Design and Implementation of Power Network Security Protection System Based on Internet of Things

Kai Yun¹, Haosheng Li¹,* and Jia Chen¹

¹State Grid Xinjiang Infomation & Telecommunication Company, Urumqi, Xinjiang, China, 830000

*Corresponding author e-mail: lihaosheng@sgxit.com

Abstract. With the progress of society, the power industry is also constantly developing. This puts forward higher requirements for the safety of our country's power grid system. In order to ensure the stable and reliable operation of the power supply network and the economic rationality, stability and security, this article first elaborates the concept of network security and network security management, secondly, it analyzes the network security protection technology. Finally, it studies the design and implementation of a store network security protection system based on the Internet of Things.

Keywords: Internet of Things, Power Industry, Network Security Protection System

1. Introduction
Nowadays, the power industry is constantly improving. At the same time, the scale of power grid construction is getting bigger and bigger. However, due to the complex and changeable network operating environment, the large number of equipment and other factors, as well as some human improper operations, many security problems have occurred. In order to ensure the stable and efficient operation of power dispatching work, we need to conduct effective research and analysis on it and propose relevant improvement measures to solve these problems [1].

2. The power network based on the Internet of Things is completely

2.1. Cyber security
Security threats to network security come from hacker attacks. In order to ensure network security, effective defenses must be made against network security. Therefore, network security can be divided into two aspects: attack technology and defense technology. They complement each other and promote each other. On the one hand, hackers need to understand the defense technology and equipment when attacking, so that they can easily bypass the defense and attack the target. On the other hand, the defender must also master the means and methods of the attacker's attack, so as to carry out effective defense [2, 3]. Attack and defense are always a contradiction, as shown in Figure 1 is the network attack and defense security system.
2. Status quo of Network security protection
In the Internet of Things, wireless network security is particularly important. Currently, commonly used wireless sensor systems are equipped with more than two intrusion prevention strategies, and traditional data encryption can no longer guarantee network security. The intruder can join the network system by way of network intrusion, so that all the keys will be effective. Finding the intruder during the intrusion is a necessary defense method.

At present, the network has developed many security protocols. However, communication nodes in sensor networks and the Internet of Things are small in size and hardware resources are limited, so these protocols cannot be used. In recent years, there have been some advances in the research of wireless sensor network security protocols. Most of them focus on key management, denial of service, and secure routing. The main considerations in the research of the Internet of Things are the key issues of networking, energy saving, and reliability. There is relatively little work on security issues.

2.3. Internet of Things technology
The Internet of Things technology has three major characteristics: comprehensive perception, interconnection and intelligent management.

The first layer of comprehensive perception is to collect a large amount of data from the lower layer in real time through various micro-sensors to support the upper layer data [4, 5]. As shown in Figure 2 is a comprehensive perception map of diverse information.
Figure 2. Comprehensive perception of diverse information

The second level is diversified information transmission channels. Through various ubiquitous wireless network technologies, the working information and collected information of various network nodes are transmitted to the network. Diversified wireless network technologies have enriched application scenarios and application characteristics [6].

The third level is intelligent management. After obtaining various information, IOT nodes can realize local autonomous intelligent management [7]. The functional model of IOT information processing is shown in Figure 3.

Figure 3. The functional model of IoT information processing

3. Network security protection technology

3.1. Firewall technology
This technology is mainly used to isolate the public Internet from the intranet safely. The firewall scans the data flowing through the network, allows normal and legal access, and filters attacks and illegal data. The purpose and function of its organization is to establish a security control point at the network boundary, and realize the protection of the intranet by configuring security policies to allow, deny, and redirect data streams. The firewall can set the security protection strategy according to the protocol and server port to achieve access control [8].

3.2. Intrusion detection technology
This technology is essentially a real-time monitoring technology. It detects, reports, and records various attack attempts, attack behaviors, or attack results in accordance with certain security policies. When the network system is found to be attacked, it will immediately make adjustments according to the actions set by the user in advance. This can guarantee the confidentiality, integrity and availability of network system resources.

3.3. Vulnerability scanning technology
Vulnerability refers to anything that can cause damage to the security of the system, usually refers to the defects in the specific implementation of software, hardware and protocols or the system security strategy. Examples include improper operation, improper configuration, and weak passwords. This allows an attacker to access or damage the system without authorization. Vulnerabilities have the characteristics of longevity, diversity, and concealment. It can be said that any system has vulnerabilities, and there is no absolutely secure system.

3.4. Antivirus technology
A computer virus is a special computer program. It can instantly damage system files, paralyze the system, and cause data loss. The target task of virus programs is to destroy computer information system programs, destroy data, occupy system resources, and affect the normal operation of computers. At present, anti-virus software is usually used to defend against viruses in network security protection, and virus monitoring and virus killing are carried out through anti-virus software. At the same time, anti-virus software can also prevent new viruses, check and kill viruses online, and update the virus database in real time to improve virus defense capabilities [8, 9].

3.5. Data encryption technology
The main purpose of this technology is to protect the information transmitted on the network, and make the information cannot be manipulated or intercepted by attackers. Data encryption technology enables data to be transmitted on the link in the form of ciphertext, so that even if the data is intercepted, the attacker cannot obtain the true content of the information, thereby protecting the security of the information. Data encryption technology is realized through various encryption algorithms. Commonly used encryption algorithms include symmetric algorithms and public key algorithms [10].

The encryption and decryption of the symmetric algorithm are expressed as formula (1) and formula (2):

\[ EK(M) = C \]  
\[ DK(C) = M \]

4. Design and implementation of power network security protection system based on the Internet of Things

4.1. General design of power network security protection system
The overall design of the system is shown in Figure 4:
4.2. System implementation
(1) Firewall protection. In the Internet domain, in-depth protection of access from the Internet is carried out through the firewall. The firewall mainly filters data packets based on conditions such as IP address, protocol, port, time, and direction. Most of the illegal traffic from the outside will be effectively filtered to ensure the security of the server.

(2) Intrusion prevention system protection. With the change of network vulnerabilities and the development of threat attack technology, network security has become a dynamic process. Static products cannot meet the needs of network security at all. Therefore, the intrusion prevention system can improve the accuracy and comprehensiveness of the system's response to security incidents, thereby making the protection system from static to dynamic, from flat to three-dimensional.

(3) Network control protection. This can ensure the security of government network data. Strictly control information exchange with the outside world through the network control and protection system, and control content filtering, virus scanning, and file type filtering when files are transmitted through the Internet. This can prevent the leakage of sensitive information and resist attacks from external networks.

5. Conclusion
Internet technology develops rapidly, various industries are very concerned about the problem of network information security protection. This paper mainly studies the existing network problems and the design and implementation of the power network security protection system. The research and development of network security protection system has finally brought tremendous progress to the development of the electric power industry.

References
[1] Liang Song. Network protection model based on multiple security technologies [J]. Journal of Henan University of Technology (Natural Science Edition), 2009:77-80.
[2] Gong Xiaohua. Research on Network Protection Technology and Security Gateway Based on NAT [J]. Computer Knowledge and Technology, 2009:100-101.
[3] Zhu Haihai. IPSec-based network security system design and VPN construction implementation [J]. Digital World, 2017.
[4] Meng Zhijun. Hu Menglin. Design and implementation of network security early warning system based on network behavior analysis [J]. Electronic Technology and Software
Engineering, 2018:205.
[5] Gao Wenqi. Power inspection system based on Internet of Things technology [J]. Shenzhou. 2020:279-279.
[6] Xu Yong. Design and Implementation of the Forbidden City Power Monitoring System Based on the Internet of Things [J]. Intelligent Buildings and Smart Cities, 2016:69-73.
[7] Zhu Peng, Zhu Guoyi, Yang Shun, Zhou Jian. Research on power consumption management system based on ubiquitous power Internet of Things [J]. Power Demand Side Management, 2020:75-80.
[8] Cheng Weihua, Chen Yang, Zhao Lin. Design and Application of Environmental Monitoring System for Power Ring Network Cabinet Based on Internet of Things Technology [J]. Electronic Technology and Software Engineering, 2016:39-40+51.
[9] Lu Weixin. Design and implementation of computer communication network security protection system [J]. Information and Computer (Theoretical Edition), 2018:177-178.
[10] Zhang Zhiguo. Analysis of the design and implementation of a dynamic protection system for network security [J]. Science and Technology Vision, 2014:77+213.