energies

MDPI

Review

Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation

Derya Betul Unsal [1,*], Taha Selim Ustun [2], S. M. Suhail Hussain [2] and Ahmet Onen [3]

[1] Department of Energy Science and Technology, Renewable Energy Research Center, Cumhuriyet University, Sivas 58140, Turkey
[2] Fukushima Renewable Energy Institute, AIST (FREA), Koriyama 963-0298, Japan; selim.ustun@aist.go.jp (T.S.U.); suhail@ieee.org (S.M.S.H.)
[3] Department of Electrical and Electronics Engineering, Abdullah Gul University, Kayseri 38170, Turkey; ahmet.onen@agu.edu.tr
* Correspondence: dbunsal@cumhuriyet.edu.tr; Tel.: +90-(346)-219-1153

Abstract: Integration of information technologies with power systems has unlocked unprecedented opportunities in optimization and control fields. Increased data collection and monitoring enable control systems to have a better understanding of the pseudo-real-time condition of power systems. In this fashion, more accurate and effective decisions can be made. This is the key towards mitigating negative impacts of novel technologies such as renewables and electric vehicles and increasing their share in the overall generation portfolio. However, such extensive information exchange has created cybersecurity vulnerabilities in power systems that were not encountered before. It is imperative that these vulnerabilities are understood well, and proper mitigation techniques are implemented. This paper presents an extensive study of cybersecurity concerns in Smart grids in line with latest developments. Relevant standardization and mitigation efforts are discussed in detail and then the classification of different cyber-attacks in smart grid domain with special focus on false data injection (FDI) attack, due to its high impact on different operations. Different uses of this attack as well as developed detection models and methods are analysed. Finally, impacts on smart grid operation and current challenges are presented for future research directions.

Keywords: smart grid cybersecurity; false data injection; power system operation; power system protection; cybersecurity attacks; intruder detection; cybersecurity for scada systems

Citation: Unsal, D.B.; Ustun, T.S.; Hussain, S.M.S.; Onen, A. Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. *Energies* **2021**, *14*, 2657. https://doi.org/10.3390/en14092657

Academic Editor: Seon-Ju Ahn

Received: 12 April 2021
Accepted: 28 April 2021
Published: 6 May 2021

1. Introduction

The traditional electricity grid system of the 20th century is insufficient to meet today's needs. Novel technologies such as Electric Vehicles (EVs), smart inverters and renewable energy-based generators are continually being deployed [1]. They change power system operation paradigms, introduce bi-lateral power flow and create a dynamic operation structure which was not originally envisioned [2]. To tackle these issues, power systems are equipped with more measurement, communication, and control capabilities. More accurate information about the grid's current state can be obtained in this fashion, and a decision can be made in pseudo-real time [3]. This modern power system structure is collectively called the Smart Grid (SG). There are many definitions of SG concept, such as "A network where all consumers can reach efficient, cheap, accessible, and reliable energy by using control and communication technologies" [4]. Alternatively, SG is a system that is adaptive, reliable, interactive and allows for renewable energy sources integration and optimization [5,6]. In addition to these definitions, the National Institute of Standards and Technology (NIST) gives a high-level perspective and classifies SGs. Moreover, application characteristics and requirements of SG infrastructure are divided into different layers [7]:

- Application;
- Security;

- Communication;
- Control of Power;
- Power system.

As shown in Figure 1, SGs are divided into generation, transmission, distribution, service providers, and consumers. According to fields of study, control of power and communication technologies should solve possible problems encountered in the SG [7]. The working principles of all power electronics elements integrated into the network should be well analysed to achieve effective SG system [8]. Stable and efficient transmission of energy to the end customer is crucial for a reliable network implementation. If it is made, energy efficiency and local renewable energy usage will increase, and the ideal grid system will be realised by reducing the transmission losses [9].

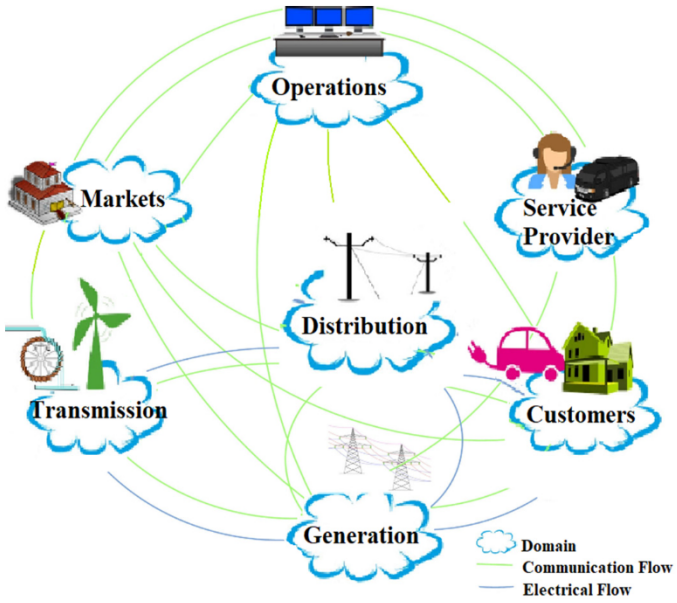


Figure 1. NIST SG Model.

Considering the vast geographical span of SGs and the number of devices they host, it is inevitable that the cybersecurity vulnerabilities become more prevalent than the other. Furthermore, the consequences of security breaches in such critical infrastructure will have significant ramifications, as all organizations with energy-providing authorities agree [10]. According to [11], SG can be considered an electrical system that uses cyber secure information and communication technologies. The system works to obtain a safe, reliable, and efficient computational intelligence system integrated with electricity transmission, generation, and distribution substations. It is possible to classify cybersecurity into three systems, as shown below in Figure 2: Smart energy, information, and communication systems listed under smart infrastructure system. They must work simultaneously with the smart management system and support its protection system [12]. Existing cybersecurity solutions have difficulties in meeting the needs of SG communication systems. When recent research is examined, it can be understood that traditional cybersecurity methods and algorithms have usually studied, and there are separate studies on power and communication regarding cyber risks. If critical systems such as the power system communication infrastructure have cybersecurity risks, that can have severe consequences and traditional risks are now included in risk assessments. However, SG communication systems security is a relatively new topic; few academic and experimental studies have been found [13].

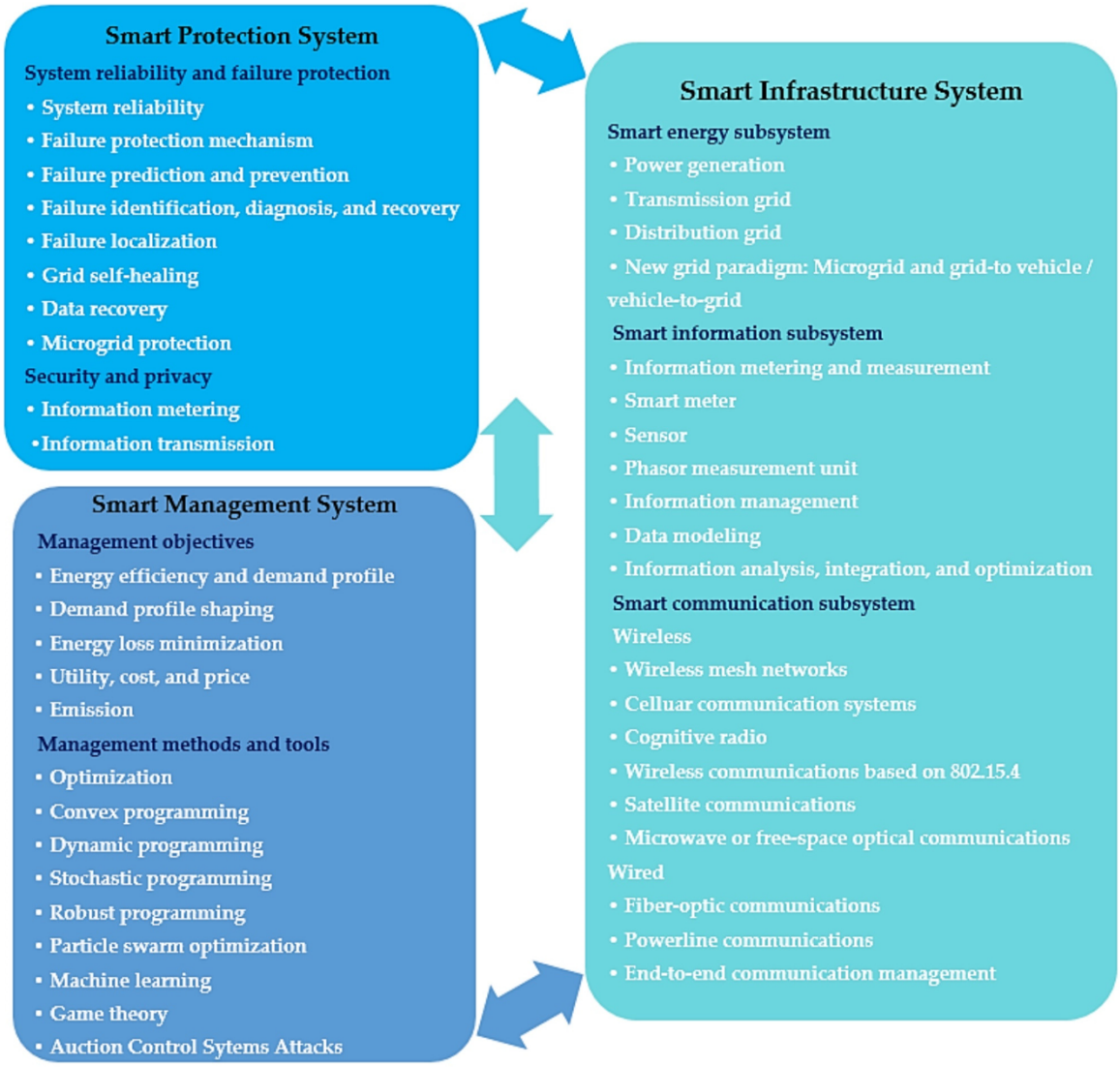


Figure 2. SG Cyber-Security System Structure and Relationship Diagrams.

A general assessment of the vulnerabilities can split into five categories:

- Interaction control framework security;
- Smart meter measurement security;
- Assessment of power system status security;
- Intelligent network communication convention security;
- Security analysis with SG simulation.

Cybersecurity in SGs is an emerging field [14]. Therefore, they need cybersecurity protection studies for each security component because traditional techniques are applied for the first time. Because the SG system is a cyber-physical and communication system, the power is also exchanged [15]. A thorough review that studies components of the SG system security is required. Several reviews focus only on bad data detection and state estimation attacks [16,17]. Moreover, both attacks' effects may be different, and all processes should terminate within a certain period. The aims and objectives of the research focus on this point. This paper presents a comprehensive review of security concerns in different system parts of smart grids, different types of attacks, standards, and available mitigation techniques to fill this gap. Due to its enormous impact, False Data Injection (FDI) attack and detection methods are discussed in detail. The rest of the paper is organized as follows: Section 2 introduces the cybersecurity concerns in SGs and discusses the mitigation requirements.

Section 3 reviews different types of cyber-attacks and discusses the impacts of attacks on SG. Section 4 introduces false data detection methods and proposed efficiency analysis, and Section 5 concludes the paper. See Appendix A for abbreviations and meanings. Main contributions of this survey paper are as follows:

- A thorough discussion on changing paradigms in power systems is presented. Different levels of communication and information exchange are discussed so that readers can grasp why smart grid cybersecurity became important in recent times.
- Different communication standards used in power system communication are studied. Issues that are unique to each standard and the protocols it uses are presented. Benefits and drawbacks of using single or multiple standards in a system are presented.
- A thorough review of SG attacks is performed so that readers can understand the types of attacks and their impacts on the system. Among these attacks, FDI attacks have significant potential to disrupt power system operation or cause damages. For this reason, a survey is performed on techniques developed to detect FDI attacks.
- Based on the discussions and insights of this work, future research directions are provided.

2. Cybersecurity Vulnerabilities in Smart Grids and Mitigation Requirements

Secure and safe operation of SG is critical for ensuring its effective operation [18]. Cybersecurity for the SG promotes both the grid's reliability and the stability of the information transmitted [19]. SG automatically modifies electrical power and communication systems to optimize their operation. For example, SG is defined as "The transition from today's power systems to future systems based on information, transmission and communication technologies" and it monitors all components to prevent its attacks because cybersecurity holds a special place in it [19]. The vital information can be understood in a way that all the security risks in the system can be protected with measures. In this context, it will be useful to examine some studies to understand mitigation requirements. Cybersecurity challenges and existing solutions within the SG environment are reviewed in [13] and [20]. This is classified as the SG communication security studies into software and hardware simulations [21–23]. Risk definition within the scope of information security can express the loss of integrity, privacy, or continuity in the data by using vulnerabilities in information data by malicious threats [24]. The security aspects, especially the Internet of Things (IoT) and the types of cyber threats facing the SG, are examined in [25], and the environmental conditions related to cybersecurity of the SG are split into three categories:

- Power grid vulnerabilities at the time of the cyber-attack;
- The facilitate of infraction to the control system;
- Describe the ease of earning control over the management system.

Cyber-attacks are dissociated into three steps: First step is the attacker has in mind to control the management and communication system. Once the management access is acquired, the attacker should identify the system to initiate a smart and effective malicious attack. In the third step, the attacker launches the control of SG component or tries to influence its operation. These attacks may be directed at power systems equipment [26] or auxiliary systems such as Advanced Metering Infrastructures (AMI) [27,28]. Security vulnerabilities in power and communication protocols can cause dangerous attacks on the SG system. When the content of the applied standards is examined to prevent this, it can be seen that they are based on authentication, encryption, and confidentiality technologies to ensure SG security. Malicious people may be interested in launching large-scale attacks on the smart grid with potentially unpredictable consequences. In light of these concerns, security is one of the most important issues in the SG's current development and future deployment [14,29]. Figure 3 illustrates the importance of cyber security in SGs.

Figure 3. Illustration of cyber security in smart grids.

2.1. Cyber Security Requirements in SGs

The term "Cyber-Physical systems" (CPS) relates to the currently prevalent terms Industry 4.0, Internet of Things (IoT), Machine-to-Machine (M2M), the Internet of Everything, TSensors (Trillion Sensors), and the Fog. These reflect a view of a technology that profoundly engages the physical world with the information world [30].

Cyber means computed, communicated, and controlled but discrete, logical, and switched. On the other hand, physical means that systems are bound by physics laws and operating continuously. Cyber-Physical (CP) means the systems in which the cyber and physical systems are closely integrated at all environmental conditions and levels.

Therefore, SG is a typical CP System which integrates a physical energy transmission and distribution system with the cyber process of communication and control [31]. As SGs grow, millions of smart assets with two-way communication ability will be integrated. This situation causes new security problems in a large geographical area [32]. More complex system security can be obtained using real-time communication standards to modify the control system between generation, transmission, distribution, and consumers in the network structure [33].

In electrical infrastructures, various organizations have established some security standards to regulate issues such as the system's proper operation, protection of information and against attacks. Various standards are established by the organizations working within the scope of cybersecurity in SGs. Some of the organizations that constitute these standards can be listed as follows.

International Society of Automation (ISA) [34], National Infrastructure Protection Plan (NIPP/CISA) within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, being a shareholder with the National Institute for Hometown Security (NIHS) [35], National Institute of Standards and Technology (NIST) [36], Institute of Electrical and Electronics Engineers (IEEE), Computer Security Division (CSD), Com-

puter Security Resource Center (CSRC), Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Federal Energy Regulatory Commission (FERC), and The North American Electric Reliability Corporation (NERC) [37].

In addition to these organizations, ISO 17,799 (27,000 series) security standard is fundamental in establishing more secure, consistent, and scalable systems [38].

In this study, security standards are researched about all the SG parts, which is shown in Figure 4, and divided into three sections and then examined detail in the following section:

- Examining the firewalls of communication systems and the vulnerabilities in the protocols;
- Based on attacks on energy transmission and distribution systems;
- Applied for remote control security of the devices connected to the system.

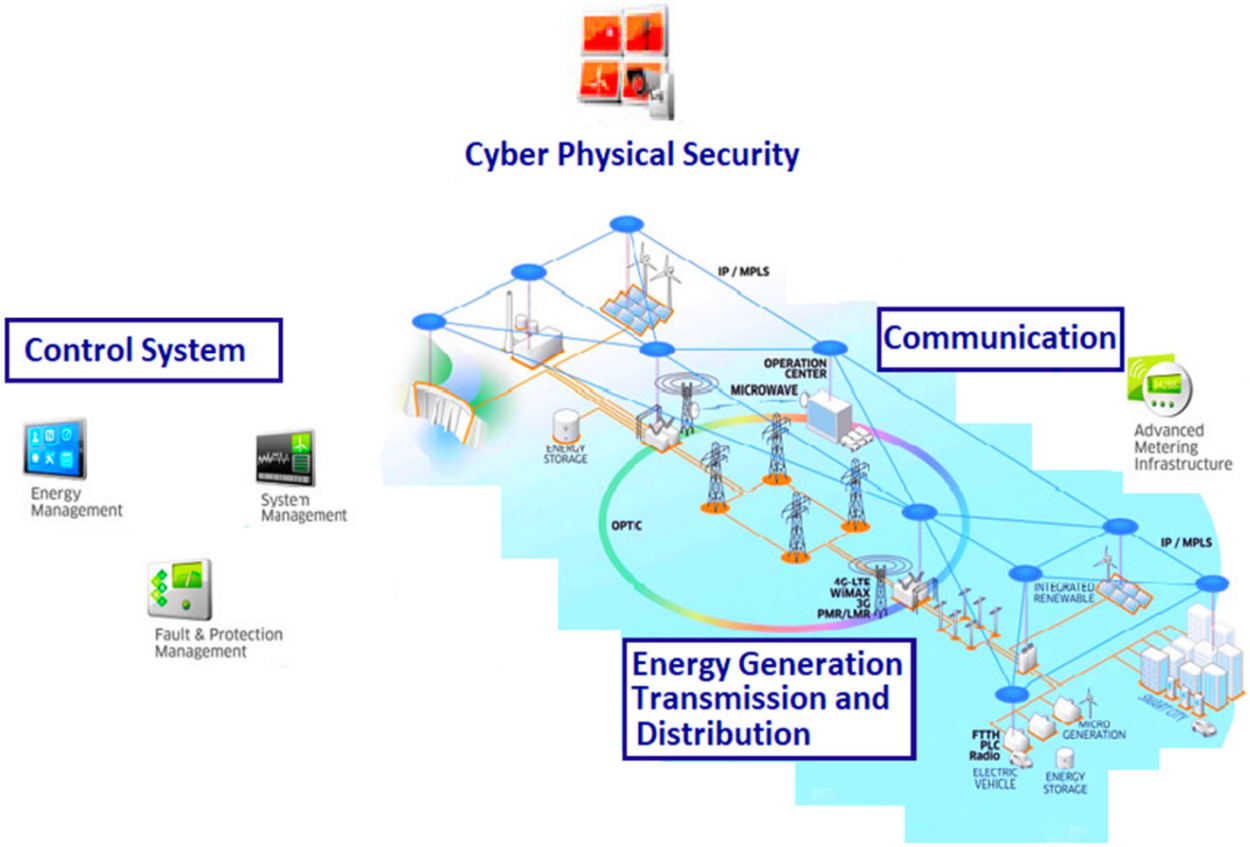


Figure 4. Smart Grid subsystems.

2.2. Security Standards of Communication Systems Mitigation

Substation communication of SG plays a critical role in intelligent power energy system management. Therefore, communication security and related causes are crucial to power system security and should be carefully studied. Communication problems concerning information can be classified into five general categories for their objectives, availability, integrity, confidentiality, authenticity, and non-repudiation [6]. SG systems have too many interconnected devices. It is also highly susceptible to cyber-attacks due to security vulnerabilities found in devices connected to the network. The defence and security layers of SG protect the network against cyber-attacks, unwanted changes, and data theft. For reasons such as efficiency, cost, and integration to big data, SGs depend on comprehensive internet networks where common information is shared. Due to the internet networks to which SGs are connected, they are vulnerable to many attacks that cause interruption of power supplies [39,40]. This increase in security attacks has created a more demanding control requirement to ensure a smooth SG communication system. Therefore, it is exposed to the general problems and threats of internet networks.

As power systems become more secure and complex, SGs also need more connections to highly external networks, especially the internet. However, this commitment to the said external networks causes cybersecurity vulnerabilities and violations [41–44]. Therefore, all communication links in SG networks must have access to high security. When choosing encryption technologies and standards, the criticality and risks of the communication system that needs to be protected should be evaluated.

- The ISO 27,001 standard is vital in providing communication security. It defines the functions that must be performed within the scope of living information security. Information security management system (ISMS) standard defines the organizations' needs to establish an ISMS. ISO/IEC 27,001 consists of twelve parts. These are risk operation, security of human resources, security policy, physical security, environmental security, communication and operation management, asset management, entry control, development and reparation, information security management, acquisition and business permanence management submission [33].
- The NIST standard started with the priorities determined by for SGs and added the subjects it determined. The eight priorities identified are: Meeting the demands and consumer energy adequacy, Large area application awareness, Energy storage, Electricity transport, Advanced measurement infrastructure, Distribution network management, Cybersecurity, and Network communication [41,42].
- The FERC SSEMP standard sets the standards that must be followed in communication networks connected to power systems [42].
- The Common Criteria (CC) that can be evaluated among the standards is internationally accepted SC evaluation criteria for information technology products. They were created as a result of the merger of The Information Technology Security Evaluation Criteria (ITSEC) in Europe, Trusted Computing Security Evaluation Criteria (TCSEC) in the USA, and Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [44] in Canada, which are accepted as information security evaluation criteria. CC are defined in the ISO/IEC 15,408 standard. It also defines the Evaluation Assurance Level (EAL) levels [44,45].
- AGA Report No. 12 Part 3 includes protection of SCADA Communications Networked Systems. It is focused on high-speed communication systems, including the Internet [44,45]. It is notable that AGA series are voluntary standards and do not mandate any companies to install encryption technology as recommended in the standards.
- Virtual Private Networks (VPNs) and Internet Protocol Security (IPSec) technologies provide the security of wired grids. A VPN system can make on top of existing CP networks, providing a safe communications contraption for message and information transmitted among two addresses. The data exchange in the middle of the web browser and the VPN device is encrypted with the Secure Sockets Layer (SSL), Transport Layer Security (TLS), SSL/TLS [46] or Secure Shell (SSH), which are high layer security mechanisms, can also be used [46,47].
- ISO/IEC 62,351 standard covers communication security issues for energy systems management and information sharing. It deals with communication protocols and network and operating systems [48]. IEC Standards provide communication and information security, security for profiles containing TCP/IP, Quality of service (QoS), mobility, multi-homing, and other enhancements essential for SG applications to be efficiently secured and well-controlled if TCP/IP is to be adopted [36].
- IEC S63 report generally includes status and advisory standards for smart grid cybersecurity requirements. It covers industrial security standards, access controls, identity management, secure network, wired and wireless connection standards [48].
- Security for profiles with Manufacturing Messaging Specifications (MMS) [49], Security for IEC 60870-5, and its derivatives (DNP) [50] Security for IEC 61,850 profiles, Elements (targets) to grid security can be counted [43].

- The level of security provided by the different degrees of wireless communication protocols is also varied. IEEE 802.11i [50] and IEEE 802.16e [51] standards can be used to safety wireless grids.
- IEC 61,850 structure provides digital fast communication and use Internet Protocol (IP) based addresses [52].
- Federal Information Processing Standard (FIPS) certifies the Advanced Encryption Standard (AES) [53].
- Triple Data Encryption Standard (3DES) [54] for robust security and high performance.

SG communication system has an architecture in which data collection and control can be performed [13]. Distributed control centre (DCC) supports metering and metering systems, power system stability, data management, power system activities, and data exchange control. Transformer centre includes Remote Management Units (RTU) and fuses, Human Machine Interfaces (HMI), Control and communication assets (equipment of switchers or routers), log servers, data collectors, and protocol gateways. Intelligent Electronic Devices (IED) are field equipment which includes a set of converter tools, tap changers, circuit terminators, phase measuring units (PMUs), and protection relays. It is defined in the IEC 61,850, when data transmitted with the IED contains the MAC (Media access control) address. When this address determines which device or equipment will receive this message, they allow data transmission with DCS securely. Accessibility means that data can be used to open, close, hold, and allow the system; they work in compliance with communication protocols. Therefore, this authentication allows authorization.

The purpose of security in the SG is to protect the user's integrity [6]. The advanced smart grid system should prevent sensitive data from being exposed to unauthorized persons or harmed by others. The security definition should ensure that the smart grid system's use does not endanger the individual's privacy. Different stakeholders' combined efforts, including government, consumers, industry, and academia, are needed [29].

Table 1 summarizes communication technologies which have to work simultaneously with standards and protocols.

Table 1. Classification of communication technologies in Smart Grid.

SG Structure	Category		Reference
Communication Technologies	Wireless	IEEE 802.15	[52,53]
		Wireless Mesh Network	[4,54]
		Cellular Communication	[55]
		Cognitive Radio	[56]
		Bluetooth, ZigBee, Microwave and Free Space Optical Communication	[4,6,11]
		Satellite Communication	[57]
	Wired	Fibre Optic Communication	[58]
		Powerline Communication: Broadband PLC Technology (BPLC)	[8,59,60]
		Powerline Communication: Narrowband PLC Technology (NBPLC)	[8,60,61]

2.3. Security Standards of Generation, Distribution, and Transmission Systems Mitigation

Cybersecurity in the generation, transmission, and distribution of electrical energy should be considered together with all the power system components integrated on SG. Cauterizing the protection of the produced energy until it reaches the consumer is one of the main tasks of the SG. In this section, standards that will ensure the safe transmission of power to the user are examined.

- IEEE 2030-2011 Standard provides a guide for SGs electrical power systems, and energy technologies can be used together. It is the first combined application that

includes IEEE 2030 standards in smart grids. Three additional standards complement in [62].

- IEEE P2030.1, Guidelines for Electrically Based Transport Infrastructures.
- IEEE P2030.2, Guidelines on the Interoperability of Energy Storage Systems Integrated in Electric Power Infrastructures.
- IEEE P2030.3, Guide to Test Practices for Electrical Energy Storage Equipment and Systems [62].
- IEC 1686-2007 is an informative document about the standards on cybersecurity features, capabilities, and functions for Smart Electronic Devices used in the substation and the security of critical infrastructures [47,48].
- NIST has proposed a 3-phase plan to fulfil the requirements of the Energy Independence and Security Treaty (EISA) and to set the standards initially required for the installation of smart grids [41]:
    1. To engage with stakeholders to identify applicable standards and requirements, gaps and priorities in existing standards in the open process;
    2. To create mutual usability of smart grids to ensure long-term operability;
    3. To develop and implement a framework for compliance testing and certification.
- NERC 1200 standard covers energy transmission and distribution units, and studies in NERC 1200 CIP 002-1 and CIP 009-2 series have been extended to include production facilities [42].
- Federal Energy Regulatory Commission (FERC) compliance with standards has become an obligation for the energy industry [42]. Electricity transportation and distribution network management, one of the leading departments of NIST FERC, establishes the necessary safety standards for energy transmission and distribution.
- In the IEEE 1402-2000 (R2008) standard, the security of electrical power generation and distribution stations is mostly subject to the physical level, and leakages from the electronic environment are also included [63].
- Another standard aimed at controlling data is NISTIR 7628, which includes the three following topics on risk assessment and security analysis [36,64]:
    1. The security architecture section: includes Cybersecurity strategy; Logical architecture, including high-level security requirements; Cryptography, and key management topics.
    2. Requirements section: includes privacy and smart grid issues.
    3. Supporting analysis and references section: concerning Vulnerability classification, Security in bottom-up smart networks analysis, Research and development on cybersecurity in smart networks, Overview of standard controls, Solutions used by switch power systems for security topics.

2.4. Security Standards of Control Systems Mitigation

Control systems in SGs are generally used in a distributed or centralized manner to manage power generation facilities. DCS can be thought of as a process control architecture that controls, in particular, more than one region's integrated subsystem. The DCS is designed to oversee a smaller group of supervisors who share responsibilities in order to run the entire production operation [65].

Control is often used in conjunction with bilateral communication systems. During the process, parameters that should be controlled should be provided with high security through communication and control systems. Distributed Network Protocol 3 (DNP3) and Generic Object Oriented Substations Events (GOOSE), IEC 61,850 and IEC 608750-5 standards have been developed for control systems [14] to use the implementation of consistent security solutions, but adequate standardization has not been achieved yet [66]. Isolated industrial and distributed control systems are safely accepted, and cybersecurity dimension is substantially negligible in the first years of its installation. However, over time, the industrial control system and communication protocol standards have shifted to open international standards to control and monitor a geographically dispersed structure

far apart from each other to increase productivity and efficiency and the need for internet or intranet connectivity [67].

Transportation, energy, medical, security, and logistical control systems are used for different purposes, such as using other protocols and services despite sharing similar characteristics [68]. For this reason, the additional control systems are used similar methods against cybersecurity threats. Control systems used for different purposes can be found in the SG as follows [53]: AMI, Building Automation Systems (BAS), Building Management Control Systems (BMCS), Closed-Circuit Television (CCTV) Surveillance Systems, CO2 Monitoring, Digital Signage Systems (DSS), Digital Video Management Systems (DVMS), Electronic Security Systems (ESS), Emergency Management Systems (EMMS), Energy Management Systems (EMS), Intrusion Detection Systems (IDS), Physical Access Control Systems (PACS), Public Safety/Land Mobile Radios, Renewable Energy Geothermal Systems (REGS), Renewable Energy Photovoltaic Systems (PVS), etc.

With these various purposes, the changes of paradigm, digitalization, standardization, and their impacts on the smart grids are summarized in Table 2.

Table 2. Paradigm changes in power systems.

	Paradigm Change	**Digitalization**	**Standardization**
Impact On	Operation	Easy maintenance Serves Scalability More and High-Quality Data Collection	Interoperability and Interchangeability Addition of new equipment is easy Paves the way for Plug and Play (PnP)
	Cyber Security	Physical Security is compromised Easier Access to Networks Connectivity is disadvantageous	Security by obscurity is lost Hackers can use legitimate models to identify All the data objects are known

As shown in Table 2, standardization is needed for easy connection, integration, and operation. The digitalization has advantages as serving scalability, easy operation, and access to the communication networks and this connection can be used for malicious aims. However, this means attackers can model themselves as a legal device as a relay or circuit breaker, exchange information with other entities as the parameters and messages are well-known [13]. In order to ensure the stability, especially in Supervisory Control and Data Acquisition systems, Modbus: Master/Slave—Port 502, BACnet2: Master/Slave—Port 47,808, LonWorks/LonTalk3: Peer to Peer—Port 1679, DNP3: Master/Slave—Port 19,999, IEEE 802.x, ZigBee, and Bluetooth—Master/Slave Protocols [53] and standards in the following should be used.

- NIST SP 800-53, Standard titled security and privacy management for Federal Information Systems and Organizations (FISO), includes selecting a security control center, adapting the power lines to security control, recording control selection process, new methods and legal systems [36].
- ISA-SP99 production and control systems safety standard has been published in 2 technical report parts. The standard covers improving the accessibility, integrity and confidentiality of the elements and systems used in control. It aims to establish security control systems. It includes technical reports, specifically data to control systems, safety standards and publications [43].
- SA-99 contains advice and guidance on many security technology products for industrial automation and control systems. It deals with risk analysis, countermeasures, and cybersecurity management systems [48].
- NIST 800-82 provides a direct security checklist and provides security requirements and solutions for risk assessment studies. The standard examines the hardware and software components used in the cybersecurity infrastructure, makes recommendations for more secure network and application services, and provides examples [62].

NIST 800-82 control systems security guideline is listed under the following four sub-headings [59]:

1. An overview of the reasons for security needs as well as physical measures take in control systems;
2. Differences between control and communication systems within the scope of openness, threats, and events;
3. Suggestions for assembling security solutions into typical grid structures found in control systems, with decompression point on network distinction implementations;
4. Summary of managerial, operational, and technical controls.

- NERC 1300 standards are developed for the identification and certification of procedures. The standards can be applied to entities performing the specified activities such as control regions and generation company owners [43]. It contains comprehensive information on critical issues under the following headings [69]:

1. 1301 Security Management Issues;
2. 1302 Critical Cyber Assets;
3. 1303 Personnel Subjects and Training;
4. 1304 Electronic Security;
5. 1305 Physical Security;
6. 1306 System Security Management;
7. 1307 Incident Response Plans;
8. 1308 Recovery Plans.

Different species of control systems (CS) holding imitative behaviours and many of the suggestions from [53] are practicable and could be used as a sample to protec systems in the face of cyber-secure assaults. Even though numerous different systems such as construction, medical, transportation, defence, and logistics use different procedures and standards, they all run in similar modes and have similar characteristics to conventional CS [53].

3. Classifications of Cyber-Attacks in SGs

According to EPRI, all the parts of SGs must work in simultaneously in a secure way [48]. Thus, complete security cannot be provided without cybersecurity technologies, policies, and risk assessments and one of the most critical dimensions: education and awareness. This is because security vulnerabilities are also seen in the studies as mostly occurring depending on the human factor [29,55]. By overcoming the people in control of the system, it is much easier to circumvent antivirus software, systems reporting attacks, or bypass firewalls. Even if all technical regulations and security policies are developed and determined, users with lack of awareness will disable these technical solutions. Although information security gaps can never be eliminated, they can be reduced to an acceptable level by developing information security awareness among employees and transforming this awareness into behaviour [39]. All the attacks are critically dangerous for the infrastructure sector, but there is a great danger if they originate from a disgruntled insider who knows the system's features. Institutions generally rely on existing SCADA systems' tight physical security and consider that they are safe from such an attack. Therefore, when faced with an attack, they are exposed to severe losses and damages. When the attacker gains control over the system, the management and activation of the attack have begun. In this process, after the malware is loaded on computers, a connection is opened with the command-and-control systems that allows attackers to access infected systems remotely. After remote access was achieved, the attackers upgraded the privileged accounts, obtaining user credentials [70]. The SG works with advanced technologies such as big data, IoT, and cloud computing to preserve complex CPS security [71]. CPS refers to a system that monitors and controls people and their physical processes in the cyber world using advanced computing and communication technologies [72]. Since CPS security is important at all levels, attacks can have an effect on both cyber and physical infrastructure [73]. Due

to its own physical and logical regulations, CPS is a crucial part of the SG. It regulates the infrastructures of communication, information technology (IT), security, automated control, protocols, standards, and features [74,75]. Moreover, the threat of cyber physical attack is a critical issue in human society, where an attacker can exploit and leverage vulnerabilities in the SG for personal advantage or to advance political goals [76]. Because of attacks challenge, NIST is working on the future power grid, which includes components for connectivity, electricity, and information [77], and it is considered the light shed between the physical and cyber worlds. SGs architecture and infrastructure are faced with cybersecurity attacks and challenges ranging from thefts, terrorism, natural disasters, etc. In the event of SG's breakdown due to any of the threats, potential consequences include power system blackouts (small and large outages), IT infrastructure failures, false visualization of the actual system's condition, damaged consumer devices, energy market chaos, endangered human safety, etc. [78].

It can be seen in Figure 5 [79] that CPS is an essential part of control systems architecture which is related to the field of integrated sensor and actuator networks [80]. Significant disruptions to critical infrastructures due to deliberate attacks on SG Control systems or unintentional attacks such as slammer worms can cause far more national economic damage than the infrastructure itself. For example, an attack [81] includes the examination, loading, and execution. The attackers used a virtual private network (VPN) to gain access to the control system. Then, workstations, servers, and some HMIs and logs are deleted with KillDisk software and other machines' events to avoid leaving traces. It was stated that at least 27 transformers and 225,000 customers were affected due to the attack [81]. Results of an attack is provided in [82]:

- By stopping or delaying the flow of information between the control networks, the fulfilment of critical-time functions can be prevented;
- Threshold values that can damage or deactivate or turn off the hardware by unauthorized changes in instructions, commands, or alarm;
- It may create negative environmental consequences;
- Wrong information can be sent to system operators;
- Software or configuration settings can be changed;
- Operation of security systems that may endanger human life can be intervened.

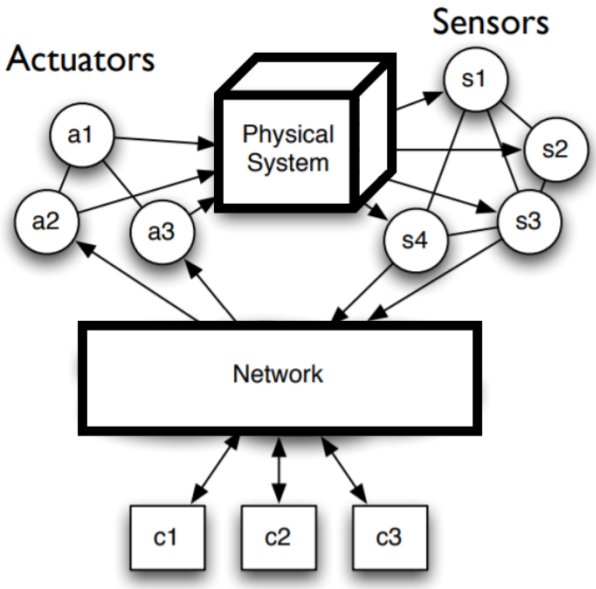


Figure 5. The architecture of Control System with CPS.

The criticality and sensitivity of the infrastructures managed by CS have made it one of the primary targets of cyber terrorism and cyber warfare. Therefore, it is vital to analyse

it in depth to reveal gaps in control systems' protocols and components [81]. Only in this way it will be possible to take precautions against the detected gaps and prevent them from being re-exploited by the attackers [82,83]. As discussed in the study [84], vulnerabilities in control systems can cause attackers to infiltrate the network, access control software, and cause unwanted damage by changing the systems' operating conditions. All connections used that only belong to the relevant institution and organization can be very useful in preventing unauthorized access and keeping the network confidential. However, it is impossible to manage systems with such an "isolated" network today, which is almost mandatory to use interconnected networks [85]. A significant part of the communication or control system attacks is not disclosed to the public by many countries due to bad reputation. However, most of the research work in CPS security focused on transmission or control systems.

Accordingly, a great deal of the assumptions made for attacks formulation and detection algorithms do not hold for both systems [81]. The renewal and integration of SG communication sheets in the power grids have authorized significant improvements and have composed new issues and challenges. In this way, the communication architecture is operated to receive real-time (RT) data between control and digital centres. This combination has allowed a few challenges like incorporating high DER's [82] and sufficient microgrids coupling [83]. Besides, integrating the AMI has authorized two-way communication between customers and utilities and the constitutional ingredient of demand side management [84]. However, when communication architecture includes a large geographic area, power and control systems become vulnerable to CPS attacks, which was recently assumed as one of the most crucial issues for SG [85–90].

The most threats and hazardous attacks in the world are examined in detail with a timeline in Figure 6 for the last two decades. It can be seen different countries were affected and miscellaneous systems have been damaged for years since 1982. Moreover, the impacts of these malicious attacks are summarized.

Unwanted events that may be encountered in smart grids can be summarized as follows:

- Disruption of control and monitoring operations as a result of blocking or delay of information carried on the network;
- Endangering the lives of the environment, employees, and other people as a result of the system components being shut down, disabled, or damaged by unauthorized modification of commands, instructions, and alarm thresholds;
- The adverse effects of situations that cause operators to send inappropriate commands by sending incorrect information to system operators or hiding unauthorized changes risk people's lives by intervening in secure systems.

Malicious CPS attacks can have severe impacts ranging from economic effects to partial malfunctioning of equipment, all the way to cascading failures and shut-down of entire power systems [54,86].

These attacks can target both the cyber part, which consists of the software and communication layer, and the physical part, which consists of the electrical power devices [91]. Common attack templates include, but are not limited to, man in the middle attacks [92], rogue devices attacks [81], denial of service attacks [86], false data injection (FDI) [16] attacks, etc. While a variety of hazardous attacks that can be classified according to the purpose, target, or effects generally can be expressed as follows.

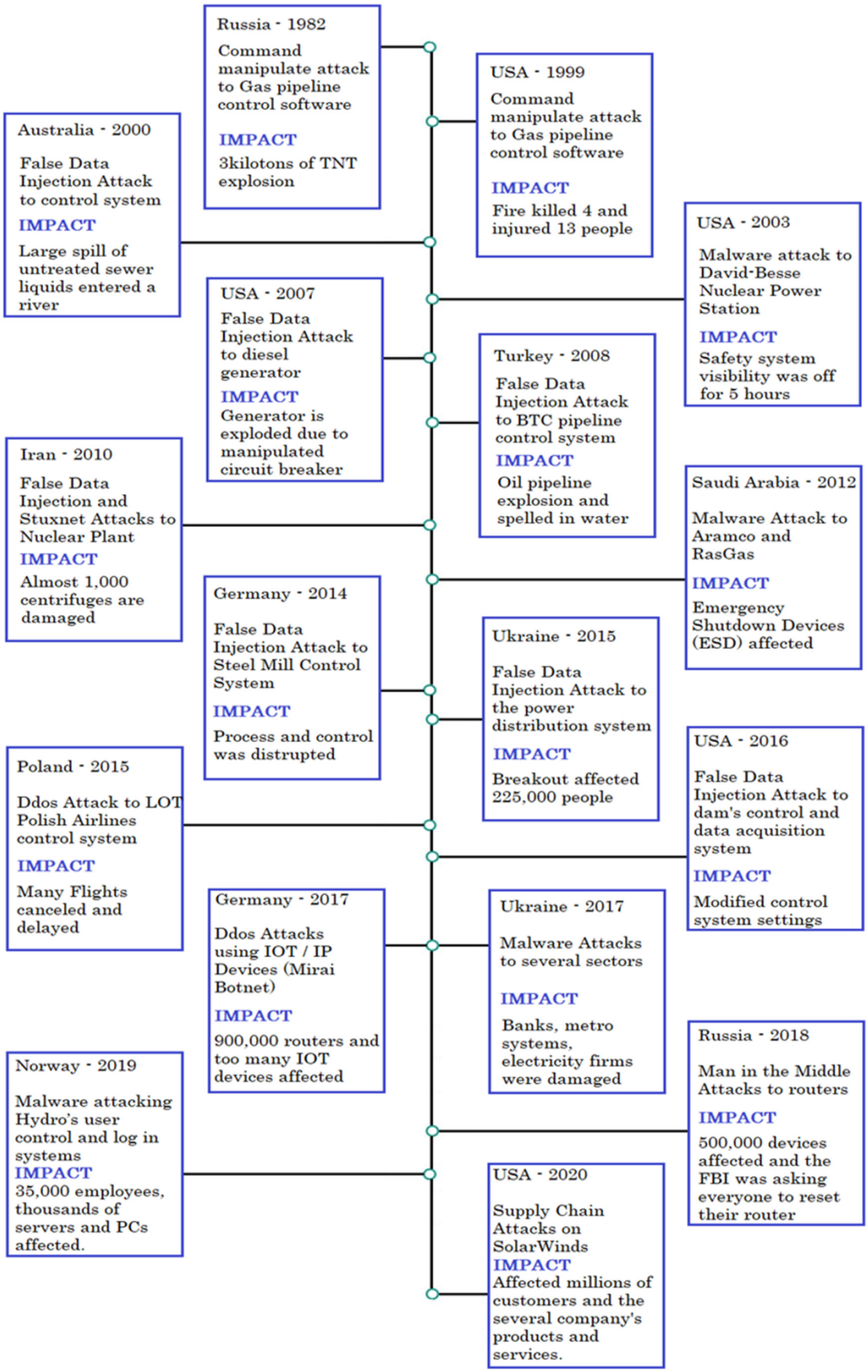


Figure 6. Timeline of essential cyber-attacks over the past two decades.

3.1. Denial of Service (Dos) Attacks

DoS (Denial of Service) means disrupting the service or destroying the function of the service. It does not allow users to access or offer prolonged service. The purpose of the DoS attack type is to exceed the limit of resources and disable the system. The attack usually occurs over a single Internet Protocol (IP), and in this case, it can be prevented by using a Firewall [86,93].

3.2. Distributed Denial of Service (DDos) Attacks

DDoS aimed to disrupt the service or make it unable to provide any service like DoS. The attacker created it before the target's attack with the machine or computer community. However, the attacker can easily be concealed without revealing their identity. Unlike the DoS attack, many machines are used in a DDoS attack, and IP detection is more complicated than others. A firewall may not be sufficient, making DDoS more dangerous and effective than DoS attack. Moreover, Distributed Reflective Denial of Service (DRDoS) is similar to DDoS and uses additional networks to attack more frequently. Attacks on the protocol, grid operation control, communication infrastructure, bandwidth, consistency observation, and billing mechanisms are all possible forms of DDoS attacks in the SG environment [86,93].

3.3. Packet Sniffing Attacks

This type of attacks is designed to capture information packets in the network and read their content. The term of sniffing is to listen to data traffic. An attacker aims to capture and store all data between two entities by monitoring the network traffic. It is one of the most used methods, and connections must be encrypted for protection [81].

3.4. Man in the Middle (MitM) Attacks

MitM attack consists of three systems, one attacker and two victim computers. The attack starts when the attacker sending signals to the first victim system claims that it is the second victim system while sending other signals to the second victim system, indicating that it is the first victim system. The first victim sends all packages to the attacker, transmitted to the second victim via himself with the MitM effect. When the fake connection is established, the victim thinks they are using the usual network connection. MitM attacks are most commonly carried out by taking advantage of the Address Resolution Protocol (ARP) and changing the MAC address information expressed as ARP poisoning. In parallel with the proliferation of internet networks, security vulnerabilities have increased [94]. Approximately 30 years have passed since the vulnerability in the ARP protocol was detected. However, damaging systems is still one of the widely used methods. This result shows that the security measures taken were insufficient [95–97]. Especially considering how easy it is to join and leave the mobile network, which is widespread today; the difficulty of preventing ARP poisoning and MitM attack is clearly understood.

3.5. Ip Spoofing Attacks

Internet Protocol (IP) connection between computers is provided through various protocols. When connected to another computer through these protocols, the connected computer introduces its identity to the other party. The real IP address of a connected computer not shown is the concealment of the actual identity called IP spoofing. The computer receiving the fake IP packet cannot detect whether the packet came from the address from which it was sent. Although this is possible in theory, in practice, it will not be possible to connect to someone else's computer from a different IP unless the system on the other side is seized. Deception is generally used to hide the source during an attack [98,99].

3.6. SQL Injection Attacks

Today, numerous databases are designed to comply with codes written in Structured Query Language (SQL), then many websites that receive information from users receive this data to SQL databases. Attackers take control of victims' databases by exploiting SQL

vulnerabilities. For example, in a SQL injection attack, a hacker writes some SQL codes into a web form which requests identification information. If the website and database are not checked correctly, the database may experiment to run these codes [95].

3.7. Command Manipulation Attacks

Usually, these types of attacks are directly targeted the servers unlike SQL injection. It targets access to information on the operating system, database management system, and server remotely using the web application's command line. There are applications such as Code manipulation or Database manipulation attacks depending on the usage [24,99].

3.8. Chameleon Attacks

Working like a typical program, the "chameleon" actually applies several tricks and deceptions, saving usernames and passwords in multi-user systems thanks to its ability to mimic a secret file, warning that the system will be shut down temporarily for maintenance. Using the chameleon program seizes the usernames and passwords by accessing this secret file [97].

3.9. Keylogger Attacks

Key loggers are spy programs that record keyboard operations. Unaware of the user, they record every key touched on the keyboard and send them to previously determined addresses when they find the opportunity. Due to such software recording keyboard operations, it can be understood how dangerous is the information containing the users' private information [98].

3.10. Back Door Attacks

The attacks methods provide remote access. It can pass without found by the normal authentication processes on the computer. Hackers who make a laborious effort to infiltrate a system want to add an easier way to access the same system. The most common backdoor method is to keep a port on the target system with an attached listening agent open. Backdoor attacks are mostly malicious software that can infiltrate the target system. When many viruses infect a computer, they always try to open a backdoor. Malicious people who are aware of this situation can use these structures. One of the most famous claims about the backdoor is that Microsoft has installed a backdoor for the NSA (American National Security Agency, Fort Meade, MD, USA) in all versions of the Windows operating system. This claim is an additional input key in the name of NSAKey in the CryptoAPI structure found in all versions of Microsoft [99].

3.11. Supply Chain Attacks

An attack could contain any methods which come to an agreement with system's accuracy prior to it being delivered. When the supply chain needs high sophistication attacking, current statements propose that of plenty foreign network devices may include back door attacks that ensure unauthorized users access [100]. Supply chain attacks do not need any hacker person to access the physical system. Supply chain matters are also associated to the need to have confidence in system updates and pieces utilized in improved cyberattacks [101].

3.12. Spywares and Malware Attacks

The primary purpose of these software, which cannot be called viruses in the full sense, is to collect information from the computer where they are installed and send it to the people who created these programs. The danger of this software to the computer or control systems may differ in their degree of spying, and they can be considered more innocent than other malicious software. On the other hand, the most dangerous derivatives can access user information by changing the data.

Software is intended to implement an unauthorized process that will harm the confidentiality, knowledge system's credibility, or functionality in the following terms: a virus or other command based asset contaminates a host. Some forms of Spyware are also examples of Malware attacks with malicious code [36].

3.13. Trojan Horses

It can be defined as computer software that appears to have a useful function and contains hidden and potentially harmful functions that can bypass security mechanisms and sometimes exploit the legitimate authority of a control and communication system unit [71,102]. Since they are confusing terms, it is useful to highlight the feature that distinguish viruses from Trojans, Worms, and Stuxnet here:

- Trojans appear to be harmless software that do not interfere with the system. However, when a situation arises, they will come into play and exploit times for other malicious applications.
- Worms are programs on their own that can spread themselves in the net. On the contrary, a virus is not a self-sufficient program to infect. It spreads by attaching itself to other files, but if the infected file is not opened, the virus cannot spread to other environments [36,102].
- Stuxnet is using spread USB devices and changing the Ladder logic code of PLCs [70]. This attack involves human factors as well as technology and process management.

3.14. Rogue Devices Attacks

These attacks give attackers an excellent opportunity to settle with the supply chain attacks and then re-install malicious software into a device before shipment to target location and later use it as a backdoor attack [100].

3.15. False Data Injection Attacks (FDIA)

False Data Injection Attacks aim to inject malicious measurements and modify the results. FDIA could violate data integrity in various regions as transmission, communication, generation, control, etc.

It can be seen in a different part of the SG that contains data. In this section, the FDIA will be evaluated in the grid without categorizing. It will be examined with the same approach for all regions. Figure 7 depicts the diagram of the following formulated system [100].

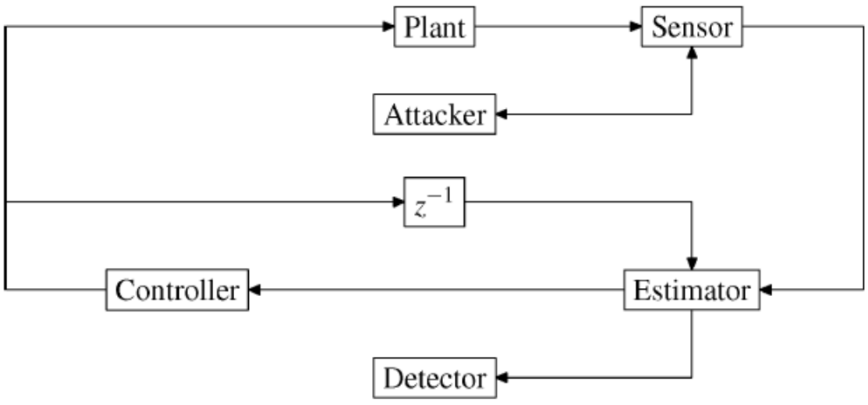


Figure 7. FDIA general block diagram.

In terms of common features in systems, basic principles of FDIA can be formulated as follows [102]:

Let z_d represent the measurements vector which contains false and malicious data, and z_d can be formulated as; $z_d = z + d$, where z is the original vector measurements $z = (z_1, z_2, \ldots, z_m)^T$, and d is false or malicious data $d = (d_1, d_2, \ldots, d_m)^T$ which added to

the original measurements. It is referred to d as a false data attack vector. The element of d_i means non-zero, and the attacker conciliates the i_{th} meter and then displaces its original mensuration z_i with a false extent $z_i + d_i$. Let $\hat{X}_{false}$ and $\hat{x}$ specify the forecasts of x using the false mensuration's z_d and the original values z, respectively. $\hat{X}_{false}$ may be written as $\hat{x} + f$, where f is a non-zero n-dimensional vector. It is worth noting that f states the attacker's calculation error. The intruder, on the other hand, should choose f as a linear combination of H's column vectors (i.e., $d = H_f$). Therefore, FDIA with complete information is following and z_d can pass the detector as long as z is able to pass it [102]. It is assumed that an attacker accesses the H matrix and injects false measurements in [103], m meters provide m measurements $z_1, \ldots, z_m$, and also, it is assumed that there are n state variables $x_1, \ldots, z_n$. The $m \times n$ matrix H can be characterized by a relationship between m meter measurements and n state variables. The measurement noise [104] is formulated with W diagonal matrix as

$$\hat{x} = \left(H^T W H\right)^{-1} H^T W_Z \tag{1}$$

In [102], an attack in which the attack vector d equals H_f, where f is an arbitrary non-zero vector, is a false data injection attack. Seeing that z can pass the detection and where τ is the threshold, $\|z - H\hat{X}\| \leq \tau$ is had; then, the vector of estimated state variables acquired from z_d can be demonstrated as $\hat{x} + f$. Described previously if $d = H_f$, the resulting measurement follows:

$$\begin{aligned} \|z - H\hat{X}_{false}\| &= \|z + d - H(\hat{x} + f)\| \\ &= \|z - H\hat{x} + (d - Hf)\| \\ &= \|z - H\hat{x}\| \leq \tau \end{aligned} \tag{2}$$

Attackers generate malicious measurements based on the H matrix and then inject it by starting FDIAs; they can manage the injected false data to overcome the bad measurement detection and represent random errors into the state estimation (SE) output. On the contrary, if attackers have no complete information about H matrix, if $d \neq H_f$, φ error matrix is created, then the solution of the state estimation follows:

$$\begin{aligned} \hat{x}_d &= \left(H^T W H\right)^{-1} H^T W_{Zd} \\ &= \left(H^T W H\right)^{-1} H^T W(z + d) \\ &= \left(H^T W H\right)^{-1} H^T W\left(z + H_f + \varphi_f\right) \\ &= \hat{x} + f + \left(H^T W H\right)^{-1} H^T W \varphi_f \\ &= \hat{x} + \overline{f} \end{aligned} \tag{3}$$

$$\text{where } \overline{f} = f + \left(H^T W H\right)^{-1} H^T W \varphi_f \tag{4}$$

The attacker aims to hack the multiple sensors and phasor measurement units (PMUs) readings to mislead the smart grid's decision-making process in FDIA [103,104]. False Data Injection is one of the most dangerous types of attack among cyber-attacks. Therefore, it should be examined most carefully. Due to its high level of importance, FDIAs are currently the most studied cyber-physical SG security attacks [105]. For example; two versions of FDIA scenarios have been found in [56] where in Generalized and Random FDIA, an attacker uses small false data error in measurements and has some necessities for an accomplished attack, like they must comprehend the topology of the energy system to control and manipulate the measurement of the AMI. In random FDIA, attackers direct

a wrong estimation. Figure 8 shows various false data injection attacks scenarios on smart grid [106].

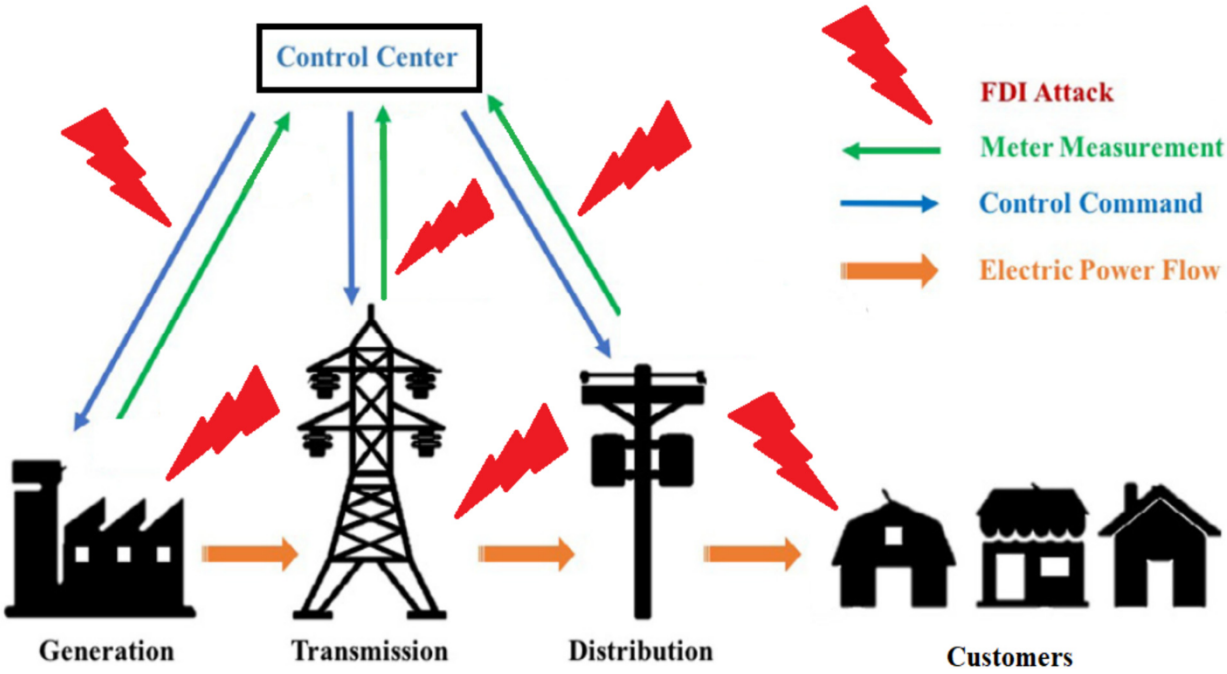


Figure 8. FDIA Scenarios in SG.

In [107], the study is examined with the architectural structure of FDIA and divided into two mains criteria's: cyber and physical. According to [108], it only focused on the physical criteria and the extensive classification of [107] study and a new control centre model. Authors in [109] finished the work in [108] and their formulation studied the impact of state estimation of FDIAs on electricity market operations.

In the AC power transmission system, FDI attacks on the SE are summarized in [92, 110,111] as a stealthy FDI attack with two steps.

The first, "Intrusion into the System" is examined. If the attacker who trying to intervene in the system is on the outside of the system, he attacks the system using one or more of the usual cyber hacks by endangering the wired or wireless communication channel. In addition to this situation, the attacker may be successful in integrating malware. In this case, the attacker may be capable of stealing system information, particularly the bus topology.

The second step is "Carry out stealthy FDI attack" aims to perform a stealthy FDIA by changing the measurement data. The manager supposes that the data are right and also estimates the other values based on this false assumption. It causes the system to reverse and hence an incorrect condition causing malfunctions or substantial deductions.

Another type of FDIA presented in [112] on power system protection suggests two targeted attack scenarios: fake safe and fake vulnerable signal attacks. The first fake protected signal attack attempts to trick the control centre into performing a required corrective acts such as load shedding and neglecting a power line peak demand by switching from an unstable to a secure state. The second fake unstable signal attack attempts to move from a safe to an insecure state in order to deceive the control centre into performing inappropriate corrective steps, thus inflating costs unnecessarily.

Security-constrained economic dispatch (SCED) proposed in [112], and SCED FDIAs can be divided into two types: attack optimizing operating cost and attack causing overload. The first is to boost the cost of generation or load shedding or to make an illegitimate profit [113]. The second group aims to overwhelm power lines in order to inflict physical harm [114].

Contingency analysis (CA) is one of the significant functions of power system security. These kinds of FDIAs are proposed in [115]; an attacker who knows network topology and system parameters can smoothly run the control algorithm to have the contingency list. CA can calculate complexity in real-time power market operations, flow-based SCED with DC assumptions.

The study [115] constructs an attack vector by modifying the contingency list using both analogue and optical dimensions. The problem is modelled as a mixed-integer non-linear programming-based (MINLP) optimization problem, and the physical and economic effects of these attacks on the SG power system have been quantified.

The attackers inject types, and FDIA measurement reports aim to disrupt the smart grid operation through the compromised meters and sensors [116]. FDIA attacks can disrupt the grid system state estimation and cause energy distribution false. Moreover, meters and sensors lacking tamper-resistance hardware increase the possibility to be compromised. The injecting FDIA types of energy systems are [116]:

- Energy-request Deceiving Attack;
- The attacker compromises demand-nodes and injects a forged quantity of demanded energy;
- Energy-supply Deceiving Attack;
- The attacker compromises supply nodes and injects a forged quantity of energy that it could provide to the grid.

Different FDIAs classifications divided into three-level classifications proposed in [117]. The FDIAs are categorized concerning the targeted systems at the first level, second is targeted subsystems and can be divided into subsystems and the attack's impact, which can be physical and economic attacks targeting the subsystems at the third level. According to [116], another FDIA attack assumes that the hacker can only reach specific measurements due to the meters' different physical protections. With this study "building a valid FDIA by minimizing the number of attached meters", research started, and several attacks with various conclusions and aims have been suggested on the basis of this analysis.

FDI attacks are divided into random and target FDI attacks in [118,119]. In random FDI, attackers aim to inject any false data to cause bad state estimation in the state variables. The target FDI is injecting an attack vector that causes an error into certain state variables. Other types of FDI attacks, such as scaling, ramp, and pulse are proposed in [120]. Previous studies have mostly focused on the FDIA issue in the transmission network. Unlike them, [110] proposes attack models in transmission, storage, and micro-grid networks, with a focus on determining the effect of FDIA on the power grid's economic and stable activity.

FDI attacks are described into three major categories as Bad Data Injection Attacks, Replay Attacks (RA), and Zero Dynamics Attacks (ZDA), and many end devices that enable the smooth functionalities of energy systems even from a remote area are proposed in [85]. The RAs are challenging to detect due to cryptography operations' limited capability [96,109]. ZDAs indicate a cluster of attacks using unstable zeros as the bug to attack smart meters [121,122]. Then, they will inject the false output through the communication channel. In the end, the real state increases as the time passes, while nearing close to the output-nulling space. In this way, the corresponding outcome is referred to as a stealthy attack and too close to zero [82].

FDI attacks aim to mislead the service providers, disable the sensor nodes to cause service failure between physical systems and the networks, or hijack the communication channels [123]. There are two points to consider in order to understand the success of an attack target:

- The first is to access data by infiltrating the current energy system. This way, data in sandboxes can also be manipulated.
- Second, they control data without being detected [24,25,42,78,124,125]. A successful attack can reduce the actual flow of power to destabilize energy systems [126]. As a result, FDI Attacks pose major threats to both energy systems and communication and other physical systems and are difficult to detect in real-time [100,117,127,128].

The FDIA and all its derivatives aim to damage transmitted data; this may cause a chain reaction between different systems in SG, when an attack is accessed in the communication system can affect the transmission or generation system [17,114,119,129,130].

According to the general nature of all FDI, attacks have the same goal [126]. The objectives are to use physical systems or malicious packets to deceive service providers, capture communication channels, or disable sensor nodes and create an attack that bypasses the traditional bad data detector [71,127,131]. By the way, Detection methods are examined in the following section.

4. False Data Injection Attacks Detection Modelling and Methods

The mathematical formulation for modelling false data injection attack (FDIA) for both power and communication system and how stealthy FDIAs are carried out on SG describes in this section.

4.1. Mathematical Modelling of False Data Injection Attacks Detection

An attacker can inject a malicious attack in a vectorial form with perfect knowledge of the Jacobian matrix and FDIA calculation described previously. So, the mathematical formulation of FDIA detection should be understood clearly. It is aimed to make sure that the FDIA vector elements are the same in the sense of energy, so the comparison stage and simulations are current and significant.

The classic FDIA detector $J(\hat{x})$ is created first in [132] with hypothesis test in to detect FDIA, H_0 and H_1. H_0 is the null hypothesis, where the measurement is valid; and H_1 is the alternative hypothesis, where the measurement is under attack. So, $J(\hat{x})$ as follows:

$$r^T W r \underset{H_1}{\overset{H_0}{\gtrless}} \gamma \tag{5}$$

Meanwhile in [133], if $\varepsilon_0 = Trace(\Sigma_x - KH\Sigma_x)$ offers minimum mean square error (MMSE), when it is in the asset of the attack would be $\varepsilon_0 + \|Ka\|_2^2$ which refers MMSE can be controlled by energy. In the MMSE, an optimum attack is produced with the minimum residue to limit the probability of detection that can be formed: $min\|Ga\|_2^2$ subject to $\|Ka\|_2^2 \geq$ C where $G \triangleq I - HK$ and C is attack's minimum energy value. The sparsity pattern presented in [134] and assumed the full measurement assumption.

4.2. Detection Methods of FDIA

The detection part of cyber-security in SG is vital for resisting cyberattacks in its large-volume data-driven architecture. In this architecture, cybersecurity has become more complicated than before, and traditional manual and signature-based approaches are no longer useful have revealed the need for a new approach [99]. Thus, it has been heavily investigated in contemporary literature. The signature-based detection approaches for FDIAs have not prepared for data challenges caused by the large-scale deployment of PMU in the CPS on SG. Real-time big data produced by PMU causes storage and computational issues [133–135].

However, there is a remarkable fact that this issue becomes an opportunity for data analytics techniques such as Machine Learning (ML) to detect and block FDIAs. ML has excellent non-linear analysis capabilities to detect FDIA in more complex systems when more data is obtained from the system; it can be solving the challenges easier [133]. Thus, it is applied very beneficially in the smart grid's cybersecurity areas with complex sensor networks.

For detecting FDIA, general ML techniques artificial neural network (ANN) and support vector machines (SVM) were the most recent works and used previously, while implementation of other techniques in such detection was also conducted. Different methods for detecting and identifying FDIA on SG have been proposed to in this section. Classify of different FDIA detection methods are depicted in Table 3. The attack to data integrity is a significant threat to energy consumption and the state estimation process.

It becomes possible for attackers to make control centres and wrong decisions through manipulations of various SG measurements [136]. Remarkable methods are used for data integrity aim are particle swarm optimization (PSO), Bayesian framework (BF), Adaboost, Random Forests (RF), and Common Path Mining Method [128,137–140]. In [119], data analytical approaches are analysed, and the Margin-setting algorithm (MSA) is a novel data analytical approach applied to the system based on ML and MSA; it reaches better results than the ANN and SWM methods. It is the first work to use MSA to detect FDIAs. Kalman Filter (KF) is one of the primary detection methods for power state estimation process on online operation [141]. In [142], KF was utilized to detect FDIA in automatic generation control (AGC) systems. Extended Kalman filter (EKF) proposed in [143], and Distributed Kalman Filter (DKF) can be found in [144]. The benefit of EKF provides to reach more precise estimate and detection of FDIA. According to [145] distributed support vector machine (DSVM) algorithm is studied for training and principal component analysis (PCA) on an IEEE 118-bus system simulated by MATPOWER. In [146], a detection method on phasor measurement unit (PMU) using MSA for spherical classification with data from an IEEE 6 bus system simulated in MATLAB. The result is that FDIAs are stealth attacks that can overcome the existing detection scheme [146]. In [137] the methods used were perceptron, kernels nearest neighbours (k-NN), SVM with Gaussian and linear kernels, sparse logistic regression (SLR), and the semi-supervised SVM (S3VM) studied on the models with using IEEE 9, 57, and 118 bus systems. In [131] conditional deep belief network (CDBN) which have one of the various deep neural network infrastructures, so catching is proposed to the high-dimensional temporal characteristics of the stealthy FDI attacks. Unknown input observation (UIO) was used in FDIA detection in [147]. The method which used supervised learning to classify measurement data is proposed in [137], and it was capable of identifying unobservable attacks and predict attacks using observation sets. Euclidean distance-based approach is proposed in [148] to detect FDIAs. They have also investigated on feature selection schemes with less complexity with improved accuracy that studied genetic algorithm for BDD. In [149] FDIA and stealth attack detections in wide area measurement in SG monitoring system is examined.

ML and Deep Learning methods for intrusion detection examined in detail for different categories in [150]. Detection of electricity theft is discussed in [151]. ML techniques such as PCA [125,145,152,153], game theory approaches [113], and the Stackelberg game [154] can be used for detecting energy theft. Five ML models k-NN, SVM, ANN, NB, and DT, and tested all proposed approaches on MATPOWER are used in [146].

Furthermore, [155] is used one-class SVM (OCSVM), robust covariance (RC), isolation forest (ISOF), and local outlier factor (LOF) as individual classifiers for detection FDIA.

A feed-forward neural network (FFNN) is proposed in [111] for stealthy FDIA detection with used random forest for feature selection and compared the deep learning scheme with three methods as gradient boosting machines (GBM), generalized linear models (GLM), and the distributed random forests (DRF). Isolation forest (ISOF) is used in [155] to detect FDI attacks with simulated data; it reduces the data's dimensionality using PCA, to show that ISOF outperforms their findings using four ML methods: SVM, k-NN, NB, and MLP. It does not say how long it took to train the models, but the fact that ISOF outperformed the other models is surprising. On the same sample, supervised models do better than unsupervised models in terms of precision.

Table 3. Overview of FDIA detection methods in the SGs.

Detection Methods	References	Year	Datasets
MGD Based	[16]	2017	Synthetic Datasets in Matpower
KPCA	[17]	2020	Synthetic Datasets in Matpower
FFNN	[111]	2020	Random Data simulated in Matpower
RF, Adaboost	[128]	2019	Synthetic Datasets in Matpower
CDBN	[131]	2017	Synthetic Datasets in Matpower
Perceptron, k-NN, SLR	[137]	2016	Synthetic Datasets in Matpower
XGBoost	[138]	2019	Provided by Endsea
KF, DKF, EKF	[141–144]	2017, 2018	Simulated
DSVM	[145]	2017	Synthetic Datasets in Matpower
MSA	[146]	2017	Synthetic Datasets in Simulink
UIO	[147]	2019	Random Data for each grid subarea
OCSVM	[155]	2018	Synthetic Datasets in Matpower
DT and SVM	[156]	2016	Real Dataset in USA
SVM Based	[157]	2016	Smart Energy Datasets from Ireland
S3VM Based	[158]	2019	Irish Smart Energy Trial Data
ANN	[159]	2013	Real Datasets in Brazil
PARX	[160]	2016	Synthetic Datasets in Matpower
ARIMA and ANN	[161]	2015	Real Datasets in Amsterdam
GBTD	[162]	2019	Irish Smart Energy Trial Data
RNN	[163]	2018	Synthetic Datasets in Matpower
CNN and Encryption	[164]	2019	Released by SGCC
MFEFD	[165]	2019	Irish Smart Energy Trial Data
KLD Based	[166]	2015	Synthetic Datasets in Matpower
SARSA	[167]	2018	Synthetic Datasets in Matpower
ISOF	[168]	2019	Synthetic Datasets in Matpower
Deep autoencoder	[169]	2019	Real PMU data
GAN	[170]	2019	IoT-based smart home data
RNN and CNN	[171]	2019	Released by SGCC
MLR and NN	[172]	2019	CEFcom 2012
NNS and Game Theory	[173]	2019	Synthetic Datasets in Matpower
NB	[174]	2019	ISO New England
POMDP	[167]	2018	Synthetic Datasets in Matpower
LR and DBSCAN	[175]	2018	Real PMU Data
DRE	[176]	2016	Synthetic Datasets in Matpower
SVM & ANN	[177]	2019	Nigerian Power Grid
C-Vine Copulas Based	[178]	2016	Low carbon London load dataset
DNN and LRC	[179]	2019	Released by SGCC
GoDec	[180]	2011	Simulated
ALM-based, LMaFit, GoDec	[181]	2018	Simulated
D-FACTS	[182]	2012	Synthetic Datasets in Matpower
D-FACTS	[183]	2014	Random Data simulated in Matpower
NARX	[184]	2019	Synthetic Datasets in Matpower
RPCA	[185]	2011	Released by SGCC
LMP	[186]	2011	Real Time Marketing Data
Subspace Methods	[187]	2015	Simulated Probability Detections

Another FDIA detection method is presented in [171], a framework with anomaly and FDIA detectors. LSTM-based CNN are used for time series anomalies of attacks formulation. RNN with an LSTM cell is delivered to get the dynamic behaviour of cyber activities on IEEE 39 bus system.

SAE, one of the DNN architectures with advanced feature extractor and LRC, used to detect anomalies caused by stealthy FDI attacks, is proposed in [179]. A classification scheme which is based on ERT algorithm and KPCA is presented in [17] and used for dimensionality degradation. A sparse PCA approximation-based method used sparse data sets to aim recovery functions which precision is inversely proportional to the sparsity of available data presented in [153]. A detection method using a semi-supervised ML technique known as the DRE is proposed [176]. It aims to validate a semi-supervised

approach by comparing its performance with SVM and MLP; and four-phase classification is proposed in [16]:

- Dimension degradation using PCA;
- Mixed Gaussian model structure using a positively labelled set;
- Collection of classification thresholds using a mixed dataset;
- An unlabelled dataset was used for testing.

Another detection mechanism using SARSA(λ) is proposed in [167]: reinforcement learning algorithm with formulated problem of stealthy FDIA detection as a POMDP.

In FDIA detection as matrix separation problem, it is difficult to get global optimum [180]. To address that, four algorithms are proposed in [181], the traditional ALM, double-noise-dual-problem ALM (DNDP-ALM), the LMaFit, and "Bilateral random projections (BRP) with Go Decomposition (GoDec)". GoDec achieves higher efficiency than others. Another new detection approach using D-FACTS (Distributed Flexible AC Transmission System) is analysed in [182,183].

ANN-based State estimation method NARX in [184] and Robust Principal Component Analysis (RPCA) are examined in [185]. LMP method for FDIA detection is used in [186]. Different subspace methods and examined [187] Bayesian or another dynamic state approaches might be more appropriate to detection FDIA.

An attacker can increase his current attack's privacy with an alternative attack password, turning it into an undetectable FDI attack. It can be named "Blind FDIA" [188]. PCA based attacks can occur if there is a significant error in the measurement data and ALM-based stealth FDI attacks can be successfully injected [188]. MTD to detect blind FDIA is implemented in [189]. Moreover, [190] is used PCA to Blind False Data Injection Attack.

Data Driven [191] and Geometric Approach are used to detect blind false data injection in [192].

Observations can be made from the review of the studies above and the works listed in Table 3:

- The researchers had attempted various approaches. However, no attempts to use general SG-based learning approach have been undertaken up to now.
- Almost all the studies used simulated datasets for validating their methods. Power flow data from the Ireland power grid is used in [162], but it seeded synthetic attacks into the dataset later or [177] used data from the Nigerian power grid, but it seeded synthetic attacks into the dataset.
- A few works mentioned here used classifiers as individual methods for communication or power but none used any ensemble fields method.

All the mentioned attacks are caused by the security vulnerabilities used with the standards examined in the table below. In this sense, the mitigations of the protocols most preferred by the standards are summarized in Table 4.

Table 4. Vulnerabilities of protocols.

	Standards	Protocols	General Issues
Communication	NIST, FERC	Structured Query Language (SQL) or Hypertext Transfer Protocol (HTTP), TCP and User Datagram Protocol (UDP) Internet Control Message Protocol (ICMP), Path Maximum Transmission Unit (PMTU) and Internet Protocol Security (IpSec)	IPv4 and IPv6 discussions [41,42,193].
	ISO/IEC 15,408/EAL, ITSEC, TCSEC, CTCPEC	IoT and Internet Protocols such as REST, CoAP, MQTT, MQTT-SN, AMQP . . . etc.	Insufficient for complex infrastructures [43,194].
	ISO/IEC 27,000 Series	Security Management System Protocols, ISMS, SSL/TLS/SSH, VPN, IPSec	Unauthorized Access [193].
	ISO/IEC 62,351, IEC 60870-5 and DNP, IEC 563	TCP/IP and specify security requirements for communication protocols as QoS, MMS, DNP, GOOSE defined by IEC Technical Committee 57, specifically the IEC 60870-5, the IEC 60870-6, the IEC 61,850, the IEC 61,970, and the IEC 61,968 families.	Vulnerabilities about protocol-based attack such as IP spoofing and DoS [48,194].
	IEEE 802.11.i and IEEE 802.16.e, IEEE 61,850	Wireless Communication protocols (Bluetooth, Zigbee, WiMax . . . etc), Internet Protocol (IP), Information and Communication Technologies (ICT), Dynamic Host Configuration Protocol (DHCP), SMTP (Simple Mail Transfer Protocol) with Communication Technology-Interoperability architectural perspective (CT-IAP)	Setting security level and protecting to MitM [194,195]
	AES	Structured Query Language (SQL) or Hypertext Transfer Protocol (HTTP), TCP, UDP, Internet Control Message Protocol (ICMP), Path Maximum Transmission Unit (PMTU) and IpSec with AES-128, AES-192, AES-256 Algorithms for cryptography.	Despite being approved by many organizations, selection of encryption techniques is not trivial [196].
	3DES	Public key-based protocols may also be used (e.g., ANSI X9.42).	Expected to be rolled out by 2030 due to insufficient security, as stated by NIST [197].
Power	IEEE 2030-2011, IEEE 1686-2007, IEEE 1402-2000	IPSec, VPN, TCP/IP, Smart Energy Profile Protocol version 2.0 (SEP 2.0), IETF with Power Systems Interoperability architectural perspective (PS-IAP)	Non-homogenous protocol structure of IEEE standards is a cause of vulnerability [62,63,195,198]. Bilateral information and power flow is targeted with IEEE 2030 [199].
	EISA, NIST, NISTIR 7628, FERC	Structured Query Language (SQL) or Hypertext Transfer Protocol (HTTP), TCP and User Datagram Protocol (UDP) port filtering and Internet Control Message Protocol (ICMP), Path Maximum Transmission Unit (PMTU) and Internet Protocol Security (IpSec)	NIST and FERC should coordinate the development and adoption of smart grid guidelines and standards [41].
	NERC, CIP	SCADA, for dial-up accessible Critical Cyber Assets that use non-routable protocols	Unauthorized access issues [42,200].
Control	IEC 61,850, IEC 608750-5, IEEE 802.x	DNP3, GOOSE, Supervisory Control and Data Acquisition systems, Modbus, BACnet, LonWorks, Wireless (ZigBee, Bluetooth) Protocols, Information Technology Interoperability architectural perspective (IT-IAP) protocols	SCADA needs holistic security solutions as it combines monitoring and control which creates significant vulnerabilities in the system [59,66,88,195]
	NIST SP 800-41, NIST 800-82 and 53	Structured Query Language (SQL) or Hypertext Transfer Protocol (HTTP), TCP and User Datagram Protocol (UDP) port filtering and Internet Control Message Protocol (ICMP)	Used in corporate networks behind a firewall. However, it is weak against MitM, Trojan or Ddos launched within the network [59].
	ANSI/ISA-SP99, SA-99	SCADA, DNP-3, Ethernet/IP and Modbus/TCP.	Heterogeneous protocol use inherently secures the system such as "push for productivity" and "Son-of-Stuxnet". Needs mitigation of MitM and Ddos for all protocol types [43,48,201].
	NERC 1300	NERC Cyber Security Standards	Needs constant updates in parallel with experiences in the field [43,69].

- NIST and FERC standards' discussions about IPv4 and IPv6 continue. When it is needed to install or change the equipment, usage of two protocols can cause more issues and require more complex infrastructure. Furthermore, against upper-layer protocols attacks such as SQL injection and FDIA, IPv4 or IPv6 stack can be used to communicate with the client. Organizations will need time to achieve solutions for IPv6, since they have been working on IPv4 over the years [41,42,193].
- FERC does not indicate the adoption of standards or how effective they are, but given the increasing use of communication and information technology in the field of electricity and energy and the evolving nature of cyber threats, it tries to offer solutions that will help reduce the risk posed by these threats on the electricity grid, which require constant attention [41,42].
- ISO/IEC 15,408/EAL, ITSEC, TCSEC, CTCPEC Standards are built to be used as the reference for evaluation of Internet security, but they are insufficient for complex infrastructures. Mainly, ISO/IEC 30,111 Standard describes processes for potential vulnerabilities in IoT services [43,194].
- In the Information Security Management System (ISMS) with ISO/IEC 27,000 Series, following requirements can be used to provide access to facilitate organization's data. When the ISMS allow to access the information security requirements of customers and other stakeholders, meet the data and manage information assets to facilitate improvement and adjustment to current organizational goals [193].
- ISO/IEC 62,351, IEC 60870-5 and DNP, IEC 563's IP usage causes devices to be vulnerable to IP-based network attacks such as IP spoofing, DoS, and others. In the usage of TCP/IP, Adequate standardization has not been achieved for the implementation of consistent security solutions. Since the security level of different wireless protocols also changes, it becomes difficult to adjust the security level of IEEE 802.11.i and IEEE 802.16.e, IEEE 61,850 standards, and it can be concluded that IEEE standards working with different protocols are more vulnerable to MitM attacks [194,195].
- AES is confirmed from many organizations because of its strong security and high performance. However, encryption technologies' choice depends on the criticality and risks of the communication system that needs to be protected [196].
- Traditional physical access approach in NERC-CIP standard needs to be revised to address unauthorized access issues [42,200]. NERC1300 is dedicated to identification and mitigation of cybersecurity vulnerabilities of critical assets [43,69].

5. Conclusions

This paper presents a review of cybersecurity vulnerabilities in smart grids. It discusses how information technologies are integrated with power systems, creating novel issues that were previously unknown. Then, mitigation requirements are documented as discussed in different standards and research outputs. It also includes an overview of possible cyberattacks in smart grids, focusing on false data injection attacks. These attacks are handled separately as their possible impact on the power system operation is much larger. A thorough review of the literature is given on research dedicated to detecting false data injection in the smart grid domain.

When using synthetic datasets, SVM-based methods (e.g., KF, EKF, DKF, RBF kernel, and Gaussian and linear kernels) were used dominantly and performed better than the classical attacks detection methods (PCA, BDD, etc.) that employ the state estimation (SE) approach for the FDIA. The studies also showed that the semi-supervised learning approaches (supervised learning over labelled data and trained SVM) are stronger to deal with the different data sparsity degrees than the fully supervised learning approaches. PCA does not require to train data to detect the deviation of the measurements. However, in real-time data, another method of detecting FDIA against a complex system using deep autoencoders offers better detection performance than SVM-based methods. Besides, deep autoencoders are more comfortable to train since they do not require labelled data

for training and can detect different attacks because they can learn hidden, complicated correlation structures in the data.

In this study, cyber-attacks that can be encountered in grids have been examined, with a particular focus on false data injection attacks. Future deep learning and deep autoencoders approach such as SARSA and POMDP can be investigated as it can work on different systems.

(1) Machine learning/AI integrated cybersecurity systems are required since hackers are getting smarter, and attacks are getting diverse.
(2) More holistic cybersecurity designs are required instead of solutions that only focus on 1 aspect of security such as access control or encryption.

Author Contributions: Conceptualization, D.B.U.; T.S.U.; S.M.S.H., and A.O.; methodology, T.S.U. and D.B.U.; software, D.B.U. and T.S.U.; validation, T.S.U.; S.M.S.H. and A.O.; investigation, D.B.U.; T.S.U. and S.M.S.H.; writing—original draft preparation, D.B.U. and T.S.U.; writing—review and editing, D.B.U., T.S.U., S.M.S.H., and A.O.; visualization, D.B.U., T.S.U., S.M.S.H., and A.O.; supervision, T.S.U. and A.O.; funding acquisition, T.S.U. and S.M.S.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

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

Appendix A

Nomenclature

3DES	Triple Data Encryption Standard
AEP	Advanced Encryption Standard
ALM	Augmented Lagrange Multiplier
ALM	Augmented Lagrange Multipliers
AMI	Advanced Metering Infrastructures
ANN	Artificial Neural Network
ANN	Artificial Neural Network
ARP	Address Resolution Protocol
ARP	Address Resolution
BAS	Building Automation Systems
BDDA	Bad Data Injection Attacks
BF	Bayesian Framework
BMCS	Building Management Control Systems
BPLC	Broadband PLC Technology
BRP	Bilateral random projections
CA	Contingency analysis
CC	Common Criteria
CCTV	Closed-Circuit Television Surveillance Systems
CDBN	Conditional Deep Belief Network
CP	Cyber-Physical
CS	Control Systems
CSD	Computer Security Division
CSRC	Computer Security Resource Center
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DCC	Distributed control centre
DDos	Distributed Denial of Service Attacks
D-FACTS	Distributed Flexible AC Transmission System
DKF	Distributed Kalman Filter
DNDP-ALM	Double-Noise-Dual-Problem Augmented Lagrange Multipliers
DNP	Distributed Network Protocol Security for IEC 60870-5
DNP3	Distributed Network Protocol 3
DoS	Denial Of Service Attacks

DRE	Density Ratio Estimation
DRF	Distributed Random Forests
DSS	Digital Signage Systems
DSVM	Distributed Support Vector Machine
DT	Decision Tree
DVMS	Digital Video Management Systems
EAL	Evaluation Assurance Level
EISA	Energy Independence and Security Treaty
EKF	Extended Kalman filter
EMMS	Emergency Management Systems
EMS	Energy Management Systems
ERT	Extremely Randomized Trees
ESS	Electronic Security Systems
EV	Electric Vehicle
FDIA	False Data Injection Attacks
FERC	Federal Energy Regulatory Commission
FERC	Federal Energy Regulatory Commission
FFNN	A Feed-Forward Neural Network
FIPS	Federal Information Processing Standard
FISO	Federal Information Systems And Organizations
GBM	Gradient Boosting Machines
GLM	Generalized Linear Models
GoDec	Go Decomposition
GOOSE	Generic Object Oriented Substations Events
HMI	Human Machine Interfaces
IDS	Intrusion Detection Systems
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISA	International Society of Automation
ISMS	Information security management system
ISO/IEC	Organization for Standardization/International Electrotechnical Commission
ISOF	Isolation forest
IT	Information Technology
ITSEC	The Information Technology Security Evaluation Criteria
KF	Kalman Filter
k-NN	Kernels Nearest Neighbors
KPCA	Kernel Principal Component Analysis
LMaFit	Low Rank Matrix Factorization
LMP	Locational Market Price
LOF	Local Outlier Factor
LRC	Logistic Regression Classifier
LSTM	Long Short-Term Memory
M2M	Machine-to-Machine
MAC	Media access control
MINLP	Mixed-Integer Non-Linear Programming-Based
MitM	Man in The Middle
ML	Machine Learning
MMS	Manufacturing Messaging Specifications
MSA	Margin-Setting Algorithm
MTD	Moving Target Defenses
NARX	Nonlinear Autoregressive Exogenous
NB	Naive Bayes
NBPLC	Narrowband PLC Technology
NERC	The North American Electric Reliability Corporation
NIHS	National Institute for Hometown Security
NIPP/CISA	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSA	American National Security Agency
PACS	Physical Access Control Systems
PCA	Principal Component Analysis
PMUs	Phasor Measurement Units
POMDP	Partially Observable Markov Decision Process
PSO	Particle Swarm Optimization

PVS	Renewable Energy Photovoltaic Systems
QoS	Quality of service
RA	Replay Attacks
RC	Robust Covariance
RCPA	Robust Principal Component Analysis
REGS	Renewable Energy Geothermal Systems
RF	Random Forests
RNN	Recurrent Neural Network
RT	Real-Time
RTU	Remote Terminal Unit
S3VM	Semi-supervised Support Vector Machine
SAE	Stacked Auto-Encoder
SCED	Security-Constrained Economic
SG	Smart Grid
SLR	Sparse Logistic Regression
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SVM	Support Vector Machine
TCSEC	Trusted Computing Security Evaluation Criteria
TLS	Transport Layer Security
UIO	Unknown input observation
VPN	Virtual Private Network
ZDA	Zero Dynamics Attacks

References

1. Aleem, S.A.; Hussain, S.M.S.; Ustun, T.S. A review of strategies to increase PV penetration level in smart grids. *Energies* **2020**, *13*, 636. [CrossRef]
2. Ustun, T.S.; Ayyubi, S. Automated network topology extraction based on graph theory for distributed microgrid protection in dynamic power systems. *Electronics* **2019**, *8*, 655. [CrossRef]
3. Ustun, T.S.; Farooq, S.M.; Hussain, S.M.S. Implementing Secure Routable GOOSE and SV Messages Based on IEC 61850-90-5. *IEEE Access* **2020**, *8*, 26162–26171. [CrossRef]
4. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38. [CrossRef]
5. Amin, S.M.; Wollenberg, B. Toward a smart grid: Power delivery for the 21st century. *IEEE Power Energy Mag.* **2005**, *3*, 34–41. [CrossRef]
6. Wang, W.; Xu, Y.; Khanna, M. A survey on the communication architectures in smart grid. *Comput. Netw.* **2011**, *55*, 3604–3629. [CrossRef]
7. Metke, A.R.; Ekl, R.L. Security technology for smart grid networks. *IEEE Trans. Smart Grid* **2010**, *1*, 99–107. [CrossRef]
8. Unsal, D.B.; Koc, A.H.; Yalcinoz, T.; Onaran, I. Medium Voltage and Low Voltage applications of new power line communication model for smart grids. In Proceedings of the 2016 IEEE International Energy Conference, Leuven, Belgium, 4–8 April 2016. [CrossRef]
9. Fan, J.; Borlase, S. The evolution of distribution. *IEEE Power Energy Mag.* **2009**, *7*, 63–68. [CrossRef]
10. Clements, S.; Kirkham, H. Cyber-security considerations for the smart grid. In Proceedings of the 2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008. [CrossRef]
11. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
12. Ustun, T.S.; Ozansoy, C.; Zayegh, A. Recent developments in microgrids and example cases around the world—A review. *Renew. Sustain. Energy Rev.* **2011**, *15*, 4030–4041. [CrossRef]
13. Ustun, T.S.; Hussain, S.M.S. A Review of Cybersecurity Issues in Smartgrid Communication Networks. In Proceedings of the 2019 International Conference on Power Electronics, Control and Automation (ICPECA), New Delhi, India, 16–17 November 2019; Volume 2019. [CrossRef]
14. Ustun, T.S.; Farooq, S.M.; Hussain, S.M.S. A novel approach for mitigation of replay and masquerade attacks in smart grids using IEC 61850 Standard. *IEEE Access* **2019**, *7*, 156044–156053. [CrossRef]
15. Hussain, S.M.S.; Aftab, M.A.; Nadeem, F.; Ali, I.; Ustun, T.S. Optimal Energy Routing in Microgrids with IEC 61850 Based Energy Routers. *IEEE Trans. Ind. Electron.* **2020**, *67*, 5161–5169. [CrossRef]
16. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]
17. Camana Acosta, M.R.; Ahmed, S.; Garcia, C.E.; Koo, I. Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks. *IEEE Access* **2020**, *8*, 19921–19933. [CrossRef]

18. Congressional Research Service. Cybersecurity for Energy Delivery Systems: DOE Programs. Available online: https://crsreports.congress.gov (accessed on 10 October 2020).
19. NIST. *Guidelines for Smart Grid Cybersecurity*; NIST: Gaithersburg, MD, USA, 2014. [CrossRef]
20. Hussain, S.M.S.; Ustun, T.S.; Kalam, A. A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges. *IEEE Trans. Ind. Inform.* **2019**, *16*, 5643–5654. [CrossRef]
21. Godfrey, T.; Mullen, S.; Griffith, D.W.; Golmie, N.; Dugan, R.C.; Rodine, C. Modeling Smart Grid Applications with Co-Simulation. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 291–296. [CrossRef]
22. Kundur, D.; Feng, X.; Liu, S.; Zourntos, T.; Butler-Purry, K.L. Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 244–249. [CrossRef]
23. Lu, G.; De, D.; Song, W.-Z. SmartGridLab: A Laboratory-Based Smart Grid Testbed. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 143–148. [CrossRef]
24. Musleh, A.S.; Chen, G.; Dong, Z.Y. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2020**, *11*, 2218–2234. [CrossRef]
25. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet Things* **2019**, 100111. [CrossRef]
26. Ustun, T.S. Cybersecurity Vulnerabilities of Smart Inverters and Their Impacts on Power System Operation. In Proceedings of the 2019 International Conference on Power Electronics, Control and Automation (ICPECA), New Delhi, India, 16–17 November 2019; Volume 2019. [CrossRef]
27. Cleveland, F. Cyber security issues for Advanced Metering Infrastructure (AMI). In Proceedings of the 2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008. [CrossRef]
28. Farooq, S.M.; Hussain, S.M.S.; Ustun, T.S.; Iqbal, A. Using ID-based Authentication and Key Agreement Mechanism for Securing Communication in Advanced Metering Infrastructure. *IEEE Access* **2020**, *8*, 210503–210512. [CrossRef]
29. Wen, M.H.; Leung, K.-C.; Li, V.O.; He, X.; Kuo, C.-C.J. A survey on smart grid communication system. *APSIPA Trans. Signal Inf. Process.* **2015**, *4*, 1–20. [CrossRef]
30. Norbert Wiener. *Cybernetics or Control and Communication in the Animal and the Machine*; MIT Press: Cambridge, MA, USA, 1965; Volume 25, pp. 210–252.
31. 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]
32. Don Von Dellon. Report to NIST on the Smart Grid Interoperability Standards Roadmap, EPRI, (SB1341-09-CN-0031). January 2009. Available online: http://www.nist.gov/smartgrid/ (accessed on 19 October 2020).
33. Guerrero, J.M.; Vasquez, J.C.; Teodorescu, R. Hierarchical control of droop-controlled DC and AC microgrids—A general approach towards standardization. In Proceedings of the 2009 35th Annual Conference of IEEE Industrial Electronics, Porto, Portugal, 3–5 November 2009; pp. 4305–4310. [CrossRef]
34. Cichonski, P.; Millar, T.; Grance, T.; Scarfone, K. *Computer Security Incident Handling Guide*; National Institute of Standards and Technology Special Publication 800-61 Revision 2; U.S. Department of Commerce: Washington, DC, USA, 2012. [CrossRef]
35. The Smart Grid Interoperability Panel—Smart Grid Cybersecurity Committee. *Guidelines for Smart Grid Cyber Security, Guidelines for Smart Grid Cybersecurity Volume 1—Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*; National Institute of Standards and Technology Publication, Computer Security Division, Information Technology Laboratory 100 Bureau Drive (Mail Stop 8930); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014. [CrossRef]
36. Kiuchi, M.; Serizawa, Y. Security technologies, usage and guidelines in SCADA system networks. In Proceedings of the 2009 ICCAS-SICE, Fukuoka, Japan, 18–21 August 2009; pp. 4607–4612.
37. Rohjans, S.; Uslar, M.; Bleiker, R.; Gonzalez, J.; Specht, M.; Suding, T.; Weidelt, T. Survey of Smart Grid Standardization Studies and Recommendations. In Proceedings of the 2010 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 583–588. [CrossRef]
38. Hauser, C.; Bakken, D.; Bose, A. A failure to communicate: Next generation communication requirements, technologies, and architecture for the electric power grid. *IEEE Power Energy Mag.* **2005**, *3*, 47–55. [CrossRef]
39. Shawkat Ali, A.B.M. *Smart Grids: Opportunities, Developments, and Trends*; Springer: London, UK, 2013.
40. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-physical system security for the electric power grid. *Proc. IEEE* **2012**, *100*, 210–224. [CrossRef]
41. Cárdenas, A. *Securing Cyber-Physical Systems (NISTIR 7916)*; NIST Special Publication: Gaithersburg, MD, USA, 2012.
42. Gallagher, P.; Locke, G. *Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*; NIST Special Publication: Gaithersburg, MD, USA, 2010. Available online: https://www.nist.gov/system/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf (accessed on 23 October 2020).
43. Goel, S.; Hong, Y. *Security Challenges in Smart Grid Implementation*; Springer: London, UK, 2015; pp. 1–39.

44. Cisswg, N. *A Summary of Control System Security Standards Activities in the Energy Sector Enhancing Control Systems Security in the Energy Sector NSTB*; U.S. Department of Energy Office of Electricity Delivery and Energy Reliability Publishing: USA, 2005. Available online: https://www.energy.gov/sites/prod/files/Summary%20of%20CS%20Standards%20Activities%20in%20the%20Energy%20Sector.pdf (accessed on 23 October 2020).
45. Security Architecture and Design/Security Product Evaluation Methods and Criteria. Available online: https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Product_Evaluation_Methods_and_Criteria (accessed on 20 October 2020).
46. Bačić, E.M. The Canadian trusted computer product evaluation criteria. In Proceedings of the Sixth Annual Computer Security Applications Conference, Tucson, AZ, USA, 3–7 December 2002; pp. 188–196. [CrossRef]
47. Harmening, J.T. Chapter 58—Virtual Private Networks. In *Computer and Information Security Handbook*, 3rd ed.; Morgan Kaufmann Publishing (an Imprint of Elsevier Inc.): Burlington, MA, USA, 2017; pp. 843–856, ISBN 978-0-12-803843-7.
48. Bendahmane, A.; Essaaidi, M.; El Moussaoui, A.; Younes, A. Grid computing security mechanisms: State-of-the-art. In Proceedings of the 2009 International Conference on Multimedia Computing and Systems, Ouarzazate, Morocco, 2–4 April 2009; pp. 535–540. [CrossRef]
49. Falk, R.; Fries, S. Smart Grid Cyber Security—An Overview of Selected Scenarios and Their Security Implications. *PIK-Prax. Inf. Kommun.* **2011**, *34*, 168–175. [CrossRef]
50. Sørensen, J.T.; Jaatun, M.G. An analysis of the manufacturing messaging specification protocol. In *Lecture Notes in Computer Science (Including Subse-Ries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer Publishing 5061; Springer: Oslo, Norway, 2008; Volume 5061 LNCS, pp. 602–615. [CrossRef]
51. East, S.; Butts, J.; Papa, M.; Shenoi, S. A taxonomy of attacks on the DNP3 protocol. In *Critical Infrastructure Protection III, IFIP Advances in Information and Communication Technology*; International Federation for Information Processing Publishing: Laxenburg, Austria, 2009; Volume 311, pp. 67–81. [CrossRef]
52. IEEE. IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corri [Online]. Available online: https://standards.ieee.org/standard/802_11-2016.html (accessed on 19 October 2020).
53. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition. NIST Special Publication 800-82*; NIST: Gaithersburg, MD, USA, 2015. [CrossRef]
54. Wang, X.; Yi, P. Security framework for wireless communications in smart distribution grid. *IEEE Trans. Smart Grid* **2011**, *2*, 809–818. [CrossRef]
55. Shaw, R.S.; Chen, C.C.; Harris, A.L.; Huang, H.J. The impact of information richness on information security awareness training effectiveness. *Comput. Educ.* **2009**, *52*, 92–100. [CrossRef]
56. Deng, R.; Chen, J.; Cao, X.; Zhang, Y.; Maharjan, S.; Gjessing, S. Sensing-performance tradeoff in cognitive radio enabled smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 302–310. [CrossRef]
57. Deep, U.D.; Petersen, B.R.; Meng, J. A smart microcontroller-based iridium satellite-communication architecture for a remote renewable energy source. *IEEE Trans. Power Deliv.* **2009**, *24*, 1869–1875. [CrossRef]
58. McGranaghan, M.; Goodman, F. Technical and system requirements for advanced distribution automation. In Proceedings of the 18th International Conference and Exhibition on Electricity Distribution (CIRED 2005), Turin, Italy, 6–9 June 2005; Volume 5, pp. 477–481. [CrossRef]
59. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2*; NIST Special Publication 800-82 rev 2; NIST: Gaithersburg, MD, USA, 2015; pp. 1–157. Available online: http://industryconsulting.org/pdfFiles/NISTDraft-SP800-82.pdf (accessed on 23 August 2020).
60. Barmada, S.; Musolino, A.; Raugi, M.; Rizzo, R.; Tucci, M. A wavelet based method for the analysis of impulsive noise due to switch commutations in Power Line Communication (PLC) systems. *IEEE Trans. Smart Grid* **2011**, *2*, 92–101. [CrossRef]
61. Hasirci, Z.; Cavdar, I.H.; Ozturk, M. Modeling and link performance analysis of busbar distribution systems for narrowband PLC. *Radioengineering* **2017**, *26*, 611–620. [CrossRef]
62. Thomas Basso, R.D. IEEE Smart Grid Series of Standards IEEE 2030 (Interoperability) and IEEE 1547 (Interconnection) Status: Preprint, 2012. Available online: https://www.researchgate.net/publication/254994410_IEEE_Smart_Grid_Series_of_Standards_IEEE_2030_Interoperability_and_IEEE_1547_Interconnection_Status_Preprint (accessed on 20 October 2020).
63. IEEE. 1402–2000—IEEE Guide for Electric Power Substation Physical and Electronic Security—IEEE Standard, 2008 [Online]. Available online: https://ieeexplore.ieee.org/document/836296 (accessed on 21 October 2020).
64. Chan, A.C.F.; Zhou, J. On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. *IEEE Commun. Mag.* **2013**, *51*, 58–65. [CrossRef]
65. Almalawi, A.; Yu, X.; Tari, Z.; Fahad, A.; Khalil, I. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. *ACM Comput. Surv.* **2014**, *53*, 2. [CrossRef]
66. Patel, S.; Yu, Y. Analysis of SCADA Security Models. *Int. Manag. Rev.* **2017**, *3*, 68. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.4461&rep=rep1&type=pdf (accessed on 21 October 2020).
67. Pires, P.S.M.; Oliveira, L.A.H.G. Security aspects of SCADA and corporate network interconnection: An overview. In Proceedings of the International Conference on Dependability of Computer Systems, DepCoS-RELCOMEX 2006, Szklarska Poreba, Poland, 25–27 May 2006; pp. 127–134. [CrossRef]

68. United States Government Accountability Office. Federal facility cybersecurity DHS and GSA Should Address Cyber Risk to Building and Access Control Systems Report to Congressional Requesters United States Government Accountability Office. 2014. Available online: https://www.gao.gov/products/GAO-15-6 (accessed on 21 October 2020).
69. North America Electric Reliability Council. NERC Standard 1300—Cyber Security. 2004. Available online: https://www.nerc.com/pa/Stand/Pages/Cyber-Security-Permanent.aspx (accessed on 20 October 2020).
70. Assante, M.J.; Lee, R.M. The Industrial Control Systems Cyber Kill Chain. In *ICS Cybersecurity: Models for Success*; SANS Technology Institute Publishing: Swansea, UK, 2015.
71. Xue, Y.; Yu, X. Beyond Smart Grid—Cyber-Physical-Social System in Energy Future. *Proc. IEEE* **2017**, *105*, 2290–2292. [CrossRef]
72. Bahati, R.; Gill, H. Cyber-Physical Systems. The Impact of Control Technology. *Open J. Soc. Sci. Sci. Res. Publ.* **2011**, *5*, 161–166. Available online: https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=2154098 (accessed on 29 October 2020).
73. Friedberg, I.; McLaughlin, K.; Smith, P.; Laverty, D.; Sezer, S. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *J. Inf. Secur. Appl.* **2017**, *34*, 183–196. [CrossRef]
74. Adamiak, M.G.; Apostolov, A.; Begovic, M.; Henville, C.; Martin, K.; Michel, G.; Phadke, A.; Thorp, J. Wide area protection—Technology and infrastructures. *IEEE Trans. Power Deliv.* **2006**, *21*, 601–609. [CrossRef]
75. Hashemi-Dezaki, H.; Askarian-Abyaneh, H.; Haeri-Khiavi, H. Impacts of direct cyber-power interdependencies on smart grid reliability under various penetration levels of microturbine/wind/solar distributed generations. *IET Gener. Transm. Distrib.* **2016**, *10*, 928–937. [CrossRef]
76. Jahromi, A.A.; Kemmeugne, A.; Kundur, D.; Haddadi, A. Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes. *IEEE Trans. Power Syst.* **2020**, *35*, 440–450. [CrossRef]
77. Greer, C.; Wollman, D.A.; Prochaska, D.E.; Boynton, P.A.; Mazer, J.A.; Nguyen, C.T.; Fitzpatrick, G.J.; Nelson, T.L.; Koepke, G.H.; Hefner, A.R., Jr.; et al. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*; NIST Special Publication: Gaithersburg, MD, USA, 2014. [CrossRef]
78. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart grids security challenges: Classification by sources of threats. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 468–483. [CrossRef]
79. Cárdenas, A.A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500. [CrossRef]
80. Anderson, R. *Security Engineering—A Guide to Building Dependable Distributed Systems*, 3rd ed.; Wiley: New York, NY, USA, 2008; Volume 2.
81. Tsegay, T. Cybersecurity Solutions for Active Power Distribution Networks. Doctorate Thesis, Lausanne Polytechnic University, Lausanne, Switzerland, 2017.
82. Ayad, A.; Farag, H.; Youssef, A.; El-Saadany, E. Cyber-physical attacks on power distribution systems. *IET Cyber-Phys. Syst. Theory Appl.* **2020**, *5*, 218–225. [CrossRef]
83. Arefifar, S.A.; Mohamed, Y.A.R.I.; El-Fouly, T. Optimized multiple microgrid-based clustering of active distribution systems considering communication and control requirements. *IEEE Trans. Ind. Electron.* **2015**, *62*, 711–723. [CrossRef]
84. Corbett, J.; Wardle, K.; Chen, C. Toward a Sustainable Modern Electricity Grid: The Effects of Smart Metering and Program Investments on Demand-Side Management Performance in the US Electricity Sector 2009–2012. *IEEE Trans. Eng. Manag.* **2018**, *65*, 252–263. [CrossRef]
85. Xu, J.; Wei, L.; Wu, W.; Wang, A.; Zhang, Y.; Zhou, F. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. *Future Gener. Comput. Syst.* **2020**, *108*, 1287–1296. [CrossRef]
86. Tsiatsikas, Z.; Kambourakis, G.; Geneiatakis, D.; Wang, H. The Devil is in the Detail: SDP-Driven Malformed Message Attacks and Mitigation in SIP Ecosystems. *IEEE Access* **2019**, *7*, 2401–2417. [CrossRef]
87. Li, S.; Yilmaz, Y.; Wang, X. Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids. *IEEE Trans. Smart Grid* **2015**, *6*, 2725–2735. [CrossRef]
88. 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 (TAEECE), Beirut, Lebanon, 29 April–1 May 2015; pp. 139–143. [CrossRef]
89. Wang, D.; Guan, X.; Liu, T.; Gu, Y.; Shen, C.; Xu, Z. Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids. *Energies* **2014**, *7*, 1517–1538. [CrossRef]
90. Bou-Harb, E.; Fachkha, C.; Pourzandi, M.; Debbabi, M.; Assi, C. Communication security for smart grid distribution networks. *IEEE Commun. Mag.* **2013**, *51*, 42–49. [CrossRef]
91. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [CrossRef]
92. Kim, J.; Tong, L. On topology attack of a smart grid: Undetectable attacks and countermeasures. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1294–1305. [CrossRef]
93. Huang, Y.L.; Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Tsai, H.Y.; Sastry, S. Understanding the physical and economic consequences of attacks on control systems. *Int. J. Crit. Infrastruct. Prot.* **2019**, *2*, 73–83. [CrossRef]
94. Ustun, T.S.; Hussain, S.M.S. An Improved Security Scheme for IEC 61850 MMS Messages in Intelligent Substation Communication Networks. *J. Mod. Power Syst. Clean Energy* **2020**, *8*, 591–595. [CrossRef]

95. Geneiatakis, D.; Kambourakis, G.; Lambrinoudakis, C.; Dagiuklas, T.; Gritzalis, S. A framework for protecting a SIP-based infrastructure against malformed message attacks. *Comput. Netw.* **2007**, *51*, 2580–2593. [CrossRef]
96. Xiong, Y.; Yang, Z.; Wang, B.; Xun, P.; Deng, T. False sequential command attack of large-scale cyber-physical systems. *Electronics* **2018**, *7*, 176. [CrossRef]
97. Elyashar, A.; Uziel, S.; Paradise, A.; Puzis, R. The Chameleon Attack: Manipulating Content Display in Online Social Media. Available online: http://arxiv.org/abs/2001.05668 (accessed on 29 October 2020).
98. Sagiroglu, S.; Canbek, G. Keyloggers: Increasing threats to computer security and privacy. *IEEE Technol. Soc. Mag.* **2009**, *28*, 10–17. [CrossRef]
99. Gao, Y.; Doan, B.G.; Zhang, Z.; Ma, S.; Zhang, J.; Fu, A.; Nepal, S.; Kim, H. Backdoor Attacks and Countermeasures on Deep Learning: A Comprehensive Review. Available online: https://github.com/ (accessed on 29 October 2020).
100. 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* **2012**, *100*, 195–209. [CrossRef]
101. Fuloria, S.; Anderson, R. Towards a security architecture for substations. In Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, Manchester, UK, 5–7 December 2011. [CrossRef]
102. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*. [CrossRef]
103. Rahman, M.A.; Mohsenian-Rad, H. False data injection attacks with incomplete information against smart power grids. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 3153–3158. [CrossRef]
104. Sou, K.C.; Sandberg, H.; Johansson, K.H. Electric Power Network Security Analysis via Minimum Cut Relaxation. In Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), Orlando, FL, USA, 12–15 December 2011; pp. 4054–4059.
105. Lun, Y.Z.; D'Innocenzo, A.; Smarra, F.; Malavolta, I.; di Benedetto, M.D. State of the art of cyber-physical systems security: An automatic control perspective. *J. Syst. Softw.* **2019**, *149*, 174–216. [CrossRef]
106. 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]
107. Wang, D.; Guan, X.; Liu, T.; Gu, Y.; Sun, Y.; Liu, Y. A survey on bad data injection attack in smart grid. In Proceedings of the 2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Hong Kong, China, 8–11 December 2013. [CrossRef]
108. Guan, Z.; Sun, N.; Xu, Y.; Yang, T. A comprehensive survey of false data injection in smart grid. *Int. J. Wirel. Mob. Comput.* **2015**, *8*, 27–33. [CrossRef]
109. Deng, R.; Zhuang, P.; Liang, H. False Data Injection Attacks Against State Estimation in Power Distribution Systems. *IEEE Trans. Smart Grid* **2019**, *10*, 2871–2881. [CrossRef]
110. Liu, X.; Li, Z. False data attack models, impact analyses and defense strategies in the electricity grid. *Electr. J.* **2017**, *30*, 35–42. [CrossRef]
111. Ashrafuzzaman, M.; Chakhchoukh, Y.; Jillepalli, A.A.; Tosic, P.T.; De Leon, D.C.; Sheldon, F.T.; Johnson, B.K. Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 219–225. [CrossRef]
112. Zhu, J. *Optimization of Power System Operation*, 2nd ed.; Wiley-IEEE Press: Piscataway, NJ, USA, 2015; Print ISBN: 9781118854150, Online ISBN: 9781118887004. [CrossRef]
113. Peng, D.; Dong, J.; Jian, J.; Peng, Q.; Zeng, B.; Mao, Z.H. Economic-driven FDI attack in electricity market. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Blue Eyes Intelligence Engineering and Sciences Publication: Bhopal, India, 2018; Volume 11287 LNCS, pp. 216–224. [CrossRef]
114. Liu, X.; Li, Z. Trilevel Modeling of Cyber Attacks on Transmission Lines. *IEEE Trans. Smart Grid* **2017**, *8*, 720–729. [CrossRef]
115. Kang, J.W.; Joo, I.Y.; Choi, D.H. False Data Injection Attacks on Contingency Analysis: Attack Strategies and Impact Assessment. *IEEE Access* **2018**, *6*, 8841–8851. [CrossRef]
116. Yu, W. False Data Injection Attacks in Smart Grid: Challenges and Solutions, NIST Cyber Security for CPS Workshop, 23–24 April 2012, 8000 York Rd, Towson, MD 21252, USA. Available online: http://www.towson.edu/~{}wyu (accessed on 5 January 2021).
117. Aoufi, S.; Derhab, A.; Guerroumi, M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *J. Inf. Secur. Appl.* **2020**, *54*. [CrossRef]
118. Ericsson, G.N. Cyber security and power system communication essential parts of a smart grid infrastructure. *IEEE Trans. Power Deliv.* **2010**, *25*, 1501–1507. [CrossRef]
119. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Generalized FDIA-Based Cyber Topology Attack with Application to the Australian Electricity Market Trading Mechanism. *IEEE Trans. Smart Grid* **2018**, *9*, 3820–3829. [CrossRef]
120. Sridhar, S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. [CrossRef]
121. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. Revealing stealthy attacks in control systems. In Proceedings of the 2012 50th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2012, Monticello, IL, USA, 1–5 October 2012; pp. 1806–1813. [CrossRef]

122. Pasqualetti, F.; Dorfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Automat. Contr.* **2013**, *58*, 2715–2729. [CrossRef]
123. Yu, X.; Xue, Y. Smart Grids: A Cyber–Physical Systems Perspective. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7433937 (accessed on 3 November 2020).
124. Savin, V.D.; Serban, C. Cybersecurity Vulnerabilities and Threats of Scada Systems in Critical Infrastructures. In Proceedings of the IMC, Amsterdam, The Netherlands, 1–3 October 2019; Volume 13, pp. 234–237. Available online: https://ideas.repec.org/a/rom/mancon/v13y2019i1p234-237.html (accessed on 29 October 2020).
125. Esmalifalak, M.; Member, S.; Liu, L.; Member, S. Machine Learning in Smart Grid. *IEEE Syst. J.* **2014**, *11*, 1644–1652. [CrossRef]
126. Lan, T.; Wang, W.; Huang, G.M. False data injection attack in smart grid topology control: Vulnerability and countermeasure. In Proceedings of the IEEE Power and Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017; Volume 2018-January, pp. 1–5. [CrossRef]
127. Musleh, A.S.; Debouza, M.; Khalid, H.M.; Al-Durra, A. Detection of False Data Injection Attacks in Smart Grids: A Real-Time Principle Component Analysis. In Proceedings of the IECON 2019—45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, 14–17 October 2019; Volume 2019-October, pp. 2958–2963. [CrossRef]
128. Zhang, M.; Shen, C.; He, N.; Han, S.; Li, Q.; Wang, Q.; Guan, X. *False Data Injection Attacks Against Smart Grid State Estimation: Construction, Detection and Defense*; China Technological Sciences; Springer Nature Switzerland AG, Springer: Cham, Switzerland, 2019; Volume 62, pp. 2077–2087. [CrossRef]
129. Yuan, Y.; Li, Z.; Ren, K. Modeling load redistribution attacks in power systems. *IEEE Trans. Smart Grid* **2011**, *2*, 382–390. [CrossRef]
130. Musleh, A.S.; Khalid, H.M.; Muyeen, S.M.; Al-Durra, A. A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications. *IEEE Syst. J.* **2019**, *13*, 710–719. [CrossRef]
131. He, Y.; Mendis, G.J.; Wei, J. Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [CrossRef]
132. Yang, Q.; Yang, J.; Yu, W.; An, D.; Zhang, N.; Zhao, W. On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures Bad Data Injection in Smart Grid—Attack and Defense Mechanisms. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 1–11.
133. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [CrossRef]
134. Hendrickx, J.M.; Johansson, K.H.; Jungers, R.M.; Sandberg, H.; Sou, K.C. Efficient computations of a security index for false data attacks in power networks. *IEEE Trans. Automat. Contr.* **2014**, *59*, 3194–3208. [CrossRef]
135. Wallace, S.; Zhao, X.; Nguyen, D.; Lu, K.T. Big Data Analytics on a Smart Grid: Mining PMU Data for Event and Anomaly Detection. In *Big Data: Principles and Paradigms*; Elsevier Inc.: San Leandro, CA, USA, 2016; pp. 417–429.
136. Pan, S.J.; Yang, Q. A survey on transfer learning. *IEEE Trans. Knowl. Data Eng.* **2010**, *22*, 1345–1359. [CrossRef]
137. Ozay, M.; Esnaola, I.; Vural, F.T.Y.; Kulkarni, S.R.; Poor, H.V. Machine Learning Methods for Attack Detection in the Smart Grid. *IEEE Trans. Neural Networks Learn. Syst.* **2016**, *27*, 1773–1786. [CrossRef]
138. Buzau, M.M.; Tejedor-Aguilera, J.; Cruz-Romero, P.; Gomez-Exposito, A. Detection of non-technical losses using smart meter data and supervised learning. *IEEE Trans. Smart Grid* **2019**, *10*, 2661–2670. [CrossRef]
139. Hink, B.; Beaver, J.M.; Buckner, M.A.; Morris, T.; Adhikari, U.; Pan, S. Machine learning for power system disturbance and cyber-attack discrimination. In Proceedings of the 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 August 2014. [CrossRef]
140. Pan, S.; Morris, T.; Adhikari, U. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. *IEEE Trans. Smart Grid* **2015**, *6*, 3104–3113. [CrossRef]
141. Kurt, M.N.; Yilmaz, Y.; Wang, X. Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 498–513. [CrossRef]
142. Khalaf, M.; Youssef, A.; El-Saadany, E. Joint Detection and Mitigation of False Data Injection Attacks in AGC Systems. *IEEE Trans. Smart Grid* **2018**. [CrossRef]
143. Karimipour, H.; Dinavahi, V. Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack. *IEEE Access* **2017**, *6*, 2984–2995. [CrossRef]
144. Khalid, H.M.; Peng, J.C.H. Immunity Toward Data-Injection Attacks Using Multisensor Track Fusion-Based Model Prediction. *IEEE Trans. Smart Grid* **2017**, *8*, 697–707. [CrossRef]
145. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* **2017**, *11*, 1644–1652. [CrossRef]
146. Wang, X.; Luo, X.; Zhang, M.; Guan, X. Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers. *Int. J. Electr. Power Energy Syst.* **2019**, *110*, 208–222. [CrossRef]
147. Jindal, A.; Dua, A.; Kaur, K.; Singh, M.; Kumar, N.; Mishra, S. Decision Tree and SVM-Based Data Analytics for Theft Detection in Smart Grid. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1005–1016. [CrossRef]
148. Wang, Y.; Amin, M.M.; Fu, J.; Moussa, H.B. A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids. *IEEE Access* **2017**, *5*, 26022–26033. [CrossRef]
149. Jokar, P.; Arianpoo, N.; Leung, V.C.M. Electricity theft detection in AMI using customers' consumption patterns. *IEEE Trans. Smart Grid* **2016**, *7*, 216–226. [CrossRef]

150. Messinis, G.M.; Rigas, A.E.; Hatziargyriou, N.D. A Hybrid Method for Non-Technical Loss Detection in Smart Distribution Grids. *IEEE Trans. Smart Grid* **2019**, *10*, 6080–6091. [CrossRef]
151. Costa, B.C.; Alberto, B.L.A.; Portela, A.M.; Maduro, W.; Eler, E.O. Fraud Detection in Electric Power Distribution Networks using an Ann-Based Knowledge-Discovery Process. *Int. J. Artif. Intell. Appl.* **2013**, *4*, 17–23. [CrossRef]
152. Liu, X.; Nielsen, P.S. Regression-based Online Anomaly Detection for Smart Grid Data. January 2016. Available online: http://arxiv.org/abs/1606.05781 (accessed on 9 November 2020).
153. de Nadai, M.; van Someren, M. Short-term anomaly detection in gas consumption through ARIMA and Artificial Neural Network forecast. In Proceedings of the 2015 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS) Proceedings, Trento, Italy, 9–10 July 2015; pp. 250–255. [CrossRef]
154. Punmiya, R.; Choe, S. Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing. *IEEE Trans. Smart Grid* **2019**, *10*, 2326–2329. [CrossRef]
155. Ayad, A.; Farag, H.E.Z.; Youssef, A.; El-Saadany, E.F. Detection of false data injection attacks in smart grids using Recurrent Neural Networks. In Proceedings of the 2018 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 19–22 February 2018; pp. 1–5. [CrossRef]
156. Yao, D.; Wen, M.; Liang, X.; Fu, Z.; Zhang, K.; Yang, B. Energy Theft Detection with Energy Privacy Preservation in the Smart Grid. *IEEE Internet Things J.* **2019**, *6*, 7659–7669. [CrossRef]
157. Hu, T.; Guo, Q.; Shen, X.; Sun, H.; Wu, R.; Xi, H. Utilizing Unlabeled Data to Detect Electricity Fraud in AMI: A Semisupervised Deep Learning Approach. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, *30*, 3287–3299. [CrossRef]
158. Yang, C.; Wang, Y.; Zhou, Y.; Ruan, J.; Liu, W. False Data Injection Attacks Detection in Power System Using Machine Learning Method. *J. Comput. Commun.* **2018**, *06*, 276–286. [CrossRef]
159. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting False Data Injection Attacks in AC State Estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
160. Kurt, M.N.; Ogundijo, O.; Li, C.; Wang, X. Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach. *IEEE Trans. Smart Grid* **2018**, *10*, 5174–5185. [CrossRef]
161. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest. *IEEE Trans. Forensics Secur.* **2019**, *14*, 2765–2777. [CrossRef]
162. Wang, J.; Shi, D.; Li, Y.; Chen, J.; Ding, H.; Duan, X. Distributed Framework for Detecting PMU Data Manipulation Attacks with Deep Autoencoders. *IEEE Trans. Smart Grid* **2019**, *10*, 4401–4410. [CrossRef]
163. Li, W.; Logenthiran, T.; Phan, V.T.; Woo, W.L. A novel smart energy theft system (SETS) for IoT-based smart home. *IEEE Internet Things J.* **2019**, *6*, 5531–5539. [CrossRef]
164. Niu, X.; Li, J.; Sun, J.; Tomsovic, K. Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning. In Proceedings of the 2019 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019. [CrossRef]
165. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. A framework for cyber-topology attacks: Line-switching and new attack scenarios. *IEEE Trans. Smart Grid* **2019**, *10*, 1704–1712. [CrossRef]
166. Barreto, C.; Koutsoukos, X. Design of Load Forecast Systems Resilient Against Cyber-Attacks. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer Nature Switzerland AG: Cham, Switzerland, 2019; Volume 11836 LNCS, pp. 1–20. [CrossRef]
167. Cui, M.; Wang, J.; Yue, M. Machine Learning-Based Anomaly Detection for Load Forecasting Under Cyberattacks. *IEEE Trans. Smart Grid* **2019**, *10*, 5724–5734. [CrossRef]
168. Zhou, R.; Cui, Q.; Hao, J. A reliability evaluation method of high reliability products based on evidence fusion. *System Eng. Theory Pract.* **2018**, *38*, 2979–2986. [CrossRef]
169. Chakhchoukh, Y.; Liu, S.; Sugiyama, M.; Ishii, H. Statistical outlier detection for diagnosis of cyber attacks in power state estimation. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5. [CrossRef]
170. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M. Real Time Security Assessment of the Power System Using a Hybrid Support Vector Machine and Multilayer Perceptron Neural Network Algorithms. *Sustainability* **2019**, *11*, 3586. [CrossRef]
171. Sun, M.; Konstantelos, I.; Strbac, G. C-Vine Copula Mixture Model for Clustering of Residential Electrical Load Pattern Data. *IEEE Trans. Power Syst.* **2017**, *32*, 2382–2393. [CrossRef]
172. Ahmed, S.; Lee, Y.; Hyun, S.-H.; Koo, I. Covert Cyber Assault Detection in Smart Grid Networks Utilizing Feature Selection and Euclidean Distance-Based Machine Learning. *Appl. Sci.* **2018**, *8*, 772. [CrossRef]
173. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Feature Selection-Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning. *IEEE Access* **2018**, *6*, 27518–27529. [CrossRef]
174. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning, Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
175. Wei, L.; Rondon, L.P.; Moghadasi, A.; Sarwat, A.I. Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid. In Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference, Denver, CO, USA, 16–19 April 2018. [CrossRef]

176. Krishna, V.B.; Weaver, G.A.; Sanders, W.H. PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure | TCIPG: Trustworthy Cyber Infrastructure for the Power Grid. Available online: https://tcipg.org/publications/pca-based-method-detecting-integrity-attacks-advanced-metering-infrastructure.html (accessed on 12 November 2020).
177. Hao, J.; Piechocki, R.J.; Kaleshi, D.; Chin, W.H.; Fan, Z. Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids. *IEEE Trans. Ind. Inform.* **2015**, *11*, 1198–1209. [CrossRef]
178. Amin, S.; Schwartz, G.A.; Cardenas, A.A.; Sastry, S.S. Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure. *IEEE Control Syst.* **2015**, *35*, 66–81. [CrossRef]
179. Wang, H.; Ruan, J.; Wang, G.; Zhou, B.; Liu, Y.; Fu, X.; Peng, J.-C. Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4766–4778. [CrossRef]
180. Zhou, T.; Tao, D. GoDec: Randomized Low rank & Sparse Matrix Decomposition in Noisy Case. In Proceedings of the International Conference on Machine Learning, ICML 2011, Bellevue, WA, USA, 28 June–2 July 2011; pp. 33–40.
181. Li, B.; Ding, T.; Huang, C.; Zhao, J.; Yang, Y.; Chen, Y. Detecting False Data Injection Attacks Against Power System State Estimation with Fast Go- Decomposition (GoDec) Approach. *IEEE Trans. Ind. Inform.* **2018**. [CrossRef]
182. Morrow, K.L.; Heine, E.; Rogers, K.M.; Bobba, R.B.; Overbye, T.J. Topology Perturbation for Detecting Malicious Data Injection. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 2104–2113.
183. Kuntz, K.; Smith, M.; Wedeward, K.; Collins, M. Detecting, locating, & quantifying false data injections utilizing grid topology through optimized D-FACTS device placement. In Proceedings of the 2014 North American Power Symposium (NAPS), Pullman, WA, USA, 7–9 September 2014; pp. 1–6.
184. Ganjkhani, M.; Fallah, S.N.; Badakhshan, S.; Shamshirband, S.; Chau, K.-W. A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation. *Energies* **2019**, *12*, 2209. [CrossRef]
185. Candes, E. Robust Principal Component Analysis? *J. ACM* **2011**, *58*, 11. [CrossRef]
186. Xie, L.; Mo, Y.; Sinopoli, B. Integrity data attacks in power market operations. *IEEE Trans. Smart Grid* **2011**, *2*, 659–666. [CrossRef]
187. Kim, J.; Tong, L.; Thomas, R.J. Subspace Methods for Data Attack on State Estimation: A Data Driven Approach. *IEEE Trans. Signal Process.* **2015**, *63*, 1102–1114. [CrossRef]
188. Higgins, M.; Teng, F.; Parisini, T. Stealthy MTD Against Unsupervised Learning-Based Blind FDI Attacks in Power Systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1275–1287. [CrossRef]
189. Yu, Z.; Chin, W. Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 1219–1226. [CrossRef]
190. Anwar, A.; Mahmood, A.N.; Pickering, M. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. *J. Comput. Syst. Sci.* **2017**, *83*, 58–72. [CrossRef]
191. Xie, S.; Yang, J.; Xie, K.; Liu, Y.; He, Z. Low-sparsity unobservable attacks against smart grid: Attack exposure analysis and a data driven attack scheme. *IEEE Access* **2017**, *5*, 8183–8193. [CrossRef]
192. Chin, W.L.; Lee, C.H.; Jiang, T. Blind false data attacks against AC state estimation based on geometric approach in smart grid communications. *IEEE Trans Smart Grid.* **2017**. [CrossRef]
193. ISO/IEC 27000: 2018 International Standard, Information technology—Security techniques—Information security management systems—Overview and vocabulary. Available online: https://www.iso.org/standard/73906.html (accessed on 23 November 2020).
194. Maynard, P.; McLaughlin, K. *Towards Understanding Man-in-the-Middle Attacks on IEC 60870-5-104 SCADA Networks*, 2nd ed.; International Symposium for ICS & SCADA Cyber Security Research: St Polten, Austria, 2014; pp. 1–11.
195. IEEE Std 2030–2011 Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads. Available online: http://grouper.ieee.org/groups/scc21/dr_shared/2030/ (accessed on 27 November 2020).
196. National Institute of Standards and Technology. *Announcing the Advanced Encryption Standard (AES)*; Federal Information Processing Standards Publication; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001.
197. U.S. Department of Commerce. *Data Encryption Standard (DES)*; Federal Information Processing Standards (FIPS) Publication 46-7; U.S. Department of Commerce: Washington, DC, USA, 1999.
198. IEEE 1547 Series of Standards. Available online: http://grouper.ieee.org/groups/scc21/dr_shared/ (accessed on 19 January 2021).
199. Davis, M. Recoverable Advanced Metering Infrastructure. In Proceedings of the Black Hat security conference, Las Vegas, NV, USA, 3–8 August 2019. Available online: https://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html (accessed on 21 January 2021).
200. Lauriat, N. *NERC 1200 and CIP-002 through CIP-009 Comparison*; Network & Security Technologies: Pearl River, NY, USA, 2006. Available online: http://www.netsectech.com/wp-content/uploads/2013/05/WP_NERC_CIP_Analysis_NST.pdf (accessed on 23 January 2021).
201. Byres, E. Revealing Network Threats, Fears: How to Use ANSI/ISA-99 Standards to Improve Control System Security. 2006. Available online: https://www.tofinosecurity.com/system/files/Professional/Articles/Intech-Jan-Feb-2011-Using-ISA99.pdf (accessed on 27 January 2021).

1 result from Web of Science Core Collection for:

Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation (Title)

Copy query link

Publications You may also like...

New default sort order

You may notice your results look different than classic Web of Science.

Previously, the default sort order for search results was **Date - Newest to Oldest**. In the new Web of Science, the default search order is **Relevance**.

If you want to change the sort order, you can do so with this dropdown menu.

Refine results

Search within results for...

Quick Filters

- Review Articles 1
- Open Access 1

Publication Years

- 2021 1

Document Types

- Review Articles 1

Web of Science Categories

- Energy Fuels 1

Authors

- Hussain SMS 1
- Onen A 1
- Unsal DB 1
- Ustun TS 1

Affiliations

- ABDULLAH GUL UNIVERSITY 1
- CUMHURIYET UNIVERSITY 1
- NATIONAL INSTITUTE OF ADVANCED INDUS… 1

Publication Titles

- ENERGIES 1

Publishers

- Mdpi 1

Funding Agencies

Open Access

Editorial Notices

Editors

Group Authors

Research Areas

0/1 Add To Marked List Export Sort by: **Relevance** 1 of 1

1 Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation

Unsal, DB; Ustun, TS; (...); Onen, A

May 2021 | ENERGIES 14 (9)

…recedented opportunities in optimization and control fields. …ter understanding of the pseudo-real-time condition of power …his is the key towards mitigating negative … Show more

1 Citation

199 References

Related records

ENERGIES

Journal Impact Factor™

2020	Five Year
3.004	3.085

JCR Category	Category Rank	Category Quartile
ENERGY & FUELS *in SCIE edition*	70/114	Q3

Source: Journal Citation Reports™ 2020

Page size 1 of 1

1 record match

Free Full Text from Publisher Export Add To Marked List 1 of 1

Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation

By: Unsal, DB (Unsal, Derya Betul) [1] ; Ustun, TS (Ustun, Taha Selim) [2] ; Hussain, SMS (Hussain, S. M. Suhail) [2] ; Onen, A (Onen, Ahmet) [3]

View Web of Science ResearcherID and ORCID (provided by Clarivate)

ENERGIES

Volume: 14 **Issue:** 9

Article Number: 2657

DOI: 10.3390/en14092657

Published: MAY 2021

Indexed: 2021-06-05

Document Type: Review

Abstract

Integration of information technologies with power systems has unlocked unprecedented opportunities in optimization and control fields. Increased data collection and monitoring enable control systems to have a better understanding of the pseudo-real-time condition of power systems. In this fashion, more accurate and effective decisions can be made. This is the key towards mitigating negative impacts of novel technologies such as renewables and electric vehicles and increasing their share in the overall generation portfolio. However, such extensive information exchange has created cybersecurity vulnerabilities in power systems that were not encountered before. It is imperative that these vulnerabilities are understood well, and proper mitigation techniques are implemented. This paper presents an extensive study of cybersecurity concerns in Smart grids in line with latest developments. Relevant standardization and mitigation efforts are discussed in detail and then the classification of different cyber-attacks in smart grid domain with special focus on false data injection (FDI) attack, due to its high impact on different operations. Different uses of this attack as well as developed detection models and methods are analysed. Finally, impacts on smart grid operation and current challenges are presented for future research directions.

Keywords

Author Keywords: smart grid cybersecurity; false data injection; power system operation; power system protection; cybersecurity attacks; intruder detection; cybersecurity for scada systems

Keywords Plus: ELECTRICITY THEFT DETECTION; CYBER-PHYSICAL ATTACKS; STATE ESTIMATION; SECURITY; COMMUNICATION; SYSTEM; STRATEGIES; PROTECTION; MESSAGES

Author Information

Corresponding Address: Unsal, Derya Betul (corresponding author)

Cumhuriyet Univ, Dept Energy Sci & Technol, Renewable Energy Res Ctr, TR-58140 Sivas, Turkey

Addresses:

1 Cumhuriyet Univ, Dept Energy Sci & Technol, Renewable Energy Res Ctr, TR-58140 Sivas, Turkey

2 AIST FREA, Fukushima Renewable Energy Inst, Koriyama, Fukushima 9630298, Japan

3 Abdullah Gul Univ, Dept Elect & Elect Engn, TR-38170 Kayseri, Turkey

E-mail Addresses: dbunsal@cumhuriyet.edu.tr; selim.ustun@aist.go.jp; suhail@ieee.org; ahmet.onen@agu.edu.tr

Categories/Classification

Research Areas: Energy & Fuels

+ See more data fields

Journal information

ENERGIES

eISSN: 1996-1073

Current Publisher: MDPI, ST ALBAN-ANLAGE 66, CH-4052 BASEL, SWITZERLAND

Research Areas: Energy & Fuels

Web of Science Categories: Energy & Fuels

3.004

Journal Impact Factor ™ (2020)

Citation Network

In Web of Science Core Collection

1

Citation

Create citation alert

1

Tim

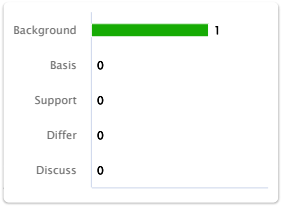
Data

Click here to be sent an email when this publication is cited.

+ See more times cited

Citing items by classification New

Breakdown of how this article has been mentioned, based on available citation context data and snippets from 1 citing item(s).



Ciornei, I; Kyriakides, E;
Recent methodologies and approaches for the economic dispatch of generation in power systems
INTERNATIONAL TRANSACTIONS ON ELECTRICAL ENERGY SYSTEMS

Hu, ZJ; Liu, SC; Wu, LG; et al.
Intrusion-Detector-Dependent Distributed Economic Model Predictive Control for Load Frequency Regulation With PEVs Under Cyber Attacks
IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I-REGULAR PAPERS

Neergheen-Bhujun, V; Awan, AT; Kagansky, A; et al.
Biodiversity, drug discovery, and the future of global health: Introducing the biodiversity to biomedicine consortium, a call to action
JOURNAL OF GLOBAL HEALTH

Pazouki, S; Bibek, KC; Asrari, A; et al.
Modelling of Smart Homes Affected by Cyberattacks
2020 52ND NORTH AMERICAN POWER SYMPOSIUM (NAPS)

Basumallik, S; Ma, R; Eftekharnejad, S;
Packet-data anomaly detection in PMU-based state estimator using convolutional neural network
INTERNATIONAL JOURNAL OF ELECTRICAL POWER & ENERGY SYSTEMS

See all

Most Recently Cited by

Liu, R; Mustafa, HM; Srivastava, AK; et al.
Reachability-Based False Data Injection Attacks and Defence Mechanisms for Cyberpower System
ENERGIES

Use in Web of Science

Web of Science Usage Count

7
Last 180 Days

11
Since 2013

Learn more