

Review

Cyber-Security of Smart Microgrids: A Survey

Farzam Nejabatkhah ^{1,*}, Yun Wei Li ², Hao Liang ² and Rouzbeh Reza Ahrabi ²

¹ CYME International T&D, Eaton, Saint-Bruno, QC J3V 3P8, Canada

² Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada; yunwei.li@ualberta.ca (Y.W.L.); hao2@ualberta.ca (H.L.); rezaahra@ualberta.ca (R.R.A.)

* Correspondence: FarzamNejabatkhah@eaton.com

Abstract: In this paper, the cyber-security of smart microgrids is thoroughly discussed. In smart grids, the cyber system and physical process are tightly coupled. Due to the cyber system's vulnerabilities, any cyber incidents can have economic and physical impacts on their operations. In power electronics-intensive smart microgrids, cyber-attacks can have much more harmful and devastating effects on their operation and stability due to low inertia, especially in islanded operation. In this paper, the cyber-physical systems in smart microgrids are briefly studied. Then, the cyber-attacks on data availability, integrity, and confidentiality are discussed. Since a false data injection (FDI) attack that compromises the data integrity in the cyber/communication network is one of the most challenging threats for smart microgrids, it is investigated in detail in this paper. Such FDI attacks can target state estimation, voltage and frequency control, and smart microgrids' protection systems. The economic and physical/technical impacts of the FDI attacks on smart microgrids are also reviewed in this paper. The defensive strategies against FDI attacks are classified into protection strategies, in which selected meter measurements are protected, and detection/mitigation strategies, based on either static or dynamic detection. In this paper, implementation examples of FDI attacks' construction and detection/mitigation in smart microgrids are provided. Samples of recent cyber-security projects in the world, and critical cyber-security standards of smart grids, are presented. Finally, future trends of cyber-security in smart microgrids are discussed.



Citation: Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. <https://dx.doi.org/10.3390/en14010027>

Received: 25 November 2020

Accepted: 20 December 2020

Published: 23 December 2020

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



Copyright: © 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: cyber-physical system; cyber-security; cyber-attacks; power electronics converters; smart microgrids

1. Introduction

In recent years, the development of smart grids is increasing rapidly. The smart grids encompass interconnected clusters of AC-DC microgrids, in which smart power electronics converters are widely used to interface distributed generations (DGs) and energy storage as well as loads. In such microgrids, information and communication technologies play a crucial role in their operation and control. Since the cyber system and the physical process are tightly coupled, any cyber incidents can impact their reliable operations. In other words, power electronics-intensive microgrids operation depends on efficient and reliable data flows in the cyber system. Any delay or corruption of data may affect the physical system's smooth operation and jeopardize smart grids' efficiency, stability, and safety [1,2]. For example, it is estimated that the U.S. PV and wind installations reach around 16,000 MWdc and 11GW in 2021, respectively, which will require around 2081 MW energy storage deployment [3,4]. Increasing renewable generations and energy storage resources and emerging loads such as electric vehicles require more coordination and reliable cyber system for proper operation.

Different cyber incidents have resulted in massive electric power outages, where Italy blackout in 2003 (affected more than 56 million customers), Arizona Blackout in 2007 (affected more than 100,000 customers), Florida blackout (affected more than 1 million customers), and Southwest blackout (affected more than 2.7 million customers), and

Ukraine blackout in 2016 were all wake-up calls [5]. Based on the study, a blackout across 15 U.S. states would affect 93 million people, which cost between 243 billion and 1 trillion dollars [6,7].

Considering the disruptive effects of cyber-attacks and smart grids' vulnerability, several projects and plans have been initiated recently. The federal governments of the United States and Canada have started a collaborative effort to protect the emerging power grid from cyber-attacks (National Electric Grid Security and Resilience action plan). Moreover, the Department of Energy (DoE) of the United States has initiated several projects addressing cyber-security issues. For example, the DoE has funded \$12.2 million for the Secure Evolvable Energy Delivery Systems (SEEDS) project at the University of Arkansas. In another project, the DoE has funded \$28.1 million for a project called Cyber Resilient Energy Delivery Consortium (CREDC) at the University of Illinois, Urbana-Champaign. In addition to North American projects, the European Union has funded the Smart Grid Protection Against Cyber-Attacks (SPARKS) project considering EU energy objectives for 2030. In Section 3, examples of projects on cyber-security will be provided.

Data should meet three fundamental requirements in the cyber system; (1) availability where data are timely and accessible, (2) integrity in which data are accurate and trustworthy, and (3) Confidentiality where data are viewed and used by an authorized person. Among different cyber-attacks, a false data injection (FDI) attack targeting data integrity is one of the most challenging smart grid threats. If such attacks are crafted intelligently, they can penetrate the system without being detected by the conventional attack detection method [8,9]. Those attacks are also called stealth attacks [10–12]. The successful FDI attack could introduce major economic problems as well as steady-state and dynamic stability issues. Please refer to the U.S. Department of Energy GMLC project in [13] for more information on distinguishing cyber events from physical events.

The smart grids' cyber-physical systems and their security have been studied in some literature, such as in [1,14–17]. In [1], the importance of cyber-security in microgrids operation and control are discussed in general. The common cyber vulnerabilities in microgrids are addressed, and the potential risks of cyber-attacks are studied. The cyber-physical electrical energy systems are thoroughly reviewed in [14], and their critical scientific problems, including co-simulation, the interaction between energy and information networks, failure in the communication system, and security of the cyber-physical system, are discussed. The FDI attacks in power systems are studied in [15]. In addition to the theoretical basis, the impacts of successful FDI attacks on power systems are studied. Although such surveys provide valuable discussions on cyber-physical systems and smart power systems' security, they do not address smart microgrids with AC-DC subgrids and high penetration of power electronics converters in detail.

In smart microgrids with high penetration of power electronics converters, the cyber-attacks can be much harmful. Although the optimal economical operation is not the primary concern in such microgrids, cyber-attacks could have devastating effects on microgrids' stability, especially in islanded mode. In other words, due to the low inertia of such microgrids, the cyber-attacks could affect the transient and steady-state stability of microgrids. Further, in the hybrid AC-DC microgrids, any cyber-attack in either AC or DC subgrid will affect the other side. For instance, if any cyber-attack affects the AC subgrid's frequency stability, it will affect DC voltage stability on the DC side through AC-DC subgrids interlinking power converters. Considering the future roadmap of smart microgrids (e.g., E-LANs and IoE), the cyber-security will receive more and more attention in the near future.

In this paper, the cyber-security of smart microgrids is studied. First, the cyber-physical systems in smart microgrids and their challenges are presented in Section 2. In Section 3, examples of current cyber-security projects are provided in detail. A few critical standards and protocols associated with cyber-security of smart grids are discussed in Section 4. In Section 5, the cyber-attacks on data availability, integrity, and confidentiality are studied. Due to the importance and devastating effects of FDI attacks targeting data

integrity, the rest of the paper studies the FDI attacks. The economic and physical/technical impacts of FDI attacks on smart microgrids are addressed in Section 6. In Section 7, various construction methods of FDI attacks targeting state estimation, voltage and frequency regulations, and protection systems in smart microgrids are reviewed. In Section 8, different defensive strategies against FDI attacks are addressed. The implementation examples of cyber-attack construction, impact, and defensive strategy are provided in Section 9. Finally, future trends of cyber-security in smart microgrids are discussed in Section 10.

2. Cyber-Physical Systems in Smart Microgrids and Challenges

2.1. Cyber-Physical System

The smart microgrids are dominated by power electronics converters used for interfacing distributed generations and energy storage and loads. In such systems, the physical, electrical components are tightly interconnected by information and communication technologies, and their operations are tightly coupled to cyber system functionality. In Figure 1, a typical power electronics-intensive smart microgrid with the cyber-physical networks is shown.

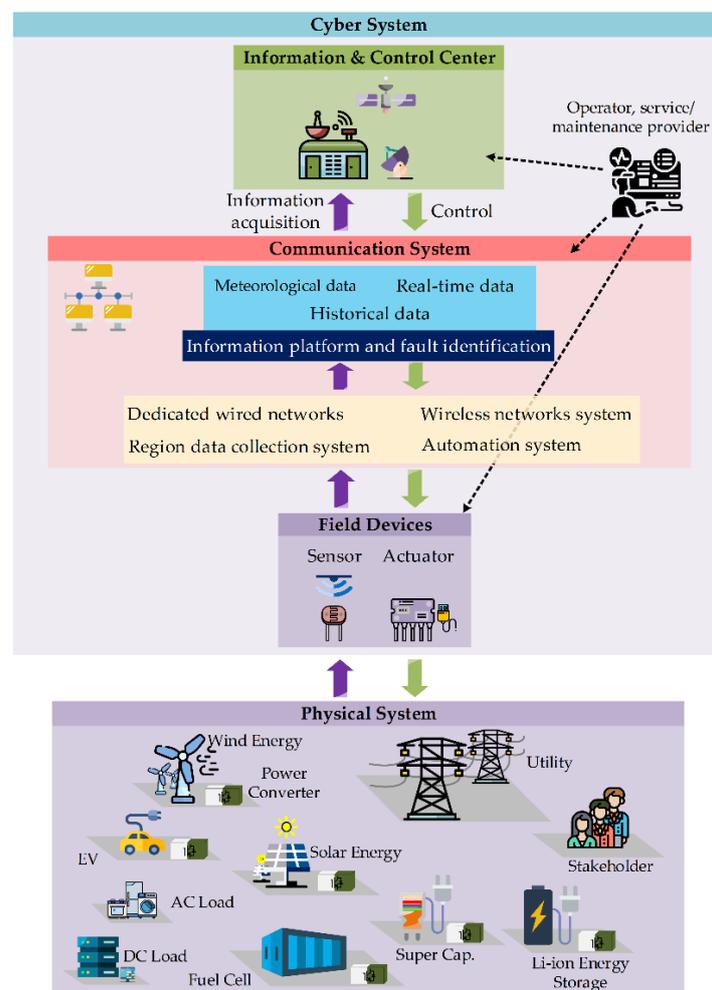


Figure 1. A typical smart microgrid with cyber-physical systems.

The smart microgrid's cyber-physical model includes four layers in general; (1) physical power system layer, (2) sensor and actuator layer, (3) communication layer, and (4) management and control layer. In the following, brief explanations about layers are provided.

The physical layer contains the microgrid's power components, such as transformers, generators, power electronics converters, circuit breakers, and loads.

The sensor and actuator layer consists of sensors and measurement devices, and devices to implement the control decisions (made in the management layer). The sensors and measurement devices are responsible for measuring information about the system's state, including voltage, frequency, current, and circuit breaker status. The actuators and control devices include generator controllers, distributed generation controllers, and relays of circuit breakers.

The communication layer consists of devices such as routers, switches, and the communication medium and is responsible for information exchange among relevant layers. In smart microgrids, the communication system can be wired or wireless, depending on system requirements.

The management layer is a central control system that is responsible for the microgrid operation under different conditions. This layer receives measurement layer data through the communication layer and produces control signals for the smart microgrids' optimal operation. The control signals are sent to actuators through the communication layer again.

Some studies have been done on the cyber–physical system approach for smart power system design, modelling, simulation, and verification of cyber–physical systems, real-time requirements in cyber–physical systems, etc. [18–21]. It should be mentioned that cyber–physical system is not a new concept, and it has been used in a variety of domains, including thermal management [22], gaming and social network [23,24], cloud computing [25], and air-traffic management [26].

From the discussions above and Figure 1, it can be concluded that accurate and optimal operation of smart microgrids is impossible without the secure and safe communication infrastructure, distributed computation technologies, and information processing.

2.2. Challenges and Issues

Based on the interaction of the physical and cyber systems, smart microgrids can be monitored and controlled efficiently and reliably. However, due to the tight interconnection between cyber and physical components, vulnerabilities are introduced to the system, and challenges and issues should be studied for their development and seamless operation. In detail, the smart microgrid's cyber–physical system contains complex structures, including distributed sensors and actuators, controllers, and power components and interfaces, and coordination between those components through high-precision and timely communication is a must. Therefore, several challenges and issues, such as reliability of communication, data safety, and mass data processing, should be addressed for smart microgrids. In this paper, the cyber-attacks are studied in detail due to their significant impacts on smart microgrids operations.

3. Sample of Recent Cyber-Security Projects

A few examples of currently running projects on the cyber-security of smart grids are discussed in this section.

3.1. Blockchain-Based Security Framework for the Internet of Thing-Enabled Solar Micro-Inverters

Researchers of the Texas A&M University-Kingsville are investigating threats of cyber-attacks on the Internet of Things (IoT)-enabled solar micro-inverters [27]. Currently, the penetration of distributed solar micro-inverters is increasing rapidly, in which they require communication for power-sharing and distributed hierarchical control [28]. Although the IoT provides the opportunity for module-to-module communications, it could introduce security challenges. In this system, the IoT device connected to the solar micro-inverters acts as a security module. The cloud-based PV management platform supports the PV system, and the blockchain server provides blockchain service. This system can enhance communication security, data security, software/firmware security, hardware component security (supply chain), and cyber-attack detection. The future work includes the blockchain technology validation for software security, the effectiveness of this security strength under

cyber-attacks, and designing a novel blockchain platform for PV systems to overcome potential issues.

3.2. Consequence-Driven Cyber-Security for High Power EV Charging Infrastructure

In this project, led by Idaho National Laboratory (iNL), events with the high consequence for high power EV charging stations are prioritized, in which the focus is on high-speed charging (higher than 350 kW) and wireless power transfer systems. The high consequence events are prioritized based upon severity impact and cyber manipulation complexity. Based on the research results, extreme fast charging thermal system manipulation and wireless power transfer operation with no vehicle present are two events with higher consequences. It is proven that the spoofed attacks on thermal sensors of extreme fast chargers cause no cooling of cable and connector. This attack will cause cable failure and melting. On the other hand, the spoofed attacks on wireless communications will cause wireless charging operation with no electric vehicle present. In this event, the primary coil (ground side coil) of the wireless power transfer operates at full current, which could potentially endanger public safety. As a future work of this project, methods to identify such cyber-attacks and mitigate them will be provided [29,30].

3.3. Design of Cryptographic Module for Distributed Energy Resources

The National Renewable Energy Laboratory (NREL) is designing a cryptographic module suitable for distributed generations [31,32]. This module utilizes distributed cryptography for command and control messages on an operational technology network. For this project, the current device's security controls are tested, and the gaps are identified. Then, the module is designed, developed, and tested. The lab testing setup for the designed module in NREL contains two virtual machines as a grid controller and a third-party controller, in which both use the modules across their communications with each other and the distributed generations site. Another module connected to the distributed generations site transfers messages to the relevant distributed generation controllers.

3.4. Design for Secure Reconfigurable Power Converters

In this project completed by the University of North Carolina at Charlotte, a secure power converter is designed. A Trusted Platform Module (TPM) is integrated into the power converter system, a hardware module that offers different cryptographic functions. In detail, the TPM provides services including encryption, key provisioning, and data signing, and the onboard microprocessor of FPGA provides an interface to the TPM [33].

3.5. Securing Vehicle Charging Infrastructure

Lead by Sandia National Laboratories, this project's primary goal is to protect US infrastructure and increase energy security since cyber-attacks on electric vehicle charging could affect nearly all US infrastructure. This project focuses on the vulnerabilities of EV chargers and analyzes the electric vehicle supply equipment's risk. In detail, this project contains two tasks: assess the vulnerability of EV charging and develop a threat model and study the consequences of vehicle charging vulnerability [34]. In the future, this project will try to prepare standardized policies for chargers' infrastructure management, develop effective defenses, design intrusion detection/prevention systems, and develop response techniques to prevent further effects [34].

4. Review of Cyber-Security Standards and Protocols

In this section, some recognized and important standards and protocols of cyber-security are reviewed.

4.1. AMI System Security Requirements (AMI-SEC)

The AMI-SEC is established under UCA International Users Group (UCAIug) to develop a robust security guideline for the initial AMI (Advanced Metering Infrastructure)

portion of the Smart Grid. The AMI-SEC supports all of the AMI system's use cases, including AMI communications network device, AMI forecasting system, AMI head end, AMI meter, AMI meter management, and home area network. The AMI-SEC also recommends a control system and communication protection, including security function isolation, cryptographic key establishment and management, the transmission of security parameters, voice-over-internet protocol, and many more.

4.2. NERC CIP

NERC CIP plan is to establish the requirements for a secure operation of North America's bulk electric system. The NERC CIP plan consists of 9 standards and 45 requirements, and they are about the Critical Cyber Asset Identification, Security Management Controls, Personnel and Training, Electronic Security Perimeters, Physical Security of Critical Cyber Assets, Systems Security Management, Incident Reporting, and Response Planning, and Recovery Plans for Critical Cyber Assets. The NERC's standards for governing critical infrastructure apply to units that significantly impact the bulk power system's reliability.

4.3. NISTIR 7628

The National Institute of Standards and Technology Interagency Report (NISITR) 7628 presents an analytical framework for organizations to develop effective cyber-security strategies for their smart grid systems. The organizations in different areas of smart grids, including utilities that provide energy management services to manufacturers of electric vehicles and charging stations, can benefit from the methods and supporting information. This approach acknowledges that the electric grid is changing from a closed system to complex and highly interconnected systems, which result in multiplying and diversifying the threats to grid security. The guideline has more than 600 pages within three-volume; Vol. 1—smart grid cybersecurity strategy, architecture, and high-level requirements, Vol. 2—privacy and the smart grid, and Vol. 3 supportive analyses and references [35].

4.4. IEC 62351

IEC 62351 provides the security recommendations for different power system communication protocols of TC 57 series, including IEC 60870-5 series, IEC 60870-6 series, IEC 61850 series, IEC 61970 series, and IEC 61968 series. The different security objectives, such as authentication of data transfer through digital signatures, intrusion detection, eavesdropping prevention, and spoofing and playback prevention, are covered. The standard includes 16 parts covering an introduction to various aspects of the communication network and system security associated with power system operations. Moreover, terms and acronyms, specified messages, procedures, and algorithms for securing Manufacturing Message Specification (MMS) based applications are some of the other titles. Eventually, addressing end-to-end information security, including security policies, access control, key management, and others, can be embraced by these titles [36].

4.5. ISO/IEC 27001 and 27002

As the most fundamental standard of information security management, the ISO/IEC 27001 has a broad domain, including system security testing, compliance with security policies (periodical checks), and technical compliance review (contains operational systems testing to make sure that implementation of hardware and software controls are accurate). The auxiliary and practical guidance on the ISO/IEC 27001 implementation is provided in ISO/IEC 27002. ISO/IEC 27001 and 27002 can be applied to all smart grid components [37–39].

4.6. GB/T 22239

This standard is a Chinese standard for information systems called "Information Security Technology—Baseline for Classified Protection of Information System Security". This standard defines five security protection abilities for the information system, where

the system can defend against threats and restore to the previous state. The compliance of all smart grid components can be tested with this standard [37,40].

4.7. NIST SP 800-82

This standard is about the security of industrial control system, which is recognized and used worldwide. The standard validates and certifies that the specified security controls are implemented correctly, and they are operating and producing the desired outcomes. This standard also provides particular recommendations about vulnerability and penetration testing tools [37,41].

The standards above and protocols are reviewed and compared in Table 1. For more information about the cyber-security standards and protocols, please refer to [37].

Table 1. Review of Standards and Protocols of Cyber-Security.

Descriptions	Titles						
	AMI-SEC	NERC CIP	NISTIR 7628	IEC 62351	ISO/IEC 27001 27002	GB/T 22239	NIST SP 800-82
Critical Cyber Asset Identification	x	✓	✓	x	✓	✓	✓
Security Management Controls	x	✓	✓	x	✓	x	✓
Personnel and Training	x	✓	x	x	✓	✓	x
Electronic Security Perimeters	x	✓	✓	x	✓	x	✓
Physical Security of Critical Cyber Assets	x	✓	✓	x	✓	✓	✓
Systems Security Management	✓	✓	✓	x	✓	✓	✓
Incident Reporting and Response Planning	x	✓	✓	x	x	✓	✓
Recovery Plans for Critical Cyber Assets	x	✓	✓	x	x	✓	✓
Security guidance for AMI systems	✓	x	x	x	x	x	x
Privacy and the Smart Grid	x	x	✓	x	x	x	✓
Security of Power System Information Exchange	✓	x	✓	✓	x	x	x

In the following, important initiatives involved in smart grid standardization are listed [37]:

- CEN-CENELEC-ETSI Smart Grid Coordination Group [42]
- Smart Grid Interoperability Panel [43]
- European Commission Smart Grid Mandate Standardization M/490 [44]
- OpenSG SG Security Working Group [45]
- German Standardization Roadmap E-Energy/Smart Grid [46]
- The State Grid Corporation of China (SGCC) Framework [47]
- IEC Strategic Group 3 Smart Grid [48]
- IEEE 2030 [49]
- Japanese Industrial Standards Committee (JISC) Roadmap to International Standardization for Smart Grid
- ITU-T Smart Grid Focus Group

5. Cyber-Attacks: General Classification

The cyber system in smart microgrids collects, transmits, and processes data to control physical system operation. The cyber system's data flow should be efficient, reliable, and timely to govern physical process operation. The cyber-attacks on smart microgrid data flow can be classified into three attacks: attacks compromising availability, integrity, and confidentiality [1,50,51].

5.1. Attacks on Data Availability

The cyber system should guarantee that the data are timely and accessible, which is crucial for power electronics converters control in the smart microgrids, especially under islanded mode and transients. The attacks that their primary purpose is to block or delay the data communications are referred to as attacks on data availability. The denial of service (DoS) and distributed denial of service (DDoS) are examples of attacks on data availability. These attacks can be started from one source or several sources by transferring malformed packets to the target or flooding the network/communication layer by exhausting the routers' processing capacity, network bandwidth, or servers [52–54]. Moreover, data time latency cannot exceed its limit in microgrids. For example, the max latency of protective relay is in 4 ms, PMU-based situational awareness monitoring is in sub-second, SCADA system is in seconds, and the energy management system is in minutes [1,55].

5.2. Attacks on Data Integrity

In addition to availability, data in the cyber system should be accurate and trustworthy over their entire lifecycle and under all operating conditions. Any attack that compromises data integrity modifies the information flowing in the cyber system. These attacks can be made by corrupting the measurements or command signals in the communication network and may lead to microgrid malfunctions and affect its control, including regulation of frequency and voltage, power and energy management, islanding detection and resynchronization. A typical example of attacks compromising data integrity is False Data Injection (FDI) cyber-attacks [12,56]. The FDI attack is one of the most challenging threats for microgrids, and the impacts of FDI on modern power grids can be unacceptable [57–60]. In such attacks, hackers can penetrate in communication network without changing the system observability, and system operators may be unaware of any attacks [8,9,52]. Those attacks are also called stealth attacks [10–12]. In this paper, these attacks are studied in detail due to their importance and disruptive impacts on smart microgrids.

5.3. Attacks on Data Confidentiality

Data confidentiality states that data should be protected from being accessed and comprehended by unauthorized parties. Cyber-attacks compromising confidentiality allows hackers to spy on the communication network to retrieve information about customers (identity and electricity usage) and microgrid operation and control strategies. Although these attacks may not have a high impact on microgrids operation, the revealed information can be used by hackers to attacks data availability and integrity effectively.

The impacts of cyber-attacks on smart microgrids operation and the construction of cyber-attacks and defensive strategies against them with a particular focus on FDI attacks are presented.

6. Impacts of Cyber-Attacks on Smart Microgrids

In general, the cyber-attacks can cause significant economic and technical/physical issues in smart microgrids. In the following, these impacts are reviewed.

6.1. Economic Impacts

Although much recent research has focused on the technical/physical impacts of cyber-attacks, it is also essential to study such attacks' potential financial risks. The cyber-attacks can cause significant economic problems in smart microgrids [61,62], especially in

grid-connected mode with high penetration of renewable energy resources. It should be mentioned that optimal economic operation in microgrids' islanded operation is not as important as the grid-connected mode (in an islanded mode, other factors such as stability is more important).

Most deregulated electricity markets consist of a day-ahead market and a real-time market [57,63]. In the day-ahead market, the load is forecasted, and an optimization problem is solved to minimize the cost. The optimization problem's outcome would be the predicted power generated at each bus (economic dispatch), which is used to define the locational marginal price (LMP) at each bus. The LMP is the buy/sell cost of power at different locations within electricity markets. Since FDI cyber-attacks can affect load forecasting, the day-ahead market is vulnerable to such attacks.

The real-time market uses the state estimation to estimate the power generated and power load at each bus, which is used to calculate the power flow through each line (for instance, optimal power flow can be used). Based on each line's calculated power, the congestion pattern is achieved (if the estimated power in each line exceeds the maximum power limit, the line is congested). In the real-time market, real-time LMP is determined based on the calculated power. It can be seen that the state estimation is involved in congestion pattern calculations and loads and generation estimation. Thus, the FDI cyber-attacks that change the estimated state has impacts on the real-time market. More information about the economic impacts of cyber-attacks can be found in [57,62–66].

6.2. Physical/Technical Impacts

In addition to economic impacts, the FDI attacks can have physical/technical impacts on microgrids. In general, the FDI attacks can impact on transient and steady-state stability of the microgrids. In terms of steady-state stability, the FDI attacks can impact voltage control of microgrids (AC or DC voltage control in AC-DC microgrids), energy management systems and demand power/current management [11,67–70].

In addition to the adverse effects of cyber-attacks on microgrids' steady-state operation, the microgrids' transient and dynamic stability can be impacted by the FDI attacks. For instance, the FDI can impact on frequency control of the microgrids. Furthermore, rotor angle stability can be affected by FDI attacks in microgrids [67,71–75]. Moreover, the attacks can impact on protection system of smart microgrids. More detail of the physical/technical impacts of cyber-attacks on microgrids in accompaniment with construction strategies of attacks is discussed in the following section.

7. Construction of Cyber-Attacks in Smart Microgrids

In recent years, much research effort has been devoted to the study of possible FDIA construction methods. To construct an attack, hackers usually have partial cyber-physical system information [56,76]. In case that hackers have full network information, the attack would be more effective and destructive. The hacker's knowledge of the system and the access degrees determine the level of destructive impacts and the possibility of detection/mitigation by defenders.

To study the construction of cyber-attacks in power electronics-intensive smart microgrids, such microgrids' control system is reviewed first. In smart microgrids, the multi-layer control structure is usually used, in which the outer and inner layers are called supervisory and primary control layers, respectively [77]. The supervisory control center receives data from the power electronics converters of distributed generations and other power production resources and power sensors measurement devices and makes decisions based on defined objectives. The decision signals are then sent to all the local controllers (where the primary controls are running). In general, the supervisory control can be separated into tertiary and secondary controls [77,78]. The tertiary control is usually used to determine each power source (real and reactive powers), and usually, an optimization problem is solved to achieve a global optimum. It also controls power flows between the primary grid and the microgrid. The objectives of secondary control include system frequency restora-

tion, unbalanced voltage compensation, harmonic compensation. The primary control instantaneously reacts to local events in predefined ways. The supervisory control system structures can be categorized as centralized, distributed, and master–slave, discussed in detail in [77]. Figure 2 shows the multi-layer control structure of power electronics-intensive smart microgrids with centralized supervisory control.

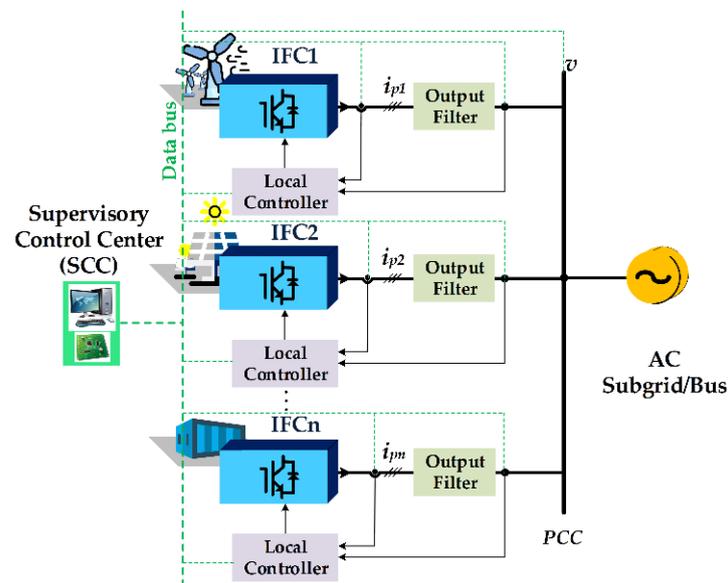


Figure 2. Centralized structure of supervisory control in power electronics-intensive smart microgrids.

As mentioned above, the FDI attacks can target steady-state and transient operations of smart microgrids. Among several attacks, the FDI attacks targeting state estimation, voltage and frequency regulations, and system protection are explained in the following due to their importance in smart microgrids.

7.1. Cyber-Attacks on State Estimation

The state estimation is used to determine the system operation status, including bus voltage magnitudes and phase angles from available measurements. Such attacks' primary purpose is to introduce errors in estimating state variables in microgrids by manipulating sensors' measurement data. The state estimation helps monitor and control microgrids effectively and efficiently, and it is one of the most critical tasks in microgrids operation and energy management strategies. The estimated states can also be used for contingency analysis, stability analysis, load forecasting, optimal power dispatch, bad data detection, and power markets' locational marginal pricing [79–81]. Any FDI attacks inducing errors into estimated states can have disruptive effects on microgrids' operation and performance.

In general, there are two types of state estimation in power systems: DC state estimation and AC state estimation (for more information about AC and DC state estimation, please refer to [80] and [82]). Due to simple analytical models, power systems with DC state estimation have been studied more than AC state estimation in literature [15,83–85]. However, FDI attacks construction targeting AC state estimation is gradually gaining attention [86–89]. It should be highlighted that for the state estimation and the associated FDI attack in the smart microgrid, most researches are addressing power transmission system approaches. A few works on the state estimation and FDI attack in MV power distribution systems, such as [90,91], are more applicable for the smart microgrids.

Although research on the construction of FDI attacks mostly focuses on attacks targeting state estimation, FDI attacks construction targeting voltage, frequency, and protection systems have also been studied [16,92,93].

7.2. *Cyber-Attacks on Voltage Control*

The smart microgrid's voltage is usually controlled by power electronics-interfaced distributed generations and rotational-based generators (such as diesel generators). In such systems, the system's voltage level and/or reactive power is measured, and the control system produces reactive reference powers for the power generations. As another option, the transformer tap changer is also controlled for microgrid voltage regulation. The FDI attacks that modify sensor measured voltage and/or reactive power data and control parameters within the control layers can impact the voltage regulation of microgrid [67,68,70]. Moreover, the hackers may access the microgrid multi-layer control system and modify control signals among layers (e.g., induce errors into DGs reference power signals and transformer tap changer signal) [92,94,95]. An implementation example of an FDI cyber-attack targeting DC microgrid voltage control is presented in Section 9.

7.3. *Cyber-Attacks on Frequency Control*

The attacks targeting microgrids frequency are referred to as attacks on transient stability. Like attacks on microgrids' voltage stability, hackers can introduce errors into control signals among control layers, modify control parameters and sensor measurements, or change outputs of power sources to affect microgrid frequency stability. It should be mentioned that the microgrid frequency control is susceptible to active powers and frequency measurements, and reference signals. In microgrids, frequency is usually regulated by rotating machines. Any attacks targeting rotor speed or angle measurements can affect microgrids' frequency stability [71–75]. Recently, energy storage systems are used for transient stability improvement in microgrids [96–98]. In such systems, sensor measurements are used in the control system to actuate the storage systems to absorb and/or inject active power from the microgrid. Since energy storage systems are evolving in microgrids frequency control, the security of measurement and control signals should be guaranteed to provide stable operating conditions. More discussions on cyber-attacks on load frequency control can be found in [93,99–102]. In Section 9, an example is provided.

7.4. *Cyber-Attacks on Protection System*

One of the main challenges of microgrids is protection system design, which should operate under grid-connected and islanded operation mode (review of classical protection technical challenges can be found in [16]). Depending on the operation mode, the relay setting should be adjusted to the proper current level. One of the conventional approaches is adaptive protection techniques based on the IEC 61850 communication standard. In such protection systems, a secure, reliable, and fast communication network is necessary. However, the communication link failures or any FDI cyber-attacks may affect the protection system performance and lead to disastrous microgrids. In [103], protection and control systems' cyber-security is explained, and proper cyber-attack mitigation strategies are discussed.

8. **Defensive Strategies against Cyber-Attacks**

The defense strategies against cyber-attacks can be classified into strategies based on protection and detection/mitigation. In the following, these two groups are discussed in detail.

8.1. Defensive Strategies Based on Protection

In the defensive strategies based on protection, meters/sensors are protected against cyber-attacks [57,63,75,104,105]. Since many smart sensors and meters exist in emerging smart microgrids, protecting all meters is not cost-effective. Thus, only a set of critical sensors and corresponding measurements are usually protected [8,58].

It should be mentioned that the number of meters/sensors under attacks is a fundamental criterion in FDI cyber-attack detection. In some cases, the number of sensors is increased to enhance the microgrids' visibility; however, it increases the microgrid's vulnerability for cyber-attacks [69]. In defensive strategies based on protection, the number of protected sensors (and their locations) can be achieved considering the budget and the system's sensitivity. For example, in [8], an optimization problem is formulated to minimize the defender budget and determine the meters' number and position for protection against attacks.

8.2. Defensive Strategies Based on Detection/Mitigation

In the detection-based defense strategies, the measured data are analyzed to detect cyber-attacks and mitigate/reduce their adverse effects on the microgrid operation. In general, detection strategies can be categorized into static and dynamic [93].

8.2.1. Static Detectors of Cyber-Attacks

The defense strategies that detect attacks on steady-state stability are called static detectors. One of the well-known static detectors is detectors of attacks on state estimation. To date, several strategies have been developed to detect/mitigate FDI attacks targeting state estimation, such as statistical methods [2,106], Kalman filter [107], sparse optimization [108], state forecasting [109,110], network theory [111], time-series simulation [69], machine learning [112–116], generalized likelihood ratio [117], Chi-square detector, and similarity matching [118]. However, these strategies are used to recover DC state information and are suitable for FDI attacks on DC state estimation.

In AC system models that are usually used in most real-world power system, the performances of such strategies are not satisfactory [89,119]. A few researches have been done to detect FDI attacks on AC state estimation such as Kullback–Leibler distance [120], information-network-based state estimation technique [121], transmission lines' parameters variation techniques [122], Bayesian detection scheme [57], and discrete wavelet transform algorithm together with deep neural networks technique [9]. However, more research is needed.

The defense strategies against attacks targeting voltage regulations in microgrids can also be categorized as static detectors. For example, the voltage control of smart AC microgrid with high penetration of PV systems under cyber-attack is addressed in [92], in which the detection algorithm is embedded into the converters control system. In [123], supplementary control loops are added to the DGs power converters controllers to defend against large voltage deviations resulting from cyber-attacks in AC microgrids. A cooperative mechanism to detect cyber-attacks in the DC microgrid distributed controllers with two control layers is proposed in [11]. This mechanism provides accurate current sharing and voltage regulation in power electronics-intensive DC microgrids, discussed in the next section as an example. Furthermore, in [69], the FDI attack detection in DC microgrid is studied. The detection problem is formalized as identifying a change in sets of inferred candidate invariants (invariants are defined in terms of bounds over the output voltage and current of individual power converters).

8.2.2. Dynamic Detectors of Cyber-Attacks

Information on system dynamics is used in dynamic detection methods to detect cyber-attacks [124–129]. Various dynamic detectors have been studied in recent years; however, they mainly focus on linear systems, which cannot effectively detect real-world power system attacks due to the non-linearity. As an example, load frequency control depends on power system dynamics, and FDI attacks targeting frequency control are detected by dynamic detection methods [93,99–102,130]. As another example, an image-processing-based technique is proposed in [2] to detect FDI attacks in real-time. This method is built on the dynamics of measurement variations. In [71], the FDI attacks on the power system's transient stability are studied, and errors on rotor speed and angle are quantified. An adaptive control strategy is then proposed to eliminate or minimize the impact of FDIA attacks on system dynamics. The impact of FDI attacks on frequency control of microgrids is studied in [131], and complementary control is added to deal with the attack. In [68], a cyber-attack dependent model of the microgrid is developed and sliding mode observer theory is used to diagnose cyber-attack on the current component of smart converters in microgrids.

In Table 2, all the discussions mentioned above and research on cyber-attacks are reviewed. The correlation between the cyber-attacks and the defensive strategies against the attacks in smart microgrids is shown in Figure 3.

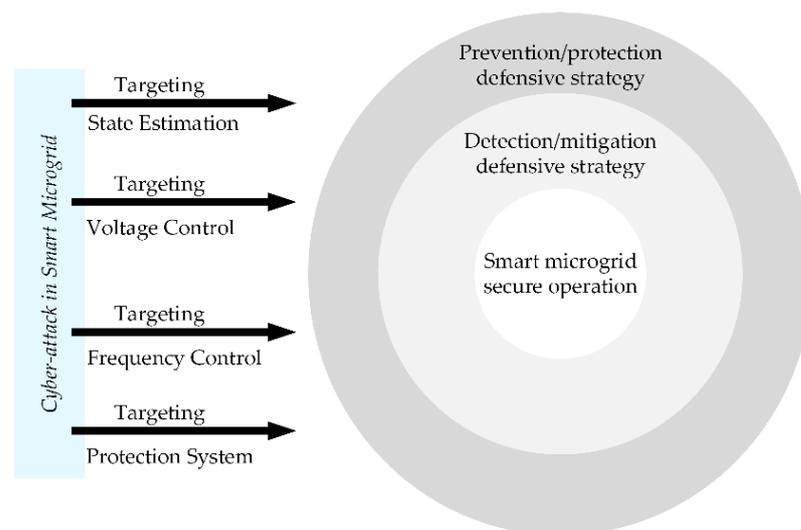


Figure 3. Cyber-attacks in smart microgrids and defensive lines.

In the following, implementation examples of FDI attacks' construction and detection/mitigation in smart microgrids are provided.

Table 2. Review of Cyber-Attacks in Smart Power Systems.

Cyber-attacks in Smart Microgrids	Impacts of Cyber-Attacks	Economic Impacts	<ul style="list-style-type: none"> Especially in grid-connected mode, optimal economic operation can be affected. FDI cyber-attacks can affect load forecasting and change the estimated state, which affect the day-ahead market and real-time market.
		Physical/Technical Impacts	<ul style="list-style-type: none"> FDI attacks can impact on transient and steady-state stability of the microgrids. FDI attacks can impact on voltage control of microgrids, energy management systems, demand power/current management, etc. FDI attacks can impact on frequency control, rotor angle stability, protection system, etc.
	Constructions of Cyber-Attacks (main attack targets)	Attacks on State Estimation	<ul style="list-style-type: none"> Main purpose of attacks is to introduce errors into the state estimation by manipulating sensors measurement. FDI attacks inducing errors into estimated states have disruptive effects on microgrids operation. FDI attacks targeting DC state estimation has been addressed more than AC (due to simplicity)
		Attacks on Voltage Control	<ul style="list-style-type: none"> FDI attacks can modify sensor measured voltage and/or reactive power data and control parameters within the control layers and impact the voltage regulation of microgrid. FDI attacks may modify control signals among microgrid multi-layer (for example, induce errors into DGs reference reactive power signals and transformer tap changer signal).
		Attacks on Frequency Control	<ul style="list-style-type: none"> Microgrid frequency control is very sensitive to active powers and frequency measurements. FDI attacks targeting microgrids frequency are referred to as attacks on transient stability. Hackers can induce errors into control signals among control layers, modify control parameters and sensor measurements, or change outputs of power sources.
		Attacks on Protection System	<ul style="list-style-type: none"> One of the main challenges of microgrids is protection system design. Depend on the operation mode, relays setting should be adjusted to the proper current level. FDI attacks may affect the protection system performance and may lead to disaster events.
	Defensive Strategies Against Cyber-Attacks	Strategies Based on Protection	<ul style="list-style-type: none"> Meters/sensors are protected against cyber-attacks. Number of protected sensors and their locations are determined based on budget, the sensitivity of the system, etc.
		Strategies Based on Detection/Mitigation	<ul style="list-style-type: none"> Measured data are analyzed to detect attacks and mitigate its adverse effects on the microgrid. Can be classified into static detectors (detect attacks targeting steady-state stability) and dynamic detectors (information of system dynamics is used for detection).

9. Implementation Examples

9.1. Example 1: Cyber-Attacks in Power Electronics-Intensive DC Microgrids

The FDI cyber-attack construction and detection in DC microgrid in [11] are presented here. The studied DC microgrid is shown in Figure 4, in which N -number of DC power generators are connected to the DC microgrid through DC/DC converters. The power converters are controlled to adjust their output voltages to the local primary and secondary controllers' reference values.

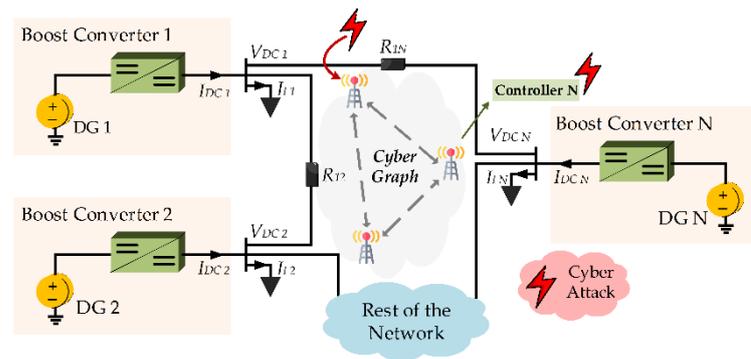


Figure 4. DC microgrid with the cyber-physical model.

In DC microgrids, the secondary controller uses local and neighboring measurements to globally tune the average voltage and share the currents proportionately to reduce the circulating currents. Typically, sublayers of secondary control are cooperated to achieve those objectives in which the first sublayer is responsible for average voltage restoration while the current sharing is done in the second sublayer.

To regulate average voltage globally in the first sublayer, a voltage observer is used to estimate the average voltage $\bar{V}_{DC_i}(k)$ for i th converter. This value is updated by a dynamic consensus algorithm [132], which uses neighboring estimates $\bar{V}_{DC_j}(k) \forall j \in N_i$ (N_i represents neighbour converters). The estimated average voltage for the i th converter is provided:

$$\begin{aligned} \bar{V}_{DC_i}(k+1) - \bar{V}_{DC_i}(k) &= V_{DC_i}(k+1 - \tau_{output}^i) - V_{DC_i}(k - \tau_{output}^i) \\ &+ \sum_{j \in N_i} a_{ij} (\bar{V}_{DC_j}(k - \tau_{input}^i - \tau_{comm}^{ij}) - \bar{V}_{DC_i}(k - \tau_{input}^i)) \end{aligned} \quad (1)$$

In (1), τ_{input}^i , τ_{output}^i , and $V_{DC_i}(k)$ represent the input and output delays, and the measured voltage in the i th converter, and τ_{comm}^{ij} denotes the communication delay between the i th and j th converters. Further, a_{ij} is the elements of the adjacency matrix of the communication graph.

In the second sublayer, which is used to share current among converters proportionally, the i th converter normalized current regulation cooperative input is achieved by

$$\bar{I}_{DC_i}(k) = \sum_{j \in N_i} w_i a_{ij} (I_{DC_j}(k - \tau_{output}^i - \tau_{comm}^{ij}) / I_{DC_j}^{max} - I_{DC_i}(k - \tau_{output}^i) / I_{DC_i}^{max}) \quad (2)$$

where $I_{DC_j}(k) \forall j \in N_i$ is the measurements of neighboring output current, and w_i , I_{DC_i} , I_{DC_j} , $I_{DC_i}^{max}$, and $I_{DC_j}^{max}$ denote the desired coupling gain, measured output current in the i th and j th converters, and maximum output current allowed for the i th and j th converters, respectively.

To implement the above objectives into the i th converter to regulate the output voltage, two voltage correction terms are considered as follows:

$$\Delta V_i^1(k) = K_{P1} \underbrace{(V_{DC}^* - \bar{V}_{DC_i}(k))}_{e_1^i(k)} + K_{I1} \sum_{p=0}^k (V_{DC}^* - \bar{V}_{DC_i}(p)) \quad (3)$$

$$\Delta V_i^2(k) = K_{P2} \underbrace{\left(I_{DC}^* - \bar{I}_{DC_i}(k - \tau_{input}^i) \right)}_{e_2^i(k)} + K_{I2} \sum_{p=\tau_{input}^i}^k \left(I_{DC}^* - \bar{I}_{DC_i}(p - \tau_{input}^i) \right) \quad (4)$$

where K_{P1} , K_{I1} , K_{P2} , and K_{I2} are the first and second sublayers' PI controller gains (see Figure 5). Moreover, global reference current and voltage values are represented by I_{DC}^* and V_{DC}^* , respectively.

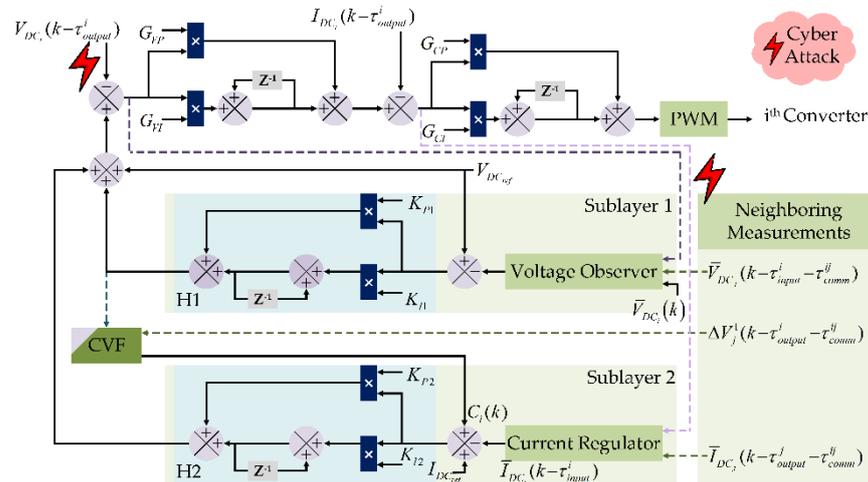


Figure 5. The i th-converter controller for sensors and communication link attacks' detection in DC microgrids [11].

Finally, the correction terms in (3) and (4) are added to the global reference voltage to obtain the reference value for the local voltage of i th-converter.

$$V_{DC_i}^*(k) = V_{DC}^* + \Delta V_i^1(k) + \Delta V_i^2(k) \quad (5)$$

In such DC microgrid, using the cooperative-based consensus algorithm, (1) and (2) shall converge to

$$\lim_{k \rightarrow \infty} \bar{V}_{DC_i}(k) = V_{DC}^*; \quad \lim_{k \rightarrow \infty} \bar{I}_{DC_i}(k) = 0 \quad \forall i \in N \quad (6)$$

For cyber-attacks in a single sensor/communication link, (6) is modified as follows:

$$\lim_{k \rightarrow \infty} \bar{V}_{DC_i}(k) = V_{DC}^{*'}; \quad \lim_{k \rightarrow \infty} \bar{I}_{DC_i}(k) \neq 0 \quad \forall i \in N \quad (7)$$

This criterion can be used to detect cyber-attacks, including DoS and jamming. However, the stealth attacks can penetrate the system without operators' knowledge and can multiple sensors/communication links (the stealth attack can be crafted so that (6) is satisfied). It is proven in [11] that if a constant value P exists such that

$$\sum_{k=0}^{\infty} |u_{V_i}^a(k)| \leq P, \quad \sum_{k=0}^{\infty} |u_{I_i}^a(k)| \leq P \quad \forall i \in N \quad (8)$$

Then, the state convergence (6) is not affected in the presence of stealth attacks. In (8), $u_{I_i}^a(k)$ and $u_{V_i}^a(k)$ represent the i th-converter current and voltage attack vectors at the k th instant.

In the DC microgrid controlled by cooperative systems, it is challenging to detect the attacked node since the entire system is affected by the intrusion in any node. Considering Figure 4, each converter output current depends on voltage levels between two different points. Thus, any stealth attacks on current value (e.g., attacks on current sensors) will result in voltage variations across the DC microgrids, which leads to errors in current sharing among converters. Typically, the current sharing error could be a sufficient criterion to

detect the attacks on current sensors. However, if multiple voltage sensors/communication links are attacked stealthily, attack detection would not be easy. In more details, the voltages will be manipulated so that (6) still holds even under attacks.

In [11], the voltage regulation control input is used to provide a strong stealth attack. This control input signal for the i th-converter is presented as in (9).

$$u_i(k) = \sum_{j \in N_i} a_{ij} \underbrace{\left(\bar{V}_{DC_j}(k) - \bar{V}_{DC_i}(k) \right)}_{u_{ij}(k)} + b_i e_1^i(k). \tag{9}$$

If a cyber-link or sensor is attacked in the i th controller, the model of attacked control input would be as in (10) and (11), respectively.

$$u_{ij}^f(k) = u_{ij} \left(k - \tau_{input}^i - \tau_{comm}^{ij} \right) + k u_i^a(k) \tag{10}$$

$$u_i^f(k) = u_i \left(k - \tau_{input}^i \right) + k u_i^a(k) \tag{11}$$

where k shows attack presence (when $k = 1$, there is an attack in the system) and $u_i^a(k)$ represents i th-converter attack vector. From (10) and (11), local investigation of $u_i^f(k)$ can be done in each converter to detect nonzero synchronization error with the residual output. However, since each residue comparison needs global information, this is not an appropriate criterion to detect attacks' node(s). To verify this case, the controller attempt to adjust the output to a given reference voltage is considered for attack indication.

Using the change in PI output in sublayer 1, a cooperative vulnerability factor (CVF) is defined in [11] as in (12) for each converter to determine the attacked nodes accurately.

$$C_i(k) = c_i \left[\sum_{j \in N_i} a_{ij} \left(\Delta V_j^1 \left(k - \tau_{comm}^{ij} \right) - \Delta V_i^1(k) \right) \right] + \left[\sum_{j \in N_i} a_{ij} \left(\Delta V_j^1 \left(k - \tau_{comm}^{ij} \right) - \Delta V_i^1(k) \right) \right] \tag{12}$$

where c_i is a positive constant value. If the calculated $C_i(k)$ for each node is a positive value, that node is the attacked node. While the non-attacked nodes have the $C_i(k)$ value of zero. The proposed CVF in [11] is a proper criterion to detect the attacked node, especially when multiple sensor/communication links are stealthily attacked. The value of $C_i(k)$ is cross-coupled with the current sublayer to protect against attack to $C_i(k)$. In Figure 5, the i th-converter controller to detect stealth attacks on communication links and sensors in DC microgrids is shown. For more detailed information, please refer to [11].

9.2. Example 2: Cyber-Attacks on Frequency Control of AC Microgrid

In this example, the FDI cyber-attack construction targeting frequency control of AC microgrid and its detection scheme is discussed, which is obtained from [93]. In this study, the power system is divided into two areas connected through the tie-line. The schematic of the two-area power system frequency control is shown in Figure 6. In this figure, each area can be islanded microgrid, which is connected through the tie-line. Alternatively, area A can be an AC microgrid connected to the main grid (area B), or otherwise.

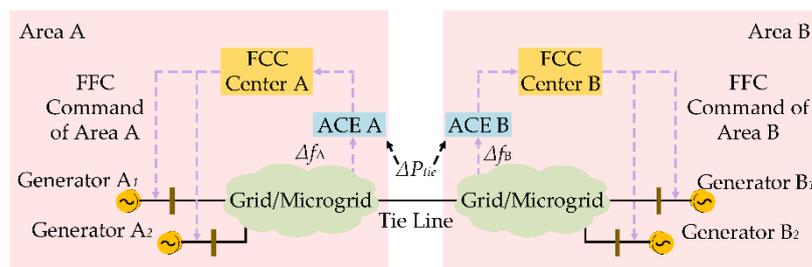


Figure 6. Frequency control schematic of the two-area system.

Figure 6 shows that area control error (ACE) centers receive measured frequency and power signals and provide frequency error values to the frequency control centers (FCCs). Then, the FCCs send out frequency control signals to the power sources (e.g., local controllers of power electronics converters interfaced distributed generations or governor of generators) to balance active power consumption. In this example, it is assumed that hackers attack only area A since it is proven that when both areas are compromised, the generators on both sides act in the opposite direction to deal with attacks' negative impacts.

The ACE center signals sent to FCCs are as follows:

$$ACE = \Delta P_T + \alpha \Delta f = (P_T^a - P_T^n) + \alpha(f^a - f^n) \quad (13)$$

where P_T^a and P_T^n represent actual and nominal powers of tie-line, and f^a and f^n denote actual and nominal frequency.

In this example, high security is considered for the power components and controllers (physical system), and hackers could only intrude through communication systems. Furthermore, it is assumed that the channel transmits FCC signals is equipped with advanced encryption techniques; thus, measured signals can be the only target of hackers. Here, the measured tie-line interchange power and frequency signals are potential targets of attacks. It should be mentioned that they are the main variables of interest in frequency control centers.

In general, the false data injections can be classified into two groups: exogenous attack in which disturbance signal is added into the measured signals (can be pulse, ramp, or random signals [133]), and scaling attack where the measured signal is multiplied by disturbance signal. Considering these two categories, four possible attacks may exist in the system: exogenous attack on the measured frequency and tie-line power signals, and scaling attacks on the measured frequency and tie-line power signals. In this paper, the exogenous attack and scaling attack on the tie-line active power measurement are discussed, and the other two similar attacks on the measured frequency can be found in [93].

9.2.1. Exogenous Attack on Measurement of Tie-Line Active Power

In this attack, disturbance Z_{Dis} is added to the measured tie-line active power signal in area A while area B is free of attack. Thus, the resultant ACEs would be as follows:

$$ACE_{Dis_A} = \Delta P_T + Z_{Dis} + \alpha_A \Delta f_A = ACE_{tA} + Z_{Dis} \quad (14)$$

$$ACE_B = -\Delta P_T + \alpha_B \Delta f_B \quad (15)$$

where ACE_{Dis_A} is the attacked ACE, which is used in FCC-A to produce frequency control signals, and ACE_{tA} is the actual measurement value. From (14), since the goal is to keep $ACE_{Dis_A} = 0$ if $Z_{Dis} > 0$, the value of ACE_{tA} would be negative and f^a falls below f^n . It is also clear that when Z_{Dis} is a negative value, then $\Delta P_T > 0$ and $f^a > f^n$. This kind of attack can deteriorate system stability since low f^a may lead to load shedding (or high f^a value may lead to generator tripping) and large ΔP_T value may cross the exchange power limits.

9.2.2. Scaling Attack on Measurement of Tie-Line Active Power

In this attack, the measured tie-line active power signal in area A is scaled by a hacker. Thus, area A's ACE value is modified due to the attack, while (15) is still valid for area B, as follows.

$$\begin{aligned} ACE_{Dis_A} &= k_{Dis} \Delta P_T + \alpha_A \Delta f_A \\ ACE_B &= -\Delta P_T + \alpha_B \Delta f_B \end{aligned} \quad (16)$$

Considering that ACE_{Dis_A} and ACE_B are regulated to zero, (16) has infinite answers if and only if k_{Dis} is equal to $k_{Dis} = -\alpha_i/\alpha_j$. Otherwise, (16) does not have any solution ($\Delta f_A = \Delta f_B = \Delta f_o = 0$), which means it is not possible to deteriorate system stability by this type of attack.

It should be highlighted that hackers should have full information about the system to design an effective scaling attack to destabilize the system. In other words, $k_{Dis} = -\alpha_i/\alpha_j$ should be satisfied to affect the system stability, which requires full information about the system. Thus, it can be concluded that scaling attacks on sensor measurements of tie-line active power and system frequency may not affect the system frequency stability. On the other hand, when comparing exogenous attack on measured line active power and system frequency signals, it is concluded that tie-line active power measurement is much more susceptible to attacks (since frequency signal deviation is easily detectable by comparing with nominal value). Thus, an exogenous attack on active power measurement has the most destructive effects on the AC microgrid frequency. In [93], the detection method of such attacks has been addressed in detail.

9.3. Example 3: Cyber-Attacks on State Estimation

In this example, the construction of an FDI attack on state estimation in smart power systems and designing the protection-based defense strategy are presented. The provided discussions have been thoroughly obtained from [8]. The defense strategy determines which meter should be protected and how much budget should be allocated to defend against attacks.

In the steady-state condition of $n + 1$ buses power system with m meters measurement $d = [d_1, d_2, \dots, d_m]^T$ (measurements are bus active power generation minus load, and branch active power flows), the state estimation problem is to estimate n state variables $x = [x_1, x_2, \dots, x_n]^T$ which are n bus voltage angles here. The relationship between state variables and measurements are as follows:

$$d = r(x) + e \quad (17)$$

where e is the independent random measurement errors $e = [e_1, e_2, \dots, e_m]^T$ (the error is considered to have Gaussian distribution with diagonal covariance matrix Σ and zero means) and r is the matrix of the nonlinear function of x , which can be considered as $r(x) = [r_1(x), r_2(x), \dots, r_m(x)]^T$. In DC power flow, the nonlinear relationship in (17) can be approximated:

$$d = Rx + e \quad R = \left. \frac{\partial r(x)}{\partial x^T} \right|_{x=0} = \left[\left. \frac{\partial r_i(x)}{\partial x_j} \right|_{x_j=0} \right]_{m \times n} \quad (18)$$

In which R is the measurement Jacobian matrix.

The purpose of state estimation is to find the estimation of state variables (\hat{x} is the estimation of state variable x), which is the best fit to (18). According to (18), the residual of the observed and estimated measurements would be $\Delta d = d - \hat{d} = d - R\hat{x}$, which is used in the state estimation problem solution. For instance, the weighted least-squares (WLS) criterion is one way to solve the state estimation problem. In this method, the objective function of $(d - R\hat{x})^T W (d - R\hat{x})$ is minimized to find \hat{x} where the weight matrix W is defined as Σ^{-1} (here, it is a diagonal matrix that entries are reciprocals of the measurement errors e variances).

In the state estimation method, the FDI can attack the measurement data. The current approach to detect FDI attack is that the Euclidean norm of the measurement residual $\|\Delta d\|_2$ is calculated and compared with prescribed residual τ . If $\|\Delta d\|_2 > \tau$, bad measured data exist in the system.

Here, the malicious measurements are denoted by $d_u = d + u$, where $u = [u_1, u_2, \dots, u_m]^T$ is the attack vector. In [56], it is proven that when the attack vector is crafted as

$$u = Rc \quad (19)$$

where $c = [c_1, c_2, \dots, c_n]^T$ is an arbitrary nonzero vector, the malicious measurements d_u can bypass the bad data detection system. Thus, errors c can be injected into actual state estimation values \hat{x} (it is called \hat{x}_u here) without being detected. As explained earlier, such attacks could affect electricity prices in the power market, power system optimal operation, and stability.

As discussed earlier, one common method to protect the power system against cyber-attacks is securing some meter measurements and/or state variables. It should be mentioned that the defense budget devoted to the meter determines whether the meter measurement can be compromised or not. In this example, the defense strategy is designed in which the defense budget is minimized. This strategy determines which meters should be protected and how much is the defense budget should be deployed on each meter.

Let us assume that the system has a set of state variables as $N = \{1, 2, \dots, n\}$ and set of measurement as $M = \{1, 2, \dots, m\}$, and defender budget allocation vector is as $b = [b_1, b_2, \dots, b_m]^T$ (b_i is the allocated budget for protecting the meter measurement d_i). Thus, the attack cost for a successful compromise of meter measurement d_i can be considered as a function of a devoted budget as follows:

$$F_i = f_i(b_i) \quad \forall i \in M \quad (20)$$

where $F = [k_1, k_2, \dots, k_m]^T$ denotes the cost vector of attack.

9.3.1. Attack Strategy Formulation

For simplicity, R^* is defined by using the R matrix as follows:

$$r_{ij}^* = \begin{cases} 0, & \text{if } r_{ij} = 0 \\ 1, & \text{otherwise} \end{cases} \quad \forall i \in M, \forall j \in N \quad (21)$$

From (21), the j th column of R^* is defined as $r_j^* \in \mathbb{R}^{m \times 1}$, which represents the state variable j relationship with meter measurements from 1 to m . Considering the R^* matrix, to successfully attack the state variable x_j without being detected, the attack cost would be as follows:

$$q(j) = r_j^{*T} k = \sum_{i=1}^m r_{ij}^* k_i \quad \forall j \in N \quad (22)$$

Since the attackers will choose the easiest target of state variable with the least cost, the attacker's strategy can be considered as

$$\begin{aligned} & \min_{j \in N} q(j) \\ & \text{subjected to} \quad (20)-(22) \end{aligned} \quad (23)$$

9.3.2. Defense Strategy Formulation

In cyber-attacks, the reasonable assumption is that attackers do their best to get information about the defender's strategy while defenders do not have any information about attackers' strategy. However, attackers more information cannot help them reduce the least attack cost, and only the probability of a successful attack will be increased. Therefore, as the best strategy, defenders can maximize the least attack cost by considering the total defense budget B as in (24).

$$\begin{aligned} & \max_{b \geq 0} \min_{j \in N} q(j) \\ & \text{subjected to} \quad \begin{cases} \sum_{i=1}^m b_i \leq B \\ (20)-(22) \end{cases} \end{aligned} \quad (24)$$

Assume that the attackers have limited resources R . Since the defenders try to keep the defense budget as low as possible, (24) can be written as follows:

$$\begin{aligned} & \min_{b \geq 0} \sum_{i=1}^m b_i \\ \text{subjected to } & \begin{cases} \min_{j \in N} q(j) \geq R \\ (20)-(22) \end{cases} \end{aligned} \quad (25)$$

It should be mentioned that the least attack cost should always be higher than the attacker's limited resource R . This optimization problem can determine meters to be protected and the defence budget to deploy on such meter. More details about this example can be found in [8].

10. Discussions and Future Trends

The conventional power systems are evolving into smart grids, which compasses interconnected microgrids. The smart microgrids will play an essential role in the next generation of the power system. The hybrid AC/DC microgrids are considered to be the most likely future microgrid structure, in which high penetration of power electronics converters interface distributed generation, energy storages, and loads as well as interlink AC and DC subgrids. The smart hybrid AC/DC microgrids require a reliable and secure cyber system and communication network for optimal, uninterrupted, and smooth operation, and any cyber-attacks may lead to unforeseen incidents in microgrids' operation. It should be emphasized that microgrids are more prone to stability issues if a cyber-attack happens due to their low inertia. Due to the tight coupling of AC and DC subsystems in hybrid AC/DC microgrids, any cyber incident in one subsystem may have destructive effects on the other side.

In this Section, some discussions and recommendations about future trends of microgrids cyber-attacks are provided:

10.1. State Estimation of AC/DC Microgrids under Cyber-Attack

In a power system, extensive research on the detection/mitigation of cyber-attacks on DC and AC state estimations has been done. However, in hybrid AC/DC microgrids, state estimation under cyber-attacks has not been addressed adequately. Thus, the hybrid AC/DC microgrids should be modelled first for estimating the state information. Then, appropriate strategies should be developed to detect the attacks and recover the state information.

10.2. Frequency Control of AC/DC Microgrids under Cyber-Attack

In hybrid AC-DC microgrids, frequency stability is one of the main concerns due to the low inertia of power electronics-based distributed generations and energy storage. The presence of cyber-attacks will even make the situation worse. It should be mentioned that any cyber-attack targeting frequency stability of the AC subsystem may jeopardize the DC voltage stability in the DC side. Therefore, a proper control strategy design to detect and mitigate cyber-attacks on frequency control of hybrid microgrids could be the right research direction for the future.

10.3. Voltage Regulation of AC/DC Microgrids under Cyber-Attack

In hybrid AC/DC microgrids, any voltage variations in the AC or DC side transfer to the other side through interlinking power electronics converters. Therefore, regulation of voltage in such a hybrid microgrid is challenging, especially under cyber-attacks, and it is needed to be considered in the future.

10.4. Electric Vehicles and Cyber-Attacks

Electric vehicles (EVs) and electric vehicle charging stations are increasing rapidly in modern power systems, in which they can be considered smart microgrids (i.e., EV charging stations can be considered grid-connected microgrids). Such microgrids are prone

to cyber-attacks, and recently several research groups are working on cyber-security of EVs and EVs charging stations (please see Section 3 project examples). The cyber-security of EVs and their charging station technologies are in their early development stages that require more study in the future.

10.5. Blockchain and Cyber-Security in Modern Grids

The primary purpose of blockchain technology is to achieve direct peer-to-peer electronic payments where the trusted third party does not participate. In practice, blockchain technology is focused on the financial domain, and the Bitcoin system is its most popular application. Recently, applications of blockchain technology in the power engineering sector have also been addressed, for example, in IoT and smart homes. A few research types have been done to secure the smart grids' operation under cyber incidents by blockchain, and more investigation is needed in the future.

10.6. Software-Related Techniques and Cyber-Attacks

The worldwide cyber-attacks are not only wake-up calls for power system operators, but they are for power system asset suppliers that are using digital systems and software to control their assets. Such suppliers have also begun to make plans to counter cyber-attacks to their digital control system. For example, power supply manufacturer CUI, which uses digital software (called software-defined power) to manage and optimize power delivery intelligently, has started several steps to safeguard its software [6]. Meanwhile, software-defined networking (SDN) technologies emergence provides opportunities to improve the security of microgrid operations by offering global visibility, direct controllability, and programmability [1,6,134]. Although researchers have paid attention to this topic in the past few years, more investigation is necessary for this field.

11. Conclusions

The cyber-security of smart microgrids have been reviewed in this paper. Since smart microgrids require cyber systems and communication networks, they are much more vulnerable to cyber-attacks. In addition, such power electronics-dominated microgrids have low inertia; thus, cyber-attacks can negatively affect their stability and operation. This paper has focused on cyber-attacks on data availability, integrity, and confidentiality after investigating the cyber-physical system in smart microgrids. Due to the importance of false data injection (FDI) attacks that compromise the data integrity, this paper has studied various construction methods, impacts, and detection/defensive strategies of FDI attacks in smart microgrids. Implementation examples support the provided discussions. In this paper, recent worldwide projects on cyber-security are also presented. Moreover, important standards and protocols associated with the cyber-security of smart grids are discussed. Finally, discussion and recommendations about the future research directions on smart microgrids' cyber-security are provided.

Author Contributions: Conceptualization, F.N., Y.W.L., and H.L.; methodology, F.N.; validation, F.N., Y.W.L., H.L., and R.R.A.; investigation, F.N.; writing—original draft preparation, F.N.; writing—review and editing, Y.W.L., H.L., and R.R.A.; visualization, R.R.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Li, Z.; Shahidepour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388. [CrossRef]
2. Singh, S.K.; Khanna, K.; Bose, R.; Panigrahi, B.K.; Joshi, A. Joint-Transformation-Based Detection of False Data Injection Attacks in Smart Grid. *IEEE Trans. Ind. Inf.* **2018**, *14*, 89–97. [CrossRef]
3. Available online: <https://www.greentechmedia.com/research/subscription/u-s-solar-market-insight#gs.wpfDw8k> (accessed on 20 November 2020).
4. Wind Vision. Energy.gov. Available online: <https://www.energy.gov/eere/wind/maps/wind-vision> (accessed on 20 November 2020).
5. Lee, R.M.; Assante, M.J.; Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid. 2016. Available online: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf (accessed on 20 November 2020).
6. Bindra, A. Securing the Power Grid: Protecting Smart Grids and Connected Power Systems from Cyberattacks. *IEEE Power Electron. Mag.* **2017**, *4*, 20–27. [CrossRef]
7. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. 2016; [ebook] Mission Support Center, Idaho National Laboratory. Available online: <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf> (accessed on 20 November 2020).
8. Deng, R.; Xiao, G.; Lu, R. Defending Against False Data Injection Attacks on Power System State Estimation. *IEEE Trans. Ind. Inf.* **2017**, *13*, 198–207. [CrossRef]
9. Yu, J.J.Q.; Hou, Y.; Li, V.O.K. Online False Data Injection Attack Detection with Wavelet Transform and Deep Neural Networks. *IEEE Trans. Ind. Inf.* **2018**, *14*, 3271–3280. [CrossRef]
10. Zhao, J.; Mili, L.; Wang, M. A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures. *IEEE Trans. Power Sys.* **2018**, *33*, 4868–4877. [CrossRef]
11. Sahoo, S.; Mishra, S.; Peng, J.C.; Dragicevic, T. A Stealth Cyber Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174. [CrossRef]
12. Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey. *IEEE Trans. Ind. Inf.* **2017**, *13*, 411–423. [CrossRef]
13. Available online: https://www.energy.gov/sites/prod/files/2018/01/f46/GMI%20Peer%20Review%20Report%202017_1-2%20FINAL%20online.pdf (accessed on 20 November 2020).
14. Shi, X.; Li, Y.; Cao, Y.; Tan, Y. Cyber-physical electrical energy systems: Challenges and issues. *Csee J. Power Energy Syst.* **2015**, *1*, 36–42. [CrossRef]
15. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [CrossRef]
16. Habib, H.F.; Lashway, C.R.; Mohammed, O.A. A Review of Communication Failure Impacts on Adaptive Microgrid Protection Schemes and the Use of Energy Storage as a Contingency. *IEEE Trans. Ind. Appl.* **2018**, *54*, 1194–1207. [CrossRef]
17. Cintuglu, M.H.; Mohammed, O.A.; Akkaya, K.; Uluagac, A.S. A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 446–464. [CrossRef]
18. Kang, K.; Son, S. Real-time data services for cyber physical systems. In Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 483–488.
19. Lin, K.; Panahi, M. A real-time service-oriented framework to support sustainable cyber-physical systems. In Proceedings of the 2010 8th IEEE International Conference on Industrial Informatics, Osaka, Japan, 13–16 July 2010; pp. 15–21.
20. Huang, H.M.; Tidwell, T.; Christopher, G.; Chenyang, L.; Xiuyu, G.; Shirley, D. Cyber-physical systems for real-time hybrid structural testing: A case study. In Proceedings of the 1st ACM/IEEE International Conference Cyber-Physical Systems, Stockholm, Sweden, 13–15 April 2010; pp. 69–78.
21. Venkataramanan, V.; Hahn, A.; Srivastava, A. CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency. *IEEE Trans. Smart Grid* **2020**, *11*, 1055–1065. [CrossRef]
22. Qian, H.; Huang, X.; Yu, H.; Chang, C.H. Real-time thermal management of 3D multi-core system with fine-grained cooling control. In Proceedings of the 2010 IEEE International 3D Systems Integration Conference (3DIC), Munich, Germany, 16–18 November 2010; pp. 1–6.
23. Wu, F.; Chu, F.; Tseng, Y. Cyber-physical handshake. In Proceedings of the ACM SIGCOMM Computer Communication Review, Toronto, ON, Canada, 15–19 August 2011; pp. 472–473.

24. Miluzzo, E.; Lane, N.D.; Fodor, K.; Peterson, R.; Lu, H.; Musolesi, M.; Eisenman, S.B.; Zheng, X.; Campbell, A.T.; Campbell, A.T.; et al. Sensing meets mobile social networks: The design, implementation and evaluation of the cenceme application. In Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, Raleigh, NC, USA, 5–7 November 2008; pp. 337–350.
25. Craciunas, S.S.; Haas, A.; Kirsch, C.M.; Payer, H.; Röck, H.; Rottmann, A.; Sokolova, A.; Trummer, R.; Love, J.; Sengupta, R. Information-acquisition-as-a-service for cyber-physical cloud computing. In *2nd USENIX Conference on Hot Topics in Cloud Computing*; USENIX Association: Berkeley, CA, USA, 2010; p. 14.
26. Zhang, W.; Kamgarpour, M.; Sun, D.; Tomlin, C.J. A Hierarchical Flight Planning Framework for Air Traffic Management. *Proc. IEEE* **2012**, *100*, 179–194. [[CrossRef](#)]
27. Kim, T. Blockchain-Based Security Framework for IoT-Enabled Solar Micro Inverters: Opportunities and Challenges. In Proceedings of the CyberPELS 2019 Presentations, Knoxville, TN, USA, 29 April–1 May 2019.
28. Available online: <https://www.nrel.gov/grid/virtual-oscillator-controls.html> (accessed on 20 November 2020).
29. Carlson, R.; Rohde, K. Consequence-driven Cybersecurity for High Power EV Charging Infrastructure. In Proceedings of the CyberPELS 2019 Presentations, Knoxville, TN, USA, 1 May 2019.
30. Available online: <https://inl.gov/research-programs/control-systems-cyber-security/> (accessed on 20 November 2020).
31. Saleem, D. Design Considerations of Cryptographic Module for Distributed Energy Resources. In Proceedings of the CyberPELS 2019 Presentations, Knoxville, TN, USA, 15 May 2019.
32. Available online: <https://www.energy.gov/sites/prod/files/2018/12/f58/NREL%20-%20Module-OT.PDF> (accessed on 20 November 2020).
33. Siddiqui, A.S.; Chowdhury, P.R.; Gui, Y.; Manjrekar, M.; Essakiappan, S.; Saqib, F. Design for Secure Reconfigurable Power Converters. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS), Knoxville, Tennessee, 29 April–1 May 2019.
34. Johnson, J. Securing Vehicle Charging Infrastructure. In Proceedings of the CyberPELS 2019 Presentations, Knoxville, TN, USA, 29 April–1 May 2019.
35. Harvey, M.; Long, D.; Reinhard, K. Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security. In Proceedings of the 2014 Power and Energy Conference at Illinois (PECI), Champaign, IL, USA, 28 February–1 March 2014; pp. 1–8.
36. 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.* **2020**, *16*, 5643–5654. [[CrossRef](#)]
37. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [[CrossRef](#)]
38. ISO/IEC. *ISO/IEC 27001:2013: Information Technology Security Techniques Information Security Management Systems Requirements*; ISO: Geneva, Switzerland, 2013.
39. ISO/IEC. *ISO/IEC 27002:2013: Information Technology –Security Techniques –Code of Practice for Information Security Controls*; ISO: Geneva, Switzerland, 2013.
40. Barbara, L.; Bohua, Y. *GB/T 22239:2008–Information Security Technology–Baseline for Classified Protection of Information System Security*; Technical Report; National Standard of the People’s Republic of China: Beijing, China, 2008.
41. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. *NIST SP 800-82 Guide to Industrial Control Systems ICS Security Revision 2*; Technical Report; NIST: Gaithersburg, MD, USA, 2015.
42. CEN-CENELEC-ETSI Smart Grid Coordination Group, SG-CG/M490/H_Smart Grid Information Security. Technical Report. 2014. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf (accessed on 20 November 2020).
43. NIST. *NIST SP 1108r3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*; Technical Report; IST: Gaithersburg, MD, USA, 2014. [[CrossRef](#)]
44. European Commission. M/490 Smart Grid Mandate Standardization Mandate to European Standardisation Organisations ESOS to support European Smart Grid deployment. Technical Report. 2011. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/2011_03_01_mandate_m490_en.pdf (accessed on 20 November 2020).
45. OpenSG, Security Working Group. 2017. Available online: <http://osgug.ucaiug.org/utilisec> (accessed on 20 November 2020).
46. DKE. *German Roadmap E-Energy/Smart Grid 2.0*; Technical Report; German Commission for Electrical, Electronic & Information Technologies of DIN and VDE: Ann Arbor, MI, USA, 2013.
47. State Grid Corporation of China. *SGCC Framework and Roadmap to Strong & Smart Grid Standards*; Technical Report; State Grid Corporation of China: Beijing, China, 2010.
48. IEC. Smart Grid Standards Map 2017. Available online: <http://smartgridstandardsmap.com/> (accessed on 20 November 2020).
49. IEEE Standards Association. IEEE Smart Grid Interoperability Series of Standards. IEEE, 2015. Available online: http://grouper.ieee.org/groups/scc21/2030_series/2030_series_index.html (accessed on 20 November 2020).
50. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-physical system security for the electric power grid. *Proc. IEEE* **2012**, *100*, 210–224. [[CrossRef](#)]
51. NIST. *Guidelines for Smart Grid Cyber Security: Volume 3; Supportive Analyses and References*; NIST: Gaithersburg, MD, USA, 2010.
52. Chlela, M. Cyber Security Enhancement Against Cyber-Attacks on Microgrid Controllers. Ph.D. Thesis, McGill University, Montréal, QC, Canada, 2017.
53. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM Sigcomm Comput. Commun. Rev.* **2004**, *34*, 39–53. [[CrossRef](#)]

54. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *Commun. Surv. Tutor. IEEE* **2013**, *15*, 2046–2069. [[CrossRef](#)]
55. NISTIR 7628: *Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*; The Smart Grid Interoperability Panel–Cyber Security Working Group: Washington, DC, USA, 2010.
56. Liu, Y.; Reiter, M.K.; Ning, P. False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 21–32.
57. 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](#)]
58. 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. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 717–729. [[CrossRef](#)]
59. Chen, J.; Liang, G.; Cai, Z.; Hu, C.; Xu, Y.; Luo, F.; Zhao, J. Impact analysis of false data injection attacks on power system static security assessment. *J. Mod. Power Syst. Clean Energy* **2016**, *4*, 496–505. [[CrossRef](#)]
60. Tan, S.; Song, W.-Z.; Stewart, M.; Yang, J.; Tong, L. Online data integrity attacks against real-time electrical market in smart grid. *IEEE Trans. Smart Grid* **2018**, *9*, 313–322. [[CrossRef](#)]
61. Zhao, C.; He, J.; Cheng, P.; Chen, J. Analysis of consensus-based distributed economic dispatch under stealthy attacks. *IEEE Trans. Ind. Electron.* **2017**, *64*, 5107–5117. [[CrossRef](#)]
62. Li, P.; Liu, Y.; Xin, H.; Jiang, X. A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks. *IEEE Trans. Ind. Inf.* **2018**, *14*, 4343–4352. [[CrossRef](#)]
63. Xie, L.; Mo, Y.; Sinopoli, B. Integrity Data Attacks in Power Market Operations. *IEEE Trans. Smart Grid* **2011**, *2*, 659–666. [[CrossRef](#)]
64. Thomas, R.J.; Tong, L.; Jia, L.; Kosut, O.E. Some economic impacts of bad and malicious data. *PSerc 2010 Workshop* **2010**, *1*, 1.
65. Xie, L.; Mo, Y.; Sinopoli, B. False data injection attacks in electricity markets. In Proceedings of the IEEE 2010 SmartGridComm, Gaithersburg, MD, USA, 4–6 October 2010.
66. Jia, L.; Thomas, R.J.; Tong, L. Impacts of malicious data on real-time price of electricity market operations. In Proceedings of the IEEE Hawaii International Conference on System Sciences (HICSS), Maui, HI, USA, 4–7 January 2012; pp. 1907–1914.
67. Liu, X.; Shahidehpour, M.; Cao, Y.; Wu, L.; Wei, W.; Liu, X. Microgrid Risk Analysis Considering the Impact of Cyber Attacks on Solar PV and ESS Control Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1330–1339. [[CrossRef](#)]
68. Gholami, S.; Saha, S.; Aldeen, M. A cyber-attack resilient control for distributed energy resources. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conf. Europe (ISGT-Europe), Torino, Italy, 26–29 September 2017; pp. 1–6.
69. Beg, O.A.; Johnson, T.T.; Davoudi, A. Detection of false-data injection attacks in cyber-physical DC microgrids. *IEEE Trans. Ind. Inf.* **2017**, *13*, 2693–2703.
70. Hao, J.; Kang, E.; Sun, J.; Wang, Z.; Meng, Z.; Li, X.; Ming, Z. An Adaptive Markov Strategy for Defending Smart Grid False Data Injection from Malicious Attackers. *IEEE Trans. Smart Grid* **2018**, *9*, 2398–2408. [[CrossRef](#)]
71. Farraj, A.; Hammad, E.; Kundur, D. On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control. *IEEE Trans. Ind. Inf.* **2017**, *13*, 3322–3333. [[CrossRef](#)]
72. Farraj, A.; Hammad, E.; Kundur, D. A systematic approach to delay adaptive control design for smart grids. In Proceedings of the IEEE International Conference on Smart Grid Communications, Miami, FL, USA, 2–5 November 2015; pp. 768–773.
73. Farraj, A.; Hammad, E.; Kundur, D. Enhancing the performance of controlled distributed energy resources in noisy communication environments. In Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering, Vancouver, BC, Canada, 15–18 May 2016; pp. 1–4.
74. Farraj, A.; Hammad, E.; Kundur, D. A cyber-physical control framework for transient stability in smart grids. *IEEE Trans. Smart Grid* **2016**, *9*, 1205–1215. [[CrossRef](#)]
75. Bobba, R.B.; Rogers, K.M.; Wang, Q.; Khurana, H.; Nahrstedt, K.; Overbye, T.J. Detecting false data injection attacks on DC state estimation. In Proceedings of the Preprints 1st Workshop Secure Control Systems (CPSWEEK), Stockholm, Sweden, 12–15 April 2010; pp. 1–9.
76. Salmeron, J.; Wood, K.; Baldick, R. Analysis of electric grid security under terrorist threat. *IEEE Trans. Power Syst.* **2004**, *19*, 905–912. [[CrossRef](#)]
77. Nejabatkhah, F.; Li, Y.W.; Tian, H. Power Quality Control of Smart Hybrid AC/DC Microgrids: An Overview. *IEEE Access* **2019**, *7*, 52295–52318. [[CrossRef](#)]
78. Unamuno, E.; Barrena, J.A. Hybrid ac/dc microgrids—Part II: Review and classification of control strategies. *Renew. Sustain. Energy Rev.* **2015**, *52*, 1123–1134. [[CrossRef](#)]
79. Sou, K.C.; Sandberg, H.; Johansson, K.H. On the exact solution to a smart grid cyber-security analysis problem. *IEEE Trans. Smart Grid* **2013**, *4*, 856–865. [[CrossRef](#)]
80. Abur, A.; Exposito, A.G. *Power System State Estimation: Theory and Implementation*; CRC Press: New York, NY, USA, 2004.
81. Monticelli, A. Electric power system state estimation. *Proc. IEEE* **2000**, *88*, 262–282. [[CrossRef](#)]
82. Monticelli, A. *State Estimation in Electric Power Systems*; Springer Science and Business Media, LLC: New York, NY, USA, 1999.
83. Liang, J.; Sankar, L.; Kosut, O. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Trans. Power Syst.* **2016**, *31*, 3864–3872. [[CrossRef](#)]
84. Yu, Z.H.; Chin, W.L. Blind false data injection attack using PCA approximation method in smart grid. *IEEE Trans. Smart Grid* **2015**, *6*, 1219–1226. [[CrossRef](#)]

85. Liu, X.; Bao, Z.; Lu, D.; Li, Z. Modeling of local false data injection attacks with reduced network information. *IEEE Trans. Smart Grid* **2015**, *6*, 1686–1696. [[CrossRef](#)]
86. Hug, G.; Giampapa, J.A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Trans. Smart Grid* **2012**, *3*, 1362–1370. [[CrossRef](#)]
87. Zhao, J.; Zhang, G.; Dong, Z.Y.; Wong, P.K. Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation. *IEEE Trans. Smart Grid* **2016**, *7*, 6–8. [[CrossRef](#)]
88. Liu, X.; Li, Z. False data attacks against AC state estimation with incomplete network information. *IEEE Trans. Smart Grid* **2017**, *8*, 2239–2248. [[CrossRef](#)]
89. Chakhchoukh, Y.; Ishii, H. Coordinated Cyber-Attacks on the Measurement Function in Hybrid State Estimation. *IEEE Trans. Power Syst.* **2015**, *30*, 2487–2497. [[CrossRef](#)]
90. Zhuang, P.; Deng, R.; Liang, H. False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems. *IEEE Trans. Smart Grid* **2019**, *10*, 6000–6013. [[CrossRef](#)]
91. 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](#)]
92. Isozaki, Y.; Yoshizawa, S.; Fujimoto, Y.; Ishii, H.; Ono, I.; Onoda, T.; Hayashi, Y. Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids with PVs. *IEEE Trans. Smart Grid* **2016**, *7*, 1824–1835. [[CrossRef](#)]
93. Chen, C.; Zhang, K.; Yuan, K.; Zhu, L.; Qian, M. Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1932–1941. [[CrossRef](#)]
94. Domínguez-García, A.D.; Hadjicostis, C.N.; Vaidya, N.H. Resilient networked control of distributed energy resources. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 1137–1148. [[CrossRef](#)]
95. Qi, J.; Hahn, A.; Lu, X.; Wang, J.; Liu, C.-C. Cybersecurity for distributed energy resources and smart inverters. *IET Cyber Phys. Syst. Theory Appl.* **2016**, *1*, 28–39. [[CrossRef](#)]
96. Mercier, P.; Cherkaoui, R.; Oudalov, A. Optimizing a battery energy storage system for frequency control application in an isolated power system. *IEEE Trans. Power Syst.* **2009**, *24*, 1469–1477. [[CrossRef](#)]
97. Wei, J.; Kundur, D.; Zourmtos, T.; Butler-Purry, K. A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control. *IEEE Trans. Smart Grid* **2014**, *5*, 2687–2700. [[CrossRef](#)]
98. Farraj, A.; Hammad, E.; Kundur, D. A cyber-enabled stabilizing control scheme for resilient smart grid systems. *IEEE Trans. Smart Grid* **2016**, *7*, 1856–1865. [[CrossRef](#)]
99. Sargolzaei, A.; Yen, K.; Abdelghani, M. Delayed inputs attack on load frequency control in smart grid. In Proceedings of the IEEE PES Innovative Smart Grid Technology Conference, Washington, DC, USA, 19–22 February 2014; pp. 1–5.
100. Esfahani, P.M.; Vrakopoulou, M.; Margellos, K.; Lygeros, J.; Andersson, G. Cyber-attack in a two-area power system: Impact identification using reachability. In Proceedings of the 2010 American Control Conference, Baltimore, MD, USA, 30 June–2 July 2010; pp. 962–967.
101. Esfahani, P.M.; Vrakopoulou, M.; Margellos, K.; Lygeros, J.; Andersson, G. A robust policy for automatic generation control cyber-attack in two area power network. In Proceedings of the 49th IEEE Conference Decision Control, Atlanta, GA, USA, 15–17 December 2010; pp. 5973–5978.
102. Tan, R.; Nguyen, H.H.; Foo, E.Y.S.; Dong, X.; Yau, D.K.Y.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Optimal false data injection attack against automatic generation control in power grids. In Proceedings of the 7th International Conference Cyber-Physical Systems, Vienna, Austria, 11–14 April 2016; pp. 1–10.
103. Manson, S.; Anderson, D. Cybersecurity for Protection and Control Systems: An Overview of Proven Design Solutions. *IEEE Ind. Appl. Mag.* **2019**, *25*, 14–23. [[CrossRef](#)]
104. TKim, T.; Poor, H.V. Strategic protection against data injection attacks on power grids. *IEEE Trans. Smart Grid* **2011**, *2*, 326–333.
105. Bi, S.; Zhang, Y.J. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Trans. Smart Grid* **2014**, *5*, 1216–1227. [[CrossRef](#)]
106. 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](#)]
107. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control Netw. Syst.* **2014**, *1*, 370–379. [[CrossRef](#)]
108. Liu, L.; Esmalifalak, M.; Ding, Q.; Emesih, V.A.; Han, Z. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Trans. Smart Grid* **2014**, *5*, 612–621. [[CrossRef](#)]
109. Zhao, J.; Zhang, G.; Scala, M.L.; Dong, Z.Y.; Chen, C.; Wang, J. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. *IEEE Trans. Smart Grid* **2017**, *8*, 1580–1590. [[CrossRef](#)]
110. Xu, R.; Wang, R.; Guan, Z.; Wu, L.; Wu, J.; Du, X. Achieving efficient detection against false data injection attacks in smart grid. *IEEE Access* **2017**, *5*, 13787–13798. [[CrossRef](#)]
111. Guan, Y.; Ge, X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. *IEEE Trans. Signal Inf. Process. Netw.* **2018**, *4*, 48–59. [[CrossRef](#)]
112. 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](#)]

113. Adhikari, U.; Morris, T.H.; Pan, S. Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection. *IEEE Trans. Smart Grid* **2016**, *9*, 3928–3941. [[CrossRef](#)]
114. 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](#)]
115. 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 Netw. Learn. Syst.* **2016**, *27*, 1773–1786. [[CrossRef](#)] [[PubMed](#)]
116. Khanna, K.; Panigrahi, B.K.; Joshi, A. AI-based approach to identify compromised meters in data integrity attacks on smart grid. *IET Gener. Transmiss. Distrib.* **2018**, *12*, 1052–1066. [[CrossRef](#)]
117. 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](#)]
118. Rawat, D.; Bajracharya, C. Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Process. Lett.* **2015**, *22*, 1652–1656. [[CrossRef](#)]
119. Rana, M.M.; Li, L.; Su, S.W. Cyber-attack protection and control of microgrids. *IEEE/CAA J. Autom. Sin.* **2017**, *5*, 602–609. [[CrossRef](#)]
120. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in AC state estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [[CrossRef](#)]
121. Liu, T.; Sun, Y.; Liu, Y.; Gui, Y.; Zhao, Y.; Wang, D.; Shen, C. Abnormal traffic-indexed state estimation: A cyber-physical fusion approach for smart grid attack detection. *Future Gener. Comput. Syst.* **2015**, *49*, 94–103. [[CrossRef](#)]
122. Tian, J.; Tan, R.; Guan, X.; Liu, T. Enhanced hidden moving target defense in smart grids. *IEEE Trans. Smart Grid* **2018**, *10*, 2208–2223. [[CrossRef](#)]
123. Chlela, M.; Mascarella, D.; Joos, G.; Kassouf, M. Cyber-resilient control of inverter based microgrids. In Proceedings of the 2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Washington, DC, USA, 7–9 December 2016; pp. 841–845.
124. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [[CrossRef](#)]
125. Ntalampiras, S. Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling. *IEEE Trans. Ind. Inform.* **2015**, *11*, 104–111. [[CrossRef](#)]
126. Fawzi, H.; Tabuada, P.; Diggavi, S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Control* **2014**, *59*, 1454–1467. [[CrossRef](#)]
127. Chen, Y.; Kar, S.; Moura, J.M. Cyber-physical systems: Dynamic sensor attacks and strong observability. In Proceedings of the 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brisbane, Australia, 19–24 April 2015; pp. 1752–1756.
128. Mo, Y.; Chabukswar, R.; Sinopoli, B. Detecting integrity attacks on SCADA systems. *IEEE Trans. Control Syst. Technol.* **2014**, *22*, 1396–1407.
129. Chen, Y.; Kar, S.; Moura, J.M. Dynamic attack detection in cyber physical systems with side initial state information. *IEEE Trans. Autom. Control* **2016**, *62*, 4618–4624. [[CrossRef](#)]
130. Liu, S.; Liu, X.P.; el Saddik, A. Denial-of-service (DOS) attacks on load frequency control in smart grids. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
131. Liu, S.; Liu, P.X.; Wang, X. Effects of cyber-attacks on islanded microgrid frequency control. In Proceedings of the 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanchang, China, 4–6 May 2016; pp. 461–464.
132. Zhu, M.; Martinez, S. Discrete-time dynamic average consensus. *Automatica* **2010**, *46*, 322–329. [[CrossRef](#)]
133. Siddharth, S.; Manimaran, G. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591.
134. Jin, D.; Li, Z.; Hannon, C.; Chen, C.; Wang, J.; Shahidehpour, M.; Lee, C.W. Toward a Cyber Resilient and Secure Microgrid Using Software-Defined Networking. *IEEE Trans. Smart Grid* **2017**, *8*, 2494–2504. [[CrossRef](#)]