Optimization of Network Security Management and Protection Mechanism in Smart Grid

Haobo Liang*, Yingxiong Leng, Jinman Luo, Jie Chen, Xiaoji Guo
Dongguan Power Supply Bureau, Guangdong Power Grid Corporation, Dongguan, Guangdong, China
**Corresponding Author.*

Abstract: Smart grids significantly improve the reliability, security and efficiency of power systems by integrating network and information technology with power systems. However, in a highly informatized and interconnected environment, smart grids also face increasingly complex and evolving cybersecurity threats. This paper mainly analyzes the characteristics and architecture of the smart grid, describes the common security vulnerabilities of smart grid network security from the level of network and data operation security, and puts forward an optimized protection mechanism in a targeted manner to enhance the overall security performance of smart grid. This paper expects to provide a theoretical basis for the security of the smart grid, so as to promote the safe development and application of the smart grid.

Keywords: Smart Grid; Network Security; Network Attack; Protection Strategy

1. Introduction

Over the past few decades, the demand for electricity in all countries has climbed dramatically in response to global climate change and dramatic population growth. However, for most countries around the globe, growing demand for electricity also means placing greater burdens on traditionally old, overloaded, and fragile power infrastructures. This growing demand and the complex nature of power networks have led to many network congestion and security issues. Traditional power networks lack effective communication, monitoring, troubleshooting, and automation mechanisms, making it difficult to cope with single points of failure in the network leading to cascading effects and significant security threats.

In order to solve the above problems, Smart Grid has emerged, which is a critical national infrastructure whose security directly affects the country's economic and social stability. Smart Grid infrastructure, such as smart sensors, real-time data collection systems, automation equipment and distributed energy systems, makes the operation of the grid more flexible, but also greatly increases the potential risk of cyberattacks. Compared to the traditional power network smart grid integrates bidirectional and secure information, communication technology and computational intelligence in all aspects of power generation, transmission, transformation, distribution and consumption, so as to realize rational scheduling and security assessment of power resources [1].

Smart grids add new Information and Communication Technology (ICT) functions and features to traditional power systems. While these features facilitate the monitoring, scheduling and management of the grid, they also bring new security risks. In smart grids, vulnerabilities may exist in SCADA systems, phase measurement units (PMUs), and remote terminal units (RTUs), including lack of firewalls, misconfigurations, lack of security audits, insufficient security measures, and improper authentication, which can lead to the failure of the entire smart grid system and make it a target for attackers. Attacks on smart grids may include intrusion into sensitive user data, dissemination of malware, damage to communication equipment, injection of false information, and attack or modification of monitoring and control equipment, all of which may jeopardize the operation of the grid and lead to power interruptions, etc., which may have serious socio-economic consequences, and may even compromise national security. On August 14, 2003, a large-scale power outage occurred in parts of the U. S. and

Canada. power outage in parts of the United States and Canada. The accident left about 50 million people affected and caused economic losses of between $4 billion and $10 billion and nearly $2. 3 billion CAD to the U. S. and Canada, respectively [2]. In 2009, there was an attacker who injected malicious code into the U. S. power grid and remotely controlled its seizure, which ultimately paralyzed the power system in some parts of the U. S. [3]. In March 2019, hackers exploited known vulnerabilities in the Cisco firewall to launch a denial-of-service (DoS) attack against the Renewable Energy Electricity Company in the US state of Utah. Service (DoS) attack. The incident affected California (Kern and Los Angeles counties), Utah (Salt Lake), and Wyoming (State of Wyoming); and in June 2020, Light S. A, a Brazilian electric utility, was attacked and its ransom of $14 million was extorted by hackers, which was analyzed by AppGate's security researchers as the Sodinokibi ransomware software [4]. Therefore, the security of smart grids is still an urgent problem related to the economic and social stability of the country.

This paper analyzes in depth the key features and architecture of the smart grid, focusing on the common security vulnerabilities that the smart grid may face at the level of network and data operation security. By elaborating on the current security challenges, this paper proposes a series of targeted optimization strategies aimed at strengthening the system's protection capability and enhancing the overall security of smart grids. These strategies cover a wide range of aspects from network access control to data encryption and protection, aiming to ensure the stable operation of the power grid and the safe transmission of data, and provide a strong guarantee for the sustainable development and efficient operation of the smart grid.

2. Architecture and Characteristics of Smart Grids

2.1 Architecture of the Smart Grid

Smart grid means smarter generation, transmission, distribution, and integration of users, operations, markets, and service providers. The biggest difference between the Smart Grid and the traditional grid is its bi-directional interactability, i.e., the two-way flow of power and information. While the traditional grid is a unidirectional system where power plants are unable to obtain timely feedback from the user side to adjust their power supply strategies, the smart grid is a two-way adjustable network that analyzes user information to formulate power supply strategies, smooth out peaks and valleys, enable more efficient integration of fluctuating renewable energy sources, and minimize the cost of power generation. The infrastructure of Smart Grid contains the power production, transmission, distribution and usage segments in the traditional grid, in addition to the segments of information transmission. IEEE proposes the basic architecture of Smart Grid (Figure 1[5]) based on the NIST conceptual model [6], which consists of 8 logical domains and 32 sub-domains, in terms of the main business processes of Smart Grid [5]. Among them, all the domains can interact with each other in both directions, while the generation, transmission, distribution and user domains can carry out the two-way flow of information and power.

The smart grid's communications network connects the grid, service providers and users, with communications taking place over many different channels and protocols. The integration of smart meters, sensors, and control devices in the Smart Grid makes the grid more flexible and intelligent, with advanced metering infrastructures (AMIs) connecting customers to the communications network, and smart meters providing electricity usage, outage, and tariff data to suppliers. In addition, the Smart Grid includes various operational management components, such as an Energy Management System (EMS) for transmission and a Distribution Management System (DMS) for distribution, and the entire transmission network is monitored and controlled through a Supervisory Control and Data Acquisition (SCADA) system. Since the information flow of the smart grid is distributed in a wide range of segments from power production to consumption, the “cyber-attack interface” in the power system is greatly broadened, and its advanced automation and communication functions expose the whole system to cyber threats with various security limitations and loopholes. In smart grids, vulnerabilities may exist in SCADA systems, Phase Measurement

Units (PMUs), and Remote Terminal Units (RTUs), including lack of firewalls, misconfiguration, lack of security audits, insufficient security measures, and improper authentication, which can lead to the failure of the entire smart grid system and make it a target for attackers. Attacks on smart grids may include intrusion into sensitive user data, dissemination of malware, damage to communication equipment, injection of false information, and attack or modification of monitoring and control equipment, which may jeopardize the operation of the grid and lead to power interruptions, etc., and may have serious socio-economic consequences, or even compromise national security.

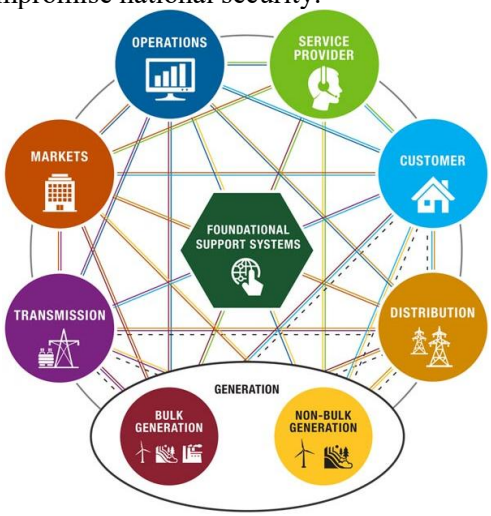

Figure 1. IEEE Smart Grid Architecture

2.2 Characteristics of Smart Grid

Smart grid is developed from the traditional power grid through technological innovation, which is the main direction of the current power grid development [7]. The characteristics of modern smart grid can be summarized as the following, strong, integrated, compatible, economic and humanized. Different from the performance of ordinary power grids, the smart grid can do a good job of real-time monitoring and analysis of grid operation data, can automatically determine the grid operation faults and make some fault warnings, in the event of grid operation faults, the strong characteristics of the smart grid allows it to quickly make remedial measures in a short period of time, disconnect the faults, and realize the restoration of the grid by virtue of its unique performance, which will Reduce the probability of widespread power failure, as far as possible to create a more stable power environment. Secondly, the smart grid focuses on the integration of circuit data, which can make the power grid system more standardized and unified, and is conducive to improving the efficiency of the power grid industry. In addition, the smart grid has high attainments in compatibility, and can effectively utilize new energy generation. Smart grid also has economic performance and humanized service mode, these characteristics will make the smart grid is accepted by more users in society.

3. Key Challenges of Network Security Management in Smart Grids

Smart grids are complex systems that integrate physical networks, information technology, and operational technology and interact with other infrastructures. Therefore, security vulnerabilities may exist in its own grid system as well as in external systems connected to it.

this, its security vulnerabilities may exist in its own grid system as well as external systems connected to it, mainly physical vulnerabilities, information technology and operational technology vulnerabilities, data management vulnerabilities, service and application vulnerabilities, etc., as summarized in Table 1 [8-10]. These vulnerabilities may have a direct or indirect impact on grid security, leading to a variety of consequences such as power outages, economic losses, or in severe cases, affecting the entire grid and causing significant losses.

As one of the important products under the background of China's Internet development, the current smart grid brings a lot of convenience to people's daily life and work, and at the same time promotes the rapid development of the entire urban economy. However, due to the overall structure of the smart grid process has a strong complexity, in the use of the process will inevitably appear a variety of security risks, the relevant staff of the smart grid for many years to summarize and analyze the work experience, that the smart grid in the operation of the process of the following types of network security issues:

3.1 Network-Level Issues

The smart grid system, which combines information technology and operation technology, relies on complex communication networks and data exchange to realize remote monitoring, management and control. A

vulnerability or weakness in the system may become an entry point for attacks. The following are several common security vulnerabilities:

Table 1. Security Vulnerabilities in the Smart Grid

Type	Description	Characteristics or impact
Physical Vulnerabilities	Vulnerabilities in various physical components of the smart grid, such as inadequate monitoring, damaged components, substation redundancy constraints, and deficiencies in the grid operating environment	Problems that exist with the traditional grid may be overlaid with cyber attacks in a smart grid environment, resulting in larger impacts
Information Technology and Operational Technology Vulnerabilities	With the application of information and operation technologies in the power grid, there are vulnerabilities in the hardware/software of the relevant smart devices; various communication technologies and protocols used in the smart grid may also have various vulnerabilities, which can become a channel connecting external attacks and internal operation systems	Vulnerabilities that increase as smart grid information and operational systems evolve and have the potential to threaten the entire network
Data Management Vulnerabilities	Smart grids need to collect and manage real-time data from a large number of nodes, and there are many vulnerabilities in the process of collecting, analyzing, processing, and maintaining massive amounts of data	Wide-area network-based data exchange between entities can be a major cause of network vulnerability, and most smart grids have deficiencies in data security and privacy management, as well as a lack of specialized protection technologies for data specific to the smart grid sector
Service and Application Vulnerabilities	Vulnerabilities in digital services and applications provided by smart grids such as demand-side management, distributed generation resource management, transmission and distribution automation, etc., such as obsolete operating system versions, incorrect maintenance documentation, lack of patch policies and maintenance updates, lack of intrusion detection systems, improper authentication, and insufficient device and system compatibility	These vulnerabilities are inherent in the information technology used by smart grid services and applications

3.1.1 Hacker attacks

In the smart grid, there are often some software and hardware vulnerabilities, and they provide an opportunity for hacker attacks. Once hackers find vulnerabilities in smart terminal equipment, they can easily launch attacks on smart grids, which can cause security problems such as overall power outages, grid overloading, electricity theft or false reporting of electricity consumption. Specifically, first, because smart grid devices can track the current in an entire building, hackers often take advantage of this to block the current or cancel service, and sometimes can infect systems other than the grid in which they are located, resulting in an overall power outage for multiple grid systems. Secondly, as smart grid equipment can generate and transmit power according to the actual demand for electricity to ensure load balancing, so once the smart grid equipment is hacked and shows wrong information about the demand for electricity, the load balancing will be broken, resulting in a shortage of electricity in some areas and overloading of electricity in some areas, which may also cause serious safety accidents. Furthermore, since power companies use smart grid equipment to monitor users' electricity consumption and collect electricity charges accordingly, some hackers may deliberately invade the grid system and change the electricity consumption displayed on users' meters, thus causing false alarms on the meters, which in turn affects the reasonableness and accuracy of electricity charges collection.

3.1.2 Malicious code

Malicious code refers to those programs that have a malicious purpose and are able to

function through execution, such as computer viruses, Trojan horses, worms, etc., which are often referred to as malicious code. These malicious codes usually take advantage of the vulnerability of the software itself and the behavior of the user to spread. Since there is a large amount of data information in the smart grid, and they interact with many smart terminals, there are many unknown software vulnerabilities, which greatly increases the chance of the grid being infected by malicious code. For example, if the meter equipment is implanted with malicious code, it will greatly disrupt the transmission network, and if the number of hijacked meters is large, it may also lead to the rapid disappearance of the current load in the wires, which may cause damage to the equipment and even cause an explosion. Furthermore, if the smart grid terminal is attacked by a virus and the account password is leaked, it will allow illegal people to steal important data and make improper use of it, which will ultimately harm the interests of the power companies and the country.

3.1.3 DoS attack

DoS attack, i.e. denial of service attack, is a common hacker attack means, specifically refers to the use of computer network bandwidth attacks and connectivity attacks, so that the server can not normally provide network services, and even lead to system paralysis. In the smart grid, whether it is the power generation system, power distribution system, or in the process of using electricity, may be subject to DoS attacks. For example, if the distribution network is subjected to DoS, it will lead to the delay, blockage and destruction of relevant data information, thus affecting the accuracy of judgment and decision-making on the status of the power grid.

For example, if the distribution network is subjected to DoS, it will cause delay, blockage and destruction of relevant data information, thus affecting the accuracy of judgment and decision-making on power grid status; if the meter is subjected to DoS by setting a public IP address, it will receive too much spoofing information, which will lead to operation errors, and ultimately result in communication interruption and power outage.

3.2 Data and Backup Security Issues

In the working process of the smart grid, the security of the data is of great significance to ensure the quality of the work of the data grid, which is mainly manifested in the security of the data itself, which can be directly encrypted through the system data encryption method, to ensure that the data will not be infringed upon by external hackers. At the same time, to ensure the security of data protection work, you can use the information storage method to carry out active protection processing of data. For example, through the method of cloud storage to ensure the security of smart grid operation work data. The following are two common data attack methods:

3.2.1 False data injection

False Data Injection (FDI) attacks pose a significant threat to the efficiency and reliability of smart grids. These attacks target the grid infrastructure by injecting erroneous data into the periodic reports from measurement units to the Control Center (CC). For an FDI attack to be successful, it must pass the State Estimator (SE) test and avoid triggering alarms. The attacker manipulates the injected measurements in such a way that the residuals remain below a predefined threshold. As a result, FDI attacks can mislead the CC into making incorrect decisions, potentially undermining the grid's performance and leading to catastrophic consequences, such as widespread power outages. Furthermore, FDI attackers may exploit the system to redistribute power loads and illegally manipulate electricity prices for financial gain. [11].

3.2.2 Side channel attack

The core concept of a Side Channel Attack (SCA) is to exploit the relationship between dynamic changes in physical parameters and the operations performed on hardware to extract sensitive information. SCA uses information gathered from the implementation of cryptosystems to deduce cryptographic keys. Common types of side-channel attacks include power analysis, electromagnetic analysis, and timing attacks. Smart grid devices exposed to external environments, such as substation equipment, pole-top devices, smart meters, and internal devices, are particularly vulnerable to these attacks. Such vulnerabilities could lead to the leakage of user privacy, usage data, and passwords, or even grant attackers unauthorized administrative access to the smart grid system. Given that smart grids manage vast amounts of real-time data, including power consumption, load forecasts, and

equipment status, the processes of collecting, storing, and transmitting this data present significant risks, including potential data leakage, tampering, or loss.

4. Optimization Strategies for Network Security Protection in Smart Grids

The threats facing smart grid are ever-changing, and its security protection is imminent. The security of smart grid requires that the physical layer, data link layer, network layer and transmission layer realize safe interconnection, and at the same time ensure the availability, integrity and confidentiality of transmitted data. According to the technical characteristics of the smart grid system, combined with the conventional protection technology of network security, this paper argues that the network security protection of the smart grid system can be considered from the network level as well as the data operation security and other aspects.

4.1 Network-Level Improvements

In smart grids, improvements at the network level are essential to ensure the security, stability and efficiency of the system. Through technical means such as virtual local area network (VLAN) optimization, firewall setup and user authentication, the isolation, access control and security protection of the network can be effectively enhanced to cope with the increasingly complex network security threats

4.1.1 Optimization of virtual LAN VLAN

Virtual LAN VLAN is a networking technology that realizes the construction of logical networks across network segments and terminals through switches and supporting network management software. In VLAN, even if multiple hosts are in different network segments, they can be interconnected through policy configuration, just like in the same LAN. Common VLAN segmentation methods include per-port segmentation based on the physical layer, per-MAC address segmentation based on the data link layer, and per-network layer and per-IP multicast segmentation based on the network layer. For the network in the smart grid system, the network can be divided into a number of VLANs according to specific types of services and organizations, i.e., logical isolation between the subsystems is achieved, and secure interconnection between the subsystems can be realized by setting corresponding access policies on the switching equipment.

4.1.2 Firewall settings

Smart grid in the operation and management process, often need to exchange data with the external network, so the network level must have an interoperable port with the outside world, which facilitates the management, but the probability of security threats is also significantly higher. For this reason, firewalls can be used for border management. Border firewalls should have a high swallowing capacity, according to the internal business characteristics, organizational and deployment characteristics of different security domains, for different networks to draw clear boundaries. Border firewalls should enable packet filtering policies for precise control of mutual access to the network. The firewall should also support ultra-high concurrent access for DDoS attacks at the level of millions of packets/ second. For the outside of the network, IPS intrusion prevention, AV gateway anti-virus and AS anti-spam triple protection strategy should be used to ensure that external threats can be accurately intercepted by the border firewall to ensure intranet security.

4.1.3 Authentication of user identity

In the smart grid system, because of the sensitive grid and user information involved, it is necessary to authenticate the identity of users accessing the grid system. Identity authentication can be said to be the first barrier for network security management of smart grid systems, and plays a crucial role in the whole system. Any user who wants to operate the internal system of the smart grid must first verify his account password through the identity authentication module, and only legitimate users with correct passwords can enter the system home page. In the identity authentication process, the user enters the account password, but also needs to fill in the random verification code, and receive the dynamic verification code through the cell phone, the above information in real time through the encrypted packets sent to the back-end servers, the server will match this information with the user information in the database, such as the existence of the user list of consistent information user information, then the requesting end to return to the success of the instruction and then jump to the home page of the system. At this point, the user can

enter the system to browse and operate.

4.2 Enhancements in Data Operation Security

In the operation of smart grid, data security is the core element to ensure the stable and efficient operation of the system. With the wide application of information technology, data face the risk of being stolen, tampered with or lost during transmission, storage and processing. Therefore, it is crucial to strengthen the management of data operation security in smart grid.

4.2.1 Data authentication and backup

Authentication and backup of data are basic measures to ensure data security. By authenticating data, unauthorized access and tampering can be effectively avoided. In addition, regular backup of data ensures that data can be recovered in time in case of failure or disaster events to avoid loss or leakage of important information.

4.2.2 Privilege control and encryption protection

Privilege control and encryption protection are important means to ensure data security. By managing the rights of the staff inside the smart grid, it ensures that only authorized personnel can access sensitive data to prevent information leakage. At the same time, the use of data encryption technology can effectively prevent data from being eavesdropped or tampered with during transmission, especially in the era of big data, smart grids need to deal with a large amount of complex information and data flow, and the security protection of data transmission is particularly important. In order to ensure data integrity and confidentiality, appropriate data encryption algorithms should be used to ensure transmission efficiency while balancing encryption strength and system performance, and avoiding performance degradation caused by excessive encryption.

4.2.3 Security control system for data transmission

The security control system of data transmission is the key link to ensure data security. By building a perfect security system for data transmission, including modules such as certification authority, registration and auditing authority, digital certificate storehouse and certificate revocation system, it can ensure the security of data in the process of transmission. The use of digital certificates can provide strong authentication for each data exchange, ensure the reliability of the source and destination of data transmission and prevent malicious tampering and attacks.

5. Conclusion

With the continuous development and application of smart grid technology, network security has become an important factor affecting its stable operation and security. By analyzing the architecture and characteristics of smart grid, this paper discusses in depth the main vulnerabilities and potential attack risks it faces in terms of network security and data operation security, revealing the complexity and diversity of network security threats in the context of highly informatized and interconnected smart grid. Aiming at these security risks, this paper proposes a series of optimization strategies, including strengthening network protection measures, enhancing data encryption and identity authentication mechanisms, optimizing firewalls and intrusion detection systems, and so on, so as to effectively improve the network security management level of the smart grid. These measures can not only effectively prevent external network attacks, but also enhance the protection of internal data, providing a solid guarantee for the stable operation and sustainable development of the smart grid. In conclusion, with the promotion and application of smart grid worldwide, its security will continue to be the focus of future research and practice, and the optimization strategy proposed in this paper provides strong theoretical support and practical guidance for the security of smart grid and promotes the development of smart grid in the direction of more efficient and safer.

References

[1] Amin SM, Wollenberg S. Toward a smart grid power delivery for the 21st century. IEEE Power and energy magazine, 2005, 3 (5): 34-41.

[2] Andersson G, Donalek P, Farmer R, et al. Causes of the 2003 major grid blackouts in North America and Europe, and recommended mans to improve system dynamic performance. IEEE transactions on Power System, 2005, 20 (4): 1992-1928.

[3] Gorman S. Electricity grid in US

penetrated by spies. The Wall Street Journal, 2009, 8.

[4] Pop C, Cioara T, Antal M, et al., "Blockchain based decentralized management of demand response programs in smart energy grids", Sensors, 2018, 18(1): 162.

[5] IEEE. IEEE smart grid domains & sub-domains. [2023-08-04]. https://smartgrid. ieee.org/domains

[6] NIST. NIST framework and roadmap for smart grid interoperability standards, release 3. 0. (2014-10-01) [2023-08-04]. https://www.nist.gov/system/files/docu-ments/smartgrid/NIST-SP-1108r3.pdf.

[7] Cheng J, Shang ZJ, Hu W, et al. Security Hazards and Response Strategies of Smart Grid Information System. Electrical Application, 2020, 39 (04): 99-102.

[8] Ding J G, Qammar A, Zhang Z M, et al. Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. Energies, 2022, 15(18): 6799-6835.

[9] Lázaro J, Astarloa A, Rodríguez M, et al. A survey on vulnerabilities and countermeasures in the communications of the smart grid. Electronics, 2021, 10 (16): 1881.

[10] Ericsson G N. Toward a framework for managing information security for an electric power utility-CIGRÉ experiences. IEEE Transactions on Power Delivery, 2007, 22(3): 1461-1469.

[11] Huang Y, Li H, Campbell A, et al. "Defending False Data Injection Attack On Smart Grid Network Using Adaptive CUSUM Test", Proc. 45th Annual Conf. Info. Sciences and Sys, March 2011.

