3-3-2021

Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review

Fazel Mohammadi
University of Windsor

energies

MDPI

Review

Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review

Fazel Mohammadi

Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 1K3, Canada; fazel@uwindsor.ca or fazel.mohammadi@ieee.org

Abstract: In this paper, a brief survey of measurable factors affecting the adoption of cybersecurity enhancement methods in the smart grid is provided. From a practical point of view, it is a key point to determine to what degree the cyber resilience of power systems can be improved using cost-effective resilience enhancement methods. Numerous attempts have been made to the vital resilience of the smart grid against cyber-attacks. The recently proposed cybersecurity methods are considered in this paper, and their accuracies, computational time, and robustness against external factors in detecting and identifying False Data Injection (FDI) attacks are evaluated. There is no all-inclusive solution to fit all power systems requirements. Therefore, the recently proposed cyber-attack detection and identification methods are quantitatively compared and discussed.

Keywords: cyber-attacks; cyber-attacks detection; cyber-attacks identification; cybersecurity; False Data Injection (FDI) attacks; cyber resilience; smart grid

Citation: Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380. https://doi.org/10.3390/en14051380

Academic Editors: William Holderbaum and Mouloud Denai

Received: 10 January 2021
Accepted: 6 February 2021
Published: 3 March 2021

1. Introduction

The smart grid is an advanced infrastructure in modern power systems with numerous benefits, such as the efficient integration of Renewable Energy Sources (RESs). However, the smart grid is highly dependent on advanced communication infrastructure since a large amount of data should be exchanged to properly operate such a complex system [1–3]. Hence, the smart grid has become more vulnerable to cyber-attacks. Communication systems attacks can significantly increase operation costs [4] or damage proper system operation [5]. For instance, cyber-attacks against Ukraine's power grids in 2015 led to a widespread power outage for several hours [1]. To ensure the safe and proper operation of the smart grid, power systems operators need to efficiently detect, identify, and locate such attacks and take immediate actions to protect the entire grid. This process is called cyber resilience. From the power systems operators' point of view, the initial step of resilience enhancement in the attack phase and/or post-attack phase is to successfully detect cyber-attacks. This is due to the unpredictable nature of the attack. Therefore, many research studies with different approaches have been carried out in the last decade to successfully detect and identify cyber-attacks as a part of enhancing the resilience of the smart grid [5–9].

Power systems operators face different challenges in detecting and identifying cyber-attacks in the smart grid. The major challenges are as follows:

- The accuracy of cyber-attack detection and identification.
- Computational burden when detecting and identifying cyber-attacks.
- Robustness against various factors affecting cyber-attack detection and identification.

Such issues must be well-addressed by cyber-attack detection and identification methods. Otherwise, attackers can successfully damage power grids.

In recent years, several research studies have been carried out to ensure cyber-attack detection and identification accuracy, as well as to minimize computational time and improve robustness against external factors. In [10], an Artificial Intelligence (AI)-based method

was proposed to accurately identify malicious meters. In [11], a machine learning-based method was presented to increase the accuracy of identifying various sets of disturbances and cyber-attacks in power grids. Online identification of cyber-attacks was formulated as a Partially Observable Markov Decision Process (POMDP) in [12] and a model-free Reinforcement Learning (RL) was presented to deal with different POMDPs. The robustness of the method proposed in [12] was improved by training the defender with low magnitude attacks and reducing the attacking space of an attacker. In [13], a multivariate Gaussian-based model was presented to accurately and effectively detect transient and steady cyber-attacks in power distribution systems. An unsupervised method that employs the isolation forest algorithm was proposed in [14] for the accurate identification of covert data integrity assault in the smart grid. In addition, the proposed method operated with low complexity, leading to faster detection of the attack. In [15], an extremely randomized trees-based machine learning scheme was introduced to accurately detect stealthy cyber-attacks in the smart grid. Furthermore, the proposed approach had lower computational time compared to different machine learning-based attack detection techniques, and it showed robustness against noisy data. In [16], the differences between data manipulation changes and physical grid changes were investigated, which enabled the attack detection method to properly operate under concept drift. The proposed unsupervised False Data Injection (FDI) attack method in [17] accurately detected attacks under various conditions and presented robustness against the reconfiguration and integration of RESs into power systems. In [18], a detection method based on the Maximum Likelihood (ML) estimation was developed to accurately detect FDI attacks in the smart grid. In addition, the proposed method was capable of reducing the computational burden by decreasing the complexity of the ML estimation problem. In [19], an accurate and computationally efficient method to detect FDI attacks in the smart grid was investigated. The proposed method showed robustness against noisy data. The Markov Decision Process (MDP) approach in [20] was used to detect cyber-attacks in a dynamic environment and assess the vulnerability of power grids to such attacks. The proposed method in [21] showed robustness in identifying FDI attacks under noisy conditions.

This paper mainly focuses on cyber-attack challenges and the resilience of the smart grid. FDI attacks, which are the most common type of cyber-attacks, are reviewed in this paper. Further comparison and discussion of the recently published research studies are provided.

The rest of this paper is organized as follows. Section 2 presents the fundamentals of cyber-attacks detection and identification in the smart grid and Section 3 discusses recent cyber-attack detection and identification methods from a quantitative point of view. In Section 4, methods are compared based on resilience criteria. Lastly, Section 5 concludes this paper.

2. Fundamentals of Cyber-Attacks Detection and Identification in the Smart Grid

The smart grid, as one of the emerging cyber-physical systems, is formed based on physical power infrastructure, including power generation, distribution, and consumption systems, with the dense integration of communication infrastructure with specific hierarchical control architectures [22,23]. At the local control level, communication systems mainly consist of smart sensors and actuation units, and at the higher control levels, e.g., cyber layers, such systems consist of smart controllers, smart meters, Phase Measurement Units (PMUs), distributed generations, and automation units [24]. The high penetration of communication infrastructure into the smart grid makes them highly susceptible to cyber-attacks. The majority of cybersecurity threats in power distribution systems refer to intelligent buildings equipped with smart meters, which arise from four types of threat agents: (1) malicious outsiders, (2) malicious insiders, (3) non-malicious insiders, and (4) nature. The risks from malicious agents may be indiscriminate, such as the distribution of malware and viruses or targeted attacks attempting to compromise, disrupt, or damage specific systems. Threats from nature relate to damage or interference to advanced meter-

ing building systems from solar, weather, animal, or insect threat agents. It is crucial to recognize such interferences in anomaly detection modules.

Denial of Service (DoS) and FDI attacks are the most common forms of cyber-attacks in the smart grid [25]. In DoS attacks, the attacker usually targets communication infrastructure to entirely disrupt the data packet transfer process. In such attacks, either the communication bandwidth can be persistently overloaded with streams of scam data or the transfer of control signals is particularly targeted by synchronized data flooding [25]. In contrast to DoS attacks aiming at interrupting transferring data, FDI attacks commonly occur as data packet manipulation with different degrees of severity [25]. In addition, FDI attacks can target various data packets within communication protocols, such as command and feedback signals, protective relays, and sensor/actuator software calibrations [25]. FDI attacks can have broader impacts on the smart grid, such as weak performance, instability, and blackouts [26].

In smart grid cybersecurity enhancement, it is vital to precisely detect and identify any malicious cyber-attacks as quickly as possible, implement protective measures to improve/restore the system resilience against cyber-attacks, and optimize the computational complexity and costs. The major challenge in cyber-attack detection is properly distinguishing the common system disturbances and dynamics, such as load switching, connection/disconnection of power generation units, and changes in command signals, from cyber-attacks. Additionally, it is crucial to consider the nonlinear nature of the system model and use advanced control techniques to effectively detect cyber-attacks in the presence of system nonlinearities, uncertainties, and disturbances.

One solution is to estimate the system states under the normal operating condition and compare them with the actual system states to detect deviations and abnormalities. In [27], a Weighted Least Square (WLS) estimator was investigated to estimate the states of the system under the steady-state condition. To address the convergence issue related to WLS, the recursive WLS was proposed in [28]. The transient analysis of power systems needs dynamic estimation techniques that consider the previous states of the system. Kalman Filtering (KF) is a well-known non-static estimation method that contains a correction term to minimize state estimation errors [29]. Taking the system nonlinearities into account, Extended Kalman Filtering (EKF) was investigated in [30,31] to detect FDI attacks. In both model-dependent detection methods, the model inaccuracy causes a progressive change in their performance and may result in a false detection. In contrast, the use of precise models and recursive methods increases the computational burden to correctly estimate the state of the system, which makes it challenging for practical implementation.

To overcome the challenges related to model-dependent detection methods, data-driven techniques have been proposed. The data-driven methods can be generally classified into three main categories: (1) supervised, (2) unsupervised, and (3) semi-supervised learning methods. In supervised learning algorithms, the labeled dataset is employed to train the algorithm, where each input is related to a specific output. Supervised learning algorithms are mainly employed when a wide range of cyber-attack scenarios can be generated to collect the required training dataset [32,33]. In order to find a meaningful pattern among the unlabeled inputs, unsupervised algorithms can be utilized. Such algorithms are less popular than supervised algorithms for detecting cyber-attacks. In addition, they can exclusively be applied when cyber-attacks are not flagged in all collected datasets [34]. Collecting precise training datasets under various operating conditions for both supervised and unsupervised learning methods is mandatory, and accordingly, the detection methods become highly vulnerable to overfitting, where the performance of a method strictly depends on the collected datasets. Hence, the algorithm suffers from a lack of proper detection of cyber-attacks scenarios excluded from the training dataset. To properly address the mentioned issue, a combined data-driven and model-based detection method was investigated in [35]. In addition, semi-supervised learning-based methods can be used when the next control action should be corrected/modified based on the feedback of previous control actions using a trial and error method [36]. Overall, the

main barriers to cybersecurity enhancement for the smart grid in both data-driven and model-based detection schemes are the detection accuracy, computational burden, and robustness against external factors.

3. Cyber-Attack Detection and Identification Methods

3.1. Data-Driven Methods

Data-driven methods, e.g., machine learning techniques, have been widely used to efficiently detect cyber-attacks in the smart grid [37].

In [10], a supervised AI-based load estimator was proposed to determine the meters affected by FDI attacks by comparing the values of the estimated loads and their actual measurements. The presented model was able to detect FDI attacks, which led to a cumulative error of 1% in state variables. An additional load estimator was added to the existing model to effectively determine the tampered meters. A single hidden-layer forward Neural Networks (NN) and Artificial Neural Networks (ANN) was proposed for a proper learning rate. Such networks were trained using historical data, which helped to detect the FDI attack by the proposed estimator even if the attack was generated from the minimum number of compromised meters. In the case of a large-scale FDI attack, this method guarantees accurately detecting the attack and the tempered meters. In [11], a supervised learning method using historical data and log information for cyber-attack detection in the smart grid was presented. The accuracy and detection rates of the presented method were reported to be 93.9% and 93.6%, respectively, which were higher compared to several newly-proposed schemes, such as the K-Nearest Neighbors (KNN) algorithm, Random Forest (RF) method, etc. In [12], the first attempt was made to detect cyber-attacks in the smart grid online using the RL method. The cyber-attack was defined as a POMDP, as the true states of the smart grid were known before the attack, while the attacker could compromise the true states of the smart grid and such changes could be unknown/unobservable to the system operator. The proposed method in [12] is a model-free scheme and as reported, it required less computational time to be performed. A single-agent RL method from the system defender point of view was trained to successfully detect low-magnitude attacks. As a result, the defender could detect minimum variations in the smart grid states regardless of the attacker's strategy. The proposed model-free scheme was robust against the unknown states of the system. In [13], a multivariate Gaussian-based method was employed to determine FDI attacks in the cyber-physical system of power distribution grids. Identification of transient and steady attacks was performed by analyzing measurement data collected by micro-PMUs. Using the K-Means clustering method, power distribution systems were divided into areas with similar voltage profiles, and, accordingly, the number of micro-PMUs was reduced. The reported accuracy and precision were reasonable for transient attack identification. In the case of steady attacks, the proposed method was developed on prediction error that could be possibly affected by the smart grid conditions. An improved regression model is capable of reducing prediction errors and increasing the accuracy of attack detection. In [14], covert data integrity assault on the smart grid was presented. To reduce the complexity of the problem, a PCA-based feature extraction mechanism was utilized to efficiently convert data in high-dimensional to low-dimensional space. An unsupervised machine learning-based algorithm, called isolation forest, was presented to detect and identify anomalies in the state estimation measurement features. Compared with the traditional machine learning-based techniques, the proposed method was more accurate. Since the computational complexity of the presented approach was low, less computational time was required to identify cyber-attacks. In [15], a supervised learning method was used to identify stealthy cyber-attacks in state estimation-measurement features of the smart grid. The Kernel Principal Component Analysis (KPCA)-based method was used to reduce the complexity of the problem due to the high-dimensional space in large-scale power systems and accurately represent the dataset in lower-dimensional space, as well as being used as an input of the extra-trees algorithm. The proposed method was robust

against noisy data because of the characteristics of KPCA. It also needed less computational time compared to other machine learning-based schemes, such as traditional PCA, and could accurately identify cyber-attacks in the smart grid. In [16], the impact of concept drift on the cybersecurity of the smart grid was investigated, i.e., distinguish physical changes from variations associated with the data manipulation in the smart grid. To assess the behavior of the proposed method in identifying cyber-attacks, a detailed analysis was conducted. In [17], a cyber-attack identification method was presented by taking the system reconfiguration and integration of RESs into account. The F-Test was used to separate the attacked state vectors from the normal state vectors. It was noted that the suspicious samples rejecting the hypothesis of the F-Test need to be fully inspected. The difference between suspected vectors and the average from a similar system state vectors using three outlier detection algorithms, including Fuzzy C-Means (FCM) clustering, Interquartile Range (IQR), and Median Absolute Deviation (MAD) methods, was used as a comparison index to analyze the failed samples. The reported results showed that the proposed method was robust against parameter changes while presenting a high degree of accuracy in identifying FDI attacks.

3.2. State Estimation Methods

Correct state estimation can help to maintain the smart grid safe and fully-controlled [38]. However, state estimators are vulnerable to FDI attacks. Such attacks can bypass Bad Data Detection (BDD) algorithms and change the state estimation.

In [18], a decentralized method based on ML estimation was proposed to detect cyber-attacks in the smart grid. The ML estimation, which could be converted into a chordal embedding space, was utilized as an attack detection tool. Using the Kron reduction of the Markov graph of phase angles, the proposed method was capable of breaking the ML estimation problem down into several local ML estimation problems. Based on the decentralized nature of the proposed method, privacy among utilities could be increased and this led to a reduction in the size of the problem, which greatly decreased computational burden. In [19], it was shown that the FDI attack detection problem can be formed as a matrix separation problem due to the nature of the attack matrix, which is a sparse matrix, and the measurement matrix, which is a low-rank matrix. The present matrix separation approaches, such as the Augmented Lagrangian Method (ALM), Low-Rank Matrix Factorization (LRMF), and Double-Noise-Dual-Problem (DNDP)-ALM, suffer from higher computational time and lower accuracy. An algorithm, called Go-Decomposition, was investigated to efficiently solve this problem. Under the no-noise condition, the proposed method had reasonable accuracy in the separation of FDI attacks compared to the LRMF method and had almost the same accuracy as ALM and DNDP-ALM methods. The computational time of the proposed method to solve the problem was relatively low and it was capable of handling large-scale attacks in the smart grid. In [20], an MDP was presented to model the attackers attacking strategy. Two levels of attackers' knowledge scenarios about the smart grid were analyzed. Attackers could predict states of the smart grid for a small interval, which was defined as a finite-horizon MDP. The optimal attacking strategy was determined from the attackers' perspective since the attack likelihood was later analyzed based on the attack strategy. The results of the vulnerability assessment showed the robustness of the proposed method against parametric uncertainties in an MDP problem and the operators' dispatch policy. The proposed approach in [21] investigated the vulnerability of power systems nonlinear state estimators to FDI attacks from the operator point of view. A robust approach was proposed to detect FDI attacks by analyzing the measurement statistical consistency using a subset of secure PMU measurements. Such secure measurements can be used to identify FDI attacks if they are not affected by anomalies while making the system fully-observable. In addition, precise identification of FDI attacks was guaranteed using a robust Huber M-estimator. The proposed method was robust against secure measurements containing bad and noisy data. In [39], it was shown that FDI attacks could be launched on power distribution systems since the systems states

were estimated from power flow measurements. The simulation results demonstrated that by correctly estimating one state of the system, the FDI attack could be performed without being detected by BDD methods. In [40], the impact of FDI attacks on estimated states of power grids was investigated assuming attackers have partial knowledge of the system information. Then, the partial grid FDI attack was applied to demonstrate how FDI attacks could be undetectable. Subsequently, a method based on state estimation was presented to identify a subset of existing measurements and protect power grids against undetectable FDI attacks aimed at compromising the state of the system. In [41], an algorithm was proposed to protect the smart grid against FDI attacks by securing $n - 1$ meters, called the Basic Measurement Set (BMS), in n-bus power systems. Then, the method was extended to find a subset of the optimal BMS to minimize the vulnerability of the system if less than $n - 1$ meters could be secured.

3.3. Other Methods

As stated earlier, the main goal in cyber-attacks is to manipulate the state estimation of the smart grid. Except for the data-driven and state estimation methods, other approaches, such as Game Theory, have been used for vulnerability assessment of the smart grid to potential cyber-attacks [9,37].

In [42], the characteristics of FDI attacks were determined from the attacker's perspective to find the weaknesses of existing BDD methods. Then, from the defender's perspective, a two-layer defense model, including identification and protection schemes, was proposed. A zero-sum static Game Theory was employed to identify the optimal strategies of the defender and attacker. In [43], the minimax-regret method was utilized to determine a cost-effective policy against the load redistribution attack. The algorithm attempted to minimize the economic loss of a load redistribution attack under load variations. Since the defense strategy of the smart grid is highly sensitive to time-varying loading conditions, it is mandatory to use an algorithm against load variations. To address this requirement, a Game-Theoretic model was proposed under various loading conditions, and then, a multi-level intractable problem was converted to a bi-level tractable optimization problem. A greedy implicit enumeration algorithm was also employed to find the global optimum. The impact of FDI attacks on compromising the forecasted demand data was investigated in [44]. To assist the utilities in preventing such attacks, a Game Theory model was proposed, and the Nash equilibrium was determined. It is noted that no monitoring is the appropriate strategy for certain types of low-impact cyber-attacks whereas mixed strategies should be developed for the rest of the attacks. In [45], a game between attacker and defender in a dynamic cyber-attack scenario was investigated. From the attacker's perspective, critical power substations were identified and targeted to maximize the system damage with an allocated budget. Simultaneously, from the defender's perspective, most critical power substations were secured to minimize the system damage with an allocated protection budget. The worst dynamic attack and the best defense strategy were specified from polynomial-time algorithms. The presented algorithm was relatively efficient and simpler than the state-of-the-art algorithms and also was capable of covering a wider attack area. In [46], the cyber-physical system vulnerability assessment was proposed using a dynamic Game Theory scheme. A tri-level defender-attacker-defender mathematical programming model was investigated under a time-delay of the system recovery and distributed DoS attack conditions. An advanced Particle Swarm Optimization (PSO) technique was employed to solve the optimization problem. The proposed model was highly efficient in determining vulnerable power transmission lines of power grids.

4. Comparison of Different Cyber-Attack Detection and Identification Techniques

Table 1 demonstrates a comparison of different cyber-attack detection and identification schemes discussed in this paper. Three resilience criteria, including accuracy, computational burden, and robustness against external factors, are used for comparison.

Table 1. Comparison of different cyber-attack detection and identification techniques.

Reference	Main Objective(s)	Proposed Method	Resilience Criteria		
			Accuracy	Computational Burden	Robustness against External Factors
[10]	Malicious Meters Identification	Artificial Intelligence-Based Algorithm	✓	-	-
[11]	Cyber-Attack Detection and Identification	Supervised Learning Algorithm	✓	-	-
[12]	Online Cyber-Attack Identification	Reinforcement Learning-Based Algorithm	✓	✓	✓
[13]	Cyber-Attack Detection	Multivariate Gaussian-Based Method	✓	-	-
[14]	Cyber-Attack Detection	Isolation Forest PCA-Based Method	✓	✓	-
[15]	Cyber-Attack Detection	Extremely Randomized Trees KPCA-Based Method	✓	✓	✓
[16]	Cyber-Attack Detection	Isolation Forest Method	✓	-	✓
[17]	Cyber-Attack Detection and Identification	Unsupervised Learning Algorithm	✓	-	✓
[18]	Cyber-Attack Detection	Gaussian Markov Random Field Method	✓	✓	-
[19]	Cyber-Attack Detection	Go-Decomposition Algorithm	✓	-	✓
[20]	Intrusion Detection and Vulnerability Analysis	Markov Decision Process-Based Method	-	✓	✓
[21]	Intrusion Detection and Vulnerability Analysis	Huber M-Estimator	-	✓	✓
[39]	Cyber-Attack Vulnerability Analysis	State Estimation	✓	-	✓
[40]	Cyber-Attack Vulnerability Analysis	State Estimation Based on Power Flow Analysis	✓	✓	-
[41]	Cyber-Attack Vulnerability Analysis	State Estimation	✓	-	-
[42]	Cyber-Attack Detection and Identification	Zero-Sum Static Game Theory	✓	-	-
[43]	Cyber-Attack Detection	Game Theory Based on Minimax-Regret Method	✓	✓	✓
[44]	Cyber-Attack Detection and Identification	Game Theory	✓	-	✓
[45]	Cyber-Attack Detection	Game Theory	✓	✓	-
[46]	Cyber-Attack Detection and Vulnerability Analysis	Dynamic Game Theory	✓	-	-

This table shows that accuracy has been at the center of attention in recent research studies. Accuracy remains a major challenge in preventing data-driven-based techniques from being widely used in the power industry. The computational burden can be directly related to the cost as, in most cases, the computations can be enhanced by deploying a stronger processor and computing methods, e.g., parallel or distributed computing, which require financial investments. Therefore, the computational burden may translate into the unwanted but unavoidable cost of safe operation. Robustness against external factors is also discussed in different sets of literature. However, to what degree the security of the smart grid is enhanced is an important concern that has remained unresolved in many recent research studies. Table 1 also indicates that online cyber-attack detection and identification are the essential objectives among other operating objectives. The volatility, intermittent nature, and unpredictability of RESs behavior creates a high level of uncertainty and stochasticity in energy management systems. On the other hand, the integration of the Internet-of-Things (IoT), smart meters, and PMUs provides sophisticated attack surfaces. This increases the difficulties in the control and operation of the smart grid, particularly, cyber-attack detection and identification in narrow time windows. Among the variety of the proposed models, Game Theory and RL satisfy all three criteria, showing the importance of AI models in dealing with the minimum number of datasets for training and testing and the complicated behavior of attacker and defender models. Future research may use such advanced methods to tackle the complexity, scalability, and difficulties of cyber-attack detection in power grids management.

5. Conclusions

This paper provided an overview of the emerging challenges in smart grid cybersecurity enhancement. In recent research studies, numerous methods have been proposed to protect the smart grid against cyber-attacks. In this paper, three resilience criteria, including accuracy, computational burden, and robustness against external factors, in False Data Injection (FDI) attacks detection and identification were further investigated. The mentioned criteria considered in this paper are all quantifiable, and they help the system operators to determine to what extent the resilience can be enhanced by proposing methods with reasonable financial resource allocation.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Aoufi, S.; Derhab, A.; Guerroumi, M. Survey of False Data Injection in Smart Power Grid: Attacks, Countermeasures and Challenges. *J. Inf. Secur. Appl.* **2020**, *54*, 102518. [CrossRef]
2. Mohammadi, F.; Neagoe, M. Emerging Issues and Challenges with the Integration of Solar Power Plants into Power Systems. In *Solar Energy Conversion in Communities–Springer Proceedings in Energy*; Springer: Cham, Switzerland, 2020.
3. Mohammadi, F.; Nazri, G.-A.; Saif, M. A Fast Fault Detection and Identification Approach in Power Distribution Systems. In Proceedings of the 2019 International Conference on Power Generation Systems and Renewable Energy Technologies, Istanbul, Turkey, 26–27 August 2019.
4. Nikmehr, N.; Moghadam, S.M. Game-Theoretic Cybersecurity Analysis for False Data Injection Attack on Networked Microgrids. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 365–373. [CrossRef]
5. Wang, Q.; Tai, W.; Tang, Y.; Ni, M. Review of the False Data Injection Attack against the Cyber-Physical Power System. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 101–107. [CrossRef]
6. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
7. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart Grids Security Challenges: Classification by Sources of Threats. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 468–483. [CrossRef]
8. Sharafeev, T.R.; Ju, O.V.; Kulikov, A.L. Cyber-Security Problems in Smart Grid Cyber Attacks Detecting Methods and Modelling Attack Scenarios on Electric Power Systems. In Proceedings of the 2018 International Conference on Industrial Engineering, Applications and Manufacturing, Moscow, Russia, 15–18 May 2018.
9. Biggio, B.; Roli, F. Wild Patterns: Ten Years after the Rise of Adversarial Machine Learning. *Pattern Recognit.* **2018**, *84*, 317–331. [CrossRef]
10. Khanna, K.; Panigrahi, B.K.; Joshi, A. AI-Based Approach to Identify Compromised Meters in Data Integrity Attacks on Smart Grid. *IET Gener. Transm. Distrib.* **2018**, *12*, 1052–1066. [CrossRef]
11. Wang, D.; Wang, X.; Zhang, Y.; Jin, L. Detection of Power Grid Disturbances and Cyber-Attacks Based on Machine Learning. *J. Inf. Secur. Appl.* **2019**, *46*, 42–52. [CrossRef]
12. Kurt, M.N.; Ogundijo, O.; Li, C.; Wang, X. Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach. *IEEE Trans. Smart Grid* **2019**, *10*, 5174–5185. [CrossRef]
13. An, Y.; Liu, D. Multivariate Gaussian-Based False Data Detection against Cyber-Attacks. *IEEE Access* **2019**, *7*, 119804–119812. [CrossRef]
14. Ahmed, S.; Lee, Y.; Hyun, S.-H.; Koo, I. Unsupervised Machine Learning-Based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2765–2777. [CrossRef]
15. Acosta, M.R.C.; Ahmed, S.; Garcia, C.E.; Koo, I. Extremely Randomized Trees-Based Scheme for Stealthy Cyber-Attack Detection in Smart Grid Networks. *IEEE Access* **2020**, *8*, 19921–19933. [CrossRef]
16. Mohammadpourfard, M.; Weng, Y.; Pechenizkiy, M.; Tajdinian, M.; Mohammadi-Ivatloo, B. Ensuring Cybersecurity of Smart Grid against Data Integrity Attacks Under Concept Drift. *Int. J. Electr. Power Energy Syst.* **2020**, *119*, 105947. [CrossRef]
17. Mohammadpourfard, M.; Sami, A.; Weng, Y. Identification of False Data Injection Attacks with Considering the Impact of Wind Generation and Topology Reconfigurations. *IEEE Trans. Sustain. Energy* **2017**, *9*, 1349–1364. [CrossRef]
18. Moslemi, R.; Mesbahi, A.; Velni, J.M.; Fast, A. Decentralized Covariance Selection-Based Approach to Detect Cyber Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2018**, *9*, 4930–4941. [CrossRef]
19. Li, B.; Ding, T.; Huang, C.; Zhao, J.; Yang, Y.; Chen, Y. Detecting False Data Injection Attacks Against Power System State Estimation With Fast Go-Decomposition Approach. *IEEE Trans. Ind. Inform.* **2019**, *15*, 2892–2904. [CrossRef]

20. Hao, Y.; Wang, M.; Chow, J.H. Likelihood Analysis of Cyber Data Attacks to Power Systems with Markov Decision Processes. *IEEE Trans. Smart Grid* **2018**, *9*, 3191–3202. [CrossRef]
21. Zhao, J.; Mili, L.; Wang, M. A Generalized False Data Injection Attacks against Power System Nonlinear State Estimator and Countermeasures. *IEEE Trans. Power Syst.* **2018**, *33*, 4868–4877. [CrossRef]
22. Ostadijafari, M.; Jha, R.R.; Dubey, A. Conservation Voltage Reduction by Coordinating Legacy Devices, Smart Inverters and Battery. In Proceedings of the 2019 North American Power Symposium, Wichita, KS, USA, 13–15 October 2019.
23. Mohammadi, F.; Nazri, G.-A.; Saif, M. A Real-Time Cloud-Based Intelligent Car Parking System for Smart Cities. In Proceedings of the 2019 IEEE 2nd International Conference on Information Communication and Signal Processing, Weihai, China, 28–30 September 2019.
24. Mohammadi, F.; Nazri, G.-A.; Saif, M. A Bidirectional Power Charging Control Strategy for Plug-in Hybrid Electric Vehicles. *Sustainability* **2019**, *11*, 4317. [CrossRef]
25. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebsari, A.; Dehghanian, P. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access* **2020**, *8*, 87592–87608. [CrossRef]
26. Liu, C.; Liang, H.; Chen, T.; Wu, J.; Long, C. Joint Admittance Perturbation and Meter Protection for Mitigating Stealthy FDI Attacks Against Power System State Estimation. *IEEE Trans. Power Syst.* **2020**, *35*, 1468–1478. [CrossRef]
27. 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]
28. Sreenath, J.G.; Meghwani, A.; Chakrabarti, S.; Rajawat, K.; Srivastava, S.C. A Recursive State Estimation Approach to Mitigate False Data Injection Attacks in Power Systems. In Proceedings of the 2017 IEEE Power and Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017.
29. 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]
30. Abbaspour, A.; Sargolzaei, A.; Forouzannezhad, P.; Yen, K.K.; Sarwat, A.I. Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks. *IEEE Trans. Ind. Electron.* **2020**, *67*, 7951–7962. [CrossRef]
31. Chakhchoukh, Y.; Lei, H.; Johnson, B.K. Diagnosis of Outliers and Cyber Attacks in Dynamic PMU-Based Power State Estimation. *IEEE Trans. Power Syst.* **2020**, *35*, 1188–1197. [CrossRef]
32. Fenza, G.; Gallo, M.; Loia, V. Drift-Aware Methodology for Anomaly Detection in Smart Grid. *IEEE Access* **2019**, *7*, 9645–9657. [CrossRef]
33. Ayad, A.; Farag, H.E.Z.; Youssef, A.; El-Saadany, E.F. Detection of False Data Injection Attacks in Smart Grids Using Recurrent Neural Networks. In Proceedings of the 2018 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, Washington, DC, USA, 19–22 February 2018.
34. Zanetti, M.; Jamhour, E.; Pellenz, M.; Penna, M.; Zambenedetti, V.; Chueiri, I. A Tunable Fraud Detection System for Advanced Metering Infrastructure Using Short-Lived Patterns. *IEEE Trans. Smart Grid* **2019**, *10*, 830–840. [CrossRef]
35. Sargolzaei, A.; Yazdani, K.; Abbaspour, A.; Crane, C.D., III; Dixon, W.E. Detection and Mitigation of False Data Injection Attacks in Networked Control Systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4281–4292. [CrossRef]
36. Chen, Y.; Huang, S.; Liu, F.; Wang, Z.; Sun, X. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control. *IEEE Trans. Smart Grid* **2019**, *10*, 2158–2169. [CrossRef]
37. Apruzzese, G.; Colajanni, M.; Ferretti, L.; Marchetti, M. Addressing Adversarial Attacks Against Security Systems Based on Machine Learning. In Proceedings of the 2019 11th International Conference on Cyber Conflict, Tallinn, Estonia, 28–31 May 2019.
38. Yong, S.Z.; Foo, M.Q.; Frazzoli, E. Robust and Resilient Estimation for Cyber-Physical Systems under Adversarial Attacks. In Proceedings of the 2016 American Control Conference, Boston, MA, USA, 6–8 July 2016.
39. 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]
40. Margossian, H.; Sayed, M.A.; Fawaz, W.; Nakad, Z. Partial Grid False Data Injection Attacks Against State Estimation. *Int. J. Electr. Power Energy Syst.* **2019**, *110*, 623–629. [CrossRef]
41. Sreeram, T.S.; Krishna, S. Managing False Data Injection Attacks during Contingency of Secured Meters. *IEEE Trans. Smart Grid* **2019**, *10*, 6945–6953. [CrossRef]
42. Wang, Q.; Tai, W.; Tang, Y.; Ni, M.; You, S. A Two-Layer Game Theoretical Attack-Defense Model for a False Data Injection Attack against Power Systems. *Int. J. Electr. Power Energy Syst.* **2019**, *104*, 169–177. [CrossRef]
43. Abusorrah, A.; Alabdulwahab, A.; Li, Z.; Shahidehpour, M. Minimax-Regret Robust Defensive Strategy against False Data Injection Attacks. *IEEE Trans. Smart Grid* **2019**, *10*, 2068–2079. [CrossRef]
44. Pilz, M.; Naeini, F.B.; Grammont, K.; Smagghe, C.; Davis, M.; Nebel, J.-C.; Al-Fagih, L.; Pfluegel, E. Security Attacks on Smart Grid Scheduling and Their Defences: A Game-Theoretic Approach. *Int. J. Inf. Secur.* **2019**, *19*, 1–17. [CrossRef]
45. Hasan, S.; Dubey, A.; Karsai, G.; Koutsoukos, X. A Game-Theoretic Approach for Power Systems Defense against Dynamic Cyber-Attacks. *Int. J. Electr. Power Energy Syst.* **2020**, *115*, 105432. [CrossRef]
46. Gao, B.; Shi, L. Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System. *IEEE Access* **2020**, *8*, 30322–30331. [CrossRef]