Design of Network Security Active Defense Mechanism for Power Monitoring System

Xiaolei Ma, Pengfei Duan and Yandong Yang
State Grid Xinjiang Electric Power Co., Ltd，Urumqi, China

Keywords: Power Monitoring, Network Security, Active Defense.

Abstract: Power Network Monitoring System is a key link in the economic and social development of our country, its network security problem is attracting more and more attention. Based on the practical background of northeast power grid, this paper proposes a new type of security system for general network security system, the network security system with "Trusted Computing as the core, safety controllable protection as the goal and safety immunity as the feature" has been applied in practice.

1 INTRODUCTION

With the gradual deepening of the security protection of the power monitoring system, each power generation company and power grid company have taken a lot of security protection measures, and installed the isolation device in the lateral transmission, separating the production control and management information, a set of longitudinal password authentication device is arranged in the longitudinal transmission part, which can verify the information between the master and the auxiliary stations. In order to realize the real-time monitoring of the security equipment and the real-time early warning, centralized visualization and comprehensive analysis of the network security events, all the security protection equipment in the power monitoring system are connected to the internal network security monitoring platform, it provides reliable data source and analysis method for power grid security evaluation, and improves the level of power grid security management and control. Figure 1 shows the general architecture of the existing internal network security monitoring platform.

The current power grid monitoring system, mainly depends on the internal network security monitoring platform, based on the grid network to build a complete network security defense system, but the internal network security monitoring platform, only the edge equipment in the secure area of the power grid and the local equipment with vertical encryption authentication are monitored, which cannot effectively monitor the equipment and system in the power grid (Shi Zhiguo, 2018). Therefore, we cannot control the source of virus and danger in the power grid, and cannot guarantee that the hidden trouble in the power grid will not be found, thus causing a series of security accidents. In a word, an effective network security active defense system is set up to detect the status of the access network equipment, so as to realize the monitoring and positioning of the access network equipment.

2 PLATFORM DESIGN

The characteristics of the power monitoring system are: the network is private and relatively closed, equipment and users are relatively stable, in the internal network or port use of proprietary internal services, the use of autonomous procedures to deal with network messages, therefore, when a user or device exceeds its authority, it may be considered a security risk. The electric power monitoring system runs on the special service network, its service type is special, the data flow direction is relatively fixed, the service system structure is homogeneous, all monitoring equipment is transmitted according to the protocol required in the power system and is managed by the grid company or power generation company. With the related technology and Management Foundation, the implementation of network security monitoring can be transferred from the edge node of the network to the network switches, routers, servers, hosts, work nodes and other specific equipment, the detection program is used to detect and deal with

Ma, X., Duan, P. and Yang, Y.
Design of Network Security Active Defense Mechanism for Power Monitoring System.
DOI: 10.5220/0012281200003807

In *Proceedings of the 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (ANIT 2023)*, pages 275-279
ISBN: 978-989-758-677-4

various security risks such as malicious attacks and program tampering as early as possible from the events and behaviors of the devices and personnel connected in each network (Ma Jianwei, 2018). Therefore, it is necessary to establish a network security management system that organically combines "Perception recognition", "Collection-induction" and "Management-control".

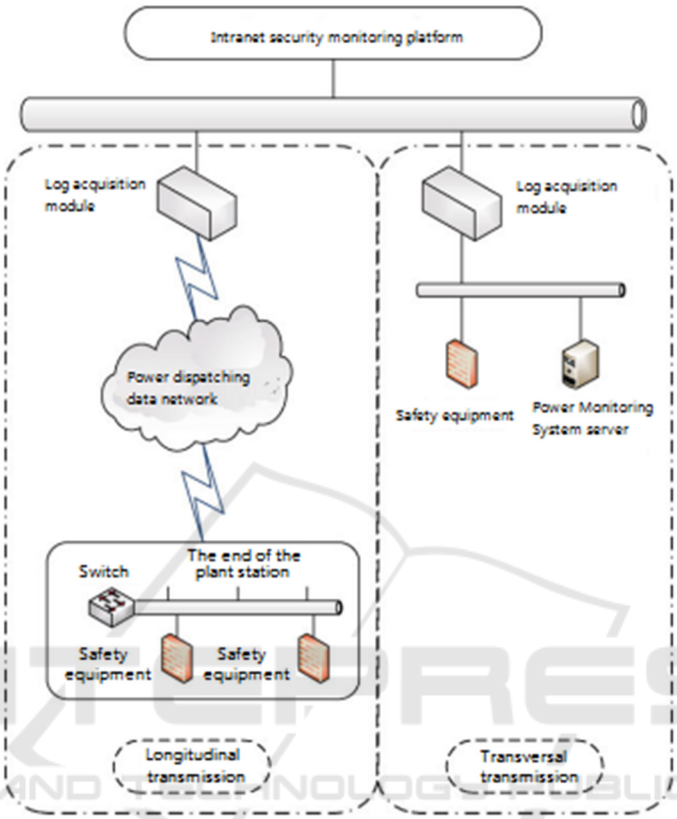

Fig. 1. Architecture of intranet security monitoring platform.

The main technologies used are:

(1) The principle, Method and technology of a network device-oriented self-perception-based security event. Through the security awareness of each device in the network, the potential dangerous events can be detected quickly and accurately.

(2) Data acquisition, transmission and aggregation technology based on the security of monitoring equipment. By setting up a security monitoring device in a network, we can complete the collection, analysis and processing of the network threat data in the device collection area, and the analysis results will be transmitted to the higher level of network security information synthesis and management platform.

(3) Collaborative design of management platform and control system under hierarchical deployment. It realizes the distributed management of online monitoring, real-time early warning, accurate analysis, check, audit and control of network security.

According to the above description, the power system network security management platform designed in this paper is shown in Figure 2 below.

The substations and power plants in Figure 2 are intended to set up a network security monitor, which collects and collects local security information and reports to the above dispatch platform. The communication transmission between the management platforms at all levels and between the management platforms of substations and power plant equipment is based on the power dispatching data network of the National Grid, and in order to ensure the reliability and security of the data, a special VPN is also used for data interaction.

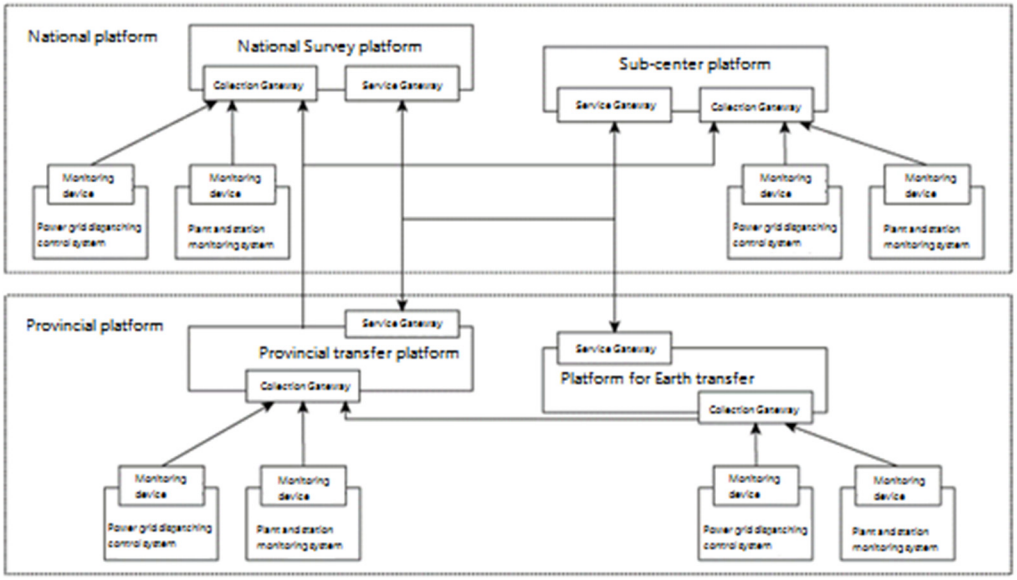

Fig. 2. Overall design of network security management system.

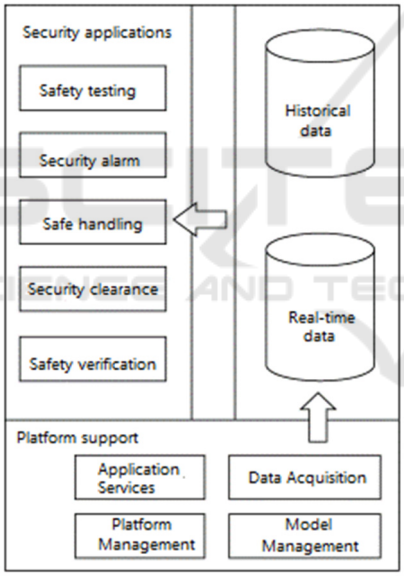

Figure 3. The overall architecture of network security management.

In the data collection of security events, our platform uses a set-oriented collection method, which changes the original way of analyzing and mining the packets spread in the network, it provides a new monitoring method for network security events (Sudan, 2018). In particular, the method is based on the operating system of the local host and the devices and components connected with the network to collect the security data of the events related to the network device On the basis of control and transformation data network connectivity, between systems such as plant, power plant, master control system, load control system and distribution network service system, to achieve the unified control of network security events. Based on the above research, the integrated management and control functions of centralized verification, monitoring, processing and auditing of information security events will be realized, and a complete set of system framework and security application services oriented to power consumption business will be formed, to ensure that the system's security monitoring function in the correct use of multiple dimensions. To sum up, the overall function of the NCS system established in this paper needs to combine 4 types of security support modules with 5 types of integrated application modules. 4 major security support modules, namely: Security Data Collection, model design, platform function management, application integration services, it provides the basic functions of platform for communication analysis, service access and registration request of platform basic security data. 5 comprehensive applications, including: Network Security Event Monitoring, security alarm and processing, security audit and verification. In order to meet the demand of network security and control function of the new generation power monitoring system, the platform function designed in this paper can be as shown in Figure 3.

With the above architecture, the following functional requirements are implemented:

Security monitoring, extending from dedicated protection devices at the edge of the network to all servers, workstations, network devices, and other

infrastructure in the network area of the overall network security management architecture shown in Figure 3. (2) the monitoring of network security events has changed from the original monitoring of Edge events to an all-round and overall monitoring, covering both internal and external aspects of unsafe behavior (Gu Zhuoyuan, 2019). (3) from simple monitoring and early warning, to network security analysis and location, traceability processing, Audit and verification, interactive management. (4) a network integrated security management mode from "Edge monitoring, static control" to "Comprehensive monitoring, dynamic real-time management".

3 PLATFORM APPLICATION

The implementation of the platform follows the overall design principle of hierarchical deployment and cooperative management, and the network security distributed management platform is configured to all levels of regulatory agencies, and the network security monitoring equipment is configured to all plant stations, thus, a new and comprehensive network security management system is formed, which can cover the whole power network.

(1) to increase the monitoring and collection of mainframe services, data exchange equipment, network security equipment, database operation and alarm information in the power monitoring system, the security events of the monitoring target are recorded and analyzed to provide the data basis for the cooperative protection of the whole network. (2) plant and station monitors shall be installed in fossil-fuel power station stations and substations to collect and manage them, so as to supplement the deficiencies of safety management methods for their equipment and systems. (3) providing an interface for daily operation, centralized monitoring and management of the software and hardware operation status of the power monitoring system, and providing recording functions such as Operation Information and alarm information, provide effective data tracking support for problem resolution and traceability (Chen Wuhui, 2019). (4) by verifying the security configuration of the host computer and evaluating the security risk, it is easier to find the security defect of the host computer, so that the security work is changed from passive defense to active monitoring. (5) it provides an effective management method for the occurrence and disposal of security incidents, which can manage the whole life cycle of security incidents from occurrence to disposal, and monitor the operation of resources in real time. With the ability to view data and topology, from passive reception to active monitoring; a unified management of threats and vulnerabilities.

4 CONCLUSION

The construction and effective operation of network security management platform is the basic technical means to improve the ability of network security situation awareness, early warning and emergency response, it is also the primary work of network security system of electric power monitoring system. Compared with the previous generation internal network security monitoring and management platform, a power monitoring and management platform based on Trusted Computing, security controllable, security immune, the utility model can play a more efficient safety protection effect in the practical application.

ACKNOWLEDGEMENTS

This work was supported by New generation of dispatching technology support system.

REFERENCES

Shi Zhiguo, Computer Network Security Tutorial (M). Second edition. *Beijing: Tsinghua University Press*, 2018.

Ma Jianwei, Wan Huijiang, Wang Xiangdong. The present situation and improvement method of network security of electric power monitoring system (J). *Information and computing (theoretical edition)*, 2018(22): 193-194.

Sudan, Yang Rui, Wu Jia, etc. Design and application of monitoring model for electric power information communication system (J). *Science and Technology Bulletin*, 2018(8): 164-167.

Gu Zhuoyuan, Tang Yong, Sun Huadong, etc. Response-based power system security and stability, integrated defense technology (J). *Chinese Journal of Electrical Engineering*, 2019, 39(4): 196-204.

Chen Wuhui, Chen Wengan, Xue Ancheng. Physical power system for cooperative information attack, system security risk assessment and defense resource allocation (J). *Grid technology*, 2019(7): 2353-2360.

Xue Mei Hou. Noise-Robust Speech Recognition Based on RBF Neural Network (J). *Advanced Materials Research*. 2011， VOL. 217-218: 413-418

Maha El Meseery,Mahmoud Fakhr El Din, Heba El Nemer. A Hybrid Particle Swarm/Nelder-Mead Clustering Algorithm for Face Recognition (J). *International*

Journal of Artificial Intelligent Systems and Machine Learning, 2011, 3(10)

Tomo MIYAZAKI, Shinichiro OMACHI. Representative Graph Generation for Graph-Based Character Recognition (J). *Journal of the Institute of Image Electronics Engineers of Japan*. 2011, 40(3):439-447

Pei Ye,Tao Jiang. Research on Unconstrained Handwritten Numeral Recognition by BP Feature Screening Based on Fuzzy Clustering (J). *Applied Mechanics and Materials*, 2015 VOL. 734: 504-507