energies

MDPI

Article

Reachability-Based False Data Injection Attacks and Defence Mechanisms for Cyberpower System

Ren Liu [1,*], Hussain M. Mustafa [2], Zhijie Nie [3] and Anurag K. Srivastava [2]

[1] State Key Laboratory of HVDC, National Energy Power Grid Technology R&D Centre, Guangdong Provincial Key Laboratory of Intelligent Operation and Control for New Energy Power System, CSG Key Laboratory for Power System Simulation, Electric Power Research Institute, China Southern Power Grid, Guangzhou 510663, China
[2] Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506, USA; mh00075@mix.wvu.edu (H.M.M.); anurag.srivastava@mail.wvu.edu (A.K.S.)
[3] GE Digital, Bothell, WA 98011, USA; niezj93@gmail.com
* Correspondence: liuren@csg.cn; Tel.: +86-180-2726-9052

Abstract: With the push for higher efficiency and reliability, an increasing number of intelligent electronic devices (IEDs) and associated information and communication technology (ICT) are integrated into the Internet of Things (IoT)-enabled smart grid. These advanced technologies and IEDs also bring potential vulnerabilities to the intelligent cyber–physical smart grid. State estimation, as a primary step of system monitoring and situational awareness, is a potential target for attackers. A number of other smart grid applications, such as voltage stability assessment and contingency screening, utilize state estimation results as input data. False data injection (FDI) is a specific way to attack state estimation by manipulating input data. Existing research mainly focuses on the mathematical analysis of FDI attacks; however, in these methods, discussions of reachability requirements to compromise measurements considering cyberinfrastructure are limited. Reachability is defined as a measure that estimates the number of hosts to compromise for the possible FDI. Most of the existing FDI attack methods require the simultaneous manipulation on multiple measurement devices in different substations, in order to bypass the bad data detection, which may be impractical. In this paper, a new type of reachability-based FDI attack considering the cybernetwork with a practical attack is proposed and validated on two IEEE test systems. The corresponding defence mechanisms are (a) decentralized state estimation (DSE), (b) DSE with additional backup computational nodes, (c) communication network rerouting, and (d) intrusion detection system, and they were developed and presented with validation for two IEEE test systems with superior performance for an IoT-enabled intelligent smart grid system.

Keywords: state estimation; cyber–physical analysis; false data injection attacks; smart grid communication; smart grid measurements; IoT

Citation: Liu, R.; Mustafa, H.M.; Nie, Z.; Srivastava, A.K. Reachability-Based False Data Injection Attacks and Defence Mechanisms for Cyberpower System. *Energies* **2022**, *15*, 1754. https://doi.org/10.3390/en15051754

Academic Editors: Pierluigi Siano, Antonio Moreno-Munoz and Hassan Haes Alhelou

Received: 31 December 2021
Accepted: 19 February 2022
Published: 26 February 2022

1. Introduction

With the integration of information and communication technology (ICT) and the Internet of Things (IoT) enabling advanced control automation in the intelligent cyber–physical systems, smart grid technology is confronted with an increasing number of challenges from cyber vulnerabilities [1–5]. Cyber–physical analysis for these vulnerabilities is focused on multiple aspects such as developing robust computational architecture [6–9] and analyzing the impact of cyberattacks on IoT-enabled smart grid applications [10–13]. State estimation is one of the most popular prevention methods commonly addressed for cyber–physical analysis. The results of state estimation are utilized by many other smart grid applications, such as voltage stability monitoring and security analysis. Different types of hybrid state estimation, linear state estimation, and distributed state estimation were developed [14–16]. However, the performance of the state estimator is prone to measurement errors, communication noises, and possible cyberattacks [17,18].

False data injection (FDI) is one of the most commonly discussed attack methods in the previous literature. An FDI attack requires manipulating certain estimated system states and having the capability of bypassing existing bad data detection techniques. Existing FDI attack scenarios are mostly focused on building the mathematical model of FDI attacks. For example, an imperfect implementation method of false data injection attacks was developed in [19]. The authors performed a developed FDI attack on both a nonlinear state estimation model and a DC state estimation model. In [20], the authors proposed a local FDI attack with reduced network information. The effectiveness of the proposed FDI attack was validated by extensive simulations. The developed FDI only needs information within the subnetwork of the smart grid to attack the results of optimal power flow calculation. In [21], the authors reviewed cybersecurity and different vulnerabilities with mitigation strategies of recent smart grid technologies. They classified cyberattacks, keeping the focus on FDI attacks with several use cases due to their prevalence in different operational domains of the smart grid. In [22], a method of FDI attack was proposed to target Volt/Var optimization that manipulates the voltage profiles of distribution feeders and leads to adversary power losses. In [23], the principal component analysis approximation method was utilized for blind FDI without Jacobian matrix information. Unlike many other FDI algorithms for analyzing attacks on DC state estimation, a new FDI algorithm was proposed in [24] that analyzes attacks against AC state estimation with limited network information. In [25], a new FDI algorithm focused on phasor measurement unit (PMU) measurements was developed to selectively compromise the minimal number of devices. The corresponding countermeasures are also proposed in this paper to detect this new FDI algorithm. In [26], a new FDI attack algorithm focused on switching network topology is developed. The countermeasures for this new FDI are also discussed in the paper. In [27], the authors analyzed the impact of FDI on automatic generation control and developed a defence mechanism to detect this kind of FDI attack. One of the most common issues on existing FDI attack methods is that complete observability and selective controllability were assumed in the research works mentioned above; however, in practice, a trade-off is presented to the attacker between the exposure risk of getting detected and the extensive intervention of multiple electronic devices. To avoid being caught, the attacker needs to intervene in the electronic devices as little as possible to perform the attack. Thus, the reachability of the attacker is defined as the capability of attackers to compromise several hosts at the same time. Some notable assumptions are impractical and hard to be achieved in real life:

- An attacker has access to selected data points at multiple substations even though that requires compromising multiple routers and switches with higher exposure risks.
- Excessive assumptions about reachability and a higher level of cyberexposure risk, while the attack objective remains to be undetected with stealth FDI attack.
- The probability of appearance of these existing FDI attacks is significantly low in the real world as it contradicts the motives of cyberattacks.

To further analyze FDI attacks, research works proposed to limit the information range that attackers could access. In [28], an algorithm was developed to optimize the installation locations of PMU devices against FDI attacks in the state estimation. In [29], a new method of constructing FDI attack vectors was proposed on the basis of the least probability of detection and incomplete topological information. Identifying the location(s) under FDI attacks is also important. A model-free deep-learning-based location detection method was proposed in [30]. Table 1 listed the primary characteristics of typical FDI methods, including applied FDI methods, state estimation model, and the number of states to be compromised. To the best of our knowledge, a communication network with components (e.g., gateways, routers, intelligent electronic devices(IEDs)) is not considered in FDI attack analysis. The listed papers demonstrated various stealthy FDI methods that are able to manipulate data points directly without considering the willingness of the attacker to compromise the minimum number of digital devices to avoid being caught. In Table 1, in the compromised states column, “All” indicates that the FDI attack method must compromise all variables in the attack vector; “Selective” indicates that the FDI method was optimized to selectively

choose the variables to compromise in the attack vector, which considers the risk of cyber exposure to a certain level; lastly, "Limited" means the FDI method requires to compromise states in a specific physical area according to geographical partitions or regulation control regions. Compared to other works, our research effort provides the following contributions:

- Developing a new reachability-based FDI attack designed to minimize the risk of cyberexposure. A comprehensive cyber–physical approach analyzes the potential manipulation of a network router at a substation instead of multiple data points. Attackers gain access to multiple data points from the manipulated router to adversely impact the results of conventional state estimation.
- Proposing effective cyber–physical defence mechanisms such as decentralized SE, backup computational nodes, intrusion detection system (IDS), and network rerouting mechanisms to protect state estimation from the proposed reachability-based FDI attacks.
- Performing a simulation for IEEE standard test systems to demonstrate the superior performance of the proposed algorithms.

Table 1. Literature review of stealthy FDI attack on state estimation.

Ref.	Estimation Model	Stealthy FDI Method	Compromised States	Cyber Network Model
[19]	DC Model, AC Model	Relaxation error introduced	Limited	No
[20]	DC Model	Localized load-reduction maximizing operation cost	All	No
[22]	Branch Flow Model	Targeted against voltage control	All	No
[23]	DC Model	Generated attack vector by PCA approximation without topology information	All	No
[24]	AC Model	Constructed undetectable attack vectors for a specific region	Selective	No
[25]	DC Model	Minimized the required number of PMU devices to be compromised	Selective	No
[26]	DC Model	Targeted against a switching network topology	All	No
[27]	DC Model	Targeted against sensor data used for AGC control	All	No
[28]	AC Model	Constructed attack vectors with certain measurements determined by the system configurations	All	No
[29]	DC Model, AC Model	Constructed attack vectors with incomplete network topology information	All	No
[31]	AC Model	Introduced collective estimation error in Volt-VAR Control	Selective	No
Proposed	DC Model (Centralized and Distributed)	Generated attack vectors based on cybernetwork reachability to lower the risk of cyber exposure	Limited	Yes

The objective of this study is to explore a new FDI with the realistic attacker capability assumption and minimum risk of cyber exposure. The organization of this paper is shown as follows. In Section 2, the proposed reachability-based FDI is presented. The developed defence mechanisms for reachability-based FDI are introduced in Section 3. Simulation results for the proposed FDI and defence mechanisms are described in Section 4. In Section 5, the conclusion of this paper and future work are presented.

2. Reachability-Based False Data Injection Attacks

2.1. Introduction of False Data Injection

2.1.1. State Estimation

By applying state estimation applications, the operating condition is analytically determined by the measurements of system states at different measuring nodes in the smart grid. By gathering measurement values throughout the system such as bus voltage magnitudes, transferred active power, and reactive power flows on the transmission lines, and reactive power injections among the system on the basis of the mathematical formulation in [32], a DC power-flow-based measurement system can be expressed as follows. This analytical method is similarly extended for linear state estimators (LSE):

$$z = Hx + e \tag{1}$$

where $x = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix}^T$ is the vector of system states, $z = \begin{bmatrix} z_1 & z_2 & \cdots & z_m \end{bmatrix}^T$ denotes the vectors of system state measurements, $e = \begin{bmatrix} e_1 & e_2 & \cdots & e_m \end{bmatrix}^T$ denotes the corresponding vector of metering errors, and H is an m-by-n Jacobian matrix determined by the branch parameters and the network model of the system. To achieve the estimated values of system states, the DC power-flow-based state estimation problem is formulated by the weighted-least-squares method in (2).

$$\min \ J(x) = (z - Hx)^T W (z - Hx) \tag{2}$$

$$W = \begin{bmatrix} \sigma_1^{-2} & & & \\ & \sigma_2^{-2} & & \\ & & \ddots & \\ & & & \sigma_m^{-2} \end{bmatrix} \tag{3}$$

where W denotes the covariance matrix of m metered measurements errors, and σ_i^2 is the error variances for ith measurement.

With this method, the estimation of system states $\tilde{x}$ can be solved by the following equation:

$$\tilde{x} = \left(H^T W H\right)^{-1} H^T W z \tag{4}$$

2.1.2. Bad Data Detection

It is common in the smart grid that several measurements may be considerably deviated from the true values due to the lack of calibrations on the metering instruments. Identifying and eliminating such kind of bad data from state estimation applications is essential. Chi-squared test is a statistical measure commonly used for detecting bad data measurements. This test is able to tell whether the residual value of a measurement is within a certain threshold ϵ or not. The determination of Chi-squared test incorporates a particular degree of freedom $k = m - n$ (the difference between the number of measurements and the number of system state variables), and the detection confidence in errors. For the introduced DC state estimation model, if W is a identity matrix, bad data detection could be represented as follows:

$$\|z - H\tilde{x}\|^2 \leq \epsilon \tag{5}$$

2.1.3. False Data Injection

Although bad data detection is capable of eliminating the effect from errors that largely deviate from the true values, an FDI attack can still manipulate part of meters and change meter readings to bypass the chi-squared test in the bad data detection. To perform a successful FDI, the attacker needs to arrange their attack action, so that the manipulated measurement residual is still within the chi-squared test threshold.

In [33], the mathematical model of FDI was formulated as

$$z_a = z + a \tag{6a}$$

$$\tilde{x}_{\text{bad}} = \tilde{x} + c \tag{6b}$$

where z is the original system measurement vector, z_a is the manipulated system measurement vector, a is injected measurement vector manipulated by the attacker, $\tilde{x}$ is the original estimation of system states, $\tilde{x}_{\text{bad}}$ is the manipulated estimation of states, c is the falsely injected values in the state estimation, which is introduced by the attacker. When the false data injection attack is conducted, the measurement residual is presented as

$$\begin{aligned} \|z_a - H\tilde{x}_{\text{bad}}\| &= \|z + a - H(\tilde{x} + c)\| \\ &= \|z - H\tilde{x} + (a - Hc)\| \end{aligned} \tag{7}$$

To manipulate the attack vector, let $a = Hc$; then, (7) yields

$$\|z_a - H\tilde{x}_{\text{bad}}\| = \|z - H\tilde{x}\| \tag{8}$$

Equation (8) shows that the manipulated measurement residual is the same as the original measurement residual, which indicates that bad data detection could be passed without any alarms as long as the original estimated state is valid to the chi-squared test.

The reachability of this FDI assumption is very challenging to achieve. The attacker needs to manipulate multiple meters in different substations at the same time to bypass bad data detection. The reachability assumption of the attacker is too strong to be implemented in the real world. Thus, how to realistically perform an FDI attack and its corresponding defence mechanisms is a critical technical bottleneck.

2.2. Communication Network in Smart Grid

Since it is difficult for the attacker to hack into multiple metering devices at different locations to simultaneously manipulate their readings, the FDI attack could be conducted in another way, which is through the communication network.

In the traditional power grid, communication networks for the smart grids can be thought of as running in parallel and on top of a power system network. Substations containing all the sensors and actuators communicate and exchange data to a control center via a substation gateway router. All the data points encoded with power system measurements travel via a substation local area network using different standard protocols, and the substation gateway routers aggregate all those data measurements and transmit them to the control center through communication link [34]. Figure 1 shows a commonly used communication architecture. All meter measurements are transmitted from the substation monitoring devices to their substation routers. Then, each substation router sends out received meter measurements through the communication network, which consists of all the substation routers, to the control center. If an attacker could hack into one substation router, they can manipulate not only all the meter measurements from the hacked substation, but also all the meter measurements going through the manipulated router.

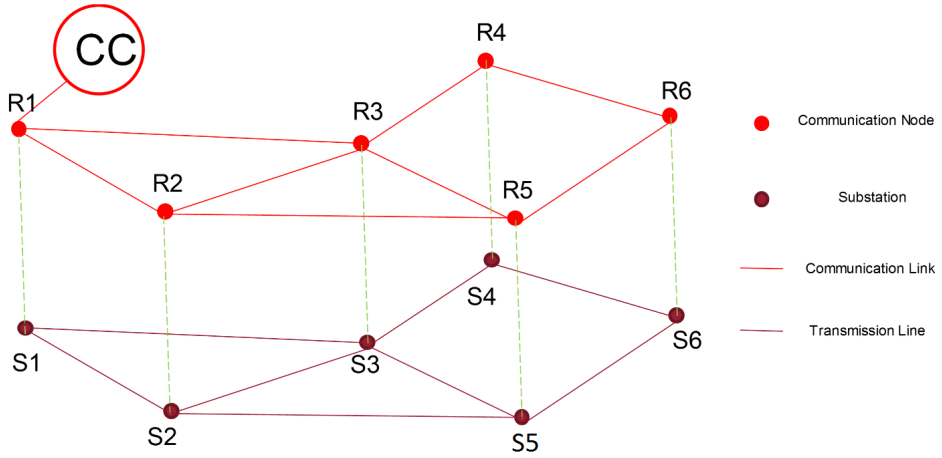

Figure 1. Communication architecture in smart grid.

The total communication delay also consists of four types of communication delays. The first priority delay is network processing delay, which depends on how many communication nodes (e.g., network routers) are passed by the data packets. The second priority delay is signal propagation delay, which mainly depends on the physical distance of network infrastructures. The commonly used routing rule in the communication network is to choose the shortest path [35] that minimizes time delays in the communication network. The attacker can also easily obtain the geographical location of the power system substation and transmission line from the satellite map. Thus, it is not difficult for an attacker to find out all routing rules in the communication network.

2.3. Reachability-Based False Data Injection

Generally, by manipulating the estimated system states, the purposes of successful FDI attacks includes causing serious device damage, leading to critical blackout, and gaining financial benefits. Thus, the attacker has some specific targets in the system states that should be manipulated. By utilizing the FDI method from [33], the attacker can learn about which meter measurements should be manipulated to finally change the specific estimated states. Once the target meter measurements are selected, the attacker needs to figure out the target substation router, which has access to all the required meter measurements.

By converting the communication network into a connected graph on the basis of the geographical location of substations and transmission lines, the attacker can utilize the shortest-path algorithm to find out the best possible path to attack out of all the communication paths from each substation to the control center. After obtaining the communication paths of all the measurement devices and comparing them to required meter measurements, the attacker can select the target substation router to attack. The flowchart of the reachability-based FDI is shown in Figure 2.

For example, if the attacker plans to manipulate the system states of Bus 12 in the IEEE 14-Bus system as shown in Figure 3, based on (7) and (8), they only need to manipulate meter measurements from Buses 6, 12, and 13, so that bad data detection cannot find this attack out. Once the attacker knows all communication routing rules, they can easily find out all that meter measurements from Buses 6, 12, and 13 go through substation router 6 to the control center. Then, the attacker only needs to obtain access to substation router 6 to process this undetectable attack to the state estimation.

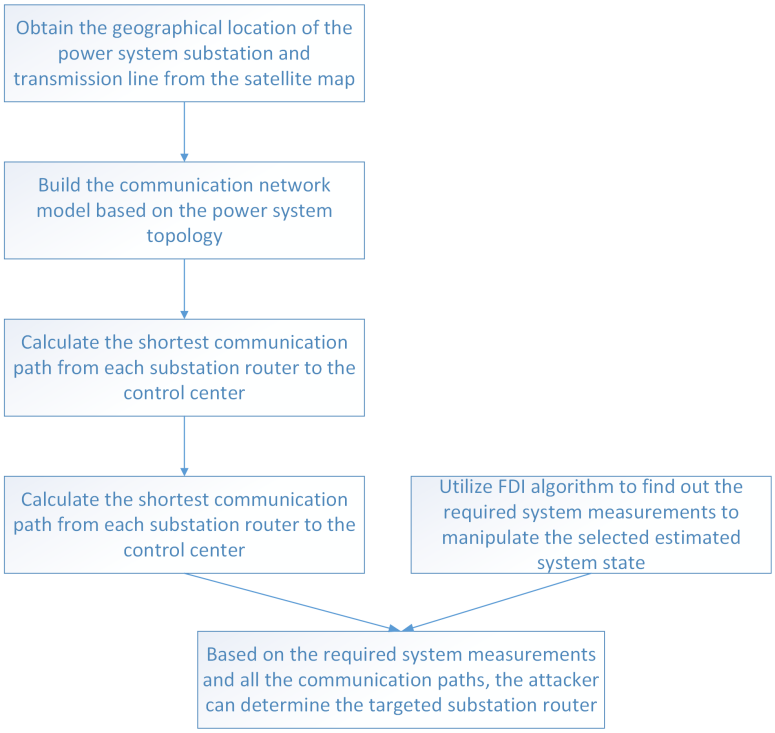

Figure 2. Flowchart of reachability-based FDI.

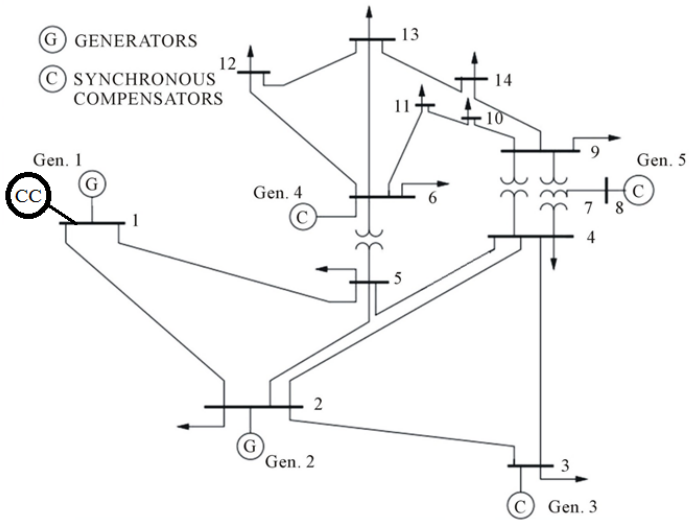

Figure 3. Architecture of IEEE 14-bus system with control center location.

3. Defence Mechanisms for Reachability-Based False Data Injections

There are many declared vulnerabilities in commercial routers from different vendors, and such cyberassets could be manipulated to perform proposed reachability-based FDI attacks. Therefore, the defence mechanism for a reachability-based FDI attack must be developed to prevent the potential attack. Different kinds of defence mechanisms are presented in this section.

3.1. Deployment of Decentralized State Estimation

On the basis of the simulation results in Section 4.1, the number of vulnerabilities in the system grows with the scale of the system size. If a large system can be divided into several subsystems with smaller sizes, the number of vulnerabilities in the whole system could be reduced. In addition, the communication paths go through fewer substation routers for a small system compared with a large-scale system. Thus, decentralized state

estimation (DSE) can be an efficient approach to mitigate the effect of reachability-based FDI attacks.

DSE needs to divide the whole system into multiple subsystems. For each subsystem, a group leader should be selected to operate DSE. Thus, DSE requires multiple computation nodes deployed in the whole system to work as the group leader, but TCSE only requires a single computation node, which is usually supported by a powerful server at the control center. Although additional computation nodes could increase the cost of installing infrastructures, the group leader for each subsystem can be selected at any generation plant since the power plants had been installed with many advanced controllers and computer-aided technology, which can be used to operate the DSE and other decentralized applications. Therefore, the deployment cost for DSE applications could be reduced.

The objective of applying DSE is to reduce computational burden by distributing power grid meter measurements to different computational nodes. The basic concept of DSE was introduced in [9]. In the following section, decentralized linear state estimation (DLSE) is utilized to validate the performance of DSE against reachability-based FDI.

3.2. Utilizing Decentralized State Estimation with Additional Backup Computational Nodes

On the basis of the simulation results from Section 3.1, DSE significantly reduces the number of potential reachability-based FDI attacks. However, there are still some potential reachability-based FDI attacks, which can successfully attack DSE. To further protect the DSE from reachability-based FDI attacks, additional backup computational nodes working as a backup group leader can be involved in each group for DSE. If the backup group leader can be utilized in the DSE, DSE can have the following features:

- A backup group leader can provide the fault tolerance. If any failure occurs at the primary leader, the backup leader can still take over the functionality of DSE and other decentralized synchrophasor applications.
- DSE simultaneously runs on the primary and backup group leaders. Estimated results from the primary and backup group leaders are compared with each other. Due to the same meter measurements that are utilized by both group leaders, estimation results from them should be identical. Since most of the meter measurements from the original meter to the primary and backup group leaders go through the different communication paths, the proposed reachability-based FDI can only attack one group leader's state estimation results. If different estimation results are found, there must be a cyberattack or communication failure occurred in the system.

If the backup group leader needs to be involved in the DSE, a decentralized coordination platform with an architecture suitable for the kinds of coordination needed for DSE needs to be developed. A robust and reliable platform plays a significant role in implementing decentralized algorithms regarding various power grid analytic applications, for instance, the proposed DSE algorithm. *DCBlocks*, as illustrated in [9], provides a solution to fulfil the requirements of decentralized coordination platform.

3.3. Communication Network Rerouting

Part of the potential reachability-based FDI, which cannot be detected by the DSE with an additional backup group leader, is due to the similar communication path to both primary group leader and backup group leader. To prevent this kind of potential reachability-based FDI, the communication network rerouting method can be leveraged. Instead of automatically selecting the shortest path as the communication path, the communication path can be manually altered with another feasible path. As long as there is no common path to both the primary and the backup group leaders, a reachability-based FDI attack can be detected.

3.4. Deployment of Intrusion Detection Systems

IDS is a cybermonitoring system that monitors abnormal communication data flow in the communication network. In a communication network, IDS is already widely utilized.

In [36], the authors presented a dynamic distributed IDS to monitor the distributed cyber attack in the communication network. In [37], another IDS based on autonomous modules was proposed to detect potential cyberattacks in the communication network. IDS is also utilized in the power grid. In [38], a distributed IDS with hierarchical architecture was developed to improve the cybersecurity of the smart grid.

Given that the deployment cost of IDS at every single substation is considerably high, the optimal location of the IDS should be decided. Some substations only have one communication path connected with the rest of the communication network. If the IDS can be deployed on the common communication path, the potential reachability-based FDI on the estimated system state can be eliminated. This is because, as long as the attacker performs the cyberattack, there is always a trace of abnormal communication data that can be detected by the IDS. Once an abnormal data flow occurs in the communication network, the IDS could send the alarm to system operators.

4. Simulation Results

4.1. Simulation Results for Reachability-Based False Data Injection

To validate the performance of reachability-based false data injection, two different IEEE test systems, IEEE 14-bus system and IEEE 39-bus system, are utilized to perform the reachability-based FDI simulation. The architectures of the IEEE 14- and 39-bus systems with specific control center (CC) locations are shown in Figures 3 and 4. All the test cases were simulated in MATLAB and run on a laptop with an Intel I7 processor and 8 GB RAM.

The communication link of the control center is only connected with substation router 1, so all meter measurements pass through substation router 1 and are finally delivered to the control center. If substation router 1 is attacked, the attacker can manipulate all the estimated system states, which is non-realistic and cannot prove the performance of reachability-based FDI. Thus, in this work, the assumption is made that special cyber defence mechanisms are installed on substation router 1, so that substation router 1 cannot be attacked as the expectation for control centers. To reveal the performance of reachability-based FDI, linear state estimation (LSE) is utilized in the following simulation.

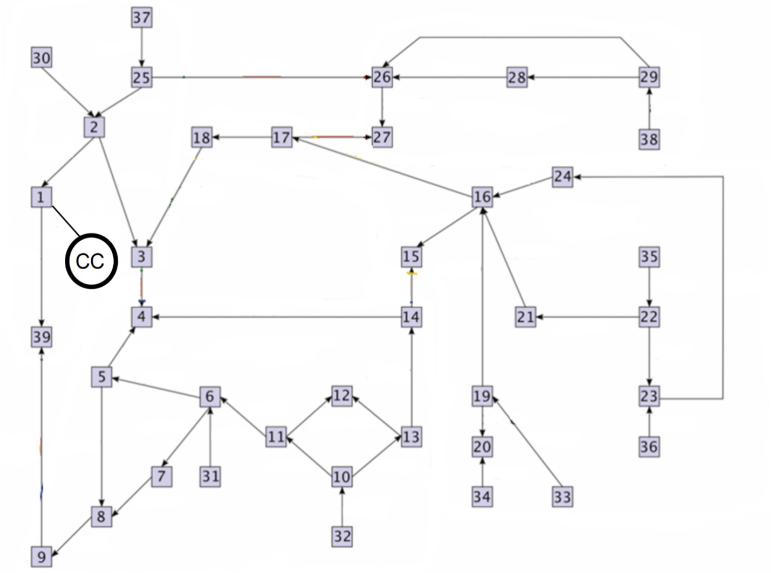

Figure 4. Architecture of IEEE 39-bus system with control center location.

Traditional centralized state estimation (TCSE) algorithm is an iterative, computationally intensive method. On the other hand, LSE is a noniterative method that needs much less computing time than what TCSE requires. The detailed algorithm of LSE is demonstrated in [9]. With the development of smart grid technology, an increasing number of smart grid IEDs are deployed in many digital substations. PMU is a special kind of IED that is synchronized with GPS clock signals and provides high-accuracy phasor

measurements with precise GPS timestamps, which is effective in implementing the LSE algorithm for state estimation. However, it is unnecessary to collect PMU measurements on every bus. For LSE, based on the increasing installation of PMUs, it is assumed that PMUs are installed at key buses. The proposed algorithm only requires the measurements from several key substations of high-voltage levels [39] and those from the substations involving LSE implementations.

To find the shortest path from all the nodes to the control center, the communication network is converted from power system topology. The weighted edge of the communication network is proportional to the resistance of the transmission line. The weight of the edge represents the signal propagation delay in the communication network. Each node in the communication network is also assigned 1 to represent the network processing delay. The weighted communication graph is shown in Figure 5. The "shortestpath" function in MATLAB is utilized to calculate the shortest path from each node to the control center. Once all communication paths are obtained, the attacker can determine which system state measurements can be manipulated by attacking a single substation router. Then, on the basis of Equations (7) and (8), the attacker can determine which estimated system state can be manipulated without being detected by bad data detection.

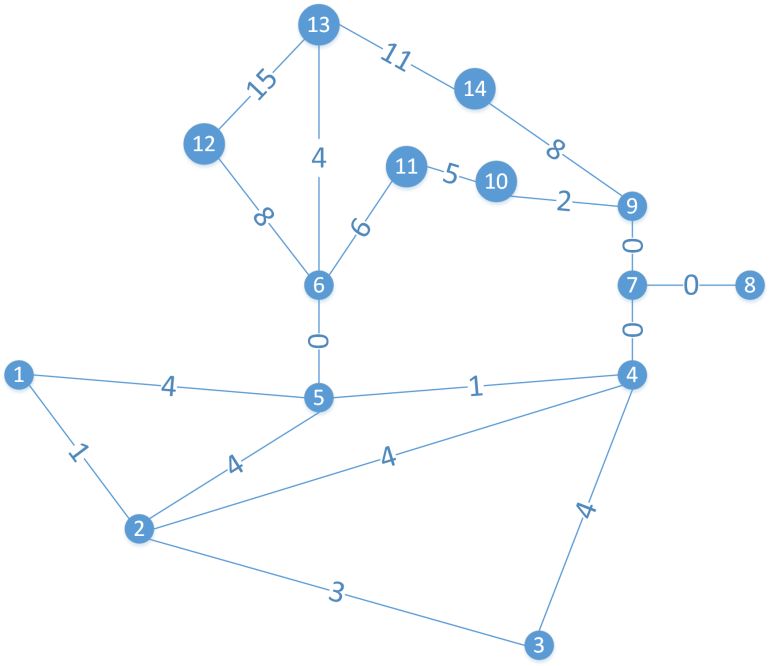

Figure 5. IEEE 14-bus system communication network weighted graph.

For an IEEE 14-bus system, simulation results for LSE are shown in Table 2. Each row represents which substation router was attacked. Columns 2–15 represent which estimated system states could be manipulated with the specific attacked substation router. The last column represents the total number of manipulatable system states for each specific attacked substation router. For example, in Table 2, the third row shows that, if substation router 4 is attacked, the attacker can manipulate estimated system states in substations 7–9 without being detected by bad data detection. Thus, there are three system states that can be manipulated when substation router 4 is attacked. As shown in Table 2, when the critical substation router, such as substation router 5 in this test case, is attacked, 9 estimated system states can be manipulated. This system vulnerability can lead to serious damage to the power grid.

Table 2. Simulation results of reachability-based FDI on LSE for IEEE 14-bus system.

Attacked Node	Attacked System Status	No. of Attacked Statuses
2	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
3	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
4	0 0 0 0 0 0 7 8 9 0 0 0 0 0	3
5	0 0 0 0 0 6 7 8 9 10 11 12 13 14	9
6	0 0 0 0 0 0 0 0 0 0 0 12 0 0	1
7	0 0 0 0 0 0 0 8 0 0 0 0 0 0	1
8	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
9	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
10	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
11	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
12	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
13	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
14	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
Total		14

For an IEEE 39-bus system, simulation results for LSE is shown in Table 3. Since the IEEE 39-bus system is relatively larger, the manipulatable system states are not listed in this table. The total number of manipulatable system states for each specific substation router is summarized in the second column for LSE. The second last row represents how many attacked substation routers can lead to a successful attempt of FDI attack. The last row presents the average number of manipulatable system states for each attacked substation router. On the basis of simulation results from two IEEE test systems, reachability-based FDI can be implemented by the attacker as long as the attacker finds out the appropriate substation router to attack. By comparing Tables 2 and 3, it is clear that there were more vulnerable substation routers in the larger system compared with the smaller system.

Table 3. Simulation results of reachability-based FDI on LSE for IEEE 39-bus System.

Attacked Node	LSE	Attacked Node	LSE
2	21	21	3
3	17	22	2
4	0	23	1
5	6	24	0
6	5	25	1
7	0	26	3
8	9	27	3
9	10	28	0
10	1	29	2
11	3	30	1
12	0	31	1
13	0	32	1
14	0	33	1
15	0	34	1
16	10	35	1
17	15	36	1
18	16	37	1
19	3	38	1
20	1	39	12
	Total		153
	No. of Attacked Nodes		30
	Avg. Attacked Statuses		5.1

4.2. Simulation Results for Decentralized State Estimation against Reachability-Based False Data Injection

As shown in Figure 6, the IEEE 14-bus system was divided into four different groups. Buses 1, 3, 6, and 9 represent the locations of Group 1–4 leaders, respectively.

Given that it is assumed that a special protection system is deployed to protect the control center from attacks, this assumption can also be applied to all group leaders. Simulation results of reachability-based FDI on different state estimations for IEEE 14-bus system are shown in Table 4. It is clear that DLSE significantly reduces the number of vulnerable substation routers in the system. The average number of manipulatable estimated system states for each vulnerable substation router is decreased by over 50%.

The IEEE 39-bus system was divided into four different groups as shown in Figure 7. Buses 37, 26, 31, and 33 represent the locations of Group 1–4 leaders, respectively. Simulation results of reachability-based FDI on four state estimations for IEEE 39-bus system are shown in Table 5. Similar to the results of IEEE 14-bus system, DLSE significantly reduced the number of vulnerable substation routers from 30 to 14 in the IEEE 39-bus system, and the average number of system states for each manipulatable substation router from 5.1 to 3.8. Therefore, DSE successfully prevented many potential reachability-based FDI attacks.

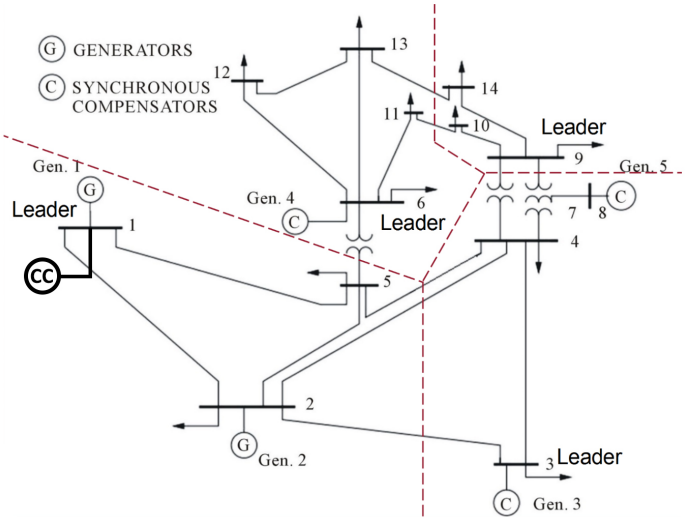

Figure 6. IEEE 14-bus System with control center location and DSE group architecture.

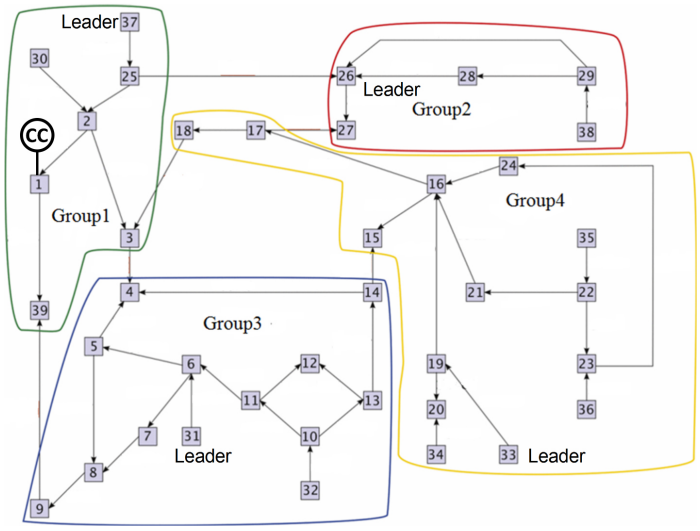

Figure 7. IEEE 39-bus system with control center location and DSE group architecture.

Table 4. Simulation results of reachability-based FDI on different state estimation methods for IEEE 14-bus system.

Attacked Node	LSE	DLSE	DLSEB	Attacked Node	LSE	DLSE	DLSEB
1	0	0	0	8	0	0	0
2	0	0	0	9	0	0	0
3	0	0	0	10	0	0	0
4	3	2	0	11	0	0	0
5	9	0	0	12	0	0	0
6	2	0	0	13	0	0	0
7	1	1	0	14	0	0	0
Total					16	3	0
No. of Attacked Nodes					5	2	0
Avg. Attacked Statuses					3.2	1.5	0

Table 5. Simulation results of reachability-based FDI on different state estimation methods for IEEE 39-bus system.

Attacked Node	LSE	DLSE	DLSEB	Attacked Node	LSE	DLSE	DLSEB
1	0	0	0	21	3	3	0
2	21	2	1	22	2	2	1
3	17	0	0	23	1	1	0
4	0	0	0	24	0	0	0
5	6	2	1	25	1	5	0
6	5	11	2	26	3	0	0
7	0	0	0	27	3	0	0
8	9	0	0	28	0	0	0
9	10	0	0	29	2	1	0
10	1	1	0	30	1	0	0
11	3	3	0	31	1	0	0
12	0	0	0	32	1	0	0
13	0	0	0	33	1	0	0
14	0	0	0	34	1	0	0
15	0	0	0	35	1	0	0
16	10	9	3	36	1	0	0
17	15	1	1	37	1	0	0
18	16	0	0	38	1	0	0
19	3	12	2	39	12	0	0
20	1	1	1				
Total					153	54	12
No. of Attacked Nodes					30	14	7
Avg. Attacked Statuses					5.1	3.8	1.7

4.3. Simulation Results for Decentralized State Estimation with Additional Backup Computational Nodes against Reachability-Based False Data Injection

The DSE with additional backup group leaders was also tested in the IEEE 14- and 39-bus systems. As shown in Figure 8, for the IEEE 14-bus system, Buses 2, 8, 13, and 14 were selected as the backup group leaders of Groups 1 to 4, respectively. The simulation results of three different state estimations against reachability-based FDI for IEEE 14-bus system are shown in Table 4. This protection mechanism is capable of preventing all the potential reachability-based FDI attacks for IEEE 14-bus system.

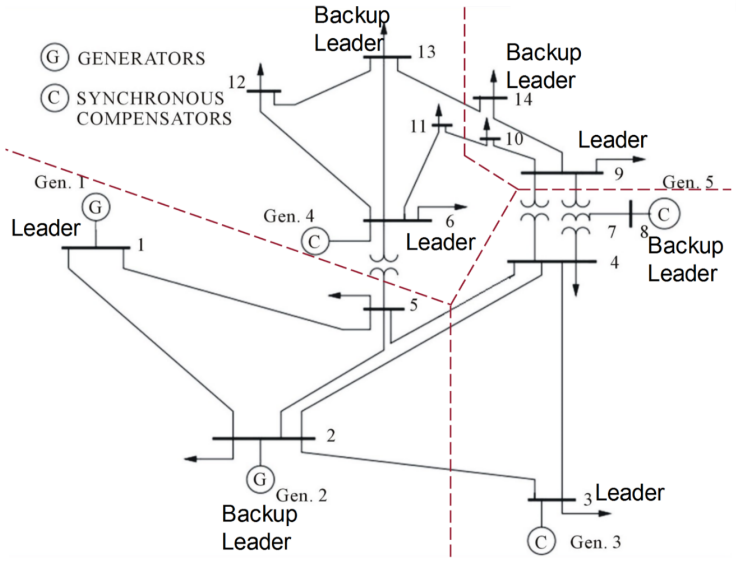

Figure 8. Group Architecture of IEEE 14-bus system for DSE with additional backup group leaders.

As shown in Figure 9, for the IEEE 39-bus system, Buses 39, 38, 32, 36 were selected as the locations of backup group leaders of Groups 1 to 4, respectively. Simulation results of three different state estimations against reachability-based FDI for IEEE 39-bus system are shown in Table 5. The number of attacked nodes reduces from 14 to 7. The average number of attack statuses was reduced from 3.8 to 1.7. It is clear that DSE with an additional backup group leader keeps significantly reducing the number of potential reachability-based FDI attacks in this test case.

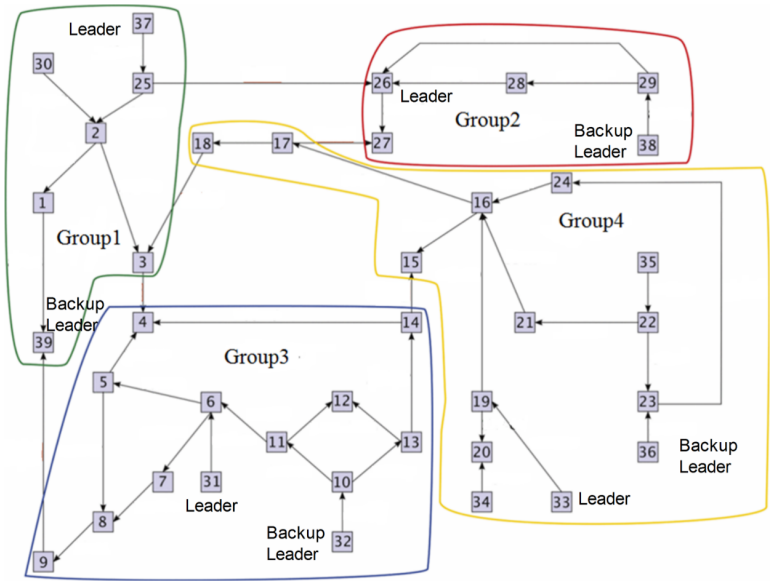

Figure 9. Group Architecture of IEEE 39-bus system for DSE with additional backup group leaders.

4.4. Simulation Results for Communication Network Rerouting and Intrusion Detection System

With the additional backup group leader involved in the DSE, all potential reachability-based FDIs were mitigated in the IEEE 14-bus system. However, in the IEEE 39-bus system, there were still few potential reachability-based FDIs that could not be detected. Thus, simulations for communication network rerouting and IDS were only performed on the IEEE 39-bus system. Simulation results are shown in the Table 6. lComparing with the simulation results for decentralized state estimation with additional backup computational nodes in Table 5, it is clear that the communication network rerouting method could detect

some of the potential reachability-based FDI, which could not be detected by the DSE with an additional backup group leader. There were only five nodes that could still be manipulated by reachability-based FDI. Once the IDSs were deployed in these five nodes, the whole system was protected from the reachability-based FDI.

Table 6. Simulation results for communication network rerouting (CNR) and intrusion detection system (INS) on IEEE 39-bus System.

Attacked Node	CNR	IDS	Attacked Node	CNR	IDS
1	0	0	21	0	0
2	1	0	22	1	0
3	0	0	23	0	0
4	0	0	24	0	0
5	0	0	25	0	0
6	0	0	26	0	0
7	0	0	27	0	0
8	0	0	28	0	0
9	0	0	29	0	0
10	0	0	30	0	0
11	0	0	31	0	0
12	0	0	32	0	0
13	0	0	33	0	0
14	0	0	34	0	0
15	0	0	35	0	0
16	3	0	36	0	0
17	0	0	37	0	0
18	0	0	38	0	0
19	2	0	39	0	0
20	1	0			
Total				8	0
No. of Attacked Nodes				5	0
Avg. Attacked Statuses				1.6	0

5. Conclusions

With the enhanced integration of digital IoT devices and associated communication networks driven by system automation activities, and increasing number of cybervulnerabilities should be taken into consideration by intelligent cyber–physical power grid applications. Existing false data injection (FDI) analysis typically produces strong assumptions with high reachability for the attacker to access multiple data points, such as manipulating multiple individual meters located at different substations while simultaneously bypassing bad data detection. If the attacker gains access to one data point at one substation, they may also access multiple data points. A new reachability-based FDI attack was developed and presented in this paper with detailed cyber–physical models. The performance of this new reachability-based FDI attack was validated in two IEEE standard test systems. On the basis of simulation results, the attacker can manipulate multiple estimated system states by compromising a single critical substation communication router with reachability-based FDI attacks. To protect the power grid from this type of reachability-based FDI attacks, four different defence mechanisms were proposed and discussed in this paper: (a) decentralized state estimation (DSE), (b) DSE with additional backup computational nodes, (c) communication network rerouting, and (d) intrusion detection system. Simulation results were presented for the IEEE standard test cases to demonstrate the superior performance of the proposed defence techniques to mitigate all possible FDI attacks.

However, the limitation of this paper is mainly regarding the assumption of communication network architecture. This paper assumed that the communication network was parallel with the power grid. In the future, if the communication network of power

system is changed into other types, such as 5G, the proposed reachability-based FDI may not work for the future power grid. Thus, a future direction is to develop a new version of reachability-based FDI that can function with the future communication network architecture.

Author Contributions: Conceptualization, R.L., Z.N. and A.K.S.; data curation, R.L. and H.M.M.; formal analysis, R.L.; funding acquisition, A.K.S.; investigation, R.L., H.M.M. and Z.N.; methodology, R.L.; project administration, A.K.S.; resources, A.K.S.; supervision, A.K.S.; writing—original draft, R.L.; writing—review and editing, H.M.M., Z.N. and A.K.S. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to acknowledge partial support from the National Science Foundation (NSF) 1840192. The APC was partially funded by Electric Power Research Institute, China Southern Power Grid.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data of IEEE 14-bus system and IEEE 39-bus system used in this paper can be found in https://icseg.iti.illinois.edu/ieee-14-bus-system/ (25 December 2021) and https://icseg.iti.illinois.edu/ieee-39-bus-system/ (25 December 2021).

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

Abbreviations

The following abbreviations are used in this manuscript:

Acronyms and Symbols	Explanation
CC	Control center
CNR	Communication network rerouting
DSE	Decentralized state estimation
DLSE	Decentralized linear state estimation
DLSEB	Decentralized linear state estimation with additional backup computational nodes
FDI	False data injection
ICT	Information and communication technology
IDS	Intrusion detection system
IED	Intelligent electronic devices
IoT	Internet of Things
PMU	Phasor measurement unit
TCSE	Traditional centralized state estimation
z	Vectors of system state measurements
h	m-by-n jacobian matrix
x	vector of system states
e	corresponding vector of metering errors
x_n	nth system state
z_n	nth system state measurement
e_n	nth metering error for corresponding system state measurement
W	covariance matrix of metered measurements errors,
σ_i^2	error variances for ith measurement.
ϵ	bad data detection threshold
z_a	manipulated system measurement vector
a	injected measurement vector manipulated by the attacker
$\tilde{x}$	original estimation of system states
$\tilde{x}_{\text{bad}}$	manipulated estimation of system states
c	falsely injected values in the state estimation

References

1. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
2. Tariq, M.; Ali, M.; Naeem, F.; Poor, H.V. Vulnerability Assessment of 6G-Enabled Smart Grid Cyber–Physical Systems. *IEEE Internet Things J.* **2020**, *8*, 5468–5475. [CrossRef]
3. Xie, J.; Stefanov, A.; Liu, C.C. Physical and Cybersecurity in a Smart Grid Environment. In *Advances in Energy Systems: The Large-Scale Renewable Energy Integration Challenge*; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 2019; pp. 85–109.
4. Lu, Z.; Hu, Z.; Ning, B.; He, R.; Ji, X.; Wang B. Review of Research Progress and Development Trend of Internet of Things Demand Attack on Power System. *South. Power Syst. Technol.* **2020**, *14*, 21–30.
5. Chen, L.; Xu, A.; Jiang, Y.; Yang, H.; Lu, H.; Kuang X.; Fan K. Attack Pattern Recognition Algorithm of Power Information Network Based on Dynamic Incremental Cluster Analysis. *South. Power Syst. Technol.* **2020**, *14*, 25–32.
6. Liu, C.; Alrowaili, Y.; Saxena, N.; Konstantinou, C. Cyber risks to critical smart grid assets of industrial control systems. *Energies* **2021**, *14*, 5501. [CrossRef]
7. Krishnan, V.V.G.; Gopal, S.; Liu, R.; Askerman, A.; Srivastava, A.; Bakken, D.; Panciatici, P. Resilient cyber infrastructure for the minimum wind curtailment remedial control scheme. *IEEE Trans. Ind. Appl.* **2018**, *55* 943–953. [CrossRef]
8. Lee, H.; Niddodi, S.; Srivastava, A.; Bakken, D. Decentralized voltage stability monitoring and control in the smart grid using distributed computing architecture. In Proceedings of the 2016 IEEE Industry Applications Society Annual Meeting, Portland, OR, USA, 2 October 2016; pp. 1–9.
9. Liu, R.; Srivastava, A.K.; Bakken, D.E.; Askerman, A.; Panciatici, P. Decentralized state estimation and remedial control action for minimum wind curtailment using distributed computing platform. *IEEE Trans. Ind. Appl.* **2017**, *53*, 5915–5926. [CrossRef]
10. Ashok, A.; Govindarasu, M.; Wang, J. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proc. IEEE* **2017**, *105*, 1389–1407. [CrossRef]
11. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [CrossRef]
12. He, X.; Tu, C.; Li, P. Analysis and Countermeasure Strategy of Cyber Attack s on D-PMU Data. *South. Power Syst. Technol.* **2020**, *13*, 37–41.
13. Liu, L.; Su, S.; Qian, B.; Cai, Z.; Xiao, Y. Impact and Protection of Satellite Time Synchronization Attacks in Advanced Metering Infrastructure. *South. Power Syst. Technol.* **2020**, *14*, 3–17.
14. Göl, M. A decentralization method for hybrid state estimators. *IEEE Trans. Power Syst.* **2018**, *33*, 2070–2077. [CrossRef]
15. Zheng, W.; Wu, W.; Gomez-Exposito, A.; Zhang, B.; Guo, Y. Distributed robust bilinear state estimation for power systems with nonlinear measurements. *IEEE Trans. Power Syst.* **2018**, *32*, 499–509. [CrossRef]
16. Jiang, W.; Vittal, V.; Heydt, G.T. A distributed state estimator utilizing synchronized phasor measurements. *IEEE Trans. Power Syst.* **2017**, *22*, 563–571. [CrossRef]
17. Zhang, L.; Abur, A. Strategic placement of phasor measurements for parameter error identification. *IEEE Trans. Power Syst.* **2013**, *28*, 393–400. [CrossRef]
18. Wang, D.; Guan, X.; Liu, T.; Gu, Y.; Shen, C.; Xu, Z. Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids. *Energies* **2013**, *7*, 1517–1538. [CrossRef]
19. Zhao, J.; Zhang, G.; Dong, Z.Y.; Wong, K.P. Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation. *IEEE Trans. Smart Grid* **2015**, *7*, 6–8. [CrossRef]
20. 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]
21. Unsal, D.B.; Ustun, T.S.; Hussain, S.M.; Onen, A. Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. *Energies* **2021**, *14*, 2657. [CrossRef]
22. Choeum, D.; Choi, D.H. Oltc-induced false data injection attack on volt/var optimization in distribution systems. *IEEE Access* **2019**, *7*, 34508–34520. [CrossRef]
23. Choeum, D.; Choi, D.H. Blind false data injection attack using pca approximation method in smart grid. *IEEE Trans. Smart Grid* **2015**, *6*, 1219–1226.
24. Liu, X.; Li, Z. False data attacks against ac state estimation with incomplete network information. *IEEE Trans. Smart Grid*. **2017**, *8*, 2239–2248. [CrossRef]
25. Deng, R.; Zhuang, P.; Liang, H. CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2420–2430. [CrossRef]
26. Wang, S.; Ren, W.; Al-Saggaf, U.M. Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks. *IEEE Syst. J.* **2017**, *11*, 2640–2651. [CrossRef]
27. Tan, R.; Nguyen, H.H.; Foo, E.Y.; Yau, D.K.; Kalbarczyk, Z.; Iyer, R.K.; Gooi, H.B. Modeling and mitigating impact of false data injection attacks on automatic generation control. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1609–1624. [CrossRef]
28. Yang, Q.; Jiang, L.; Hao, W.; Zhou, B.; Yang, P.; Lv, Z. Pmu placement in electric transmission networks for reliable state estimation against false data injection attacks. *IEEE Internet Things J.* **2017**, *4*, 1978–1986. [CrossRef]
29. Li, Y.; Wang, Y. False data injection attacks with incomplete network topology information in smart grid. *IEEE Access* **2019**, *7*, 3656–3664. [CrossRef]

30. Wang, S.; Bi, S.; Zhang, Y.J.A. Locational detection of the false data injection attack in a smart grid: A multilabel classification approach. *IEEE Internet Things J.* **2020**, *7*, 8218–8227. [CrossRef]
31. Ma, L.; Xu, G. Distributed resilient voltage and reactive power control for islanded microgrids under false data injection attacks. *Energies* **2020**, *13*, 3828. [CrossRef]
32. 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.* **2018**, *15*, 2892–2904. [CrossRef]
33. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2011**, *14*, 1–33. [CrossRef]
34. Mustafa, H.M.; Bariya, M.; Sajan, K.S.; Chhokra, A.; Srivastava, A.; Dubey, A.; von Meier, A.; Biswas, G. RT-METER: A real-time, multi-layer cyber-power testbed for resiliency analysis. In Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, Nashville, TN, USA; 19–21 May 2021; pp. 1–7.
35. Dijkstra, E.W. A note on two problems in connexion with graphs. *Numer. Math.* **1959**, *1*, 269–271. [CrossRef]
36. Benattou, M.; Tamine, K. Intelligent agents for distributed intrusion detection system. *Proc. World Acad. Sci. Eng. Technol.* **2005**, *6*, 190–193.
37. Spafford, E.H.; Zamboni, D. Intrusion detection using autonomous agents. *Comput. Netw.* **2000**, *34*, 547–570. [CrossRef]
38. Zhang, Y.; Wang, L.; Sun, W.; Green II, R.C.; Alam, M. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Trans. Smart Grid* **2011**, *2*, 796–808. [CrossRef]
39. Yang, T.; Sun, H.; Bose, A. Transition to a two-level linear state estimator—Part I: Architecture. *IEEE Trans. Power Syst.* **2011**, *26*, 46–53. [CrossRef]