Journal of Network Communications and Emerging Technologies (JNCET)
Volume 11, Issue 11, November (2021)

Cyber-Attack Process and Defense Strategies in Smart Grid Applications

Muhammed Zekeriya Gündüz
Department of Computer Science and Technology, Vocational School of Technical Sciences, Bingol University, 12000, Bingol, Turkey
mzgunduz@bingol.edu.tr

Resul Daş
Department of Software Engineering, Technology Faculty, Fırat University, 23119 Elazığ, Turkey
rdas@firat.edu.tr

Published online: 30 November 2021

ABSTRACT

A smart grid application includes information technologies intensely and it effectively transmits energy by using bidirectional communication. It also enables joining the green technologies into the system. The vulnerabilities of information and communication technologies expose smart grid systems to many security threats. Therefore many attacks and prominent countermeasures about smart grid applications have been discussed in many survey papers. Generally, these attacks are classified according to the basic security principles of confidentiality, integrity, and availability without including accountability. Moreover, suggested countermeasures concentrate on blocking particular attacks or defending specific components. In addition to these specific solutions, using a vast perspective approach to ensure the security of the whole system components provides a holistic solution. In this context, in the study, we review some severe cyber-attacks that could happen in a smart grid application and explain the process of a possible cyber-attack. We also recommend a generic cyber security approach for smart grid applications to detect and prevent the common cyber-attacks.

Index Terms – Cyber-Attacks, Cyber-Security, CIA Triad, Accountability, Smart Grid.

1. INTRODUCTION

A smart grid system is an enhanced power grid built on a sophisticated infrastructure that assures providing reliability and flexibility in a sustainable manner [1]. It enables the integration of different energy supplies, facilitates corrective capacities when failures arise, and reduces power loss in the system. A smart grid network is based on information and communication technologies (ICT). ICT cover all processes that are generation, distribution, transmission, and consumption of energy. Smart grid includes a bidirectional flow of data to establish a broadly distributed and automated system that has new characteristics, such as system resilience, better integration of renewable technologies, real-time control, self-healing, and operational efficiency [2]. Along with these features, some uncertain situations still exist in smart grid applications. There are many papers published on common topics on cyber-security in smart grid systems. The danger posed by the possibility of a cyber-attack can only be reduced by integrating the cyber-security approach into the system architecture from the beginning. Smart grid applications have digital content. It means that cyber-security vulnerabilities in the Internet environment continue to exist in smart grids. So, in addition to classical cyber-security measures, these vulnerabilities require up-to-date security solutions for smart grid applications. Knowing how a cyber-attack is carried out in smart grid applications is important to understand the attack process. Understanding the offensive process shows that the existence of a holistic defense strategy is inevitable. This strategy provides a holistic perspective in ensuring the cyber-security of the system. The development of such holistic strategies constitutes the motivation of the study.

In the study, the current and future status of cyber-security in a smart grid system is reviewed. The remainder of this paper is organized as follows. In section 2, we present the conceptual model, system elements, communication protocols, and cyber security requirements in smart grid applications. In section 3, a possible cyber-attack process is examined in a smart grid application. A cyber-security approach that includes defense strategies and countermeasures to defend the whole system is proposed in section 4. In the last section, the general results of the study are presented.

2. BACKGROUND

It is known that traditional electrical networks have become unable to meet the needs of today's modern world. This situation necessitates smart grid applications. In this context, the main differences between traditional networks and smart grids are shown in Table 1. The integration of renewable energy sources into electricity networks and the existing of applications such as smart

cars, smart meters have made the existence of smart grid systems a necessity. The conceptual model proposed by National Institute of Standards and Technology (NIST) stands out for the effective and efficient implementation of these applications. In this model, domains are clearly defined. The design of system components and communication protocols in smart grid applications considering cyber security requirements implements the conceptual model faster. In this context, the conceptual model, system components, communication protocols and cyber security requirements of the smart grid are presented in this chapter.

Traditional Electricity Grid	**Smart Grid**
Electromechanical metering	Digital metering
Generally unidirectional communication	Bidirectional communication (real-time)
Mostly centralized generation	Distributed and centralized generation
Limited control/protection	Adaptive and robust control/protection
Manual monitoring	Self-monitoring
Manual restoration	Automated (Self-healing)
Estimated reliability	Predictive reliability
Less sensors	Widespread use of sensors
Less energy efficient	Energy efficient
Time-dependent price	Real-time price
Limited costumer interaction	Extensive customer interaction
Radial system topology, generally one way power flow	Network system topology, multiple power flow paths
Less environment-friendly	Environment-friendly

Table 1 Differences between Traditional Electricity Grid and Smart Grid

2.1. Conceptual Model

The major advantages expected from a smart grid system are enhancing environmental performance and improving system resilience. Resilience means the ability of a given object to counteract unexpected or unforeseen situations and recover soon. According to NIST, smart grid systems have seven logical domains. They are generation, transmission, distribution, customer, operation, market, and service provider domains. Each domain includes applications and actors. Actors refer to the systems, devices, and programs, while applications refer to processes run by actors in each domain. Figure 1 illustrates the NIST conceptual model and the interaction of actors from each domain over a secure channel for a smart grid system [3].

Electricity generation is the initial step for carrying power to the end-users. Producers of electricity are the actors of this domain. The generated electricity is transported across distances from the generation domain to the distribution domain via various substations, in the transmission domain. Also, electricity can be generated and stored in this domain. The distribution domain contains electricity distributors to and from the end-users. The distribution domain can also store and generate energy. The distribution domain is between the customer and transmission domain. It is also connected to the metering points to measure consumption. End-users are the main actors in the customer domain. Commercial, industrial, and home users are the end-users. These actors not only consume electricity but also store, generate, and manage the using it. Managers of electricity transmission are the actors in the operation domain.

This domain sustains effective and optimum operations in distribution and transmission processes. It utilizes distribution management systems (DMS) in the distribution domain, also energy management systems (EMS) in the transmission domain [4]. The service provider domain communicates with the operation domain to provide control and situational awareness in the whole system. This domain contains companies that present smart services to utilities and customers. These companies operate services such as using energy, energy generation at home, customer account, customer interaction with the market, and billing. The participants and operators in the electricity markets are the actors in the market domain. The balance between the electrical demand and supply is provided in this domain. To match the generation with demand, it communicates with distributed energy resources (DER) and the generation domain.

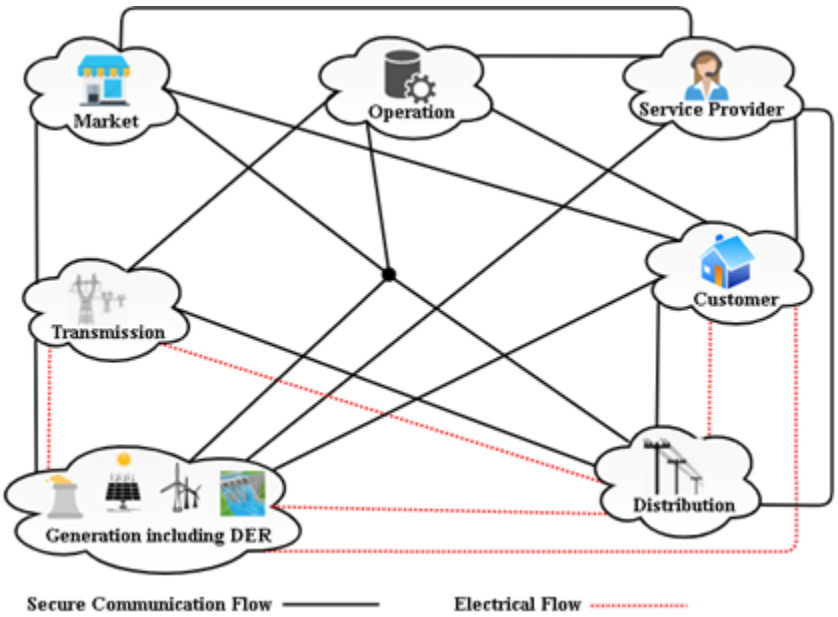

Figure 1 Conceptual Model of Smart Grid

2.2. System Components

Smart grid has some heterogeneous and distributed applications, including demand response, home energy management (HEM), SCADA, electric vehicle (EV), advanced metering infrastructure (AMI), and automation substations. In particular, we focus on SCADA, AMI, and automation substations which are critical and vulnerable applications.

Distribution and customer domains have AMI. It provides gathering, measuring, and analyzing energy usage. Furthermore, it enables bidirectional communication. AMI headend, smart meters, and the communication infrastructure are its elements. A smart meter is a developed digital meter equipped with Internet of things (IoT) features and has a local memory and microprocessor. Moreover, it can monitor and collect electricity usage of home devices. They also transmit the collected data to the AMI headend, which is a server on the utility side, in real-time. It also has meter data management system. AMI headend, home appliances, and smart meters communicate with each other via communication network protocols like Zigbee, Z-wave. Figure 2 shows the generic representation of smart grid architecture.

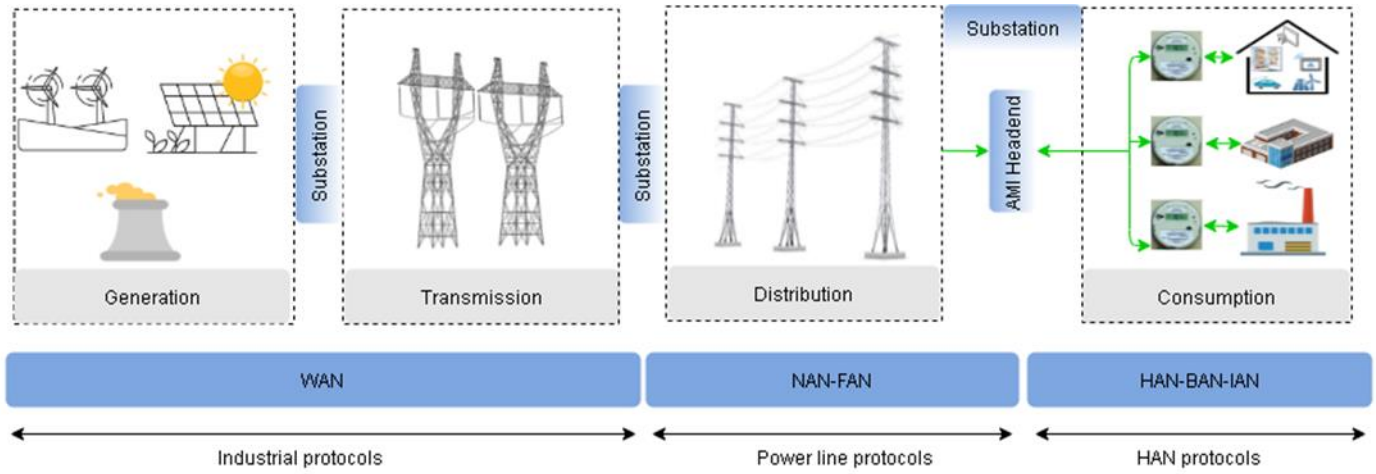

Figure 2 Generic Representation of Smart Grid Architecture

The automation system network is controlled and monitored via a SCADA system. It includes monitoring devices, control devices, and a communication network. It is situated in the operation domain and utilized to monitor, measure, and control a power system. Generally, it is used in large-scale systems. There are three components in a SCADA system which are the master terminal unit

(MTU), the human-machine interface (HMI), and the remote terminal unit (RTU). MTU controls the RTU. RTU has three components for data acquisition, running commands coming for MTU, and communication. The HMI is a graphic interface for the SCADA system operator. SCADA system communication is based on some industrial protocols such as IEC 61850 and DNP3 [5].

Substations are one of the main components of electricity networks. A substation is a significant part of the transmission, distribution, and generation domains. Also, it operates many functions such as regulating the distribution, limiting electricity fluctuation, and obtaining electricity from generating facilities. It includes appliances that distribute, control and regulate power like an HMI, intelligent electronic devices (IEDs), RTU, and a global positioning system (GPS). Substations transmit the operation data into the SCADA system to control the system. Generally, an operation is automated in a substation improving the system's reliability. Other devices communicate by IEC 61850 with automation substations in distribution and transmission processes.

2.3. Communication Protocols

Heterogeneous and distributed applications need distinct network protocols in smart grid systems. So, there are differences between internet communication architecture and smart grid communication infrastructure. Some of these differences are shown in table 2. Home appliances use Z-wave and ZigBee protocols. In general, devices are communicated via IEEE 802.16, IEEE 802.15.4, or IEEE 802.11 in the neighborhood area network (NAN). SCADA systems and wide area networks (WAN) use a few industrial protocols such as Modbus, DNP3. IEC 61850 standart protocol is applied in substation automation. DNP3 and Modbus protocols are applied in smart grid applications even though they have vulnerabilities [6].

Modbus is a standard utilized to transmit information over serial lines in real-time between appliances. It has three types which are Modbus-TCP, Modbus-RTU, and Modbus-ASCII. Messages are coded in hexadecimal in Modbus-ASCII. Although it is not fast, it is perfect for telephone communications and radio links. A message is coded in the binary system and utilized over serial communication standard (RS232) in Modbus RTU. The slaves and masters utilize IP addresses in Modbus-TCP for communication. Modbus protocol works as the master-slave system within SCADA systems, and it exchanges instructions between master-slave elements. Modbus is generally utilized in industry, for communicating raw data without the limitation of authentication, encryption, or extreme overhead. These features make it a vulnerable and easy target [7].

DNP3 is a broadly utilized protocol in critical infrastructures, especially in power grids. It manages communication between master and slave stations. Slave stations are also called outstations. DNP3 was utilized to connect master stations like RTU to outstations like IEDs in electricity stations. DNP3 was modified to run across IP networks thanks to the encapsulation of UDP or TCP packets. At first, this protocol did not ensure any security technics like authentication, encryption. The issue was solved by the secure DNP3 protocol.

2.4. Cyber-Security Requirements

Three main requirements have been identified by NIST to ensure and maintain information security in smart grid applications. These requirements are confidentiality, integrity, and availability called the CIA triad. Besides these main requirements, there are other requirements as well. Accountability is one of them.

Characteristic	**The Internet Communication Infrastructure**	**Smart Grid Communication Infrastructure**
Network type	Complex and heterogeneous	Complex and heterogeneous
System architecture	Decentralized, distributed, hierarchical	Decentralized, distributed, hierarchical
Transmission flow	Two-way flow of data	Two-way flow of power and data
Protocols	TCP/IP, DNS, DHCP etc.	IP, DNP3, DNP3overTCP/IP, Modbus etc.
Vulnerabilities	Physical, cyber	Physical, cyber
Quality of Services	Accessibility, transparency	Latency, priority
Network topology	Self-healing, adaptive, ubiquitous	Self-healing, adaptive, ubiquitous
Scalability	Cheaper, Rapid	Expensive, slow

Storage cost	Low	High
Services range	Multi-service	Single-service
Transmitted	Data	Power and data

Table 2 Differences between the Internet and Smart Grid Networks

Confidentiality protects proprietary information and personal privacy. Also, it preserves the information being obtained or revealed by unauthorized processes, entities, or individuals. Confidentiality is lost once an unauthorized revealing of information happens. For example, information like billing, metering usage, and control of a meter that is transmitted between entities and customers have to be confidential otherwise, the information of customers may be utilized for different malicious aims by attackers [8]. Availability means ensuring reliable and timely access and using information. The most vital cyber-security essential is availability in smart grid applications since the loss of availability defines interruption of information access. Loss of availability disrupts the work of the control system by denying data transfer. Hence, the network access to the control system operators is obstructed [9]. Integrity means defending against abnormal change or damage of the information in smart grid applications. Unauthorized change or damage of data is defined as loss of integrity. An attacker who manipulates measurements from smart meters and redirects them to the state estimator compromises the data integrity. Moreover, authenticity and nonrepudiation of information are a necessity to keep integrity. Authenticity means that data is generated from a legal origin. Nonrepudiation means that persons or institutions cannot deny their transactions later [10]. Accountability defines guaranteeing the tractability of the system. Also, it provides every activity applied by an appliance/person is recordable. The registerable information could be offered as evidence in a court to identify the attackers.

3. CYBER-ATTACK PROCESS IN SMART GRID

Four steps are utilized to attack smart grid applications. Reconnaissance, scanning, exploitation, and maintaining access in the given order [11]. A cyber-attack occurs in a lifecycle. In the reconnaissance step, the attacker gathers data about the victim. During the scanning step, the attacker attempts to determine the system vulnerabilities. The attempts try to determine the open ports. Also, they explore the services that run on ports along with their vulnerabilities. In the third step which is exploitation, the attacker attempt to get control of the victim system. Since the attacker wants to have admin access to the system he maintains the access. Maintaining the access step is attained with established secret and not detectable malware, so the attacker could get back to the system whenever he wants.

During each step, attackers deploy distinct techniques to compromise a specific part of the system [7]. So, attacks can be classified according to the four steps. Many types of attacks occur in the exploitation step. The attacks and malicious activities in the steps are described below.

Reconnaissance includes traffic analysis and social engineering attacks. In social engineering, technical skills are not used as much as social skills. Attackers utilize persuasion and communication technics to gain the trust of the victim. Also, they use these technics to get private information like personal identification numbers or passwords to enter into target systems. Password pilfering and phishing attacks are well-known ways used in social engineering. The network traffic could be listened to by a traffic analysis attack. In this way, the captured network traffic is analyzed to discover the hosts and devices with their IP addresses in the network. Traffic analysis and social engineering damage to the confidentiality principle of the information.

The second step is scanning. It is used to explore the hosts on the network. IP scanning, port scanning, service scanning, and vulnerability scanning are the scanning types. Firstly, an attacker to determine the hosts connected to the system by using IP scanning. The attacker determines the open ports by scanning them. The scanning is performed on explored hosts in the system. Then, the attacker applies a service scanning to determine the services running on not closed virtual ports. For example, if port 4712 or 4713 is not closed, the target service is a PMU. A vulnerability scan aims to determine the vulnerabilities concerned with services on the victim system to exploit it. DNP3 and Modbus are industrial protocols. They are vulnerable to scanning attacks.

The third step is exploitation. The attackers try to exploit smart grid appliance vulnerabilities via malicious activities such as trojan horses, viruses, replay attacks, worms, Denial of Service (DoS) attacks, popping the HMI, Man in the Middle (MiTM) attacks, jamming channels, privacy and integrity violations. Then the attackers take control of them.

A virus is used to affect certain devices for a specific purpose in a system. Worms are self-replicating programs. They use the communication line to spread, multiply, and infect other devices in the system network. Trojan horses appear to play a legal duty on the victim system. But, in the background, it operates a malicious code. Attackers utilize trojan horses to upload a worm or virus to the victim system. Generally, viruses and worms compromise the availability and confidentiality security parameters.

Attackers use several methods and tools in DoS and DDoS attacks. Time synchronization attacks, puppet attacks, smurf attacks, teardrop attacks, and SYN attacks are types of DoS attacks. SYN attacks exploit the three-way handshake utilized to set up a TCP session. Attackers flood the target network with SYN requests without answering the SYN-ACK packets. This process results in system halting. TCP and Modbus protocols are vulnerable to SYN attacks because they run over TCP. Teardrop attacks involve that sending fragmented packets to a target system. The attacker changes the fragmentation offset values and the length of sequential IP packets. Therefore, the system receiving such packets cannot reassemble them, and then it breaks because the instructions on how the fragments are offset in the IP packets are conflicted [12].

Attackers can congest the communication traffic of a network with a smurf attack. It is a form of DDoS attack that happens at the network layer. A smurf attack consists of the source, bounce, and target site. In the source site, a spoofed packet is forwarded to the bounce site via the broadcast address by the attacker. The spoofed packets include the IP address of the victim network. After the forged packets are accepted in bounce site and then they are broadcasted to hosts in the system network. It causes congestion of the target system. Puppet attacks target the AMI by consuming the network bandwidth. The time synchronization attacks (TSA) target the time data in smart grid network. Smart grid processes like event location estimation and fault detection depend on exact time information. In addition, generally, measurement appliances are equipped with GPS in smart grid applications. TSA spoofs the GPS information and threatens the system's availability. Communication and control messages are time critical. So, delay of milliseconds may disrupt the availability of the system. Therefore, DoS attacks are fatal threats for smart grid applications [13].

Spoofing, blocking between two devices, or applying an injection to a communication line means a MiTM attack occurs. The attacker transfers the data transmission between both devices over himself. The legal appliances seem to communicate without any problem, but they interact over an illegal device. For instance, a MiTM attack can be utilized to hijack TCP/IP communication between the transmission SCADA server and the substation gateway. Intercepting is a type of MiTM too. It aims to modify, and intercept the data stored in a particular device or transmitted over the network. For example, an attacker utilizes a radio-frequency interception attack to alter a private communication in AMI. Eavesdropping and IP spoofing, which are MiTM attacks, may come forward in smart grid applications. All types of MiTM attacks aim to damage accountability, integrity, and confidentiality.

The industrial control commands are forwarded in plain text. So, in a replay attack, an attacker can capture the packets, and maliciously inject them. And then attacker replays the packets to the destination by compromising the integrity of the communication. Replay attacks could be used in different components of the smart grid. IED devices may be attacked with a replay attack so that incorrect measurements are injected into particular registers. Replay attacks can be utilized to modify the behavior of a PLC, too. Authentication schemes are utilized between smart meters in AMI. Replay attacks include malicious hosts obstructing authentication packets sent from smart meters. Malicious hosts resend the packets at a later time for authenticating and get unauthorized login to the system in AMI [14].

Jamming channel attacks exploit the shared nature of a wireless network and send a continuous or random packet flow so that block the communication of legitimate devices and keep the channel occupied. It could severely reduce the efficiency of the system. Smart grid applications have time-critical nature and require an available network to meet the Quality of Service (QoS) requirements [13].

Popping the HMI attack occurs when a known component’s vulnerability, especially operating system or software, is exploited. It installs a remote connection. And so, it allows the attacker to connect remotely to get unauthorized access monitoring and controlling the compromised system. Systems that run an operating system that has a console line interface, substations, or SCADA systems are considered as a potential target of Popping the HMI attack. Improved networking skills or a lot of experience in industrial control systems and cyber-security is not a necessity to perform this attack.

In the masquerade attack, an attacker may act as a legal user to obtain access to any system or acquire more privileges to do unauthorized activities. It compromises accountability and the CIA triad of the system.

An integrity attack aims to break the accountability or the integrity by modifying the data stored in a dedicated component in the system. For example, a customer may apply an integrity attack by altering the consumption data in a smart meter to reduce the bill [15]. Disrupted data that is altered would be informed to the control center, and this situation results in a risen blackout time. Also, it may be utilized against RTU.

False data injection (FDI) is a type of integrity violation attack. It aims to damage components' measurements and affect the correctness of the state estimate [16].

Privacy violation attacks aim to break privacy by gathering the secret information of users. For instance, a smart meter gets electricity usage many times a day, and customers' electricity consumption data may be obtained by an attacker. In this way, if it

is detected that there is no electricity usage in the smart meter by an attacker for a while that usually indicates that there is nobody at house. This information may be utilized to perform a physical attack such as theft.

In the maintaining access step, attackers use backdoors to gain continuous access to the target. Backdoors are stealthily situated on the target, and also an undetectable program to get back later smoothly. If an attacker achieves embedding a backdoor into the servers of the SCADA control center, he could initiate diverse attacks that could lead to severe effects on the electricity system.

Confidentiality, integrity, accountability, and availability security requirements are listed, in the given order, in IT systems. However, they are ordered as availability, integrity, accountability, and confidentiality in smart grid applications. Therefore, it can be said that an attack that endangers the availability of a smart grid application is of high severity, while an attack that targets confidentiality is of low severity.

4. DEFENSE STRATEGIES AND COUNTERMEASURES

Many studies have been carried out in the literature to provide the cyber-security of smart grid systems [17]. In the studies, techniques for detecting and preventing certain types of attacks have been proposed. The cyber-security approach is more successful when it is handled with a comprehensive and strategic approach rather than a specific solution. So, in this section, we suggest a cyber-security strategy. As shown in Figure 3 it has three phases: before the attack, during the attack, and after the attack. Relevant published solutions about cryptography, cyber-security technologies, security protocols, and diverse cyber-attack precautions are defined for each phase.

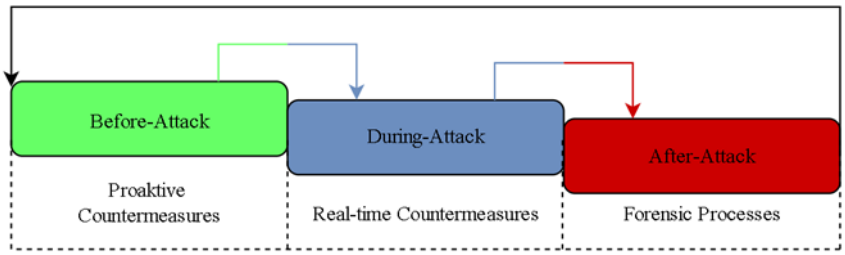

Figure 3 Cyber-Security Strategy for Smart Grid Applications

4.1. Before-Attack

Security countermeasures are generally presented in three categories in this step. They are network, data and device security. Cryptography is for data security. We discuss security protocols and technologies like security information and event management systems (SIEM), intrusion detection systems (IDS), secure DNP3, and network data loss prevention for network security. Key management, authentication, and encryption solutions are for data security. Compliance checks, host IDS, and various techniques are for device security.

A data transmission line is the backbone for communication. Therefore, network security plays a vital role to secure the whole system. Using monitoring technologies and firewalls is recommended to protect the system. Firewalls permit or reject the IP packets based on particular rules and procedures. However, advanced attack techniques could bypass usual firewall technics. Hence, firewalls should be associated with additional security systems like SIEM, machine-learning-based IDS/IPS, and network data loss prevention. An IDS detects the malicious activities of a specific host or a system network. A SIEM is an information management system that collects data from network flow, operating systems and application logs in the system. Then the gathered data is analyzed and processed by a centralized server to detect any malicious activity or potential threat in the system. Also, secure network protocols such as SSL/TLS, IPsec, secure DNP3, may be used to improve security in the system [18].

DNP3 protocol is widely used in smart grid applications. At first, the DNP3 protocol was designed without security solutions. It means that packets were transferred in plain text over the system and could be simply intercepted. For this reason, a secured type of DNP3 protocol was released called secure DNP3. In this version, encryption and authentication are attached to a secure layer. Many attacks could be prevented by using such a protocol. For instance, the authentication mechanism may counter MiTM attacks, and encryption decreases replay attacks and eavesdropping [6].

Encryption mechanisms intend to guarantee data integrity, confidentiality, and nonrepudiation. Different elements with diverse computational capabilities co-exist in smart grid applications. Hence, both asymmetric and symmetric key encryption could be utilized. So, the selection of devices depends on different metrics, including computational resources, data criticality, time constraints. Authentication verifies the validation of an object's identity, such as using a password. Objects may be smart devices, users, or components connected to the system. A special kind of authentication is multicast authentication. It is applied in smart

grid applications a lot. Shared/public key management (PKI), could guarantee the authenticity of the communication across the network. The identities of parties are approved by a certificate authority in PKI infrastructure. The operation is implemented before any connection is established between the two parties. There are four steps to maintain the security of communication in public key management. They are generation, distribution, storage, and update of keys. Due to the heterogeneous and distributed structure of smart grid applications, special necessities should be considered to design cryptographic key management.

Device security is the third important factor in smart grid application security. Host data loss prevention, anti-virus, host IDS are crucial to ensure endpoints. These tools perform control of smart grid devices on security. In particular, utilizing an automated compliance control verifies that the configuration of each device is up-to-date such as the current configuration file and the firmware. Because the smart grid units are extremely connected and a vulnerability of a device could expose the whole system to a security risk, compliance control is crucial.

4.2. During-Attack

This step has two tasks. The first one is attack detection and the second one is attack mitigation. Different technologies and approaches could be utilized in each task. These tasks aim to detect malicious actions, and then apply convenient preventions.

It is very important to minimize the cyber-attack detection time, to minimize the damage caused by the attacks, to prevent the risks that will occur, and to protect the customer and system data. For a cyber-security analyst, it should be noted that monitoring is the most significant process at this step in smart grid applications. It is recommended to use all security technologies such as IDS and SIEMS in attack detection. But, some of the solutions have constraints and need enhancements [19]. IDS is a broadly utilized security solution in communication networks such as information technology and smart grid. However, it has performance restrictions in particular reporting a high rate of false positives. Therefore, it is should be developed the IDS performance in smart grid systems, especially with machine-learning-based algorithms. In [18], an IDS, data stream mining algorithms based, is proposed. A comparison between seven data stream mining algorithms are provided: leveraging bagging, bagging using adaptive-size hoeffding trees, accuracy updated ensemble, limited attribute classifier, active classifier, bagging using ADWIN, and single classifier drift. There are several metrics for comparison, such as memory consumption, detection accuracy, and execution time [20]. The authors utilized the KDD Cup 1999 dataset. The outcomes indicated that several algorithms do not need developed computational devices. Therefore, those algorithms are proper for using IDS in some components, such as a smart meter.

The mitigation step must be executed, once the attack is detected. In [21], the authors have examined and reviewed some methods utilized to mitigate DoS attacks, particularly reconfiguration and pushback methods. The network topology is modified to isolate the attacker in the reconfiguration method. The router is configured to prevent the traffic which is coming from the IP address of the attacker, in pushback method. Other mitigation techniques for CPU exhausting, MiTM, buffer overflow, replay attack, FDI, and DDoS were examined in detail in [16].

4.3. After-attack

This step is very significant if an attack is not detected. Firstly, it is crucial to determine the asset involved in the attack. Then, the security policies, antivirus database, and IDS signature have to be kept up-to-date by learning from the attacks. It results in securing the smart grid application against similar attacks. The primary way utilized after-attack is forensic analysis. Forensic studies of smart grid applications gather digital data to recognize the object involved in the attack. These data are analyzed and so used to prevent the same or similar attacks. The data are also beneficial to discover and address the physical and cyber vulnerabilities of smart grid applications to predict possible attacks. Moreover, forensic analysis plays a significant role in inspecting cyber-crimes such as cyber-terrorism, hacking, violating the consumer's privacy, digital espionage, manipulating the operation processes, and stealing valuable information in smart grid applications [22].

Table 3 shows a summary of cyber-attack steps in smart grid applications. Cyber-attack steps are maintaining access, exploitation, scanning, and reconnaissance. Each step includes cyber-attacks, attack categories, the compromised application/protocol in smart grid applications, compromised security requirements, and the possible countermeasures. Generally, cyber-attacks could be prevented by authentication and encryption techniques, and also by utilizing secure network protocols such as secure DNP3.

Cyber-attack	Attack category (with example)	Compromised protocol-application-component	Compromised security requirements	Possible countermeasures
Social engineering, Traffic analysis	Reconnaissance (Password pilfering, Phishing)	DNP3, Modbus	Confidentiality	SSL/TLS, Authentication, Secure DNP3, PKI, Encryption, Machine Learning Based IDS

Scanning Service/Port/IP vulnerabilities	Scanning (DNP3/Modbus vulnerability scanning)	DNP3, Modbus	Confidentiality, Availability	Automated security compliance checks, SIEM, IDS
Trojan, Worm, Virus	Exploitation (Stuxnet)	Control device, PMU, SCADA	Accountability, CIA Triad	IDS, IPS, SIEM, Antivirus, DLP, Signature-Based Prevention
DoS	Exploitation (Puppet attack)	SCADA, PMU, RTU, AMI, State Estimator, Communication Channel	Availability	IDS, IPS, Sensing time measurement, Reconfiguration methods, Pushback, Signal strength, Flow entropy, Transmission failure count, SIEM
Man-in-the-middle	Exploitation (Eavesdropping)	DNP3, SCADA, AMI, PLC, HMI	Integrity, Confidentiality	SSL/TLS, Authentication, Secure DNP3, Encryption, PKI
Jamming channel	Exploitation	PMU, Communication Channel, RTU, AMI, Smart Devices, PLC, Data Concentrator	Availability	Anti-jamming
Replay attack	Exploitation	PLC, Authentication schemes within AMI, SCADA, IED	Integrity, Confidentiality	SSL/TLS, Authentication, Secure DNP3, Encryption, PKI, Neural Network Based IDS
Popping the HMI	Exploitation	Substations, SCADA, EMS	Accountability, CIA Triad	Automated security compliance checks, SIEM, DLP, Antivirus, IDS
Violation of integrity	Exploitation	RTU, EMS, SCADA, AMI, Smart meter, State Estimator, Data Concentrator, PLC	Availability, Integrity	SSL/TLS, Secure DNP3, Authentication, Encryption, PKI, IDS
Masquerade	Exploitation	PLC	Accountability, CIA Triad	PKI, Secure DNP3, IDS, DLP, SIEM, SSL/TLS, Authentication, Encryption
Violation of privacy	Exploitation	Smart meter, DMS	Confidentiality	SSL/TLS, Secure DNP3, Authentication, Encryption, PKI
Backdoor	Maintaining access	SCADA	Accountability, CIA Triad	SIEM, Antivirus, Machine Learning Based IDS, IPS

Table 3 Cyber-Attacks' Effects and Countermeasures in Smart Grid

5. CONCLUSION

In recent years, the amount of cyber-attacks targeting smart grid applications has increased. So, it has attracted the interest of many researchers in academia and industry. Smart grid applications include heterogeneous and distributed devices to smartly transfer electricity and meet the ecological necessities with renewable technologies. But, this great system has some security issues. In this study, a comprehensive survey of cyber-security in smart grid applications is provided. Also, the major malicious attacks that threaten the infrastructure, applications, and network protocols are investigated in depth. Generally, a cyber-attack process has four steps. They are sequentially reconnaissance, scanning, exploitation, and maintaining access. Attackers strive to compromise any

system, based on these steps. We present the technics used to collect adequate data about the target, such as social engineering and traffic analysis in the reconnaissance step. In the scanning step, the technics used to scan the target devices are explained. In the exploitation step, malicious activities such as viruses, DoS, replay attacks are presented used to compromise and exploit the target. Lastly, we defined the cyber-attacks utilized by attackers to get continuous access to the victim system with backdoors, in the maintaining access step. We also examined the possible effects of many attacks on information security considering the CIA triad and accountability in smart grid applications. Furthermore, we suggested a generic cyber-security strategy that has three steps. The steps are before-attack, during-attack, and after-attack. We recommended some detection and countermeasures technics for each step. At the before-attack, we described several technics for network, device, and data security. At the during-attack step, we presented technics utilized to detect and mitigate cyber-attacks. We presented forensic technics to determine the asset involved in an attack at the after-attack step. Such a wide strategy could address potential security vulnerabilities, ensure customer privacy and boost communication security in the system. In addition, such a cyber-security strategy in smart grid applications presents more permanent and predictable solutions against complex and blended cyber-attacks. Also, it ensures customer privacy and boosts communication security in the system. As a future work, the detection of a cyber-attack by embedding machine-learning methods in cyber-security strategy steps will provide faster and real-time solutions in smart grid applications.

REFERENCES

[1] M. Faheem, R. A. Butt, B. Raza, M. W. Ashraf, M. A. Ngadi, and V. C. Gungor, "Energy efficient and reliable data gathering using internet of software-defined mobile sinks for WSNs-based smart grid applications," Computer Standards & Interfaces, vol. 66, p. 103341, 2019.
[2] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi,"Cyber-security in smart grid: Survey and challenges," Computers & Electrical Engineering, vol. 67, pp. 469–482, 2018.
[3] A. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, and D. Wollman, "NIST framework and roadmap for smart grid interoperability standards, release 4.0," Tech. Rep. NIST SP 1108r4, National Institute of Standards and Technology, Gaithersburg, 2021.
[4] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari and P. Dehghanian, "Electric Power Grid Resilience to Cyber Adversaries: State of the Art," IEEE Access, vol. 8, pp. 87592-87608, 2020.
[5] M. Emmanuel and R. Rayudu, "Communication technologies for smart grid applications: A survey," Journal of Network and Computer Applications, vol. 74, pp. 133–148, 2016.
[6] M. Z. Gündüz ve R. Daş , "Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik", Journal of the Institute of Science and Technology, vol. 10, Number. 2, pp. 970-984, 2020, doi:10.21597/jist.655990
[7] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, vol. 57, pp. 1344–1371, 2013.
[8] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer Networks, vol. 169, p. 107094, 2020.
[9] E. D. Knapp and R. Samani, "Applied Cyber Security and the Smart Grid," in Applied Cyber Security and the Smart Grid," Boston: Syngress, pp. 125–145, 2013.
[10] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: Challenges and solutions," International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), pp. 170–175, 2015.
[11] P. Engebretson, "The Basics of Hacking and Penetration Testing," in The Basics of Hacking and Penetration Testing (P. Engebretson, ed.), pp. 15–41, Boston: Syngress, 2011.
[12] A. Huseinovi´c, S. Mrdovi´c, K. Bicakci, and S. Uludag, "A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid," IEEE Access, vol. 8, pp. 177447–177470, 2020.
[13] P.-B. Wang, X.-M. Ren, and D.-D. Zheng, "Event-triggered resilient control for cyber-physical systems under periodic DoS jamming attacks," Information Sciences, vol. 577, pp. 541–556, 2021.
[14] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," International Conference on Artificial Intelligence and Data Processing (IDAP), pp. 1–5, 2018.
[15] Xiaoxue Liu, Peidong Zhu, Yan Zhang, Kan Chen. "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", IEEE Transactions on Smart Grid, 2015
[16] P.Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," IEEE Communications Magazine, vol. 53, pp. 206–213, 2015.
[17] Lae Lae Win, Samet Tonyali. "Security and Privacy Challenges, Solutions, and Open Issues in Smart Metering: A Review", 6th International Conference on Computer Science and Engineering (UBMK), 2021
[18] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study," IEEE Systems Journal, vol. 9, pp. 31–44, 2015.
[19] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," Journal of Information Security and Applications, vol. 52, p. 102500, 2020.
[20] Panagiotis I. Radoglou-Grammatikis, Panagiotis G. Sarigiannidis. "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems", IEEE Access, 2019
[21] X. Liang, K. Gao, X. Zheng, and T. Zhao, "A Study on Cyber Security of Smart Grid on Public Networks," IEEE Green Technologies Conference (GreenTech), pp. 301–308, 2013.
[22] M. Bouabdellah, N. Kaabouch, F. El Bouanani, and H. Ben- Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey," Journal of Information Security and Applications, vol. 38, pp. 40–49, 2018.

Authors

Muhammed Zekeriya Gündüz received the B.S. degree from the Department of Computer Science at the Suleyman Demirel University in 2006. Then he graduated M.S. degree from the Department of Computer Science at the Fırat University in 2013 and currently he is a Ph.D. student in software engineering at the same university. Additionally, he is working as a lecturer at the Department of Computer Programming in Bingol University. His current research areas include IoT applications, communication networks, and smart grid cyber-security.

Resul Daş is a Professor at Fırat University, Faculty of Technology, Department of Software Engineering. He has been working as a trainer and coordinator in the Cisco Networking Academy Program since 2002. He graduated from Fırat University Computer Science Department in 1999 and 2002, respectively. Then, in 2008, he received his doctorate degree from the Electrical and Electronics Engineering Department of the same university. He worked as a visiting professor at the Department of Computer Science at the University of Alberta, Canada, in 2017-2018. He has many articles in international conferences and peer-reviewed journals, and actively works as a referee and editor. Since 2018, he has been Associate Editor of the Journal of IEEE Access. His current research and interests include computer networks and network security, cybersecurity, software design, software quality assurance and testing, IoT, knowledge discovery, and multi-sensor data fusion.