Evaluation method of trust degree of distribution IoT terminal equipment based on information entropy

Kong Lingda¹, Zhai Feng¹, Zhao Yingjie¹, Qin Nan²*, Li Dashuai², Cai Shaotang²

¹China Electric Power Research Institute, Beijing, 100192, China
²Tianjin University, Tianjin, 300010, China

*Corresponding author’s e-mail: qinnan88@tju.edu.cn

ABSTRACT: Power distribution Internet of Things terminal equipment is vulnerable to multiple security threats, such as identity disguise, information theft, data tampering. Traditional security methods cannot resist internal network attacks from compromised terminals. The trust evaluation system is an effective mechanism to protect power distribution IoT terminals from internal attacks. This paper proposes a trust evaluation method based on information entropy for the trust problem of power distribution Internet of Things communication terminal. First, the direct trust value is estimated by the model based on the reputation of exponential distribution, and then the direct trust value is updated by the sliding window and forgetting factor. According to the entropy theory, the uncertainty of the direct trust value is measured, and the indirect trust value is introduced to make up for the inaccuracy of the direct trust judgment, and the judgment accuracy is improved through the comprehensive evaluation of the direct trust value and indirect trust value. Experimental simulations show that the method in this paper can effectively resist switch attacks and collusion attacks. At the same time, the method proposed in this paper can better evaluate malicious and normal terminals than binomial trust management and trust evaluation based on beta distribution.

1. Introduction

Power distribution Internet of Things is a new type of power network form produced by the deep integration of traditional industrial technology and Internet of Things technology. Through the comprehensive interconnection, intercommunication, and interoperability of the distribution network equipment, the comprehensive perception, data integration and intelligent application of the distribution network can be realized. With the continuous development of power distribution Internet of Things, the security threats facing terminal equipment are increasing.

In recent years, trust management has been regarded as one of the effective protection mechanisms to ensure network security and an effective way to resist internal attacks [1]. Trust management evaluates the trust value of the terminal based on the historical behavior of the terminal, thereby estimating the credibility of the terminal to perform a specific task. Although preliminary research has been carried out, there are still some shortcomings. For example, researchers improved the trust management based on beta distribution [2] and binomial distribution [3] to improve the accuracy of trust assessment. However, both of them lead to inaccurate trust assessment due to the use of subjective distribution of trust factors.

In response to the above problems, for power distribution Internet of Things communication terminal equipment, this paper proposes an evaluation method of trust degree of distribution IoT terminal equipment based on information entropy. The method uses exponential distribution to build the reputation of the terminal, calculate the direct trust value based on historical behavior, and then introduce
the concept of sliding window to update the direct trust. The uncertainty of direct trust is determined based on the theory of information entropy, and the indirect trust value is introduced to make up for the inaccuracy of direct trust determination. Through the comprehensive evaluation of direct trust value and indirect trust value, the accuracy of judgment is improved. The practicability and advancement of the algorithm proposed in this paper are verified by simulating attack scenarios such as selective forwarding attacks, switching attacks, and collusion attacks in the internal attacks of the distribution IoT network.

2. Related work

Trust management is divided into two categories: trust model and trust management scheme. At present, in terms of trust model research, Kamvar SD et al. [5] considered the security of information storage and proposed a trust evaluation model Eigen Trust for P2P networks. The model performs distributed calculations according to the data source. Zheng Y et al. [6] proposed a probability-based trust propagation model. Teacy WTL et al. [7] proposed a hierarchical Bayesian trust model, which calculates the trust value of nodes through the correlation of node behaviors. Zhu J et al. [8] proposed a trust model combining fuzzy sets and D-S evidence theory.

In terms of trust management solutions, Bao F et al. [9] improved the attack model related to trust management and proposed a trust management model of the Internet of Things based on social relations. Chen IR et al. [10] used collaborative filtering methods to screen trust recommendation nodes, and proposed a trust management model for the Internet of Things based on social relationships.

Based on the above analysis of the trust model and trust management system, it can be seen that in most existing trust management methods, few schemes consider trust evaluation and verification under multiple hybrid attack modes.

In response to the above problems, this paper designs an evaluation method of trust degree of distribution IoT terminal equipment based on information entropy.

3. Model description

Fig.1 Architecture diagram of power distribution wireless private network communication system

Aiming at the power distribution wireless private network communication system shown in Figure 1, this paper proposes a trust and reputation evaluation method for power distribution wireless communication terminals based on the principle of information entropy. The communication terminal communicates with the base station in the uplink, and communicates with the concentrator in the downlink, which realizes the functions of control command issuance, data collection, and data transmission. When the terminal needs to interact, the terminal will decide whether to interact with
another terminal based on the level of trust.

3.1 Trust and reputation evaluation system model

3.1.1 Direct trust

(1) Calculation

Direct observation is a record of the interaction between two entities, obtained through observation, without a third party. Direct trust comes from direct observation between terminal $i$ and terminal $j$, denoted as $E_{ij}$. Since the exponential distribution represents the probability of the time interval between two adjacent events, the exponential distribution is used as the prior distribution of the interaction between terminals. Assuming that the latter interacts in the same way as the former, direct trust is expressed as follows:

$$E_{ij} = \frac{\alpha}{\alpha + \beta}$$  \hspace{1cm} (1)

In formula (1), the variable $\alpha$ represents the number of successful interactions between terminals, and $\beta$ represents the number of unsuccessful interactions.

(2) Update

The trust value is constantly changing due to the real-time update of terminal interaction history information, and the newer the history information, the greater the impact on trust. Considering the huge amount of information interaction of the power Internet of Things terminal equipment, too much historical information participating in the update will increase the system overhead and cause the trust value update speed to slow down, so the history record in the sliding window $N$ is used for trust update. The $N$ terminal interaction data records recorded by the sliding window are divided into $n$ time slots, and each time slot is sequentially numbered. There are malicious and successful historical interaction data in the time slot in the sliding window. The malicious data will cause the trust of the time slot to be seriously affected, resulting in the loss of the time slot trust. Therefore, this paper introduces the forgetting factor $r_t$ to measure the impact of malicious behavior.

$$r_t = 1 - E_{ij}^t, t = 1, 2, \ldots, n$$  \hspace{1cm} (2)

Where $E_{ij}^t$ is the direct trust of the terminal at the end of the $t$-th time slot. In time slot $t$, terminal $i$ has a monitoring behavior for terminal $j$, the number of successful interactions at the end of this time slot is recorded as $\alpha_{ij}^t$, and the number of failed interactions is recorded as $\beta_{ij}^t$.

$$\alpha_{ij}^{new} = \sum_{t=1}^{n} \alpha_{ij}^t, \quad t = 1, 2, \ldots, n$$  \hspace{1cm} (3)

$$\beta_{ij}^{new} = \sum_{t=1}^{n} \beta_{ij}^t, \quad t = 1, 2, \ldots, n$$  \hspace{1cm} (4)

The new trust value can be obtained from the above two formulas. Substituting $\alpha_{ij}^{new}$ and $\beta_{ij}^{new}$ into formula (4), the new trust value calculation formula is as follows:

$$E_{ij} = \frac{\alpha_{ij}^{new}}{\alpha_{ij}^{new} + \beta_{ij}^{new}}$$  \hspace{1cm} (5)

(3) Determination

Entropy is a measurement of the uncertainty or amount of information in a random signal or event. Assume that $H(E_{ij})$ is the directly observed entropy, and $thr$ is the uncertainty threshold. The setting of the threshold is closely related to the security of the network system. The larger the entropy threshold, the lower the system security. If $thr \leq H(E_{ij}) \leq 1$, it means that the uncertainty of direct trust is high and more relevant information is needed, so indirect trust is introduced. If not, then the total trust of terminal $j$ can be simply set to the direct trust value, that is, the total trust $OS_{ij} = E_{ij}$.

3.1.2 Indirect trust

When the terminal is deemed "uncertain", third-party advice is needed.

The terminal $i$ is evaluated by obtaining the recommendation of terminal $j$ from the neighbor terminal $k$ (denoted as $N_k$) that terminal $i$ and $j$ share. Terminal $i$ already has a priori reputation distribution of the
public neighbor terminal $k$. The terminal $i$ sends a query message to the neighbor terminal, and the common neighbor terminal of the terminal $i$ and the terminal $j$ sends an interaction record $(\alpha_{ij}, \beta_{ij})$ as a response. Therefore, the reputation of terminal $i$ and terminal $j$ can be expressed as $(\alpha_i, \beta_i)$.

Assume that the recommendation provided by the public neighbor terminal $k$ is $Y_{ik}^*$, Given $(\alpha_{kj}, \beta_{kj})$ and $(\alpha_{ik}, \beta_{ik})$, the recommended trust value is calculated as follows. In formula (11), $(Y_{\alpha_{ik}}^*, Y_{\beta_{ik}}^*)$ is the recommended interaction record, $Y_{Kij}$ represents the successful interaction record observed by the public neighbor terminal, and $Y_{\beta_{ij}}$ represents the failed interaction record observed by the public neighbor terminal.

$$Y_{\alpha_{ij}}^* = \alpha_j + \frac{\alpha_k}{\alpha_h + \beta_k} \times \alpha_i$$

$$Y_{\beta_{ij}}^* = \beta_j + \frac{\alpha_k}{\alpha_h + \beta_k} \times \beta_i$$

$$Y_{ij}^* = \frac{Y_{\alpha_{ij}}^*}{1 + Y_{\beta_{ij}}^*}$$

Estimating the trust degree of the recommender is of great significance for ensuring the accuracy of indirect trust calculation. Only suggestions from reliable terminals are acceptable. The trust degree of terminal $i$ to recommender $k$ is expressed as follows:

$$S_k = \frac{1}{\alpha_h + \beta_k}$$

In this model, the weight is assigned according to the trust degree of the recommender. The method of calculating $Y_{ij}^*$ weight is as follows [4]:

$$\mu_i = S_k \sum_{k=1}^q S_k, \quad k = 1, 2, \cdots, q$$

In formula (18), $\mu_k (0 \leq \mu_k \leq 1, \sum_{k=1}^q \mu_k = 1)$ is the weight of $Y_{ij}^*$, and $q$ is the number of suggestions received. Indirect trust is expressed as follows:

$$IE_{ij} = \sum_{k=1}^q \mu_k \times Y_{ij}^*$$

### 3.1.3 Aggregate trust

The calculation formula of aggregate trust is shown in equation (12).

$$\begin{align*}
OS_{ij} &= E_{ij} & 0 \leq H(E_{ij}) \leq \text{thr} \\
OS_{ij} &= v_{ID} E_{ij} + v_D E_{ij} & \text{thr} \leq H(E_{ij}) \leq 1
\end{align*}$$

In the above formula, $OS_{ij}$ is the aggregate trust value, $E_{ij}$ is the direct trust value, $IE_{ij}$ is the indirect trust value, $v_D$ is the direct trust weight, and $v_{ID}$ is the indirect trust weight.

### 4. Experimental simulation and analysis

This paper uses a typical power distribution wireless private network example to verify the trust authentication of communication terminals. This paper uses $(\alpha, \beta)$ settings in four different scenarios to simulate the trust evaluation under different initial trust situations, and compares them with the BRSN [13] algorithm based on binomial trust management and the Beta trust management RFSN [12] algorithm. The simulation parameters are set as follows: Initial trust 0.5, Terminal range $450 \times 450$ m$^2$, Number of terminals 120, The sampling period 6min, Communication radius 40 m, Initial weight factor $\lambda_D, \lambda_{ID}$ 0.5, 0.5, Communicate power consumption 4 J, $\text{thr}$ 0.25, Packet size 1 600 bits.

Scenario 1: Set terminal $j$ as an unreliable terminal, and one of the neighbor terminals between terminal $i$ and terminal $j$ is an unreliable terminal, and the other neighbor terminals are reliable terminals.

It can be seen from figure 2, when an unreliable terminal launches an attack, the terminal trust value of the three methods gradually decreases. But the trust value of the method in this paper decreases faster than RFSN and BRSN, which shows that the method in this paper has better response performance when resisting attacks initiated by unreliable terminals.
Scenario 2: In the 20th cycle, a small number of malicious terminals are introduced to simulate switch attacks, and the attack behavior is removed after the 40th cycle.

Fig. 2 Malicious terminal trust value

Fig. 3 Terminal trust evaluation under switch attack

It can be seen from figure 3 that the trust value of the three methods decreases significantly when the switch attack occurs, and the trust value slowly rises after the switch attack ends. However, the trust value of the method in this paper decreases much faster than RFSN and BRSN, which shows that the terminal only needs a small amount of bad behavior to quickly cause the loss of trust in a short time, which shows that the algorithm in this paper can detect malicious attacks more sensitively.

Scenario 3: Under a collusion attack, a malicious terminal can continue to work as a normal terminal. It is set that terminal $j$ is unreliable and there are unreliable neighbor terminals. At the same time, multiple malicious terminals combine their respective interaction times.

It can be seen from figure 4 that the terminal trust value of the method in this paper gradually decreases when a collusion attack occurs, but the terminal trust value of RFSN and BRSN gradually increases with the occurrence of a collusion attack. This shows that the proposed method can effectively resist collusion attacks, while RFSN and BRSN have poor performance against collusion attacks.

5. Conclusion

This paper proposes a trust evaluation method based on information entropy, which uses exponential distribution to establish a trust model of distribution network communication terminals, and uses information entropy theory to calculate terminal aggregate trust values. This method takes into account various internal network attack modes such as switch attacks, defamation attacks, and collusion attacks in the distribution communication terminal network. While ensuring the accuracy of trust evaluation, it can perform trust evaluation on the distribution network communication terminals. The simulation results show that the method in this paper can reasonably evaluate the uncertainty of the terminal and can resist a variety of internal attacks, which can verify the feasibility and advancement of the method in this paper. Subsequent work will continue to carry out research on lightweight trust models to optimize computing overhead, and research on combined attack resistance performance to improve the security performance of power distribution communication networks.
Acknowledgments
This paper was supported by the Research on Integrated Energy Metering Collection Technology for Customer Side Energy Internet (No. 1100-201919158A-0-0-00).

References
[1] Bhattarai S, Wang Y. End-to-End Trust and Security for Internet of Things Applications. Computer, 2018, 51(4):20-27.
[2] Fang W, Zhang W, Yang Y, et al. A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution[J]. Chinese Science, 2017, 060(004):P.60-70.
[3] Lopez J, Roman R, Agudo I, et al. Trust management systems for wireless sensor networks: Best practices[J]. Computer Communications, 2010, 33(9): 1086-1093.
[4] Zhao J, Huang J, Xiong N. An Effective Exponential-based Trust and Reputation Evaluation System in Wireless Sensor Networks[J]. IEEE Access, 2019, 7: 33869-33869.
[5] Kamvar S D, Schlosser M T, Garcia-Molina H. The eigentrust algorithm for reputation management in p2p networks[C]/Proceedings of the 12th international conference on World Wide Web. ACM, 2003: 640-651.
[6] Zheng Y, Li X, Wang M, et al. Flexible Data Access Control Based on Trust and Reputation in Cloud Computing[J]. IEEE Transactions on Cloud Computing, 2017, (99):1-1.
[7] Teacy W T L, Luck M, Rogers A, et al. An efficient and versatile approach to trust and Reputation using hierarchical Bayesian modelling[J]. Artificial Intelligence, 2017, 193(6):149-185.
[8] Zhu J. Wireless Sensor Network Technology Based on Security Trust Evaluation Model[J]. International Journal of Online Engineering (iJOE), 2018, 14(4): 211.
[9] Bao F, Chen I R. Trust management for the internet of things and its application to service composition[C]/ 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. Piscataway, NJ, USA: IEEE Press, 2012: 1-6.
[10] Chen I R, Bao F, Guo J. Trust-based service management for social internet of things systems[C]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(6):
[11] Sun Y L, Yu W, Han Z, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):305-317.
[12] Ren Y, Zadorozhny V I, Oleshchuk V A, et al. A Novel Approach to Trust Management in Unattended Wireless Sensor Networks[J]. IEEE Transactions on Mobile Computing, 2014, 13(7):1409-1423.
[13] You J, Shanggan J, Zhuang L, et al. An Autonomous Dynamic Trust Management System with Uncertainty Analysis[J]. Knowledge-Based Systems, 2018, 161(DEC.1):101-110.