Dynamic Trust Evaluation Model for Zero-trust Network of Power Monitoring System

Zhuo Lv[1], Cen Chen[1], Nuannuan Li[1], Zheng Zhang[1], Jianhui Zhang[2]

[1]State Grid Henan Electric Power Company Electric Power Research Institute, Zhengzhou, 450000, China

[2]SongshanLab, North Longhu Intelligent Industry Innovation Base, Zhongyuan Science and Technology City, Zhengdong New District, Zhengzhou City, Zhengzhou, 450000, China

Keywords: zero trust; dynamic authorization; trust evaluation; dynamic evaluation; beta distribution

Abstract: Dynamic trust evaluation is the key technology of dynamic authorization in zero-trust network of power monitoring system. However, the existing methods rarely consider the characteristics of zero trust network and services, or cannot adapt to large-scale network. In this paper, we abstracts various characteristics into inference rule sets, propose a dynamic trust evaluation model based on Beta distribution, and propose a time-related trust threshold calculation method, which can well serve the dynamic access control authorization depending on real-time trust level of entities. Simulation results show that the model can accurately evaluate the trust of entity and effectively detect malicious entities.

1. Introduction

With the continuous application and integration of new technologies such as the Internet of Things, big data, cloud computing and mobile network into the power system, the network boundary is becoming increasingly blurred, and the traditional protection system based on boundary defense is gradually unable to meet the security requirements of the power business[1], and a new network security architecture is urgently needed. At the same time, the static trust mechanism based on CA has been difficult to adapt to the dynamics and uncertainty of its terminal and service environment, so it is necessary to study the dynamic evaluation method of trust to adapt to the diversified entities and service resources in power monitoring system network.

Zero-trust security[2-4] has been widely concerned and researched due to its concept of "Never Trust, Always Verify", which is regarded as a new network security architecture that breaks through the traditional border defense thought. The goal of zero-trust security is to conduct continuous authentication of network entities and dynamic authorization after trust evaluation. In addition, network location/user attributes are not solely used as the sole basis for trust evaluation, but dynamic trust evaluation is carried out by combining information resources from multiple sources and multiple reserved discrimination mechanisms[5-6]. At present, scholars have explored the application of zero-trust security in power system network[7-9]. Literature [7] points out that the access of massive terminals in the current power Internet of Things greatly increases its network attack surface, and proposes to build a zero-trust network on the edgeside and combat the threat of compromised terminals through dynamic trust evaluation based on multi-source data. Considering the huge architecture of the Internet of Things, literature [8] proposes a zero-trust hierarchical mining process to verify systems and transactions at different trust levels to improve efficiency. Literature [9] investigates the application schemes of zero-trust power IoT based on continuous identity authentication and dynamic access control for various business service scenarios.

The key technology of trust engine is trust evaluation modeling. The existing trust evaluation work is mainly devoted to the research of strategy-based trust and reputation-based trust models, and few trust evaluation models combining the characteristics of zero-trust network and business

  DOI: 10.25236/icmmct.2024.030

service appeared. Literature [10] proposed a model based on the trust factor and Beta distribution hypothesis of expert recommendation to improve the accuracy of trust management, but such factors tend to cause the evaluation results to be too subjective and insufficiently accurate. Literature [11-13] proposed a trust evaluation method based on Beta distribution, and analyzed in detail the validity of Beta distribution fitting trust. Literature [14] proposed a node credit evaluation method based on blockchain consensus mechanism, which can effectively evaluate the credit of nodes in microgrid transactions. Literature [15] proposed a wireless network node trust mechanism based on fuzzy theory, and showed that it can effectively resist attacks from malicious nodes, while this method is suitable for resource-limited wireless system, and not for power system with complex network and frequent communication.

To this end, we studies the problem of dynamic trust evaluation for zero-trust network of power monitoring system. Our contributions include defining trust Spaces based on entity sets, time and inference rule sets, proposing a dynamic trust evaluation model based on Beta distribution and information entropy, and a method to calculate trust thresholds for the application of evaluation results in real-time dynamic authorization.

2. Dynamic trust evaluation

2.1 Trust space

In this model, the trust space Ω is defined as the probability space on the continuous real-valued interval[0,1].Since there are generally three roles in power system zero-trust network: terminal or user, zero-trust gateway, and service provider, we define the entity set E as the union of the business service set S and the terminal-user set C, i.e. $E=S\cup C$; the trust engine G of the zero-trust gateway acts as an observational computational node to evaluate the trust of the element of E, and makes binary judgments of events as normal and abnormal based on the set of inference rules *Contex*. Drawing on literature [16], we describe the trust relationship as a time-dependent function:

$$T : E \times E \times Contex \times t \to \Omega ;$$

Since literature [17] has verified that Beta distribution can fit the trust distribution well, we assumes T to obey the Beta distribution parameterized by α and β. In this way, the entity dynamic trust is regarded as a random variable that changes with time, and the quantitative evaluation problem is transformed into the estimation problem of probability value at a certain time, and the Bayesian method is adopted to solve it, and the lack of dynamic change in such trust evaluation methods can be overcome.

2.2 Inference rule set

The inference rule set is a refinement of the trust engine's trust factors affecting the set of entities, which is also referred to as context in the literature [16]. For example, whether the source IP of the access is correct, whether the geographic location of the device remains the same, etc. In the zero-trust network of power monitoring system, these trust factors include security authentication results based on cryptography, network agents that describe the immediate state of entity authorization[2], real-time state of terminal operation (such as security baseline, vulnerability scanning results, etc.), business traffic format and communication rules. In this way, the trust engine approximates the trust itself more realistically through the rich entity context, and the judgment of normal and abnormal historical interaction behaviors will be more stringent, thus estimating the trust value more accurately.

With the collected multi-source data the trust engine determines whether an entity is experiencing an abnormal event or not based rules on the inference rule set, and calculates the number of normal and abnormal events about a particular entity as an estimate of the parameters α and β.

2.3 Trust calculation method

2.3.1 Comprehensive trust calculation

The comprehensive trust of entity in this method is the comprehensive calculation result of its direct trust and indirect trust. We assumes that the trust engine performs evaluation on a time cycle ΔT, and denote the collected historical interaction dataset during interval $[n\cdot\Delta T,t]$ ($(n+1)\cdot\Delta T \le t < (n+k)\cdot\Delta T$), integer $n \ge 0$, integer $k > 1$) as INF_t .

(1)Direct trust

In general, it is intuitively obvious that direct trust between entities accumulates over historical interactions. At time t, the trust engine utilizes the rule set *Contex* to verify security events regarding interactions between entities η and ζ in the dataset INF_t , and calculates the number of normal interactions $s^t_{\eta,\zeta}$ and the number of abnormal interactions $f^t_{\eta,\zeta}$. The estimation formula for the direct trust of entity η to ζ at time t is

$$D^t_{\eta,\zeta} = \begin{cases} E(Beta(s^t_{\eta,\zeta}+1, f^t_{\eta,\zeta}+1)) = \dfrac{s^t_{\eta,\zeta}+1}{s^t_{\eta,\zeta}+f^t_{\eta,\zeta}+2} & \eta \neq \zeta \\ 0 & \eta = \zeta \end{cases}$$

In addition, entities that have not communicated for a long period of time should be considered less trustworthy. Therefore, we introduces the time decay factor, and the estimation formula of the direct trust degree of entity η to ζ at time t becomes:

$$D^t_{\eta,\zeta} = \begin{cases} \dfrac{s^t_{\eta,\zeta}+1}{s^t_{\eta,\zeta}+f^t_{\eta,\zeta}+2} & \eta \neq \zeta, s^t_{\eta,\zeta}+f^t_{\eta,\zeta} > 0 \\ \dfrac{s^t_{\eta,\zeta}+1}{s^t_{\eta,\zeta}+f^t_{\eta,\zeta}+2\cdot\frac{t-l\cdot\Delta T}{\Delta T}} = \dfrac{\Delta T}{2\cdot(t-l\cdot\Delta T)} & \eta \neq \zeta, s^t_{\eta,\zeta}+f^t_{\eta,\zeta} = 0 \\ 0 & \eta = \zeta \end{cases}$$

where $l\cdot\Delta T$ ($0 \le l < n$) is the starting point of theevaluation period in which the last communication occurred.

(2)Indirect trust

The indirect trust of entity η to ζ represents the trust assessment of other entities in the system on the interaction behavior of ζ, and its estimated value can be expressed as the weighted average of the direct trust of other entities to ζ. The indirect trust of entity a to ζ is expressed as the weighted average of the direct trust of other entities to ζ. At moment t, the indirect trust of entity η to ζ is estimated by the formula:

$$I^t_{\eta,\zeta} = \sum_{x \in E-\{\eta,\zeta\}} w^x_{\eta,\zeta} \cdot D^t_{x,\zeta}$$

where $w^x_{\eta,\zeta}$ is the weight of the contribution of entity x in the system in the indirect trust from η to ζ , as calculated in Section 2.3.2.

(3)Comprehensive trust

At time t, after the direct trust $D^t_{\eta,\zeta}$ and indirect trust $I^t_{\eta,\zeta}$ of entity η to ζ are calculated, we can calculate the comprehensive trust $T^t_{\eta,\zeta}$ of entity η to ζ using weighted summation by the following formula:

$$T^t_{\eta,\zeta} = w_D \cdot D^t_{\eta,\zeta} + w_I \cdot I^t_{\eta,\zeta}$$

Where w_D and w_I are the contribution weights of direct and indirect trust in the comprehensive trust, respectively, as calculated in Section 2.3.2. In particular, the comprehensive trust of an entity is initialized to 0.5 after endpoint security governance when it registers into the zero-trust network.

2.3.2 Entropy method for weight calculation

In order to determine the weights as objectively as possible, we draw on the entropy method in paper [18], and treat $I^t_{x,\zeta}, I^t_{\eta,\zeta}$ and $D^t_{\eta,\zeta}$ as random variables to calculate their weights. In the indirect trust degree estimation formula of entity η to ζ , for any other entity x in E-$\{\eta,\zeta\}$,

according to the entropy value calculation formula, the entropy value $I^t_{x,\zeta}$ is:

$$H\left(I^t_{x,\zeta}\right) = -D^t_{x,\zeta}\log_2^{D^t_{x,\zeta}} - (1-D^t_{x,\zeta})\log_2^{(1-D^t_{x,\zeta})}$$

After normalization, the weight $w^x_{\eta,\zeta}$ of $I^t_{x,\zeta}$ is:

$$w^x_{\eta,\zeta} = \left[1-\frac{H\left(I^t_{x,\zeta}\right)}{\log_2^{D^t_{x,\zeta}}}\right] \Bigg/ \sum_{x\in E-\{\eta,\zeta\}}\left(1-\frac{H\left(I^t_{x,\zeta}\right)}{\log_2^{D^t_{x,\zeta}}}\right)$$

Similarly, the corresponding weights of $D^t_{\eta,\zeta}$ and $I^t_{\eta,\zeta}$ are:

$$w_D = \left[1-\frac{H\left(D^t_{\eta,\zeta}\right)}{\log_2^{D^t_{\eta,\zeta}}}\right] \Bigg/ \left[\left(1-\frac{H\left(D^t_{\eta,\zeta}\right)}{\log_2^{D^t_{\eta,\zeta}}}\right)+\left(1-\frac{H\left(I^t_{\eta,\zeta}\right)}{\log_2^{I^t_{\eta,\zeta}}}\right)\right] \quad w_I = \left[1-\frac{H\left(I^t_{\eta,\zeta}\right)}{\log_2^{I^t_{\eta,\zeta}}}\right] \Bigg/ \left[\left(1-\frac{H\left(D^t_{\eta,\zeta}\right)}{\log_2^{D^t_{\eta,\zeta}}}\right)+\left(1-\frac{H\left(I^t_{\eta,\zeta}\right)}{\log_2^{I^t_{\eta,\zeta}}}\right)\right]$$

2.4 Model Application

2.4.1 Terminal-User Trust Evaluation

The trust of terminal-user entity is a very important basis when it accesses to many service entities in the zero-trust network of power monitoring system. According to the above, the comprehensive trust of such a terminal-user entity is determined by a particular service entity. For the convenience of application, we hope to build a unified terminal-user entity comprehensive trust that can be used by multiple service entities, and denote such a trust of terminal-user entity ζ at time t as T^t_ζ.

For those service entities have a high level of security and are well protected in power monitoring system, we reasonably assume that thy are honest and trustworthy. Therefore, T^t_ζ can be measured using the comprehensive trust of those service entities that communicate with ζ.

The trust T^t_ζ of terminal-user entity ζ at time t is defined as the mean value:

$$T^t_\zeta = \sum_{\eta\in S, s^t_{\eta,\zeta}+f^t_{\eta,\zeta}\neq 0} Trust^t_{\eta,\zeta} \Bigg/ \sum_{\eta\in S, s^t_{\eta,\zeta}+f^t_{\eta,\zeta}\neq 0} 1$$

2.4.2 Method of calculating trust threshold

The zero-trust gateway determines whether the authenticated terminal-user entity is dynamically authorized to access it by comparing the comprehensive trust of this entity with a certain pre-set trust threshold. Usually this threshold is assessed by experts, but this method is subjective and difficult to accurately measure the overall trust status of the current system, especially in a large and complex system such as power monitoring system. Denotes the average of normal interactions between all entities in set S and all entities in set C at time t (excluding all the pairs of entities that do not interact with each other) as $\bar{s}_t$, and the average of unnormal interactions as $\bar{f}_t$,.We computes the average direct trust $\overline{D_t}$ of the system at the current moment based on the formula for calculating direct trust:

$$\overline{D_t} = E(Beta(\bar{s}_t+1, \bar{f}_t+1)) = \frac{\bar{s}_t+1}{\bar{s}_t+\bar{f}_t+2}$$

$$\bar{s}_t = \sum_{\substack{\langle\eta,\zeta\rangle\in S\times C \\ s^t_{\eta,\zeta}+f^t_{\eta,\zeta}\neq 0}} s^t_{\eta,\zeta} \Bigg/ \sum_{\substack{\langle\eta,\zeta\rangle\in S\times C \\ s^t_{\eta,\zeta}+f^t_{\eta,\zeta}\neq 0}} 1 \qquad \bar{f}_t = \sum_{\substack{\langle\eta,\zeta\rangle\in S\times C \\ s^t_{\eta,\zeta}+f^t_{\eta,\zeta}\neq 0}} f^t_{\eta,\zeta} \Bigg/ \sum_{\substack{\langle\eta,\zeta\rangle\in S\times C \\ s^t_{\eta,\zeta}+f^t_{\eta,\zeta}\neq 0}} 1$$

Considering the actual production environment requirements and security strength requirements, a repeatable configurable security strength factor F_s in [0,1] is manually defined, which in turn gives a method for calculating the dynamic trust threshold $Threshold_t$, which is calculated as follows:

$$Threshold_t = \max(F_s, \overline{D_t})$$

Further considering the terminal-user entity variability and trust threshold application flexibility, it is also possible to manually define multiple types of security strength factors by entity type, and similarly define a dynamic trust threshold for a certain type of entity as described above.

3. Simulation Experiment

3.1 Simulation Experiment Environment

The simulation environment consists of a server A, four terminals B, C, D and E, and a zero-trust gateway; A is protected by the zero-trust gateway and accepts access from terminals B and E; BC, BD, BE, CD and DE communicate with each other through the zero-trust gateway.

After collecting the experimental interaction data, we use MATLAB R2020b as a simulation tool for analysis to verify the rationality and effectiveness of the above evaluation methods.

3.2 Analysis of simulation results

1) The accumulative effect of trust

We simulated node D in three states: randomly honest, completely honest and dishonest. The experimental results show that (Fig.1): the overall trend of trust is gradually accumulated with time; when a node is completely honest, its comprehensive trust increases gradually; when it is dishonest, its comprehensive trust decreases gradually; when it is sometimes honest and sometimes dishonest, its comprehensive trust fluctuates sharply over time.

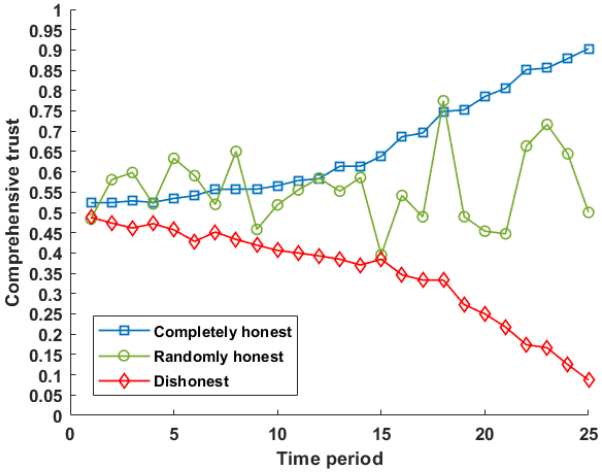

Fig.1 Accumulative effect of trust

2) Detect malicious nodes in the system

We simulated entity E attacking entity B in time period 10-19 and calculated the comprehensive trust of entity A to Entity B. The experimental results show (FIG.2) that the comprehensive trust of A to B began to decrease significantly in these periods, and it rebounded significantly after the attack. Therefore, our trust evaluation method can effectively detect the malicious nodes in the system.

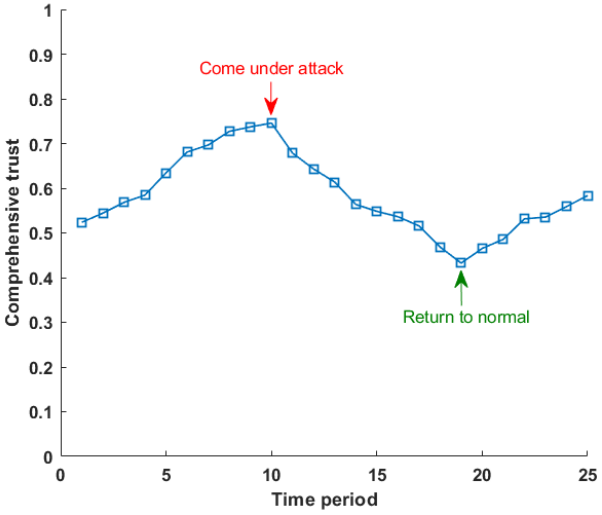

Fig.2 Change of the trust of node under attack

3) Validity of the method of calculating trust threshold

We simulated node E attacking service entity A and calculated the four comprehensive trust of A to B, C, D and E, also calculated the trust threshold using our method in section 2.4.2. The experimental results show that (Fig.3) the comprehensive trust of A to E is significantly lower than the trust threshold, and the trust engine can judge that entity E is abnormal, and it should be removed from the list of registered nodes.

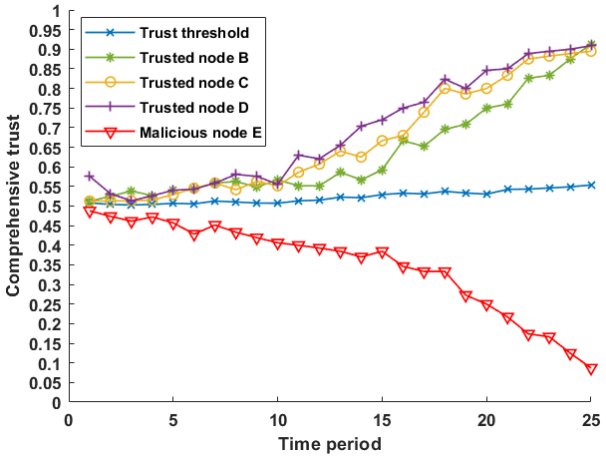

Fig.3 Comparison of comprehensive trust and trust threshold

4. Conclusion

We discuss the problem of trust dynamic assessment for zero-trust security in power monitoring systems. On the basis of defining trust relationship with entity set, inference rule set and time as parameters, and based on the assumption that the trust relationship obeys the Beta distribution, we propose a parameterized model of the normal and abnormal times of the historical interaction behaviors between entities, use the entropy method to compute the weights of the direct trust and the indirect trust, and then obtain the comprehensive trust by weighted summation. Aiming at the threshold selection problem of zero-trust dynamic authorization automation, a threshold calculation method parameterized by the average number of normal and abnormal interactions between entities in history is proposed on the basis of the dynamic trust evaluation formula. The simulation results show that our dynamic trust evaluation model can well reflect the temporal correlation and accumulation of dynamic trust, and can effectively detect node anomalies in the system.

References

[1] WU Kehe, CHENG Rui, JIANG Xiaochen, et al. Security Protection Scheme of Power IoT Based on SDP[J]. Netinfo Security, 2022, 22(2): 32-38.

[2] Evan Gilman and Doug Barth. 2017. Zero Trust Networks: Building Secure Systems in Untrusted Networks (1st. ed.)[M]. O'Reilly Media, Inc.

[3] Rose S, Borchert O, Mitchell S, et al. Zero trust architecture[R]. National Institute of Standards and Technology, 2020.

[4] Sateesh H, Zavarsky P. State-of-the-Art VANET trust models: challenges and recommendations[C]//2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2020: 0757-0764.

[5] Dimitrakos, T., Dilshener, T., Kravtsov, A., et al. Trust aware continuous authorization for Zero Trust in consumer internet of things[C]//2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, Nov 10-13,2020,Guangzhou, China:1801-1812.

[6] Papakonstantinou N, Van Bossuyt D L, Linnosmaa J, et al. A Zero Trust Hybrid Security and

Safety Risk Analysis Method[J]. Journal of Computing and Information Science in Engineering, 2021, 21(5).

[7] Feng Jingyu, Yu Tingting, Wang Ziying, Zhang Wenbo, Han Gang, Huang Wenhua. An Edge Zero-Trust Model Against Compromised Terminals Threats in Power IoT Environments[J]. Journal of Computer Research and Development, 2022, 59(5): 1120-1132. DOI: 10.7544/issn1000-1239.20211129

[8] Mayra Samaniego,Ralph Deters.Zero-Trust Hierarchical Management in IoT[C]//2018 IEEE International Congress on Internet of Things.JULY 2-7, 2018, SAN FRANCISCO, CA, USA:88-95.

[9] Zhang Xiaojian,Chen Liandong,Fan Jie,et al.Power IoT security protection architecture based on zero trust framework[C]//2021 IEEE 5th International Conference on Cryptography, Security and Privacy.January 08-10, 2021,Zhuhai, China:166-170.

[10] Fang W D, Zhang W X, Yang Y, et al. A resilient trust management scheme for defending a gainst reputation time-varying attacks based on BETA distribution[J]. Science China Information Sciences, 2017, 60(4): 040305:1-11.

[11]Yu Jiexiao,Yu Liying,Yang Ting.Blockchain basedtrust consensus method for powe rInternet of things terminal[J].Automation of Electric Power Systems,2021,45(17):1-10.

[12] Weidong Fang,Chuanlei Zhang,Zhidong Shi,et al.BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks[J].Journal of Network and Computer Applications, 59 (2016) 88–94.

[13] Zhao Guosheng, Wang Tiantian, Wang Jian.A Dynamic Trust Evaluation Model For Edge Devices [J]. Computer Engineering and Science, 2021, 43(09): 1574-1583.

[14] QIN Jinlei,SUN Wenqiang,LI Zheng,et al.Credit Consensus Mechanism for Microgrid Blockchain[J]. Automation of Electric Power Systems,2020,44(15):10-18.

[15] Chen Haibiao, Huang Shengyong, Cai Jierui.Trust Evaluation Protocol For Cross-layer Routing Based On Smart Grid[J]. Computer Science, 2021, 48(6A): 491-497.

[16] Feng Y, Ying W. A reputation-based dynamic trust model for large scale distributed environment. Journal of Computational Information Systems. 2013;9(3):1209-1215.

[17] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2008, 4(3): 1-37.

[18] Che S, Feng R, Liang X, et al. A lightweight trust management based on Bayesian and Entropy for wireless sensor networks[J]. Security and Communication Networks,2015, 8(2): 168-175.