Hindawi
Scientific Programming
Volume 2020, Article ID 8895804, 6 pages
https://doi.org/10.1155/2020/8895804

Research Article

Continuous Trust Evaluation of Power Equipment and Users Based on Risk Measurement

Congcong Shi,[1,2,3] **Jiaxuan Fei**,[2,3] **Xiaojian Zhang**,[2,3] **Qigui Yao**,[2,3] **and Jie Fan**[2,3]

[1]*State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210003, China*
[2]*Global Energy Interconnection Research Institute Co. Ltd., Nanjing 210003, China*
[3]*State Grid Key Laboratory of Information & Network Security, Nanjing 210003, China*

Correspondence should be addressed to Congcong Shi; 765734893@qq.com

Received 22 July 2020; Revised 10 November 2020; Accepted 28 November 2020; Published 11 December 2020

Academic Editor: Ting Yang

In power Internet of Things environment, the existing border-based protection system and the "one-time authentication, one-time authorization, and long-term effective" approach are difficult to deal with the threat of attacks from internal and external devices and users with legal authority. In order to solve the problem of authorized access of power equipment and users, combined with behavior risk assessment, a continuous trust evaluation scheme of power equipment and users is presented in this paper. The scheme is evaluated by the combination of direct trust, indirect trust, and comprehensive trust and adds the penalty reward factor and time attenuation function to improve the reliability of the results. In addition, this paper will quantify the risk of the behavior of power equipment and users and regard it as a factor affecting the degree of trust, so as to achieve continuous trust evaluation of equipment and users.

1. Introduction

1.1. Background. The Internet of Things technology mainly relies on related sensing equipment to connect objects to the network according to an agreed protocol. In the power system, the use of the Internet of Things technology can better control power equipments, power personnel, and the operating environment, specifically in the four aspects of perception, identification, interconnection, and control. Through the power Internet of Things technology, the operating efficiency of the power system can be greatly improved. For example, smart meters can upload user-side data to the power grid company through the network to avoid manual copying of the wrong meters. By connecting the power station to the power system, the power Internet of Things can be used to achieve dispatch control.

In the power Internet of things environment, with the extensive access of massive terminal equipment and users, the network exposure increases, which brings severe challenges to the existing protection system. However, the existing authentication and access control for IoT terminal equipment and users mostly adopts the method of "once authentication, once authorization, and long-term effectiveness." After the authentication is passed, it has legal authority for a long time and can carry out any operation within the scope of authority. Due to the lack of continuous behavior analysis and authentication and access control measures, it is impossible to solve the problem that legitimate terminal devices or users are illegally controlled by attackers and access company data and business resources in a legal capacity. At the same time, for the insiders, due to the preset trust mechanism for the insiders if the insiders carry out illegal operations or launch malicious attacks, it is difficult to effectively control and will cause huge losses.

It is difficult to meet such security requirements only by relying on the traditional security architecture based on border protection. The core idea of the zero-trust architecture is that no person, device, or system inside and outside the network should be trusted by default, and the trust basis of access control should be reconstructed based on authentication and authorization. It means a never trust and always authenticate security model. In the zero-trust

architecture mode, it can well solve the problem of internal personnel violations or malicious attacks and provide guarantee for the realization of power Internet of things "any time, any place, any person, and any thing" information connection and secure interaction [1].

Zero-trust architecture needs to study continuous identity authentication and trust evaluation, through real-time evaluation of the trust of devices and users, adjust the authority level of users, and achieve accurate management and control. In order to understand the problem of trust evaluation calculation, this paper proposes a power Internet of things equipment and user trust evaluation scheme based on risk measurement. The general trust calculation does not take into account the impact of behavioral risk factors on trust. In this paper, the behavior risk value is added to the trust degree calculation, and it is calculated as a part of the trust degree calculation by quantifying the behavior risk value of power equipment and users. In addition, when calculating the trust degree, the dynamic adaptability of the calculation and the ability of the system to resist malicious attacks are enhanced by dividing the trust degree into direct trust degree and indirect trust degree and obtaining a comprehensive trust degree.

2. Zero-Trust Model

Zero-trust architecture is an end-to-end approach to network/data security [2]. Zero trust is an architectural approach that focuses on data protection. Its focus is to restrict access to resources to those who "need to know." The traditional security architecture focuses on border defense, and authorized users can freely access resources. There is nothing this model can do about attacks from within the network. The zero-trust protection architecture is intended to eliminate unauthorized access to data and services and to make the implementation of access control as detailed as possible [3]. To reduce uncertainty (because they cannot be completely eliminated), the focus is on authentication, authorization, and narrowing the implicit trust zone, while minimizing time delays in network authentication mechanisms. Access rules are limited to minimum permissions and are as detailed as possible. A common zero-trust architecture model is shown in Figure 1.

The key components include

(1) Policy engine (PE): this component is responsible for the final decision on whether to grant the specified access subject access to the resource (access object). It gives the data to the trust engine to calculate the trust value.

(2) Policy administrator (PA): this component is responsible for establishing a connection between the client and the resource (a logical responsibility, not a physical connection). It generates any authentication tokens or credentials that the client uses to access enterprise resources. It is closely related to the policy engine and depends on its decision to eventually allow or deny the connection.

(3) Policy enforcement point (PEP): this system is responsible for enabling, monitoring, and ultimately terminating the connection between principals and enterprise resources.

The policy engine is the core of the zero-trust architecture, which decides whether to grant access to resources according to the output of the trust algorithm. The policy engine uses external information, such as IP blacklists and threat intelligence services, as input to the trust algorithm to decide whether to grant or deny access to the resource. The policy engine is paired with the policy administrator component. The policy engine makes (and records) decisions, and the policy manager executes the decisions (approve or reject). The use of appropriate trust algorithm plays a vital role in the security protection of the whole system. In the next section of this paper, we will discuss in detail the algorithm used by the trust engine when deploying the zero-trust architecture in the power IoT system.

3. Trust Evaluation Model

Eigen Trust model [4] is a trust-based access control model, which gives more weight to users with high degree of direct trust in the process of trust calculation and believes that users with greater degree of direct trust are more trustworthy. However, this method does not take into account the subjectivity and uncertainty of trust. The penalty factor is added in Claudiu's Model [5], which improves the dynamic adaptability of the model, which enhances the antiattack ability to some extent, but the model does not take into account the historical value, which will lead to the misoperation as an attack and lead to access failure.

Through the analysis and research of the above typical trust models, this paper fully considers the trust degree of historical interaction records in the process of trust calculation, and records are used to update trust after each interaction is completed, which is conducive to a virtuous circle of trust. Maintain a cloud environment with good services. The results are fed back in real time, which are used to update the trust degree. In addition, this paper also adds risk factors to the calculation of trust degree, which makes the calculation of trust degree more prepared and in line with the reality.

The trust evaluation model used in this article is shown in Figure 2.

The trust engine acquires the relevant information of the access device or user transmitted by the policy engine, such as the resource requested, the IP address of the access device, and the identity information of the user. This information is first used to calculate the initial trust degree. The initial trust

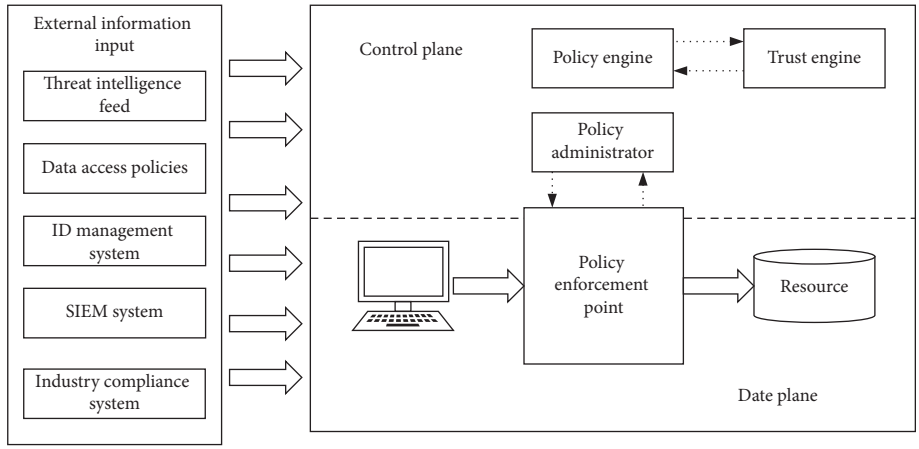

Figure 1: Zero-trust model.

degree is composed of direct trust degree and indirect trust degree. After the initial trust calculation is completed, the trust engine will evaluate the risk of this behavior and get a risk value, which will be used to calculate the new trust degree. Finally, the trust degree is fed back to the policy engine for subsequent access control.

3.1. Calculation of Direct Trust Degree. Direct trust degree (DT) is composed of direct experience (DE) and direct knowledge (DK) [6]. For the calculation of direct trust, there are the following formulas:

$$\begin{aligned} &\mathrm{DT} = \mu \mathrm{DE} + (1-\mu)\mathrm{DK}, \\ &\mathrm{DE} = \begin{cases} \min\left(\sum_{i=1}^{n} w_i \lambda_i, 1\right), \\ \max\left(\sum_{i=1}^{n} w_i \lambda_i, 0\right), \end{cases} \\ &w_i = \frac{2i}{n(n+1)}, \quad (i = 1, 2, 3, \ldots, n), \\ &\lambda_i = (e_i - 1)e^{-(1/f)} + e_i\left(\frac{n-f}{n}\right)^2, \\ &DK = \frac{n-f}{n + (sl-1)f}, \end{aligned} \tag{1}$$

where N is the number of interactive events in the recent interval, f is the number of failed interactions, λ_i is the penalty factor, which is used to adjust the trust value when the interaction fails, and sl is the service level factor.

3.2. Calculation of Indirect Trust Degree. The indirect trust degree is mainly calculated through the transitivity of trust. According to the number of recommended paths, indirect trust value can be divided into single-path recommendation and multipath recommendation. Obviously, multipath recommendation is more in line with the actual situation. However, it is obviously unreasonable to simply accumulate the trust values under multipath. According to the actual situation, the indirect trust degree can be calculated by applying different weights to different stages under multipath.

This paper introduces the basic model of dynamic reputation tree [7]. Through the dynamic reputation tree model, other individuals who have indirect trust relationship with the subject can be clearly constructed. At the same time, we can specify the weight of different levels according to the different levels of trust difference between the subject and the recommender. The general principle is that the closer to the subject, the greater the weight of the recommender. This kind of dynamic reputation tree can be maintained with less overhead, and the corresponding weights may be adjusted according to the importance of indirect trust individuals and subjects to achieve dynamic and convenient control.

The formula for calculating the indirect trust degree in the dynamic reputation tree is as follows:

$$IT(R_i, R_i) = \left\{ \sum_{k=1}^{n} \left(\omega(R_k) \times DT\left(R_k, R_j\right)\right) \times \frac{1}{\sum_{k=1}^{n} \omega(R_k)}, 0, \right. \tag{2}$$

where n is the number of indirect referrals and $\omega(R_k)$ is the weight factor of presenters, which can be changed according to different levels of referrals:

$$\omega(R_k) = \left\{ \prod_{n}^{l} \left(DT(R_m, R_n)\right), l > 0, 1, \; l = 0, \right. \tag{3}$$

where $\mathrm{DT}(R_m, R_n)$ represents the direct trust value of R_m to its successor node.

3.3. Calculation of Comprehensive Trust Degree. Previously, this paper has explained the calculation method of direct and indirect trust values, and the calculation of

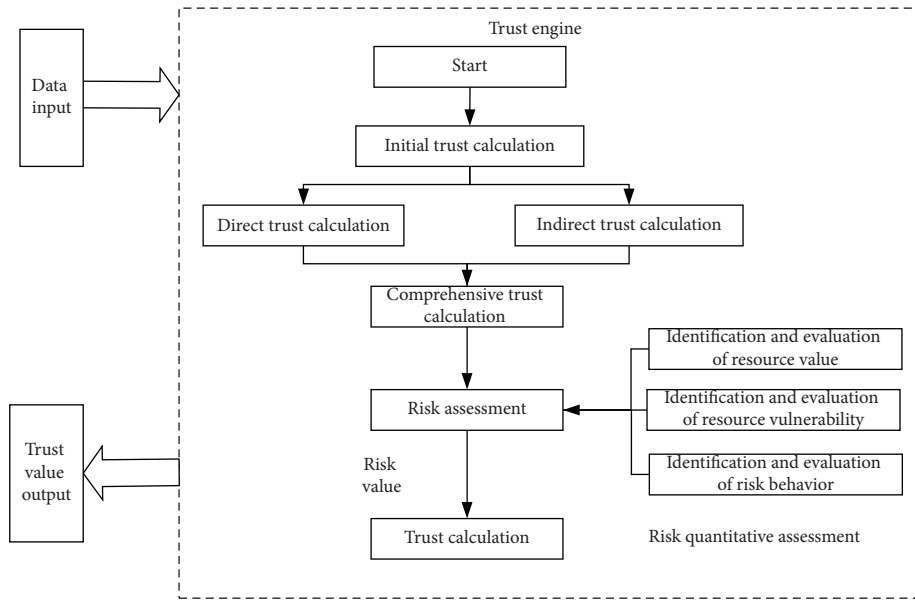

Figure 2: Trust computing model.

comprehensive trust value is based on the corresponding synthesis of the two values to get the user trust value at this time [8]. The specific calculation formula is as follows:

$$T(R_i, R_j) = \begin{cases} \mathrm{IT}(R_i, R_j), & n = 0, \\ \dfrac{1}{1+\beta(R_j)} \times \mathrm{DT}(R_i, R_j) & \\ + \dfrac{\beta(R_j)}{1+\beta(R_j)} \times \mathrm{IT}(R_i, R_j), & 0 < n < N, \\ \mathrm{DT}(R_i, R_j), & n \geq N, \end{cases} \tag{4}$$

where n is the total number of historical interactive records in the system and N is the largest total number of historical interactive records in the system. $\beta(R_j)$ is the weight of direct trust and indirect trust, and it is calculated as follows:

$$\beta(R_j) = \frac{1}{2} \times \left[\theta\left(L_{R_j}\right) + \theta(n_{all})\right], \tag{5}$$

where $\theta(x) = 1 - (1/(x+\alpha))$, $\theta(L_{R_j})$ is the number of trusted referrals, and $\theta(n_{\mathrm{all}})$ is the number of entities that have a direct trust relationship with R_j.

4. Risk Assessment Algorithm

The existing trust evaluation algorithms often use the weighted calculation method of direct trust degree and indirect trust degree [9], which will ignore the impact of user behavior risk on trust degree. This paper will quantify the user behavior risk and add it to the calculation of user trust to realize the trust evaluation of power Internet of things equipment and users based on risk measurement.

4.1. Analysis of Power Equipment and User Behavior. With the development of cloud computing, a large number of IoT devices put their services on the cloud server, which can reduce the pressure on the server and speed up the response time to a certain extent, but user behavior will also bring security risks. In this paper, the behavior of equipment terminals and users in the power things environment is divided into the following two categories:

(1) Abnormal behavior set:

The abnormal behavior set mainly refers to the fact that when the IoT terminal or user is accessing, some attributes are quite different from the usual attributes, such as landing location, accessed resources, and historical records. The details are shown in Table 1.

(2) Malicious behavior set is shown in Table 2.

5. Risk Analysis of Power Equipment and User Behavior

Combined with the definition of information security risk factors in the information security risk assessment specification, this paper defines the behavioral risk factors of IoT equipment and users in the power IoT environment as follows.

(1) Resource value (RV): the resources accessed by the equipment may be hardware resources, such as a specific watt-hour meter, or software resources, such as some data. The resource value of different levels is different. In this paper, the resource values are divided into $R = \{RV_1, RV_2, RV_3, RV_4\}$; they represent unimportant, general, important, and extremely important, respectively.

Table 1: Abnormal behavior set.

Behavior content
Location
IP address
Type of resources
Number of resources used

Table 2: Malicious behavior set.

Behavior content
SQL injection
Port scan
IP deception
Distributed deny attack
SYN flooding attack
Replay attack
Network surveillance attack
Virus attack

(2) Resource vulnerability (V): resource vulnerability refers to the difficulty in which resources are vulnerable to attack. According to the difficulty of vulnerability, resources are divided into $V = \{V_1, V_2, V_3, V_4\}$; they represent easy, ordinary, difficult, and extremely difficult, respectively.

(3) Behavioral risk level (L): in this paper, the abnormal behavior and malicious behavior mentioned above are regarded as dangerous behavior, and the risk level of behavior is classified according to the influence degree of the behavior as $L = \{L_1, L_2, L_3, L_4\}$; they represent negligible, low, medium, and high levels of behavioral risk, respectively.

5.1. Calculation of Behavior Risk of Power Equipment and Users. Above, the behavioral risk factors of power equipment and users have been transformed into resource value R, resource vulnerability V, and behavioral risk grade L; then, the behavioral risk assessment equation $R = RV \times V \times L$ can be obtained.

In order to participate in the calculation of trust degree later, you need to map the value at risk to the interval $[0, 1]$. The transformation formula is as follows:

$$R = \frac{\sqrt{RV \times V \times L}}{RV + V + L}. \tag{6}$$

The above formula can only statically reflect the risk level of a certain visit of the device and the user. After this, this paper introduces the dangerous behavior times c; when the user carries on the dangerous operation continuously, the risk value should increase exponentially. In addition, the risk attenuation factor α is introduced, and the final behavioral risk assessment formula is as follows:

$$R = \begin{cases} \alpha \times R_0, & \text{(a)} \\ R_0 + \mu \times \dfrac{c \times \sqrt{RV \times V \times L}}{RV + V + L}. & \text{(b)} \end{cases} \tag{7}$$

In the above formula, R_0 represents the result of the most recent behavior risk calculation. When (a) represents normal behavior, the calculation of user risk value $\alpha \in [0.5, 1]$ is used to adjust the attenuation rate of user risk value. When the user behaves normally continuously, the risk value of the user attenuates. (b) represents the process of calculating the value at risk when the user has dangerous behavior, and $\mu \in [1, 2]$ is used to adjust the value at risk.

5.2. Calculation of Trust Degree of Power Equipment and Users. In this paper, based on the improved information security risk assessment equation and the Trust Model based on Behavior Risk Evolution (TMBRE), the dangerous behavior times c is introduced, and the improved calculation formula of user trust degree is obtained:

$$T = \begin{cases} \lambda^c \times T_0 + (1 - \lambda)^c \times (R - \theta), \; R \in [\theta, 10], & \text{(a)} \\ T_0 + \rho^c \times (\theta - R), \; R \in [0, \theta]. & \text{(b)} \end{cases} \tag{8}$$

In the above formula, θ is the threshold constant of the risk value of power equipment and user behavior. Exceeding this value means high-risk behavior. T_0 represents the user trust level that was last calculated. λ is the trust correction factor under a high-risk value, and ρ is the trust correction factor at a low-risk value. (a) is used to calculate the trust degree of power equipment and user behavior in a high-risk state. (b) is used to calculate the trust degree of power equipment and user behavior in a low-risk state.

6. Conclusion

In order to deal with the current power Internet of Things system that is difficult to deal with attacks from internal and external devices and users with legal authority, it is necessary to study continuous identity authentication, trust evaluation, and access control technologies and establish a zero-trust access control model. In this paper, a continuous trust evaluation algorithm for power IoT equipment and users based on risk measurement is

proposed, which can be used to calculate the trust degree of zero-trust architecture. Based on the analysis of the characteristics of trust, in order to enhance the dynamic adaptability and objectivity of the trust value calculation method, this paper presents a trust value calculation method with penalty factor, service level factor, and dynamic adaptation factor. In addition, this paper also adds risk factors to the calculation of trust degree, through the analysis of user behavior, quantifies the user risk behavior, and adds the number of dangerous behavior in the risk calculation; for continuous dangerous behavior, the malicious coefficient will increase exponentially.

Data Availability

The experimental data in this paper come from the actual production and operation process of the State Grid Corporation of China and are only provided on the company's internal network.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Science and Technology Project of State Grid Corporation of China (Grant no. 5700-201958466A-0-0-00): "End-to-End Security Threat Analysis and Accurate Protection of Ubiquitous Power Internet of Things."

References

[1] R. Vanickis, P. Jacob, S. Dehghanzadeh et al., "Access control policy enforcement for zero-trust-networking," in *Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC)*, Belfast, UK, June 2018.

[2] E. Bogner, "The zero-trust mandate: never trust, continually verify," *Software World*, vol. 50, no. 4, pp. 9-10, 2019.

[3] A. Ghafourifar and J. K. Monroe, "Multi-party authentication in a zero-trust distributed system," US Patent 10,110,585, 2018.

[4] D. K. Sepandar, T. S. Mario, and G. M. Hector, "The Eigen Trust algorithm for reputation management in P2P networks," in *Proceedings of the 12th International Conference on World Wide Web*, pp. 640–651, ACM Press, Budapest, Hungary, May 2003.

[5] L. P. Kaelbling, M. L. Littman, and A. W. Moore, "Reinforcement learning: a survey," *Journal of Artificial Intelligence Research*, vol. 4, no. 1, pp. 237–285, 1996.

[6] X. Hu, R. Jiang, M. Shi et al., "A privacy protection model for health care big data based on trust evaluation access control in cloud service environment," *Journal of Intelligent and Fuzzy Systems*, vol. 5, pp. 1–12, 2020.

[7] T. Wang, H. Luo, W. Jia et al., "MTES: an intelligent trust evaluation scheme in sensor-cloud-enabled industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054–2062, 2020.

[8] R. Zhang, X. Wu, S.-Y. Zhou, and X.-S. Dong, "A trust model based on entity behavior risk assessment," *Journal of Computer Science*, vol. 32, no. 4, pp. 688–698, 2009.

[9] J. Chen, Z. Tian, X. Cui, L. Yin, and X. Wang, "Trust architecture and reputation evaluation for internet of things," *Journal of Ambient Intelligence & Humanized Computing*, vol. 10, pp. 3099–3107, 2019.