Protection and Control of Modern Power Systems

ORIGINAL RESEARCH Open Access

A review of cyber security risks of power systems: from static to dynamic false data attacks

Yan Xu

Abstract

With the rapid development of the smart grid and increasingly integrated communication networks, power grids are facing serious cyber-security problems. This paper reviews existing studies on the impact of false data injection attacks on power systems from three aspects. First, false data injection can adversely affect economic dispatch by increasing the operational cost of the power system or causing sequential overloads and even outages. Second, attackers can inject false data to the power system state estimator, and this will prevent the operators from obtaining the true operating conditions of the system. Third, false data injection attacks can degrade the distributed control of distributed generators or microgrids inducing a power imbalance between supply and demand. This paper fully covers the potential vulnerabilities of power systems to cyber-attacks to help system operators understand the system vulnerability and take effective countermeasures.

Keywords: False data injection, Economic dispatch, Power system state estimation, Distributed control, Microgrid

1 Introduction

With their extensive incorporation of information and communication technology, power systems are exposed to cyber threats. By targeting the information exchange process, malicious attackers can inject false data to cause power outage, economic loss, and system instability. False data injection (FDI) can also be employed to mask existing power system faults. This will affect operator's visibility on the faults and prevent proper countermeasures from being taken.

For example, in 2015, the Ukraine power grid was attacked and substation breakers were opened by malicious entities [1]. To design proper protection measures for the improvement of system resilience, it is necessary to explore the way FDI affects the power system. Thus, there has been a lot of research on the attacking mechanism and effect of FDI.

In general, the paths through which FDI adversely affects a power system can be classified into three categories, i.e., the estimation of system states, the generation of control commands, and the actuation of control actions, as shown in Fig. 1. FDI can induce the generation of inappropriate control commands by directly targeting economic dispatch. In [2, 3], false load data is injected into security-constrained economic dispatch which causes the line flows to exceed their overload tripping threshold, leading to line outage and even cascade failure. In [4–6], economic dispatch is intentionally affected to increase the operational cost or to obtain illegal profit from power markets. In [7], the potential risk of FDI attacks on economic dispatch is investigated where the attackers do not have full knowledge of network information. FDI can also penetrate a power system by attacking system state measurement and estimation, and cause damage to the integrity of power system state information. In [8], FDI is used as a tool to attack the supervisory control and data acquisition (SCADA) system, while in [9], false data is injected into the phasor measurement unit (PMU) to mislead the control center. By doing this, cyber attackers can affect

Correspondence: ee.yanxu85@gmail.com
College of Standardization, China Jiliang University, Hangzhou 310023, China

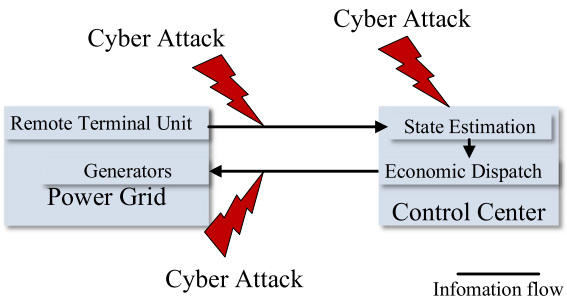

Fig. 1 Cyber-attacks on a power system

the operator's visibility on the true operating condition of the system, resulting in the failure of the operator to take appropriate countermeasures. In [10, 11], FDI is employed to induce arbitrary estimation errors of the state estimator, whereas FDI is applied to power system nonlinear state estimation in [12–15] and the corresponding countermeasures are discussed. In addition, FDI can modify the control input for the system, resulting in deteriorating power system stability. In [16], the input signal for a follower distributed generator is corrupted by FDI, causing the disagreement of a group of distributed generators. In [17], FDI is used to induce a synchronization problem for islanded microgrids, while system breakers are controlled to trigger instability in [18], and the gains of voltage control devices altered to initiate transient instability in [19]. In [20], a malicious attack is implemented through emulated inertia control to cause instability of system frequency.

At present, investigation into the impact of FDI is mainly based on the single-snapshot FDI model and/or the steady-state power system model, while the research considering the transient process of a power system is not thorough and comprehensive. To avoid being detected or reduce energy consumption during the attack process, smart attackers may change the injected data at every attack time instant. The use of the steady-state power system model is also not adequate to analyze the risk of FDI, as real power systems are networked control systems. Even though system state estimation and economic dispatch are resilient to FDI, attackers can still disrupt power system secure operation by attacking the automatic generation control system. Accordingly, considering FDI's dynamic characteristic and power system transient characteristic is of paramount importance to fully reveal the risk of FDI and then design effective countermeasures.

To unveil the risk of FDI in a comprehensive fashion, this paper reviews the research on FDI attacks on economic dispatch, state estimation, and power system dynamic stability, as shown in Fig. 1.

2 Attacks on economic dispatch

2.1 Overloads caused by FDI attack

In a real power system, generators are dispatched every 5–15 min to minimize the operational cost. The load data adopted for security-constrained economic dispatch (SCED) is from the short-term load forecast, which uses historical and/or real-time load measuring values as input. False data which can pass the bad data detection (BDD) can be deliberately injected to alter the load information for the SCED and to modify the enforcement of branch flow limits, as shown in Fig. 2.

Let ΔD denote the injected data. The limits for line flows imposed by the SCED can be represented by [4, 5]:

$$P_{FDI} = S_F\left(K_P P^0 - K_D(D + \Delta D)\right) \tag{1}$$

$$-r \le P_{FDI} \le r \tag{2}$$

where P_{FDI} is the branch flow vector and D is the actual bus load vector. K_P and K_D are the bus-generator and bus-load incidence matrices, respectively. S_F is the generation shift factor matrix and r is the normal capacity rating of the lines.

In addition, the true load used in the SCED is denoted by D and the true branch flow is given as:

$$P = S_F\left(K_P P^0 - K_D D\right) = P_{FDI} + S_F K_D \Delta D \tag{3}$$

Combining (1) and (3) shows that the true branch flow P satisfies the constraint as:

$$-r + S_F K_D \Delta D \le P \le r + S_F K_D \Delta D \tag{4}$$

Equation (4) reveals that the true line flow is greater than its limits, i.e., $|P| \ge r$. In real-time operation, if a generator follows the dispatch commands generated by the SCED under a FDI attack, severe transmission overloads may be induced, causing triggering actions of protection devices.

To launch a practical FDI attack, the injected data ΔD needs to satisfy the following constraints [6, 7]:

$$1^T \Delta D = 0 \tag{5}$$

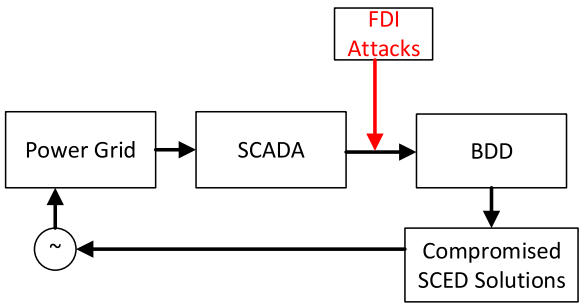

Fig. 2 Illustration of FDI attacks on economic dispatch

$$-\tau D \le \Delta D \le \tau D \tag{6}$$

Equation (5) means that the sum of load changes is zero to guarantee power balance, while (6) constrains the magnitude of the FDI attack at a load bus. Such constraints for a FDI attack are commonly employed in the existing literature.

The above FDI attack model reveals the potential risks for safe power system operation, as blackouts in a power grid are usually caused by overloads and outages [21, 22]. As described in [23], three successive transmission line and transformer tripping were the main causes of the 2003 Northeast Blackout and the 2011 Southwest Blackout, respectively. Once an ensemble of critical lines known as initial contingency (IC) is identified [24, 25], attackers can deliberately induce this initial contingency by using an FDI attack. Given the capability of the IC, sequential outrages and even cascade failures can be initiated, as illustrated in Fig. 3.

2.2 Increase of operational cost caused by FDI attack

Attackers can increase the operational cost of a power system by interrupting the SCED and changing the transmitted load data. The attack vector can be optimized by maximizing the operational cost, which is formulated as a bi-level linear programming problem as:

$$c = \max_{\Delta D} c_g^T P + c_d^T J \tag{7}$$

$$\text{Subject to (5) and (6)} \tag{8}$$

$$\min_{P,J} c_g^T P + c_d^T J \tag{9}$$

$$\text{Subject to } 1^T P = 1^T (D - J) \tag{10}$$

$$F = S_F K_P P - S_F K_D (D + \Delta D - J) \tag{11}$$

$$P_{\min} \le P \le P_{\max} \tag{12}$$

$$-f_{\max} \le F \le f_{\max} \tag{13}$$

$$0 \le J \le D + \Delta D \tag{14}$$

where c_g and c_d are the generation cost and load shedding cost vector, respectively. F is the calculated line flow vector containing false data, f_{max} is the branch flow limit vector, and J is the load shedding vector. P is the generator output power vector, and P_{min} and P_{max} are the lower and upper bounds for the generator output, respectively.

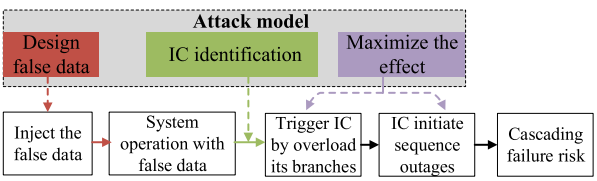

Fig. 3 Illustration of cascading failures caused by FDI [3]

The upper level (7)–(8) shows that the false data ΔD is obtained by maximizing the load shedding after SCED. In the lower level (9)–(14), the operational cost is minimized with the corrupted load data $D + \Delta D$ by considering the generator output power limits (12), transmission line flow limits (13), and load shedding limits (14).

Karush-Kuhn-Tucker (KKT) and dual based methods are widely used to solve the abovementioned bi-level optimization problem [4, 26]. The KKT-based approach requires the introduction of additional binary variables to form the so-called big-M constraints, reducing the computing efficiency of the algorithm. As regards the duality-based method, the bilinear terms of dual variables and the corresponding primal variables are involved, and thus the optimization problem is not easy to solve.

An alternative for attackers to construct the attack vector by using a fast approach is presented in [5]. In order to increase the operational cost, the loading levels of the branches in set Ω are maximized through false data injection. The resultant optimization problem to determine the false data ΔD is described by:

$$\max_{\Delta D} \sum_{l \in \Omega} \delta_l \frac{-S_l K_D \Delta D}{f_l^{\max}} \tag{15}$$

$$\text{Subject to constraints (5) - (6)} \tag{16}$$

where l denotes the transmission line and S_l is the l-th row of S_F.

The objective function is to maximize the loading levels of the transmission lines in set Ω. $\delta_l = 1$ if the flow of line l is positive, and $\delta_l = -1$ otherwise. The term $-S_l K_D \Delta D$ denotes the incremental power flow through line l caused by the injected false data ΔD.

The false data ΔD can be obtained by solving (15), based on which the optimizing operational cost problem (9) with constraints (10)–(14) can be easily solved. Since the attack vector is determined by solving the linear programming problem (15), the run time is significantly reduced compared to the KKT-based approaches.

3 Attacks on power system state estimation

For a modern power system, many smart devices are deployed to acquire the real-time data related to its operation. By exploiting these measuring data, the operators can monitor the system operation status and take effective measures to mitigate potential risks. However, the measurements need to be transmitted to the control center over communication links, and, therefore, power systems face potential cyber-attacks because

of the vulnerability of communication technologies. For example, a malicious agent may inject false data to induce the operators to make the wrong decision on the system status.

3.1 FDI attack with complete network information

Measurements are used to estimate the system state and because of the existence of measurement errors, operators predefine a threshold to detect bad data. If the threshold is exceeded, the measurements are considered to be bad data. Hence, if attackers want to launch a successful attack by FDI, the injected false data has to pass the bad data detection. Power system state estimation can be expressed as [11]:

$$\hat{x} = \arg\min \|z - Hx\|_2 \tag{17}$$

where x is the state vector and $\hat{x}$ is the estimated state vector. z is the measurement state, H the Jacobian matrix of the power system, and $\|\cdot\|_2$ the Euclidean norm.

To detect the bad data, the residue r is defined as:

$$r = \|z - Hx\|_2 \tag{18}$$

The term on the right-hand side of (18) indicates the difference between the measured and actual values. This difference is caused by measurement errors and disruptions. A threshold for r is pre-determined by the operator, and data is considered to be bad if the threshold is exceeded.

For illustration purposes, a power grid is divided into regions A and N with a set of tie lines between them, while the measurements in region A are assumed to have been attacked by a malicious entity. The measurement vector z is decomposed into z_1 and z_2, where z_1 contains all the measurements in the targeted region A without the power flow measurements on the tie lines and z_2 collects the rest of the measurements in region A. Similarly, the state vector x is divided into x_1 and x_2, where x_1 collects all the buses in the targeted region A without the boundary buses and x_2 contains the rest of the buses.

To attack the measurements in region A, attackers need to design an attack vector to pass the bad data detection in state estimation. This means that the false data injected by the attackers should prevent the residual of the state estimation from exceeding its threshold.

In the absence of the injected false data, the measurement errors contribute to the residual. If the measurements are noise-free, the residual is equal or close to zero. In reality, measurement inaccuracy causes inconsistent measurements, leading to an increase of the residual. Less consistency of measurement implies a higher residual. Smart attackers may construct false data that are consistent with the physical property of the power system. Therefore, the false data z_1' designed by the attackers is likely to follow Kirchhoff's Current Law (KCL) and Kirchhoff's Voltage Law (KVL), given by:

$$z_1' = H_{11}x_1 + H_{12}\hat{x}_2 \tag{19}$$

The measurements in the attack-free region are unchanged.

The attacking mechanisms of FDI on power system state estimation have been elucidated in [8–10, 12–15]. When the false data is not injected, the state estimation equation is given by:

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} H_{11} & H_{12} \\ 0 & H_{22} \end{bmatrix} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} \tag{20}$$

where e_1 and e_2 are the measurement errors of z_1 and z_2, respectively. It can be seen that z_2 is only a function of x_2. In the case of DC state estimation, H_{11}, H_{12}, and H_{22} are constant, while they are functions of the state vector in AC state estimation.

When the false data is injected, measurement z_1 is replaced by the attack vector z_1', and the corresponding measurement vector is denoted as $z' = [z_1' \; z_2]^T$. Then the residual is represented by:

$$r' = \min \left\| z' - Hx' \right\|_2 \tag{21}$$

To obtain a feasible estimate of the state vector $\widehat{x'} = [x_1 \; \hat{x}_2]^T$, the following constraint needs to be satisfied:

$$\begin{aligned} r' \le \left\| z' - H\widehat{x'} \right\|_2 &= \left\| \begin{matrix} z' - (H_{11}x_1 + H_{12}\hat{x}_2) \\ z_2 - H_{22}\hat{x}_2 \end{matrix} \right\|_2 \\ &= \left\| \begin{matrix} 0 \\ e_2 \end{matrix} \right\|_2 = \|e_2\|_2 < r = \left\| \begin{matrix} e_1 \\ e_2 \end{matrix} \right\|_2 \end{aligned} \tag{22}$$

Equation (22) reflects the decrease of the overall residual as the false data is injected. This can be explained by the fact that the false data injected in the attack region obey KCL and KVL, and hence have better consistency than the original measurements. It should be clarified that the decreased residual under FDI attack does not necessarily imply that the false data is close to the true value [11]. In fact, attackers can simultaneously induce severe disruptions while maintaining a small residual by FDI.

To construct the attack vector in (19), the line flows in the attack region are computed by:

$$p_{ij} = V_i^2 g_{ij} - V_i V_j \left(g_{ij} \cos(\theta_i - \theta_j) + b_{ij} \sin(\theta_i - \theta_j) \right) \tag{23}$$

$$q_{ij} = -V_i^2 b_{ij} - V_i V_j \left(g_{ij} \sin(\theta_i - \theta_j) - b_{ij} \cos(\theta_i - \theta_j) \right) \tag{24}$$

where V_i is the voltage magnitude at bus i. b_{ij} and g_{ij} are the susceptance and conductance between line i-j, respectively. p_{ij} and q_{ij} are the active and reactive power flows between line i-j.

Since KCL is applicable in (19) for the non-boundary buses in the attack region, the algebraic sum of the flows of the lines connected to a bus equals the power injected at this bus. For the boundary buses in the attack region, parts of the lines linked to this bus belong to the non-attack region (see Fig. 4). Hence, the resulting power balance equations are expressed as:

$$p_i + \sum_{j \in S_{i,A}} p_{ij} + \sum_{j \in S_{i,N}} \hat{p}_{ij} = 0 \tag{25}$$

$$q_i + \sum_{j \in S_{i,A}} q_{ij} + \sum_{j \in S_{i,N}} \hat{q}_{ij} = 0 \tag{26}$$

$$\hat{p}_{ij} = \hat{V}_i^2 g_{ij} - \hat{V}_i \hat{V}_j \left(g_{ij} \cos\left(\hat{\theta}_i - \hat{\theta}_j\right) + b_{ij} \sin\left(\hat{\theta}_i - \hat{\theta}_j\right) \right) \tag{27}$$

$$\hat{q}_{ij} = -\hat{V}_i^2 b_{ij} - \hat{V}_i \hat{V}_j \left(g_{ij} \sin\left(\hat{\theta}_i - \hat{\theta}_j\right) - b_{ij} \cos\left(\hat{\theta}_i - \hat{\theta}_j\right) \right) \tag{28}$$

where p_i and q_i are the active and reactive power injected into bus i. p_{ij} and q_{ij} are the active and reactive power flows of line i-j out from the attack region.

From (27) and (28), we see that the measurements in the non-attack region are not attacked. Thus, $\hat{p}_{ij}$ and $\hat{q}_{ij}$ in (25) and (26) are of the given values, which will change the Jacobian matrix of the power injected into the boundary buses.

Note that (17) results in the state variables on one snapshot. To account for the dynamic behavior of FDI, (17) can be easily reformulated as a summation of $z - Hx$ over T snapshots, and the resulting optimization problem can be solved in a similar way. The details can be found in [27].

3.2 FDI attack with incomplete network information

Equation (19) indicates that the constructed attack vector z_1' depends on the estimates of voltage magnitudes and phase angles of the boundary buses in the attack region. It also requires the attackers to have the topology information of the whole power network as well as line parameters [8–10, 12–15]. However, network information of a power grid is confidential and the attackers are likely to have difficulty in obtaining this. In addition, there exist thousands of buses and lines in a modern power system. This means that the attackers need to deal with extensive information concerning network topology. Therefore, the assumption that attackers are able to acquire the estimated values from state estimation is impractical.

To construct a practical attack model against state estimation, the above conditions are relaxed in [11], in which the false data injection model requires only the network information of the attack region (see Fig. 5) rather than that of the whole power network. In addition, the attack vector in [11] does not directly rely on the estimates of phase angles but rather the angle differences of the lines. The FDI attack model used in [11] is reformulated by the following steps:

1) Substitute the measured voltages for the estimates of voltage magnitudes at the boundary buses in the attack region;
2) Replace the estimates of voltage magnitudes and phase angles with the corresponding measurements to determine the flows on the tie lines.

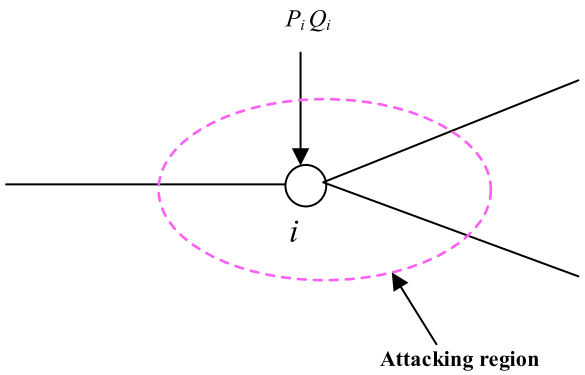

Fig. 4 A boundary bus in the attacking region

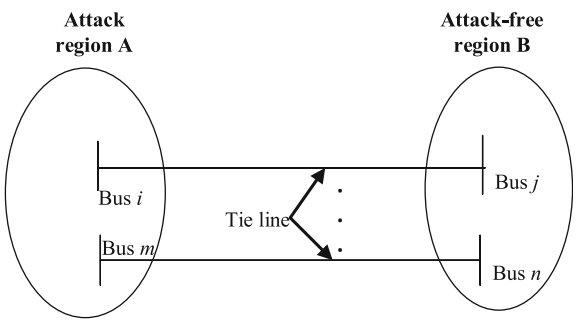

Fig. 5 A power system decomposed into attack and attack-free regions

By doing the above, the estimated state of the system is no longer required in the design of the attack vector.

The phase angles at the boundary buses in the attack region play an essential role in the implementation of the mentioned attack model. Even though the measurements of phase angles can be accessed by PMU, this would require the deployment of sufficient PMUs to provide this information, and such solutions can be hard to scale up. To successfully launch an FDI attack on a power system without sufficient PMU data, it is desirable for attackers to construct a more practical attack model without requiring the measured values of the phase angles. From the perspective of the defender, it is also of paramount importance to explore the possibility of attacking state estimation using such an attack model.

According to (23) and (24), line flow in a power system is computed using the angle difference of the line. If the angle differences between lines are known, the line flows can be determined. This means that the actual phase angles at the boundary buses are not required to determine the line flows, and the angle differences of the line can be used to compute the attack vector in (19) even in the absence of actual bus phase angles. The following investigates how to employ line angle differences instead of bus phase angles to design the attack vector.

Equation (19) implies that phase angles at the boundary buses are fixed to the estimates of the state estimator. Accordingly, the angle differences between buses are also fixed. Considering the actually estimated phase angle at bus i to be $\hat{\theta}_i$, the following expression holds:

$$\hat{\theta}_i - \hat{\theta}_j = \left(\hat{\theta}_i + \alpha\right) - \left(\hat{\theta}_j + \alpha\right) \tag{29}$$

Equation (29) shows that when the phase angles of two boundary buses are changed by α, the corresponding angle difference is unchanged. Thus, the phase angles used for the calculation of the attack vector can be obtained by the following steps [11]:

Step 1. Select an arbitrary value for a boundary bus;

Step 2. Choose the phase angles for the remaining boundary buses based on the angle differences.

Due to the random value for the boundary bus, the phase angles obtained by the steps above do not represent the actual ones. However, the angle differences are the same as the actual ones, and thus the line flows are unchanged. Therefore, there is no need for attackers to acquire the actual values of the estimated phase angles to construct the attack vector, and the only information needed is the differences of the estimated phase angles.

Assuming there is a path k that links two neighboring buses, as shown in Fig. 6, it can be proved that the following equation holds for a specified direction:

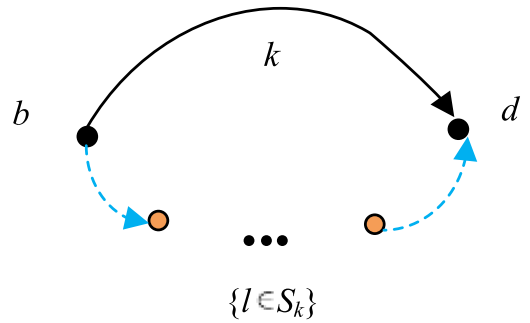

Fig. 6 A path connecting two neighboring buses

$$\sum_{l \in S_k} \delta_l = \theta_b - \theta_d \tag{30}$$

From (30), for the path $\{l \in S_k\}$ connecting bus b and d, the angle difference between the two buses can be computed by summing the angle differences of lines in this path. This means that attackers do not need to acquire the actual values of estimated phase angles at the boundary buses. To compute the angle difference without knowledge of the actual phase angles, the following approximations are considered:

$$\cos\left(\theta_i - \theta_j\right) \approx 1,\ \sin\left(\theta_i - \theta_j\right) \approx \theta_i - \theta_j, V_i \approx V_j \approx 1 \tag{31}$$

Substituting (31) into (27) yields

$$p_{ij} \approx \frac{\theta_i - \theta_j}{x_{ij}} \tag{32}$$

Thus, the angle difference can be computed as:

$$\theta_i - \theta_j \approx x_{ij} p_{ij} \tag{33}$$

Equation (33) shows that the line power measurement can be employed to compute the angle difference, while the error of the angle difference is partly caused by the use of the approximations in (31). Therefore, the accuracy of the angle difference obtained by (33) depends on the conditions under which (31) holds. It is known that the difference reduces with the increase of the X/R ratio of a line. Thus, to reduce the error induced by (31), an optimal path k in the attack region is identified by maximizing the average X/R ratio of ρ_k as [11]:

$$\rho_k = \frac{1}{n_k} \sum_{l \in S_k} \frac{X_l}{R_l} \tag{34}$$

As shown in (22), to avoid being detected by the bad data detection, the overall residual with the injected false data should be smaller than the predefined threshold.

Therefore, the false data following KCL and KVL is injected in the attack region, while the line flows are computed by (23) and (24). The injected power at the non-boundary bus is the sum of the flows over the lines connected to this bus, whereas the injected power at the boundary buses is obtained by (25) and (26). The presented algorithm to construct the attack vector can be summarized as follows.

Step 1. Set initial values to the state vector as

$$\begin{bmatrix} \theta \\ V \end{bmatrix} = \begin{bmatrix} \theta_0 \\ V_0 \end{bmatrix} \tag{35}$$

Step 2. Obtain the attack vector $[p\ q\ P\ Q]^T$ using the current state vector $x = [\theta\ V]^T$;

Step 3. Evaluate whether the injected power at a bus and the active/reactive line flows are confined within lower and upper bounds, as:

$$\begin{cases} P_{\min} \le P \le P_{\max} \\ -p_{\max} \le p \le p_{\max} \\ -q_{\max} \le q \le q_{\max} \end{cases} \tag{36}$$

This can reduce the chance of being detected as the operator can access the information of the flow distribution. If the conditions hold, it terminates; otherwise, it goes to the next step.

Step 4. Compute the incremental $\Delta x = [\Delta\theta\ \Delta V]^T$ by optimizing the objective function as:

$$\min \sum_{t=1}^{10} 1^T S_t \tag{37}$$

$$\text{Subject to} \begin{bmatrix} \Delta p \\ \Delta q \\ \Delta P \\ \Delta Q \\ \Delta V \end{bmatrix} = \begin{bmatrix} H_1 & H_2 \\ H_3 & H_4 \\ H_5 & H_6 \\ H_7 & H_8 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \Delta\theta \\ \Delta V \end{bmatrix}$$

$$\begin{cases} P_{\min} \le P + \Delta P + S_1 - S_2 \le P_{\max} \\ -p_{\max} \le p + \Delta p + S_3 - S_4 \le p_{\max} \\ -q_{\max} \le q + \Delta q + S_5 - S_6 \le q_{\max} \\ V_{\min} \le V + \Delta V + S_7 - S_8 \le V_{\max} \\ \theta_{br,\,\min} \le G\theta + G\Delta\theta + S_9 - S_{10} \le \theta_{br,\,\max} \end{cases}$$

where the slack variable S_t is non-negative, and $H_1 = \partial p/\partial\theta$, $H_2 = \partial p/\partial V$, $H_3 = \partial q/\partial\theta$, $H_4 = \partial q/\partial V$, $H_5 = \partial P/\partial\theta$, $H_6 = \partial P/\partial V$, $H_7 = \partial Q/\partial\theta$, $H_8 = \partial Q/\partial V$. The expressions of H_1-H_4 are provided in [28], while the expressions of H_5-H_8 need to be determined. G represents the transition matrix which transforms the phase angle vector into the phase angle difference vector. For the boundary buses in the attack region, using (26) leads to:

$$\frac{\delta P_i}{\delta\theta_i} = -V_i \sum_{j \in S_{i,A}} \left(-g_{ij} \sin\theta_{ij} + b_{ij} \cos\theta_{ij} \right) V_j \tag{38}$$

For the non-boundary buses in the attack region, the non-zero entries can be determined using a similar way to that shown in [28].

Step 5. Update the state vector as:

$$\begin{bmatrix} \theta \\ V \end{bmatrix} = \begin{bmatrix} \theta \\ V \end{bmatrix} + \begin{bmatrix} \Delta\theta \\ \Delta V \end{bmatrix} \tag{39}$$

and then go back to Step 2.

By using Step 1–5, attackers can attain an attack vector against power system state estimation. This method can avoid bad data detection while requiring no information on the network topology of the whole system and phase angles at buses.

4 Attacks on power control system

The power control system plays a vital role in maintaining power supply in response to customer demand. An imbalance between supply and demand can cause system frequency instability, threatening the operational security of the power system. A central control scheme is commonly employed in traditional power systems, and the scheme features a single control center which collects information from and sends control commands to all agents. However, such a central control architecture no longer meets the need of current power systems. For example, geographically dispersed distributed generators are increasingly integrated into the power grid. These are not suitable for coordination by central control because of the requirement of plug and plug operation [29, 30]. Central control is also not applicable to microgrid operation, where distributed generators are required to supply power in island mode [31]. Because of its reliability, scalability, and flexibility, distributed control is preferred over central control [32–34]. However, in distributed control, local controllers have access to local information and neighbor information, and hence are vulnerable to cyber-attack. A malicious entity can disrupt data exchange among neighboring local controllers by launching FDI attacks [16–20].

4.1 FDI attack on distributed generator

Considering a converter-based distributed generator i, P_i and $P_{i,\max}$ are the active power output and the maximal power, respectively. Using the d-q transformation, the d- and q- axis voltages can be computed by $U_{di} = U_i$ and $U_{qi} = 0$. Assuming the d- and q- axis currents are I_{di} and I_{qi}, respectively, the active power output can be obtained by:

$$P_i = U_{di}I_{di} + U_{qi}I_{qi} = U_iI_{di} \tag{40}$$

If the power converter is controlled by a grid-feeding scheme [31], I_{di} should converge to its reference value I_{di_ref} in a sampling period of T. In the k^{th} iteration, I_{di_ref} can be determined by

$$I_{di\_ref}(k) = P_{i,\max}\alpha_i(k)/U_i(k) \tag{41}$$

where the design parameter α_i denotes the utilization ratio defined by P_i / $P_{i,\max}$. When I_{di} converges to I_{di_ref} in the k^{th} iteration, $P_i(k) = P_{i,\max}\,\alpha_i(k)$.

According to (41), the active power output of distributed generator i can be regulated by altering the utilization ratio α_i. Since the rated power of converter-based distributed generators is relatively small, multiple distributed generators are used in a distribution network for increased capacity. Such a system can be considered as a virtual power plant (VPP), as shown in Fig. 7, where P_{tran} accounts for the total active power transmitted to the transmission network.

To track the dispatch command P_{ref}, the group of distributed generators in a VPP are coordinated using a leader-follower consensus algorithm [16]:

$$\alpha(k+1) = A\alpha(k) + BK\alpha(k) + KC \tag{42}$$

where $\alpha(k) = [\alpha_0(k), \ldots, \alpha_{n-1}(k)]^T$. $B = [-\hat{P}_{\max}\ O_{n\times(n-1)}]^T$ with $\hat{P}_{\max} = [P_{0,\max}, \ldots, P_{n-1,\max}]^T$ and $C = [P_{ref} + P_{loss} + P_{load}\ O_{1\times(n-1)}]^T$. $A = [a_{ij}]$ is a weighted matrix with $a_{ij} > 0$ and $a_{ii} = 1 - \sum_{j=0, j\neq i}^{n-1} a_{ij}$. K is the controller gain and O is the zero matrix. P_{load} and P_{loss} represent the aggregated load power consumption and power loss in the VPP, respectively. By selecting proper A and K, the convergence of (4) can be proved [16]. When convergence is achieved, utilization ratios of all distributed generators reach an agreement and P_{tran} is steered to its preference value P_{ref}.

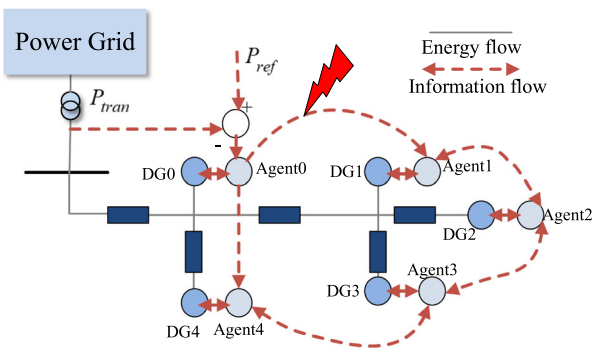

Fig. 7 Illustrative diagram of distributed control of distributed generators

Equation (42) shows that the communication network among distributed generators plays a key role in the regulation of the active power output of the VPP. If the local controller of a certain distributed generator is attacked by FDI attacks, its utilization ratio will be prevented from converging to the consensus value, resulting in failed tracking of P_{tran} to P_{ref} [35, 36].

Attackers can attack the controller of a distributed generator by injecting false data into the actuator and making it send the same control command to its geographical neighbors. Assuming that r distributed generators are subjected to FDI attacks and considering $\alpha_M(k) \equiv \alpha_M = [\alpha M, \ldots, \alpha M]^T$ and $\alpha_W(k) = [\alpha_{r+1}(k), \ldots, \alpha_{r+n}(k)]^T$ are the utilization ratio vectors of misbehaving and well-behaving distributed generators, respectively, the algorithm (42) can be rewritten as:

$$\begin{bmatrix}\alpha_0(k+1)\\ \alpha_M(k+1)\\ \alpha_W(k+1)\end{bmatrix} = \begin{bmatrix}1 - KP_{0,\max} & -KP_{M,\max} & -KP_{W,\max}\\ 0_{r\times1} & I_{r\times r} & 0_{r\times(n-r)}\\ A_0 & A_M & A_W\end{bmatrix} \times \begin{bmatrix}\alpha_0(k)\\ \alpha_M(k)\\ \alpha_W(k)\end{bmatrix} + \begin{bmatrix}K\left(P_{ref} + P_{load} + P_{loss}\right)\\ 0_{r\times1}\\ 0_{(n-r)\times1}\end{bmatrix} \tag{43}$$

where $I_{r\times r}$ is the identity matrix. $[A_0\ A_M\ A_W]$ is equal to the n-r rows of $A + BK$. $P_{M,\max} = [P_{1,\max}, \ldots, P_{r,\max}]^T$, and $P_{W,\max} = [P_{(r+1),\max}, \ldots, P_{n,\max}]^T$.

Note that the first term on the right-hand side of (43) can be represented by the sum of the matrix $\tilde{A} = \begin{bmatrix}1 & 0_{1\times r} & 0_{1\times(n-r)}\\ 0_{r\times1} & I_{r\times r} & 0_{r\times(n-r)}\\ A_0 & A_M & A_W\end{bmatrix}$ and its perturbation matrix $\Delta = -\begin{bmatrix}P_{0,\max} & P_{M,\max} & P_{W,\max}\\ 0_{n\times1} & 0_{n\times r} & 0_{n\times(n-r)}\end{bmatrix}$. Hence perturbation theory can be employed to analyze system stability [37].

It is observed that $\tilde{A}$ is a lower block-triangular matrix with the eigenvalues $\lambda_i = 1$ for $i = 1, \ldots, r+1$, and the eigenvalues λ_j for $j = r+2, \ldots, n$-r. Since the blocks A_0, A_M, and A_W are the same as the original system in (42), λ_j locates in the open unit disk. Assuming v_r and u_r are the respective left and right eigenvectors of $\tilde{A}$ with $v_ru_r = 1$, when K is sufficiently small, the perturbation on $\lambda_i = 1$ can be characterized by [16]:

$$V^T\Delta U = \begin{bmatrix}-P_{\max}\\ 0_{r\times(n+1)}\end{bmatrix}[u_1, \ldots, u_{r+1}] = \begin{bmatrix}-P_{\max}u_1 & \cdots & -P_{\max}u_{r+1}\\ 0_{r\times1} & \cdots & 0_{r\times1}\end{bmatrix} \tag{44}$$

where $V = [v_1^T, \ldots, v_{r+1}^T]$, $U = [u_{r+2}^T, \ldots, v_{n-r}^T]$, and $P_{max} = [P_{0,\max}, \ldots, P_{n,max}]^T$.

$V^T \Delta U$ has a negative eigenvalue and an eigenvalue 0 with algebraic multiplicity r. Accordingly, $\tilde{A}$ $+\Delta$ has an eigenvalue 1 with algebraic multiplicity r if K is sufficiently small. The rest of the eigenvalues lie in the open unit disk. This indicates that $\tilde{A}$ $+\Delta$ is stable. It is straightforward to verify that the system is stable at the steady state $\{\alpha_0^*, {\alpha_M^*}^T, {\alpha_W^*}^T\}^T$ with:

$$\alpha_0^* = \min\{\max\{\tilde{\alpha}_0, 0\}, 1\}, \alpha_M^* = \alpha_M \quad (44)$$

$$\alpha_W^* = (I_{n-r} - A_W)^{-1}[A_0\ A_M]\begin{bmatrix}\alpha_0^* \\ \alpha_M\end{bmatrix} \quad (45)$$

where $\tilde{\alpha}_0 = (P_{ref} + P_{load} + P_{loss} - P_{M,\max}\alpha_M - P_{W,\max}\alpha_W^*)/P_{0,\max}$.

The analytical results show that the well-behaving distributed generators converge to the space spanned by α_0^* and α_M. Thus, when the false data is injected by attackers, utilization ratios of distributed generators fail to agree, preventing the active power output of a VPP from tracking the dispatch command. In addition, according to [16], the adjustable range of P_{tran} can be narrowed by FDI attacks in a large group of distributed generators. This degrades the controllability of the VPP.

4.2 FDI attack on microgrid

In a typical microgrid, a power inverter includes a DC power source, inverter bridge, power sharing unit, output filter, and voltage and current control loops. The output power dynamics of inverter i are:

$$\begin{cases} dP_i/dt = -\omega_{ci}P_i + \omega_{ci}(v_{odi}i_{odi} + v_{oqi}i_{oqi}) \\ dQ_i/dt = -\omega_{ci}Q_i + \omega_{ci}(v_{odi}i_{odi} - v_{oqi}i_{oqi}) \end{cases} \quad (46)$$

where v_{odi} and v_{oqi} are the d- and q-axis components of the output voltage. i_{odi} and i_{oqi} are the d- and q-axis components of the output current. P_i and Q_i are the active and reactive output power. ω_{ci} is the cut-off frequency of the output filter.

The large-signal dynamic of the inverter is given by [38].

$$\begin{cases} dx_i/dt = f_i(x_i) + g(x_i)u_i \\ y_i = h_i(x_i) \end{cases} \quad (47)$$

where $x_i = [\delta_i, P_i, Q_i, \phi_{di}, \phi_{qi}, \gamma_{di}, \gamma_{qi}, i_{ldi}, i_{lqi}, v_{odi}, v_{oqi}, i_{odi}, i_{oqi}]$. The detailed model of the inverter can be found in [38].

The power sharing function is realized by droop control expressed as [39–43]:

$$\begin{cases} \omega_i = \omega_{ni} - m_{pi}P_i \\ v_{mag,i} = V_{ni} - n_{qi}Q_i \end{cases} \quad (48)$$

where $v_{mag,i}$ and ω_i are the reference voltage and frequency, respectively. m_{pi} and n_{qi} are the respective droop coefficients, and ω_{ni} and V_{ni} are the set points.

Droop control makes voltage and frequency deviate from their set points. The cooperative control structure is used to alter ω_{ni} and V_{ni} in (48) to steer voltage and frequency to their reference values. Each converter can exchange information with its neighbors. Differentiating (48) yields:

$$\dot{\omega}_i = \dot{\omega}_{ni} - m_{pi}\dot{P}_i \quad (49)$$

The auxiliary control input is defined as:

$$\dot{\omega}_i = u_i \quad (50)$$

and the cooperative control law is given by [44–50]:

$$e_{\omega_i} = \sum_{j\in N_i} a_{ij}(\omega_i(t) - \omega_j(t)) + g_i(\omega_i(t) - \omega_{ref}) \quad (51)$$

where N_i contains the inverters that neighboring inverter i, and g_i represents the non-zero gain for inverter i.

The auxiliary input u_i is:

$$u_i(t) = -c_\omega e_{\omega_i}(t) \quad (52)$$

where c_ω is a coupling gain, and the set point in (49) satisfies:

$$\omega_{ni} = \int (u_i + m_{pi}\dot{P}_i)dt \quad (53)$$

From (50)–(53), the auxiliary input u_i uses the neighbor's frequency to mitigate system frequency deviation. The information exchange among neighboring inverters is vulnerable to malicious attacks, which can make the frequency deviation fail to go back to zero. Since the traditional bad data detection evaluates the validity of the received data in a centralized way, it is not applicable to distributed control of microgrids.

Two types of attacks, namely controller attacks and communication channel attacks, are considered as shown in Fig. 8 [51]. Attacks on controllers inject false data into actuators/sensors to attack the local controller, and FDI attacks on actuators can be modeled as [52, 53]:

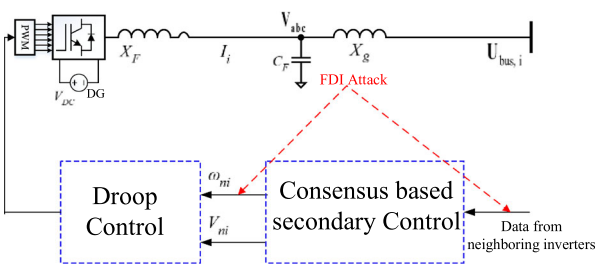

Fig. 8 Illustrative diagram of consensus-based control of inverter i under FDI attacks

$$u_i^c = u_i + \mu_i u_i^a \tag{54}$$

where u_i^a is the false data injected into actuator i. u_i^c is the corrupted control input and u_i is the original auxiliary input. μ_i is the attack signal, and when attack occurs, $\mu_i = 1$, otherwise, $\mu_i = 0$. Note that the attack signal can be either non-constant or constant. A non-constant attack signal that is viewed as noise can be handled by noise filtration techniques, while the attack signal is considered to be constant here [54].

If the whole controller is hijacked, the frequency corruption of inverter i can be expressed as

$$\omega_i^c = \omega_i + \eta_i \omega_i^a \tag{55}$$

where ω_i^a is the false frequency data injected into controller i. ω_i^c is the corrupted inverter frequency and ω_i is the reference frequency in (48). $\eta_i = 1$ represents the presence of attack.

If the communication channel between two neighboring inverters is attacked by FDI, the local controller receives the corrupted frequency signal [7, 11, 55–57]. FDI attack on the communication channel can be modeled by:

$$\omega_i^j = \omega_i + \eta_i \omega_i^a \tag{56}$$

where ω_i^a is the false data injected into controller i, and ω_i^j is the corrupted inverter frequency transmitted to inverter j. $\eta_i = 1$ implies the presence of attack.

The next step is to reveal the vulnerability of the cooperative control of a microgrid under FDI attack. Considering the cooperative control protocol (51) is under attack, the synchronization error will not return to zero for an intact inverter if it is reachable from a corrupted inverter [17]. For example, considering $\omega^a = [(\omega_1^a)^T, \ldots, (\omega_N^a)^T]^T$ and $u^a = [(u_1^a)^T, \ldots, (u_N^a)^T]^T$ are the respective attack vectors injected to sensors and actuators, the global synchronization error dynamic is obtained by applying the control strategy (50) and (52) as well as FDI attacks (54)–(56), as:

$$\dot{e}_\omega = -c_\omega (L + G) e_\omega \tag{57}$$

where L is the Laplacian matrix defined as $L = D - A$, while more properties of L can be found in [58–60]. $D = \mathrm{diag}\{N_i\}$ with N_i being the set of inverters that send data to inverter i (the neighbors of inverter i). $A = [a_{ij}]$ with a_{ij} being the weights of communication links between inverter i and j.

Let $\iota = \eta(L + G)e_\omega^a + \mu u$, $\eta = diag(\eta_i)$, and $\mu = diag(\mu_i)$, the solution to (57) is:

$$e_\omega(t) = e^{-c_\omega (L+G)t} e_\omega(0) + \int_0^t e^{-c_\omega (L+G)(t-\tau)} \iota d\tau \tag{58}$$

Given that $(L + G)$ is a positive definite matrix, the first term in (58) approaches zero for $c_\omega > 0$. Using $e^{At} = \sum_{m=1}^{\infty} (At)^m$ yields:

$$e_\omega(t) \rightarrow \sum_{m=1}^{\infty} \int_0^t (-c_\omega (L + G)(t - \tau))^m \iota d\tau \tag{59}$$

If m is the first integer such that $l_{ij}^m = ((L + G)^m)_{ij}$ is not zero, node i is reachable from node j, and m is the length of the shortest directed path from j to i. Consequently, there exists $l_{ij}^m \neq 0$ for $0 < m < N - 1$ if inverter i is reachable from the compromised inverter j.

5 Results and discussion

In current research on the impacts of FDI on power systems, the adopted FDI model is often static on a single snapshot, ignoring the complexity of the attack behavior. The risk of FDI cannot be fully revealed as attackers are capable of constructing a subtly dynamic attack to avoid detection. Future effort should be dedicated to a more detailed FDI model to account for the dynamic behavior of attacks.

Although there is a lot of literature on the influence of FDI on power system state estimation, studies on its influence on power system dynamic state estimation are limited. Power system dynamic state estimates can be used as controller inputs (e.g. wide-area damping controllers) to improve control performance, while attackers can decrease control performance by attacking the dynamic state estimation. To promote proper countermeasures, it is necessary to investigate the impacts of FDI on power system dynamic state estimation.

Most research on FDI impact on power system stability focuses on breaking the frequency stability by causing an imbalance between supply and demand. Future research needs to be conducted to study the interaction between FDI and small signal/transient stability. In the modern-day power grid, the wide area measurement system is greatly exploited for detection of power system anomalies. The data from the phasor measurement units (PMUs) is communicated to the control center to monitor and damp inter-area oscillations [61]. The communication between the PMU and the control center can be corrupted by FDI attacks. This can degrade the damping of inter-area oscillations and induce small-signal instability.

6 Conclusion

With the rapid development of the smart grid, and wide employment of information and communication technology in

the traditional power grid and microgrid, the power industry is facing cyber threats. This paper has conducted a comprehensive investigation into the potential risks of false data injection attacks on power systems. State-of-the-art models and methods are reviewed to explain how attackers might attack the system by injecting false data. First, an attack vector can be constructed by solving a linear programming problem, and false data is injected to significantly increase the operational cost of the power system. Economic dispatch can also be adversely affected by designing optimal FDI attacks and triggering an initial contingency that consequently initiates sequential outages. Second, an undetectable FDI attack can be constructed to disrupt power system state estimation, Such an attack can be launched using the full/local network information. Third, frequency instability can be caused by injecting false data that prevents the active power output of a power inverter from tracking its dispatch command. Attackers can also compromise the cooperative control of a microgrid by attacking the controllers. Finally, an assessment of research results is provided, and the findings can help to fully reveal the potential risks of FDI and promote comprehensive protection measures.

7 Methods section

The aim of this paper is to investigate the mechanism of how FDI affects power systems. This is achieved from the perspectives of economic dispatch, power system state estimation, and distributed control of distributed generators/microgrids. The mathematical models for economic dispatch and power system state estimation are presented. The design of a successful FDI attack is then formulated as an optimization problem, which can be solved in the MATLAB environment. For the cooperative control of distributed generators/microgrids, a rigorous mathematical proof method is used to construct the FDI attacks.

Abbreviations

FDI: False data injection; SCADA: Supervisory control and data acquisition; PMU: Phasor measurement unit; SCED: Security-constrained economic dispatch; BDD: Bad data detection; IC: Initial contingency; KKT: Karush-Kuhn-Tucker; KCL: Kirchhoff's Current Law; KVL: Kirchhoff's Voltage Law; VPP: Virtual power plant

Acknowledgements

Not applicable.

Author's contributions

Y. Xu proposed the methodological framework and mathematical model, and analyzed the results. The author read and approved the final manuscript.

Funding

No funding was received.

Availability of data and materials

Not applicable.

Competing interests

The author declare that they have no competing interest.

Received: 30 December 2019 Accepted: 6 August 2020
Published online: 04 September 2020

References

1. Liang, G., Zhao, J., Luo, F. J., Weller, S., & Dong, Z. (2017). A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, *8*(4), 1630–1638.
2. Che, L., Liu, X., Shuai, Z., Li, Z., & Wen, Y. (2018). Cyber cascades screening considering the impacts of false data injection attacks. *IEEE Transactions on Power Apparatus and Systems*, *33*(6), 6545–6556.
3. Che, L., Liu, X., Li, Z., & Wen, Y. (2019). False data injection attacks induced sequential outages in power systems. *IEEE Transactions on Power Apparatus and Systems*, *34*(2), 1513–1522.
4. Yuan, Y., Li, Z., & Ren, K. (2011). Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid*, *3*(3), 382–390.
5. Liu, X., Li, Z., Shuai, Z., & Wen, Y. (2017). Cyber attacks against the economic operation of power system: A fast solution. *IEEE Transactions on Smart Grid*, *8*(2), 1023–1025.
6. Xiang, Y., Ding, Z., Zhang, Y., & Wang, L. (2017). Power system reliability evaluation considering load redistribution attacks. *IEEE Transactions on Smart Grid*, *8*(2), 889–901.
7. Liu, X., & Li, Z. (2014). Local load redistribution attacks in power systems with incomplete network information. *IEEE Transactions on Smart Grid*, *5*(4), 1665–1676.
8. Zhang, Y., Wang, L., Xiang, Y., & Ten, C. (2015). Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Transactions on Smart Grid*, *6*(4), 170–1721.
9. Zhang, Z., Gong, S., Dimitrovski, A., & Li, H. (2013). Time synchronization attack in smart grid: Impact and analysis. *IEEE Transactions on Smart Grid*, *4*(1), 87–98.
10. Kosut, O., Jia, L., Thomas, R., & Tong, L. (2011). Malicious data attacks on the smart grid. *IEEE Transactions on Smart Grid*, *2*(4), 645–658.
11. Liu, X., & Li, Z. (2017). False data attacks against ac state estimation with incomplete network information. *IEEE Transactions on Smart Grid*, *8*(5), 2239–2248.
12. Zhao, J., Zhang, G., Dong, Z., & Wong, K. (2016). Foresting-aided imperfect false data injection attacks against power system nonlinear state estimation. *IEEE Transactions on Smart Grid*, *7*(1), 6–8.
13. Zhao, J., Mili, L., & Wang, M. (2018). A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. *IEEE Transactions on Power Apparatus and Systems*, *33*(5), 4868–4877.
14. Deng, R. L., Zhuang, P., & Liang, H. (2019). False data injection attacks against state estimation in power distribution systems. *IEEE Transactions on Smart Grid*, *10*(3), 2871–2881.
15. Bi, S., & Zhang, Y. (2014). False data injection attacks with limited susceptance information and new countermeasures in smart grid. *IEEE Transactions on Smart Grid*, *15*(3), 1619–1628.
16. Liu, Y., Xin, H., Qu, Z., & Gan, D. (2016). An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks. *IEEE Transactions on Smart Grid*, *7*(6), 2923–2932.
17. Abhinav, S., Modares, H., Lewis, F., Ferrese, F., & Davoudi, A. (2018). Synchrony in networked microgrids under attacks. *IEEE Transactions on Smart Grid*, *9*(6), 6731–6741.
18. Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., & Bulter-Purry, K. (2012). *A smart grid vulnerability analysis framework for coordinated variable structure switching attacks*, (pp. 1–6). San Diego: Proc. IEEE PES. Gen. Meeting.
19. Chen, B., Mashayekh, S., Butler-Purry, L., & Kundur, D. (2013). *Impact of cyber attacks on transient stability of smart grids with voltage support devices*, (pp. 1–5). Vancouver: Proc. IEEE PES Gen. Meeting.
20. Brown, H., & DeMarco, C. (2018). Risk of cyber-physical attack via load with emulated inertia control. *IEEE Transactions on Smart Grid*, *9*(6), 5854–5866.
21. Athari, M., & Wang, Z. (2018). Impacts of wind power uncertainty on grid vulnerability to cascading overload failures. *IEEE Transactions on Sustainable Energy*, *9*(1), 128–137.
22. Liang, G. Q., Weller, S. R., Luo, F. J., Zhao, J. H., & Dong, Z. Y. (2018). Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism. *IEEE Transactions on Smart Grid*, *9*(4), 3820–3829.
23. Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations. https://energy.gov/sites/prod/files/oeprod/documentsandmedia/blackoutfinal-web.pdf. Accessed 3 Dec 2019.

24. Vaiman, M. (2012). Risk assessment of cascading failures: Methodologies and challenges. *IEEE Transactions on Power Apparatus and Systems*, *27*(2), 631–641.
25. Eppstein, M., & Hines, P. (2012). A random chemistry algorithm for identifying collections of multiples contingencies that initiate cascading failure. *IEEE Transactions on Power Apparatus and Systems*, *27*(3), 1698–1705.
26. Liang, J., Sankar, L., & Kosut, O. (2016). Vulnerability analysis and consequence of false data injection attack on power system state estimation. *IEEE Transactions on Power Apparatus and Systems*, *31*(5), 3864–3872.
27. Wang, H. Z., Ruan, J. Q., Zhou, B., Li, C. B., Wu, Q. W., Raza, M. Q., & Cao, G. Z. (2019). Dynamic data injection attack detection of cyber physical power systems with uncertainties. *IEEE Transactions on Industrial Informatics*, *15*(10), 5505–5518.
28. Wood, A., & Wollenberg, B. (1996). *Power generation, operation and control*, (2nd ed.,). Hoboken: Wiley.
29. Qu, Z., & Simaan, M. (2014). Modularized design for cooperative control and plug-and-play operation of networked heterogeneous systems. *Automatica*, *50*(9), 2405–2414.
30. Dorfler, F., Simpson-Porco, J., & Bullo, F. (2014). *Plug-and-play control and optimization in microgrids*, (pp. 211–216). Los Angeles: IEEE Conference on Decision and Control.
31. Rocaber, J., Luna, A., Blaabjerg, F., & Rodriguez, P. (2012). Control of power converters in AC microgrids. *IEEE Transactions on Power Electronics*, *27*(11), 4734–4749.
32. Simpson-Porco, J. (2015). Secondary frequency and voltage control of islanded microgrids via distributed averaging. *IEEE Transactions on Industrial Electronics*, *62*(11), 7025–7038.
33. Schiffer, J., Seel, T., Raisch, J., & Sezi, T. (2016). Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control. *IEEE Transactions on Control Systems Technology*, *24*(1), 96–109.
34. Nasirian, V., Shafiee, Q., Guerrero, J., Lewis, F., & Davoudi, A. (2016). Droop-free distributed control for AC microgrids. *IEEE Transactions on Power Electronics*, *31*(2), 1600–1617.
35. Guo, M., Dimarogonas, D., & Johansson, K. (2012). *Distributed real-time fault detection and isolation for cooperative multi-agent systems*, (pp. 5270–5275). Montreal: Proc. Amer. Control Conf.
36. Gusrialdi, A., Qu, Z., & Simaan, M. (2014). *Robust design of cooperative systems against attacks*, (pp. 1456–1462). Portland: Proc. Amer. Conf.
37. Horn, R., & Johnson, C. (1985). *Matrix analysis*. Cambridge: Cambridge Univ. Press.
38. Bidram, A., Lewis, F., & Davoudi, A. (2014). Distributed control systems for small-scale power networks: Using multiagent cooperative control theory. *IEEE Control Systems*, *34*(6), 56–77.
39. Vyver, J., De Kooning, J., Meersman, B., Vandevelde, L., & Vandoorn, T. (2016). Droop control as an alternative inertial response strategy for the synthetic inertia on wind turbines. *IEEE Transactions on Power Apparatus and Systems*, *2*(31), 1129–1138.
40. Ye, H., Pei, W., & Qi, Z. (2016). Analytical modeling of inertial and droop responses from a wind farm for short-term frequency regulation in power systems. *IEEE Transactions on Power Apparatus and Systems*, *31*(5), 3414–3423.
41. Ramtharan, G., Ekanayake, J., & Jenkins, N. (2007). Frequency support from doubly fed induction generator wind turbines. *IET Renewable Power Generation*, *1*(1), 3–9.
42. Morren, J., Pierik, J., & DeHaan, S. (2006). Inertial response of variable speed wind turbines. *Electric Power Systems Research*, *76*(11), 980–987.
43. Liu, W., Gu, W., Sheng, W., Meng, X., Xue, S., & Chen, M. (2016). Pinning-based distributed cooperative control for autonomous microgrids under uncertain communication topologies. *IEEE Transactions on Power Apparatus and Systems*, *2*(31), 1320–1329.
44. Guo, F., Wen, C., Mao, J., Chen, J., & Song, Y. (2015). Distributed cooperative secondary control for voltage unbalance compensation in an islanded microgrid. *IEEE Transactions on Industrial Informatics*, *11*(5), 1078–1088.
45. Manaffam, S., Talebi, M., Jain, A., & Behal, A. (2018). Intelligent pinning based cooperative secondary control of distributed generators for microgrid in islanding operation mode. *IEEE Transactions on Power Apparatus and Systems*, *33*(2), 1364–1373.
46. Su, H., Rong, Z., Chen, Q., Wang, X., Chen, G., & Wang, H. (2013). Decentralized adaptive pinning control for cluster synchronization of complex dynamic networks. *IEEE Transaction on Cybernatics*, *43*(1), 394–399.
47. Bidram, A., Davoudi, A., Lewis, F., & Guerrero, J. (2013). Distributed cooperative secondary control of microgrids using feedback linearization. *IEEE Transactions on Power Apparatus and Systems*, *28*(3), 3462–3470.
48. DeLellis, P., Di Bernardo, M., & Garofalo, F. (2013). Adaptive pinning control of networks of circuits and systems in Lur'e form. *IEEE Transaction Circuits System I, Reg*Papers, *60*(11), 3033–3042.
49. Chen, T., Liu, X., & Lu, W. (2007). Pinning complex networks by a single controller. *IEEE Transaction Circuits System I, Reg*Papers, *54*(6), 1317–1326.
50. Manaffam, S., Talebi, M., Jain, A., & Behal, A. (2017). Synchronization in networks of identical systems via pinning: Application to distributed secondary control of microgrids. *IEEE Transactions on Control Systems Technology*, *25*(6), 2227–2234.
51. Amin, S., Schwartz, G., & Sastry, S. (2013). Security of interdependent and identical networked control systems. *Automatica*, *49*(1), 186–192.
52. Pasqualetti, F., Bicchi, A., & Bullo, F. (2012). Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, *57*(1), 90–104.
53. Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, *58*(11), 2715–2729.
54. Abhinav, S., Schizas, I., Lewis, F., & Davoudi, A. (2018). Distributed noise-resilient networked synchrony of active distribution systems. *IEEE Transactions on Smart Grid*, *9*(2), 836–846.
55. Pan, K., Teixeira, A., Cvetkovic, M., & Palensky, P. (2019). Cyber risk analysis of combined data attacks against power system state estimation. *IEEE Transactions on Smart Grid*, *10*(3), 3044–3056.
56. Teixeira, A. (2010). *Cyber security analysis of state estimators in electric power systems*, (pp. 5991–5998). Atlanta: Proc. 49th IEEE Conf., on Decisions and Control.
57. Andersson, G. (2012). *Cyber-security of SCADA systems*, (pp. 1–2). Washington, DC: Proc. IEEE PES Innovative Smart Grid Technologies.
58. Olfati-Saber, R., & Murray, R. (2005). Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, *49*(9), 1520–1533.
59. Fax, J., & Murray, R. (2004). Information flow and cooperative control of vehicle formations. *IEEE Transactions on Automatic Control*, *49*, 1465–1475.
60. Olfati-Saber, R., & Shamma, J. (2005). Consensus filters for sensor networks and distributed sensor fusion. In *Proc. 44th IEEE Conf. Decision and control /European control Conf*, (pp. 6698–6703).
61. Appasani, B., & Dusmanta, M. (2018). A review on synchrophasor communication system: Communication technologies, standards and applications. In *Protection and control of modern power systems*.