Intrusion Tolerance Quantitative Calculation for Energy Internet Data

Zhanwang Zhu[1] and Song Deng[2(✉)]

[1] College of Automation, Nanjing University of Posts Telecommunications, Nanjing 210003, China

[2] Institute of Advanced Technology, Nanjing University of Posts Telecommunications, Nanjing 210003, China

dengsong@njupt.edu.cn

Abstract. In the energy Internet, the deep integration of various en- ergy networks and information communication systems, as well as the operation characteristics of openness, interconnection and sharing, lead to more complex network security risks. Data security is another huge challenge facing the energy Internet. In this paper, a quantitative model of energy Internet data intrusion tolerance is constructed by studying the data autonomy and the quantitative principle of data survival based on set theory. Based on the quantitative model of data intrusion tol- erance, an adaptive intrusion response model based on game theory is proposed. By analyzing the gains and losses of both sides of the game, the profit model of both sides is derived, The optimal Nash equilibrium of both sides is obtained based on game theory. The analysis shows that the proposed data intrusion tolerance quantification and adaptive intru- sion response model can provide theoretical basis and support for active defense of energy Internet data security under network attacks.

Keywords: Energy Internet · Intrusion tolerance · Information security · Data security · Quantitative calculation of intrusion tolerance

1 Introduction

The large-scale development and utilization of renewable energy will become the development trend of global energy field. The emergence of energy Internet promotes the coupling of power, solar energy, natural gas and other energy net- work systems, and changes the traditional energy utilization mode [1, 2]. As an important part of renewable energy development and energy conservation and emission reduction of the whole society, energy Internet has the characteristics of complex structure, wide data sources, huge data scale and open data sharing, which brings great challenges to the security protection of energy Internet data. In the energy Internet, the security protection of data basically

Supported by the National Natural Science Foundation of China (No.51977113), BAGUI Scholar Program of Guangxi Zhuang Autonomous Region of China (201979) and NUPTSF (No.NY219095).

S. Yang and H. Lu (Eds.): ISAIR 2022, CCIS 1700, pp. 183–192, 2022.
https://doi.org/10.1007/978-981-19-7946-0_16

stays in the aspects of data encryption, access control, authorization and log audit. It is difficult to resist the increasingly complex network intrusion attacks only relying on these security means. At the same time, these security technologies are de- signed to maximize the avoidance of network attacks, and do not consider how to comprehensively assess the threat of data security risks to information systems and physical systems in the case of network intrusion. The existing quantitative calculation methods for data security in the energy Internet generally calculate the security risk value or its state value according to the confidentiality, integrity and availability of the data in the information and physical system, without considering the response of data under the incentive of intrusion attacks and the response mechanism of data after intrusion. Therefore, this paper analyzes and constructs the energy Internet data intrusion tolerance quantitative model from the perspective of data survival quantification principle, describes the data autonomous domain, the basic data security component chain corresponding to the attack scenario, and the evolution of data attack resistance, identifiability and data recoverability, so as to enrich the data security protection means of energy Internet [3, 4].

The traditional means of data security protection are to avoid the occurrence of intrusion attacks, but these technical means are difficult to truly avoid the occurrence of intrusion attacks and provide timely response after the occurrence of intrusion, and ultimately cannot provide normal business system data services in the energy Internet. Therefore, under the premise of considering attacks, this paper constructs an adaptive intrusion response game model for energy Internet data services from the perspective of data service effectiveness and response cost, so as to enhance the robustness of energy Internet data services.

The remaining of this paper is organized as follows. Section 2 analyzes related work. The energy Internet architecture and data security risk analysis under business scenarios is presented in Sect. 3. Section 4 introduces the quantitative calculation method of energy Internet data intrusion tolerance. And we conclude the whole paper in Sect. 5.

2 Related Work

The research on intrusion tolerance technology by foreign scholars was about 20 years earlier than that in China. The concept of intrusion tolerance was first proposed by Fraga and Powel [5]. Huimin LU et al. [6] propose the decentralized blockchain-based route registration framework-decentralized route registration system based on blockchain (DRRS-BC).Foreign scholars have achieved rich results in the research of this hot topic. Wang et al. [7] conducted intrusion detection on the system from various levels, and established a supervision system with functions such as policy reconfiguration and service monitoring. Liu et al. [8] proposed an intrusion tolerance technology based on incomplete information dynamic game, which combines game theory with intrusion tolerance technology, and determines the optimal strategy of both sides of the game by solving the Nash equilibrium. Mostefaoui et al. [9] proposed a digital signature protocol that is conditionally tolerant of intrusions against network attacks based on cryptographic systems to ensure that the system can still provide minimal authentication services when the system is under attack.

In recent years, domestic scholars have also done corresponding research on intrusion tolerance technology. Li et al. [10] combined threshold cryptography with intrusion tolerance technology, and proposed a threshold ECC-based intrusion-tolerant CA private key protection scheme, which ensured that even if the system is attacked. Wang et al. [11] proposed a network distance election calculation model that supports intrusion tolerance, which had a stronger predictive ability than traditional benchmark algorithms. Yu et al. [12] proposed an intrusion tolerant public key encryption scheme to reduce the harm of key leak- age to the encryption system. Zhao et al. [13] proposed a virtual machine-based intrusion tolerance system quantitative performance evaluation method, which improves the security of the computer compared with traditional methods. Wei et al. [14] used an improved semi-Markov process model to describe the process of normal and penetration attacks against the intrusion tolerance system in the data acquisition and monitoring (SCADA) system.

Energy Internet, as a research field that has only emerged in recent years, has been highly valued at home and abroad. Due to the open intercommunication of the Energy Internet, the interaction between various energy data is extremely vulnerable to intruders. As a newly developed field, quantitative calculation and adaptive intrusion response for energy Internet data intrusion tolerance technology are rarely involved.

3 Data Security Risk Analysis for Energy Internet

3.1 Energy Internet Architecture

The development of the Energy Internet not only breaks the shackles that the use and transmission of traditional energy can only rely on electric energy, so that various types of energy can be dispatched and transformed into each other in a unified manner, and the power system network is closely connected with the natural gas network and other types of energy networks. Combine to form an energy sharing network with multiple energy interoperability. Energy flow of Energy Internet is shown in Fig. 1.

The function of the energy center is mainly to realize the conversion between various types of energy, or to store the energy inside the energy center and use it for load consumption [15, 16]. It can be seen from Fig. 1 that the energy Internet is mainly composed of four parts: the primary energy side, the energy center, the power generation unit, and the load side. The primary energy side is mainly composed of the power grid, the natural gas grid, the cooling grid, and the heating grid. The power generation unit mainly includes wind power, solar power, thermal power, etc. The energy center is responsible for the conversion between various types of energy, as well as the input and output of energy, including energy storage equipment, refrigerators, fuel cells, boilers, etc. The load end corresponds to primary energy side input fully meets the diverse needs of users.

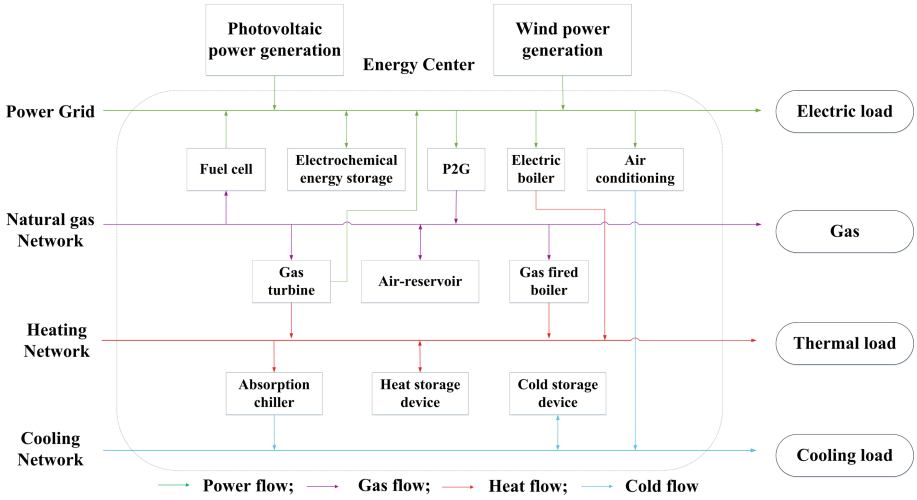

Fig. 1. Energy flow of energy internet.

The complete life cycle of the Energy Internet can be described as the energy flow process from the generation of energy to the transmission and conversion of energy, as well as energy storage and energy use. Figure 2 summarizes the entire life cycle of energy input, conversion, transmission and output of the Energy Internet, including the energy supply layer, energy production control layer, energy consumption layer and energy storage layer. The energy supply layer is the energy source of the entire energy Internet, which mainly includes primary energy such as solar energy and petroleum. The energy production control layer is mainly responsible for receiving the collected primary energy, taking the primary energy as input, and converting the primary energy into electrical energy through the energy router and as the input of the next level. The energy consumption layer is the most frequent link of data interaction in the entire energy Internet, which mainly includes users' inquiries on electric and thermal energy and transmission rights transactions. The energy storage layer is the "warehouse" of the entire energy Internet. When the physical system fails, it can ensure the normal operation of the business and improve the stability of the grid.

3.2 Data Security Risk Analysis

The information network of the Energy Internet has the characteristics of open- ness and sharing, and more levels of data sources, generally showing the characteristics of wide sources, large scale and complex types. Information in the Energy Internet accompanies the flow of energy, forming a wide-area distributed data application environment in all fields. However, the openness, interconnection and sharing mechanism of the Energy Internet will cause malicious network attacks to occur continuously. This section will analyze the various links of data flow in the Energy Internet, expounding possible data security risks from three aspects.

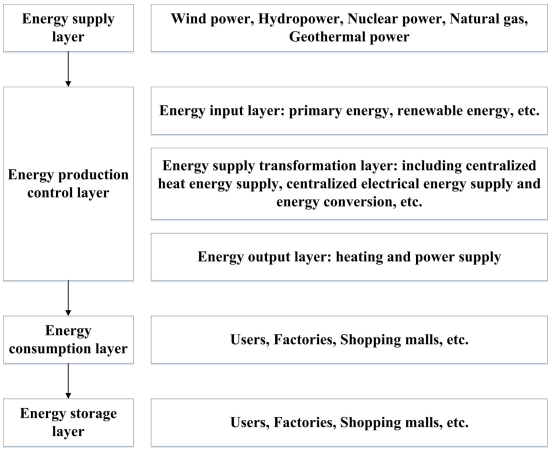

Fig. 2. The architecture of energy internet.

The security of energy Internet-related business scenarios mainly includes infrastructure security, system and interaction security, and smart terminal se curity. The specific analysis is as follows:

(1) The stable operation of infrastructure is inseparable from data transmission. The information transmission of the energy Internet usually uses traditional transmission methods such as optical fiber, local area network, and wire. Common data risks mainly include fiber-optic eavesdropping, tampering with status data and misoperation by operators.
(2) With the development of the Energy Internet, business exchanges between users and systems are increasing. The gradual improvement of information ser vices enhances user experience and increases system data security risks. Typical data attacks include DOS attacks and fake data attacks.
(3) The security threats of smart terminals mainly come from traditional devices such as mobile handheld terminals, energy Internet data collection terminals, and smart energy efficiency terminals. The information communication between the system and the terminal makes the security of the system inevitably threatened. The main threats are data loss, tampering, and Dos and DDos attacks initiated by intruders.

4 Quantitative Calculation Method of Data Intrusion Tolerance for Energy Internet

In order to carry out the quantitative analysis and calculation of the cyber- physical system data of each link of the Energy Internet after being attacked, what must be solved is to analyze the survival situation of the cyber-physical system of each link of the Energy Internet (that is, whether these systems can still provide external information. Service), this article draws on the traditional theory and methods of system intrusion tolerance to analyze the quantitative calculation method of data intrusion tolerance from the perspective of data sur vivability.

Definition 1. Let A_i denote the source of energy Internet data collection, T_i denote the type and mode of transmission, S_i and P_i denote the data storage and processing platforms, respectively, E_i denote the data interaction between energy Internet links, and D_i denote the means of data destruction. Then we call $AS_i = \{A_i, T_i, P_i, S_i, E_i, D_i\}$ as the autonomous domain of energy Internet data securety $\{ASi = Ai, Ti, Pi, Si, Ei, Di\}$.*N* autonomous domains AS_i form the autonomous domain set $\{AS_i, i = 1, 2,\ldots\}$.

Definition 2. Let AS_i denote the i-th autonomous domain and CS_i denote the basic security logic components contained in the i-th autonomous domain, then we call$\{ CS_i$,i $= 1, 2\}$, denotes the set of basic security components.

Based on the data location and environment in the energy Internet and the overall posture of the data security autonomous domains, N typical data attack scenarios against AS_i are constructed to form a data attack scenario set Fi (e.g., virus and malware attacks, DoS, eavesdropping, tampering, etc.). The data attack flow formed by the whole data attack scenario *Fi* is mapped to the data logical components to form another security component set SC_i, which finally forms the basic security component chain corresponding to the autonomous domain and attack scenarios as shown in Fig. 3.

4.1 Resistability Quantification Calculation

Resistance refers to the ability of the Energy Internet as a whole to provide data services normally when the system is under attack. The emphasis is on the overall system rather than the performance of individual components. This article constructs the criticality value of the event set $\{E_{qn}\}$of the data-attack damage level q from indicators such as

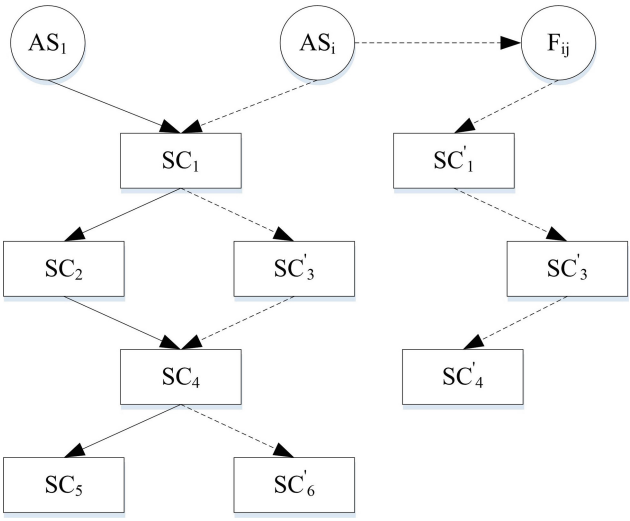

Fig. 3. Basic security component chain corresponding to autonomous domain and attack scenario.

autonomous domain and criticality weight, as shown in the following formula:

$$\omega_q = \frac{\sum_{n=1}^{N} \omega_{qn}}{N} \tag{1}$$

where N is the number of data attack events and w_{qn} is the harm value of the n-th data attack event.

On this basis, AS_i constructs the data security domain to the data attack scenario set and the data security autonomy domain resistibility quantification formula respectively, as shown in formula (2) and (3):

On this basis, the resistibility quantification formulas of data security au- tonomous domain AS_i to data attack scenario set F_{ij}, and data security au- tonomous domain AS_i are constructed respectively.

$$Resis\_F_{ij} = \Sigma_k(\Sigma_k(W_q \times p\_res_q \times d_q) \times m_{ijk}). \tag{2}$$

$$Resis\_AS_i = \Sigma_j(Resis\_F_{ij} \times f_{ij}). \tag{3}$$

where p_res_q is the resistance rate of data to attack events at this level, d_q is the distribution rate of data attack events at all levels, m_{ijk} is the weighted value of logical relationship and attack scenario relationship among data sets in data security autonomous domain, and f_{ij} is the jeopardy weight value of F_{ij} in data attack scenario.

If the importance of each data security domain AS_i is represented by a weight s_i, then the resistibility of energy Internet is shown as follows:

$$Resis = \Sigma_i(Resis\_AS_i \times s_i). \tag{4}$$

4.2 Recognizability Quantification Calculation

Recognizability emphasizes the monitoring and identification of the data security status in the cyber-physical system of the entire energy Internet, not just for a certain event. This paper intends to construct the overall recognition time of the event set {Eqn} of the attack hazard level q by the data as shown as follows:

$$T_q = \frac{\sum_{n=1}^{N} t_{qn}}{N} \times n. \tag{5}$$

where N is the number of data attack events, and tqn is the regularized value of the recognition time of the nth data attack event.

On this basis, the data attack scenario Fij and the data security autonomous domain AS_i identifiable quantitative model are constructed respectively, as shown in Eqs. (6) and (7).

$$Recog\_F_{ij} = \Sigma_k(\Sigma_q(W_q \times p\_recog_q \times d_q \times T_q) \times m_{ijk}). \tag{6}$$

$$Recog\_AS_i = \Sigma_j(Recog\_F_{ij} \times f_{ij}). \tag{7}$$

where p_recog_q is the recognition rate of q level attack events in the attack scenario event set by data, d_q is the distribution rate of data attack events at this level, and m_{ijk} is the weighted value of the logical relationship between each data set in the data security autonomous domain and the data attack scenario relationship, f_{ij} is the hazard weight of F_{ij} in the data attack scenario.

The recognizability of the Energy Internet can be summarized as the weighting of the recognizability values of all data security autonomous domains, as shown in Eq. (8)

$$Recog = \Sigma_i(Recog\_AS_i \times s_i). \tag{8}$$

4.3 Recoverability Quantitative Calculation

The recoverability of data is defined as whether the impact on the data caused by a network attack is recoverable, and the extent to which the data autonomous domain can be recovered within a certain period of time.

This paper intends to construct the recoverability function model of each link N_{ik} in the data security autonomous domain AS_i, as shown in Eqs. (9) and (10), respectively.

$$Recov\_N_{ik} = \Sigma_j[f_{ij} \times p\_recov_{kj} \times p\_recov_{kj}. \times recovT_{ik}/TureT_{kj}]. \tag{9}$$

$$Recov\_AS_i = \Sigma_k(Recov\_N_{ik} \times a_{ik}). \tag{10}$$

where $recovT_{ik}$ is the recovery time requirement of each link of the N_{ik} in the data security autonomous domain AS_i, $TureT_{kj}$ is the time interval from the start of the data attack scenario set F_{ij} to the complete recovery of each link in the data security autonomous domain AS_i, and p_recov_{kj} is the data within the $TureT_{kj}$ time interval The degree of recovery of the N_{ik} of each link in the security autonomous domain AS_i, a_{ik} is the recoverability weight of each link of the N_{ik} in the data security autonomous domain AS_i.

On this basis, the formula for summarizing the recoverability of Energy Internet data is shown as follows:

$$Recov = \Sigma_i(Recov\_AS_i \times s_i). \tag{11}$$

5 Conclusions

This article gives a detailed introduction to the concept of data intrusion tolerance and its quantitative calculations in the context of the Energy Internet. On the basis of constructing the basic security component chain of the cyber- physical system data for each link of the Energy Internet, from the aspects of resistance, identifiability and The data intrusion tolerance is quantitatively calculated at three levels of recoverability, and the adaptive intrusion response based on game theory is theoretically deduced. Compared with other existing models, the adaptive intrusion response model based on game theory analyzes the cost of intrusion tolerance and the benefits obtained, and the decision made fully considers the gains and losses of both parties in the game and is reasonable.

Acknowledgements. We would like to thank the anonymous reviewers for their comments and constructive suggestions that have improved the paper. The subject is sponsored by the National Natural Science Foundation of P. R. China (No. 51977113) and BAGUI Scholar Program of Guangxi Zhuang Autonomous Region of China (201979).

References

1. Wang, K., et al.: A survey on energy internet: architecture, approach, and emerging technologies. IEEE Syst. J. **12**(3), 2403–2416 (2017)
2. Zhou, K., Yang, S., Shao, Z.: Energy internet: the business perspective. Appl. Energy **178**, 212–222 (2016)
3. Sani, A.S., Yuan, D., Jin, J., Gao, L., Yu, S., Dong, Z.Y.: Cyber security framework for internet of things-based energy internet. Futur. Gener. Comput. Syst. **93**, 849–859 (2019)
4. Wang, H., Ruan, J., Ma, Z., Zhou, B., Fu, X., Cao, G.: Deep learning aided interval state prediction for improving cyber security in energy internet. Energy **174**, 1292–1304 (2019)
5. Veríssimo, P.E., et al.: Intrusion-tolerant middleware: the road to automatic security. IEEE Secur. Priv. **4**(4), 54–62 (2006)
6. Lu, H., Tang, Y., Sun, Y.: Drrs-bc: Decentralized routing registration system based on blockchain. IEEE/CAA J. Automatica Sinica **8**(12), 1868–1876 (2021)
7. Wang, F., Gong, F., Sargor, C., Goseva-Popstojanova, K., Trivedi, K., Jou, F.: Sitar: A scalable intrusion-tolerant architecture for distributed services. In: Workshop on Information Assurance and Security. vol. 1, p. 1100 (2003)
8. Liu, P.: Engineering a distributed intrusion tolerant database system using cots components. In: Proceedings DARPA Information Survivability Conference and Exposition. vol. 2, pp. 284–289. IEEE (2003)
9. Mostéfaoui, A., Raynal, M.: Intrusion-tolerant broadcast and agreement abstractions in the presence of byzantine processes. IEEE Trans. Parallel Distrib. Syst. **27**(4), 1085–1098 (2015)
10. Li, X.: An intrusion tolerant protection scheme of ca private key based on threshold ecc. Computer Simulation **26**(12), 115–117 (2009)
11. Wang, C., Zhang, F.L., Yang, X.X., Li, M., Wang, R.J.: A voter model supporting intrusion-tolerance for network distance estimation. J. Electron. Inf. Technol. **35**(11), 2637–2643 (2013)
12. Yu, J., Cheng, X.G., Li, F.G., Pan, Z.K., Kong, F.Y., Hao, R.: Provably secure intrusion-resilient public-key encryption scheme in the standard model. Ruanjian Xuebao/Journal of Software **24**(2), 266–278 (2013)
13. Zhao, F., Jin, H., Jin, L., Yuan, P.: Vfrs: a novel approach for intrusion tolerance in virtual computing environment. J. Computer Res. Development **47**(3), 493 (2010)
14. Wei, K., Zhang, F.: Based on markov network tolerate invasion ability evaluation model. Computer Simulation **33**(7), 289–292 (2016)
15. Deswarte, Y., Powell, D.: Internet security: an intrusion-tolerance approach. Proc. IEEE **94**(2), 432–441 (2006)
16. Moniz, H., Neves, N.F., Correia, M., Verissimo, P.: Ritas: Services for randomized intrusion tolerance. IEEE Trans. Dependable Secure Comput. **8**(1), 122–136 (2008)
17. Huimin, L., Zhang, M., Xu, X.: Deep fuzzy hashing network for efficient image retrieval. IEEE Trans. Fuzzy Syst. **29**(1), 166176 (2020). https://doi.org/10.1109/TFUZZ.2020.2984991

18. Huimin, L., Li, Y., Chen, M., et al.: Brain Intelligence: go beyond artificial intelligence. Mobile Networks Appl. **23**, 368–375 (2018)
19. Huimin, L., Li, Y., Shenglin, M., et al.: Motor anomaly detection for unmanned aerial vehicles using reinforcement learning. IEEE Internet Things J. **5**(4), 2315–2322 (2018)
20. Huimin, L., Qin, M., Zhang, F., et al.: RSCNN: A CNN-based method to en-hance low-light remote-sensing images. Remote Sensing 13(1), 62 (2020)
21. Huimin, L., Zhang, Y., Li, Y., et al.: User-oriented virtual mobile network resource management for vehicle communications. IEEE Trans. Intelligent Transportation Syst. **22**(6), 3521–3532 (2021)