Network Attack Detection and Defense Mechanisms in Smart Grid

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

Abstract: With the wide application of renewable energy, smart grid gradually becomes the core of power system. However, the network security problem of smart grid is increasingly prominent, facing a variety of network attack threats. This paper discusses the types and detection methods of network attacks in smart grid, analyzes the main security threats at present, and puts forward the corresponding defense mechanism. Through the evaluation of existing detection technologies, combined with the challenges of new attack and defense technologies, this paper aims to provide effective protection for the safe operation of smart grids and promote sustainable development in the future energy field.

Keywords: Smart Grid; Network Attacks; Detection Methods; Defense Mechanisms; Security

1. Introduction

Traditional energy resources are increasingly exhausted, and environmental pollution is becoming more and more serious. Renewable energy sources such as wind and solar have great potential to reduce dependence on traditional energy sources and reduce the negative impact of energy use on the environment. However, the fluctuation and instability of wind and solar energy make it have adverse effects on the grid when it is connected to the grid on a large scale. Traditional power grids are designed based on stable, controllable centralized generation models and rely on traditional transmission and distribution networks to reliably deliver power to customers. However, new energy sources such as wind energy and solar energy often have intermittent and random characteristics. When a large number of such energy sources are connected to the power grid, it will cause a mismatch between power supply and demand, resulting in threats to the security and stability of the system. Especially under the influence of load fluctuation, unstable power generation or climate change, the traditional power grid is difficult to cope with this series of dynamic changes and cannot ensure the continuity and reliability of power supply. Under this background, smart grid emerges as the times require, using advanced information technology, automation control technology and communication technology, which can monitor and adjust power flow in real time, and realize flexible scheduling and efficient management of new energy access.[1,2] By integrating advanced prediction, control and optimization algorithms, smart grids can not only cope with the volatility of new energy sources, but also improve the response speed and adaptability of power systems, thus ensuring the stability and security of power supply. The network architecture of smart grids includes not only traditional power transmission and distribution networks, but also a wide range of sensors, actuators, control systems and communication infrastructure. Grid control system regulates power distribution and Load Balancer through real-time data acquisition and remote command execution, which makes the operation and maintenance of smart grid increasingly dependent on the stable operation of information system. Therefore, the research on network attack detection and defense mechanism in smart grid has become an important issue to ensure the security of power system. [3,4]

As smart grids are closely connected to external communication networks, smart grids are also facing an increasing number of cyber attack threats. Attackers can attempt to disrupt the normal operation of the grid, tamper with data, disrupt control signals, and even physically damage grid equipment through various means, such as fake data injection, denial of service attacks, malware propagation,

phishing attacks, etc. The network security of smart grid involves many aspects, including both external attack defense and internal system vulnerability identification and repair. The research on network attack detection and defense mechanism of smart grid has important practical significance. First, effective attack detection and defense technologies can help detect and prevent potential network attacks in time, thus minimizing losses and outages in the grid system. Second, as the scale of smart grids continues to expand, the network security management of power grids has become more complex and challenging. Based on the shortcomings of traditional defense methods, smart grids urgently need to use more advanced technical means, such as artificial intelligence (AI) and machine learning (ML), to improve the intelligent level of network attack detection and response. Thirdly, with the continuous evolution of various network attack technologies, smart grids must constantly improve their security protection systems and update their defense mechanisms to cope with the increasingly severe network security situation.

Under this background, the core goal of this study is to deeply explore the network attack detection and defense mechanism in smart grid, focus on analyzing the main security threats faced by smart grid, evaluate the existing attack detection methods and defense strategies, and propose targeted solutions. With the popularization and application of smart grid in the world, how to ensure its safety, stability and reliability will be a long-term technical challenge. Through in-depth research on network attack detection and defense mechanisms, it can provide a strong guarantee for the safe operation of smart grids and promote the sustainable development and application of smart grids in the future energy field.

2. Composition and Security Requirements of Smart Grid

Compared with the traditional grid, the smart grid not only provides the transmission of electricity, but also supports the two-way flow of information, making the production, transmission, distribution and use of electricity smarter. The core components of a smart grid include smart meters, distribution automation systems, energy management systems, communication networks, etc, as shown Figure 1. These constitute the multilayered architecture of a smart grid, and each part plays a vital role in the grid. The China Electric Power Research Institute defines a smart grid as: “A smart grid is a new type of grid that is based on the traditional grid infrastructure and applies advanced computer technology, information technology, and intelligent control technology to the physical grid, which enables uninterrupted monitoring, control, and unmanned operation, thus realizing a clean, highly efficient, safe, and reliable electric power operating environment. “The Smart Grid, in terms of its main technological components, can be divided into four main parts: Advanced Measurement System (AMI), Advanced Transmission Operation (ATO), Advanced Distribution Operation (ADO), and Advanced Asset Management (AAM). Each component plays an important role in the overall architecture of the Smart Grid. [5,6]

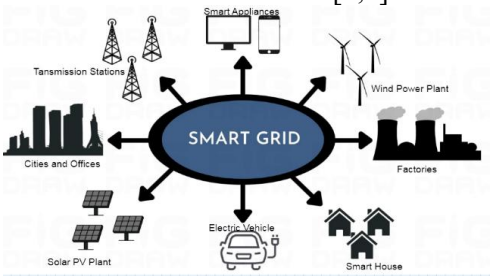

Figure 1. Smart Grid Composition Framework

(1). Advanced Measurement System (AMI): The main function of AMI is to realize the interaction between the power supplier and the power consumer. Through smart meters and communication networks, this system is able to monitor power consumption in real time and support bidirectional data transmission, thus establishing a close connection between the power system and the power load. Users can not only view their electricity consumption in real time, but also participate in demand response programs to optimize their electricity consumption behavior. Through dynamic pricing, users can use more power when electricity prices are low and vice versa, thus promoting grid flexibility and stability. In addition, AMI is able to support fault detection and remote management, which reduces manual intervention and improves the efficiency of electricity services.

(2). Advanced Transmission Operations (ATO): The Advanced Transmission Operations (ATO)

component is dedicated to the effective blockage management of the power system to ensure the reliable delivery of power. Through real-time monitoring and data analysis, ATO can identify and predict potential congestion in the grid in a timely manner, and take measures to optimize current flow, thereby significantly reducing the probability of grid shutdown. In addition, the ATO system also supports intelligent scheduling, which can automatically adjust the load distribution of transmission lines when energy demand fluctuates, ensuring the efficient delivery of power and the safe operation of the system. This intelligent transmission management not only improves the stability of the grid, but also enhances the adaptability to renewable energy access.

(3). Advanced Distribution Operation (ADO): Advanced Distribution Operation (ADO) can effectively guarantee the continuous operation of the grid by monitoring the operation of the distribution grid in real time. The ADO system integrates distribution automation technology, which is able to automatically detect faults and quickly respond to them, reducing the duration of power outages. Meanwhile, ADO also supports the access and management of distributed energy sources, making the production and consumption of electricity more flexible. Through smart sensors and data analytics, ADO is able to dynamically adjust the load of the distribution network to ensure a balanced supply of power during peak and trough times. This capability not only enhances the reliability of the distribution network, but also improves the customer's power experience.

(4). Advanced Asset Management (AAM): Closely integrated with the first three components, AAM can effectively improve the operation of the grid and increase the efficiency of power system assets. AAM helps utilities to monitor the status of assets, predict equipment failures, and formulate reasonable maintenance strategies through data collection and analysis. This system optimizes equipment lifecycle management, reduces operating costs and extends equipment life. In addition, AAM can provide decision support to help utilities make more scientific choices in investment and resource allocation, thereby improving the overall economy and sustainability of the power system. [7,8]

The security issues of smart grid include both physical security and network information security. Smart grid informatization and the deep integration of its physical and information systems have introduced new security risks, and cyber attacks on information systems can be transmitted to physical systems and threaten their safe operation while destroying their functions. In recent years, cyber attacks on smart grids have occurred from time to time. The power system, as a national critical infrastructure, has become an important target of network attacks, which can achieve effects similar to physical attacks, leading to the paralysis of substations and even the entire energy supply system. Therefore, in-depth analysis should be conducted to identify the network attack behavior in smart grid, study the information security technology applicable to smart grid, and construct the smart grid information security defense mechanism in a targeted manner as shown Figure 2. There are different types of networks in smart grid, including: power information network, scheduling information network, extranet and so on. Grid scheduling network is the core platform for power production and operation, carrying huge and real-time data information. This network requires high security to prevent potential network attacks and data leakage. Therefore, it must be configured with multi-layered security measures, including intrusion detection systems (IDS), firewalls and virus protection systems. These devices are able to monitor network traffic in real time, recognize abnormal activities, and block malicious intrusions in a timely manner to ensure the security and integrity of dispatch information. Equally important is the power information network, which is responsible for the collection, storage and transmission of power data. To protect user information and power transaction data, this network needs to implement strong encryption measures to ensure the confidentiality of data during transmission. In addition, regular security audits and vulnerability assessments can help identify potential security risks so that timely remedial measures can be taken. The extranet, on the other hand, is the bridge that connects the smart grid to the outside world, undertaking the task of exchanging data with external users, partners and regulators. As this network is exposed to a variety of attack threats from the outside, it is important to strengthen border protection. This includes the use of advanced

firewalls and intrusion prevention systems to ensure that only authorized users and traffic can access the internal network.

In addition to the configuration of network security devices mentioned above, optimizing network architecture is also an important aspect of smart grid security requirements. The speed and security of the network go hand in hand. An efficient network architecture can reduce delays and increase data transmission rates, as well as enhance resistance to attacks. For example, by designing redundant network paths, it is possible to quickly switch to alternate paths to ensure the normal operation of the power system when a certain part is under attack.

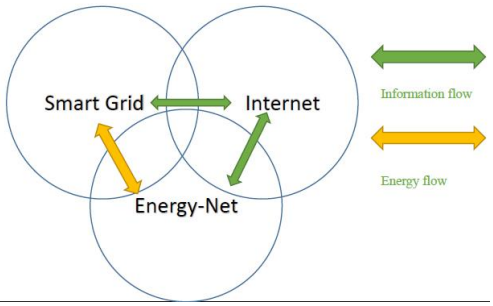

Figure 2. Smart Grid and Energy Grid Integration Technology

In summary, the security needs of the smart grid are not only to prevent external attacks, but also to ensure the stability and reliability of the entire power system. With the continuous progress of technology, the security measures of smart grid also need to evolve to adapt to emerging threats and challenges. Through the comprehensive use of advanced network security equipment and optimized network configuration, the State Grid can effectively enhance the security protection capability of the smart grid, providing a solid guarantee for the reliability of power supply and the safety of users.

3. Network Attack Types and Detection Methods

3.1 Common Types of Network Attacks in Smart Grids

Network attacks on smart grids can be carried out at all stages of data generation, communication, storage and application. For smart grid, vulnerability assessment under attack scenarios is very important. There are many ways to achieve it, such as analyzing the information security vulnerability of supervisory control and data acquisition (SCADA) system, evaluating the security level by calculating the information physical security index, calculating the upper and lower limits of system vulnerability, etc. The deployment and use of a large number of intelligent electronic devices (IED), remote terminal units (RTU) and advanced metering infrastructure (AMI) in smart grids make it possible for attack technologies already existing in computer networks to pose threats to critical infrastructure of power systems. Network attack techniques in smart grid include denial of service (DoS) attack, network intrusion attack, password cracking attack, protocol attack, worm/spyware/malware attack, etc. Among them, the last type of attack technology is mainly designed for important power infrastructure, and its damage is increasingly prominent. For example, in 2003, the Slammer Worm virus attacked the monitoring system of the David Basse nuclear power plant in Ohio, USA, causing the system to stop working for nearly five hours, while in 2010, the Stuxnet virus attacked the industrial control system of Iran's Bushehr nuclear power plant, causing damage to its nuclear facilities in Natanz, which directly led to the serious consequences of delaying the start-up of Iran's nuclear energy plant. In recent years, the number, scale and complexity of malicious code attacks have shown a rapid growth trend. With the deepening of grid openness, such attacks will have a wider impact on the power system and power market at a deeper level.

Denial-of-Service (DoS) attacks represent a malicious behavior aimed at rendering servers (controllers) unable to provide services, making them one of the most common tools employed by hackers for disruption. These attacks primarily target physical systems with the objective of obstructing the information exchange between controllers and executing devices. By exploiting malicious programs, attackers consume communication bandwidth, thereby preventing control commands and feedback signals from reaching their intended destinations or overwhelming routers and servers with an excessive number of invalid service requests. The characteristics and operational mechanisms of DoS attacks indicate that conventional responses in closed-loop control systems often rely on previously obtained information when effective

information is rendered inaccessible. The occurrence of DoS phenomena can lead to disconnections in control loops and feedback loops, resulting in the controller's inability to receive timely feedback. This disruption can ultimately cause system instability, degraded performance, and even complete system failure. [9,10]

Network intrusion, on the other hand, involves exploiting vulnerabilities within the applications or communication infrastructure deployed in the power grid to gain unauthorized access to critical systems. In the context of smart grids, when an attacker conducts reconnaissance and scanning to identify system vulnerabilities, they can circumvent the embedded security measures (such as firewalls and system passwords) to access human-machine interfaces within the grid. Malware and viruses exploit vulnerabilities in system software, Programmable Logic Controllers (PLCs), or protocols to launch attacks. Such malicious software typically scans the network for potential target computers, leveraging specific vulnerabilities to replicate code that enhances their payload, subsequently propagating throughout the network. In recent years, the frequency and complexity of these attacks have escalated, making them a focal point of concern for researchers focused on the security of critical infrastructure systems in the power sector. Notably, the Stuxnet virus serves as a classic example of malware specifically designed to target power facilities. The network protocols utilized in power systems, such as ICCP, IEC 61850, and DNP3, pose additional risks. If these protocols are not designed with adequate security measures, they may be susceptible to exploitation by attackers to initiate network attacks. These protocols are typically used for controlling remote devices within the smart grid; thus, once an attacker gains network access, they can manipulate the communication process to inject malicious state data and control commands. Consequently, it is imperative that secure versions of these protocols not only provide a requisite level of security assurance but also meet the latency and reliability requirements stipulated by applications operating within the power grid.

3.2 Network Attack Detection Technology

The smart grid is a spatiotemporal multidimensional heterogeneous system that deeply integrates power systems and information communication systems. Analyzing its cybersecurity characteristics can no longer be performed through single power or communication simulation tools. A novel joint simulation platform for power information security analysis is required. This platform must be capable of accurately simulating security incidents related to the information network of the smart grid, such as network attacks and information disruptions, and it should be able to interact across multiple platforms to precisely simulate the consequences of these incidents within the physical power system. Network attack detection and identification must not only determine whether the smart grid has been attacked, but also identify the specific devices or communication links affected by the attack. After detecting and identifying network attacks, measures can be taken to isolate the attacked nodes, thereby achieving the goal of defending against network attacks at a lower cost.

Network attack detection techniques can be classified into several categories, depending on the detection requirements and environment. Firstly, statistical detection methods, such as the Chi-squared (x^2) detector and the SUM x^2 detector, construct statistical metrics to assess whether the system has been attacked, typically relying on the assumption of Gaussian white noise. Additionally, Kullback- Leibler divergence (KLD) is used to measure the entropy difference between probability distributions, and KLD-based detectors are built to identify network attacks. Furthermore, the Euclidean norm of residual signals is employed in attack detection, where thresholds are set to determine the presence of anomalous behavior. In recent years, the application of cryptographic techniques has also increased, such as the use of watermark generation and removal techniques, along with encryption matrices to protect wireless transmission data, thus enhancing attack detection capabilities. However, these methods are mainly geared towards man-in-the-middle attacks and are limited in detecting device-level attacks.

Artificial intelligence technologies have also played a crucial role in network attack detection, particularly through the use of trained neural networks and reinforcement learning methods, which can improve detection

accuracy and response speed. These diverse detection technologies provide more comprehensive protection for network security, adapting to the ever-evolving landscape of cyber threats.。

3.3 Challenges of New Attack and Defense Technologies

As smart grid technology continues to evolve, network security faces increasingly severe challenges. As a highly integrated and complex system, the smart grid not only needs to defend against traditional cyber-attacks but also emerging attack methods, such as Advanced Persistent Threats (APTs), zero-day attacks, and threats targeting Internet of Things (IoT) devices. The unique structure and diverse characteristics of the smart grid make its network security more difficult to protect. The smart grid consists of a wide range of physical devices, sensors, communication networks, and control systems, creating a broad attack surface. Attackers can not only infiltrate through the network but may also target critical components like smart devices, sensors, or SCADA systems to compromise the grid's security. Trusted computing technologies provide strong identity authentication and data protection mechanisms at the hardware level to enhance the security of the smart grid. However, as attack techniques continue to evolve, relying solely on hardware protection faces new threats. For example, malicious software may bypass hardware-level defenses or directly attack the hardware itself, compromising the trusted computing mechanisms. Therefore, the defense system of the smart grid needs to integrate trusted computing with other advanced protection technologies, such as artificial intelligence and machine learning, to build a more intelligent protection framework.

To address new types of cyber-attacks, smart grid defense systems are increasingly adopting cutting-edge technologies such as artificial intelligence, machine learning, and data mining. These technologies can learn from historical data to help the system automatically detect potential attack patterns and respond in real-time. However, the introduction of AI and machine learning also brings new challenges, such as algorithm accuracy and the prevention of adversarial attacks. Particularly when dealing with vast amounts of device and sensor data, how to extract valuable attack information from massive data and effectively respond remains a core issue in system protection. The network security challenges faced by the smart grid are becoming more complex, and traditional protection methods can no longer effectively address modern attacks. To successfully defend against these threats, the smart grid needs to establish a multi-layered, intelligent security framework, integrating emerging technologies like artificial intelligence and machine learning to continuously enhance its detection, response, and defense capabilities against new attacks. Additionally, cross-sector collaboration and policy improvement are also key factors in ensuring the security of the smart grid.

4. Performance Evaluation of Attack Detection and Defense Mechanisms

With the continuous evolution of network attacks, the importance of attack detection and defense mechanisms in safeguarding systems grows increasingly critical. To ensure that these mechanisms can effectively respond to changing threats, performance evaluation becomes a vital component. By rigorously assessing attack detection and defense mechanisms, we can measure their effectiveness across different environments, ensuring they provide robust security without compromising the normal operation of the system. This paper discusses the methods for evaluating the performance of these mechanisms, focusing on the analysis of evaluation metrics, methodologies, and their applicability in complex systems, such as smart grids.

The design objectives of attack detection and defense mechanisms encompass timely identification of potential malicious activities within the network, implementation of appropriate protective measures based on detection results, and minimizing any adverse impact on system performance during operation. Achieving these objectives relies on accurately evaluating the detection and defense mechanisms, enabling system designers to select optimal solutions in complex network environments. This is especially crucial in high-traffic and intricate settings, where maintaining system stability and responsiveness is paramount. Consequently, establishing a comprehensive evaluation

framework provides a quantitative foundation to ensure the efficiency and effectiveness of attack detection and defense measures.

Evaluating the performance of attack detection and defense mechanisms typically hinges on several key metrics, including detection rate, false positive rate, false negative rate, response time, and system resource consumption. These metrics offer a quantitative basis for evaluation, aiding security experts in making thorough comparisons and selections among different mechanisms. The primary evaluation methods include experimental assessment, simulation assessment, and real-world deployment assessment, each with its unique applicable scenarios, advantages, and limitations. Experimental assessments yield accurate results in controlled environments, while simulation assessments leverage tools to verify performance under variable network conditions. Real-world deployment assessments reflect the effectiveness of defense mechanisms in actual environments. Through detailed analysis of the evaluation results, designers can gain insights into the strengths and weaknesses of various mechanisms under different conditions, enabling them to optimize defense strategies and enhance overall network security.

5. Conclusion

The security of the smart grid is essential for its stable operation, and the network attack detection and defense mechanisms play a crucial role in ensuring this security. This paper reviews the common types of network attacks and their detection methods in the smart grid, examines the challenges posed by emerging attack and defense technologies, and proposes a multi-layered security protection strategy. As technology continues to advance, network security measures for smart grids must evolve to address new threats and challenges. By integrating advanced detection and defense technologies, these measures can provide robust protection for the safe operation of the smart grid, supporting the efficient use of renewable energy and fostering the sustainable development of the grid.

Acknowledgement

This work is supported in part by the project of ID. 031900KC23070047 (GDKJXM20230960).

Reference

[1] Zou Hong. Research on smart grid information security defense system architecture and key technologies. Network Security Technology and Application, 2020, (01):113-115.

[2] MA Liya, GUO Jianfeng, WANG Zhe, et al. Analysis of security protection technology in smart grid scheduling control system. Integrated Circuit Applications, 2023, 40(08):260-261.

[3] Wu Tao. Exploration of smart grid data security protection. Light Industry Science and Technology,2024,40(03):95-97.

[4] YANG Guanghong, LU Anyang, AN Liwei. A review of research on security state estimation of infophysical systems under cyber attack. Control and Decision Making, 2023, 38(08):2093-2105.

[5] Liu Wanchao. Research on Risk Analysis and Insurance Design of Power System Cyber Attack. University of International Business and Economics, 2020.

[6] Tang Yi, Chen Qian, Li, Mengya. et al. A review of research on cyber-attacks in power information-physical fusion system environment. Power System Automation, 2016, 40(17):59-69.

[7] Cui Keqing. Research on security control problems of information physical system under complex cyber attack environment. Lanzhou University of Technology, 2023.

[8] Liu Jidong. Modeling and risk assessment of power grid infophysical system based on cyber attack. North China Electric Power University (Beijing), 2024.

[9] Ge Hui. Research on security control method of information physical fusion system under cyber attack. Nanjing University of Posts and Telecommunications, 2018.

[10] Cheng Pengzhi. Research on the prevention of network attack in intelligent substation. North China Electric Power University, 2019.

