Chapter 16
Construction of Security Control and Protection of Internal and External Networks of Communication Terminals Under the Heterogeneous Network Environment

Jian Zhang, Ying Zeng, Bo Li, Xingnan Li, and Zhan Shi

Abstract The construction of network security control and protection system of internal and external communication terminals under the heterogeneous network environment can promote the research and development of power network security technology, promote the information construction and intelligent upgrading of the power grid, and improve the overall operation level and competitiveness of the power grid. Based on this, this paper proposes the construction of security control and protection of communication terminals under the heterogeneous network environment of the power grid. By analyzing the condition of grid heterogeneous network environment, the communication terminal network security control system to build design, build the network isolation, certification and authorization, traffic monitoring, and security reinforcement, in order to improve the network heterogeneous network environment communication terminal network security control efforts, comprehensive guard against all kinds of network attacks or malicious software intrusion, improve the overall security performance of power grid system.

16.1 Introduction

Heterogeneous network refers to the network environment composed of multiple different types of networks, including the traditional wired network and wireless network, as well as all kinds of new networks such as the Internet of Things and 5G. Surrounded by the multiple network environment, the security control and protection of the internal and external networks of communication terminals is particularly important [1]. The security protection system designed in the internal and external

J. Zhang (✉) · Y. Zeng · B. Li · X. Li · Z. Shi
Electric Power Dispatching and Control Center of Guangdong Power Grid Co., Ltd., Guangzhou 510000, China
e-mail: minwell@126.com

R. Kountchev et al. (eds.), *Proceedings of International Conference on Artificial Intelligence and Communication Technologies (ICAICT 2023)*, Smart Innovation, Systems and Technologies 369, https://doi.org/10.1007/978-981-99-6956-2_16

network of the communication terminal can effectively carry out real-time monitoring and security protection of the power grid, which is conducive to ensuring the overall safe and stable operation of the power grid, and can improve the reliability and security of the power grid to a certain extent [2]. Based on this, according to the current needs of the power grid, the overall design of the security control and protection system under the heterogeneous network environment. By constructing the full aspects of the system, enhance the security of data transmission and user authentication from the authentication and authorization design. By monitoring the data flow of the power grid, realize the functional requirements of the system to automatically identify and handle the power grid security events. If a problem occurs, the security audit system can promptly issue alarms and address the corresponding issues, thereby enhancing the efficiency of power grid security management and emergency response. It helps to safeguard against various types of cyber attacks and malicious software intrusions, protecting network and information security.

16.2 Overall Design of the Security Control and Protection System

Under the heterogeneous network environment of the power network, the network environment involved includes internal network, public network, Internet of things, etc., the characteristics of the network environment are different, with the deepening of the power grid information construction, the power grid is facing increasing network security threats, the power grid contains a large number of key information, Such as: energy production, transmission and distribution, equipment operation and other data, once such data leakage or damage will cause serious impact and loss on the operation of the power grid [3]. To strengthen the power grid communication terminal network's internal and external security, to prevent all kinds of network attacks or malicious software intrusion, through the communication terminal network's internal and external security protection system construction, the control system can realize from the application layer to the network layer comprehensive security protection, improve the use of the overall network security and stability, protect the information security of communication terminal, reduce manual intervention, improve the management efficiency, shorten the troubleshooting time [4]. The general design of the security control system of internal and external networks of communication terminals under heterogeneous network environment is shown in Fig. 16.1.

As can be seen from Fig. 16.1, the security control system of the communication terminal is constructed by the application layer, system layer, data layer and network layer respectively, the application layer contains various applications and security management control platforms, mainly responsible for implementing various security functions such as authentication, access control, security audit, etc.; the system layer is various operating systems and system management tools, It is mainly responsible for providing basic system resource management and security control functions,

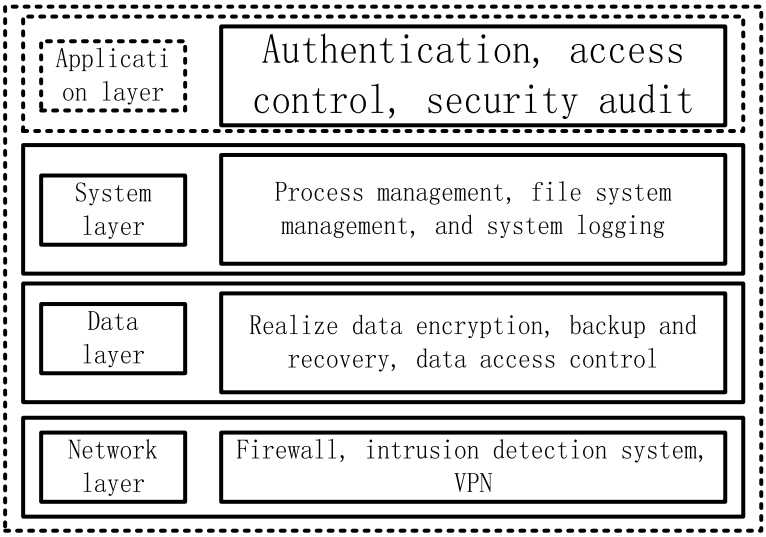

Fig. 16.1 General design diagram of the internal and external network security control system of the communication terminal

such as process management, file system management, system logging, etc. [5]. The data layer includes various data storage and management tools, mainly responsible for realizing data encryption, backup and recovery, data access control and other functions to ensure the security and reliability of data; the network layer is various network equipment and security protocols, mainly responsible for realizing the security and reliability of network communication, such as firewall, intrusion detection system, VPN, etc. [6].

16.3 Software Design

16.3.1 Internal and External Network Isolation

Network isolation and security authentication are the key steps in guarding against cyber attacks and data leakage. Filter and control of network traffic through network devices, to realize the physical isolation and logical isolation between different network areas, its purpose is to prevent attackers from spreading viruses, Trojan horses and other malicious code through the network, so as to avoid damage to terminal devices [7]. By deploying the Virtual Private Network (VPN) server, the data of the internal network is encrypted, the VPN client is installed on the terminal device of the internal network, and configured to establish a secure communication tunnel with the VPN server. When the internal network terminal devices request the

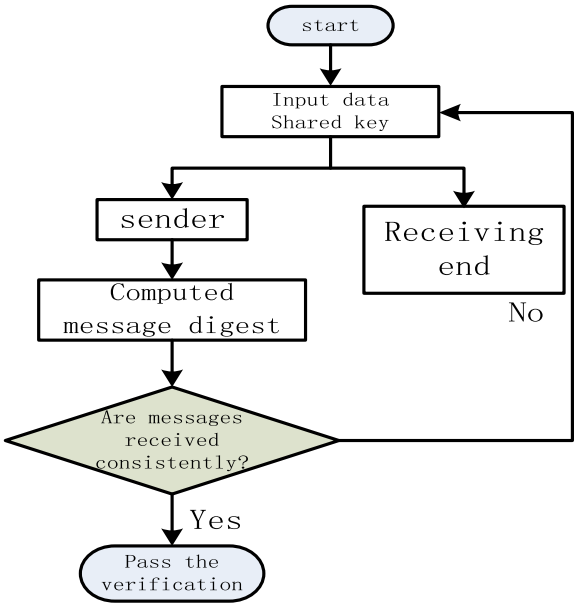

Fig. 16.2 SHA-2 authentication process

VPN server through the VPN client to establish the secure communication tunnel. After establishing the VPN connection, the data transmission between the internal network terminal device and the external network will be encrypted to ensure the confidentiality and integrity of the data transmission [6]. The SHA-2 encryption hash algorithm in the communication side can be verified by the configuration in the VPN device. Its implementation process is shown in Fig. 16.2.

According to Fig. 16.2, the process of SHA-2 authentication is realized by sharing the key in the communication. During setting up the key, note that the key should be sufficiently long and complex. To ensure safety, during the communication process, the sender takes as input the data to be sent and the shared keys and calculates a message summary using the SHA-2 algorithm. The sender sends the calculated summary of the message to the receiver [8]. After the receiving party receives the message, also takes the data to be received and shared keys as input, calculates a message summary using the SHA-2 algorithm, the receiver compares the calculated message summary with the message summary sent by the sender. If the same occurs, the authentication is considered to have passed. Otherwise, the authentication is considered to fail [9].

16.3.2 Communication Terminal Authentication and Authorization

The secure communication between the communication terminal and the authentication server can be realized using the TLS/SSL protocol. The communication terminal applies for a certificate from the authentication server [10]. After verifying the identity of the communication terminal, the authentication server generates the certificate and returns it to the communication terminal. The certificate contains the public key of the communication terminal and the public key of the authentication server, and the authentication and authorization structure are shown in Fig. 16.3.

During the TLS/SSL handshake process, the communication terminal and the authentication server exchange information such as the certificate and encryption algorithm, and conduct authentication and key negotiation [11]. The communication terminal and the authentication server use the symmetrical key generated during the handshake process to encrypt and decrypt the communication data to ensure the confidentiality and integrity of the communication. The communication terminal and the authentication server need to configure the TLS/SSL protocol to ensure the security of the protocol. The configuration items include the password suite, key length, certificate expiration time, TLS version, etc. Before transmitting the data, the communication terminal needs to encrypt the data, and the authentication server needs to decrypt the data. After receiving the data, the authentication server needs to verify the data to ensure the integrity of the data and the legitimacy of the identity. During the communication process, abnormal situations of TLS/SSL handshake failure, certificate verification failure, and key negotiation failure may occur [12]. The communication terminal and the authentication server need to handle such abnormal situations and take corresponding security measures, such as connection interruption, recording and logging, etc.

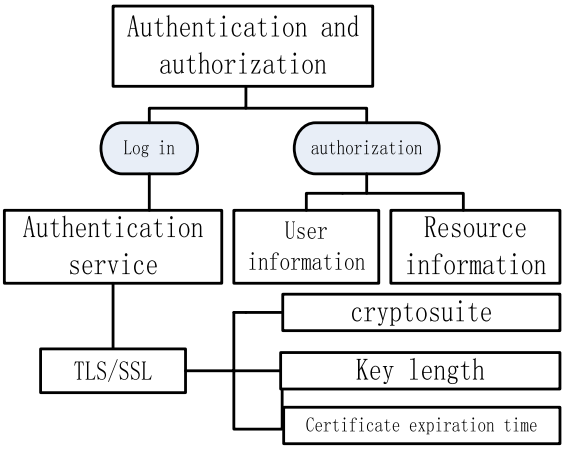

Fig. 16.3 Communication terminal authentication and authorization structure

16.3.3 Data Traffic Monitoring

Using tcpdump can monitor the security control of internal and external networks of communication terminals in the heterogeneous network environment. In Linux system, use sudo apt-get install tcpdump command and use ifconfig command to view the network card, IP address, MAC address and other information network interfaces. According to the network interface required to be monitored, select the corresponding network card for monitoring [13]. With the tcpdump command, you can set the corresponding filtering rules according to the protocol, source IP address, target IP address, port and other information to be monitored, and then start the network traffic monitoring and record the corresponding data. The Wireshark network protocol analysis tool is used to analyze the captured data, find abnormal traffic, determine network performance problems, find security vulnerabilities, etc., according to the monitoring data analysis results, and realize the system alarm and defense measures [14]. Its test method is shown in Fig. 16.4.

Using Wireshark analysis and detection, we can effectively detect and defend against network security problems. After opening the Wireshark software, select the network interface from which you want to capture packets and start capturing.

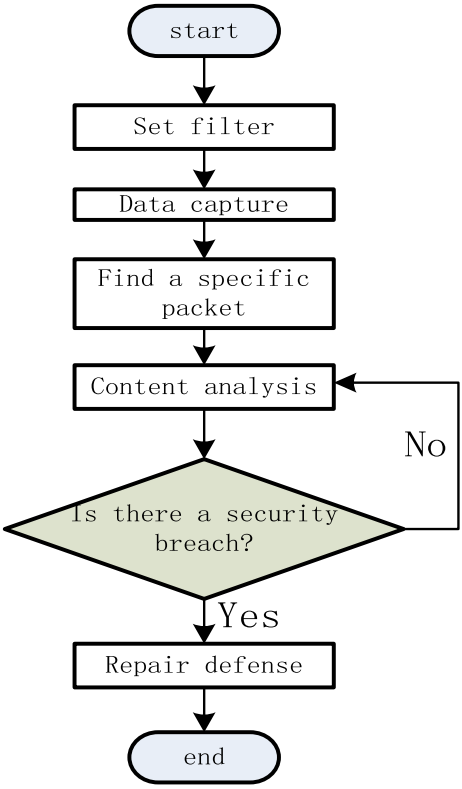

Fig. 16.4 Wireshark Flow chart of network protocol analysis

Wireshark will listen to the selected network interface and display the captured packets [15]. By using Wireshark's filtering capabilities, you can selectively display the packets of interest. The filtering expressions allow you to limit the displayed packets based on criteria such as source/destination IP addresses, port numbers, and protocol types. For example, filtering packets with the source IP address of 192.168.0.1: ip.src = = 192.168.0.1; filtering packets with source or destination port numbers of 80 or 443: tcp.port = = 80 or tcp.port = = 443; filtering packets with the TCP protocol: tcp. By using Wireshark's analysis features, you can inspect the captured packets and identify potential security vulnerabilities through packet analysis. Based on the analysis results, you can then set up alert rules to implement the system's alerting functionality.

16.3.4 Safety Reinforcement

To set alarm rules, you must first determine the monitoring and alarm targets. These include abnormal traffic, abnormal behavior of specific protocols, and security vulnerabilities. Second, the packets captured by Wireshark are analyzed and noted for potential security issues or patterns of unusual behavior. For example, frequent connection attempts, a large number of error packets, abnormal packet sizes, and so on. Based on the analysis results, you can define alarm rules to detect and trigger alarms. Alarm rules can be based on specific packet characteristics, traffic modes, and protocol behaviors. For example, "If an unauthorized access attempt (such as an unknown IP address) is detected, an alarm is triggered; an alarm is triggered if the abnormal behavior of a specific protocol, such as an abnormal HTTP request or DNS query, is detected. This section describes how to configure alarm rules in the system to implement the alarm function. Then, determine the severity of the alarm and the notification method. Alarm levels can be classified into different severity levels to facilitate alarm classification and handling [16]. Alarms can be notified by email, short message, or instant message to ensure that related personnel receive alarm notifications in a timely manner. Finally, periodically evaluate the validity and adaptability of the alarm rules. This section describes how to update and optimize alarm rules based on the actual situation and experience to improve alarm accuracy and reduce the false positive rate.

16.4 Conclusion

In the heterogeneous network environment of the power grid, the internal and external network is of positive significance for the long-term construction of power grid. Through adopting modern security management technologies, such as VPN, tcpdump and AES, it can effectively collect, process, visualize and analyze various types of log data to help power grid administrators quickly discover security threats and

abnormal events. At the same time, with the help of advanced network isolation, certification and authorization and other security technologies, the comprehensive security protection and control of the internal and external networks of communication terminals can be realized to ensure the stable operation of the power grid in the heterogeneous network environment of the power grid. In the future, further exploration and application of emerging security technologies such as blockchain, AI, and machine learning can be conducted to continuously enhance the level of power grid network security and ensure the reliability, security, and stability of the power grid.

Acknowledgements This work is supported by The Key Science and Technology Project of China Southern Power Grid Co., Ltd. (036000KK52220038).

References

1. Zhao, H.S., Sun, J.J., Peng, Y.H., et al.: Radio power terminal identification method based on multiscale windows and regional attention residual network. J. Electr. Technol. **38**(01), 107–116 (2023)
2. Huang, J.T., Wang, Z.Y.: Design of electric power safety production monitoring system for real-time data analysis. Energy Environ. Prot. **44**(12), 256–261 (2022)
3. Li, Y.C., Yang, H.F., Cui, J.B., et al.: D2D communication security and reliability analysis of power 5G network based on the nearest location relay selection strategy. Comput. Appl. **42**(S2), 168–174 (2022)
4. Kang, C.Q., Chen, Q.X., Su, J., et al.: Scientific problems and research framework of large-scale flexible resource virtual power plant. Autom. Electr. Power Syst. **46**(18), 3–14 (2022)
5. Qian, W., Liu, S.S., Sun, J.Y., et al.: Design of power data monitoring and management system based on component security situation awareness. Big Power Data **25**(08), 76–83 (2022)
6. Wu, Q.: Thinking on security problems in embedded communication system design based on Zigbee—Review of zero trust network: building security system in untrusted network. Chin. J. Saf. Sci. **31**(09):199 (2021)
7. Li, Y.F., Liu, R., Cao, L.J., et al.: Research and practice of power mobile application and terminal security traceability management and Control technology. Inf. Secur. Commun. ConfidIty. **08**, 94–100 (2022)
8. Lan, Z., Wu, F.R., Yu, X.P., He, D., Tu, C.M., Xiao, F.: Transient instability analysis and stability strategy research of isolated island microgrids containing heterogeneous micro sources. Power Grid Technol. 1–16 (06–26) (2023)
9. Ma, X.M., Dong, C., Mao, X.Y., Jiao, Y.X., Li, H.: A method for compressing and storing massive multi heterogeneous smart grid data based on state estimation. Mot. Control. Appl. **50**(02): 67–72+81(2023)
10. Lan, Z., Diao, W.Y., Zeng, J.H., He, D., Tu, C.M., Jiang, F.: Pre synchronization control strategy for virtual synchronous generators in heterogeneous micro source isolated island microgrids. Power Syst. Autom. **46**(19), 154–161 (2022)
11. Chen, X., Xin, Y.Z., Zhao, W.Y., Sun, B.Y., Talipeng Nurbaheti.: Multi source heterogeneous data fusion model for smart early stage platform of power grid construction. J. Electr. Power, **37**(01): 76–83 (2022)
12. Qiu, H.J., Lian, G.X.: Design of power grid security perception system based on heterogeneous dual active data model continuity multilevel indicators. Microcomput. Appl. **37**(08), 197–200 (2021)

13. Peng, Y.L., Huang, W., Shuai, Z.K.: Research on instantaneous active power distribution of isolated island micro grid with heterogeneous micro sources. J. Electr. Eng. China **41**(15), 5167–5179 (2021)
14. Leng, O.Y., Hui, Q., Song, Y.P., Sun, P.: Optimal control model for power output of transmission end grid considering uncertainty and data heterogeneity of renewable energy. Renew. Energy **38**(08), 1116–1121 (2020)
15. Xu, D.M., Li, Z., Cui, G.Z., Hao, W.J.: Distributed finite time secondary control of heterogeneous battery energy storage systems in isolated microgrids. Control. Decis. **36**(08), 2034–2041 (2021)
16. Yan, M.Q., Leng, D., Liu, W.: Research on load balancing algorithm for heterogeneous wireless networks in smart grid based on matter element analysis. Commun. Power Technol. **36**(09), 114–115 (2019)