




Article

Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects

Usman Inayat ¹, Muhammad Fahad Zia ², Sajid Mahmood ¹, Tarek Berghout ³
and Mohamed Benbouzid ^{4,5,*}

¹ Department of Informatics & Systems, School of Systems & Technology, University of Management and Technology, Lahore 54770, Pakistan

² Department of Electrical and Computer Engineering, American University in Dubai, Dubai 28282, United Arab Emirates

³ Laboratory of Automation and Manufacturing Engineering, University of Batna 2, Batna 05000, Algeria

⁴ Institut de Recherche Dupuy de Lôme (UMR CNRS 6027 IRL), University of Brest, 29238 Brest, France

⁵ Logistics Engineering College, Shanghai Maritime University, Shanghai 201306, China

* Correspondence: mohamed.benbouzid@univ-brest.fr

Abstract: Smart grid is an emerging system providing many benefits in digitizing the traditional power distribution systems. However, the added benefits of digitization and the use of the Internet of Things (IoT) technologies in smart grids also poses threats to its reliable continuous operation due to cyberattacks. Cyber-physical smart grid systems must be secured against increasing security threats and attacks. The most widely studied attacks in smart grids are false data injection attacks (FDIA), denial of service, distributed denial of service (DDoS), and spoofing attacks. These cyberattacks can jeopardize the smooth operation of a smart grid and result in considerable economic losses, equipment damages, and malicious control. This paper focuses on providing an extensive survey on defense mechanisms that can be used to detect these types of cyberattacks and mitigate the associated risks. The future research directions are also provided in the paper for efficient detection and prevention of such cyberattacks.

Keywords: cyber-physical power system; cybersecurity; cyberattack; false data injection; denial of service; spoofing attack; smart grid



Citation: Inayat, U.; Zia, M.F.; Mahmood, S.; Berghout, T.; Benbouzid, M. Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects. *Electronics* **2022**, *11*, 3854. <https://doi.org/10.3390/electronics11233854>

Academic Editor: Ahmed F. Zobaa

Received: 1 November 2022

Accepted: 21 November 2022

Published: 23 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

An electricity network, in which the bidirectional flow of electricity and data is achieved using digital technologies for communication, is called a smart grid [1]. The purpose of a smart grid is to transform traditional electricity networks into the modern grid with the help of information and communication technologies (ICTs) [2]. Transmission of large data was not possible in traditional grids with the high-voltage transmission cables [3]. The electric power transfer from centralized power plants to the consumers involves various electrical components [4], such as transmission lines, transformers, and substations, among others [5]. Furthermore, traditional grids have no energy storage devices available on a large scale. Renewable power generation and demand response at the distribution end need effective communication for information exchange among different components of a smart grid [6]. Smart grid has the best possible solutions for almost all the challenges a traditional network can face [7,8]. To achieve reliability, security, efficient monitoring, and enhanced transfer of electricity, smart grid researchers introduced communication between electrical and digital data [9]; however, the advantages of digitization in smart grids have also increased data security issues for the electricity networks; therefore, smart grid security is also a vital challenge [10].

The complete infrastructure of a smart grid is highly dependent on its communication system that is coupled with power system [11]. A power system relies on the power flow,

whereas a cyber system relies on the information flow. The communication channel uses various devices and technologies for communication. The communication systems are extremely vulnerable to cyberattacks [12]. The attackers aim to attack the communication links to access physical systems and modify or block information flow [13].

Cybersecurity refers to the practice of protecting data confidentiality, availability, and integrity in the systems or devices that are associated with the Internet [14]. It defends electronic devices and networks such as mobile devices, computers, and electronic systems by protecting their data from misuse by unauthorized users and attackers [15]. Cybersecurity in the smart grids defends their data confidentiality, availability, and integrity from such dangers [16]. Security mechanisms built for IT networks are not sufficient for securing grid networks because of different system dynamics [17]. Availability, integrity, and confidentiality of smart grid network data must be secured for its reliable and continuous operation; therefore, well-defined cybersecurity mechanisms are needed to protect the smart grid system from malicious attacks and vulnerabilities [18].

Data attacks in a smart grid can be categorized into three major divisions: Confidentiality, integrity, and availability attacks [18]. These data attacks can happen on devices, network topology, and network protocols [19,20]. False data injection (FDI) attacks are the influential attacks that target the communication protocols of the smart grid network. Denial of Service (DoS) is another attack that disturbs the network topology due to which operators cannot have a wider observation and control of the power system [21]. Malware, replay attack, and eavesdropping are some foremost attacks on meters and sensors of a smart grid. The main objective of the attacker is to obtain, modify or block the information to adversely affect the smart grid operation, steal confidential information, or gain financial benefits [22–24].

The schematic representation of a smart grid system is given in Figure 1, which shows different components of a smart grid [25]. The power generation plants, transmission and distribution system, information and communication systems, distributed generation and energy storage, and prosumers are major parts of the smart grid system. Power sources for bulk generation are hydroelectric plants, diesel power plants, microturbines, nuclear power plants, wind turbines, and photovoltaic plants [26]. Using these primary sources, power is generated to transmit it for use in domestic and industrial applications. In a transmission network, interconnected lines facilitate the power transmission to distribution end. High voltage AC current is transferred through transmission lines whereas voltage is reduced for local distribution of current. In the primary stage, bulk electric power is transferred from the generating station to the substation. In the secondary stage, power is transferred from substations to different cities and villages. To store the excess electricity, grid energy storage is used to store energy on a large scale. Smart grid system can be monitored, controlled, and managed remotely with sensors and intelligent electronic devices (IEDs) [27]. The transmission and distribution levels include power lines, intelligent substations, monitoring and control automation systems, and smart transformers that are equipped with sensors. All the devices and components are managed at the upper level by an energy management system, transmission and distribution management system, centralized and decentralized management system, and outage management system. The supervisory and management systems are interfaced with the power network by information and communication technologies (ICT) layer.

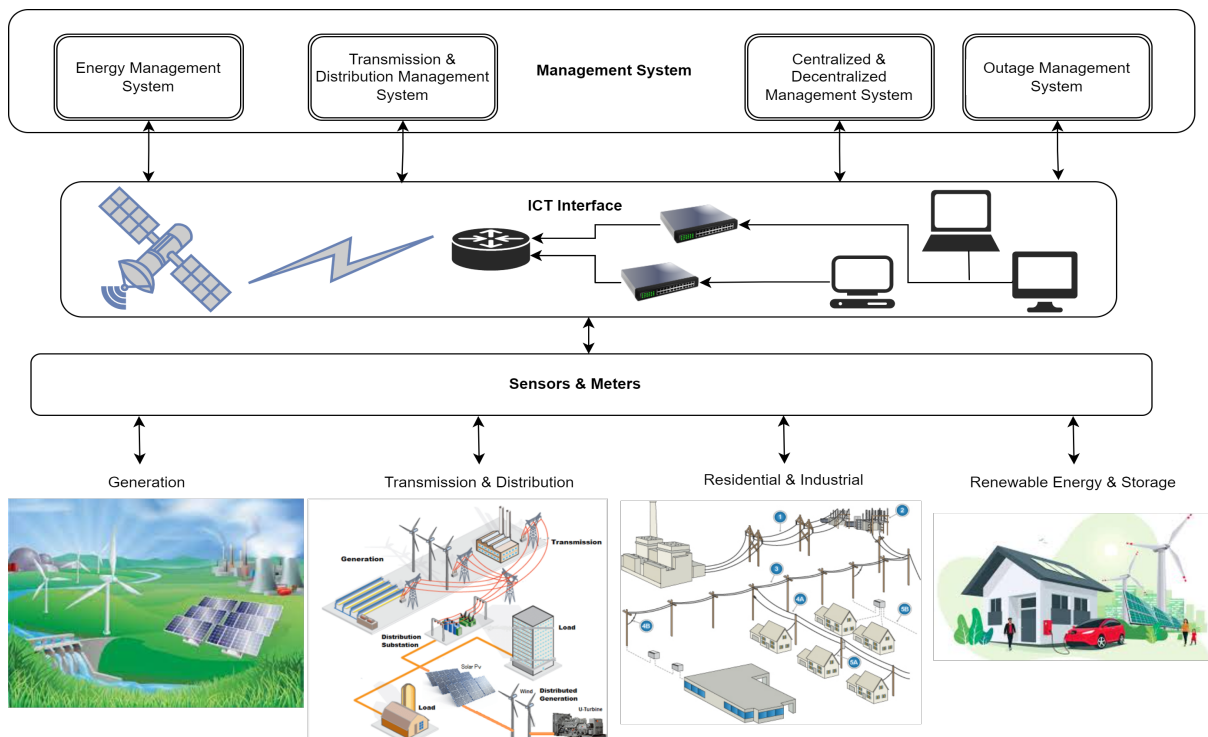


Figure 1. General illustration of smart grid infrastructure.

1.1. Preceding Affined Review Papers

Different reviews on cyberattacks for smart grid already exist in the literature. However, they most cover only the FDI attacks, DoS attacks, and their machine and deep-learning-based detection methods within the smart grid system. The summary of these reviews is given in Table 1. In [28], FDIA is introduced and its physical and economic impact on smart grids along with detection approaches are discussed. In [29], the impacts of cyberattacks on smart grids are analyzed and potential research progress in China is discussed. The authors in [30] assessed the security risks of DoS and integrity attacks in smart grid system. In [31], only machine-learning-based detection methods are discussed for only FDIA in smart grid systems. In [32], the impacts of cyberattacks on control and stability of smart grid system are discussed. However, these review papers do not express the DDoS and GPS spoofing attacks together with FDIA and DoS attacks. Moreover, these review papers are mainly focused on machine-learning-based defense strategies for cyberattacks detection in smart grid, which formed the main motivation for this paper.

Table 1. Review papers on cyberattacks in smart grid systems.

Ref.	Description
[28]	This paper reviewed the FDIA attacks and discussed the economic and physical impact of the successful FDIA in smart grids. It also presented the defense strategies against FDIAs.
[29]	The authors analyzed the impacts of cyberattacks on interactive models of smart grids and presented corresponding solution approaches as graphic dimension, mechanism dimension, and probability dimension methods.
[30]	The authors introduced a layered approach to evaluate the security risks of both cyber and physical power systems against integrity and denial of service attacks.
[31]	This paper detected the FDIA impacts toward non-technical losses, state estimation, and load forecasting using machine learning methods.
[32]	This paper summarized the modeling methods of smart grid systems. This paper also analyzed the impacts of cyberattacks on control and stability of power system, and types of cyberattacks from the perspectives of simulation, probability, topology, and mechanism. It also introduced a unified framework for modeling physical and cyber components.

1.2. Necessity for an Up-To-Date Review

In the existing literature/research, the main focus was on either false data injection or denial of service attack. The attacks, such as GPS spoofing and distributed denial of service attacks, were not included in the past research; we have considered both denial of service attacks and false data injection with other important attacks, such as GPS spoofing and distributed denial of service attacks. The types of attacks are increasing with the rapid improvement and extensive acquisition of smart grid technology devices. This makes the security concerns further complicated, which increases the need to constantly update the security systems by researching and investigating them. As the utilization of technology increases, and with the rise in the amount of information available on networks, quicker and more proficient ways to identify attacks are required, and undoubtedly there are a large number of progressing ways of further developing the security of networks. Moreover, these reviews focused on artificial intelligence-based detection methods for FDIA and DoS attack. However, this review includes both artificial intelligence and other detection methods for cyberattacks detection within smart grid. According to the Google Scholar database, there is a continuous increase in the number of publications dealing with smart grid attacks, from 4900 in 2018 to 5060 publications in 2022. The focus of the research community for smart grid applications and cyberattacks on them is globally emerging. Detecting the location of the attack is also pretty important; however, the previous smart grid research focuses only on the presence of FDI and DoS attacks.

1.3. Review Methodology Brief Description

Various sources of information, namely, Scopus, IEEE Xplore, Google Scholar, MDPI, and Web of Science were used to find the existing research for conducting this literature review. The key step was to retrieve the relevant review articles on the basis of some selected keywords. The primary selection for this review was made with respect to several characteristics, as provided in Figure 2. These keywords are smart grid, cyber-physical power system (CPPS), cybersecurity, cyberattack, cyberthreats, FDIA, DOS, DDoS, and GPS spoofing attack. Articles published in English between 2012 and 2021 were selected for review. The second step involved the grouping of these articles into different sections. The articles were divided into two main groups: articles related to smart grid applications and articles related to smart grid attacks. Articles related to cyberattacks are further divided into FDI attacks, spoofing attacks, DoS attacks, and DDoS attacks. Every single article is further distributed with respect to the core of its research findings.

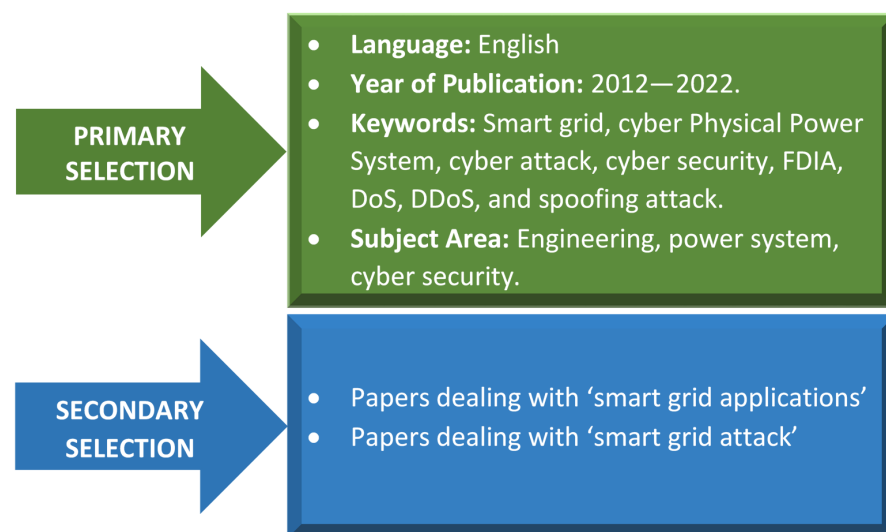


Figure 2. Research papers selection procedure.

1.4. Formation of the Remaining Work

The rest of the article is structured as follows: Cyberattacks (FDIA, DoS, DDoS, and GPS spoofing) in smart grid and their detection methods are described in Section 2. Future research directions are provided in Section 3. Finally, conclusions are summarized in Section 4.

2. Cyberattacks in Smart Grid

Smart grid is a combination of the power grid and a communication network, security attacks may take place in both the physical space, as in the conventional power grid, and cyber space as in any communication network. There are numerous types of attacks that may be carried out on a smart grid system. The most commonly occurring attacks in smart grid are FDIA, DoS, DDoS, and GPS spoofing attacks. The detection methods proposed for these attacks are discussed in the following sections.

2.1. False Data Injection Attacks

False data injection attack (FDIA) is the most vicious attack in the smart grid systems. In FDIA, an attacker intrudes the system and modifies sensor readings such that undetected errors are to be introduced into estimation of state variables and scheduling decisions. The direct access of the physical network is considerably difficult compared to accessing the communication channel. In this attack, the attacker focuses on the communication network and communication channel to manipulate the sensors reading as shown in Figure 3. Detecting such kinds of attacks is extremely complex and challenging.

A deep-learning-based location detection (DLLD) architecture is proposed in [33] to detect the real-time location of FDIA attacks. A bad data detector is also used to filter the low-quality data. A convolutional neural network (CNN) is employed for capturing the inconsistent power flow measurements; however, it does not modify the current bad data detection system and also does not leverage any prior statistical assumptions. In [34], a linear model is presented for a general FDIA attack, which is based on a short-term state forecasting with the temporal correlation. It presents the consistency test to examine the deviations among the received measurements and the forecasted measurements. Furthermore, a detector is also proposed to check the shortcomings of the previous detectors and to handle critical estimations.

An adaptive sliding mode controller is presented in [35] to detect FDIA and dynamic load altering attack (DLAA). The developed controller is able to secure the reliable operations of the under attacked power system. Moreover, the upper bound of the attack signals is also estimated to eliminate the effect of multiple attacks. In [36], authors claim to develop the quickest intrusion detection algorithm for FDIA detection. The detection algorithm is developed by analyzing the statistical properties of dynamic state estimations. It is claimed that the algorithm minimizes the worst-case detection delay while identifying FDIA attacks and sudden system changes.

A hybrid FDIA detection mechanism is introduced in [37] to ensure the security of power system operations and control. The proposed mechanism combines machine learning and variational mode decomposition (VMD) technology. VMD is used to disintegrate the system state time series into an ensemble of elements with distinct frequencies. The consequence of attack intensity and environmental noise on the performance of the aimed technique is also examined. In [38], combination of weighted residual method and equivalent measurement transformation is used to identify and detect false data. To test the effectiveness of the algorithm IEEE 14 bus system was used in the MATLAB environment. In [39], an improved extreme learning machine method is proposed to suppress the redundancies of the feature vectors and use the obtained features vectors for training a time-series analysis-based LSTM detection method. This proposed mechanism can efficiently detect the new type of FDIA by examining the variations between the feature vectors in both the temporal and spatial aspects.

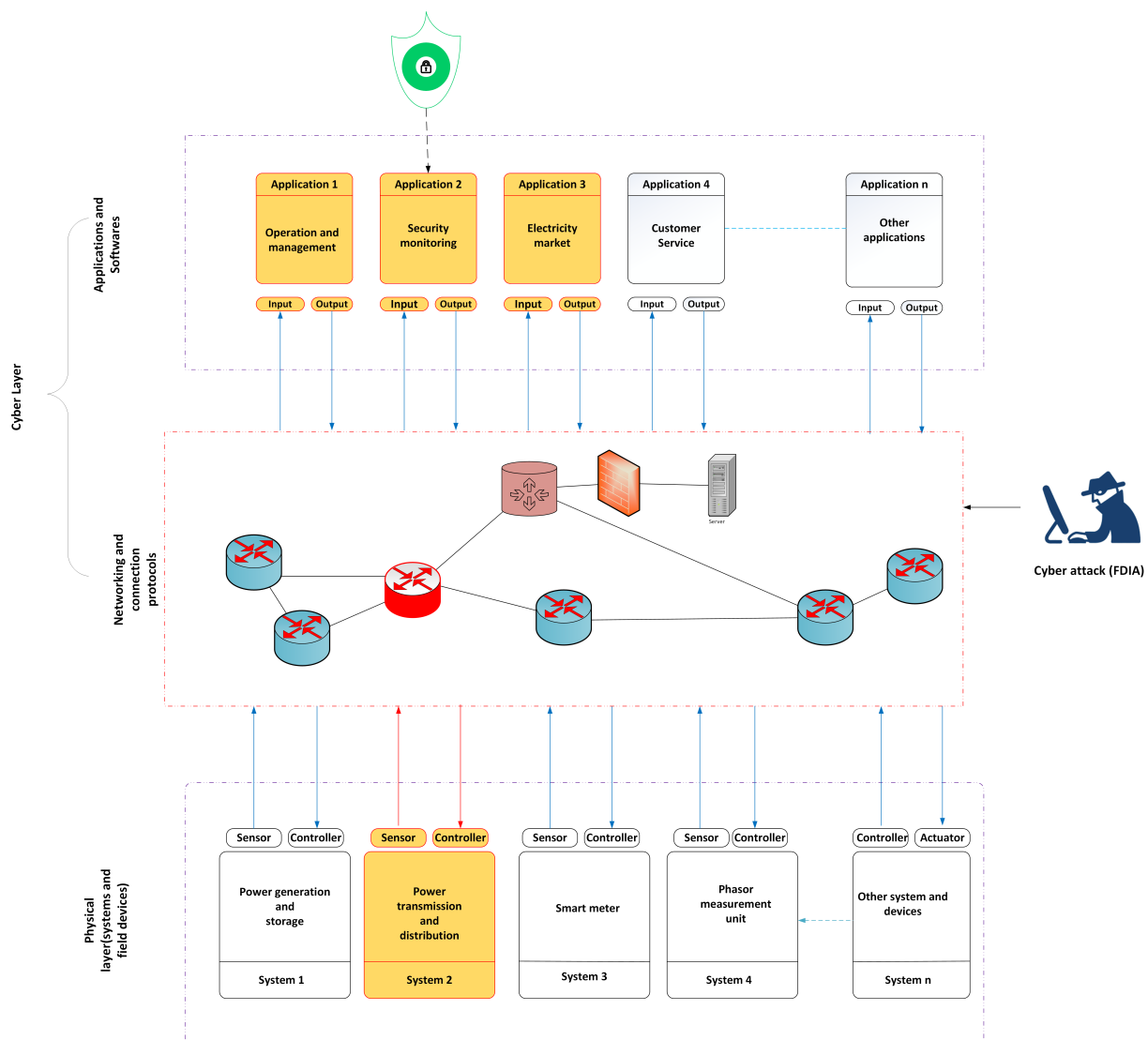


Figure 3. General illustration of false data injection attack in a smart grid system.

In [40,41], cumulative sum (CUSUM)-based statistics are used to detect FDIA in real-time. In the general CUSUM-based statistics method, maximum possible loss is minimized using the known probability distribution functions of both pre- and post-attacks events. The smart grid system is considered under attack if the CUSUM-based statistic exceeds predefined threshold; however, [40] proposed a generalized likelihood ratio-based centralized and distributed sequential detection method using a level-triggered sampling technique. It is reported to be computationally efficient to detect the FDIA attack and reduce the communication overhead in the system; on the contrary, the authors in [41] proposed a modified real-time FDIA detection method using a residual pre-whitening technique. It aims to reduce the average detection delay and provide the quickest stopping point for declaring that the system is under attack. A power load forecasting model is proposed in [42], which is based on the framework of the cyber-physical-social systems to take social implications into account for load balancing. The authors of [43] introduced the Padé approximation-based method and explicit infinitesimal generator discretization-based method against delayed cyber-physical power systems.

In [44], the worst-case impact of FDIA is investigated in smart grid with both fixed and switching locations. In [45], a method for extracting patterns based on temporal-topological correlation is proposed to restore the complete attack path for all network attacks; however, it is merely limited to small topologies. To capture ideal measurements in state estimation

against FDIA, generative adversarial network (GAN) based data model is introduced in [46] and results showed promising outcomes. In [47], authors introduced cognitive risk control (CRC) as a physical model and research tool to unit the cognitive-dynamic systems (CDS). Yet, it is not able to identify the specific sensor which is affected by the FDIA attack. Table 2 presents the summary of detection methods developed for FDIA detection in smart grid system. The targeted devices and contributions are also summarized in it.

Table 2. Review of false data injection attack detection in smart grid systems.

Ref.	Victim Device	Type of Attack	Solution Method	Description
[33]	State estimator	FDI-Power buses	Convolutional neural network	It captures the inconsistency and co-occurrence dependency in the power flow measurements due to the potential attacks and detects the exact locations of FDIA in real-time by concatenating convolutional neural network with a standard bad data detector.
[34]	SCADA and PMU measurements	FDI-Power measurements	Short-term state forecasting-based method	Proposed detector addresses the shortcoming of previous detectors in terms of handling critical measurements using temporal correlation.
[35]	Smart grid	FDI- Control and Dynamic load altering attack	Adaptive sliding mode controller	It presents and adaptive sliding mode controller to ensure the reliable operation of the power system under unknown attack by using the adaptive mechanism.
[36]	SCADA system	FDI-power grid state transitions and worst case detection delays	Quickest intrusion detection algorithm and Dynamic state estimation algorithm	It estimates and tracks the time-varying and non-stationary power grid states using Rao-CUSUM detector.
[37]	Power system state estimators	FDI-Power buses and Sensors	Online sequential extreme learning machine and variational mode decomposition	An effective FDIA detection method is presented with temporal correlation.
[38]	State estimation system	FDI-Power measurement	Equivalent-current based measurement transformation method	A weighted residual method is presented to detect and identify the FDIAs.
[39]	Communication System	FDI-Generation scheduling and power shedding	LSTM	Attacks are detected by analyzing the feature vectors that learn the temporal correlations of the feature vectors in time sequence.
[40]	Power monitoring meters and State estimators	FDI-Power measurements	Generalized CUSUM algorithm	A distributed sequential detector is proposed which uses level-triggered sampling technique.
[41]	State estimation system	FDI-Power Buses and measurements	Residual pre-whitening algorithm	Residual pre-whitening technique based on the CUSUM of the one-shot statistic is used to resolve real-time FDIA detection mechanisms.
[42]	Power network and Social network	FDI-Load Measurement	LSTM	A power load forecasting model based on deep learning and statistical method is proposed which is able to mitigate FDIA.
[44]	Generator bus	FDI- Generator frequency and switching attack	Optimal partial state feedback law	A scheme based on manipulating the subset of control signals and changing the locations of attack continually to degrade system performance at a minimum cost using convex relaxation and Pontryagin's maximum principle.
[46]	Power system state estimator	FDI-Power measurement	Generative Adversarial Network (GAN)-based data model	Novel smooth training technique for GAN is developed and an online adaptive window is explored to maintain the state estimation integrity in real-time.
[47]	Smart grid	FDI-Power bus	Cognitive risk control	The entropic state is used to detect and bring FDI attacks under control using CRC with task-switch control.

2.2. Denial of Service (DoS) Attacks

In a DoS attack, the attacker mainly focuses on making an intelligent device inaccessible for its intended use by flooding it with large unexpected data traffic. Data flooding blocks the regular traffic from reaching to its target device as shown in Figure 4. Flooding the service and crashing the service are two main methods of DoS attacks. The flooding includes three types of attacks: buffer overflow attack, synchronization, and ICMP flood attacks. The advanced form of DoS is Distributed Denial of Service (DDoS) attack. Instead of flooding, a DDoS attack focuses on crashing the target machine by attacking the machine from multiple compromised hosts rather than one source. In the smart grid, DoS attack exploits the network topology and attacks all the possible attack sources, whereas DDoS attacks use compromised hosts to launch an organized DoS attack towards multiple targets—it effectively expands the power of attack and makes defense more obscure and complex.

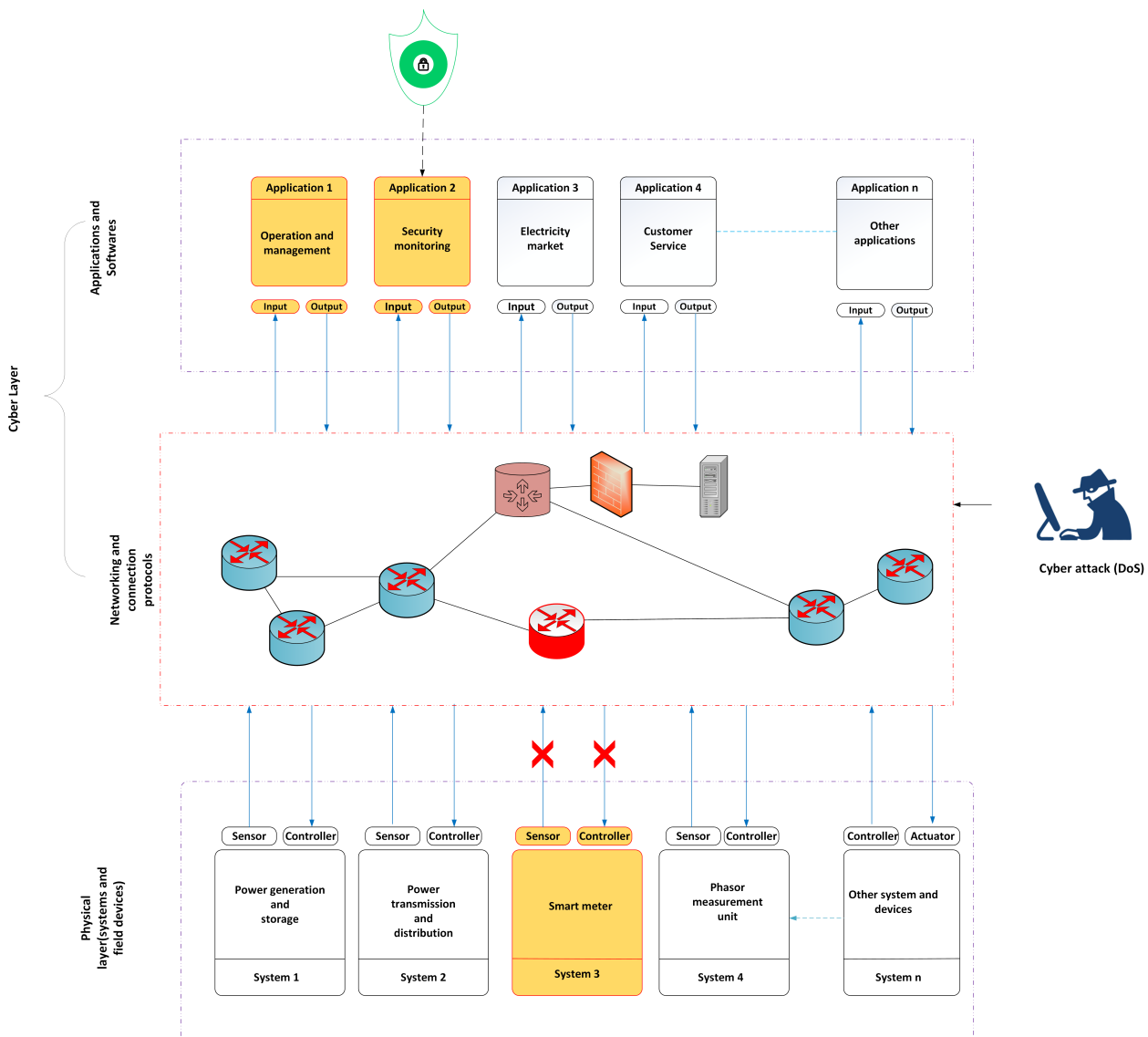


Figure 4. Schematic representation of the denial of service attack.

A Gaussian process model is presented in [48] for malicious DDoS attacks detection. A warning system is introduced in smart grid control to predict such malicious events and enable smart grid control center to develop the mitigation strategy. Moreover, this system can also predict fluctuations and abnormal voltage surges. In [49], DoS detection methods in different layers of sensor networks are discussed. It is also concluded that cybersecurity

enhancement must be considered at the design stage of sensors to maximally avoid DoS attacks in their real-time operation.

Different methods for DDoS attack detection are proposed in [50]. A pattern detection mechanism uses a model that stores the signatures of previously identified attacks. The second method is the anomaly detection method. In this method, a model is created on the basis of the expected state of the system. This model is then compared with the current state of the system. In the third-party detection mechanism, it rely on externals to handle the detection process and provide attack characterization. Authors in [51] deployed a pseudo-state estimation application to detect the DoS attack or clock accuracy. It provides valid and realistic results built on a proof-of-concept prototype. However, it uses an overlay-based proactive defense mechanism that can offer smart grid network nodes to create a first-level firewall against DDoS attacks. By using a pub-sub infrastructure, it can also provide secure data delivery in a light-weight manner.

Honeypots are introduced in [52] for enhancing security against DDoS attacks in the advanced metering infrastructure network of the smart grid. Honeypot game strategy is used to analyze the strategic interactions between attackers and defenders to protect data and improve the security of the advanced metering infrastructure network. In [53], a reputation-based topology configuration scheme is presented against DOS attacks that enables cyber elements to distributively reconfigure the system's routing topology to isolate malicious nodes in the micro grid.

A detection framework is proposed in [54] that allows sufficient readings from meters to be continuously collected through various local controllers for estimating the states of a grid and provide self-healing capability against jamming and DOS attacks. In [55], a general and scalable mitigation approach is developed that is aimed to be capable of timely detection of DDoS attacks in IoT devices.

The authors in [56] implemented parametric feedback linearization controller to control the delay that occurred between sensors and controllers due to DOS attack; however, they tested this controller on limited nodes. In [57], an advanced communicated-assisted protection scheme is introduced to examine the vulnerabilities such as permissive over-reaching transfer trip to DDoS and FDIA attacks. The authors of [58] established a new lightweight, secure, and reliable communication platform that can allow both secure and cost-effective communication. Table 3 presents the summary of detection methods developed for DoS and DDoS attacks detection in smart grid system. The targeted devices and contributions are also summarized in it.

Table 3. Review of DoS and DDoS attacks detection in smart grid systems.

Ref.	Victim Device	Type of Attack	Solution Method	Description
[48]	Smart meter and electric appliances	DDoS	Gaussian process	Gaussian process is used to detect DDoS attack using mean and covariance functions of underlying system model to predict its abnormal mode of operation.
[49]	Sensors	DoS	Authorization, redundancy, and real-time location-based methods	Attacks in different communication layers and their defense mechanisms are discussed and dropped data are recorded even outside the sensor network.
[50]	Electric system devices	DDoS	Activity level, cooperation degree, and deployment location-based defense mechanisms	Taxonomies of DDoS attacks and their corresponding defense mechanism are briefed.
[51]	Cloud assisted applications	DDoS	Port hopping spread spectrum	DDoS attacks are prevented with the help of open port switching over time in a pseudo-random manner. The proposed method is verified on the PlanetLab test-bed and Amazon's EC2.

Table 3. Cont.

Ref.	Victim Device	Type of Attack	Solution Method	Description
[52]	Advanced Metering Infrastructure	DDoS	Honeypot game strategy	The propose method helps in better analysis of strategic interactions between defenders and attacks. Attack detection rate are considerably improved, which shows promising security enhancement of AMI networks.
[53]	Wireless relay nodes	DoS	Reputation-based topology configuration method	Successful isolation of attacked cyber nodes are achieved and data are continuously transmitted at low latency.
[54]	Smart meter	DoS and channel jamming attacks	Intelligent local controller switching with channel hopping	Sufficient readings from meters are continuously collected through various local controllers to estimate the states of a grid under considered attacks. Optimal placement strategy of local controllers is also provided to avoid jamming attacks.
[55]	Smart appliances	DoS	Minimally invasive attack mitigation via detection isolation and localization	The proposed mitigation method is scalable and has capability of timely detection of DDoS attacks.
[56]	Sensor and controllers	DoS	Parametric feedback linearization control	Time-delay tolerance of power system is enhanced using communication latency values between controllers and sensors.
[57]	Distance relay	DDoS	Directional comparison unblocking scheme	Only permissive overreaching transfer trip protection is studied. DDoS attacks are avoided in power system protection relays to some extents only.
[58]	Client nodes	DDoS and replay attacks	Multi-homing based enhanced packet diffusion mechanism	Secure end-to-end data delivery is ensured with light weight mechanism against DDoS and replay attacks.

2.3. Spoofing Attacks

In a spoofing attack, the attacker focuses on the communication links. GPS spoofing attack is the widely studied spoofing attack in smart grid system. A general illustration of GPS spoofing attack is depicted in Figure 5. The communication links between a monitoring device and the control center are vulnerable to spoofing attacks [59,60].

Smart grid systems need sub-microsecond precision at power substations to provide better performance measurements, fault detection, automated network management, and protection relay operations. This sub-microsecond precision relies on time reference sources such as global navigation satellite system (GNSS) clocks. In order to enable real-time automatic control of the smart grid, low-cost and high-precision GPS receivers are being embedded into a large number of intelligent grid sensors, such as phasor measurement units. However, GPS receivers can be spoofed by nearby attackers that transmit high-power false signals with the same GPS frequency. Moreover, the position of each satellite in the global navigation satellite system is publicly available online; therefore, a GPS signal can be easily spoofed or jammed by a malicious attacker [61]. Timing inaccuracies at the time source or between the time source and the time stamping site might result in erroneous measurement data, missing data, and/or failed data frame compilation. Data gaps caused by unreliable data delivery to data concentrators, control centers, and applications within acceptable latency times could impede early warning information about dynamic grid issues [62]. Hence, It is essential that the GPS signals are resilient to interference, and increasingly to jamming and spoofing, given the importance of the power system and the possibility that the smart grid will depend on high-precision timing in the future.

A fast GPS spoofing detection method is presented in [63], which is based on multi-antenna by applying the probabilistic metric of the carrier signal to noise ratio from two receive antennas to conduct the speediest GPS spoofing detection. A test bed is also set up to verify their results. The results demonstrated the effective scheme to glimpse and stop spoofing attacks.

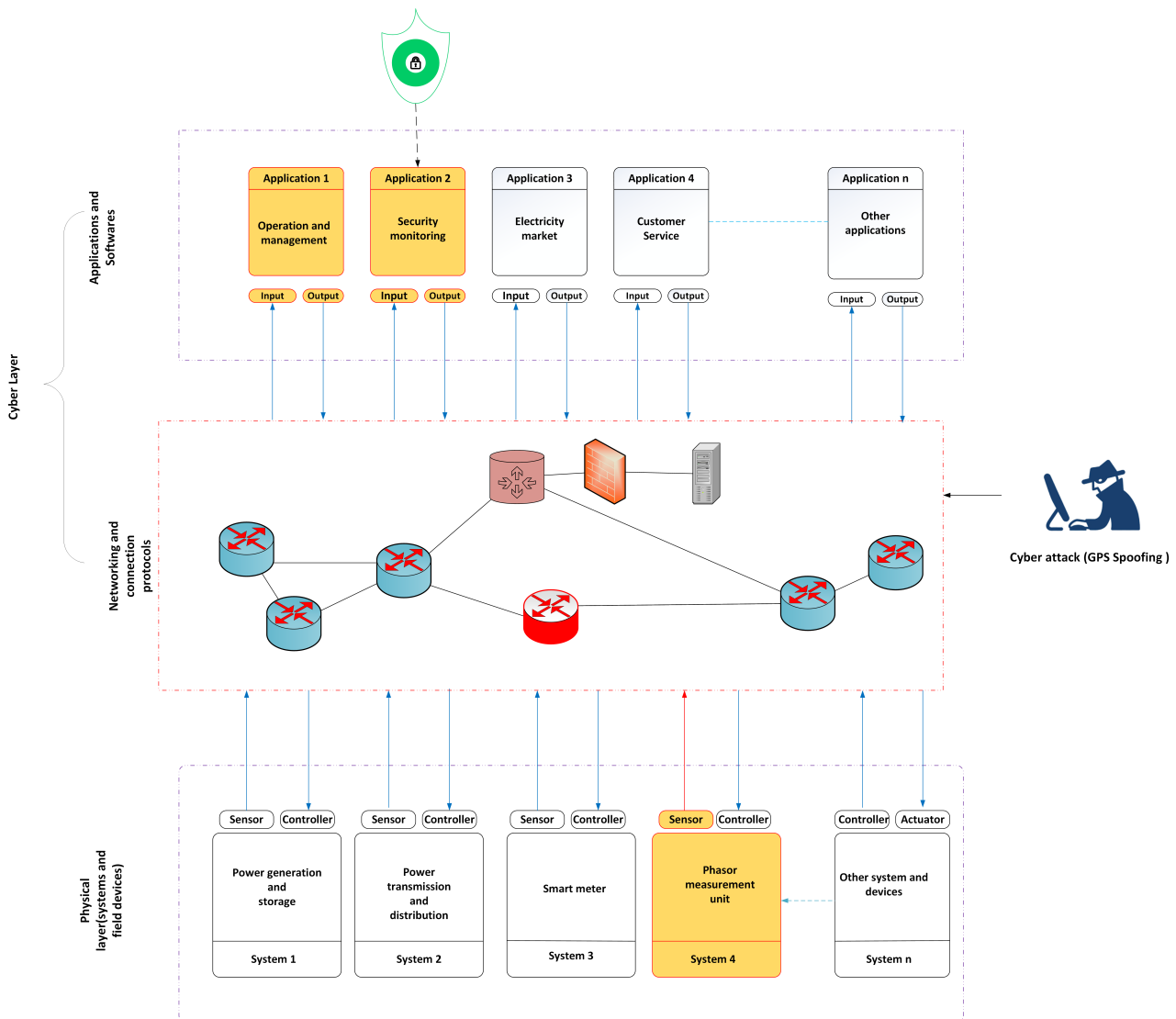


Figure 5. General illustration of GPS spoofing attack in smart grids.

The authors in [64] aimed to secure the phasor measurement unit model combined with the dynamic network model against spoofing attacks in the power grid. These models are appropriate for receiving GPS measurements in the state estimation. The performance of this dynamic network model is better as compared to the static model. In [65], a neural network method named neural network GPS spoofing detection (NNGSD) is proposed to diagnose the spoofing attack and its location by operating phasor measurement unit data with the help of a dynamic power system. This method has been experimented in different conditions and the results show the promising real-time performance.

The authors in [66] proposed a strategy against GPS spoofing attacks while considering its dynamic nature in the power grid. They used dynamic monitoring mechanism to observe the measurements using a state-space model combined with the data of SCADA and PMU. The developed anti-GPS spoofing attack mechanism detects these attacks and measurement corrections using a dynamic model of the smart grid system. Table 4 presents the summary of detection methods developed for spoofing attacks detection in the smart grid system. The targeted devices and contributions are also summarized in it.

Table 4. Review of spoofing attacks detection in smart grid systems.

Ref.	Victim Device	Type of Attack	Solution Method	Description
[63]	Phasor measurement unit	GPS spoofing time stamp attack	multi-antenna based quickest detection	The probabilistic metric is used which takes information of the carrier signal to noise ratio from two receive antennas to conduct the quickest GPS spoofing detection.
[64]	Phasor measurement unit	GPS spoofing attack	Weighted lest square state estimation	The detection method estimates the state variables such as nodal voltages in rectangular coordinates, generator rotor angles and its rotor speed, as well as the time-varying attacks.
[65]	Phasor measurement unit	GPS spoofing phase angle attack	multilayer perceptron neural network	The proposed neural network detection method is able to diagnose the GPS spoofing attacks and determine their location as well. The learning process of neural network is executed only once.
[66]	Phasor measurement unit	GPS spoofing time attack	Kalman filter-based dynamic fusion estimator	The proposed method uses a state-space model combined with the data of SCADA and PMU under dynamic system conditions. Proposed detection approach can detect multi-GPS spoofing attacks.

3. Research Directions

Many researchers have proposed methods for the detection of FDIA, DoS, and spoofing attacks on smart grid systems. There are also works reported in the literature for the study of the impact of these attacks. However, most of these studies are focused on individual components of the smart grid systems. This entails further research on smart grid systems that focuses on the protection of a whole smart grid.

To achieve an enhanced and improved the impact analysis of FDIA, further research work is required on the distribution system other than the transmission system. Time duration of an attack could have an impact on smart grid failure due to a cyberattack; therefore, it is important to analyze the detection duration and impact of the cyberattack on the power system in that duration.

Optimization of the network topology should also be performed while considering 5G technology in sensors, smart meters, local controllers, state estimators, and other advanced metering infrastructure. Moreover, there is also need to analyze the impact of cyberattacks on voltage ride-through of the inverter in the smart grid. Encryption methods can also be introduced for secure data transmission to enhance the defense against these malicious attacks. Moreover, potential deep federated learning should also be explored for securing smart grid systems against cyberattacks. Cost estimation of cyberattacks on smart grid for the protection of infrastructure is an essential research area. It can help in prioritizing the parts of a smart grid for security.

As real data collection is still challenging, hence it will be beneficial to simulate cyberattacks to collect key characteristics that resemble real ones using virtual reality (VR). VR may potentially offer a potential solution by including reinforcement learning. Additionally, artificial intelligence experts will be able to predict the kind of attacks, which resembles real cybersecurity problems in smart grid system.

Transfer learning can also be explored to transfer data from models learned real datasets to simulation models or vice versa. GANs also need to be explored to extract novel instances from data obtained using different components of the smart grid. Lowering computational costs and convergence of different defense mechanisms need to be studied to have a better realization of their real-world implementations.

Privacy protection of data using the confidentiality, integrity, and availability triad in a form of decentralized/centralized learning is the key topic to be covered in the cybersecurity of smart grid systems. Privacy is a crucial issue that has not been addressed keeping the artificial intelligence model itself intact. Future research needs decentralized federated learning to be taken into account to protect the attack modeling procedure and add more security measures.

4. Conclusions

Smart grid, a cyber–physical power system, can be adversely affected by various cyberattacks due to digital evolution. This paper provided a comprehensive review on the detection of most occurring cyberattacks including false data injection attacks, denial of service, distributed denial of service, and GPS spoofing attacks in the smart grids. It also provided an analysis of the impact these attacks can have on a smart grid. The false data injection attack is a type of cyberattack that targets the supervisory control and data acquisition systems, state estimators, monitoring meters, and sensors. In contrast, the DoS and DDoS attacks target smart meters, sensors, local controllers, state estimator, and advanced metering infrastructure. The security of these targeted devices must be strengthened to limit the occurrence of cyberattacks. Different defense mechanisms, both artificial intelligence and traditional solution methods, are also highlighted to provide insight into enhancing the security of smart grid systems; however, there is still a need to explore more defensive strategies against such types of cyberattacks. Digital twin models and data-driven methods such as machine and deep learning should be explored for both analyzing different types of attacks and mitigating the impact of these attacks in smart grid systems; therefore, future recommendations are also highlighted for the improvement and more secure operations of the smart grid system against cyberattacks.

Author Contributions: Conceptualization, U.I., M.F.Z. and M.B.; methodology, U.I. and M.F.Z.; formal analysis, U.I., M.F.Z., S.M. and T.B.; investigation, U.I., M.F.Z. and S.M.; resources, U.I. and M.F.Z.; data curation, U.I. and M.F.Z.; writing—original draft preparation, U.I. and M.F.Z.; writing—review and editing, U.I., M.F.Z., S.M., T.B. and M.B.; supervision, M.F.Z., S.M., T.B. and M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All data are available in the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ICTs	Information and communication technologies
FDIA	False data injection attack
DoS	Denial of service
IEDs	Intelligent electronic devices
GPS	Global positioning system
DDoS	Distributed denial of service
CPPS	Cyber physical power system
DLLD	Deep learning-based location detection
CNN	Convolutional neural network
DLAA	Dynamic load altering attack
VMD	Variational mode decomposition
LSTM	Long short term memory
CUSUM	Cumulative sum
GAN	Generative adversarial network
CRC	Cognitive risk control
ICMP	Internet control message protocol
GNSS	Global navigation satellite system
SCADA	Supervisory control and data acquisition
PMU	Phasor measurement unit
NNGSD	Neural network GPS spoofing detection

References

1. Wang, H.; Qian, Y.; Sharif, H. Multimedia communications over cognitive radio networks for smart grid applications. *IEEE Wirel. Commun.* **2013**, *20*, 125–132. [[CrossRef](#)]
2. Kabalci, E.; Kabalci, Y. *Smart Grids and Their Communication Systems*; Springer: Singapore, 2019.
3. Merabti, M.; Kennedy, M.; Hurst, W. Critical infrastructure protection: A 21 st century challenge. In Proceedings of the 2011 International Conference on Communications and Information Technology (ICIT), Amsterdam, The Netherlands, 13–15 July 2011; pp. 1–6.
4. Amin, S.M. Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems. In Proceedings of the IEEE PES General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–5.
5. Annaswamy, A.M.; Amin, M. *Smart Grid Research: Control Systems-IEEE Vision for Smart Grid Controls: 2030 and Beyond*; IEEE: New York, NY, USA, 2013.
6. Ali, M.; Zia, M.F.; Sundhu, M.W. Demand side management proposed algorithm for cost and peak load optimization. In Proceedings of the 2016 4th International Istanbul Smart Grid Congress and Fair (ICSG), Istanbul, Turkey, 20–21 April 2016; pp. 1–5.
7. Ruester, S.; Schwenen, S.; Batlle, C.; Pérez-Arriaga, I. From distribution networks to smart distribution systems: Rethinking the regulation of European electricity DSOs. *Util. Policy* **2014**, *31*, 229–237. [[CrossRef](#)]
8. Zafar, A.; Shafique, A.; Nazir, Z.; Zia, M.F. A comparison of optimization techniques for energy scheduling of hybrid power generation system. In Proceedings of the IEEE 21st International Multi-Topic Conference (INMIC), Karachi, Pakistan, 1–2 November 2018; pp. 1–6.
9. Kuzlu, M.; Pipattanasomporn, M. Assessment of communication technologies and network requirements for different smart grid applications. In Proceedings of the 2013 IEEE PES innovative smart grid technologies conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
10. Gharavi, H.; Chen, H.H.; Wietfeld, C. Guest editorial special section on cyber-physical systems and security for smart grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2405–2408. [[CrossRef](#)]
11. Metke, A.R.; Ekl, R.L. Smart grid security technology. In Proceedings of the 2010 Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–7.
12. Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid, H.M.; Benbouzid, M. Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. *Electronics* **2022**, *11*, 1502. [[CrossRef](#)]
13. Chen, P.Y.; Cheng, S.M.; Chen, K.C. Smart attacks in smart grid communication networks. *IEEE Commun. Mag.* **2012**, *50*, 24–29. [[CrossRef](#)]
14. Inayat, U.; Zia, M.F.; Ali, F.; Ali, S.M.; Khan, H.M.A.; Noor, W. Comprehensive Review of Malware Detection Techniques. In Proceedings of the 2021 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 9–10 November 2021; pp. 1–6.
15. Nguyen, T.N.; Liu, B.H.; Nguyen, N.P.; Chou, J.T. Cyber security of smart grid: attacks and defenses. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
16. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [[CrossRef](#)]
17. Aloul, F.; Al-Ali, A.; Al-Dalky, R.; Al-Mardini, M.; El-Hajj, W. Smart grid security: Threats, vulnerabilities and solutions. *Int. J. Smart Grid Clean Energy* **2012**, *1*, 1–6. [[CrossRef](#)]
18. Berghout, T.; Benbouzid, M.; Muyeen, S. Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100547. [[CrossRef](#)]
19. Wei, D.; Lu, Y.; Jafari, M.; Skare, P.M.; Rohde, K. Protecting smart grid automation systems against cyberattacks. *IEEE Trans. Smart Grid* **2011**, *2*, 782–795. [[CrossRef](#)]
20. Wei, D.; Lu, Y.; Jafari, M.; Skare, P.; Rohde, K. An integrated security system of protecting smart grid against cyber attacks. In Proceedings of the 2010 Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–7.
21. Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
22. Wang, X.; Yi, P. Security framework for wireless communications in smart distribution grid. *IEEE Trans. Smart Grid* **2011**, *2*, 809–818. [[CrossRef](#)]
23. Aravinthan, V.; Namboodiri, V.; Sunku, S.; Jewell, W. Wireless AMI application and security for controlled home area networks. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–8.
24. Mo, Y.; Kim, T.H.J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber-physical security of a smart grid infrastructure. *Proc. IEEE* **2011**, *100*, 195–209.
25. Moreno Escobar, J.J.; Morales Matamoros, O.; Tejeida Padilla, R.; Lina Reyes, I.; Quintana Espinosa, H. A comprehensive review on smart grids: Challenges and opportunities. *Sensors* **2021**, *21*, 6978. [[CrossRef](#)]
26. Salkuti, S.R. Emerging and Advanced Green Energy Technologies for Sustainable and Resilient Future Grid. *Energies* **2022**, *15*, 6667. [[CrossRef](#)]
27. Elbouchikhi, E.; Zia, M.F.; Benbouzid, M.; El Hani, S. Overview of signal processing and machine learning for smart grid condition monitoring. *Electronics* **2021**, *10*, 2725. [[CrossRef](#)]

28. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [[CrossRef](#)]
29. Shi, L.; Dai, Q.; Ni, Y. Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electr. Power Syst. Res.* **2018**, *163*, 396–412. [[CrossRef](#)]
30. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2011**, *100*, 210–224. [[CrossRef](#)]
31. Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J. Netw. Comput. Appl.* **2020**, *170*, 102808. [[CrossRef](#)]
32. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. [[CrossRef](#)]
33. Wang, S.; Bi, S.; Zhang, Y.J.A. Locational Detection of the False Data Injection Attack in a Smart Grid: A Multilabel Classification Approach. *IEEE Internet Things J.* **2020**, *7*, 8218–8227. [[CrossRef](#)]
34. Zhao, J.; Zhang, G.; La Scala, M.; Dong, Z.Y.; Chen, C.; Wang, J. Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks. *IEEE Trans. Smart Grid* **2017**, *8*, 1580–1590. [[CrossRef](#)]
35. Li, J.; Yang, D.F.; Gao, Y.C.; Huang, X. An adaptive sliding-mode resilient control strategy in smart grid under mixed attacks. *IET Control. Theory Appl.* **2021**, *15*, 1971–1986. [[CrossRef](#)]
36. Nath, S.; Akingeneye, I.; Wu, J.; Han, Z. Quickest detection of false data injection attacks in smart grid with dynamic models. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**, *10*, 1292–1302. [[CrossRef](#)]
37. Dou, C.; Wu, D.; Yue, D.; Jin, B.; Xu, S. A hybrid method for false data injection attack detection in smart grid based on variational mode decomposition and OS-ELM. *CSEE J. Power Energy Syst.* **2020**. [[CrossRef](#)]
38. Hu, Z.; Wang, Y.; Tian, X.; Yang, X.; Meng, D.; Fan, R. False data injection attacks identification for smart grids. In Proceedings of the 2015 Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAECE), Beirut, Lebanon, 29 April–1 May 2015; pp. 139–143.
39. Yang, L.; Zhang, X.; Li, Z.; Li, Z.; He, Y. Detecting bi-level false data injection attack based on time series analysis method in smart grid. *Comput. Secur.* **2020**, *96*, 101899. [[CrossRef](#)]
40. Li, S.; Yilmaz, Y.; Wang, X. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Trans. Smart Grid* **2014**, *6*, 2725–2735. [[CrossRef](#)]
41. Jiang, Q.; Chen, H.; Xie, L.; Wang, K. Real-time detection of false data injection attack using residual prewhitening in smart grid network. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 83–88.
42. Liu, T.; Zhang, Y.; Zhao, H.; Liu, X.; Gao, T.; Yuan, H.; Zhang, J. Social Implications of Cyber-Physical Systems in Electrical Load Forecasting. In Proceedings of the 2020 IEEE 16th International Conference on Automation Science and Engineering (CASE), Hong Kong, China, 20–21 August 2020; pp. 582–587.
43. Ye, H.; Liu, K.; Mou, Q.; Liu, Y. Modeling and formulation of delayed cyber-physical power system for small-signal stability analysis and control. *IEEE Trans. Power Syst.* **2019**, *34*, 2419–2432. [[CrossRef](#)]
44. Wu, G.; Wang, G.; Sun, J.; Chen, J. Optimal partial feedback attacks in cyber-physical power systems. *IEEE Trans. Autom. Control* **2020**, *65*, 3919–3926. [[CrossRef](#)]
45. Wang, L.; Qu, Z.; Li, Y.; Hu, K.; Sun, J.; Xue, K.; Cui, M. Method for extracting patterns of coordinated network attacks on electric power CPS based on temporal–topological correlation. *IEEE Access* **2020**, *8*, 57260–57272. [[CrossRef](#)]
46. Li, Y.; Wang, Y.; Hu, S. Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach. *IEEE Trans. Ind. Inform.* **2019**, *16*, 2031–2043. [[CrossRef](#)]
47. Oozeer, M.I.; Haykin, S. Cognitive risk control for mitigating cyber-attack in smart grid. *IEEE Access* **2019**, *7*, 125806–125826. [[CrossRef](#)]
48. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Shen, X.; Nozaki, Y. An early warning system against malicious activities for smart grid communications. *IEEE Netw.* **2011**, *25*, 50–55. [[CrossRef](#)]
49. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [[CrossRef](#)]
50. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 39–53. [[CrossRef](#)]
51. Demir, K.; Ismail, H.; Vateva-Gurova, T.; Suri, N. Securing the cloud-assisted smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *23*, 100–111. [[CrossRef](#)]
52. Wang, K.; Du, M.; Maharjan, S.; Sun, Y. Strategic honeypot game model for distributed denial of service attacks in the smart grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2474–2482. [[CrossRef](#)]
53. Srikantha, P.; Kundur, D. Denial of service attacks and mitigation for stability in cyber-enabled power grid. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2015; pp. 1–5.
54. Liu, H.; Chen, Y.; Chuah, M.C.; Yang, J.; Poor, H.V. Enabling self-healing smart grid through jamming resilient local controller switching. *IEEE Trans. Dependable Secur. Comput.* **2015**, *14*, 377–391. [[CrossRef](#)]
55. Yilmaz, Y.; Uludag, S. Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *J. Frankl. Inst.* **2019**, *358*, 172–192. [[CrossRef](#)]

56. Farraj, A.; Hammad, E.; Kundur, D. A cyber-physical control framework for transient stability in smart grids. *IEEE Trans. Smart Grid* **2016**, *9*, 1205–1215. [[CrossRef](#)]
57. Jahromi, A.A.; Kemmeugne, A.; Kundur, D.; Haddadi, A. Cyber-physical attacks targeting communication-assisted protection schemes. *IEEE Trans. Power Syst.* **2019**, *35*, 440–450. [[CrossRef](#)]
58. Demir, K.; Suri, N. SeReCP: A secure and reliable communication platform for the smart grid. In Proceedings of the 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), Christchurch, New Zealand, 22–25 January 2017; pp. 175–184.
59. Song, M.; Xin, C.; Zhao, Y.; Cheng, X. Dynamic spectrum access: from cognitive radio to network radio. *IEEE Wirel. Commun.* **2012**, *19*, 23–29. [[CrossRef](#)]
60. Peng, Q.; Cosman, P.C.; Milstein, L.B. Tradeoff between spoofing and jamming a cognitive radio. In Proceedings of the 2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, USA, 1–4 November 2009; pp. 25–29.
61. Meng, Q.; Hsu, L.T.; Xu, B.; Luo, X.; El-Mowafy, A. A GPS spoofing generator using an open sourced vector tracking-based receiver. *Sensors* **2019**, *19*, 3993. [[CrossRef](#)]
62. Wei, X.; Aman, M.N.; Sikdar, B. Exploiting correlation among GPS signals to detect GPS spoofing in Power Grids. *IEEE Trans. Ind. Appl.* **2021**, *58*, 697–708. [[CrossRef](#)]
63. Gong, S.; Zhang, Z.; Trinkle, M.; Dimitrovski, A.D.; Li, H. GPS spoofing based time stamp attack on real time wide area monitoring in smart grid. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 300–305.
64. Risbud, P.; Gatsis, N.; Taha, A. Multi-period power system state estimation with PMUs under GPS spoofing attacks. *J. Mod. Power Syst. Clean Energy* **2020**, *8*, 597–606. [[CrossRef](#)]
65. Sabouri, M.; Siamak, S.; Dehghani, M.; Mohammadi, M.; Asemiani, M.H. Intelligent GPS spoofing attack detection in power grids. *arXiv* **2020**, arXiv:2005.04513.
66. Siamak, S.; Dehghani, M.; Mohammadi, M. Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA. *IEEE Syst. J.* **2020**, *15*, 2531–2540. [[CrossRef](#)]