Research on information security interaction based on behavior trust measurement mechanism

Jian Gao*, *Huadong* Yu, *Hongmian* Wang, *Huifeng* Bai, *Chao* Huo, and *Ganghong* Zhang

Dept. of Terminal Communication, Beijing Smartchip Microelectronics Technology Co., Ltd, Beijing, China

Abstract. Along with the computer, communication, control, the rapid development of automation technology, based on the analysis of the information security requirements, combined with the trusted computing provide security solution, the communication control information security interaction model and the key technology to realize information security interaction, put forward a real-time evaluation model based on credible global terminal entities. By introducing penalty factor and time factor, the evaluation method is improved from single evaluation to global evaluation. Taking the user information collection system as an example, the information security communication model of behavior trust measurement mechanism is simulated. The simulation results show that this model has the ability of continuous trust measurement in dynamic uncertain network environment, and can accurately determine the trust of terminal entities in real time, and it is more realistic, which lays a good foundation for the research of trust connection, trust management and trust decision based on trust measurement.

Keywords: Information communication, Trust measurement, Security model, Dynamic control.

1 Introduction

Industrial Internet is the information technology, communication technology, computer technology and the original infrastructure highly integrated and formed a new network, with improving energy efficiency, reduce the impact on the environment, improve security and reliability, reduce loss and many other advantages. Intelligence is embodied in observability, controllability, distributed intelligence, advanced analysis, self-adaptability, self-healing and so on. The rapid advance in the industrial informatization related industrial robot application is more and more widely, due to the complex diversity of application scenarios and the scope of application of universality, make it easy to intelligent terminal by various types of security threats and attacks, such as denial of service attacks, such as wiretaps, illegal invasion, thus easy to cause the leakage of sensitive information and

* Corresponding author: gaoj6666@163.com

terminal by hackers control risk, Thus posing a threat to the normal operation of the whole production[1,2]. The secure interaction of information is the premise of the normal operation of the business system, and ensuring the secure interaction of information is an important subject of the construction of industrial Internet.

Traditional network security technologies mostly adopted static trust mechanism. However, in the actual network environment, the terminal platform environment and user behavior are often changing, which can eventually lead to false authorization and no longer adapt to the current dynamic and complex network environment[3-4].

On the basis of analyzing the requirements of data credibility and system reliability in industrial Internet, this paper proposes a reliability evaluation model of information data oriented to communication control, and a dynamic and hierarchical reliability evaluation method based on data source dependency.

2 Relevant definitions of trusted measurement

Trusted computing technology provided three basic functions: trusted measurement, trusted storage and trusted reporting. Among these three basic functions, trustworthiness measurement is the core of building a trusted operating environment [5].

Behavior trustworthiness: When two or more users interact with each other, they evaluate the user's behavior in the process of interaction.

Behavior evidence: Refers to the basic value that can be obtained directly through software and hardware detection to quantitatively evaluate the user's overall behavior.

Trust value: It is an evaluation of the trustworthiness of the subject to determine whether the subject has the trustworthiness characteristic it should have as a trustworthiness subject. It is expressed in T and $T \in [0,1]$. The greater the value, the higher the credibility.

Interaction success rate: It refers to the proportion of the number of successful interactions among users in the whole network. Interaction success rate index is used to measure the accuracy of trusted evaluation strategy in dynamic network environment. The success rate of interaction is higher, the trusted evaluation strategy is more accurate, and the dynamic adaptability is stronger.

3 Behavior trusted measurement evaluation model

A typical trusted measurement model system, as shown in Figure 1, usually consists of eight parts, three basic elements: subject, object and authority, two additional attributes used in usage control: subject attribute and object attribute, and three decision-making factors: authorization, responsibility and condition. It can be abstracted into a quintuple: M= (T, PA, PC, AA, AB), where:

T is a continuous set of system states;

PA is a set of authorization decision based on the attributes of subject and object;

PC is a set of condition determination based on system or running environment;

AA is a finite set of using control behavior;

AB is a limited set of responsible acts.

4 Trusted measurement computing

When there is direct context interaction between two data entities or when the similarity of data or behavior provided by two data entities exceeds a certain threshold, it is said that there is local credibility between data sources at this time. Trust (A-B, t) denotes the

comprehensive reliability of data entity A to target data entity B at time t, which is composed of local and remote credibility of data entity[6.7].

4.1 Local credibility

Local trustworthiness represents the trustworthiness of data entity A at time t. It is the comprehensive trustworthiness of all historical data provided by data sources and the recommended trustworthiness of data sources at all layers of the trusted network. The calculation formula is as follows:

$$T_1(A,t) = \begin{cases} Random()or0, t = 0 \\ T_1(A,t\text{-}1) \cdot \mu_s(t), \Delta t), \Delta C\ (A,t) = 0 \\ \left[\sum T(Data_A, t)/Sum(Data_A) + (\gamma_n \cdot Rec_n(A,t))\right] \cdot \lambda s(t) \end{cases} \tag{1}$$

The initial value is a random number or 0, indicating that data entity A has some or no trustworthiness.

μ s(t) is the time attenuation coefficient at time t.

$$\mu_s(t) = 1\text{-}t/(t\text{-}t_0) \tag{2}$$

When data source A has the same local credibility value at t Time and t-1 time, or has no context interaction, it is punished by time attenuation. Context (A, t) denotes whether data source A interacts directly with new contexts at time t. Where:

$$\Delta C\ (A,\ t) = Context\ (A,\ t) - Context\ (A,\ t\text{-}1) \tag{3}$$

λ S(t) denotes the penalty coefficient of the model for the credibility of data sources at time t. Among them:

$$\lambda s(t) = \begin{cases} 1, \Delta \mathrm{Trust}(\ \mathrm{A}\quad \mathrm{t}) \geq 0 \\ 0 \leq \mathrm{x} < 1, \Delta \mathrm{Trust}(\ \mathrm{A}\quad \mathrm{t}) < 0 \end{cases} \tag{4}$$

Among them, Δ Trust(A, t) denotes the difference of trust in data source A between t and t-1 at time t.

$$\Delta Trust\ (A,\ t) = Trust\ (A,\ t) - Trust\ (A,\ t\text{-}1) \tag{5}$$

4.2 Remote credibility

Let T_2 (A-B, t) denote the remote reliability of local data entity A to destination data entity B at time t. It is composed of the reliability of context interaction between data sources and the similarity between two data sources. The formula is as follows:

$$T_2(A\text{-}\mathrm{B},t) = \begin{cases} Random()or0, t = 0 \\ T_2(A\text{-}\mathrm{B},t\text{-}1) \cdot \mu_{\mathrm{L}}(t), \Delta \mathrm{C}_{txt}(A\text{-}\mathrm{B},t) = 0 \\ \left[\mathrm{T}_2(\mathrm{A}, B, C_{txt}(A,B,t)) + \mathrm{Acp}_n(A\text{-}\mathrm{B},t)\right] \cdot \lambda_{\mathrm{L}}(t) \end{cases} \tag{6}$$

Formula:

T_2 (A, B, Ctxt (A, B, t)) denotes the trustworthiness of data source A to data source B under interaction condition C_{txt} (A, B, t) at time t.

A_{cpn} (A-B, t) denotes the recognition of similarity between data source A and data source B at time t.

λ L(t) denotes the penalty coefficient of the model for local credibility at time t.

$$\lambda_L(t) = \begin{cases} 1, \Delta T_2(\text{A - B}, \text{ t}) \geq 0 \\ 0 \leq x < 1, \Delta T_2(\text{A - B}, t) < 0 \end{cases} \tag{7}$$

4.3 Comprehensive credibility

The trust measure of entity A to B is expressed by Trust (A-B). The formula of the trusted measure is as follows:

$$\text{Trust}(\text{A - B} \quad t) = \omega_1 T_1(\text{A} \quad t) + \omega_2 T_2(\text{A - B} \quad t) \tag{8}$$

Among them, T_1 (A, t) denotes local credibility, T_2 (A-B, t) denotes channel credibility, and W elements of weight vector are direct and indirect credibility weights, respectively. The weight index of reliability in the formula: ω 1 + ω 2 = 1.

5 Dynamic trustworthiness measurement process model

The process included: initialization of data, establishment of a dynamic data node trust network, calculation of the reliability of the node and the channel reliability of the node and the system. The comprehensive trust measures included identity authentication, user registration, data attribute extraction and trust judgment, etc[8].

6 Evaluation and analysis

The validity of the model was verified on the compiled simulator, which followed the measurement rules of Trust mechanism. To facilitate verification, simulation parameters were set as shown in Table 1.

Table 1. Application parameters test results of different user.

Parameter	Set value	Description
μ(t)	0.9	Time attenuation coefficient
λ(t)	0.5	Punishment coefficients
ω1	0.65	Local credibility weightiness
ω2	0.35	Remote credibility weightiness
Δ	1s	time interval

In order to analyze the reliability changes of the same node under different trusted events, the initial value of the allocated trusted level was 0.50, only high, medium and low trusted level events were input in 20 time periods respectively. The simulation results were shown in Figure 4. It could be seen from Figure 4 that through the accumulation of a large number of legitimate events, legitimate events enhanced the trusted level values of relevant terminal entities. The final trusted value was greater than 0.8. According to the rules, terminal entities would get all the necessary permissions of the system. Moderate legitimate events slowly increased the terminal entities trustworthiness level. Violations reduced the

trustworthiness level of the associated terminal entities. The final trusted value was smaller than 0.2. According to the rules, terminal entities would not be able to obtain any privileges of the system; the trustworthiness level of users can quickly and dynamically reflect the nature of events at various time intervals.

For terminal entities with different initial trustworthiness levels, the initial trustworthiness was set as 0.8, 0.5 and 0.4, respectively. Under the same input conditions, it could be seen that the same event would make the terminal entities trustworthiness level converge.

Furthermore, considering the influence of different timeliness factors and penalty factors on trustworthiness measurement, the level of evidence collected from specific target entities was set to H, H, H, L, H, M, H, H and H. The time-effect factor and penalty factor were (0.95, 0.6), (0.9, 0.5), (0.85, 0.4) respectively.

When the number of trusted events increased gradually, the comprehensive reliability value of the evaluated entity node increased slowly. The larger the timeliness factor was, the smaller the time influencing factor would be, and the faster the trusted value would increase. Similarly, for untrusted events, the comprehensive credibility of the terminal entities would be rapidly reduced to below the credibility threshold by adopting punishment strategy, and the effective isolation would be carried out, so as to reduce its threat and damage to the network.

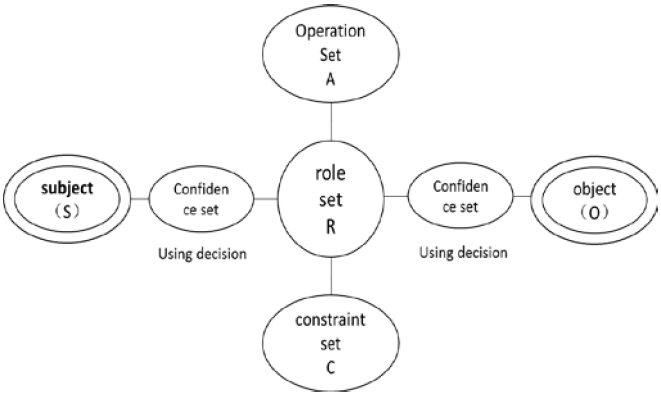

Fig. 1. The structure scheme of encryption system.

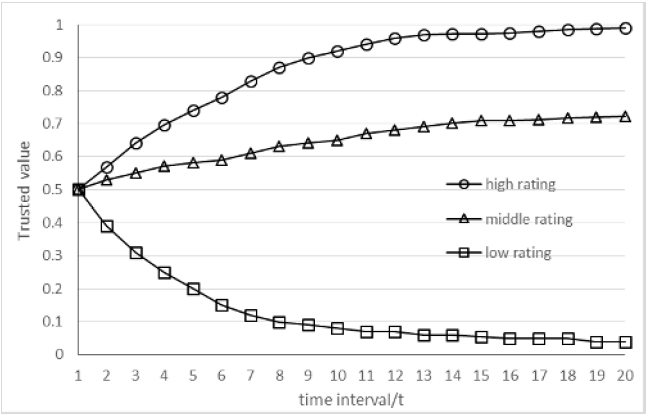

Fig. 2. The change curve of trust value of the same entity under different trusted events.

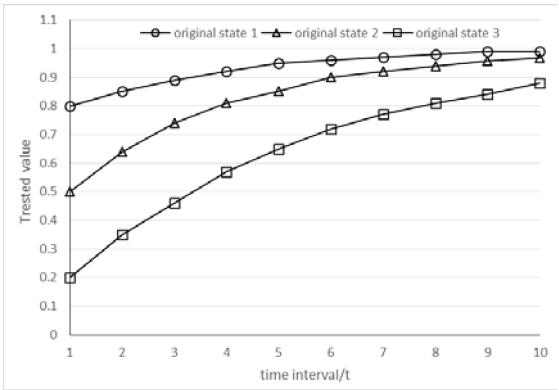

Fig. 3. The trusted value curves under different initial conditions.

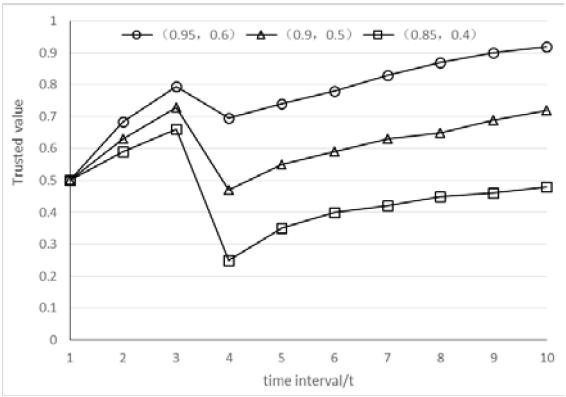

Fig. 4. The trusted value with different parameter settings.

Through the above simulation experiments and analysis, compared with access control, the way of behavior trustworthiness had finer granularity and stricter requirements, which could better meet the needs of data security on the network. In the case that the terminal entities may be dangerous, the system takes the initiative to limit the behavior of the node, so as to play the role of active defense and ensure the information security of the smart grid system.

7 Summary

With the construction of the Internet industry, the information network is more and more complex, in order to solve the information under the network environment safety of each terminal node data exchange credible measurement model based on behavior is proposed in this paper, record the basic attributes of node data and operation, through unified security exchange protocol for information transmission, on the basis of data attributes analysis abnormal behavior, and behavior are credible inspection, The timeliness of interaction context is fully considered. By introducing historical interaction evidence window, timeliness factor and penalty factor, the reliability value between network entities can be calculated sensitively and effectively, with excellent environmental adaptability and dynamic performance, and easy to implement.

Project Supported by State Grid Science and Technology Project: Ultra-low power multi-connection and high-security object-to-object communication chip (546856200059)

References

1. Singh A. Smart Grid Wide Area Monitoring, Protection and Control [J]. International Journal of Engineering Research and Applications (IJERA), 2012.
2. HAO Jinping, PIECHOCKI R J,KALESHI D, et al. Sparse malicious false data injection attacks and defense mechanisms in smart grids [J].IEEE Transactions on Industrial Informatics,2015,11(5):1198-1209.
3. Du Wei, Zhang Xiaochen, Yang Dongmei, Chen Yonghua, Zeng Ming. Architecture and application of information physics system for comprehensive energy [J]. Electric power construction, 2020, 41(04): 90-99.
4. Liu Wanggen, Zheng Huicheng, Rong Guoping. Large-scale distributed computing data sensing scheduling system in cloud environment [J]. Big data, 2020, 6(01): 81-98.
5. Du Helin, Miao Shiyu, Du Wenxia, Lu Feng. Study on fault diagnosis of improved principal component analysis method and data reconstruction in industrial system [J]. Journal of nanjing university of science and technology, 2019, 43(01): 72-77.
6. Hu Wei, Zhao Wenhui. Energy Internet data fusion method based on time window and adaptive weighting [J]. Journal of systems management, 2016, 25(05): 907-913.
7. Al-Zubaedi W, Al-Raweshidy H S. A parameterized and optimized BBU pool virlualization power model for C-RAN architecture[C]// IEEE Eurocon 2017-International Conference on Smart Technologies. IEEE, 2017:38-43.
8. Zhang Yan, Zhang Tao, Liu Yajie, et al.Stochastic model predictive control for energy management optimization of an energy local network[J]. Proceedings of the CSEE, 2016, 36(13): 3451-3462.