluation. The current trust value of the target node is obtained, which is noted as the direct trust value.

1) Confidence factor determination

Interaction trust factor. The higher the number of interactions between the target node and the historical access node, the higher the trust level of the historical access node and the more trustworthy the trust score provided by that node. Therefore, the ratio of the number of successful interactions between the target node and the historical access node in the past certain period INT_{suc} to the total number of interactions INT_{total} is used to indicate the positivity of the node to participate in the interaction. The interaction trust factor between target node A and the historical access node r_i is calculated as:

$$T_{Ai}^{int} = \frac{INT_{suc}}{INT_{total}} \quad (1)$$

Energy trust factor. During the interaction process, a certain amount of energy is consumed. If more energy is consumed by a node, it indicates that the more complex the node is and the higher the possibility of risk. Therefore, the energy trust factor is expressed by the energy loss of the target node when accessing the historical nodes. The energy trust factor T_{Ai}^{ene} between the target node A and the historical access node is calculated as:

$$T_{Ai}^{ene} = \frac{E_A^{last}}{E_A^{initial}} \quad (2)$$

Location trust factor. If the distance between two nodes in the network is too far, the higher the possibility of long-distance dangerous access between nodes. Therefore, the physical distance between the target node A and the historical access node r_i and the communication service radius R_A of the target node are combined to determine the location trust factor of the target node. To simply presentation, the trust factor is expressed in a composite triad form as $T_{Ai}(t) = [T_{Ai}^{int}, T_{Ai}^{ene}, T_{Ai}^{loc}]$.

$$T_{Ai}^{loc} = 1 - \frac{dis_{Ai}}{R_A} \quad (3)$$

2) Direct trust calculation

After obtaining the data related to the three trust factors from the database, the server calculates the direct trust value in a local field. As historical access records are time-sensitive, the closer the time interval to the current one, the greater the value of the data provided by the record. For this reason, the access records from the target node A with the historical access nodes are framed from the access data with a time window of t intervals from the current time. The trust factor at different moments $T_{Ai}(1), \dots, T_{Ai}(t)$ is calculated to predict the trust factor for the next moment. For example, the trust factor of the location is predicted at the next moment by the following formula.

$$p_{Ai}^{loc} = \frac{\sum_{t \in (0, T]} T_{Ai}^{loc}(t)}{T} \quad (4)$$

Assuming that there are N historical access nodes within the time window, the trust factor of all historical access nodes with respect to the target node is calculated as follows. Here, take the location trust factor as an example.

$$\phi_A^{loc} = \frac{\sum_{i=1}^N p_{Ai}^{loc}}{N} \quad (5)$$

Finally, the direct trust value of the target node is calculated in combination with the predicted values of the above three trust factors.

$$\varphi_A = \frac{\phi_A^{loc} + \phi_A^{ene} + \phi_A^{int}}{3} \quad (6)$$

3.3 Consensus trust

A consensus mechanism for indirect trust assessment is introduced in this paper. The specific consensus process is shown in Figure 2. Each round of the consensus process includes 3 stages: node division, consensus process, and consensus verification. Before the first round, the list of consensus nodes that can participate in the consensus needs to be filtered. The consensus nodes will send the feedback trust value to the master node to trigger the trust aggregation and verification mechanism. Till the end of consensus, the nodes participating in this round of consensus will be updated with reputation, and malicious nodes will be replaced to guarantee the security of the next round of consensus.

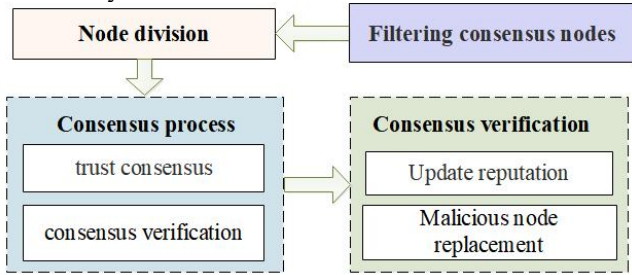


Figure 2. Framework of the consensus process

1) Consensus node determination

To reduce the cost of communication between numerous nodes, the initial reputation value of nodes in a voting mechanism is designed before consensus. Node reputation is assumed as an indicator to filter nodes with high credibility values to participate in consensus. To avoid nodes cooperating with each other to falsify voting data, the organization node is defined to be responsible for counting the voting results. The specific steps are as follows.

Construct a list of relevant nodes. The nodes with the largest average value coefficients, which represent node sensitivity, are selected to form the list of relevant nodes. The time decay factor $TI(t_n)$ determines the decay rate of the historical trust assessment value. $T_{A,i}^{old}$ represents the historical trust assessment vector of the historical access node r_i to the target node A in the time range $[t_1, t_n]$.

$$Value_{A,i}^{t_n} = \frac{TI(t_n)}{1 - \sum_{r_i \in R} \sqrt{T_{A,i}^{old}}} \quad (7)$$

$$TI(t_n) = \frac{1}{1 + |t_n - t_1|} \quad (8)$$

Construct a consensus node list. The node that the target node has visited most recently is selected as an organization node, which broadcasts voting messages to all relevant nodes. Other nodes receive the message, vote on all involved nodes in turn, and send the voting result to the organization node. The organization node calculates the initial reputation value of each node according to equation (9). Nodes with the largest

initial reputation value are picked as consensus node $Q^l = \{q_1, q_2, \dots, q_l\}$. The initial reputation value and reputation ranking of elected nodes are broadcast.

$$fame_i^{vote} = \frac{\sqrt{n_i / \sum_{i=1}^n n_i}}{1 + e^{-[vote_i * G / V_i - (V_i - vote_i) * g / V_i]}} \quad (9)$$

Where $fame_i^{vote}$ denotes the initial reputation value of node q_i , which is in range of $[0, 1]$. n_i denotes the number of votes received by node q_i . $vote_i$ denotes the number of valid votes cast by node q_i . V_i denotes the number of votes participated by node q_i . If the vote is successfully finished without invalid votes, add G to the node. Or, deduct g points.

2) Node division

The nodes of the initial reputation value ranking top 30 percent in the consensus node list are assigned to the master node candidate set, where nodes with the highest reputation are the master node for the first consensus. The rest 70 percent of the nodes are listed in descending order to select the top M nodes as the consensus node set for the first consensus, and the rest are added to the consensus node candidate set. Nodes with low reputation will be replaced by nodes in a candidate set, and the replaced nodes are automatically added to the candidate set.

The number of feedback from consensus nodes in each consensus process is inversely proportional to the reputation value. The more feedback, the more interference information, specifically the method of updating reputation is defined as below.

$$fame_i^t = \frac{fame_i^{t-1}}{1 + fame_i^{vote}}, t = 1, 2, \dots, n \quad (10)$$

Where $fame_i^t$ denotes reputation of consensus node q_i at the t th feedback of the subjective trust assessment value. $fame_i^0$ denotes the initial reputation value of the node, equal to $fame_i^{vote}$.

3) Trust consensus

Reaching a consensus [16] is the core of feedback trust variability of consensus nodes. Considering that consensus nodes have been previously classified through the reputation mechanism, it can be assumed that the nodes involved in the consensus process are reliable and honest nodes. The trust consensus process is described as follows.

(1) The server sends feedback trust upload instructions to a master node, which receives and broadcasts it to all consensus nodes.

(2) The consensus nodes upload the feedback trust value about the target node to the master node and save another copy locally.

(3) When the master node receives the feedback trust values from at least 2/3 consensus nodes, feedback trust aggregation mechanisms are triggered. Consensus node reputation values based on the feedback behavior characteristics will be updated and used as the weight of node feedback trustworthiness. Then the final consensus trust value is broadcast to all nodes.

(4) Consensus nodes verify the consensus trust value and send verification results to the organization node. If the

number of consensus nodes participating in verification is more than 1/2 and the number of votes “for” is greater than the number of votes “against”, the validation process ends. The organization node broadcasts the validation passed message.

(5) The master node receives the verification pass message and uploads the consensus trust value to the server. This round of consensus is over.

3.4 Combined trust value

The server weights the aggregated direct trust value and consensus trust value to obtain the integrated trust value and uses adaptive dynamic weights to assign the weight coefficients according to equation (11). The flowchart of the comprehensive trust evaluation of the target node is shown in Figure 3.

$$T_A = \varphi_A \times \gamma + T_A^{com} \times (1 - \gamma) \quad (11)$$

Where γ is the adaptive weighting factor, which takes values in the range [0,1].

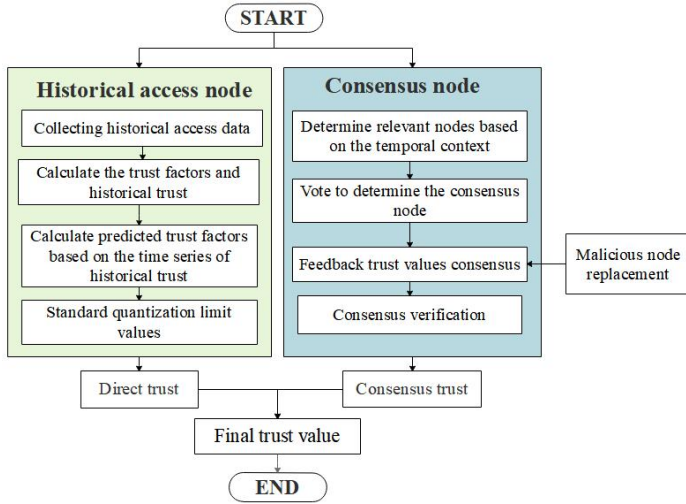


Figure 3. Flowchart of terminal comprehensive trust assessment

IV. EXPERIMENTAL ANALYSIS

4.1 Experimental environment and parameter settings

To verify whether the model can effectively reflect the trust value and defend against malicious nodes, we build a simulation environment in Matlab. 100 terminal nodes are randomly distributed in a square area of 100*100 in Figure 4. Normal nodes are marked as black dots and malicious nodes are marked as stars. Normal nodes were set at 90% and malicious nodes are 10%. Other simulation parameter values are shown in Table 1.

TABLE 1. SIMULATION PARAMETER SETTINGS

Parameter name	Simulation value
Total number of interactions INT_{total}	10
Initial energy of the target node $E_A^{initial}$ (J)	100

Initial reputation value of history node $fame_i^{vote}$	0.7
Communication service radius R_A (m)	20
Consensus packet size (bit)	600
Consensus cycle (s)	1200

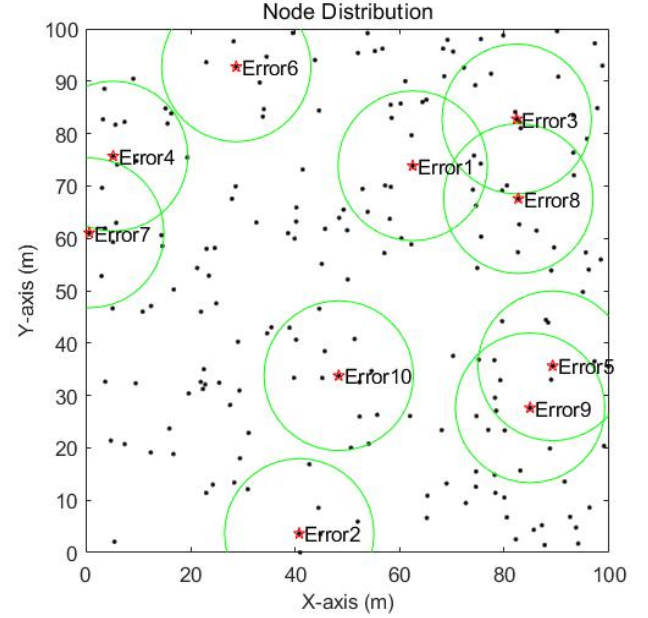


Figure 4. Distribution diagram of terminal nodes

4.2 Analysis of simulation results

The trust assessment method proposed in this paper is compared with existing trust assessment methods [17-18]. With the guarantee of no packet loss, the historical access trust assessment factors of the target node are set validly. Then the server selects consensus nodes to participate in the consensus, and master node aggregates the feedback trust value of each consensus node. Here, the relevant parameters are continuously adjusted to obtain consensus trust values under different experimental conditions.

1) Reliability analysis

Assuming the server is always trustworthy in the experiment, the reliability analysis mainly determines whether the consensus trust value is reliable or not. Here, a consensus success rate $SR = 1 - \frac{\text{first}}{\text{max}}$ is used to judge the reliability of trust. first indicates the number of rounds while the first consensus ends. max indicates the maximum number of consensus rounds the system allowed, which is set to 50.

2) Consensus process energy loss

The energy loss of nodes can be expressed by the number of feedback. The higher the number of feedback, the higher the energy consumption. Assuming that the initial energy of each consensus node is 100J. In each round of feedback trust transmission, 5J energy will be consumed. As shown in Figure

5, the total energy loss of all nodes with different numbers of nodes is compared with other models[19-21] separately. Due to the constraints of the decreasing reputation mechanism, nodes need to ensure the feedback number reasonable, which effectively avoids malicious nodes from feeding back invalid information. Thus, the total energy loss of CMTA is less than the other two models.

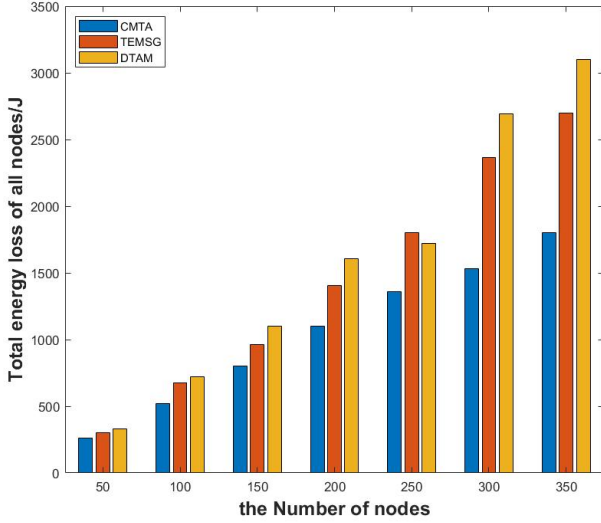


Figure 5. Energy loss during feedback trust transmission

3) Malicious node detection rate

The factors that threaten system safety are mainly the malicious feedback and voting of malicious nodes in the feedback trust consensus. Therefore, the number of malicious nodes is adjusted from the initial 10% to 20% and 40%. The detection rate of malicious nodes is identified by the ratio of the number of replaced malicious nodes to the total number of malicious nodes. As shown in Figure 6, the rate of detection accuracy is decreasing while the number of malicious nodes increases. As the master node needs to verify the feedback trust of consensus nodes, and malicious nodes replaced module, CMTA model ensures a higher consensus success rate. The reputation update mechanism can also better screen out malicious nodes and reduce the probability of participation.

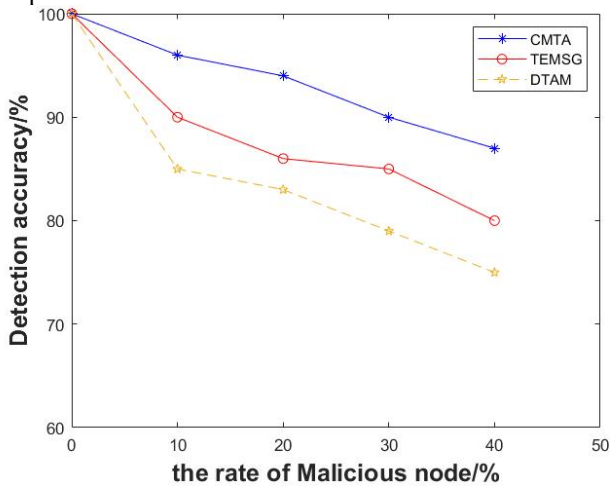


Figure 6. Interaction success rate under different ratios of malicious nodes

V. CONCLUSION

In this paper, we propose a trust evaluation method for end devices in an edge computing environment, which combines node reputation and consensus mechanism to carry out the evaluation, considering energy trust, location trust, and interaction trust among nodes in direct trust evaluation, and selecting recently active nodes considering the time decay of node trust. To ensure the security of consensus, the initial reputation is determined by voting in the initial stage, which effectively resists malicious nodes from tampering with the reputation value at will. The proposed consensus verification module effectively alleviates the problem of master nodes falsely reporting the uploading of incorrect trust values and failing to objectively evaluate the target nodes. Based on Matlab simulation environment and several evaluations, the final experimental data shows that the CMTA model can effectively reflect the trust change of the target node, and also performs well in resisting malicious tampering, misrepresentation, and energy loss during data transmission. Future research will focus on methods for trust factor selection and feedback trust aggregation.

ACKNOWLEDGMENT

This work is supported by the program of Research and Application of Power Business Dynamic Access Control Technology based on Zero Trust Framework under Grant number 522814220002.

REFERENCES

- [1] Y. Dong, B. Sun, and W. Gang, "Research on modeling method of power system network security risk assessment based on object-oriented Bayesian network," *Energy Reports*, 7(S7), 289-295, 2021.
- [2] M. Manisha and J. Shivani, "MATEM: A Multi-Agent-Based Trust Evaluation Model for Discovery and Delivery of Reliable Cloud Services," *International Journal of Cloud Applications and Computing (IJCAC)*, 12(1), 1-17, 2022.
- [3] R. Rani, S. Kumar, and U. Dohare, "Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach," *IEEE Internet of Things Journal*, 6(5), 8421-8432, 2019.
- [4] D. Velusamy, G. Pugalandhi, and K. Ramasamy, "A Cross-Layer Trust Evaluation Protocol for Secured Routing in Communication Network of Smart Grid," *IEEE Journal on Selected Areas in Communications*, 38(1), 193-204, 2020.
- [5] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks," *Journal of Network and Computer Applications*, 59(1), 88-94, 2016.
- [6] X. Wu, J. Huang, J. Ling, and L. Shu, "BLTM: Beta and LQI Based Trust Model for Wireless Sensor Networks," *IEEE Access*, 7, 43679-43690, 2019.
- [7] Shabut, M. Antesar, Dahal, P. Keshav, Bista, S. Kumar, and U. Irfan, "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs," *IEEE transactions on mobile computing*, 14(10), 2101-2103, 2015.
- [8] R. Feng, X. Han, and Q. Liu, "A credible bayesian-based trust management scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, 2015(11), 678926-678928, 2015.
- [9] A. Anuoluwapo, H. Cheng, Q. Shi, and J. Cao, "CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things," *IEEE Internet of Things Journal*, 6(3), 5432-5445, 2019.

- [10] X. Zhu, "Research on Key Technologies and Applications of Energy Internet Blockchain," *E3S Web of Conferences*, 118-122, 2019.
- [11] S. Besfort, T. Ulrich, L. Armin, and G. Bogdan, "Novel trust consensus protocol and blockchain-based trust evaluation system for M2M application services," *Internet of Things*, 7, 100058-100060, 2019.
- [12] L. Kong, B. Chen, and F. Hu, "Lightweight Asynchronous Provable Byzantine Fault-Tolerant Consensus Mechanism for UAV Network," *Drones*, 6(8), 187-191, 2022.
- [13] Y. Wang, M. Zhong, and T. Cheng, "Research on PBFT consensus algorithm for grouping based on feature trust," *Scientific Reports*, 12(1), 2022.
- [14] Y. Wang, J. Wen, and W. Zhou, "A trust-based evaluation model for data privacy protection in cloud computing," *IJHPCN*, 14(2), 147-156, 2019.
- [15] L. Kong, F. Zhai, Y. Zhao, and N. Qin, "Evaluation method of trust degree of distribution IoT terminal equipment based on information entropy," *Journal of Physics: Conference Series*, 1754(1), 1-6, 2021.
- [16] J. Ping, D. Li, Z. Yan, X. Wu, and S. Chen, "A trusted peer-to-peer market of joint energy and reserve based on blockchain," *Electric Power Systems Research*, 214(PA), 2022.
- [17] Y. Yang, "An Efficient Trust Evaluation Scheme for Node Behavior Detection in the Internet of Things," *Wireless Personal Communications*, 93(2), 571-587, 2017.
- [18] Q. K. Naseer, I. M. Najam, and J. Gwanggil, "A trust evaluation model for secure data aggregation in smart grids infrastructures for smart cities," *Journal of Ambient Intelligence and Smart Environments*, 13(3), 235-252, 2021.
- [19] Q. Wu, X. Zhang, M. Zhang, Y. Zhou, and R. Zheng, "Reputation Revision Method for Selecting Cloud Services Based on Prior Knowledge and a Market Mechanism," *The Scientific World Journal*, 2(17), 2014.
- [20] J. Yuan, X. Li, "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion," *IEEE Access*, 6, 23626-23638, 2018.
- [21] T. N. Binh, L. G. Myoung, U. T. Won, and M. Michael, "Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things," *IEEE Transactions on Information Forensics and Security*, 14(10), 2705-2719, 2019.



Shixin Cheng born in 1995, received the Bachelor degree in Electronic Engineering from Tsinghua University in 2020. His research interests include Cyberspace Security and Data Security.



Jinzhe Zhang born in 1997, received the Bachelor degree in Software Engineering from Chongqing University in 2020. His research interests include Terminal Security and Network Penetration.



Liping Han born in 1997, received the Bachelor degree in Computer Science and Technology from Qinghai University in 2020. Her research interests include Network Security Defense Based on Honeypot Technology.