Scientific Research Publishing

Communications and Network, 2022, 14, 119-170
https://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

Cyber-Security of Smart Grids: Attacks, Detection, Countermeasure Techniques, and Future Directions

Tala Talaei Khoei, Hadjar Ould Slimane, Naima Kaabouch

School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, USA
Email: tala.talaeikhoei@und.edu

How to cite this paper: Khoei, T.T., Slimane, H.O. and Kaabouch, N. (2022) Cyber-Security of Smart Grids: Attacks, Detection, Countermeasure Techniques, and Future Directions. *Communications and Network*, **14**, 119-170.
https://doi.org/10.4236/cn.2022.144009

Received: October 12, 2022
Accepted: November 21, 2022
Published: November 24, 2022

Abstract

One of the significant challenges that smart grid networks face is cyber-security. Several studies have been conducted to highlight those security challenges. However, the majority of these surveys classify attacks based on the security requirements, confidentiality, integrity, and availability, without taking into consideration the accountability requirement. In this survey paper, we provide a classification of attacks based on the OSI model and discuss in more detail the cyber-attacks that can target the different layers of smart grid networks communication. We also propose new classifications for the detection and countermeasure techniques and describe existing techniques under each category. Finally, we discuss challenges and future research directions.

Keywords

Smart Grid, Architecture, Cyber-Attacks, Network Security, Confidentiality, Integrity, Availability, Accountability, Countermeasures, Detection Techniques

1. Introduction

The traditional power grid is no longer a practical solution for power delivery and distribution due to several shortcomings including: chronic blackouts, energy storage issues, high cost of assets, and high carbon emissions. Briefly, several cases prove that there is a serious need to improve the functionality of the traditional power system. For example, in February 2020, the storm Ciara caused a power cut for around 130,000 homes in France. During the same month, in Bavaria, the storm Sabine caused a blackout for approximately 60,000 homes [1]. In March 2016, at least 70 million people in Turkey were

impacted by a power blackout. These examples are the obvious reasons why using a traditional power grid is no longer considered an effective power system [2].

To address the limitations of the traditional grid, a new approach, microgrid, was introduced. A microgrid can be defined as a local and small distribution system that consists of sets of micro sources, namely micro turbines, fuel cells, photovoltaic arrays wind turbines, and some storage systems like energy capacitors. It can be connected to a main grid or work independently. Microgrids provide some benefits, such as a higher efficiency, reduction of emissions, and cheaper and cleaner energy. Also, this technology deals with some challenges, including the resynchronization with the main grid, which can be problematic to the network, due to the network inconsistency. To address these challenges and limitations, a holistic solution, smart grid, was proposed [3] in 2007. This new electrical grid includes a variety of operations and energy measures, including smart meters, smart appliances, renewable energy resources, and energy-efficient resources. It utilizes information technology to deliver energy to end-users through a two-way flow of communications, which changes the power infrastructure in terms of efficiency, scalability, reliability, and interoperability.

The National Institute of Standard and Technology (NIST) state that smart grids consist of seven logical domains, namely bulk generation, transmission, distribution, customer, markets, service provider, and operations. These logical domains have actors and applications that are presented as smart grid's conceptual model. Actors are defined as programs and systems, while applications are considered as tasks. These tasks are conducted by a single or multiple actors in every domain. In the customer domain, the major actor is the end-user, which is divided into three types: home, commercial, and industrial. This domain mainly has a close communication with the distribution, operation, service provider, and market domains. Within the market domain, the users have to be the operators that participate in electricity markets. The service provider consists of the organizations that can provide services to customers and utility companies. More importantly, the bulk generation domain has some electric generators in bulk quantities, and the transmission domain can carry out the generated electric power over long distances from the generation domain to the distribution domain via a variety of substations [3]. The transmission network can monitor and control via Supervisory Control and Data Acquisition (SCADA) system. The distribution domain can distribute the electricity to and from end-users in different structures, like radial, looped, or meshed. This domain is capable of supporting energy generation and storage, which is mainly connected to the transmission domain, customer domain, and metering points for electricity consumption [4].

The smart grid is expected to create a reliable, efficient, and clean energy distribution by combining various technologies. It promises reliability, improved

efficiency, and economical means of power transmission and distribution. It also reduces greenhouse emissions to deliver clean, affordable, and efficient energy to users [4]. However, this infrastructure can be subject to cyber-attacks that can violate the availability, integrity, confidentiality, and accountability of smart grid's security requirements. For example, in March 2018, a cyber-attack launched on a U.S. power grid targeted numerous nuclear power plants and water facilities. Another instance of cyber-attacks happened in Ukraine in December 2015. During this incident, the attackers turned off 30 substations that led to a complete blackout for about 6 hours, leaving around 230,000 people without electricity. To improve the security level of the power systems, the US National Electric Sector Cybersecurity Organization (NESCOR) and the Department of Energy (DOE) joined their efforts. For this purpose, they collaborated with some federal U.S. agencies, such as the Cybersecurity for Energy Delivery Systems (CEDS) and the Federal Energy Regulatory Commission (FERC). They involved experts, developers, and users to test the security of the power systems. They collaboratively worked together to enhance security risks of smart and mitigation strategies. Their investigations proved that using this modern technology requires some holistic solutions to defend and prevent cyber-security issues. Despite the critical advancements of smart grids, the detection and prevention of sophisticated cyber-attacks are still at an early stage and need more attention [5] [6].

Over the last decade, several surveys provided an overview of smart grid's cyber-security, as shown in **Table 1** [7]-[16]. The authors of [7] [8] [9] [11] [14] reviewed the main cyber-attacks that can damage the smart grid infrastructure, the detection techniques, and the countermeasures. In [10] [16], the authors mainly focus on the cyber-physical attacks in smart grid networks, their impacts, along with their defense strategies. In [16], the authors also highlight a classification for detection techniques for cyber-physical attacks in smart grids and compare the efficiencies of various detection techniques. In [12], the authors review cyber-security related to smart homes and smart grid networks. They classify cyber-attacks in smart home/smart grid networks according to confidentiality, integrity, availability, authorization, and authenticity. The authors of [15] also provide a survey on cyber-security and privacy of smart metering networks. They briefly review cyber-attacks in traditional power systems and smart grid networks and introduce future research trends in depth.

As shown in **Table 1**, the aforementioned studies did not cover several aspects of smart grid security. Therefore, our study fills the gaps by providing a comprehensive classification for cyber-attacks in the smart grid. This study also provides a new classification for both detection and countermeasure methods, while the previous works did not provide such security strategies. Precisely, in this paper, we present an in-depth survey of technological advances in smart grid infrastructure security. First, we provide a classification of cyber-attacks that target the OSI communication layers. We also propose two classifications, one for

Table 1. Existing surveys related to the cyber-security of smart grids.

Related Work	Topic	Cyber-Attacks Mentioned	Concepts Covered	Concepts Not Covered
[8]	Survey on cyber-security solutions of IOT-based smart grids.	Different kinds of cyber-attacks against CIA tirade and five OSI communication layers.	Cyber-attack types and the general importance of countermeasures. Analysis of various cyber-attacks and their security requirements along with future directions.	Countermeasure methods and detection techniques.
[9]	Survey on security communications in smart grids.	Traffic analysis, social engineering, scanning I.P., scanning port, scanning vulnerability, worms, DoS, FDI, replay, privacy violation, backdoor.	Cyber-physical security of smart grids, and potential IT-based attacks scenarios. Detection/protection methods and challenges regarding to threats of smart grids.	Accountability as a security requirement in smart grids.
[10]	Survey on cyber-physical attacks and solutions in smart grids.	Generation system attacks, transmission system attacks, distribution system/customer side attacks, electricity market attacks.	Critical cyber-physical attacks and their defense methods. Analyzing the impact of cyber-physical attacks in smart grids.	Detection techniques for cyber-physical attacks in smart grids.
[11]	Survey of cyber-security in smart grids.	DoS/ DDoS attacks	Smart grid and its components. Existing methods for communication protocols and their architectures. DoS/DDoS attacks and their impacts on smart grids.	Existing cyber-attacks that targets smart grids, their countermeasures, and detection techniques.
[12]	Comprehensive review of cyber-attacks and their solutions in smart grids.	Traffic analysis, social engineering, scanning IP, scanning port, scanning vulnerability, worms, Trojan horse, DoS, FDI, replay, privacy violation, integrity violation, backdoor, MITM, jamming, popping the HMI, masquerade.	Important cyber-attacks in smart grid and their impacts. Various security methods to address cyber-security issues in smart grids.	Detection techniques and countermeasure approaches.
[13]	Survey on cyber-security in smart homes and smart grids.	Different kinds of cyber-attacks against confidentiality, integrity, availability, authorization, authenticity.	Most common threats against smart homes and smart grids. Different cyber-attack scenarios with their specific countermeasures. Methods to defend against or prevent cyber-attacks.	Smart grid cyber-attacks, countermeasures, and detection techniques.
[14]	Survey on cyber-security aspects of IOT aided smart grids.	MITM, jamming, FDI, spoofing, DoS, malware, replay attacks.	Bibliometric analysis of published journals. Different cyber-attacks targeting smart grids and their security mechanisms. Future trend of smart grid cyber-security.	Countermeasure techniques.
[15]	Survey of cyber-security and privacy of smart grid metering networks.	Different kinds of attacks on energy companies, renewable energy resources, and metering networks.	Cyber-attacks vulnerabilities in the traditional energy network. Security and privacy requirements for smart grid metering networks. Future research trends and challenges.	Countermeasures and detection methods.

Continued

[16]	Survey on detection techniques for cyber-physical attacks in smart grids.	Different kinds of cyber-physical attacks that take place in smart grids.	Cyber-physical attacks and the classification of detection techniques in smart grids. Analysis of false data injection attacks and their impacts. Study of future trends and their challenges.	Countermeasure techniques.

detection techniques and another one for countermeasure methods.

The contributions of this survey are summarized as follows:

- Review and classification of cyber-attacks in the smart grid network.
- Description and comparison of these attacks, along with their purposes and impacts.
- Review, analysis, and classification of detection techniques.
- Analysis and classification of countermeasure methods.
- Discussion of the challenges and open issues related to the security of smart grid and future research directions to address them.

The remaining of this paper is organized as follows: Section II provides an overview of the smart grid system and its features and architectures. Section III describes the smart grid architecture, its technologies, and protocols. Section IV reviews the smart grid's security, discusses the security requirements that are expected to be met, and provides a classification of cyber-attacks that target the OSI communication layers. The purposes and impacts of these cyber-attacks are also evaluated in this section. Section IV also provides a classification of detection techniques, the state-of-the art in detection techniques, and summarizes existing countermeasures against various cyber-attacks. Section V describes several research challenges and future research directions. Finally, Section VI closes the survey with a conclusion.

2. Overview of Smart Grid

In this section, we mainly discuss the smart grid's features and applications. In the following, we provide a short description of the most critical features in smart grids and the important applications in this network.

2.1. Smart Grid's Features

The significant features expected from the smart grid are improving grid resilience, self-healing, increasing environmental and system performance [7] [17]. Grid resilience means that the power grid can recover quickly and fulfill the mission during power interruptions and outages [18]. This can be provided by adding extra disperse power supply and integrating modern resources into the power grid when an interruption happens [19]. The self-healing feature allows the system to identify faults quickly, decrease the duration of the outage, and help the system to recover faster. Therefore, by providing a higher level of flexibility

and reliability, the grid's resilience and self-healing features have a critical impact on the economy [20].

Another expected feature in the smart grid is improving system's performance. In the traditional power grid, energy loss may happen due to several reasons, including faults in power stations or damages in transmission lines. The smart grid promises to increase the system performance by optimizing asset utilization and operations, reducing energy costs, and transmitting electricity in an effective manner. These benefits may directly increase the quality of power and efficient asset management, which indicates the increased level of system performance [20]. Moreover, the smart grid is expected to expedite the replacement of electric vehicles with conventional vehicles. These replacements may lead to enhance environmental performance by reducing the energy used for end-users and decreasing energy loss through the grid [19].

2.2. Smart Grid Applications

As illustrated in Figure 1, the smart grid includes a variety of heterogeneous, distributed applications and capabilities, such as Advanced Metering Infrastructure (AMI), Supervisory Control and Data Acquisition (SCADA), Substation Automation, Electrical Vehicles (E.V.s) charging, Demand Response Management (DRM), Outrage Management (O.M.), Distribution Management (D.M.), and Home Energy Management (HEM) [21] [22]. This section will discuss three vulnerable applications in the smart grid infrastructure, namely AMI, SCADA, and DRM. The other applications were discussed in detail in [21]-[28].

Advanced Metering Infrastructure (AMI) is one of the essential components of smart grid infrastructure. AMI is mainly responsible for reading the power usage of home appliances and some other integrated devices, such as water heaters,

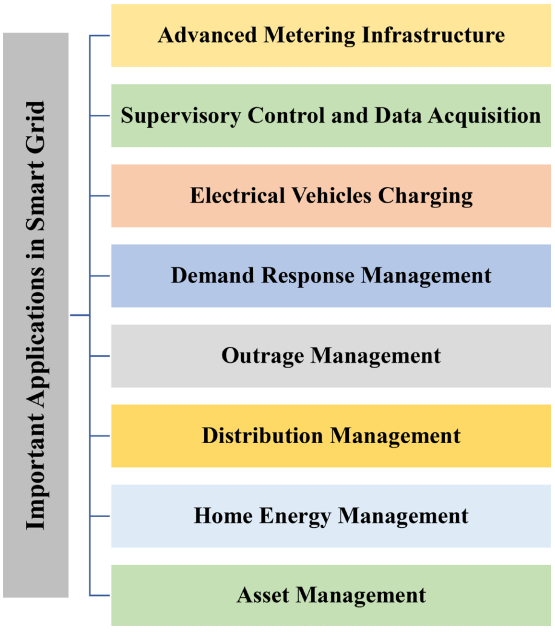

Figure 1. Important applications in the smart grid.

gas meters, smart thermostats, rooftop photovoltaic systems, etc. AMI consists of three main components: a smart meter, a data concentrator, and a central system (AMI headend), with a two-way flow of communications between these components [29]. The meter data that are collected from the power usage of home appliances are received by the AMI host system and transmitted to the meter data management system (MDMS). MDMS is responsible for data storage management and data analysis for the utilities. The AMI system provides financial benefits and increased service quality (multi-utility service and multi-vendor service) [30].

Supervisory control and data acquisition (SCADA) are a type of Process Control System (PCS) that is responsible for monitoring, measuring, and analyzing real-time data of the electrical power grid [7]. SCADA mostly effective for large-scale environments; however, it can ensure both short-range and long-range communications [31]. This system consists of three main elements: The Remote Terminal Unit (RTU), Master Terminal Unit (MTU), and Human-Machine Interface (HMI). RTU, as a device, consists of three components. The first component is the one that can perform data acquisition, the second component runs logic programs that are coming from the MTU, and the third component is mostly responsible for developing the communication infrastructure [32]. Another element in SCADA is the MTU, which is a device for monitoring and controlling the RTU. As the last element in SCADA, HMI considers as a graphic interface for the SCADA operator [22].

Demand Response Management (DRM) is one of the essential systems in the smart grid infrastructure. This system refers to the routines conducted to control the energy consumption of consumers. DRM can achieve a balance between electrical energy supply and demand. DRM's benefits are to decrease the peak-to-average ratio of the demand and power supply, reduce user bills and power generation costs, improve energy efficiency, and address short-term reliability [22].

3. Smart Grid Architecture

As the smart grid infrastructure connects a huge variety of systems, the hierarchical architecture of the smart grid with few sub-networks is considered critical in the infrastructure; however, each sub-network is only responsible for specific geographical regions. Smart grid network includes three main sub-networks, Wide Area Network (WAN), Neighborhood Area Network (NAN), and Home Area Network (HAN), as shown in **Figure 2** [33]. To these three sub-networks, the authors of [34] add several sub-networks, namely Field Area Network (FAN), Local Area Network (LAN), and Building Area Network (BAN). BAN is divided into two sub-networks, Home Area Network (HAN) and Personal Area Network (PAN), as shown in **Figure 3**.

WAN is one of the major networks in the smart grid architecture. In [35], the authors highlight WAN as the main network that can create a connection backbone to connect highly distributed smaller networks for power systems at various

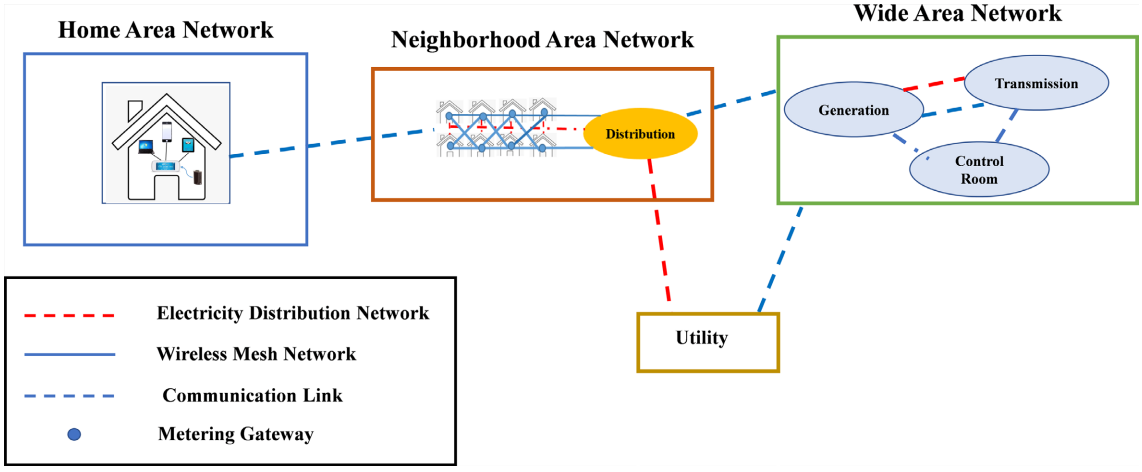

Figure 2. Main sub-networks in the smart grid architecture.

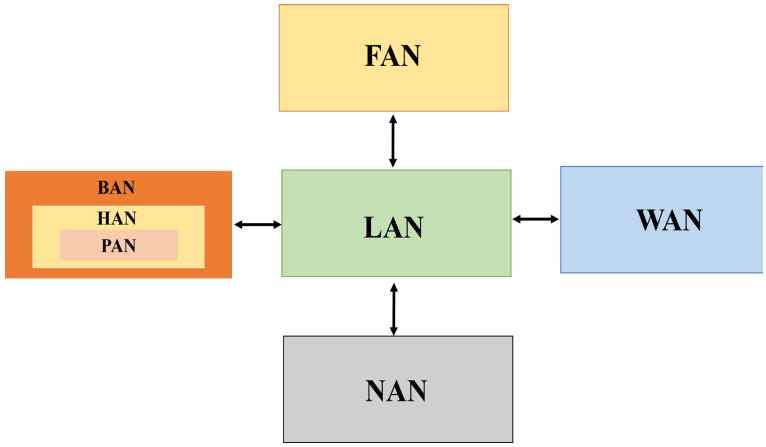

Figure 3. Different communication networks in smart grids.

locations. This network is a high-bandwidth connection network, which can deal with long-distance data transmission over advanced monitoring and sensing applications. WAN provides a bidirectional communication for automation, monitoring, and communication of smart grid systems. The authors of [36] describe the NAN as a network that is expected to connect smart meters and distribution automation devices to the WAN gateways. It is a bridge between user premises and substations with access points, collectors, and data concentrators. This sub-network may be considered as low bandwidth that is highly robust for secure data communication.

HAN is necessary for customers to monitor and control smart devices and execute some functionalities, such as DRM and AMI. It allows users to know about their electricity consumption cost and handle their usage behaviors. According to [37], this network supports low-bandwidth communication between home appliances and smart meters. In [35], the authors define BAN as a network that can perform any communications among homes and offices within a building. PAN is responsible for any communication between personal appliances, such as laptops, tablets, phones, etc. In LAN and FAN, any distant communica-

tion in backhaul networks, smart homes, factories, or even power generation plants can be performed.

In a sophisticated smart grid architecture, different networks demand various communication technologies and protocols to deliver reliable and secure data or power to utilities and users. In the following sections, we will describe smart grid communication technologies and few numbers of well-known protocols.

3.1. Smart Grid Communication Technology

In smart grid, secure, reliable, and real-time information is considered a key factor for an efficient delivery of power between generators and users. Equipment failures, natural accidents, catastrophes, and capacity constraints can be the main reasons for power disturbances in grid systems. To deal with these issues, new communication and information technologies with modern intelligent monitoring systems play an indispensable role in securing data transmission between smart meters and utilities, while they apply two different communication media, namely wired and wireless. In [38], the authors discuss the benefits of wired and wireless communication technologies. In this study, the authors highlighted some of the benefits of wireless communications over wired communications, such as reasonable infrastructure prices and stronger connections in unreachable regions; however, this technology is only able to provide a connection in short distances with low data rates, compared to wired communications. Wireless technologies include Zonal Intercommunication Global-standard (Zigbee), Z-wave, worldwide interoperability for microwave access (WiMAX), Wi-Fi, DASH7 (D7A), and cellular and satellite.

Wired communications also have some advances. For example, it can provide higher connection capacity and shorter communication delay with less interference in comparison with wireless communication. Examples of wired communication technologies include Powerline Communication (PLC) and Digital Subscriber Lines (DSL) [39]. In this section, we mainly focus on satellite, PLC, and DSL. For further reading, Zigbee, Z-wave, WiMAX, WiFi, DASH7, and Cellular are discussed in detail in [39]-[44]. Main features, including bandwidth, coverage rate, data rate, application, and application area of the most common communication technologies along with their standards, are summarized in **Table 1**. More details about smart grid communication technologies can be found in [38]-[48].

PLC is a wired communication technology that can support high-speed data from one device to another one. It simply connects smart meters to a data concentrator via a power line, and its data can be transmitted to the data center with cellular network technologies [39]. It is suitable for some applications, including smart metering, home automation, Heating, Ventilation and Air Conditioning (HVAC) control, and lighting. This technology reduces installation costs; however, it has some technical issues, including low bandwidth, high dependency on Quality of Service (QoS), and high sensitivity to disturbances. Because of these

limitations, PLC does not provide full connectivity, and it has to be combined with other technical communications, such as General Packet Radio Services (GPRS), and Global System for Mobiles (GSM) [39] [40] [41].

Digital Subscriber Lines (DSL) is another wired communication technology that has fast speed digital data transmission and can conduct effectively on the voice telephone network [40]. Although this technology provides cheap, high data bandwidth, and expected availability, it has some disadvantages, such as lack of reliability, downtime, and proper standardization. In [35], the authors also mention that as this technology requires cables, it is difficult to use in rural areas due to high installation expenses in low-density regions. Satellite communication is one instance of wireless communication technology that is usually used in radio broadcasting, plane TVs, and vehicles. Although this technology provides some benefits, including reliability and flexibility, its performance heavily impacted by weather conditions [35], and it is not considered cost-effective. Satellite communication also reduces the need for backhaul networks, which demonstrates a good fit for smart grid infrastructure [42] [43]. This technology can provide SCADA and distant communication remote substations, making it a viable option for future use.

3.2. Smart Grid Protocols

Initially, the Transmission Control Protocol/Internet Protocol (TCP/IP) was used in the smart grid to ensured end-to-end data communications. However, this protocol is not considered a good option for smart networks due to its sophisticated memory management problems and the fact that it is only suitable for wide area networks. Alternatively, several different smart grid protocols were developed to meet the different smart network requirements [44]-[49].

SCADA and AMI are important key components in smart grid infrastructure. A few protocols were developed over the years to provide secure and reliable communications for these systems. The main technologies are shown in **Table 2**. The communication within SCADA depends on several industrial protocols, such as Modicon communication bus (Modbus), Distributed Network Protocol version 3 (DNP3), Process field bus (Profibus), and International Standard Defining Communication Protocol 61850 (IEC61850). However, the communications among the AMI, home appliances, and smart meters are done through various communication protocols. They vary widely in their inherent security requirements and vulnerabilities. In this section, we mainly focus on four vulnerable protocols that are used in smart grid infrastructure, including Modbus, DNP3, Profibus, and IEC61850.

According to [50], DNP3 is an optimized open communication protocol used for power grid equipment. Initially, this protocol's major aim was to be used in the traditional power grid; however, this protocol has recently been used as a solution for delivering data measurements in the smart grid because of its reliability, efficiency, and compatibility in comparison with previous protocol versions.

Table 2. Communication technologies of smart grids.

Technology	Frequency	Coverage Rate	Data Rate	Application	Application Areas
ZigBee	915 MH and 2.4 GHz	30 - 100 m	Up to 250 Kbps	HAN	Energy Monitoring, Automatic Meter Reading, Home Automation
PLC	24 - 500 KHz	1 - 3 Km	2 - 3 Mbps	HAN NAN	Automatic Meter Reading, Low Voltage Distribution
Bluetooth	2.402 - 2.48 GHz	1- 30 m	1 Mbps	HAN	Home Automation
Fiber Optic	100 - 1000 THz	AON: up to 10 Km BPON: up to 20 - 60 km EPON: up to 20 km	AON:100 Mbps up/down BPON:155 - 622 Mbps EPON: 1 Gbps	WAN	AMI, Metering reading, Distribution automation, Service switch operation Demand response, Wide-area monitoring
WiFi	2.4 and 5 GHz	Up to 1 Km	Up to 600 Mbps	HAN, FAN NAN, BAN, WAN	AMI
WiMAX	2.3 - 2.7 and 3.4 - 3.6 GHz	Almost 10 - 100 Km	Up to 75 Mbps	HAN, NAN FAN, WAN	Wireless Automatic Meter, Reading, Outage Detection, AMI
GSM	850 - 1900 MHz	1 - 10 Km	14.4 Kbps	HAN	AMI, Demand Response
Satellite	1 - 40 GHz	100 - 6000 km	Iridium: 2.4 - 28 kbps Inmarsat - B: 9.6 up to 128 kbps BGAN: up to 1 Mbps	WAN	AMI, Remote generation plants, Electric Vehicles Remote automation, Distribution Automation
GPRS	800 - 1900 MHz	1 - 10 Km	179 Kbps	HAN	AMI, Demand Response
Z-Wave	868 and 915 MHz	30 - 100 m	40 Kbps	HAN	Home automation, energy automation
DSL	4 KHz - MHz	ADSL: up to 5 Km ADSL2: up to 7 km ADSL2þ: up to 7 km VDSL: up to 1.2 km VDSL2: 300 m - 1.5 km	ADSL: 8 Mbps down/1.3 Mbps up ADSL2: 12 Mbps down/ 3.5 Mbps up ADSL2þ: 24 Mbps down/ 3.3 Mbps up VDSL: 52 - 85 Mbps down/16 - 85 Mbps up VDSL2: up to 200 Mbps down/up	HAN NAN WAN	Smart Grid City Smart Metering
LTE Mobile Network	0.41 - 2.1 GHz	5 - 30 Km	75 Mbps - 300 Mbps	HAN	AMI Demand Response

The DNP3 inherently was not a secure protocol; hence the authentication features were added to DNP3 protocol to addresses the security issue. Modicon communication bus or Modbus is another protocol designed in 1979 as a serial

communication protocol to permit communication between various machines over twisted wires. This protocol consists of three types, Modbus American Standard Code for Information Interchange (ASCII), Modbus Remote Terminal Unit (RTU), and Modbus Transmission Control Protocol (TCP). In general, Modbus ASCII enables the messages to be coded in hexadecimal, while this is the slowest type of Modbus in comparison with other types, and it is ideal for telephone modems. In Modbus RTU, the messages are expected to be coded in a binary manner. Modbus RTU is suitable to be applied over RS232 and can generate communications between master and slaves by using their IP addresses instead of their device addresses. Modbus TCP is defined as a specific data frame protocol, which has a function code for an action that has to be completed. This protocol is particularly one of the most popular industrial control protocols, which generates a simple request or reply method between the control center and field devices [51].

Process Field Bus (PROFIBUS) is yet another communication protocol in smart grid infrastructure used for automation technology [52]. This protocol is considered as one of the well-known Fieldbus protocols standardized as EN50170. PROFIBUS can address the real-time requirements on MAC layer. It is used as a token-passing protocol, same as IEEE 802.4 in a Token Bus. This protocol is mainly divided into two categories, PROFIBU Decentralized Peripherals (DP) and PROFIBUS Process Automation (PA). PROFIBUS DP is used for conducting sensors and actuators via centralized controllers, and the PROFIBUS PA can be used in hazardous areas, and it is mainly designed as an improvement version of some convenient systems, like Highway Addressable Remote Transducer (HART) in process automation.

Another protocol is IEC 61850 [53], also known as the communication protocol in the smart grid, is mainly designed for communication networks and systems in order to provide better interoperability between Intelligent Electronic Devices (IEDs). It provides several opportunities to increase the efficiency of the grid and reduce its cost. This protocol can introduce five variant types of communication services, including Abstract Communication Service Interface (ACSI), Generic Object-Oriented Substation Event (GOOSE), Generic Substation Status Event (GSSE), Sampled Measured Value multicast (SMV), and Time Synchronization (T.S.).

4. Security of Smart Grid

With the transformation of traditional power grids to smart grids, the security became one of the critical challenges in the last few decades. To address this challenge, the system and its infrastructure must be designed following secure architectural conditions. Therefore, cyber-security as an integral and complimentary process needs to follow a set of comprehensive security requirements. Initially, the National Institute of Standards and Technology (NIST) defined three security requirements that need to be met in the smart grid: confidentiality, integrity,

and availability. However, the authors of [54] demonstrate that accountability also plays an important role in the security of smart grids.

In general, when unauthorized access to some information happens, confidentiality is lost. While integrity seeks to deliver accurate data by protecting it from any improper modification or data destruction done by an unauthorized user. Availability, on the other hand, is defined as an important aspect of smart grids that can guarantee access to the system's data. Loss of availability indicates that the data is not available or accessible to use by users. In addition to the requirements previously mentioned, accountability plays an important role in smart grid security; it guarantees the system's traceability that must be recorded by a person, device, or public authority. Moreover, the recorded data can be used as an evidence in case of an attack to prove the action made by every user, or even administrator, and the integrity of the data collected from each device [5]. Hence, following these four requirements, including confidentiality, integrity, availability, and accountability can provide adequate protections to smart grid infrastructures.

Due to the inherent vulnerabilities of communication, smart grid networks are subject to several cyber-attacks, which can be classified in different ways. In the following section, we discuss existing cyber-attack classifications along with our proposed classification, and describe the possible attacks, with their purposes and impacts on the networks.

4.1. Classification of Cyber-Attacks in Smart Grid

Figure 4 provides a visual representation of existing cyber-attack classifications in smart grids. In [55] [56], the authors classify these cyber-attacks based on the security requirements, confidentiality, integrity, and availability; however, they excluded accountability from this classification [7] [54]. As shown in **Figure 4**,

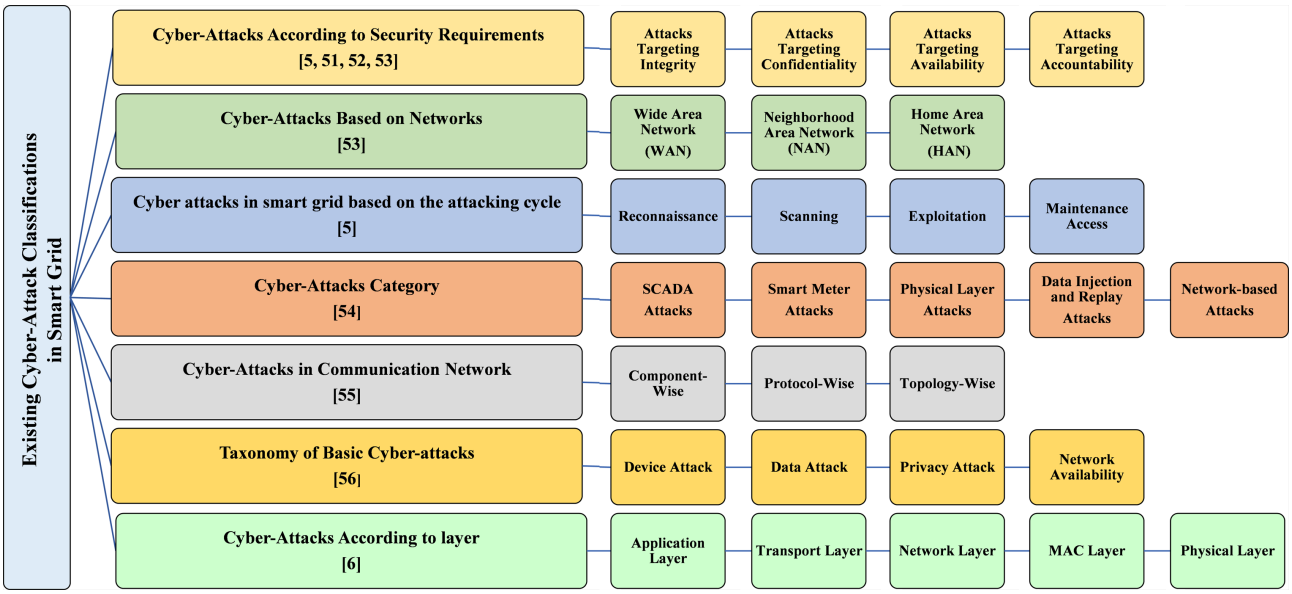

Figure 4. Review of the current classifications of cyber-attacks in smart grids.

the authors of [56] also provide another cyber-attack classification, which is according to the subnetworks and architecture of smart grids, namely home area network, wide area network, and neighborhood area network. This classification does not include cyber-attacks on the other sub-networks, such as Building Area Network (BAN), Field Area Network (FAN), and Personal Area Networks (PAN). In this paper, the authors also describe the impact of each cyber-attack on three security requirements (confidentiality, integrity, and availability), while they excluded the attacks targeting accountability [57].

In [7], the authors propose a classification based upon the attacking cycle, including reconnaissance, scanning, exploitation, and maintenance access, as shown in **Figure 4**. This classification also did not include all cyber-attacks. Several cyber-attacks, such as intrusion, brute-force, and spoofing attacks, are primary concerns in a smart grid, and they require multiple security mechanisms. However, these attacks are not included in the classification. As illustrated in **Figure 4**, the authors in [58] also provide a general classification divided into three categories: component-wise, protocol-wise, and topology-wise. The authors indicate that some cyber-attacks such as replay attacks and eavesdropping attacks might be excluded from this classification. The authors of [59] propose a taxonomy of basic cyber-attacks, including devices, data, privacy, and network availability attacks. This classification also does not include cyber-attacks like social engineering attacks. In [8], the authors classify cyber-attacks according to five communication layers, including the application layer, transport layer, network layer, MAC layer, and physical layer. Several attacks target the session layer and presentation layer, which both were excluded from the classification. This paper also did not provide clear descriptions of cyber-attacks, with their impacts, purposes, and security requirements they target, and did not cover the detection and mitigation techniques.

A number of survey papers related to cyber-attacks on smart grid networks have been published over the last decade. Some of these papers focus on cyber-attacks that target one or some of the communication layers, such as the physical layer or the network layer. For example, a survey published in 2020 focused on the attacks based on the layers of the TCP/IP model; however, the TCP/IP model does not distinguish between the cyber-attacks that target the application, presentation or session layer and the data link or physical layer. Therefore, motivated by the limitations of the current studies, we classify cyber-attacks on smart grids based on the seven communication layers of the OSI model, which provides a comprehensive conceptual detail of the networking process. The seven layers of this model are introduced to perform a set of unique functions in a data communication. As a result, the OSI model is more detailed and informative compared to the TCP/IP model. Since several cyber-attacks may target these layers, it is important to select a model that considers a set of distinct functions for every layer. Therefore, we classify the cyber-attacks in smart grids into the physical, data-link, network, transport, session, presentation, and appli-

cation layers.

4.2. Cyber-Attacks in Smart Grid

As we mentioned, multiple cyber-attacks may target smart grid infrastructures. Figure 5 illustrates possible cyber-attacks in a smart grid, with their target layers in OSI model. According to this figure, multiple cyber-attacks can target the same communication layers or target more than one layer simultaneously. In the following, we describe these cyber-attacks, along with their purposes, targeted layers' impacts, and their security requirements, as summarized in Table 3.

One of the cyber-attacks that are more likely to occur in a smart grid is jamming. In these attacks, an attacker broadcasts continuous or random signals to keep the channel busy and prevent authorized devices from transmitting and receiving [7] [59]-[67]. Different types of jammers include constant, random, deceptive, and reactive jammers [64] can target the physical layer [55] [8] [59] [60] [61], data-link layer [8], and network layer [62] of the smart grid, which can compromise the availability of the network [7] [8] [57].

Spoofing attacks are yet another category of cyber-attacks that target smart grid networks. This category includes identity/data spoofing, Address Resolution Protocol (ARP) spoofing, Global Position System (GPS) spoofing, IP spoofing, and Media Access Control (MAC) spoofing. In any of these attacks, the spoofer pretends to be a legitimate node [7] [8] [57] to mislead other nodes in the network in order to disrupt the security, reliability, stability, and operation of the

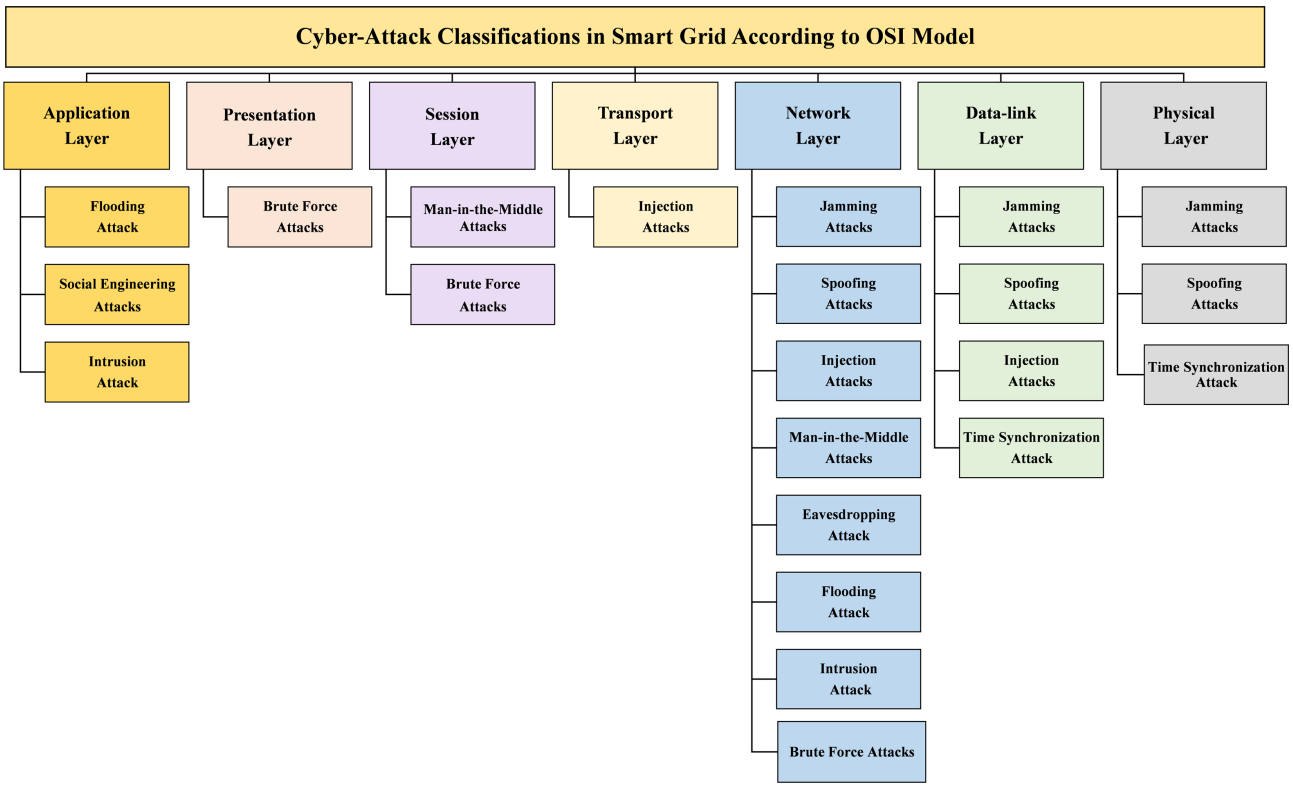

Figure 5. Cyber-attack classification based on communication layers.

Table 3. Cyber-attacks in smart grids.

Cyber-Attacks	Objectives/Purpose	Targeting Layers	Impacts	Security Requirements
Jamming Attacks	Disrupting the transmission and the reception of data.	Physical Data Link Network	Blocking one or several nodes to transmit and receive information collisions.	Availability
Spoofing Attacks	Pretending to be a legitimate node to compromise the system.	Physical Data Link Network Transport	Misleading other nodes.	Integrity Availability Confidentiality Accountability
Injection Attacks	Injecting false/untrusted data packets into a network.	Data Link Network Transport Application	Injecting false data Corrupting the legitimate processes and operations Appearance of illegitimate nodes in the network.	Integrity
Flooding Attack	Depleting, and exhausting system resources.	Data Link Network Transport Application	Malfunction of nodes and loss of availability in a network.	Availability
Man-in-the-Middle Attacks	Preventing, or modifying data during transmission through the network.	Data Link Network Session	Unauthorized access to sensitive information.	Integrity Confidentiality
Social Engineering Attacks	Manipulating users to reveal sensitive information.	Application	Violation of users' privacy. Temporary or permanent damage to the system. Steal sensitive and private information. Identity theft.	Confidentiality
Eavesdropping Attack	Monitoring and capturing all network traffic.	Physical Network	Loss of privacy.	Confidentiality
Intrusion Attack	Gain illegal access to the node or network.	Network Application	Misusing available resources in the network.	Integrity Confidentiality
Brute Force Attacks	Cracking usernames and passwords.	Network Session Presentation	Gaining unauthorized access to users' system or accounts.	Integrity Confidentiality
Time synchronization Attack	Targeting timing data and disrupting the time synchronization between nodes.	Physical Data Link	Compromising events, such as location estimation and fault detection Performance degradation.	Integrity Availability
Traffic Analysis Attack	Control the hosts and the devices that are connected to the network.	Data Link	Sniff and analyze the message in order to achieve information about the patterns of communications between nodes.	Confidentiality
Masquerade Attack	Pretend to be an authorized user.	Data Link	Gaining unauthorized access to users' system.	Integrity Availability Confidentiality Accountability

Continued

Smart Meter Tampering Attack	Modification the transmitted data for any customers.	Physical	Pay higher or lower electricity bills.	Integrity
Buffer Overflow Attack	Sending improper or incorrect data to the specific system.	Transport Application	System crash or exhaust resources.	Availability
Puppet Attack	Sending fake data in the AMI network.	Network	Reduce packet delivery to 10% or 20% Exhaust the communication network bandwidth.	Availability
Teardrop Attack	Modification of the length and the fragmentation offset in sequential IP packets.	Network	System crash.	Availability
Smurf Attack	Modifying the traffic of an entire system.	Network	Replay and saturate the target network.	Availability
Popping the HMI Attack	Get unauthorized access	Application	Controling the compromised system.	Integrity Availability Confidentiality Accountability

network [8], which can violate the integrity, the confidentiality and the accountability of the smart grid [8] [57]. These attacks can target the physical layer [60]-[70], the data link layer [2] [8] [71], and the network layer [72].

According to the authors of [73], injection attacks can be conducted when an adversary attempts to delete, alter and add new manipulated data to the network, which may disrupt the smart grid operations and lead to a blackout. Violation of the data integrity, corruption, and appearance of illegitimate nodes in the network are also considered as other impacts of this type of cyber-attacks. Like the above-described attacks, injection attacks can target one or several communication layers, such as the data-link layer [8] [72], network layer [8] [72], and transport layer [8] [74]. Another potential cyber-attack that targets smart grid networks, as illustrated in **Figure 5**, is the flooding attack which aims to flood the network with several random packets and requests. This attack can occur in the application layer [8] [74] and the network layer [57] to disrupt the system's availability. It may exhaust the target's resources by processing the received fake messages [75]. Another impact of this attack is the lack of node functionality in the network [73].

Other cyber-attacks on smart grid infrastructures are the Man-in-the-Middle (MITM) attacks. Such cyber-attacks target the network layer [8] [13] and the session layer [76]. MITM in a smart grid is performed when an adversary intercepts the traffic by inserting himself between two authorized devices, connecting to the devices, and relaying the traffic between them [7] [10]. The devices seem to communicate directly; however, the adversary is communicating with these devices as a third device [7] [8]. The main purpose of this kind of cyber-attacks is to prevent network data from being transmitted, modify it during the transmission, and gain unauthorized access to valuable data [7] [26]. MITM also can

compromise the confidentiality and integrity of the network [57] [75].

Other possible cyber-attacks on smart grid infrastructure are social engineering attacks. These attacks target the application layer and violate the confidentiality of the system [77] [78]. In [78], the authors state that social engineering attacks are considered the biggest cyber-security threat. They describe several types of social engineering attacks, including phishing, pretexting, baiting, tailgating, ransomware, fake software, reverse social engineering, phone/windows fraud, and robocalls attacks. All these attacks aim at manipulating users in order to discover and steal valuable and sensitive information. Violating consumers' privacy, identity theft, and stealing sensitive information are the consequences of these attacks.

Eavesdropping attack is another well-known passive attack on smart grid communication channels that targets the network layer [8] [79] [80] [81] and compromises the confidentiality security requirement of the smart grid [8]. In [57], the authors explain that eavesdropping attacks occur when a malicious user listens to the communication between two nodes on a LAN network and gains access to some information. The malicious user may also use this private data to disrupt or compromise the network [8]. These attacks violate the privacy requirement of networks [57] [81].

Time Synchronization Attacks (TSA) are well-known potential cyber-attacks on a smart grid that target timing information [7] [80]-[87] at the physical layer [8] and data link layer [8]. TSA can target phasor measurement units and wide area protection, monitoring, and control [57] [8]. The authors of [88] provide a detailed overview of TSA impacts on smart grids. In a smart grid, several applications use synchronous measurements, and the majority of the measurement devices are equipped with GPS for accurate timing information. These devices can also be subject to GPS spoofing attacks. Since the communication and control messages are time-sensitive, GPS spoofing and TSA can be both amongst cyber-attacks that can more likely be carried out in smart grids [7].

Brute-force attacks consist of hybrid brute-force (dictionary attacks), reverse brute-force, and credential stuffing attacks that target the presentation layer, session layer, and network layer [74]. These attacks can occur when malicious attackers crack passwords or passphrases to access the user's accounts or systems. The authors of [67] highlight the consequences of these attacks, including gaining unauthorized access to the system and user accounts and exploiting the security of the system by compromising the confidentiality and the integrity of the system. In smart grids, an attacker usually benefits from brute-force attacks by gaining access to the private information of consumers in the network [65].

Another cyber-attack against smart grid is the intrusion attack, in which an adversary exploits the vulnerabilities of the network to gain illegal access to the nodes. In other words, any unauthorized or even forcible action may subject to an intrusion attack [75]. It also aims at misusing the available resources in the network by disrupting the integrity, and the confidentiality of the network [5] in

both the application layer [83] and the network layer [82]. Due to the smart grid's vulnerable critical nature, the intrusion attack plays an essential role in security disruptions in the network. For example, modern SCADA systems in smart grids experience a lack of authentication and integrity, which causes them to be more exposed to cyber-attacks, such as intrusion attacks. Therefore, the detection and prevention of this attack can improve the network's general performance and avoid system disruptions.

Traffic analysis attack is applied when an adversary listens and analyzes the traffic. The goal of this attack is to control the hosts and devices that are connected to the smart grid network [88]. This attack can violate the confidentiality of the network and target the data link layer. In this attack, the intruder can sniff and analyze the messages, therefore getting information about the patterns of communication between nodes. Masquerading attack is also another known cyber-attack that targets the data link layer in the smart grid [89]. This attack mainly compromises the confidentiality, integrity, availability, and accountability of the network. In such attack, a malicious user may pretend to be an authorized user in order to gain access to the network or be able to conduct unauthorized actions. In the smart grid, the attacker mostly changes a Programmable Communicating Thermostat (PCT) in order to decrease electronic power at a residential location [2] [3].

In the smart grid, one of the most common attacks is the smart meter tampering attack. It can violate the integrity of the network while it targets the physical layer. In smart meter tampering attack, the intruder can modify the transmitted data for any customers. As a result, the user may need to pay higher or lower electricity bills. One cyber-attack that is more likely to happen in the smart grid is known as buffer overflow, in which the malicious attacker sends data to specific components or systems. It also targets the application and transport layers, while it compromises the availability requirement of the network. This attack may lead to system crash and exhausting the network resources [2].

Another known attack that targets the smart grid is the puppet attack, which violates the availability of the network and targets the network layer. This attack targets the AMI network in the smart grid, using a vulnerability in the Dynamic Source Routing (DSR) protocol. Then, it can exhaust the communication network bandwidth. One of the main impacts of this attack is the reduction of the packet delivery by 10% or 20% [3]. In addition, the smurf attack is one of the potential cyber-attacks in the smart grid that violates the availability of the network. This attack can not only target a specific unit of the smart grid, but also saturates and congests the traffic of an entire system. This attack consists of three factors, namely the source site, bounce site, and target site. In the source site, an adversary sends some spoofed packets to the broadcast address of the bounce site. As soon as the bounce site receives the forged packets, it can broadcast these packets to all hosts. This process may lead to saturate the target network. This attack type mostly targets the network layer [3].

Popping the HMI attack is one of the disruptive cyber-attacks targeting the smart grid. In this case, an adversary uses a common devices's attack (device's software or operating system vulnerabilities) and installs a remote shell, which permits the attacker to connect remotely to the server from the attacker's computer. The aim of this attack is to get unauthorized access and be able to control the compromised system. SCADA and substations of smart grid are considered good targets for this attack. Because the devices' documentaries are publicly available, this attack does not need any advanced networking skills. Therefore, launching such attack is easy and provides full control of the target system to the attacker. It violates the availability, integrity, confidentiality, and accountability and targets the application layer [3].

4.3. Detection Techniques of Cyber-Attacks on Smart Grid

Techniques to detect cyber-attacks that target smart grids can be mainly classified into six categories: localization-based techniques, AI-based techniques, prediction models, Channel characteristic-based techniques, filtering-based techniques, and intrusion detection systems, as shown in **Figure 6**.

4.3.1. Localization-Based Techniques

Several localizations or ranging techniques have been proposed in the literature and received considerable attention from researchers. In [90], the authors divide the localization techniques into Received Signal Strength (RSS-based), Received Signal Strength Indicator (RSSI-based), Time Difference of Arrival (TDoA-based), and Angle of Arrival-based localization (AoA-based).

RSS signals are widely used in communication technologies for various purposes. One information that can be derived from RSS is the transmitter's location, which has been the focus of numerous studies. For instance, the authors of [91] propose an RSS-based technique for detecting spoofing attacks based on a spatial correlation feature. In this study, the authors extracted RSS stream features in order to decrease the redundancy of data and applied two distinguishable features of RSS streams, including the Summation of Detailed Coefficient (SDCs) in Discrete Haar Wavelet Transform (DHWT) and the ration of out-of-bound frames [92]. Their proposed approach provides an effective, low-cost method for detecting spoofing attacks in a network. However, the authors of [92] highlight that the RSS-based technique suffers from poor localization accuracy, which is a critical disadvantage of this technique. It is one of the simplest localization techniques

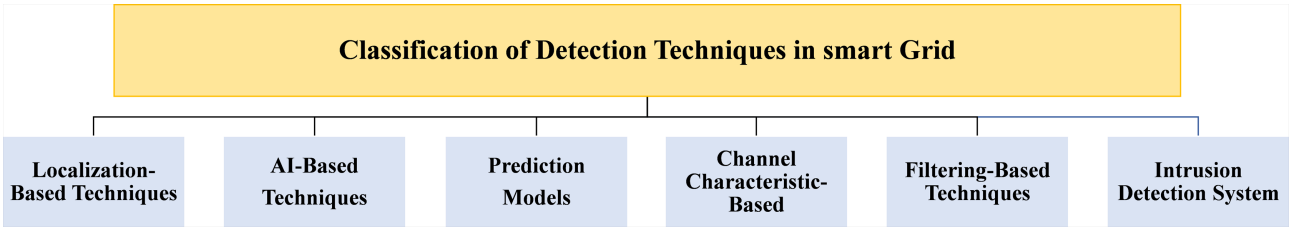

Figure 6. Classification of detection techniques in smart grids.

that consider a cost-effective method in networks.

In [93], the authors propose RSSI-based detection mechanism for MITM attacks. In this study, RSSI values are commonly arbitrary integers, which are received by antennas. These values can be evaluated using a sliding window, that leads to static information about signals' characteristics, including mean and standard deviation. Their proposed technique can detect MITM attacks by analyzing these profiles. In [94], the authors also take advantage of RSSI-based techniques for detecting spoofing attacks in smart grids. They developed a cosine-similarity method of RSSI in home area networks in a smart grid. Their proposed technique provides a higher detection rate compared to other related studies [95]-[101]. The authors of [102] combine RSS-based technique with the maximum likelihood estimation to handle uncertainty in measurements. According to their simulation results, this technique outperforms the existing RSS-based techniques in detecting attackers.

Localization-based techniques also consist of another common type, TDoA-based. Methods under this type are well-known techniques that measure the distance between nodes. For instance, the authors of [102] [103] introduce a lightweight TDoA-based technique between source and beacon nodes. The authors of [104] also propose a TDoA-based technique to detect time synchronization attacks in a network. In this work, the authors focus on using TDoA-based techniques on fixed sensors whose time reference could be maliciously affected. Their proposed solution mainly exploits the weighted least squares estimator with newly generated weights and the measurements of TDoA conducted from an unknown source. In [105], the authors describe a TDoA-based technique combined with the Maximum Likelihood Estimator (MLE), which provides superior performance compared to some other existing approaches.

In [106], the authors introduce a new localization technique, AoA-based technique. This technique mainly focuses on the angle of arrival signals to calculate transmitters' locations. In [107], the authors discuss this localization technique, which can achieve the angle of data by using radio array approaches. They highlight two ways to evaluate the angles of arrival, multiple and directional antennas. Multiple antennas work based on time analysis or even phase difference between the signals at various array elements in which the locations are known. While, directional antennas can compute the RSS ratio between several directional antennas in order to have an overlap between their major beams. In [108], the authors demonstrate that AoA-based localization techniques are not a good fit for cyber-attack detection of an indoor system in networks. In this study, the system's accuracy was reduced because of intensive multi-path components and Non-Line of Sight (NLOS) communications.

4.3.2. AI-Based Techniques

AI-based techniques category consists of various machine-learning and deep learning algorithms, data mining techniques, evolutionary algorithms, and fuzzy logic methods. For detecting cyber-attacks, machine learning category has re-

ceived more attention from researchers. For example, the authors of [55] use machine-learning to detect jamming attacks, namely random forest, support vector machine, and neural network. Their numerical results show that the proposed technique based on random forest achieves high accuracy. In [109], the authors also use machine learning algorithms to detect social engineering attacks. The technique performs based on unsupervised learning, which means that there is no previous knowledge about the observed cyber-attacks. They compare the performance of different machine learning algorithms (support vector machine, biased support vector machine, artificial neutral, scaled conjugate gradient, and self-organizing map) in terms of reliability, accuracy, and speed. Their simulations show instead of proved that support vector machine gives better results compared to other algorithms.

In [81], the authors use machine-learning techniques to detect brute force attacks on the Secure Shell protocol (SSH) at the network layer. The authors used different classifiers, including K-Nearest Neighbors (KNN), decision tree, and Naïve Bayes (N.B.), to develop scalable detection models that can provide good prediction results. Another study in the literature that exploits machine-learning is detailed in [110]. In this study, the authors highlight a concept from statics and economics, named "first difference", which led them to develop a classifier to detect time synchronization attacks in the network. Their results show that Artificial Neural Networks (ANN) are the best choice for detecting these attacks in the network. In [111], the authors use an ANN model to detect MITM attacks and their results did provide a good detection rate. In [112], the authors use machine learning techniques to detect and locate intruders in smart grids. The simulation results of this study showed that the proposed method could achieve a good detection rate. In [113], the authors propose ensemble techniques, namely bagging, boosting, and stacking to detect intrusions in smart grid. The results show that the stacking technique provides satisfactory results. In [114], the authors use boosting ensemble technique along with Tree-structured Parzen Estimator Optimization to detect and classify attacks on smart grid. The authors show that optimization techniques improve the detection performance of the mode. Overall, these proposed techniques provide good results.

Deep learning techniques have also been used to detect cyber-attacks targeting smart grid infrastructure. For instance, in [115], the authors propose ensemble deep learning techniques, using deep neural network (DNN) and decision tree. The proposed model is evaluated based on the 10-fold cross validation. The evaluation results show instead of showed that the proposed model outperforms other traditional techniques, including random forest, AdaBoost, and DNN. In [116], the authors apply a deep reinforcement learning based technique to identify the physical tripped line and the fake outrage line. Another study [117] also employ a deep learning technique, called encoders to reduce dimensions and feature extraction, followed by an advanced Generative Adversarial Network (GAN) to detect false data injection attacks. In addition, in [118], the authors propose a deep learning approach, namely residual neural network to detect attacks on smart

grid. The results show that the proposed approach outperforms other existing techniques. in literature.

Another type of AI-based category is data mining algorithms that can be useful for detecting cyber-attacks in the smart grid. In [16], the authors survey existing studies that used data mining techniques for detecting false data injection attacks (FDIA) in the smart grid. These techniques can determine patterns in huge datasets in order to analyze invisible patterns of data. Some studies use a data mining method, Common Path Mining (CPM), to detect FDIA in networks. They introduce a path as a sequence of samples in a temporal order. For any unique event, there is a path, which consists of various types of faults [119] [120] [121] [122]. Hence, when a sequence is compatible with the paths, it will be listed as an attack. In [112], the authors also introduce a Casual Event Graph (CEG) to detect FDIA in smart grids. The main objective of data mining techniques in this study is to train historical datasets. Although data-mining techniques provide some benefits, they may sometimes require low computational complexity (based on the data size) when a training process is over, which is considered a benefit in detecting FDIA in a smart grid.

Fuzzy logic-based methods have also been proposed to effectively detect various attacks in a network. For example, the authors of [116] propose artificial immune systems and fuzzy logic in order to detect flooding attacks in a network. In this study, the aim of using fuzzy logic is to reduce uncertainty whenever there is no clear line between malicious and legitimate traffic. Another study that applied fuzzy logic in cyber-attack detection is described in [117], in which the authors describe a detection technique based on fuzzy logic for jamming attacks. This technique uses the clear channel assessment, bad packet ratio, and received strength signal parameters to detect link loss due to jamming or other causes. The efficiency of their proposed techniques for constant and random jamming is high. Other authors [118] combine fuzzy logic with other approaches, such as genetic algorithms and Hidden Markov Model (HMM), to detect various cyber-attacks.

Another important type in AI-based techniques is that of evolutionary algorithms, which are widely used for global optimizations. One popular instance of evolutionary algorithms is genetic algorithms. These algorithms can mimic the evolution and natural selection process. In [119], the authors propose a technique based on a genetic algorithm that consists of two stages, training and detection. In their work, they applied a genetic algorithm for reducing the set of features in the detection stage. According to the authors' results, this technique provides a high level of accuracy for various cyber-attacks in networks. In [120], the authors also analyze the impact of genetic algorithms on various machine-learning techniques, such as SVM, KNN, and ANN. The simulation results show that genetic algorithms and these three machine learning techniques effectively detect FDIA in smart grids. However, KNN and SVM were found more efficient in detecting these attacks than some existing techniques.

In another work, the authors propose a hybrid technique based on Genetic

algorithms and fuzzy logic [121]. They developed a multi-objective genetic-fuzzy model for detecting anomalies in networks. The numerical results show that the proposed method is not suitable for detecting attacks in networks. In [122], the authors also analyze a hybrid framework for detecting different cyber-attacks that apply both genetic and fuzzy logic techniques. This method provides good accuracy and better results compared to some other existing techniques.

4.3.3. Prediction Models

With the increasing variety and number of cyber-attacks in smart grids, it has become challenging to detect cyber-attacks in any network. The process of detecting attacks usually occurs late for a victims' network. Therefore, detection and identification of attacks in an early stage are considered a challenge for modern systems. Prediction models are well-adapted methods to predict attacks at an early stage in the systems. They mainly apply statistics for the prediction of the results of any unknown events. Several studies focused on using prediction models for attack detections in smart grid infrastructures. For example, the authors of [123] proposed a detection method that uses cosine similarity and chi-square detector to identify FDIA in networks. They also employed Kalman filter to find expected measurements and calculate any deviation between actual measurements and estimated values. Their results show that both chi-square detector and cosine similarity machining are effective methods for the detection of random attacks. In addition, the authors concluded that chi-square detector cannot detect FDIA based on their methodology; however, using cosine similarity provided better results in detecting FDIA in networks.

In another study, Kalman filter is used to improve cyber-attack detection performance [124]. They modeled the smart grid network as a discrete linear dynamic system and exploited Kalman filter as the state estimation. Several studies also used Kalman filter as a technique to enhance cyber-attack detection in a smart grid, along with other techniques, such as the Euclidean detector [125] [126] [127], cosine similarity detector [126], and chi-square detector [120]. Auto Regressive Moving Average (ARMA) and Auto Regressive Integrated Moving Average (ARIMA) are other instances of prediction models that have been proposed for detecting cyber-attacks in networks. In fact, auto regression-based models can predict future trends from past behavior, while moving averages can predict long-term behaviors. ARIMA is also another statistical model that uses time-series data to forecast future behaviors.

In [128], the authors describe an early-stage method to detect SYN flooding attacks. In this method, the SYN traffic is predicted by using ARIMA model, and a cumulative sum algorithm is used to discover SYN flooding attacks. Other studies also used these time series models for detecting cyber-attacks smart grid networks [129]-[158].

4.3.4. Filtering-Based Techniques

Filtering-based techniques represent another common category for cyber-attack

detections in a smart grid. This survey will discuss two main techniques in this category, namely threshold-based and bloom filtering techniques. Several studies evaluated the efficiency of threshold-based techniques in detecting cyber-attacks in any system. For example, the authors of [103] used threshold-based techniques to detect social engineering attacks in networks. They are easy to develop but not efficient due to their values' limitations. On the other hand, the authors of [135] used bloom filters to detect flooding attacks against signaling protocols. They also introduced a metric called session distance to detect flooding attacks. In addition, they also used the bloom filters in the SCADA system. Because these filters need low memory and computing power, they can effectively help detect any existing anomalies in the SCADA system.

In [136], the authors describe a hybrid model for detecting intrusion attacks in SCADA systems. They proposed an approach using multi-level methods to detect anomalies using bloom filters in SCADA networks. They also suggested an algorithm for secure feature extraction and multi-level anomaly detection. Their experimental results show that the proposed approach can achieve an accuracy of 97%. In [81], the authors compare filtering techniques with some other detecting techniques to detect some social engineering attacks. In this work, the authors highlighted filtering techniques as easy techniques to use, but ineffective and costly. Despite their limitations, these techniques, particularly bloom filters, are known as space efficiency techniques, which are useful in specific scenarios in a smart grid.

4.3.5. Intrusion Detection System

Intrusion detection systems (IDS) are considered as one of the main techniques to detect cyber-attacks in smart grid infrastructure [12]. These systems can audit and analyze security information to detect any possible malicious vulnerabilities. One of the important benefits of these systems is to detect unknown or zero-day attacks effectively [137].

Several studies have been proposed to detect cyber-attacks using IDS. For example, the authors of [138] propose a hierarchical distributed IDS based on a distributed fog architecture. This system consists of three different layers of architecture, namely home area networks, residential area networks, and fog operation center networks. Their proposed system demonstrated good performance results over different conditions of the smart grid infrastructure.

In [137], the authors propose an IDS system to detect operational data. For this purpose, they used real power plant data and described a new architecture for the proposed system. Their simulation results proved that this system has some benefits compared to other existing systems. In [139], the authors propose a network-based IDS system based on a moving target defense technique in the smart grid. In this study, the authors mainly focused on IPV6 advanced metering infrastructure. The authors of [140] also developed an IDS system, called ARIES, which is able to detect any cyber-attacks, such as DoS, brute-force, port scanning, and bots attacks, against network flows, Modbus/Transmission Con-

trol Protocol (TCP), and operational data. They highlighted that the proposed system provides a high efficiency in detecting cyber-attacks. In addition, some works primarily attempted to improve signature-based IDS systems. In [141], the authors compare different types of IDS systems, including anomaly-based and signature-based. In particular, the authors focused on the improvement of signature-based IDS. To address this challenge, they employed Snort using a layered dataset.

In [142], the authors propose a signature-based IDS system that can detect DoS attacks in a network. For this purpose, they simulated different types of DoS attacks, such as Hello flooding attacks using Cooja simulator and IPV6 routing (RPL) protocol. Their proposed system provided effective results. In addition to these traditional methods, some studies used hybrid methods that combine IDS with other techniques. For instance, in [143], the authors apply a hybrid model to detect cyber-attacks. This model combines AI-based algorithms, including decision tree, K Nearest Neighbor (KNN), and Support Vector Machine (SVM), along with an IDS system to improve the performance of this system. Their results showed that their proposed system achieves high performance results. The authors of [144] propose an IDS system that is capable of detecting lethal. The proposed system uses the Cumulative Sum (CUSUM) algorithm with the characteristics of IDS systems. Their achieved detection rate is high, while the false positive rate is relatively low.

4.4. Countermeasures in Smart Grid

Several countermeasures have been proposed in the literature that can be used against various cyber-attacks introduced in the next section. For example, in [63], the authors survey several countermeasures, including frequency hopping spread spectrum for jamming attacks in wireless sensor networks (WSNs). In [145], the authors compare several encryption techniques and showed that one-time pad (OTP) is the only secure cryptosystem countermeasure solution for brute-force attacks. According to the shift-invariant feature of the transmission policy, the authors of [146] propose a countermeasure technique for time synchronization attacks. This technique can construct a shift-invariant transmission policies by characterizing the lower and upper bounds for the system estimation, while the attacker does not have any knowledge of the system.

Several studies provided countermeasure classifications. For instance, in [97], the authors propose a countermeasure classification comprised of four categories, cryptographic functions, personal identification, classification algorithms, and channel characteristics. In [55], the authors divide cyber-attack countermeasures into two categories, cryptographic and network countermeasures. In this section, as **Figure 7** illustrates, we classify countermeasure techniques in smart grid networks into two main categories, computer-based and non-computer-based. Computer-based countermeasures are classified into five types, namely secure protocols and standards, cryptographic functions, intrusion preventions, spread spectrum

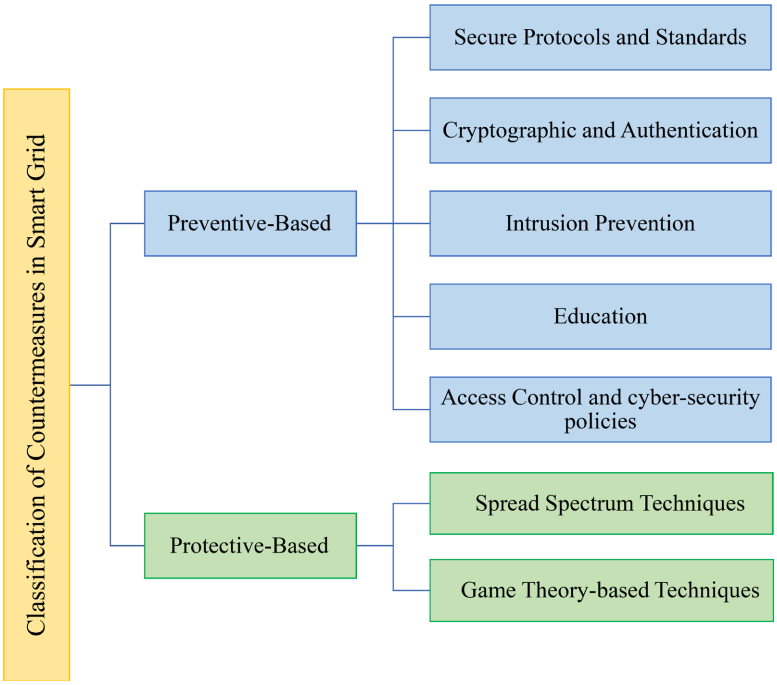

Figure 7. Classification of countermeasure techniques in smart grids.

techniques, and game theory-based techniques. Non-computer-based countermeasures include two types, education, and access control and cyber-security policies. Relevant countermeasures techniques and cyber-security strategies for each category are described below.

4.4.1. Preventive-Based Countermeasures

To be prepared for potential cyber-attacks in smart grid network, it is important to understand the different categories of countermeasures. This section only considers computer-based countermeasures that mainly focus on Information technology and software aspects of countermeasures. We will briefly discuss each of these categories with several suggested solutions for smart grid.

1) Secure protocols and Standards

Secure protocols, such as IPsec, transport layer security (TLS), secure sockets layer (SSL), and secure DNP3, play critical roles in data transmission's security and integrity in smart grid network. However, DNP3 and secure DNP3 are the most widely used protocols as industrial protocols without any other security mechanism [7]. The authors of [55] suggest these protocols for dealing with several attacks, such as man-in-the-middle, jamming, and eavesdropping attacks in networks.

In [148], the IEEE 802.1 1i protocol is proposed for more confidentiality, integrity, authentication, and availability in a smart grid network. This protocol was designed to replace the Wired Equivalent Privacy (WEP) in the original IEEE 802.11 with AES-CCM, which has multiple confidentiality and integrity issues [149]. However, even after all the enhancements, the IEEE 802.1 1i protocol remained vulnerable to different attacks. In [148], the authors propose a Smart

Grid Secure Protocol (SGSP) solution that creates a more secure node-server connection to achieve DoS resistance. In [150], the authors describe a new security protocol that adds authentication and preserves integrity and confidentiality. This protocol controls smart grid transmission lines in a sensor network, and it preserves the network connectivity during node failures.

In addition, the authors of [151] propose a protocol called scalable, secure transport protocol (SSTP) for smart grid data collection. They stated that integration of transmission control protocol (TCP) with transport layer security (TLS) protocol could provide some scalability issues. Their simulation results based on SSTP showed a high level of security and scalability for smart grid. They also showed that this protocol can reduce memory overhead exponentially. In [152], the authors propose a lightweight protocol for reliable communication in smart grid network. This protocol solved the security issues of some other protocols, such as IEC 62351 and IEC 61850. Their results show a reduction of the communication cost, solving overhead issues, and improving the privacy and security of data exchange.

In [153], the authors also discuss a countermeasure that uses IPSec and secure neighbor discovery (SEND) protocols. This study focused on using these protocols to prevent any vulnerabilities that may occur in communication with other protocols, such as IPV4 and IPV6. In [154], the authors describe compressed transport protocols, such as the datagram transport layer (DTL) in the network layer, which can be considered a good protection mechanism against cyber-attacks in networks. This protocol can mainly protect networks against cyber-attacks that influence data integrity and confidentiality.

Several other studies also introduced and discussed the standards in smart grid as efficient techniques to mitigate the detected cyber-attacks in a network. For example, the author of [155] highlight some standards, including The US Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 5.71 (NRC RG 5.71), IEEE Std 1686 - 2013 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities (IEEE 1686), Security Profile for Advanced Metering Infrastructure (security profile for AMI), and the ISO/IEC 27000 series (or ISO27k for short, such as ISO 27001, and ISO 27002) as critical countermeasures in smart grid infrastructure. In general, NRC RG 5.71 is mainly able to establish a comprehensive analysis for computer systems and smart grid networks, identifying the necessary digital assets, and deploying the required security controls. This security measure can mitigate the detected attacks in scope of nuclear infrastructure of smart grid networks.

Another important standard in smart grid is the IEEE 1686, which can provide a complete security control in a network. This standard can mitigate any detected vulnerability in the network. In addition, some other standards, like security profile for AMI, can provide baseline controls for AMI systems in smart grid infrastructures. Also, ISO27k series standards are critical security controls for managing information through conducting information security management

system (ISMS). These standards are capable of identifying the detected threats during the testing and assessment process in the network.

In addition [156], the authors of describe a few other standards, such as IEC 62443 -3-3 and IEEE C37.240. For instance, they discuss in-depth the importance of security controls, such as IEC 62443 -3-3 and IEEE C37.240, which can perform security controls and reliable countermeasures mostly through SCADA systems in the network. Other standards include NISTIR 7628, IEEE 1686, IEEEE C37.240, IEEE 1402, IEC 62056, and ISO/IEC 19790. An overview of essential standards as security controls are provided in **Table 4**.

2) Cryptographic and Authentication

As previously mentioned, one other basic type of countermeasure techniques in smart grid is cryptography and authentication. Most of these techniques aim to protect data integrity, privacy, and confidentiality. In this section, we discuss most common cryptographic functions and authentication methods.

In general, there are two types of cryptographic functions: symmetric and asymmetric functions. In symmetric functions, the encryption and decryption keys are the same or a transformation of one another. The well-known algorithms used as symmetric methods are advanced encryption standard (AES), one-time pad (OTP), and data encryption standard (DES). In asymmetric methods, different keys are used for encryption or decryption: a public key and a private key.

Table 4. List of important security controls in smart grid [155] [156] [157] [158].

Security Control	Scope
NRC RG 5.71	Security of Nuclear Infrastructure
ISO 27001, and ISO 27002	Security Information System Management
Security profile for AMI	Security of AMI
IEC 62443 -3-3	SCADA
IEEE C37.240.	Security of Communication Substations
NISTIR 7628	Security of all Components of Smart Grid Infrastructure
IEEE 1686	Security of Vehicular-based Communication Systems in Smart Grid
IEEE 1402	Security of Electric Power Substation in Smart Grid
IEC 62056	Security of meter data exchange in Smart Grid
ISO/IEC 19790	security characteristics of cryptographic modules
IEC 62351	Security of communication protocols
IEEE 2030	Smart Grid interoperability for all components
IEC 61400-25	Wind power plant component in smart grid
IEEE 1402	Security of physical and electrical substations
IEC 62056-5-3	Security of AMI component for data exchange
ISO/IEC 14543	Security of home electronic system component

The most known asymmetric algorithm is RSA (Rivest, Shamir, and Adleman) [121] [122]. In fact, these techniques' efficiency depends on various factors, such as computational resources, processing time, and time complexity. Another technique is elliptic curve cryptosystems. The authors of [92] introduce elliptic curve cryptosystems as a public-key cryptography with the same power as RSA, despite its key size smaller than RSA [123].

Key management techniques play an important role in encryption and authentication approaches. Public key infrastructure (PKI) is a type of key management that guarantees authentication through a network. In [125], the authors discuss some smart grid requirements regarding key management approaches, such as secure management, scalability, evaluability, and efficiency. These requirements must be followed in order to establish a secure key management scheme. Several examples of key management frameworks are provided in [7] as key establishment scheme for SCADA systems (SKE), key management architecture for SCADA systems (SKMA), advanced key management architecture for SCADA (ASKMA), advanced ASKM (ASKMA+), and scalable method of cryptographic key management (SMOCK).

Authentication methods are widely applied in smart grids as countermeasures. In [124], the authors introduce a privacy-preserving data aggregation scheme using authentication methods in the smart grid. Another countermeasure in smart grid is blockchain which is a new emerging technology [126] that can bring considerable advantages to the smart grid's cyber-security. In blockchain technology, distributed structures or ledgers can store digital data without any central authority in peer-to-peer networks. It provides potential solutions as a countermeasure approach, particularly for preventing or eliminating different cyber-attacks, such as man-in-the-middle attacks [127] [128] [129] [130] and eavesdropping attacks [128] [130].

3) Intrusion Prevention

Any malicious activity in the network, called intrusion, has to be prevented or eliminated to enhance smart grid performance. One of the traditional methods of preventing attacks on any system is to use firewalls and antivirus. The authors of [131] define firewalls as a software or hardware systems that can monitor network activities by using several protocols or policies; however, using firewalls and antivirus cannot effectively deal with unknown or sophisticated cyber-attacks. For this purpose, other security techniques, such as network data loss prevention (DLP), intrusion prevention systems (IPS), security information and event management systems (SIEM), File integrity monitoring (FIM), and automated security compliance have been proposed to diminish or prevent the impacts of cyber-attacks on the network [159].

In general, DLP is a system that can prevent the theft or loss of data through the network, while IPS is an intrusion system that can prevent the identified attacks in the network. IPS and DLP observe the network continuously, identifying malicious activities and abnormalities, and reporting them to the network

administrator to prevent them. In [160], the authors evaluate thirty-seven different IPS for smart grid in terms of their architecture, intrusion methodology, and programming characteristics. They also specified that none of these IPS has a self-healing mechanism that they can help during emergencies. In [161], the authors propose an IPS that mainly protects ZigBee-based home area networks in the smart grid against multiple attack types. Their simulation results demonstrate that this proposed system secures the network against multiple attacks, such as spoofing, eavesdropping, and DoS attacks.

In addition, a few studies used DLP systems as techniques to prevent cyber-attacks in the network. For example, the authors of [162] mention DLP as a monitoring system that can diminish the impact of any breach or vulnerabilities in the network; however, this technique usually cannot ensure security for heterogeneous networks such as a smart grid. To address this issue, several other security mechanisms, such as security information and event management systems (SIEM) and automated security compliance, have been proposed to prevent possible intrusions in a network and reduce the risk of cyber-attacks in smart grid [163]. For instance, SIEM can connect security information management (SIM) and security event management (SEM) system. This system constantly analyzes events and provides security alerts if anything unusual occurs [163]. In [164], the authors state that this system can be used as a good technology to prevent cyber-attacks.

Another practical solution to prevent intrusion in a network is file integrity monitoring (FIM) that prevents any changes in sensitive data and files and determines the possible breaches in the network. In [165], the authors apply the FIM system to protect the integrity of consumers' sensitive data and privacy in smart grid networks. In [166], the authors introduce another technique, called automated security compliance, which is considered an automated tool in the network. The proposed automated security compliance can check through smart grid components in order to guarantee the system configurations are updated. This tool can show a fault in any smart grid component, leading to a security breach in other components. Another practical solution to mitigate the detected intrusion in smart grid network is to sanitize the dataset. For instance, SQL injection attacks mainly happen when a malicious SQL statement is submitted to a web form. To prevent such attacks, sanitizing the dataset can be effective approach in the network [167].

Address space layout randomization (ASLR) is yet another countermeasure in smart grid networks. ALSR is defined as a memory-protection technique for any network against buffer-overflow attacks. These techniques can insert an address space target in any unpredictable locations of the network. Hence, ASLR can reduce or even prevent the risk of memory corruptions in smart grid network. Other simple mitigation techniques for detecting cyber-attacks are web browser extensions (for users), Spam Ware, and moving-target defense. Moving-target defense techniques (MTD) consist of several technologies which are required to in-

crease their security resilience through improving their software diversity. MTD techniques in smart grid are considered as crucial techniques to defer any blended cyber-attacks. For instance, the authors of [168] propose an MTD-based technique that is considered as a defense technique in order to mitigate detected false data injection attacks in the network. Their simulation results demonstrated that the proposed approach can reduce the attacker's ability to estimate the underlying space model, and that can prevent such cyber-attacks in network [168].

4) Education

In smart grid, utility services play a significant role in preventing cyber-attacks. For this purpose, the authors of [133] recommend that suitable security training and education for both employees and customers can efficiently prevent the impact of some attacks on networks. For example, tailgating attacks, a common type of social engineering attacks, can be prevented by training professionals. More precisely, employees are trained to never give access to any users who do not have badges [159]. Moreover, employees may be required to discard sensitive data and materials and important files to avoid such attacks.

Some companies implemented security defense frameworks to analyze and mitigate cyber-attacks in their networks. Using these frameworks, they can analyze consumers' profiles to show the existing threats and attacks in smart grid. However, this is not sufficient to minimize the impacts of cyber-attacks. They also need to increase the awareness of employees about cyber-attacks, such as social engineering, and how to prevent them. Another security education is to report security incidents to the IT support team. Reporting incident procedures may help the utility services identify possible vulnerabilities and malicious actions for further reference and avoid that they happen in the future. In addition to employee education, users are responsible for preventing cyber-attacks on smart grid networks. Users must avoid letting someone use their personal ID or password. They also need to be check if they are using legitimate websites before entering any personnel information. Another important venue for cyber-attacks are emails; users and employees have to verify that the email is coming from the utility company before clicking on any link embedded in the email [81].

5) Access Control and Cyber-Security Policies

There are a variety of strategies that are effective in managing smart grid networks and determining privileges' access to users and employees. These strategies mainly manage permissions along with providing assurance for an enterprise in a scalable solution. For example, policy-based access control techniques, also known as attribute-based access control, are practical solutions to tackle data security and management. In smart grid infrastructure, authorized employees are required to define some authorization policies in order to give permissions to other employees and users. These policies mostly show the regulations for individuals to provide protection against physical vulnerabilities or cyber-attacks.

Furthermore, integrity checking policy is another method to check if the data has been altered. Therefore, any changes to the network can be observed, and a

set of core controls can be applied. Integrity checking in smart grid networks can be performed as a security countermeasure and an indicator of malicious activity. Integrity checking methods can be monitored by authorized employees. Another countermeasure in this category is associated with physical protections. A physical protection is a set of hardware, software, data, and network that protect a network from external or internal vulnerabilities [169]-[181] and actions that may cause serious loss or damage to the infrastructure. In addition, a physical protection is an efficient approach in dealing with meter measurement modification attacks that can happen accidentally or intentionally when AMI reports incorrect measurements [167]-[173].

Security policies can also improve the security of a smart grid network and reduce the impact of cyber-attacks. These policies are primarily defined by authorized mangers or higher authorities, and they change over time. Such security policies include acceptable user policies, risk assessment standards, personnel security policies, end user key protection controls, and monitoring and logging policies. Although these policies usually focus on providing confidentiality and integrity, they cannot individually guarantee efficient protection in smart grid. Therefore, using several other security controls are considered as necessary steps to secure the network [173].

4.4.2. Protective-Based Countermeasures

In this section, we discuss two main categories of protective-based countermeasures, namely spread spectrum and game theory-based techniques.

1) Spread Spectrum Techniques

In smart grid, spread spectrum techniques are defined as a major approach in which a generated signal with specific bandwidth is deliberately spread in a frequency domain leading to a wider bandwidth. Spread spectrum techniques are known as effective techniques to prevent jamming attacks in networks. These techniques can be divided into frequency hopping (FHSS) and direct sequence (DSSS). In the following, we briefly describe these two types in the scope of smart grid infrastructure.

In FHSS techniques, signals are transmitted by changing a carrier frequency among several distinct occupied frequencies. In [174] [175], the authors introduce an FHSS technique to provide protection against jamming and collision attacks in the network. Their results showed that the total required bandwidth of this technique is wider than similar data with a single carrier frequency. In [60], the authors mention the advantages of FHSS techniques as countermeasures, including dealing effectively with the multipath effect.

DSSS techniques are used to decrease the overall signal interference. The direct sequence creates the transmitted signals much higher than the information signals. For example, in [176], the authors use a DHSS-based approach to mitigate the detected jamming attacks in the network. In this study, the authors conducted their approach according to the dynamic tree-based scheme; however, it generates a huge maintenance overhead. Although the proposed method

provided good protection against jamming attacks at the physical layer, this technique required very expensive computational resources. In [177], the authors also investigate the use of a DSSS technique by applying code division multiple access (CDMA) to prevent jamming attacks in the network. In [178], the authors recommend a hybrid approach that combines FHSS and DSSS to protect the network against jamming attacks. The authors compared their results with FHSS and DSSS, and concluded that a hybrid of FHSS/DSSS can provide a low probability of detection, low probability of interception, and improvement of the ability to deal with near far problems.

2) Game Theory-Based Techniques

Game theory-based techniques are considered as mathematical models that have strategic interactions among rational decision makers [179]. In [180], the authors propose a two-layer game theory prevention technique for false data injection attacks in smart grid. In this study, they used data from multiple sources in order to increase the prevention rates of attacks. So, they developed a zero-sum static game theory that optimizes the deployment of various defense resources. The authors of [181] also propose a game theory model based on the minimax regret method. This multi-level game theoretic framework provides a cost-effective and computationally efficient approach for large-scale power systems and smart grid infrastructure.

In [182], the authors introduce an approach based on game theory for defending against cyber-attacks in smart grid. In this work, they applied a game theory-based method which can identify cyber-attacks for smart energy scheduling of smart grid. The authors of [183] also designed a game theory approach to prevent against dynamic cyber-attacks in smart grid networks. Their model strategically identifies the chronological order of cyber-attacks that can occur, then protects the network against these attacks. Their simulation results proved that the proposed model is good and effective in detecting cyber-attacks.

The authors of [184] developed a game theory-based technique for smart grid, which according to their results, is 4.5 times faster than other existing studies. This technique also achieves a low communication and storage cost. In [185], the authors also propose a system, using dynamic game theory technique, as countermeasure that analyzes the attacks in cyber-physical system of the network. They mostly used a hybrid model that combines particle swarm optimization technique, game theory, and sequential quadratic programming technique to validate their model.

4.5. Comparison and Discussion

Each detection and countermeasure category has some advantages and disadvantages. In this section, we briefly describe these benefits and shortcomings of these techniques as shown in **Table 5** and **Table 6**. As we discussed earlier, our proposed classification has different categories, namely localization-based, AI-based, prediction models, and intrusion detection systems. A comprehensive

summary of advantages and disadvantages of these techniques are provided in Table 5. As shown in Table 5, localization-based techniques, the first category of the detection classification, have some limitations, such as high processing time and synchronization. In addition, these techniques present lower complexity, and having the locations of the malicious users is not always necessary for detecting attacks.

The second category, AI-based techniques, can provide a high level of detecting cyber-attacks in smart grid networks; however, these techniques, such as machine learning, deep learning, data mining, and fuzzy logic methods, have a very high implementation cost for smart grid networks. Nevertheless, their detection rates are high. Furthermore, these techniques mostly provide a low false alarm rate in risky situations and are also considered as the fastest techniques in detecting cyber-attacks. It is worth to mention that AI-based methods require a proper dataset to test and implement their algorithms; however, due to security reasons, working with real data may not be possible in smart grid networks.

The third category of our detection classification, prediction models, can generally provide a better knowledge about the trend of an attack occurrence, while these techniques have to be used along with proper and high-quality data. In fact, incorrect and low-quality data may lead to a poor performance of these models. In addition, using prediction models is one of the main keys of identifying future security risks and attack incidents. Therefore, they can be an effective model in detecting cyber-attacks in smart grids.

One of the most robust and flexible detection methods in smart grid is filtering-based techniques, which usually have high computational complexity. These techniques are also simple to develop and their detection rates are high. It is also worth to mention that these techniques are very cost effective. Despite all of their benefits, they require a fixed threshold, which can be challenging to select.

The last category of our detection classification presents intrusion detection

Table 5. Discussion of advantages and disadvantages of different detection techniques in smart grids.

Detection Technique	Advantage	Disadvantage
Localization-based	Less complexity. Always malicious users' location is not needed.	Needs synchronization. High processing time.
AI-based	Usually high detection rate and low false alarm.	For learning process, a proper dataset for training and testing is required.
Prediction models	Analysis of the current and historical data. Understanding a better trend. Identify potential future risks and opportunities.	Incomplete and poor data quality lead to inaccurate results.
Filtering-based	Easy implementation. Robust.	Usually fixed threshold. Usually high computational complexity.
Intrusion Detection System	No need to be centralized.	High false rate. High memory storage.

systems, which are widely used to detect multi-step cyber-attacks in the network. These systems are usually used along with other techniques, such as AI-based methods. In general, in smart grid networks, there is no need for an authorized user to control the intrusion detection systems, and they mostly perform without any centralized authorizations. Also, these techniques have high rates of false alarm and require high memory storage. Therefore, these systems still need more development and improvement to detect complicated attacks in the smart grid.

As presented in Table 6, we compare the proposed countermeasure categories to discuss their advantages and disadvantages. According to this table, secure protocols and standards provide flexible solutions to prevent cyber-attacks in the smart grid. In addition, these methods are simple to manage and maintain; however, there are still no protocols in the smart grid infrastructure that guarantee a high level of security. Moreover, secure protocols and standards deal with a limited frequency of communication, which may lead to the lack of performance in the network.

Cryptographic and authentication techniques are also used in confidential scenarios, although their implementation complexity is high and they are an inefficient solution. Another preventive countermeasure, as shown in Table 6., is intrusion prevention, which can protect the privacy of the network and users while preventing abnormal activities. Furthermore, to provide a higher security and to mitigate the detected attacks, intrusion prevention methods are not highly recommended to be used without any other techniques. Education techniques are also another category in our countermeasure classification, which is considered as a simple and easy to understand method for users. Only educating

Table 6. Summary of advantages and disadvantages of countermeasure techniques in smart grids.

Countermeasure methods	Advantages	Disadvantages
Secure protocols and standards	Flexibility. Simple to manage and maintenance.	No high secure protocols in smart grid. Limited frequency of communication.
Cryptographic and authentication	Cryptographic algorithms benefits. Confidentiality is recommended.	Implementation complexity. Not always efficient.
Intrusion prevention	Privacy protection. Prevent abnormal network activities.	Needs to implement with other countermeasure techniques to be able to prevent attacks.
Spread spectrum techniques	High level of protection.	Complicated implementations. Inefficient bandwidth.
Game theory-based	Optimal solution. High rates of data.	Mobile users are necessary.
Education	Simple. Provide enough knowledge to users and employees.	Not enough to protect and prevent the network against attacks.
Access control and cyber-security policies	High scalability. Simple to understand.	Not ensure protection against attacks. Suitable for small-scale networks.

users, however, is not enough to guarantee any attack prevention. Access control and cyber-security policies also are considered as another prevention approach that have a high scalability, which is easy to understand. Furthermore, this approach cannot guarantee the protection against cyber-attacks and is only compatible with small-scale networks.

Game theory-based techniques also protect the smart grid against multiple cyber-attacks with optimal solutions and high data rates; however, in these methods, it is necessary to have mobile users to develop such techniques. It is clear that, in some scenarios, it is impossible to have mobile users. Therefore, game-based countermeasures cannot be used in all conditions. Another protective countermeasure is spread spectrum techniques, which provide high levels of protection. However, they may have some limitations, such as a complicated implementation for smart grids and an inefficient bandwidth. Despite these challenges, spread spectrum techniques can be a good solution to mitigate the detected cyber-attacks in smart grids.

5. Challenges and Future Directions

With smart grid deployment, this technology is exposed to several cyber-attacks like any other heterogeneous system. It is found that there is a plethora of challenges in the security of the smart grid in order to provide a reliable, secure, and protective framework. Moreover, there are still several challenges and open questions about the security of the smart grid that need to be addressed and answered. Also, most smart grid advancements are in the early stage and they are considered more conceptual rather than practical. Therefore, studying challenges and future directions play an important role in the advancement of the smart grid.

For example, the increased number of connected devices with unsecure protocols makes smart grid networks vulnerable to new attacks. Each device connected to the network can be considered as a possible point of entry. There are numerous studies that aimed to enhance the security of the smart grid; however, some of the existing techniques have fundamental limitations, and there are still a number of challenges to address. For instance, existing IDSs still deal with some limitations, such as a low detection accuracy and a high false positive rate. Several studies used machine-learning techniques with these systems to improve their performance. However, machine learning models require large datasets which are not widely shared by researchers. A few groups share their datasets, and these datasets do not include data gathered from real attacks. Therefore, there is a need for developing and sharing datasets for machine learning training and validation.

Cryptographic and authentication techniques barely support AMI and WAN entities. Several techniques have been proposed on this topic; however, these techniques are only compatible with SCADA systems. Thus, one research direction is to develop key management techniques specific to AMI and WAN com-

ponents. For detection techniques that use artificial intelligence, the models have to be extensively trained before any cyber-attack happens. Therefore, there is a need for techniques that classify not only incoming signals, but also prevent new attacks and help the system recover from them. Another issue is the fact that existing techniques deal only with one attack. These techniques are inefficient in detecting complex and distributed attacks. Thus, there is a need for layered frameworks that can prevent, detect, and mitigate cyber-attacks in smart grid infrastructure. Regarding current protocols for smart grids, their main purpose is connectivity, not security. None of these protocols provide a high level of security. The confidentiality, privacy, integrity, and accountability can easily be violated with such existing protocols. Therefore, there is a need for new secure protocols for smart grid networks.

6. Conclusion

The security of smart grid networks is of paramount importance and plays a pivotal role in the implementation of smart grid systems. However, prior studies have shown a constrained role in evaluating cyber-security solutions for smart grid networks. Therefore, this paper considers the shortcomings of the existing surveys and provides an in-depth description of potential attacks that target smart grids and an evaluation of different security solutions. In this paper, we propose a benchmarking of cyber-attacks in terms of the integrity, availability, confidentiality, and accountability and a classification based on OSI communication layers. Moreover, we present a new classification for the existing detection techniques, which is mainly divided into localization-based, AI-based, prediction models, filtering techniques, and intrusion detection systems. We also classify the countermeasure techniques into preventive and protective techniques. In the preventive countermeasures, we describe secure protocols and standards, cryptographic and authentication, intrusion prevention, education, access control, and required cyber-security policies approaches. For the protective countermeasure category, we discuss spread spectrum techniques and game theory in the smart grid. Finally, we describe the existing challenges that can guide future research directions. This survey has highlighted the requirements of new solutions, which can collectively resolve the problems related to security challenges in the smart grid infrastructures without compromising the performance and functionalities of this type of network.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zhang, Z., Gong, S., Dimitrovski, A.D. and Li, H. (2013) Time Synchronization Attack in Smart Grid: Impact and Analysis. *Transactions on Smart Grid*, **4**, 87-98.

https://doi.org/10.1109/TSG.2012.2227342

[2] Al-kahtani, M.S. and Karim, L. (2019) A Survey on Attacks and Defense Mechanisms in Smart Grids. *International Journal of Computer Engineering and Information Technology*, **11**, 94-100.

[3] Yoldaş, Y., Önen, A., Muyeen, S.M., Vasilakos, A.V. and Alan, İ. (2017) Enhancing Smart Grid with Microgrids: Challenges and Opportunities. *Renewable and Sustainable Energy Reviews*, **72**, 205-214. https://doi.org/10.1016/j.rser.2017.01.064

[4] Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N. and Wollman, D. (2021) NIST Framework and Roadmap for Smart Grid Interoperability Standards. National Institute of Standards and Technology Special Publication (NIST SP), release 4.0. https://doi.org/10.6028/NIST.SP.1108r4

[5] Liu, J., Xiao, Y. and Gao, J. (2014) Achieving Accountability in Smart Grid. *Systems Journal*, **8**, 493-508. https://doi.org/10.1109/JSYST.2013.2260697

[6] Bedi, G., Venayagamoorthy, G.K., Singh, R., Brooks, R.R. and Wang, K.C. (2018) Review of Internet of Things (IoT) in Electric Power and Energy Systems. *Internet of Things Journal*, **5**, 847-870. https://doi.org/10.1109/JIOT.2018.2802704

[7] El Mrabet, Z., Kaabouch, N., El Ghazi, H. and El Ghazi, H. (2018) Cyber-Security in Smart Grid: Survey and Challenges. *Computers and Electrical Engineering*, **67**, 469-482. https://doi.org/10.1016/j.compeleceng.2018.01.015

[8] Gunduz, M.Z. and Das, R. (2020) Cyber-Security on Smart Grid: Threats and Potential Solutions. *Computer Networks*, **169**, Article ID: 107094. https://doi.org/10.1016/j.comnet.2019.107094

[9] Peng, C., Sun, H., Yang, M. and Wang, Y. (2019) A Survey on Security Communication and Control for Smart Grids under Malicious Cyber Attacks. *Transactions on Systems, Man, and Cybernetics: Systems*, **49**, 1554-1569. https://doi.org/10.1109/TSMC.2018.2884952

[10] He, H. and Yan, J. (2016) Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey. *IET Cyber-Physical Systems: Theory & Applications*, **1**, 13-27. https://doi.org/10.1049/iet-cps.2016.0019

[11] Gupta, B.B. and Akhtar, T. (2017) A Survey on Smart Power Grid: Frameworks, Tools, Security Issues, and Solutions. *Annals of Telecommunications*, **72**, 517-549. https://doi.org/10.1007/s12243-017-0605-4

[12] Komninos, N., Philippou, E. and Pitsillides, A. (2014) Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *Communications Surveys and Tutorials*, **16**, 1933-1954. https://doi.org/10.1109/COMST.2014.2320093

[13] Li, X., Liang, X., Lu, R., Shen, X., Lin, X. and Zhu, H. (2012) Securing Smart Grid: Cyber-Attacks, Countermeasures, and Challenges. *Communications Magazine*, **50**, 38-45. https://doi.org/10.1109/MCOM.2012.6257525

[14] Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R.M. and Srivastava, G. (2019) Security Aspects of Internet of Things Aided Smart Grids: A Bibliometric Survey. *Internet of Things*, **14**, Article ID: 100111. https://doi.org/10.1016/j.iot.2019.100111

[15] Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J.S. and Martin, A. (2019) Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. *Communications Surveys and Tutorials*, **21**, 2886-2927. https://doi.org/10.1109/COMST.2019.2899354

[16] Musleh, A.S., Chen, G. and Dong, Z.Y. (2020) A Survey on the Detection Algo-

rithms for False Data Injection Attacks in Smart Grids. *IEEE Transactions on Smart Grid*, **11**, 2218-2234. https://doi.org/10.1109/TSG.2019.2949998

[17] Brown, R.E. (2008) Impact of Smart Grid on Distribution System Design. *Proceedings of the Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the* 21*st Century*, Pittsburg, 20-24 July 2008, 1-4. https://doi.org/10.1109/PES.2008.4596843

[18] Knapp, E.D. and Samani, R. (2013) Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure. Elsevier, Amsterdam.

[19] Panel, S.G.I. (2010) Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, and Vol. 2, Privacy and the Smart Grid. Vol. 7628, National Institute of Standards and Technology (NIST), Gaithersburg.

[20] Elgenedy, M.A., Massoud, A.M. and Ahmed, S. (2015) Smart Grid Self-Healing: Functions, Applications, and Developments. *Proceedings of the First Workshop on Smart Grid and Renewable Energy* (*SGRE*), Doha, 22-23 March 2015, 1-6. https://doi.org/10.1109/SGRE.2015.7208737

[21] Usman, A. and Shami, S.H. (2013) Evolution of Communication Technologies for Smart Grid Applications. *Renewable and Sustainable Energy Reviews*, **19**, 191-199. https://doi.org/10.1016/j.rser.2012.11.002

[22] Gungor, V.C., *et al.* (2013) A Survey on Smart Grid Potential Applications and Communication Requirements. *Transactions on Industrial Informatics*, **9**, 28-42. https://doi.org/10.1109/TII.2012.2218253

[23] Mahmood, A., Javaid, N. and Razzaq, S. (2015) A Review of Wireless Communications for Smart Grid. *Renewable and Sustainable Energy Reviews*, **41**, 248-260. https://doi.org/10.1016/j.rser.2014.08.036

[24] Yi, P., Zhu, T., Zhang, Q., Wu, Y. and Li, J. (2014) A Denial of Service Attack in Advanced Metering Infrastructure Network. *Proceedings of the International Conference on Communications (ICC)*, Sydney, 10-14 June 2014, 1029-1034. https://doi.org/10.1109/ICC.2014.6883456

[25] Gai, K., Qiu, M., Ming, Z., Zhao, H. and Qiu, L. (2017) Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks. *Transactions on Smart Grid*, **8**, 2431-2439. https://doi.org/10.1109/TSG.2017.2664043

[26] Maynard, P., McLaughlin, K. and Haberler, B. (2014) Towards Understanding Man-in-the-Middle Attacks on IEC 60870-5-104 SCADA Networks. *Proceedings of the* 2*nd International Symposium on ICS & SCADA Cyber Security Research*, St. Pölten, 11-12 September 2014, 30-42.

[27] Faisal, M.A., Aung, Z., Williams, J.R. and Sanchez, A. (2015) Data-Streambased Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study. *Systems Journal*, **9**, 31-44. https://doi.org/10.1109/JSYST.2013.2294120

[28] Choi, D., Lee, S., Won, D. and Kim, S. (2010) Efficient Secure Group Communications for SCADA. *Transactions on Power Delivery*, **25**, 714-722. https://doi.org/10.1109/TPWRD.2009.2036181

[29] Bennett, C. and Highfill, D. (2008) Networking AMI Smart Meters. *Proceedings of the Energy* 2030 *Conference*, Atlanta, 17-18 November 2008, 1-8. https://doi.org/10.1109/ENERGY.2008.4781067

[30] Zhou, S. (2021) The Effect of Smart Meter Penetration on Dynamic Electricity Pricing: Evidence from the United States. *The Electricity Journal*, **34**, Article ID: 106919.

https://doi.org/10.1016/j.tej.2021.106919

[31] Pliatsios, D., Sarigiannidis, P., Lagkas, T. and Sarigiannidis, A.G. (2020) A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *Communications Surveys and Tutorials*, **22**, 1942-1976. https://doi.org/10.1109/COMST.2020.2987688

[32] Igure, V.M., Laughter, S.A. and Williams, R.D. (2006) Security Issues in SCADA Networks. *Computers & Security*, **25**, 498-506. https://doi.org/10.1016/j.cose.2006.03.001

[33] Chai, B., Chen, J., Yang, Z. and Zhang, Y. (2014) Demand Response Management with Multiple Utility Companies: A Two-Level Game Approach. *Transactions on Smart Grid*, **5**, 722-731. https://doi.org/10.1109/TSG.2013.2295024

[34] Gomez, C. and Paradells, J. (2010) Wireless Home Automation Networks: A Survey of Architectures and Technologies. *Communications Magazine*, **48**, 92-101. https://doi.org/10.1109/MCOM.2010.5473869

[35] Ahmed, S., Gondal, T.M., Adil, M., Malik, S.A. and Qureshi, R. (2019) A Survey on Communication Technologies in Smart Grid. *Proceedings of the PES GTD Grand International Conference and Exposition Asia* (*GTD Asia*), Bangkok, 20-23 March 2019, 7-12. https://doi.org/10.1109/GTDAsia.2019.8715993

[36] Terzija, V., Valverde, G., Cai, D., Regulski, P., Madani, V., Fitch, J., Skok, S., Begovic, M.M. and Phadke, A. (2011) Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks. *Proceedings of the IEEE*, **99**, 80-93. https://doi.org/10.1109/JPROC.2010.2060450

[37] Lo, C.-H. and Ansari, N. (2012) The Progressive Smart Grid System from Both Power and Communications Aspects. *Communications Surveys and Tutorials*, **14**, 799-821. https://doi.org/10.1109/SURV.2011.072811.00089

[38] Elyengui, S., Bouhouchi, R. and Ezzedine, T. (2014) The Enhancement of Communication Technologies and Networks for Smart Grid Applications. arXiv preprint, arXiv:1403.0530.

[39] Kabalci, Y. (2011) A Survey on Smart Metering and Smart Grid Communication. *Renewable and Sustainable Energy Reviews*, **57**, 302-318. https://doi.org/10.1016/j.rser.2015.12.114

[40] Gungor, V.C., *et al.* (2011) Smart Grid Technologies: Communication Technologies and Standards. *Transactions on Industrial Informatics*, **7**, 529-539. https://doi.org/10.1109/TII.2011.2166794

[41] Peizhong, Y., Iwayemi, A. and Zhou, C. (2011) Developing ZigBee Deployment Guideline under WIFI Interference for Smart Grid Applications. *Transactions on Smart Grid*, **2**, 110-120. https://doi.org/10.1109/TSG.2010.2091655

[42] Gezer, C. and Buratti, C. (2011) A ZigBee Smart Energy Implementation for Energy Efficient Buildings. *Proceedings of the Vehicular Technology Conference* (*VTC Spring*), Budapest, 15-18 May 2011, 1-5. https://doi.org/10.1109/VETECS.2011.5956726

[43] Lewis, R.P., Igic, P. and Zhou, Z. (2009) Assessment of Communication Methods for Smart Electricity Metering in the UK. *Proceedings of the PES/IAS Conference Sustainable Alternative Energy* (*SAE*), Valencia, 28-30 September 2009, 1-4. https://doi.org/10.1109/SAE.2009.5534884

[44] Bressan, N., Bazzaco, L., Bui, N., Casari, P., Vangelista, L. and Zorzi, M. (2010) The Deployment of a Smart Monitoring System Using Wireless Sensor and Actuator Networks. *Proceedings of the International Conference on Smart Grid Communications*, Gaithersburg, 4-6 October 2010, 49-54.

https://doi.org/10.1109/SMARTGRID.2010.5622015

[45] Khan, A.A., Rehmani, M.H. and Reisslein, M. (2016) Cognitive Radio for Smart Grids: Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols. *Communications Surveys & Tutorials*, **18**, 860-898. https://doi.org/10.1109/COMST.2015.2481722

[46] Zhai, M. (2011) Transmission Characteristics of Low-Voltage Distribution Networks in China under the Smart Grids Environment. *Transactions on Power Delivery*, **26**, 173-180. https://doi.org/10.1109/TPWRD.2010.2067228

[47] Paruchuri, V., Durresi, A. and Ramesh, M. (2008) Securing Powerline Communications. *Proceedings of the International Symposium on Power Line Communications and Its Applications*, Jeju City, 2-4 April 2008, 64-69. https://doi.org/10.1109/ISPLC.2008.4510400

[48] Laverty, D.M., Morrow, D.J., Best, R. and Crossley, P.A. (2010) Telecommunications for Smart Grid: Backhaul Solutions for the Distribution Network. *Proceedings of the PES General Meeting*, Minneapolis, 25-29 July 2010, 1-6. https://doi.org/10.1109/PES.2010.5589563

[49] Bellovin, S.M. (1989) Security Problems in the TCP/IP Protocol Suite. *ACM SIGCOMM Computer Communication Review*, **19**, 32-48. https://doi.org/10.1145/378444.378449

[50] Talaat, M., Alsayyari, A.S., Alblawi, A. and Hatata, A.Y. (2020) Hybrid-Cloud-Based Data Processing for Power System Monitoring in Smart Grids. *Sustainable Cities and Society*, **55**, Article ID: 102049. https://doi.org/10.1016/j.scs.2020.102049

[51] Ortega, A., Shinoda, A.A., Schweitzer, C.M., Granelli, F., Ortega, A.V. and Bonvecchio, F. (2014) Performance Evaluation of the DNP3 Protocol for Smart Grid Applications over IEEE 802.3/802.11 Networks and Heterogeneous Traffic. In: *Recent Advances in Communications*, 232-237.

[52] Huitsing, P., Chandia, R., Papa, M. and Shenoi, S. (2008) Attack Taxonomies for the Modbus Protocols. *International Journal of Critical Infrastructure Protection*, **1**, 37-44. https://doi.org/10.1016/j.ijcip.2008.08.003

[53] Kuzlu, M., Pipattanasompom, M. and Rahman, S. (2017) A Comprehensive Review of Smart Grid Related Standards and Protocols. *Proceedings of the International Istanbul Smart Grid and Cities Congress and Fair* (*ICSG*), Istanbul, 19-21 April 2017, 12-16. https://doi.org/10.1109/SGCF.2017.7947600

[54] Mackiewicz, R.E. (2006) Overview of IEC 61850 and Benefits. *Proceedings of the Power Engineering Society General Meeting*, Montreal, 18-22 June 2006, 8. https://doi.org/10.1109/PES.2006.1709546

[55] Wang, W. and Lu, Z. (2013) Cyber Security in the Smart Grid: Survey and Challenges. *Computer Networks*, **57**, 1344-1371. https://doi.org/10.1016/j.comnet.2012.12.017

[56] Rawat, D.B. and Bajracharya, C. (2015) Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives. *Proceedings of the Southeast Conference*, Gainesville, 27-29 September 2015, 1-6. https://doi.org/10.1109/SECON.2015.7132891

[57] Baig, Z.A. and Amoudi, A. (2013) An Analysis of Smart Grid Attacks and Countermeasures. *Journal of Communications*, **8**, 473-479.

[58] Aloul, F., Al-Ali, A.R., Al-Dalky, R., Al-Mardini, M. and El-Hajj, W. (2012) Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*, **1**, 1-6.

[59] Gupta, B.B. and Dahiya, A. (2020) Distributed Denial of Service (DDoS) Attacks:

Classification, Attacks, Challenges and Countermeasures. CRC Press, Boca Raton.

[60] Pillitteri, V.Y. and Brewer, T.L. (2014) The Smart Grid Interoperability Panel—Cyber Security Working Group, Smart Grid Cyber Security Guidelines, 1-597.

[61] Islam, S.N., Baig, Z. and Zeadally, S. (2019) Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures. *Transactions on Industrial Informatics*, **15**, 6522-6530. https://doi.org/10.1109/TII.2019.2931436

[62] Sinha, A., Vyas, R., Subramanian, V. and Vyas, O.P. (2020) Critical Infrastructure Security: Cyber-Physical Attack Prevention, Detection, and Countermeasures. Quantum Cryptography and the Future of Cyber Security, 134-162. https://doi.org/10.4018/978-1-7998-2253-0.ch007

[63] Kemi, D., Ren, X., Quevedo, D.E., Dey, S. and Shi, L. (2020) Defensive Deception against Reactive Jamming Attacks in Remote State Estimation. *Automatica*, **113**, Article ID: 108680. https://doi.org/10.1016/j.automatica.2019.108680.

[64] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C. and Pantziou, G. (2009) A Survey on Jamming Attacks and Countermeasures in WSNs. *Communications Surveys and Tutorials*, **11**, 42-56. https://doi.org/10.1109/SURV.2009.090404

[65] Arjoune, Y., Salahdine, F., Islam, M.S., Ghribi, E. and Kaabouch, N. (2020) A Novel Jamming Attacks Detection Zubair Approach Based on Machine Learning for Wireless Communication. *Proceedings of the International Conference on Information Networking* (*ICOIN*), Barcelona, 7-10 January 2020, 459-464. https://doi.org/10.1109/ICOIN48656.2020.9016462

[66] Gunduz, M.Z. and Das, R. (2018) Analysis of Cyber-Attacks on Smart Grid Applications. *Proceedings of the International Conference on Artificial Intelligence and Data Processing* (*IDAP*), Malatya, 28-30 September 2018, 1-5. https://doi.org/10.1109/IDAP.2018.8620728

[67] Karagiannis, D. and Argyriou, A. (2018) Jamming Attack Detection in a Pair of RF Communicating Vehicles Using Unsupervised Machine Learning. *Vehicular Communications*, **13**, 56-63. https://doi.org/10.1016/j.vehcom.2018.05.001

[68] Manesh, M.R., Kenney, J., Hu, W.C., Devabhaktuni, V.K. and Kaabouch, N. (2019) Detection of GPS Spoofing Attacks on Unmanned Aerial Systems. *Proceedings of the Consumer Communications and Networking Conference* (*CCNC*), Las Vegas, 11-14 January 2019, 1-6. https://doi.org/10.1109/CCNC.2019.8651804

[69] Sengupta, J., Ruj, S. and Bit, S.D. (2020) A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications*, **149**, Article ID: 102481. https://doi.org/10.1016/j.jnca.2019.102481.

[70] Delgado-Gomes, V., Martins, J.F., Lima, C. and Borza, P.N. (2015) Smart Grid Security Issues. *Proceedings of the International Conference on Compatibility and Power Electronics* (*CPE*), Lisbon, 24-26 June 2015, 534-538. https://doi.org/10.1109/CPE.2015.7231132

[71] Talaei Khoei, T., Ismail, S. and Kaabouch, N. (2022) Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs. *Sensors*, **22**, 662. https://doi.org/10.3390/s22020662

[72] Xiao, L., Li, Y., Han, G., Liu, G. and Zhuang, W. (2016) PHY-Layer Spoofing Detection With Reinforcement Learning in Wireless Networks. *Transactions on Vehicular Technology*, **65**, 10037-10047. https://doi.org/10.1109/TVT.2016.2524258

[73] Mavani, M. and Asawa, K. (2017) Modeling and Analyses of IP Spoofing Attack in 6LoWPAN Network. *Computers and Security*, **70**, 95-110.

https://doi.org/10.1016/j.cose.2017.05.004

[74] Yin, W., Hu, P., Wen, J. and Zhou, H. (2020) Ack Spoofing on Mac-layer Rate Control: Attacks and Defenses. *Computer Networks*, **171**, Article ID: 107133. https://doi.org/10.1016/j.comnet.2020.107133

[75] Wang, Y., Gamage, T.T. and Hauser, C.H. (2016) Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication. *Transactions on Smart Grid*, **7**, 807-816.

[76] Lieskovan, T., Hajny, J. and Cika, P. (2019) Smart Grid Security: Survey and Challenges. *Proceedings of the International Congress on UltraModern Telecommunications and Control Systems and Workshops* (*ICUMT*), Dublin, 28-30 October 2019, 1-5. https://doi.org/10.1109/ICUMT48472.2019.8970738

[77] Dileep, G. (2020) A Survey on Smart Grid Technologies and Applications. *Renewable Energy*, **146**, 2589-2625. https://doi.org/10.1016/j.renene.2019.08.092

[78] Tazi, K., Abdi, F. and Abbou, M.F. (2015) Review on Cyber-physical Security of the Smart Grid: Attacks and Defense Mechanisms. *Proceedings of the International Renewable and Sustainable Energy Conference* (*IRSEC*), Marrakech, 10-13 December 2015, 1-6. https://doi.org/10.1109/IRSEC.2015.7455127

[79] Kim, J. and Tong, L. (2013) On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures. *Journal on Selected Areas in Communications*, **31**, 1294-1305. https://doi.org/10.1109/JSAC.2013.130712

[80] Oppliger, R., Hauser, R. and Basin, D. (2006) SSL/TLS Session-Aware User Authentication—Or How to Effectively Thwart the Man-in-the-Middle. *Computer Communications*, **29**, 2238-2246. https://doi.org/10.1016/j.comcom.2006.03.004

[81] Fatima, S. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey. *Future Internet*, **11**, 89. https://doi.org/10.3390/fi11040089

[82] Ambili, K.N. and Jose, J. (2020) Trust Based Intrusion Detection System to Detect Insider Attacks in IoT Systems. In: Kim, K. and Kim, H.Y., Eds., *Information Science and Applications*, Springer, Singapore, 631-638. https://doi.org/10.1007/978-981-15-1465-4_62

[83] Wang, S., Zhu, S. and Zhang, Y. (2018) Blockchain-Based Mutual Authentication Security Protocol for Distributed Radio Frequency Identification (RFID) Systems. *Proceedings of the Symposium on Computers and Communications* (*ISCC*), Natal, 25-28 June 2018, 74-77. https://doi.org/10.1109/ISCC.2018.8538567

[84] Patil, H.K., Wing, D. and Chen, T.M. (2013) VoIP Security. In: Vacca, J.R., Ed., *Computer and Information Security Handbook*, Morgan Kaufmann, Burlington, 871-886. https://doi.org/10.1016/B978-0-12-394397-2.00050-7

[85] Han, W. and Xiao, Y. (2016) Privacy Preservation for V2G Networks in Smart Grid: A Survey. *Computer Communications*, **91**, 17-28. https://doi.org/10.1016/j.comcom.2016.06.006

[86] Najafabadi, M.M., Khoshgoftaar, T.M., Kemp, C., Seliya, N. and Zuech, R. (2014) Machine Learning for Detecting Brute Force Attacks at the Network Level. *Proceedings of the International Conference on Bioinformatics and Bioengineering*, Boca Raton, 10-12 November 2014, 379-385. https://doi.org/10.1109/BIBE.2014.73

[87] Gautam, T. and Jain, A. (2015) Analysis of Brute Force Attack Using TG—Dataset. *Proceedings of the SAI Intelligent Systems Conference* (*IntelliSys*), London, 10-11 November 2015, 984-988. https://doi.org/10.1109/IntelliSys.2015.7361263

[88] van Oorschot, P.C. (2020) Intrusion Detection and Network-Based Attacks. In:

Computer Security and the Internet, Springer, Cham, 309-338. https://doi.org/10.1007/978-3-030-83411-1_11

[89] Rietta, F.S. (2006) Application Layer Intrusion Detection for SQL Injection. *Proceedings of the Annual Southeast Regional Conference*, Melbourne, 10-12 March 2006, 531-536. https://doi.org/10.1145/1185448.1185564

[90] Salahdine, F. and Kaabouch, N. (2020) Security Threats, Detection, and Countermeasures for Physical Layer in Cognitive Radio Networks: A Survey. *Physical Communication*, **39**, Article ID: 101001. https://doi.org/10.1016/j.phycom.2020.101001

[91] Jokar, P., Arianpoo, N. and Leung, V.C. (2013) Spoofing Detection in IEEE 802.15.4 Networks Based on Received Signal Strength. *Ad Hoc Networks*, **11**, 2648-2660. https://doi.org/10.1016/j.adhoc.2013.04.015

[92] Zafari, F., Gkelias, A. and Leung, K.K. (2019) A Survey of Indoor Localization Systems and Technologies. *Communications Surveys and Tutorials*, **21**, 2568-2599. https://doi.org/10.1109/COMST.2019.2911558

[93] Wang, L. and Wyglinski, A.M. (2016) Detection of Man-in-the-Middle Attacks Using Physical Layer Wireless Security Techniques. *Wireless Communications and Mobile Computing*, **16**, 408-426. https://doi.org/10.1002/wcm.2527

[94] Chatfield, B. and Haddad, R.J. (2017) RSSI-Based Spoofing Detection in Smart Grid IEEE 802.11 Home Area Networks. *Proceedings of the Power and Energy Society Innovative Smart Grid Technologies Conference* (*ISGT*), Washington DC, 23-26 April 2017, 1-5. https://doi.org/10.1109/ISGT.2017.8086064

[95] Misra, S., Ghosh, A. and Obaidat, M.S. (2010) Detection of Identity-Based Attacks in Wireless Sensor Networks Using Signal Prints. *Proceedings of the Conference on Green Computing and Communications and Conference on Cyber*, *Physical and Social Computing*, Hangzhou, 18-20 December 2010, 35-41. https://doi.org/10.1109/GreenCom-CPSCom.2010.61

[96] Jokar, P., Nicanfar, H. and Leung, V.C.M. (2011) Specification-Based Intrusion Detection for Home Area Networks in Smart Grids. *Proceedings of the Conference on Smart Grid Communications* (*SmartGridComm*), Brussels, 17-20 October 2011, 208-213. https://doi.org/10.1109/SmartGridComm.2011.6102320

[97] Ferrag, M.A., Maglaras, L., Derhab, A. and Janicke, H. (2020) Authentication Schemes for Smart Mobile Devices: Threat Models, Countermeasures, and Open Research Issues. *Telecommunication Systems*, **73**, 317-348. https://doi.org/10.1007/s11235-019-00612-5

[98] Jokar, P. and Leung, V. (2016) Intrusion Detection and Prevention for Zigbee-Based Home Area Networks in Smart Grids. *Transactions on Smart Grid*, **9**, 1800-1811. https://doi.org/10.1109/TSG.2016.2600585

[99] Atassi, A., Sayegh, N., Elhajj, I., Chehab, A. and Kayssi, A. (2013) Malicious Node Detection in Wireless Sensor Networks. *Proceedings of the Conference on Advanced Information Networking and Applications Workshops*, Barcelona, 25-28 March 2013, 456-461. https://doi.org/10.1109/WAINA.2013.135

[100] Chen, Y., Yang, J., Trappe, W. and Martin, R.P. (2010) Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks. *Transactions on Vehicular Technology*, **59**, 2418-2434. https://doi.org/10.1109/TVT.2010.2044904

[101] Maivizhi, R. and Matilda, S. (2014) Distance Based Detection and Localization of Multiple Spoofing Attackers for Wireless Networks. *Proceedings of the Conference on Computation of Power*, *Energy*, *Information and Communication* (*ICCPEIC*), Chennai, 16-17 April 2014, 63-67. https://doi.org/10.1109/ICCPEIC.2014.6915341

[102] Bouabdellah, M., Ghribi, E. and Kaabouch, N. (2019) RSS-Based Localization with

Maximum Likelihood Estimation for PUE Attacker Detection in Cognitive Radio Networks. *Proceedings of the Conference on Electro Information Technology* (*EIT*), Brookings, 20-22 May 2019, 1-6. https://doi.org/10.1109/EIT.2019.8834095

[103] Cheng, M., Ling, Y. and Wu, W.B. (2017) Time Series Analysis for Jamming Attack Detection in Wireless Networks. *Proceedings of the Global Communications Conference*, Singapore, 4-8 December 2017, 1-7. https://doi.org/10.1109/GLOCOM.2017.8254000

[104] Delcourt, M. and Boudec, J.L. (2020) Time Difference of Arrival (TDOA) Source-Localization Technique Robust to Time-Synchronization Attacks. *Transactions on Information Forensics and Security*, **16**, 4249-4264. https://doi.org/10.1109/TIFS.2020.3001741

[105] Zou, Y. and Liu, H. (2020) Time Difference of Arrival (TDOA) Localization with Unknown Signal Propagation Speed and Sensor Position Errors. *Communications Letters*, **24**, 1024-1027. https://doi.org/10.1109/LCOMM.2020.2968434

[106] Peng, R. and Sichitiu, M.L. (2006) Angle of Arrival Localization for Wireless Sensor Networks. *Proceedings of the Communications Society on Sensor and Ad Hoc Communications and Networks*, Reston, 28 September 2006, 374-382. https://doi.org/10.1109/SAHCN.2006.288442

[107] Kulaib, A.R., Shubair, R.M., Al-Qutayri, M.A. and Ng, J.W.P. (2011) An Overview of Localization Techniques for Wireless Sensor Networks. *Proceedings of the Conference on Innovations in Information Technology*, Abu Dhabi, 25-27 April 2011, 167-172. https://doi.org/10.1109/INNOVATIONS.2011.5893810

[108] Zahid, F., Nordin, R. and Ismail, M. (2013) Recent Advances in Wireless Indoor Localization Techniques and System. *Journal of Computer Networks and Communications*, **2013**, Article ID: 185138. https://doi.org/10.1155/2013/185138

[109] Smutz, C. and Stavrou, A. (2012) Malicious PDF Detection Using Metadata and Structural Features. *Proceedings of the Annual Computer Security Applications Conference*, Orlando, 3-7 December 2012, 239-248. https://doi.org/10.1145/2420950.2420987

[110] Wang, J., Tu, W., Hui, L.C.K., Yiu, S.M. and Wang, E.K. (2017) Detecting Time Synchronization Attacks in Cyber-Physical Systems with Machine Learning Techniques. *Proceedings of the Conference on Distributed Computing Systems* (*ICDCS*), Atlanta, 5-8 June 2017, 2246-2251. https://doi.org/10.1109/ICDCS.2017.25

[111] Sowah, R.A., Ofori-Amanfo, K.B., Mills, G.A. and Koumadi, K.M. (2015) Detection and Prevention of Man-in-the-middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN). *Journal of Computer Networks and Communications*, **2019**, Article ID: 4683982.

[112] Prasad, G., Huo, Y., Lampe, L. and M. Leung, V.C. (2019) Machine Learning Based Physical-Layer Intrusion Detection and Location for the Smart Grid. *Proceedings of the Conference on Communications, Control, and Computing Technologies for Smart Grids* (*SmartGridComm*), Beijing, 21-23 October 2019, 1-6. https://doi.org/10.1109/SmartGridComm.2019.8909779

[113] Khoei, T.T., Aissou, G., Hu, W.C. and Kaabouch, N. (2021) Ensemble Learning Methods for Anomaly Intrusion Detection System in Smart Grid. *Proceedings of the* 2021 *IEEE International Conference on Electro Information Technology* (*EIT*), Mt. Pleasant, 14-15 May 2021, 129-135. https://doi.org/10.1109/EIT51626.2021.9491891

[114] Khoei, T.T., Ismail, S. and Kaabouch, N. (2021) Boosting-Based Models with Tree-Structured Parzen Estimator Optimization to Detect Intrusion Attacks on

Smart Grid. *Proceedings of the* 2021 *IEEE* 12*th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference* (*UEMCON*), New York, 1-4 December 2021, 165-170. https://doi.org/10.1109/UEMCON53757.2021.9666607

[115] Khoei, T.T., Hu, W.C. and Kaabouch, N. (2022) Residual Convolutional Network for Detecting Attacks on Intrusion Detection Systems in Smart Grid. *Proceedings of the* 2022 *IEEE International Conference on Electro Information Technology* (*eIT*), Mankato, 19-21 May 2022, 231-237. https://doi.org/10.1109/eIT53891.2022.9813983

[116] Khoei, T.T., Ghribi, E., Ranganathan, P. and Kaabouch, N. (2021) A Performance Comparison of Encryption/Decryption Algorithms for UAV Swarm Communications. https://doi.org/10.13140/RG.2.2.17379.48160

[117] Al-Abassi, A., Karimipour, H., Dehghantanha, A. and Parizi, R.M. (2020) An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. *IEEE Access*, **8**, 83965-83973. https://doi.org/10.1109/ACCESS.2020.2992249

[118] Wang, Z., He, H., Wan, Z. and Sun, Y. (2021) Coordinated Topology Attacks in Smart Grid Using Deep Reinforcement Learning. *IEEE Transactions on Industrial Informatics*, **17**, 1407-1415. https://doi.org/10.1109/TII.2020.2994977

[119] Zhang, Y., Wang, J. and Chen, B. (2021) Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach. *IEEE Transactions on Smart Grid*, **12**, 623-634. https://doi.org/10.1109/TSG.2020.3010510

[120] Scaranti, G.F., Carvalho, L.F., Barbon, S. and Proença, M.L. (2020) Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-Defined Networks. *IEEE Access*, **8**, 100172-100184. https://doi.org/10.1109/ACCESS.2020.2997939

[121] Reyes, H. and Kaabouch, N. (2013) Jamming and Lost Link Detection in Wireless Networks with Fuzzy Logic. *International Journal of Scientific and Engineering Research*, **4**, 1-7.

[122] Gomez, J. and Dasgupta, D. (2002) Evolving Fuzzy Classifiers for Intrusion Detection. *Workshop on Information Assurance*, **6**, 321-323.

[123] Lysenko, S., Bobrovnikova, K., Shchuka, R. and Savenko, O. (2020) A Cyberattacks Detection Technique Based on Evolutionary Algorithms. *Proceedings of the Conference on Dependable Systems, Services and Technologies* (*DESSERT*), Kyiv, 14-18 May 2020, 127-132. https://doi.org/10.1109/DESSERT50317.2020.9125016

[124] Sakhnini, J., Karimipour, H. and Dehghantanha, A. (2019) Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection. *Proceedings of the Conference on Smart Energy Grid Engineering* (*SEGE*), Oshawa, 12-14 August 2019, 108-112. https://doi.org/10.1109/SEGE.2019.8859946

[125] Tsang, C.H., Kwong, S. and Wang, H. (2007) Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection. *Pattern Recognition*, **40**, 2373-2391. https://doi.org/10.1016/j.patcog.2006.12.009

[126] Elhefnawy, R., Abounaser, H. and Badr, A. (2020) A Hybrid Nested Genetic-Fuzzy Algorithm Framework for Intrusion Detection and Attacks. *IEEE Access*, **8**, 98218-98233. https://doi.org/10.1109/ACCESS.2020.2996226

[127] Rawat, D.B. and Bajracharya, C. (2015) Detection of False Data Injection Attacks in Smart Grid Communication Systems. *Signal Processing Letters*, **22**, 1652-1656. https://doi.org/10.1109/MCOM.2015.7045410

[128] Kurt, M.N., Yilmaz, Y. and Wang, X. (2018) Distributed Quickest Detection of Cyber-Attacks in Smart Grid. *Transactions on Information Forensics and Security*, **13**, 2015-2030. https://doi.org/10.1109/TIFS.2018.2800908

[129] Manandhar, K., Cao, X., Hu, F. and Liu, Y. (2014) Detection of Faults and Attacks

Including False Data Injection Attack in Smart Grid Using Kalman Filter. *Transactions on Control of Network Systems*, **1**, 370-379. https://doi.org/10.1109/TCNS.2014.2357531

[130] Li, B., Lu, R. and Xiao, G. (2020) Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems. Springer, Berlin. https://doi.org/10.1007/978-3-030-58672-0

[131] Sun, Q., Wang, S., Yan, D. and Yang, F. (2009) An Early Stage Detecting Method against SYN Flooding Attacks. *China Communication*, **4**, 108-116.

[132] Yang, T. (2005) A Time Series Data Mining Based on Autoregressive Moving Average (ARMA) and Hopfield Model for Intrusion Detection. *Proceedings of the Conference on Neural Networks and Brain*, Beijing, 13-15 October 2005, 1045-1049.

[133] Yaacob, A.H., Tan, I.K., Chien, S.F. and Tan, H.K. (2010) Autoregressive Integrated Moving Average (ARIMA) Based Network Anomaly Detection. *Proceedings of the Conference on Communication Software and Networks*, Singapore, 26-28 February 2010, 205-209. https://doi.org/10.1109/ICCSN.2010.55

[134] Tavolato, P., Schölnast, H. and Tavolato-Wötzl, C. (2020) Analytical Modelling of Cyber-physical Systems: Applying Kinetic Gas Theory to Anomaly Detection in Networks. *Journal of Computer Virology and Hacking Techniques*, **16**, 93-101. https://doi.org/10.1007/s11416-020-00349-9

[135] Tabatabaie Nezhad, S.M., Nazari, M. and Gharavol, E.A. (2016) A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks. *Communications Letters*, **20**, 700-703. https://doi.org/10.1109/LCOMM.2016.2517622

[136] Bashar, S., Ding, Z. and Xiao, C. (2011) On the Secrecy Rate of Multi-Antenna Wiretap Channel under Finite-alphabet Input. *Communication Letter,* **15**, 527-529. https://doi.org/10.1109/LCOMM.2011.032811.102539

[137] Elkashlan, M., Wang, L., Duong, Q., Karagiannidis, K., Nallanathan, A. (2014) On the Security of Cognitive Radio Networks. *Vehicular Technology*, **64**, 3790-3795. https://doi.org/10.1109/TVT.2014.2358624

[138] Chaman, A., Wang, J., Sun, J., Hassanieh, H. and Choudhury, R. (2018) Ghostbuster: Detecting the Presence of Hidden Eavesdroppers. *Proceedings of the Annual International Conference on Mobile Computing and Networking*, New Delhi, 29 October - 2 November 2018, 337-351. https://doi.org/10.1145/3241539.3241580

[139] Geneiatakis, D., Vrakas, N. and Lambrinoudakis, C. (2009) Utilizing Bloom Filters for Detecting Flooding Attacks against Session Initiation Protocol (SIP) Based Services. *Computers and Security*, **28**, 578-591. https://doi.org/10.1016/j.cose.2009.04.007

[140] Khan, I.A., Pi, D., Khan, Z.U., Hussain, Y. and Nawaz, A. (2019) HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems. *IEEE Access*, **7**, 89507-89521. https://doi.org/10.1109/ACCESS.2019.2925838

[141] Efstathopoulos, G., Grammatikis, P.R., Sarigiannidis, P., Argyriou, V., Sarigiannidis, A., Stamatakis, K., Angelopoulos, M.K. and Athanasopoulos, S.K. (2019) Operational Data Based Intrusion Detection System for Smart Grid. *Proceedings of the* 2019 *IEEE* 24*th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks* (*CAMAD*), Limassol, 11-13 September 2019, 1-6. https://doi.org/10.1109/CAMAD.2019.8858503

[142] Chekired, D.A., Khoukhi, L. and Mouftah, H.T. (2019) Fog-Based Distributed Intrusion Detection System against False Metering Attacks in Smart Grid. *Proceed-*

ings of the ICC 2019 *IEEE International Conference on Communications* (*ICC*), Shanghai, 20-24 May 2019, 1-6. https://doi.org/10.1109/ICC.2019.8761752

[143] Chatfield, B. and Haddad, R.J. (2017) Moving Target Defense Intrusion Detection System for ipv6 Based Smart Grid Advanced Metering Infrastructure. *Proceedings of the SoutheastCon* 2017, Concord, 30 March-2 April 2017, 1-7. https://doi.org/10.1109/SECON.2017.7925307

[144] Radoglou Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G. and Panaousis, E. (2020) ARIES: A Novel Multivariate Intrusion Detection System for Smart Grid. *Sensors*, **20**, Article 5305. https://doi.org/10.3390/s21186225

[145] Firoz, N.F., Arefin, M.T. and Uddin, M.R. (2020) Performance Optimization of Layered Signature Based Intrusion Detection System Using Snort. *Proceedings of the International Conference on Cyber Security and Computer Science*, Dhaka, 15-16 February 2020, 14-27. https://doi.org/10.1007/978-3-030-52856-0_2

[146] Ioulianou, P., Vasilakis, V., Moscholios, I. and Logothetis, M. (2018) A Signature-Based Intrusion Detection System for the Internet of Things. *Proceedings of the Information and Communication Technology Form*, Graz, 11-13 July 2018.

[147] Taghavinejad, S.M., Taghavinejad, M., Shahmiri, L., Zavvar, M. and Zavvar, M.H. (2020) Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree. *Proceedings of the 6th International Conference on Web Research* (*ICWR*), Tehran, 22-23 April 2020, 152-156. https://doi.org/10.1109/ICWR49608.2020.9122320

[148] Attia, M., Senouci, S.M., Sedjelmaci, H., Aglzim, E.H. and Chrenko, D. (2018) An Efficient Intrusion Detection System against Cyber-Physical Attacks in the Smart Grid. *Computers & Electrical Engineering*, **68**, 499-512. https://doi.org/10.1016/j.compeleceng.2018.05.006

[149] Jo, H.J. and Yoon, J.W. (2015) A New Countermeasure against Brute-force Attacks that Use High Performance Computers for Big Data Analysis. *Journal of Distributed Sensor Networks*, **11**, Article ID: 406915. https://doi.org/10.1155/2015/406915

[150] Guo, Z., Ni, Y., Wong, W.S. and Shi, L. (2021) Time Synchronization Attack and Countermeasure for Multisystem Scheduling in Remote Estimation. *Transactions on Automatic Control*, **66**, 916-923. https://doi.org/10.1109/TAC.2020.2997318

[151] Mander, T., Cheung, R. and Nabhani, F. (2010) Power System Distributed Network Protocol 3 (DNP3) Data Object Security Using Data Sets. *Computers and Security*, **29**, 487-500. https://doi.org/10.1016/j.cose.2009.10.001

[152] Sridhar, H.S., Siddappa, M. and Prakash, G.C.B. (2016) Design of Secure Communication Protocol for Smart Grid. *Proceedings of the Conference on Emerging Devices and Smart Systems* (*ICEDSS*), Namakkal, 4-5 March 2016, 88-93. https://doi.org/10.1109/ICEDSS.2016.7587773

[153] Martinovic, I., Pichota, P., Wilhelm, M., Zdarsky, F.A. and Schmitt, J.B. (2009) Bringing Law and Order to IEEE 802.11 Networks—A Case for DiscoSec. *Pervasive and Mobile Computing*, **5**, 510-525. https://doi.org/10.1016/j.pmcj.2009.03.002

[154] Zhang, X., Ye, F., Fan, S., Guo, J., Xu, G. and Qian, Y. (2016) An Adaptive Security Protocol for a Wireless Sensor-Based Monitoring Network in Smart Grid Transmission Lines. *Security and Communication Networks*, **9**, 60-71. https://doi.org/10.1002/sec.1382

[155] Kim, Y., Kolesnikov, V., Kim, H. and Thottan, M. (2011) SSTP: A Scalable and Secure Transport Protocol for Smart Grid Data Collection. *Proceedings of the International Conference on Smart Grid Communications* (*SmartGridComm*), Brussels, 17-20 October 2011, 161-166. https://doi.org/10.1109/SmartGridComm.2011.6102310

[156] Moghadam, M.F., Nikooghadam, M., Mohajerzadeh, A.H. and Movali, B. (2020) A Lightweight Key Management Protocol for Secure Communication in Smart Grids. *Electric Power Systems*, **178**, Article ID: 106024. https://doi.org/10.1016/j.epsr.2019.106024

[157] Mohamed Sid Ahmed, A.S.A., Hassan, R. and Othman, N.E. (2017) IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey. *IEEE Access*, **5**, 18187-18210. https://doi.org/10.1109/ACCESS.2017.2737524

[158] Hennebert, C. and Santos, J.D. (2014) Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis. *IEEE Internet of Things Journal*, **1**, 384-398. https://doi.org/10.1109/JIOT.2014.2359538

[159] Leszczyna, R. (2019) Standards with Cybersecurity Controls for Smart Grid—A Systematic Analysis. *International Journal of Communication Systems*, **32**, e3910. https://doi.org/10.1002/dac.3910

[160] Leszczyna, R. (2018) A Review of Standards with Cybersecurity Requirements for Smart Grid. *Computers & Security*, **77**, 262-276. https://doi.org/10.1016/j.cose.2018.03.011

[161] Leszczyna, R. (2017) Cybersecurity and Privacy in Standards for Smart Grids—A Comprehensive Survey. *Computer Standards & Interfaces*, **56**: 62-73. https://doi.org/10.1016/j.csi.2017.09.005

[162] Leszczyna, R. (2018) Standards on Cyber Security Assessment of Smart Grid. *International Journal of Critical Infrastructure Protection*, **22**, 70-89. https://doi.org/10.1016/j.ijcip.2018.05.006

[163] Radoglou-Grammatikis, P.I. and Sarigiannidis, P.G. (2019) Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. *IEEE Access*, **7**, 46595-46620. https://doi.org/10.1109/ACCESS.2019.2909807

[164] Sadikin, F., van Deursen, T. and Kumar, S. (2020) A ZigBee Intrusion Detection System for IoT Using Secure and Efficient Data Collection. *Internet of Things*, **12**, Article ID: 100306. https://doi.org/10.1016/j.iot.2020.100306

[165] Tolba, A. and Al-Makhadmeh, Z. (2021) Predictive Data Analysis Approach for Securing Medical Data in Smart Grid Healthcare Systems. *Future Generation Computer Systems*, **117**, 87-96. https://doi.org/10.1016/j.future.2020.11.008

[166] Mengese, F., *et al.* (2020) Towards GDPR-Compliant Data Processing in Modern Security Information and Event Management (SIEM) Systems. *Computers and Security*, **103**, Article ID: 102165. https://doi.org/10.1016/j.cose.2020.102165

[167] Shrestha, M., Johansen, C., Noll, J. and Roverso, D. (2020) A Methodology for Security Classification Applied to Smart Grid Infrastructures. *Journal of Critical Infrastructure Protection*, **28**, Article ID: 100342. https://doi.org/10.1016/j.ijcip.2020.100342

[168] Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M. and Mohammadi-Ivatloo, B. (2020) Ensuring Cybersecurity of Smart Grid against Data Integrity Attacks under Concept Drift. *International Journal of Electrical Power and Energy Systems*, **119**, Article ID: 105947. https://doi.org/10.1016/j.ijepes.2020.105947

[169] Ullah, K.W., Ahmed, A.S. and Ylitalo, J. (2013) Towards Building an Automated Security Compliance Tool for the Cloud. *Proceedings of the Conference on Trust, Security and Privacy in Computing and Communications*, Melbourne, 16-18 July 2013, 1587-1593. https://doi.org/10.1109/TrustCom.2013.195

[170] McCary, E. and Xiao, Y. (2015) Smart Grid Attacks and Countermeasures. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, **2**, e4. https://doi.org/10.4108/inis.2.2.e4

[171] Abdelwahab, A., Lucia, W. and Youssef, A. (2020) Decoy-based Moving Target defense Against Cyber-Physical Attacks on Smart Grid. *Proceedings of the* 2020 *IEEE Electric Power and Energy Conference* (*EPEC*), Edmonton, 9-10 November 2020, 1-5. https://doi.org/10.1109/EPEC48502.2020.9320029

[172] Mouaatamid, O.E., Lahmer, M. and Belkasmi, M. (2016) Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures. *Electronic Journal of Information Technology*, **9**, 66-80.

[173] Usman, M., Raponi, S., Qaraqe, M. and Oligeri, G. (2020) KaFHCa: Key-Establishment via Frequency Hopping Collisions. arXiv preprint, arXiv:2010.09642. https://doi.org/10.1109/ICC42927.2021.9500315

[174] Chiang, J.T. and Hu, Y.C. (2008) Dynamic Jamming Mitigation for Wireless Broadcast Networks. *Proceedings of the IEEE INFOCOM* 2008—*The* 27*th Conference on Computer Communications*, Phoenix, 13-18 April 2008, 1211-1219. https://doi.org/10.1109/INFOCOM.2008.177

[175] Desmedt, Y., Safavi-Naini, R., Wang, H., Charnes, C. and Pieprzyk, J. (1999) Broadcast Anti-Jamming Systems. *Proceedings of the IEEE International Conference on Networks. ICON*'99 *Proceedings* (Cat. No.PR00243), Brisbane, 28 September - 1 October 1999, 349-355. https://doi.org/10.1109/ICON.1999.796197

[176] Pickholtz, R.L., Schilling, D.L. and Milstein, L.B. (1982) Theory of Spread Spectrum Communications—A Tutorial. *IEEE Transactions on Communications*, **30**, 855-884. https://doi.org/10.1109/TCOM.1982.1095533

[177] Mohammadi, F. (2021) Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies*, **14**, Article 1380. https://doi.org/10.3390/en14051380

[178] Wang, Q., Tai, W., Tang, Y., Ni, M. and You, S. (2019) A Two-Layer Game Theoretical Attack-Defense Model for a False Data Injection Attack against Power Systems. *International Journal of Electrical Power and Energy Systems*, **104**, 169-177. https://doi.org/10.1016/j.ijepes.2018.07.007

[179] Abusorrah, A., Alabdulwahab, A., Li, Z. and Shahidehpour, M. (2019) Minimax-Regret Robust Defensive Strategy against False Data Injection Attacks. *IEEE Transactions on Smart Grid*, **10**, 2068-2079. https://doi.org/10.1109/TSG.2017.2788040

[180] Pilz, M., Naeini, F.B., Grammont, K., Smagghe, C., Davis, M., Nebel, J.-C., Al-Fagih, L. and Pfluegel, E. (2019) Security Attacks on Smart Grid Scheduling and Their Defences: A Game-Theoretic Approach. *International Journal of Information Security*, **19**, 427-443. https://doi.org/10.1007/s10207-019-00460-z

[181] Hasan, S., Dubey, A., Karsai, G. and Koutsoukos, X. (2020) A Game-Theoretic Approach for Power Systems Defense against Dynamic Cyber-Attacks. *International Journal of Electrical Power and Energy Systems*, **115**, Article ID: 105432. https://doi.org/10.1016/j.ijepes.2019.105432

[182] Cheng, C., Qin, Y., Lu, R., Jiang, T. and Takagi, T. (2019) Batten Down the Hatches: Securing Neighborhood Area Networks of Smart Grid in the Quantum Era. *IEEE Transactions on Smart Grid*, **10**, 6386-6395. https://doi.org/10.1109/TSG.2019.2903836

[183] Gao, B. and Shi, L. (2020) Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System. *IEEE Access*, **8**, 30322-30331. https://doi.org/10.1109/ACCESS.2020.2973030

[184] Torres, B.S., Borges da Silva, L.E., Salomon, C.P. and de Moraes, C.H.V. (2022) Integrating Smart Grid Devices into the Traditional Protection of Distribution Networks. *Energies*, **15**, 2518. https://doi.org/10.3390/en15072518

[185] Roth, S., Barron, T., Calzavara, S., Nikiforakis, N. and Stock, B. (2020) Complex

Security Policy? A Longitudinal Analysis of Deployed Content Security Policies. *Proceedings of the 27th Network and Distributed System Security Symposium* (*NDSS*), San Diego, 23-26 February 2020. https://doi.org/10.14722/ndss.2020.23046