

PAPER • OPEN ACCESS

Research on Security Problems and Defense Strategies of Power Communication Networks

To cite this article: Chi Feng *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **569** 042047

View the [article online](#) for updates and enhancements.

Research on Security Problems and Defense Strategies of Power Communication Networks

Chi Feng^{1*}, Qingping Chen², Xiang Cai², Xianjie Yang², Zhou Li², Shan Chen¹, Lisha Wu¹ and Zhongkun Hu¹

¹ State Grid Anqing Power Supply Company, Anqing City, Anhui Province, 246000, China

² State Grid Anhui Electric Power Co., Ltd., Hefei City, Anhui Province, 230000, China

*Corresponding author's e-mail: fchi@163.com

Abstract: The development direction of power systems is automation, networking and intelligence. The intranet and extranet dual network operation modes have been applied in the power system, but there are still many problems. Due to the continuous expansion of the power communication network, massive communication data is continuously generated in daily operation. At the same time, the means of attack on the power system communication network has evolved, seriously threatening the security of the power communication network. Therefore, it is necessary to further increase the research on the security and protection of power communication networks. This paper discusses the current status of China's power communication network, analyzes the main factors affecting the security of power communication networks and the security problems of power communication networks. Finally, corresponding protective measures are given to provide reference for improving the security and stability of power communication networks.

1. Introduction

At present, China's power grid construction has basically achieved comprehensive coverage and a huge area. Many modern information technology and equipment are applied in power communication networks. Power communication networks are more complex and have significantly improved communication quality and efficiency. Only when the safety of the power communication network is guaranteed can the power supply network operate efficiently and meet the electricity demand of daily production and social life. Circuits and equipment are important components of power communication networks. In these two parts, there are many hidden dangers and faults. It is necessary to focus on monitoring the corresponding parts and do a good job of safety precautions. In power communication networks, the main ways to achieve power communication transmission and service information interaction include wireless communication and cable communication. During the operation of the power communication network, the network failure has a serious impact on the distribution, adjustment and transmission functions of the power network and even causes the entire power network system to collapse, resulting in the interruption of the power communication transmission function. Further research on power communication functions and continuously strengthen the improvement of communication methods, so that the power communication network runs stably. The accessed devices include traditional computer terminal devices and devices such as mobile terminals and sensors that are currently popular. There are many compatibility problems in system architecture, etc., so there will be



more security threats. Further research is needed to introduce more advanced security defensive technologies.

2. Security issues in power communication networks

2.1. Transmission network lacks hierarchical

At present, in the power communication network, the operation management is mainly divided into three levels for the optical fiber transmission network. The first level is mainly the communication cable between the national power grid and the provincial power grid; the second level is the municipal power supply company and the provincial power grid. The communication cable between the three; the third level is the communication cable between the municipal power supply bureaus. Through the three-level division, the communication optical fiber transmission network is established, which can realize systematic and clear planning and construction. Due to the large differences in development between different regions, the erection of optical fiber networks is not strictly divided into three levels, resulting in frequent confusion between the second- and third-level communication networks.

2.2. SDH ring network structure is complex

The running speed of the power communication network has an important impact on the network function, and the communication network speed is slow, which will affect the transmission efficiency of the network information. Power companies usually adopt a three-level communication network for design, and each node uses SDH network topology to connect to ensure smooth information transmission between different regions. Due to the imbalance of regional economic development, the economic development in some regions is quite different, and there is a significant difference in the demand for electricity. In China, in some economically developed regions, the demand for electricity has increased significantly and the number of substations has increased significantly in these regions. Compared with developed regions, in some underdeveloped regions, the level of economic development is relatively low, and the number of substations is relatively small. The difference between developed and underdeveloped regions leads to a large difference in the number of SDH nodes in different regions, and the SDH ring network is not balanced, which makes the SDH ring network resistant to failure events. Greatly reduced, seriously affecting the information transmission effect of the power communication network.

2.3. The risk of a security attack on a power communication network

In modern power companies, communication networks have been isolated and three lines of defense to protect network security have been constructed to prevent unrelated personnel from controlling the power communication network and to provide security for core data. However, through the analysis of the security of power communication network equipment, it is found that there are many security risks in the power communication network. Among them, Trojan horse programs and security loopholes are the main sources of security hazards. The power communication network equipment itself has many loopholes and the communication network is attacked through these security loopholes; the vulnerability is activated by the application of electromagnetic radiation or wireless signals. Before the vulnerability is activated, the wake-up procedure needs to be set in the device to expand the device radiation standard. On this basis, the device sends relevant signals to complete the deciphering work, so that the back door can be activated; the mobile terminal is used to attack the power communication network.

3. Current status of power communication security defense

With the rapid development of science and technology, compared with the traditional power communication network, the functions of the power communication network are complicated and diversified. The power communication network can realize the transmission and conversion of electric energy, and can also complete information exchange. The functions of the power network are increasing, the dependence of the power system on the power communication network is gradually increasing, and

the requirements for the power communication network are continuously increasing. At present, all power companies in China are constantly upgrading the overall network system, thereby improving the communication transmission capacity of the power network and ensuring the reliability of the power communication network; further strengthening the construction of regional and grassroots power communication networks to make electricity. From the current development situation, China's power communication network has many shortcomings in the overall design level and system detection methods; in terms of stability, security and reliability, the power communication network is still in Lower level of development.

Power communication networks face many security problems and are often attacked by various channels. Under the support of mature software development technology, security threats such as Trojans and viruses have emerged with new features, increased supply channels, longer latency periods, and broader threats. On the one hand, they attacked grid operation data and on the other hand destroyed grid hardware devices. The power supply range is increasing, the coverage of the power grid is gradually expanding and more devices are connected to the power communication network, including wired network devices and wireless devices. The wireless devices include: mobile terminals, sensors, intelligent terminals, etc., which make Trojans and viruses. Attack channels are more extensive. The power communication network carries application software such as remote meter reading and power monitoring, which involves all aspects of power grid production and operation. When Trojans and viruses invade a certain software, other software will be infected in a short time, making Safety hazard information quickly spreads across the network, ultimately jeopardizing the entire grid system.

4. Cloud computing-based power communication security defense strategy

Cloud computing provides a data center for customized services, which enables data isolation between multiple indexes and supports multiple users from the bottom. Multiple nodes on the same network segment can be set to the same cluster name to form a distributed cluster, which constitutes a horizontal expansion mode. When the data size remains unchanged, the service resources are elasticized. In the decentralized mode of cloud computing, when the central node fails, a new node will be selected, and the new central node will be fragmented to realize data migration and ensure user data security. Cloud computing is an advanced matrix operation technology that integrates a variety of hardware and software resources to improve the computing power of the system and improving security and defense performance.

The cloud computing-based power communication security defense system integrates a security management system, an intrusion access control system, and a firewall system. In the digital application platform, the integration and sharing of services are realized, and the location of the virus is accurately detected, thereby realizing Antivirus treatment. The communication security defense system is divided into a presentation layer, a logic layer and a data layer. The power communication security defense system provides users with a cloud account as a access point for users to enter various subsystems, implementing intrusion access control, firewall, Trojan horse killing and security management; providing a platform that is easy to upgrade and maintain, without requiring users to install the client Operable, as shown in Figure 1.

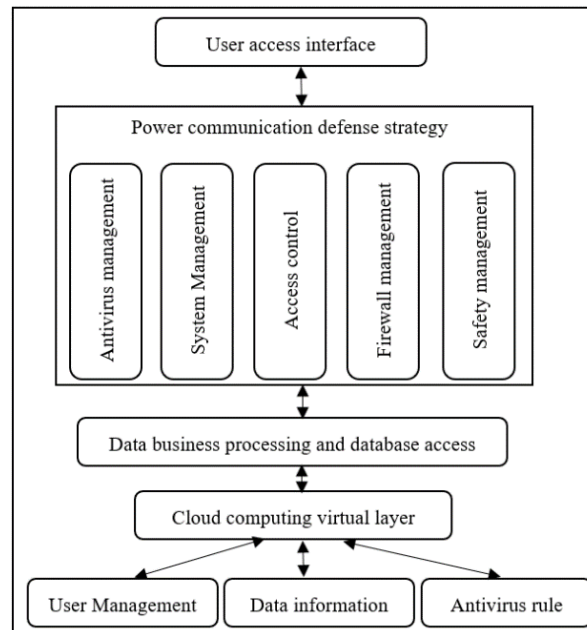


Figure 1. Cloud computing-based power communication security defense framework

The cloud computing technology is used for security defense of power communication, which can virtualize the underlying physical device resources and share the resources of the network defense system. It has good scalability and robustness, and performs real-time defense according to requirements. The power communication defense system supports online concurrent operation, forms a powerful manageable area, continuously improves processing performance, builds a batch application task model, and implements a multi-threaded anti-virus mode when a large-scale network attack occurs, thereby realizing large-scale network security defense. The power communication security defense system can effectively reduce the data exchange and analysis process, and reduce the anti-virus processing delay of the network communication, thereby improving the anti-virus defense response speed. The cloud computing-based power communication security defense system uses structured file technology to collect Internet data, adopts a scalable markup language, and utilizes security management information institutions and traffic operation modes to realize standardized operation and management of the network. The security management information base specifies Data related to network management enables formatted file pages to store various types of communication data.

After completing the data collection of the power communication network, the safety risk assessment indicators are constructed, the safety risk assessment is implemented according to the indicators and the detailed standards of the safety information level assessment are formulated, and the information processing, operation are realized according to the standard. In order to improve the accuracy of network security assessment, relevant algorithms can be introduced to integrate the minimum granularity factor for each layer of security vulnerabilities, quantify and analyze the security assessment operation function and divide the hardware and software risk data into serious, mild, general, etc. Different levels, when at a serious risk level, trigger anti-virus software to scan software and hardware systems in the power communication network to detect and kill viruses and isolate network areas.

5. Prediction of Security Status of Power Communication Network Based on Big Data

In order to ensure the safe operation of the power communication network, it is necessary to sense and evaluate the network security posture to respond to the attack behavior in real time. The security situation of the power communication network refers to the real-time status and derivation trend of the entire power communication network, which is mainly composed of the network behavior, user operation and operating status of the power communication network equipment. Therefore, the security situation is the state and trend of network operation and belongs to the global concept. In the power

communication network environment, acquire and understand the elements that may cause the network security situation, process and analyze the elements, and display and predict the development trend of the power communication network security.

In order to accurately predict the security situation of the power communication network, it is necessary to sample the operating parameters of the power communication network and obtain data indicators for the calculation of the security potential state. Through information fusion technology, a large number of power network security data are merged and merged to form a typical array. The value is called the power network security potential value. Combined with the neural network algorithm, based on the Spark mechanism, a big data calculation framework is designed, and the calculation based on massive data is used to predict the security potential of the power network. The overall framework for predicting the security situation of power communication networks is shown in Figure 2.

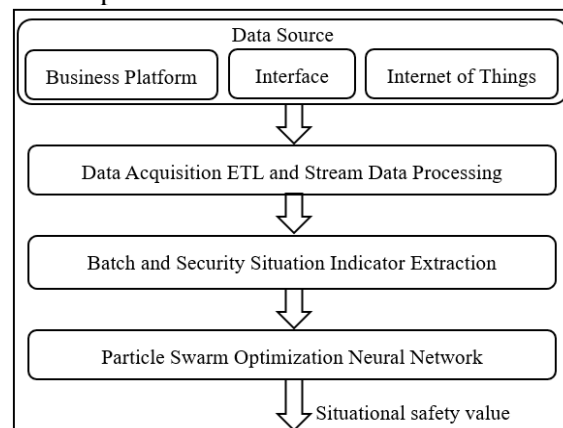


Figure 2. Grid security situation prediction big data computing framework

6. Conclusion

For the security problems existing in the power communication network, it is necessary to adopt the necessary security defense strategy. The power communication security defense is dynamic, and the defense system belongs to dynamic engineering. The structure of power communication networks is becoming more and more complex, and the types and quantities of new types of communication equipment in power communication systems are significantly increased. In the course of operation, more faults are encountered, which has a serious impact on the stable operation of power communication networks. In order to improve the security defense capability of the power communication network, it is necessary to configure security defense rules, collect power communication network data in time, and conduct risk data analysis. At the same time, it is necessary to introduce big data analysis technology to actively extract data from massive data. Further optimize the design of power communication networks to make power communication networks more complete and more reliable; strengthen monitoring and analysis of fault problems, improve fault handling speed, minimize the time for power communication network recovery and continuously optimize and improve power communication networks for power the stable operation of the system provides protection.

References

- [1] Zhong Jin. Method for improving the reliability of power dispatching communication network [J]. Electronic Technology and Software Engineering .2018(06)
- [2] Liu Yufan. On the factors affecting the safe operation of communication circuits [J]. Communication World, 2017 (23): 59-60.
- [3] Wang Kaixuan. Fault management mechanism of intelligent power communication network [D]. Beijing University of Posts and Telecommunications, 2015. [4]
- [5] Niu Bin. A discussion on the fusion technology of power communication network risk assessment and grid security operation [J]. Communication World, 2016, (23): 111-112.

- [6] Xue Yusheng, Ni Ming, Yu Wenjie, et al. Power outage defense system that takes into account communication information security warning and decision support [J]. Automation of Power Systems, 2016, 40(17): 3-12. [7]
- [8] Hu Qing, Lu Shichao, Shi Zhiqiang, et al. Advanced continuous threat cloud detection game based on expert system [J]. Computer Research and Development, 2017, 54 (10): 2344-2355.
- [9] Wang Yunan, Lin Yanjun, Li Huan, et al. Vulnerability analysis and defense of power network control system under Do S attack [J]. Control and Decision, 2017, 32(3) : 411 - 418.
- [10] Meng Jianliang, Liu Dechao. A new method for identifying bad data of power system based on Spark and cluster analysis [J]. Power System Protection and Control, 2016, 44(3): 85-91.