Application of internet of things gateway encryption technology in safe operation of electric power

Jian Yin[a,*], Chun Zhang[a], Dongxi Zheng[a]
[a]Guangdong Weide Information Technology Co., Ltd, Guangzhou Guangdong, 51000, China

ABSTRACT

At present, the power Internet of things (IoT) border protection equipment gradually exposes its functions, and the technical specifications are not unified to deal with the problems of insufficient connection ability of high concurrent data, imperfect automatic monitoring function, complex product types, and difficulty in equipment selection. Although the traditional research supports remote maintenance, the information interaction effect is poor, which can't meet the high security characteristics. This problem forces the need for a data security communication protocol with high security and suitable for application scenarios. In this paper, the encryption technology of IoT gateway based on Bayesian algorithm is proposed to ensure the safe operation of power system. The simulation results show that the IoT gateway encryption method in this paper is safe and has practical application value for the safe operation of power system. Facing the needs of different business development, the software and hardware architecture should be integrated to form typical application protection schemes in different business scenarios, so as to achieve the goal of unified application security and accurate protection of basic network security.

Keywords: Internet of things; gateway encryption; electric power system

1. INTRODUCTION

IoT technology is a new type of science and technology that integrates many disciplines and is highly integrated. In recent years, with the economic development and scientific and technological progress, IoT technology has been paid more and more attention. From the perspective of industry chain development, electronics, software, information and communication, network operation, platform services, etc. all condense the wisdom of IoT. IoT injects its fresh blood into traditional industries, which plays a huge role in driving the transformation of traditional industries [1]. At present, the power IoT border protection equipment gradually exposes its functions, and the technical specifications are not unified to deal with the problems of insufficient connection ability of high concurrent data, imperfect automatic monitoring function, complex product types, and difficulty in equipment selection [2]. In reality, the network does not form a wide range of interconnection forms like the Internet. The main reason is that different networks need to be physically isolated to prevent network attacks [3]. Therefore, before isolation, it is need to ensure the security of information exchange between different networks by means of manual ferry, which can't meet the real-time application requirements of information interaction under the network environment [4-5].

*Email: tyxyiot2806@126.com

Seventh International Conference on Mechatronics and Intelligent Robotics (ICMIR 2023), edited by Srikanta Patnaik,
Tao Shen, Proc. of SPIE Vol. 12779, 127790A · © 2023 SPIE · 0277-786X · Published under a
Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.2689821

IoT, as the representative technology of the third informatization wave, is a booming industry involving many disciplines. In the early stage of industrial development, every equipment in the factory generated data, and according to the data generated by the equipment, the running state of the equipment was detected, so that the equipment could be repaired in time and the efficiency of the whole factory could be better improved [6]. Nowadays, IoT needs to integrate the hardware and software architecture for different business development, forming typical application protection schemes in different business scenarios, and achieving the goal of unified application security protection of basic network security [7]. Harbi et al. studied the main essentials of building ubiquitous power IoT, expounded the basic concept of ubiquitous power IoT, and thought that as a typical business supporting the construction of ubiquitous power IoT, it was in line with the development trend of future power energy system [8]. Abhi et al. proposed a charging station operation and maintenance strategy formulation method based on Ubiquitous Power IoT. Taking extra time as the risk index, different stations were graded according to the risk value, and the reliability was analyzed and the operation and maintenance strategy was formulated [9]. Although these studies support remote maintenance, the effect of information interaction is poor, which can't meet the high security characteristics. This problem forces the need for a data security communication protocol with high security and suitable for application scenarios. In this paper, the encryption technology of IoT gateway based on Bayesian algorithm is proposed to ensure the safe operation of power system.

2. METHODOLOGY

2.1 Power dispatching operation risk in IoT era

With the contisnuous improvement of electric power information buildings, the dynamic management of enterprises has been gradually realized, which can effectively detect the hazards and equipment problems in electric power enterprises. With the continuous popularization of IoT technology, it plays an increasingly important role in the growth of power enterprises. The continuous improvement of science and technology has brought great risks to the automation of electric power dispatching in China. So far, most electric power dispatching work in China has cited automation technology. On the one hand, after the application of computer technology, supervision and work efficiency have been greatly improved. On the other hand, the advanced technology has been applied to the substation management process, which provides a lot of convenience for the normal operation of the power grid. Electric power enterprises are constantly transitioning from a single energy supplier to an integrated energy and information configuration service provider [10]. The premise of this change is the continuous development and application of IoT technology, which further realizes the efficient and safe production and operation of electric power enterprises, fully demonstrates the coordination between enterprises and the environment, improves the contradiction between man and nature, and ensures the sustainable and healthy growth of electric power enterprises. There are many problems in the design process of automation system, which makes the safety hidden trouble caused by engineering construction mistakes seriously affect the normal operation of electric power dispatching. At the same time, all kinds of information will be generated in the application process of automation technology, which makes some important information ignored and covered, and then leads to a series of security risks. The IoT security hierarchy model is shown in Figure 1.

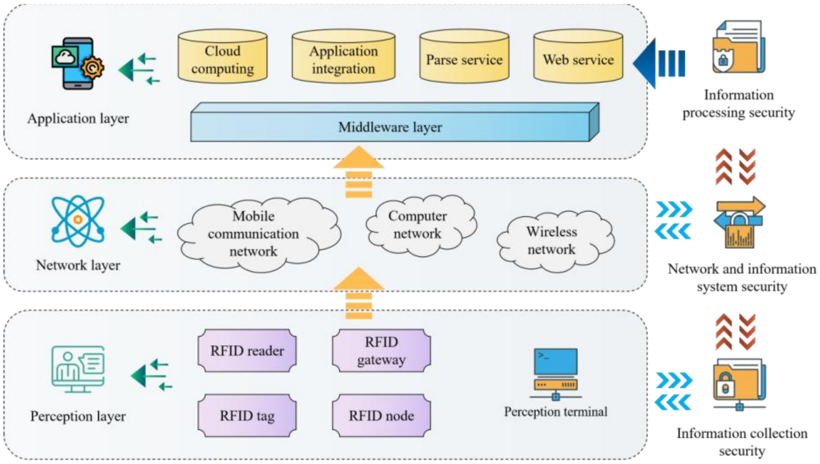

Figure 1. Security hierarchy model of power IoT

With the continuous development and improvement of China electric power enterprises for ten years, the automation construction has achieved certain results, but it is undeniable that there are still many shortcomings and deficiencies, one of which is that the information between the two systems can't communicate with each other, and only a single information can exist independently. With the continuous advancement of group management ideas, the information interconnection between systems will become a necessary trend. IoT promotes the automation, informatization and interaction of smart grid. Its effective application has successfully improved the equipment utilization rate of the existing power grid and the transmission capacity of all levels of power grids, and further improved the security, applicability and reliability of the power grid. Moreover, it will play a very important role in improving the information collection, intelligent information processing and two-way information exchange capacity of the smart grid in the five links of power generation, transmission, distribution, transformation and electricity consumption.

2.2 IoT gateway encryption algorithm

IoT and big data are all technical products in the information society. They are all modern concepts derived from Internet technology, computer technology and electronic technology. After collecting the data, the devices in wireless sensor network will use CSMA mechanism to upload the data to the gateway, so the uploaded data is random and disorganized. Because this mechanism lacks the overall scheduling of network resources, it will cause a great waste of network resources. Interaction with network content information refers to the production and performance of content with network infrastructure as the carrier. According to its storage location in the network, it can be divided into external storage and local storage. External storage means that all sensory data are concentrated and stored on the sink node, while local storage means storing sensory data on the sensor node. The security gateway structure of IoT sensor network is shown in Figure 2.

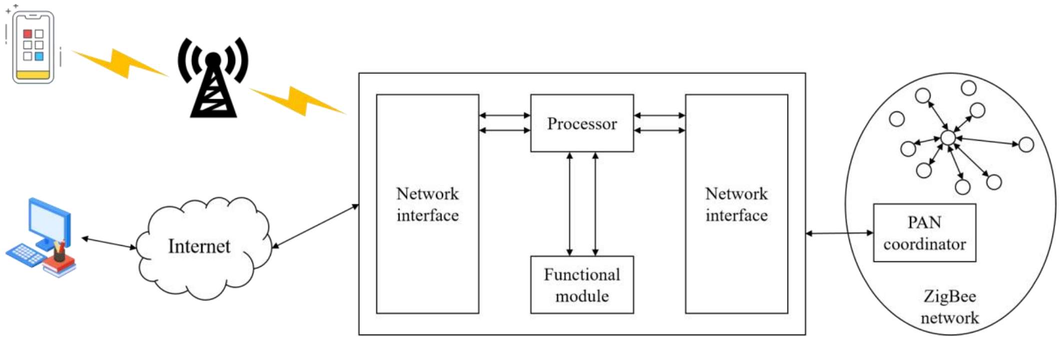

Figure 2. IoT sensor network security gateway structure

For IoT and big data, they are closely related to information transmission and security control. IoT can realize the information interaction between different objects, and carry out the overall perception, reliable transmission and intelligent processing of the operation process of power system, so as to realize the effective monitoring of power distribution and transmission [11]. Information interaction with users' content means that users can obtain interesting information from the network by means of information query. The information that users are interested in is usually the high-level semantic information perceived by nodes. The network queries according to the data organization structure, and feeds back the query results to users. Information query is realized by using the storage location of the content on the network. For external storage, the sink node can be directly queried.

Through access control, the gateway receives the data packet requested by a trusted third-party remote host or user, and judges whether the host is legitimate or not. According to the data type required by the remote host, the corresponding virtual IP address is allocated, and the remote host or user can query the required data through this virtual IP address. In the aspect of address mapping, this paper proposes an address mapping method based on data query.

Let the probability distribution of random variable set $X=\{X_1,X_2,\dots,X_n\}$ be $P(X_1,X_2,\dots,X_n)$. If all variables are $\{0,1\}$, 2^n-1 parameters are needed to determine the joint distribution. And through Bayesian formula, the joint distribution can be written as:

$$\begin{aligned}P(X_1,X_2,\dots,X_n)&=P(X_1)P(X_2|X_1)\dots P(X_n|X_1,X_2,\dots,X_{n-1}0)\\&=\prod_{i=1}^{n}P(X_i|X_1,X_2,\dots,X_{i-1})\end{aligned} \tag{1}$$

For $\forall X_i \in X$, if $\pi(X_i) \subseteq \{X_1, X_2, \ldots, X_{i-1}\}$ exists, the conditions of X_i assimilation $\{X_1, X_2, \ldots, X_{i-1}\} / \pi(X_i)$ are independent when $\pi(X_i)$ is given, and the above formula can be changed to:

$$P(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} P(X_i | \pi(X_i)) \tag{2}$$

For IoT, it is an improvement of the Internet. It can realize the process of information collection and transmission between objects and people through facilities and technologies such as information sensors. It can realize access to various networks, and has certain compatibility. As far as big data is concerned, its application in power security management and control can help provide a large amount of effective information, realize the application of intelligent technologies such as expert systems in various stages, and then combine it with cloud computing and other methods to strengthen the real-time monitoring of various power parameter ranges and avoid accidents. Complex high-dimensional multimedia information is a new challenge to the ability of data transmission, processing, storage and perception network. First of all, it is need to determine the size of the space that can carry massive multimedia information. Secondly, processing efficient multimedia network information. Finally, information interaction is realized through the cooperation between nodes.

As far as big data is concerned, it is an unimaginable data collection, which cannot be captured by conventional software. The value density of big data is very low, but it is very fast and has certain authenticity. In the application process of big data, it is usually a form linked with auxiliary tools such as cloud computing. In this information society, the application of big data and IoT can help improve the efficiency of power security management and control, and plays a very important role.

In the current application scenarios of sensor networks, the number of internal nodes in sensor networks always exceeds the number of data types to be collected by sensor network gateways. This method uses this principle to reduce some unnecessary IP address resource allocation and resource waste. It is assumed that the uplink and downlink transmission rates of task T_{ui} to the site are fixed at r_i . When the number of tasks S_i transmitted to the internal server of MEC server is D_{ui} , the transmission delay can be expressed as:

$$T_{ui} = D_{ui} / r_i \tag{3}$$

If the task S_i is executed at the mobile terminal, the total system delay from sending the uninstall request to the completion of the task execution can be expressed as:

$$TC_i = T_{ti} + tb_i + \min(P_{ci,j} + t_i) \tag{4}$$

T_{ti} represents the transmission delay, tb_i represents the delay waiting caused by insufficient bandwidth, $P_{ci,j}$ represents the delay caused by queuing at MEC, and t_i represents the delay caused by MEC server when executing tasks. If the task S_i executes related commands on the MEC server, its execution delay can be expressed as:

$$TC_{i,j} = T_{ti} + tb_i + P_{ci,j} + t_i \tag{5}$$

IoT security gateway needs to share data among different networks, and realize efficient packet reassembly and forwarding at different rates. Gateways usually collect data from the network according to the requirements of external network hosts. The data types and delay requirements of the generated data are different for different application scenarios. The delay here is the time that the gateway can save these data, so the gateway can package the data within this time and then forward it. On the premise of ensuring the integrity of data, the gateway will pack the data groups with the same destination and the same data type together and send them, which can reduce the number of packets, improve the forwarding efficiency, and improve the external network bandwidth utilization.

3. RESULT ANALYSIS AND DISCUSSION

Generally, the security mechanism adopted in the security gateway refers to the standard of security mechanism in sensor network, and combines the gateway access control mechanism, firewall function of gateway, security agent and other security mechanisms in sensor network, so as to effectively protect data packets. The Internet connection of power IoT terminals is built through the edge IoT agent, and the functions of interconnection, edge computing and regional autonomy between IoT terminals and IoT management platform are realized. In view of the existing gateway technology, this paper refers to the security mechanism requirements of sensor network, and adds the gateway security mechanism, mainly adopting cryptography and access control mechanism to realize the gateway security function. Access resources are managed through network access control and network permission control to protect data security in sensor network. Figure 3 shows the impact of IoT gateway encryption on evenly distributed data sets. Figure 4 shows the impact of IoT gateway encryption on real data sets.

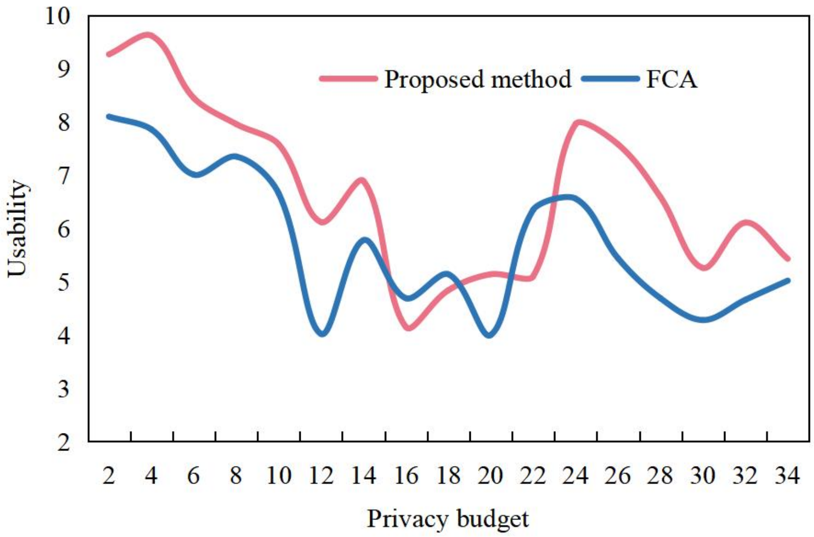

Figure 3. Impact of IoT gateway encryption on evenly distributed data sets

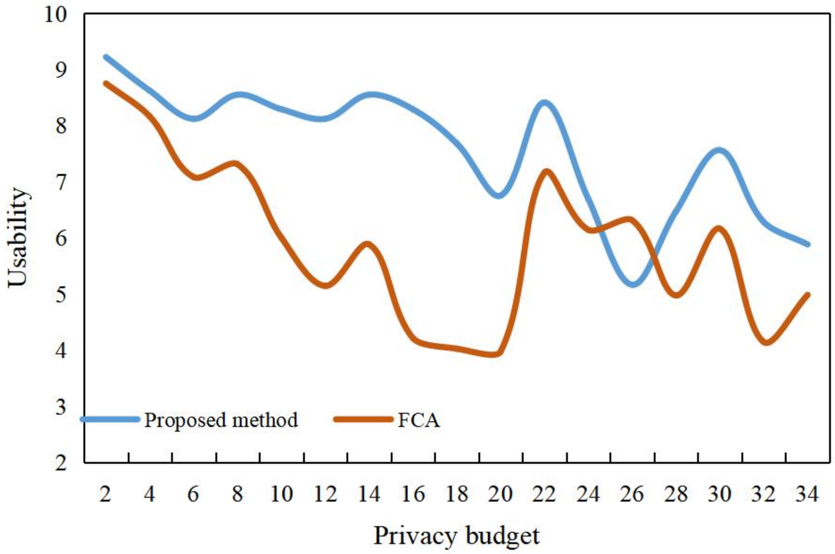

Figure 4. Impact of IoT gateway encryption on real data sets

Because the node algorithm is simplified and compressed sensing is used to process the transmitted data, the data transmission amount of this scheme is greatly reduced, so the energy consumption is also low. The deviation curve of main fault characteristics of IoT gateway is shown in Figure 5.

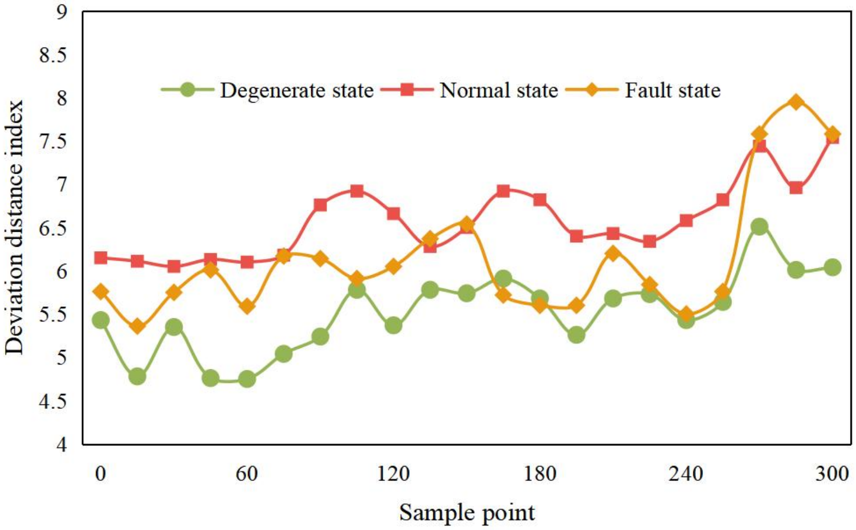

Figure 5. Selection of fault characteristic deviation curve

Build the IOT management platform, realize the unified monitoring, configuration and management of massive access acquisition terminals and edge IOT agents, support the rapid iteration and remote upgrade of various professional intelligent applications, collect massive acquisition data and standardize processing. The security comparison results of different IoT gateway encryption schemes are shown in Figure 6.

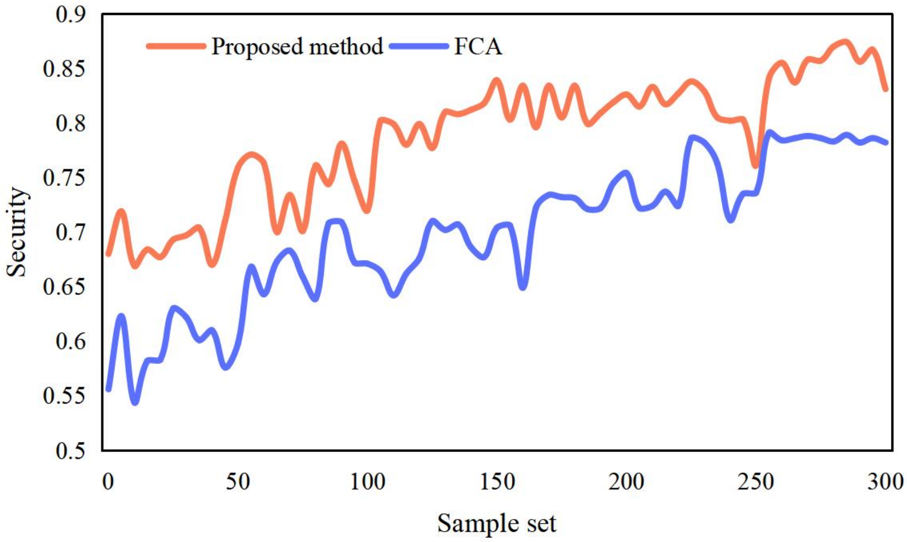

Figure 6. Security comparison of different schemes

According to the data in Figure 6, the IoT gateway encryption method in this paper is safe and has practical application value for the safe operation of power system. The way of system recording is adopted as an acquisition protocol. After the protocol completes the log data acquisition, other management devices can check the system log to know the all-weather operation of the whole platform. By using the system logging protocol, the communication between different devices can be realized. Managers only need to analyze the marked log events to master the running state of the whole network device.

4. CONCLUSIONS

IoT is a complex and huge system, and its access gateway is the key to its future development and application. It needs to carry out in-depth scientific research in stages and in a planned way. In this paper, an IoT gateway encryption technology based on Bayesian algorithm is proposed to ensure the safe operation of power system. This security solution has been applied in multiple business scenarios, which provides a strong support for network boundary security and an important guarantee for the growth of power IoT applications. Through the simulation experiment, it can be seen that the IoT gateway security mechanism proposed in this paper can effectively send data packets, thus reducing the data transmission delay, reducing the gateway load and realizing the data forwarding with low delay. The big data and IoT functions are applied to it, and the applications in power monitoring, stable control mode, power grid dispatching security and power plant security management and control are realized through information integration and perception, so as to realize the stable growth of power system.

FUNDING

This paper was supported by Technology project of Guangdong Weide Information Technology Co., LTD: Internet of Things encryption technology research and industrialization.

REFERENCES

[1] Duenas, P., Ramos, A., Tapia-Ahumada, K., et al. Security of supply in a carbon-free electric power system: The case of Iceland. Applied Energy, 212(3), pp. 443-454 (2018).

[2] Chen, C., Long, H., Zeng, X., Planning a sustainable urban electric power system with considering effects of new energy resources and clean production levels under uncertainty: A case study of Tianjin, China. Journal of Cleaner Production, 173 (2), pp. 67-81 (2018).

[3] Li, P., Zhou, J., Yu, X., et al., Design and on-orbit validation of electric power system for aoxiang-sat. Taiyangneng Xuebao/Acta Energiae Solaris Sinica, 39(4), pp. 1002-1007 (2018).

[4] Ufa, R. A., Malkova, Y. Y., Rudnik, V. E., et al., A review on distributed generation impacts on electric power system. International journal of hydrogen energy, 2022(47), pp. 47 (2022).

[5] Colbertaldo, P., Agustin, S. B., Campanari, S., et al., Impact of hydrogen energy storage on California electric power system: Towards 100% renewable electricity. International Journal of Hydrogen Energy, 44(19), pp. 9558-9576 (2019).

[6] Kato, T., Manabe, Y., Funabashi, T., et al., A Study on Influence of Ramp Event of Aggregated Power Output of Photovoltaic Power Generation on Electric Power System Frequency. Ieej Transactions on Power & Energy, 137(3), pp. 11-21 (2017).

[7] Hsu, C. L., Chen, W. X., Le, T. V., An Autonomous Log Storage Management Protocol with Blockchain Mechanism and Access Control for the Internet of Things. Sensors, 20(22), pp. 6471 (2020).

[8] Harbi, Y., Refoufi, A., Aliouat, Z., et al., Improved bio-inspired security scheme for privacy-preserving in the internet of things. Peer-to-Peer Networking and Applications, 15 (6), pp. 2488-2502 (2022).

[9] Abhi, A. I., Shin, S. Y., BUS: A Blockchain-Enabled Data Acquisition Scheme with the Assistance of UAV Swarm in Internet of Things. IEEE Access, 7(1), pp. 103231-103249 (2019).

[10] Liu, Y., Zhang, J., Zhan, J., Privacy protection for fog computing and the internet of things data based on blockchain. Cluster Computing, 2020(1), pp. 1-15 (2020).

[11] Ataei Nezhad, M., Barati, H., Barati, A., An authentication based secure data aggregation method in intemet of things. Journal of Grid Computing, 20(3), pp. 1-28 (2022).