Security architecture and technology of power Internet of things for energy interconnection

Xuesong Zhao*, Xiaofei Fan, Jing Hou
Metering management office of Shenzhen Power Supply Bureau Co., Ltd
e-mail: 125624078@qq.com*

Abstract: The power Internet of things platform is an important support for the digital innovation service of the energy Internet, covering all links of the power system. There are many new security problems. How to realize the trusted interconnection, intelligent defense and security interaction of the power Internet of things, and how to solve the data, application and key security of the power information system are important problems to be solved in the current power Internet of things. Facing the development of energy Internet, this paper analyzes the security requirements and characteristics of power Internet of things, puts forward the security framework of power Internet of things, and summarizes the key technologies of power Internet of things security.

1. Introduction
with China's social progress, the progress of energy Internet construction is accelerating. The power information system is more and more closely connected with the Internet of things technology. The development of the power system connects power users and their equipment in different ways by deploying a large number of on-site acquisition components, intelligent terminals and sensing devices, so as to form a power Internet of things with intelligent defense, security interaction and trusted interconnection, and control and perception of power system equipment. To realize the intelligence, interaction and informatization of power grid, the security framework of power Internet of things plays an important role in the construction of power grid and the rapid development of energy Internet.

2. Security requirements and characteristics of power Internet of things

2.1. Power Internet of things security requirements
(1) The operation and maintenance of the energy Internet can rely on the perceived demand. The sensors in the perception layer of the power Internet of things perceive and collect a variety of relevant data. A large number of sensors, intelligent device terminals and their different access methods bring many security risks to the energy Internet security system. Therefore, reliable edge perception and defense against cross space linkage attacks have become the premise and guarantee for the safe operation of the power Internet of things, which is a very challenging problem.
(2) Based on network interconnection, energy Internet covers all aspects of the network layer of power Internet of things, including short-range wireless communication network, wireless public/private network, EPON, boundary between master station and communication network layer, master station LAN, etc. In the connection process, different connection technologies need to be selected according to different application directions of power Internet of things. Establishing a trusted interconnection environment through secure identity authentication and password services, ensuring
the secure interaction of resources and services, and realizing the secure interconnection of the whole domain is an effective support for network sharing.

(3) Intelligent defense requires that the energy Internet has complex architecture, heavy and complex applications, and has high-frequency dynamics and massive data. Therefore, it is necessary to realize the security, comprehensive centralized control, coordination of energy efficiency, demand perception, intelligent sharing and the use and management of active defense mechanism on the application layer and data layer, combined with big data technology, imitation defense technology Artificial intelligence technology to implement business security audit, data security protection and risk intelligent processing.

3. Security Features Of Power Internet Of Things

In view of the energy Internet's characteristics of high efficiency and intelligence, open interconnection, horizontal complementarity, increasing revenue and reducing expenditure, compared with traditional security, the power Internet of things has the following characteristics. The specific composition is shown in Figure 1.

The edge computing secure energy Internet deploys a large number of different terminal devices to form an edge computing network at the edge of the power grid. It is responsible for unified access of sensor equipment nodes and data in the network to the backbone network. It has important business functions such as user control, service provision and service monitoring. Different from traditional computer terminals, there are many kinds, heterogeneous networks, different protocols and a large number of sensor equipment nodes connected to the power Internet of things in the edge computing network; At the same time, due to the limited computing resources and long-term operation of the power IOT sensor device nodes converged and accessed by the edge computing terminals, the traditional "patch" security reinforcement mechanism can not be applied to the IOT sensor device nodes. In an uncontrolled environment, the risk of malicious utilization of the sensor device nodes is very high, resulting in that the edge computing terminals are very easy to become attack targets or springboards. After the ubiquitous computing business system with the sinking of computing power, an edge distributed computing system with full time domain and spatial interconnection is formed on the edge side, which is interconnected with the power grid control network in real time across information physical space. The structure is complex, showing hybrid multi-scale dynamic characteristics and complex network characteristics. Different from the fault nature of traditional power grid n-1 or n-2, its security threat may cause chain reaction. The edge computing network attack will affect the ability of terminal equipment to perform monitoring function, increase the vulnerability of the system, cause the mutual penetration of the two networks, and even endanger the physical network and generate large disturbance, thus threatening the security of power system.
4. Key technologies of power Internet of things security

In order to protect the sensitive information of the power Internet of things, prevent the information from being obtained by the attacker through interception, and the receiver can obtain the required information normally and safely, the related technologies of the power Internet of things are divided into perception layer and network layer.

4.1. Key technologies of perception layer security

4.1.1 Vulnerability mining technology

The loopholes in the power grid cause the leakage of the network, increase the access rights of the network, so that hackers can operate inside and outside the security range, resulting in the loophole mining technology. Vulnerability mining technology includes data mining, fuzzy principle, binary comparison and web crawler. Among them, data mining is to obtain the causes of vulnerabilities according to the corresponding information. Obtain data information through web crawler and other methods, process, integrate and classify the information through crawler technology, and then extract useful information through specific algorithms or statistical data. Data mining can analyze the abnormal conditions of faults, make full use of data analysis technology, network security detection and other technologies, get the problems existing in power websites, base stations or systems, and repair the relevant abnormalities.

4.1.2 Intrusion detection technology

Intrusion detection is the basic content of intrusion detection technology. It can cause the intrusion behavior of network security hidden danger. Intrusion detection technology collects power grid operation information, including behavior information, network data and so on. Then the obtained information is systematically analyzed and detected, and the collected data information is statistically and classified.

4.1.3 Edge computing security technology

Edge computing network is a hybrid network architecture, which involves many links and technologies. The security protection technology of edge computing network includes password protection, security model, access control strategy, host reinforcement, anomaly detection, association analysis and so on. In terms of terminal penetration defense, the existing edge computing terminal security mainly adopts encryption technology and trusted computing technology to realize terminal security authentication and data storage and computing security. Dynamic learning and dynamic measurement based on the behavior characteristics of edge computing terminals can detect the penetration attack behavior of malicious terminals, and can not be controlled in advance.

4.1.4 Mimicry Defense Technology

National defense technology is based on the computing or service components with the same function and different structures, the "different redundancy" structure with high availability and high reliability, combined with the multi-mode voting mechanism that does not rely on rules and features, and disturbs the judgment of attackers through the nonlinear transformation of the external features of the system. At present, the active defense model based on the idea of pseudo defense technology is basically the ipomodel. When the submitted request is input to the system, the input agent unit first copies it into N copies and forwards it to n similar redundant actuators (P1, P2, ..., PN); Each actuator receives a copy of the request, processes it, and outputs a response after the voter votes. Taking advantage of the influence of network attacks on the environment, a specific vulnerability attack can not be effectively played in heterogeneous executors at the same time, so as to achieve the defense effect of vulnerability attacks. At present, many systems with pseudo defense structure have been formed based on pseudo defense structure router, pseudo defense structure distributed storage system and pseudo defense structure web server.
4.2. Key technologies of network layer security

4.2.1 Firewall technology
There is a barrier between the external network and the internal network of the power system, which is called firewall. Firewall can operate the data information of network security to ensure the information security and network security of power system. Isolation control technology is the most commonly used technology in firewall technology. It greatly prevents the output and access outside the protected system. Some composite protection technologies make the protected information in a safe state, and dynamic filtering has a good effect. According to the operation objectives of power equipment and firewall access strategy, the address and corresponding port can be obtained, so that the current operation status of power equipment network system can be found, which adds an effective guarantee for the security of power information.

4.2.2 Isolation switching technology
With the rapid development of information security technology, the isolated switching technology of network security has become a new technology widely used. Isolated switching technology first carries out manual data exchange, and carries out data exchange when the two networks are completely disconnected; Then there is network hardware isolation, which is to classify the power equipment separately; Finally, the network isolation switching technology is generated. This technology uses the corresponding structure model, mainly to prevent some TCP/IP protocol attacks and ensure the security of power system. Secondly, it uses the exchange memory to speed up the exchange of security information. After receiving the data, the system scans its data packets comprehensively, and obtains the required IP address, port and other relevant information according to its characteristics and data comparative analysis.

Taking the thermoelectric coupling network as an example, using the droop control method, the active and reactive power of the power network is distributed proportionally. The idea of droop control can also be used in thermal networks. According to the principle of conservation of energy, the energy output of the thermal network is:

\[ H_L = H_G - H_F \] (1)

In the formula: \( H_L \) is the load energy, \( H_G \) is the energy provided by the heat generating unit, and \( H_F \) is the line loss. The thermal pipes are usually side by side, and the resistance of each pipe to the water flow is regarded as a pipe together, namely:

\[ \frac{1}{\sqrt{S_i}} = \frac{1}{\sqrt{S_1}} + \frac{1}{\sqrt{S_2}} + \ldots + \frac{1}{\sqrt{S_M}} \] (2)

Where: \( S_i \) is the equivalent pipe area, and \( S_i \) represents the cross-sectional area of each pipe (\( i = 1,2,\ldots,M \)).

4.2.3 Identity authentication technology
Identity authentication technology is a new technology that integrates the technology of power security equipment such as parallel computing, distributed computing, virtualization technology and network storage. Identity authentication technology includes SAML based identity authentication, OAuth based authentication authorization management and openid based identity authentication technology. Taking openid identity authentication as an example, the traditional method of openid is updated, and on the basis of adapting to the original environment, the unified identity authentication of power user access is realized within and outside the domain. Secondly, according to the loopholes in the new method, the dynamic password function can be added to the new security method.

4.2.4 Quantum communication technology
Quantum communication technology belongs to the network layer of power Internet of things. It is a communication technology in which quantum bits are used as the carrier of information to transmit
data information. The biggest difference between it and traditional technology is that it uses basic mechanics and quantum principles to achieve transmission effect. Different from other technologies, quantum communication technology has the characteristics of high security, high transmission efficiency and hyperspace communication. The power Internet of things quantum communication realizes the security of data transmission through the wavelength division multiplexing technology of quantum channel and the common fiber technology of metropolitan area network. These technologies are different from traditional technologies. They can change the output pulse intensity, maintain good light intensity stability, improve the capacity of the communication network, expand the speed of the communication network, and even change the polarization state of light with the change of the environment, constantly changing various effective functions of the communication system.

5. Conclusion
There is a barrier between the external network and the internal network of the power system, which is called firewall. Firewall can operate the data information of network security to ensure the information security and network security of power system. Isolation control technology is the most commonly used technology in firewall technology. It greatly prevents the output and access outside the protected system. Some composite protection technologies make the protected information in a safe state, and dynamic filtering has a good effect. According to the operation objectives of power equipment and firewall access strategy, the address and corresponding port can be obtained, so that the current operation status of power equipment network system can be found, which adds an effective guarantee for the security of power information.

References
[1] Zhang Yiying. Research on security technology of power Internet of things [M]. Beijing: Science Press, 2016. Zhang y. research on security technology of power Internet of things [M]. Beijing: Science Press, 2016
[2] Meng Yue, Tian Xiaomeng. State Grid will be initially built in the electric Internet of things in 2021 [J]. Communications world, 2019 (8): 34-35
[3] He Ying. The importance of network security in the context of energy Internet [n]. China Energy journal, January 2, 2017. He y. The importance of network security in the context of energy Internet [n]. China Energy journal, January 2, 2017
[4] Comprehensive analysis report of attacks on Ukraine's power system [EB]. 2016