J. Mod. Power Syst. Clean Energy (2018) 6(4):630–641
https://doi.org/10.1007/s40565-018-0427-z

Intelligent data attacks against power systems using incomplete network information: a review

Yufei SONG[1], Xuan LIU[1], Zhiyi LI[2], Mohammad SHAHIDEHPOUR[2], Zuyi LI[2]

Abstract With the integration of information technologies, power system operations are increasingly threatened by cyber-attacks. It has even been revealed that an attacker can inject false data into real-time measurements stealthily without knowing the full configuration (e.g., network topology) of a power system. In this paper, we present a comprehensive review on false data injection attacks which utilize barrier conditions, blind identification techniques and data driven approaches to overcome limitations of incomplete network information. We also point out future research topics for facilitating the detection and prevention of such false data attacks.

Keywords Cyber security, False data injection attack, Incomplete network information, Power system state estimation

CrossCheck date: 5 June 2018

Received: 31 March 2018 / Accepted: 5 June 2018 / Published online: 12 July 2018

✉ Xuan LIU
xliu@hnu.edu.cn

Yufei SONG
songyufei@hnu.edu.cn

Zhiyi LI
zhiyi.li@hawk.iit.edu

Mohammad SHAHIDEHPOUR
ms@iit.edu

Zuyi LI
lizu@iit.edu

[1] College of Electrical and Information Engineering, Hunan University, Changsha, China

[2] Electrical and Computer Engineering Department, Illinois Institute of Technology, Chicago, IL, USA

1 False data attack model

The reliable and safe operation of power systems is crucial to the economy and homeland security of a nation [1, 2]. However, the operational security of modern power systems is being challenged by the high integration of information technologies [3, 4]. In fact, to monitor the real-time operation state of a power system, an increasing number of sensors and meters are being installed to collect the real-time measurements (such as bus voltages and line power flows) which are then transmitted to the control center. Power system operators make energy management decisions based on the received measurements that collectively contribute to the situational awareness of power system operations. These sensors and meters are therefore regarded as the eye of a power system. There will be certain uncontrollable noises in the real-time measurements due to the mechanical flaw of meters and measuring errors. To detect and screen out potential bad data, state estimation is employed in energy management system (EMS) to determine the most likely operating condition of the power system based on redundant power grid measurements. Random noises are not correlated with the physical characteristic of a power system, so they will increase the residual in the state estimation.

In the DC state estimation, the state vector $\widehat{\boldsymbol{\theta}}$ is estimated by solving the following non-linear optimization problem:

$$\widehat{\boldsymbol{\theta}} = \min \|\boldsymbol{z} - \boldsymbol{H}\boldsymbol{\theta}\|_2 \tag{1}$$

where $\boldsymbol{z}$ is the vector of measurements; $\boldsymbol{H}$ is the Jacobian matrix corresponding to the network configuration.

The most popular method to solve the optimization problem is the least square method [5]. After the best

possible estimation of the system state is determined, the residual r is calculated:

$$r = \| z - H\widehat{\theta} \|_2 \tag{2}$$

If the residual is less than a given threshold value, the estimated state $\widehat{\theta}$ is regarded acceptable. Otherwise, the estimated state is corrupted by bad data. According to the principle of bad data detection, Liu et al. [6] proved that if the amounts of injected bad data satisfy

$$a = Hc \tag{3}$$

where a is the injected malicious data by an attacker; c is the corresponding increment in state vector.

Then the overall residual of the power system will remain the same as if there were no bad data. That is, if the original data can pass the bad data detection, the corrupted data will escape from detection in the same manner. Therefore, this kind of false data injection attacks can hardly be detected.

DC state estimation provides us a fast and simple method to estimate the operating condition of a power system. However, it ignores bus voltages, reactive power flows and line losses. To better reflect the operating condition of the power system, AC state estimation is usually used in practical power system applications.

In a AC system, the Jacobian matrix H depends on the current state of the system so that (3) is rewritten as [7]:

$$a = H(x + c) \cdot (x + c) - H(x) \cdot x \tag{4}$$

We can see that the injected false data a depends on the current state of the power system. In other words, the attacker has to obtain or estimate the system state to construct the undetectable false data a. Since only a few number of phasor measurement units (PMUs) have been instated in power systems, phase angles at most buses are unavailable. Consequently, it will be more difficult for an attacker to launch false data attack against AC state estimation.

Recently, false data injection attack has attracted intensive research interests. Significant efforts have been dedicated to reveal the wide impacts of false data injection attacks on economic operation [8, 9], transmission line power flows [10–12], real-time electric market [13–15], transient stability [16, 17], real-time topology [18, 19], line outage detection [20], PMU data quality [21, 22], microgrids [23, 24], automation generation control (AGC) [25, 26] and so on. Note that the existing models have a common drawback that limits their applications. It is known that the Jacobian matrix H is determined by the topology and line parameters of a power network. Thus, an attacker has to obtain the full topology and network parameters of the entire power system to construct the undetectable false data. As will be discussed later, this is an impractical assumption. In this paper, we review the existing literatures on false data injection attacks based on both DC and AC power flow models under the assumption of incomplete network information.

The rest of this paper is organized as follows. Section 2 discusses the motivation of developing a local model for false data injection attacks. Sections 3–7 investigate the local attack mechanism (with incomplete network information) based on barrier conditions, blind identification and data driven approaches. Section 8 further discusses three special cases for the local false data attacks. Finally, Sects. 9 and 10 discuss the future work and conclude the paper.

2 Why we need local attack model?

Most of the existing attack models are developed based on the assumption that attackers have access to the full network configuration information including the topology and other physical properties of the targeted power system. However, this assumption is impractical due to the following reasons.

1) The amount of required power grid data is huge

Today's power grids are continually expanding their sizes for better serving electricity customers. For example, the IEEE 13659-bus system (as shown in Table 1 [27]) has 13659 buses and over 20000 lines. For such a large system, an attacker needs to obtain the reactance and resistance of over 20000 lines.

Since an attacker needs to pay a cost to obtain a certain set of line parameters, this is a difficult or even impossible task for an attacker with limited a budget to gain full information of the network configuration. In other words, the global models which are based on full network information is impractical.

2) Power grid data are difficult to obtain

On the other side, power grid is a critical infrastructure whose reliable and safe operation is very important to the economy prosperity and homeland security of a nation. In

Table 1 Numbers of buses and lines in different systems

Power grid	No. of nodes	No. of lines
IEEE 300	300	409
IEEE 2383	2383	2886
IEEE 3120	3120	3693
IEEE 6515	6515	8104
IEEE 13659	13659	20467

particular, the complicated international environment drives attackers to attack power grids. The number of cyber-attacks against power grids keeps increasing. An attacker can identify the weakness of a power system and launch a cyber or physical attack that will bring in severe consequences to the power system operation. Given these reasons, sensitive power system data are adequately protected. As a result, it is difficult for an attacker to access or obtain these data.

Considering the difficulty of obtaining the network parameters of a power system, an intelligent data attack should have the following three properties:

1) Undetectable. As the EMS uses the bad data detection procedure to remove the interruption of false data on the state estimation, the first thing for an attacker is to design the false data that can escape from being identified as bad data. One possible method is to inject the false data that obey the physical laws of the power system, such as Kirchhoff Current Law (KCL) and Kirchhoff Voltage Law (KVL). By doing so, the injected false data will not increase the residual of the state estimation and eventually avoid being detected.
2) Reduced requirement of network information. As discussed, an attacker needs to obtain the topology and line parameters of a power grid for making the injected data undetectable. However, it is difficult to for an attacker to obtain this information due to the security issue. So, from the perspective of an attacker, a more practical strategy is to compress the requirement of network information.
3) Severe consequence of data attacks. The ultimate goal of a cyber-attack is to pose severe consequences to the power system operation, e.g., transmission line outage, loss of loads, increased operation cost. So, an attacker is always active in finding the vulnerability of a power grid and then launches a cyber-attack against it.

Once these three conditions are met, such an attack can be defined as an intelligent data attack.

3 Attack model based on DC barrier condition

In this section, we first investigate the attack mechanism of false data injection attack based on incomplete network information and DC power flow equations.

3.1 DC model

In reality, an attacker constrained by its capacity/budget can only attack a limited number of measurements in a local region (denoted as region A). In the global model, false data injection initiated in region A will eventually incur changes in the power flows outside that region. That is, the measurements in the outer region also need to be attacked to hide the initial false data injection. Consequently, this attacker needs to get the topologies and line parameters of the network out of region A. So, as shown in Fig. 1, one possible strategy is to ensure that the false data injected into region A will not change the power flows in the outer region.

We proved the following theorem in [28].

Theorem 1 Suppose a power grid is decomposed into two connected regions A and N by a set of lines (tie lines). If an additional injected power $\Delta \boldsymbol{P}_{\mathrm{A}}$ into region A makes the phase angles of all its boundary buses increase or decrease by the same amount

$$\Delta\theta_r = \alpha \qquad \forall r \in \Omega_{\mathrm{BA}} \tag{5}$$

where Ω_{BA} is the set of boundary buses in region A; $\Delta\theta_r$ is the incremental phase angle at bus r; $\Delta \boldsymbol{P}_{\mathrm{A}}$ is the injected bus power injection vector in region A.

Then, the power flows in region N remain the same under the false data injection.

$$\Delta \boldsymbol{F}_{\mathrm{N}} = 0 \tag{6}$$

where $\Delta \boldsymbol{F}_{\mathrm{N}}$ is the incremental line flow vector in region N.

Theorem 1 tells that if we enforce all the changes of phase angles at the boundary buses in region A to be the same, no additional power exchange will occur between region A and the outer region. This phenomenon is referred as to the *barrier effect of power flows*. Constraint (5) is the *barrier conditions* for the DC case.

We can see that the boundary conditions met by the attacking region A enable an attacker to design the undetectable false data (that follows KCL and KVL) based on the topology and network parameters of the local attack region. There is no necessity of obtaining the network information in the outer region. The local model indicates that an attacker can launch a successful false data by paying a very low cost.

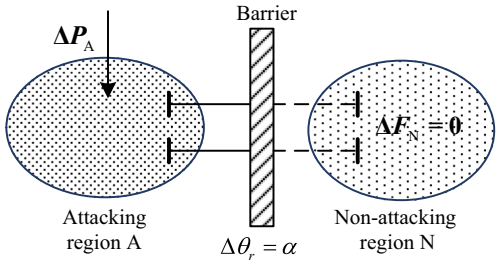

Fig.1 Power flow barrier effect for DC case

Followed by our work, a lot of research has been carried out to reveal the attack mechanism based on barrier effect of power flows.

A bilevel optimization model was proposed in [29] to evaluate the impacts of local false data attacks on the long-term power supply reliability. In the lower level, to avoid having access to the topology and line parameters of the entire power network, the authors adopted the barrier conditions to limit the additional power flows within the attacking region. Later, the impacts of the local load redistribution attacks with incomplete network information on power supply adequacy was also investigated in [30]. The attack process for modifying the measurements is modeled by the semi-Markov model.

Li et al. in [31] studied the local coordinated cyber-physical attack scheme using the incomplete network information. This is achieved by estimating the reactance of lines in the attacking region and replacing the non-attacking region with its equivalent network. It was demonstrated that such an attack can mask the outage of transmission lines.

Sun et al. [32] proposed a false data proportional attack, in which an attacker could construct the false data that is able to avoid the traditional bad data detection method just based on the topology information of a local region. The line parameters of transmission lines are not needed. In addition, it was proved that the injected false data can be adjusted proportionally when the measurement of a bus and transmission-line data is changed.

Ly et al. [33] employed the proposed local attack scheme in [28] to examine the rerouting strategy for defending false data attacks in power systems by increasing the power grid topology complexity. An algorithm was developed to evaluate the probability of a successful false data attack for a particular topology and status of circuit breakers.

The authors in [34] introduced a practical attack scheme using limited network information. Considering the limited information of the attacker, a multiple linear regression model was introduced to learn the relationship between the attack region and the outer subnetwork based on historical data. A bilevel optimization problem was set up to identify the most damaging consequences of the attack to the operation of the power system.

Zhang et al. [35] proposed a false data attack model with limited network information, in which an attacker has perfect knowledge of the network information of the targeted subnetwork but has only estimated knowledge of the power transfer distribution factor. It was revealed that such an attack scheme is able to avoid the traditional bad data detection.

3.2 Feasibility theorem

It should be pointed out that the boundary conditions will impact the feasibility of the DC power flows in region A when the phase angles at boundary buses are set the same value. So, it is necessary to develop a simple method to find a feasible region. A feasible attack region is defined as the region in which a nonzero attack vector can be constructed.

According to the graph theory, we in [28] introduced the following two theorems to find a feasible region.

Theorem 2 Suppose a power grid is decomposed into two regions A and N connected by a set of lines (tie lines). Suppose the attacking region A consists of ρ non-boundary buses and σ boundary buses. If there are at most $q = \rho - 1$ non-attackable bus injection measurements in region A, then there exists a feasible non-zero attacking vector.

Theorem 2 can also be extended to include the cases where the attacking region A is disconnected and/or the non-attacking region N is disconnected, as shown in Theorem 2E.

Theorem 2E Suppose a power grid is decomposed into an attacking region A and a non-attacking region N connected by a set of lines (tie lines). Suppose the attacking region A consists of ρ non-boundary buses and σ boundary buses. The σ boundary buses in A are connected to n non-attacking islands. If there are at most $q = \rho + n - 2$ non-attackable bus injection measurements in region A, then there exists a feasible non-zero attacking vector.

According to Theorems 2 and 2E, the only thing that we need to do is to count the number of buses. We use the following example to illustrate the two proposed feasibility theorems.

As shown in the left of Fig. 2, α and β are the corresponding bus phase increment, the attacking region includes three boundary buses. There is only one non-boundary bus in the attacking region, so $\rho = 1$. The non-attacking region is connected, $n = 1$. We can see that $q > \rho + n - 2$, and thus Theorem 2 is not satisfied. That is, the attacking region is infeasible. However, as shown in the

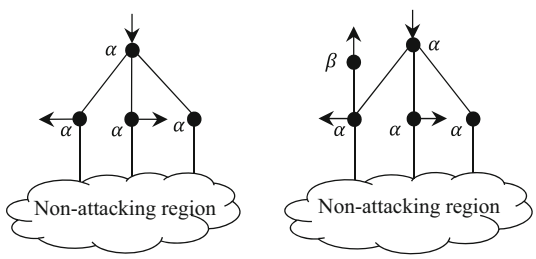

Fig. 2 Illustrative examples of feasibility theorem

right of Fig. 2, if we add one attackable bus into the attacking region, $\rho = 2$ and $q \leq \rho + n - 2$. Theorem 2 is then satisfied and the attacking region is feasible.

3.3 Optimizing the attacking region

As discussed in Sect. 2, it is difficult for an attacker to get the line parameters due to the security issues. Although the local DC model reveals that an undetectable attack vector can be constructed using incomplete network information, the following concern needs to be addressed instead: How much information is needed for launching a successful attack, given the fact that an attacker hopes to perform a successful false data injection with the same impact but based on as little information as possible?

To address this issue, we proposed a heuristic algorithm in [19, 36] to determine an optimal attacking region such that the required network information can be reduced as much as possible. As shown in Fig. 3 [19], the potential attacking region starts from a small sub-network, and gradually expands until the false data injection becomes feasible in the region. According to the boundary conditions, power flows only change in the current attacking region without impacting the power flows in the outer region E, if the phase angles at boundary buses are set the same value.

The whole algorithm can be summarized as follows [36]:

Step 1: Determine an initial attacking region of a target component.

Step 2: Obtain the parameters of all lines in the attacking region.

Step 3: Set the phase angles at boundary buses the same value and then determine the feasibility of the attacking region.

Step 4: If a feasible attacking region is found, stop. Otherwise, go to *Step 5*.

Step 5: Expand the attacking region, go to *Step 2*.

As the attacking region starts from a small one, the size of the final attacking region will be controlled not to be unnecessarily large. Accordingly, the numbers of buses and lines included in the final attacking region will be relatively small compared to global models. So, the attacking cost to obtain the network information can be reduced significantly.

4 Attack model based on AC barrier condition

In this section, we continue to investigate the attack mechanism against AC state estimation based when the network information obtained by attackers is incomplete.

4.1 Local model

In the DC power flows, the superstition principle applies. However, when the AC model is considered, incremental power flows are dependent on the current system state. In other words, the Jacobian matrix $\boldsymbol{H}$ is not constant under various operating conditions. In this sense, the boundary conditions (5) for ensuring the barrier effect of power flows are not valid. It is essential for us to develop new boundary conditions for the AC case. As shown in Fig. 4 [37], similar to the DC case, the power system is supposed to be decomposed into the attacking region A and non-attacking region N.

The measurements are separated into two parts: z_1 includes all the measurements in the attacking region A excluding the flow measurements on the tie lines; z_2 contains the remaining measurements. After that, we have

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{H}_{11} & \boldsymbol{H}_{12} \\ 0 & \boldsymbol{H}_{22} \end{bmatrix} \begin{bmatrix} \hat{\boldsymbol{x}}_1 \\ \hat{\boldsymbol{x}}_2 \end{bmatrix} + \begin{bmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \end{bmatrix} \tag{7}$$

where $\boldsymbol{e}_1, \boldsymbol{e}_2$ are the corresponding random error vectors for z_1, z_2. Different from the DC case, the Jacobian matrices $\boldsymbol{H}_{11}, \boldsymbol{H}_{12}, \boldsymbol{H}_{22}$ in the AC case depend on the state vector.

After the false data $z_1'$is injected, the residual of the system is determined by:

$$r' = \min \| \boldsymbol{z}' - \boldsymbol{H}(\boldsymbol{x}')\boldsymbol{x}' \|_2 \tag{8}$$

where $r', \boldsymbol{x}'$ are the residual and state variable after the injection of false data.

It was proved in [37] that

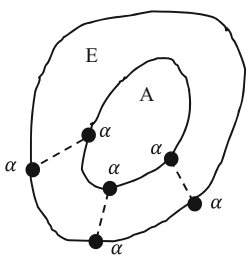

Fig. 3 Expansion of the attacking region

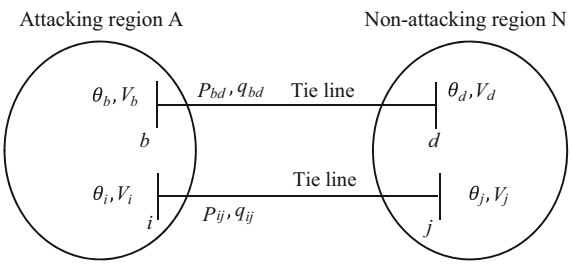

Fig.4 Power flow barrier effect for the AC case

$$r' \le r'' = \|\boldsymbol{z}' - \boldsymbol{H}(\widehat{\boldsymbol{x}}')\widehat{\boldsymbol{x}}'\|_2 = \|\boldsymbol{e}_2\|_2 < r = \left\| \begin{matrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \end{matrix} \right\|_2 \tag{9}$$

where $\widehat{\boldsymbol{x}}'$ is the estimated state vector after the injection of false data.

Constraint (9) indicates that the injected false data deceases the overall residual of the power system since the injected false data conform to physical laws in the attacked power system. The proposed practical attack model for the AC case is characterized by the three properties as follows [37]:

1) The false data injected into the attacking region follows KCL and KVL;
2) The voltage magnitudes at the boundary buses in the attacking region are set to the values of the corresponding measurements;
3) The flows on the tie lines are set to the corresponding measurements.

4.2 Estimating phase angle difference

For a pair of buses b and d (see Fig. 5 [37]), if we find a path k that connects these two buses (e.g., b, d), then it is trivial to prove that (10) holds [37],

$$\sum_{l \in S_k} \delta_l = \theta_b - \theta_d \tag{10}$$

where S_k includes all lines in path k.

Constraint (10) indicates that one can select a path k that connects buses b and d, and then sum the angle differences of all lines along the path to determine the value of $\theta_b - \theta_d$. By doing so, an attacker does not need to obtain the actual phase angles. However, the challenge here is how to calculate the angle difference of a line without knowing the phase angles at its terminal buses.

Under the DC assumptions, the power flow of line i-j is:

$$p_{ij} = \frac{\theta_i - \theta_j}{x_{ij}} \tag{11}$$

Based on (11), the angle difference of a line is calculated by

$$\theta_{ij} = \theta_i - \theta_j = x_{ij} p_{ij} \tag{12}$$

There is a trend that the greater the ratio of reactance X to resistance R of a line is, the smaller the difference would be. This motivates us to find a best path that has the largest average ratio of reactance to resistance [37].

Fig. 5 A path connecting two boundary buses

Next, we introduce another approach to estimate the angle difference of line.

From (12), it can be observed that the line flow is actually determined by the angle difference of the line instead of actual values of phase angles. This provides a method to estimate the angle difference of a line using the associated bus voltage and line flow measurements.

The estimating principle of the angle difference of line i-j is explained as follows.

In the AC case, the real power flow of line i-j is:

$$p_{ij} = V_i^2 G_{ij} - V_i V_j \left[g_{ij} \cos\left(\theta_i - \theta_j\right) + b_{ij} \sin\left(\theta_i - \theta_j\right) \right] \tag{13}$$

where V_i is the voltage magnitude at bus i; g_{ij} and b_{ij} are the parameters of line i-j.

From (13), we have

$$g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij} = \frac{V_i^2 g_{ij} - p_{ij}}{V_i V_j} \tag{14}$$

Equivalently, (15) holds:

$$\sqrt{g_{ij}^2 + b_{ij}^2} \sin\left(\theta_{ij} + \omega\right) = \frac{V_i^2 g_{ij} - p_{ij}}{V_i V_j} \tag{15}$$

where

$$\omega = \arctan \frac{b_{ij}}{g_{ij}} \tag{16}$$

Combining (15) and (16), we obtain that

$$\theta_{ij} = \arcsin\left(\frac{V_i^2 g_{ij} - p_{ij}}{V_i V_j \sqrt{g_{ij}^2 + b_{ij}^2}} \right) - \omega + 2k\pi \quad k = \mp 0, 1, \ldots \tag{17}$$

Mathematically, there are multiple solutions for θ_{ij}. However, note that

$$-15^\circ \le \theta_{ij} \le 15^\circ \tag{18}$$

and

$$\left|\theta_{ij} + 2k\pi\right| > 2\pi \qquad k = \mp 1, 2, \ldots \tag{19}$$

This implies that (17) has a unique solution that satisfies constraint (18).

Once angle differences among boundary buses in the attacking region are determined, the attacker can choose one of these boundary buses as the reference bus and set its phase angle to be zero and determine the corresponding phase angles for the other buses without changing their angle differences.

5 Attack model based on blind identification

In this section, we will review the existing literatures that study local attack schemes using incomplete network information based on blind identification techniques.

Anwar et al. [38] showed that a stealthy attack vector can be constructed without any topology information and line parameters of a power grid. They demonstrated that the subspace transformation methods of the measurement matrix can be used to generate a hidden attack. However, such an attack scheme is only valid for the cases where measurement errors are identical to Gaussian noises. In the presence of gross errors, the injected false data will still trigger the alarm of the bad data detection procedure. To overcome this issue, a technique was developed to ensure the stealth of false data if the gross error exists.

The authors in [39] introduced a strategy to mask the sensitive information of a power grid when solving the multi-party AC optimal power flow problem in a public platform. In the attack model, the attacker has knowledge of the general AC optimal power model, but has no knowledge of the topology and parameters of the power grid. It was revealed that the topology information of a power grid may be identified if the rank information of the constraints is inferable.

The authors in [40] studied the principle of blind false data injection attacks using the principal component approximation method without knowing the Jacobian matrix and the distribution of state variables. The principal component analysis (PCA) is used to transform the measurement vector into a linear combination of several vectors with uncorrelated components. The simulation results demonstrated the stealth of the attack vector generated by the PCA matrix.

In [41], Chin et al. analyzed the blind attack scheme against the AC state estimation in a power system. The geometric approach was adopted to relax the strong assumption such that an attacker does not need to obtain the full topology and line parameter information. The criteria for successful AC blind and non-blind false data attacks (FDAs) are derived. Specifically, an attacker can modify the state of the targeted bus if the additional information of the original system states is known to this attacker.

6 Attack model based on data-driven approaches

In this section, we will review the existing literature that study local attack schemes using incomplete network information based on data driven techniques.

In [42], Xie et al. proposed a data driven approach to realize an undetectable false data injection attack with incomplete network information. The principle is to relax the system matrix used for constructing the injected false data. It was proved that such knowledge can be learned by a two-stage approach. In the first stage, a blind identification approach is employed to estimate the incomplete system matrix using a sequence of intercepted meter data. In the second stage, the estimated system matrix is used to construct the attack vector by a sparsity-exploiting method.

Chen et al. in [43] proposed a new strategy of false data injection attacks to disrupt the normal operation of a power system regulated by automatic voltage controls (AVC). Such an attack can be launched by an attacker who has little knowledge of the entire power grid. A partial observable Markov decision process is used to determine the optimal attack strategy. Moreover, a Q-learning algorithm with nearest sequence memory is used to realize the real-time data attack.

In [44], the authors proposed an alternative data-driven approach to construct stealthy attacks using only the subspace network information of the measurement signals without any requirement on the prior knowledge of the system states. However, such an attack scheme will fail if the measurement signals contain missing values. In this case, low-rank and sparse matrix approximation techniques are utilized to overcome this issue. By doing so, the injected false data is able to escape from the bad data detection.

Considering the difficulty of obtaining the information, Kim et al. in [45] proposed the subspace method to learn the system operating subspace from measurements. The feasibility conditions for an unobservable subspace attack are derived under both full and limited measurement assumptions. After the system subspace is estimated, two attack strategies are presented to ensure the impacts of such an attack to the operation of the system. The first one is to affect the system state directly by hiding the attack vector in the system subspace. The second strategy induces the operator to remove the normal data.

In [46], the authors further developed a data framing attack strategy which can impact the process of state estimation by an arbitrary level under the condition that only half of the critical measurements are acquired by the attackers. This type of stealthy attacks uses the subspace information of power systems measurements and exploits normal meter measurements as sources of malicious data. It is shown that the framing attack is able to misguide the operator to remove critical measurements from the framed meters, and the attacker can adjust the disturbance degree by carefully selecting a delicate attack magnitude.

7 Other local attack models

In Sects. 3–6, we will review local attack models that use limited network information of a power grid based on barrier conditions, blind identification and data driven approaches. Besides, there are several other local attack models.

The authors in [47] investigated the possibility of launching an undetectable false data injection attack without the prior knowledge of the power grid topology. The results show that the Jacobian matrix of a power grid can be approximately estimated by the linear independent component analysis when the system dynamics are small. Once the Jacobian matrix is estimated, the attacker can use it to design the injected false data that can pass the bad data detection procedure.

Tajer et al. in [48–50] investigated the attack strategy for an attacker who only has limited and imperfect information about the power grid. An optimal attack strategy was designed to ensure the economic profit of such an attack while taking into account the bounded errors of the knowledge of the power grid network information.

Bi et al. [51] introduced an optimal undetectable data attacks against the DC state estimation with partial topological knowledge. In particular, it was proved that such topological information is not required for constructing the undetectable false data if a power grid has a special structure, e. g., bridge structure. A Min-Cut method was proposed to minimize the required topological information.

Following the local attack scheme in [28], Deng et al. in [52] proposed an attack model against distribution system state estimation. Specifically, the authors discussed the strategy to avoid having the complete knowledge of the network topology and related parameters. Similarly, it is shown that an attacker can estimate system state only with the knowledge of power flow or power injection measurements. Moreover, it was also demonstrated that the states of buses in a local region can be obtained by accessing a small number of power flow or injection measurements.

8 Discussions on special cases

In this section, we will further discuss three special cases in which the required network information can be further reduced for constructing an undetectable attack vector.

8.1 Tree topology

In general, a power grid is a meshed network. However, it is observed that the number of loops in a power grid is much less than the number of buses. So, there exist a significant number of one-degree buses. For a tree network as shown in Fig. 6, we have

$$\boldsymbol{F} = \boldsymbol{X}^{-1}\boldsymbol{K}\boldsymbol{L}'\boldsymbol{\theta} = \boldsymbol{A}\boldsymbol{\theta} \tag{20}$$

where $\boldsymbol{X}$ is the reactance matrix; $\boldsymbol{KL}$ is the bus-line incidence matrix; $\boldsymbol{\theta}$ is the bus angle vector.

For a tree structured network, suppose there are n buses, then the number of lines is $n - 1$. It is easy to prove that

$$\text{rank}\ (\boldsymbol{A}) = n - 1 \tag{21}$$

Constraint (21) implies that for any power flow vector, KVL constraint in DC power flow equations can be ignored.

By doing so, we only need to obtain the topology information of a power grid for determining DC power flows, when the resistance of lines is not required. Accordingly, the attacking cost is reduced significantly.

8.2 Single loop

As shown in Fig. 7, the topology of a power network is a single loop which is defined as the loop in which we cannot find any internal loop.

Since the power grid does not hold a tree topology, the KVL constraint cannot be discarded. That is, an attacker needs to obtain the parameters of these lines to construct the undetectable false data.

The outage of a line can be simulated by injecting a pair of additional power vector. Accordingly, we further proposed a topology attack scheme in which an attacker injects false data into buses to change the real-time topology of a power grid sensed by the control center [19].

Considering the case where the attacker disconnects one line in the single loop, it becomes a tree power network. Differently, this topology modification is not achieved by a physical attack, but by a false data injection attack. That is, an attacker changes the breaker status of one line from 1 to 0 by injecting false measurements.

In practice, a large number of PMUs have been installed to detect the outage of a line. According to the principle of line outage detection, the goal of the attacking is to

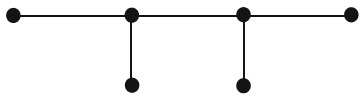

Fig. 6 Power sub-network with a tree topology

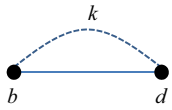

Fig. 7 A single loop

minimize the residual (22) by injecting false data into a set of measurements [20].

$$r_k = \min \left\| \Delta\boldsymbol{\theta}_{m,k} - \Delta\boldsymbol{\theta}'_{m,k} \right\|_2 \tag{22}$$

where $\Delta\boldsymbol{\theta}_{m,k}$ is observed phase angle change vector of PMU buses after line k is outaged; $\Delta\theta'_{m,k}$ is calculated phase angle change vector of PMU buses after line k is outaged with false data injection.

By doing so, the residual used to detect the outage line in the PMUs based detection method will be disrupted.

To sum up, in order to finish the false data attack without line parameters, the following conditions must be satisfied [20]:

1) The false data injected into the attacking region follows KCL and KVL;
2) The injected false data can simulate the outage of one line in this single loop;
3) The injected false data can minimize the residual value in (22) such that the PMU based line detection becomes invalid.

8.3 Single tie line

When the AC power flow model is adopted, as discussed in Sect. 4, an attacker needs to estimate the phase angle differences among boundary buses in the attacking region A. In this section, we further consider a special case where an attacking region is connected to the non-attacking region N through a single tie line.

In this case, one question needs to be reinvestigated: is there a need to estimate the angle difference?

As shown in Fig. 4, suppose that the actual phase angle at boundary b is α, if we revise its phase angle to β, then the error τ will be

$$\tau = \beta - \alpha \tag{23}$$

So, if we increase or decrease the phase angles at all buses in region N, that is

$$\begin{cases} \theta_b = \theta_b + \tau \\ \theta_d = \theta_d + \tau \end{cases} \tag{24}$$

Then, we have

$$\theta_b - \theta_d = \theta_b + \tau - \theta_d - \tau \tag{25}$$

We can see that the angle difference of tie line b-d will not be changed. Since the power flow of a line is dependent on the angle difference of a line, rather than the actual phase angles at the terminal buses. This indicates that we can randomly assign a value to the phase angle at the boundary bus in region A.

In fact, since a power grid is highly sparse network, the ratio of the number of lines to the number of buses is usually below 1.5. As a result, such cases are not common in practice. For example, a sub-network is connected to another sub-network through a HVDC tie line. In this case, the local attack scheme can be applied.

9 Future work

The required network information is crucial for the success of a false data injection attack. As an extension of the current work, we will discuss some of our future work in this section.

1) Attack mechanism against power dispatch without network parameters

We have reviewed several local attack mechanisms for launching false data injection attacks. However, in these models, the focus is to construct an undetectable attack vector based on incomplete network information. It remains to discuss sufficiently how to ensure these data can significantly impact the operation of power systems, e.g., $N-k$ contingency analysis [53], dispatch security [54]. This will be investigated in our future work.

Secondly, most models still require an attacker to obtain the network parameters of the attacking region. Considering the fact that the line parameters are more difficult to obtain, a future work is to investigate the attack strategy without any network parameter. For example, it is necessary to investigate the possibility that if an attacker can design an effective attack vector just based on the topology of a power grid to significantly disrupt the economic and secure operation of a power system.

2) Local attack mechanism against distribution systems with incomplete network information

A distribution system is characterized by lots of buses with few meters. On the other hand, the integration of renewable energies, such as wind power and PV, has significantly increased the uncertainty of the distribution system. This will pose a challenge to the accuracy of the load forecasting. Consequently, the state estimator has relative weak situational awareness to the operation of a distribution system. This gives an attacker a better chance to compromise the real-time data. Different from transmission networks, a distribution system usually has a tree topology. As discussed, for a tree structured power grid, there is no need to estimate the differences of phase angles

among boundary buses. Instead, they can be assigned with random values to construct the injected false data. Thus, it is of significance to study the local attack mechanism against distribution systems.

3) Effective detection methods

It is revealed that an attacker can launch an effective false data attack to pose severe consequences to a power system. Moreover, such an attack only requires an attacker to attack a small number of measurements with a few amount of topology and network information. So, it is necessary to develop some effective detection methods to defend against such attacks. The detection method should sufficiently considers the decision-making intelligence of an attacker. That is, the attack intelligence discussed in Sect. 2 might provide clues for developing some effective detection methods. On the other hand, increasing the complexity and unpredictability of state estimation could be an alternative countermeasure.

10 Conclusion

Today's power systems are subject to increasingly frequent cyber-attacks due to the integration of information technologies. The existing models for analyzing malicious behaviors of an attacker share one shortcoming that the full network information of a power grid must be available to the attacker. To address this issue, we perform a literature review on false data injection attacks using incomplete network information based on barrier conditions, blind identification and data driven approaches. We also discussed several special cases in which an attacker can launch an effective data attack without knowing line parameters. These studies provide a more practical model to analyze the attack behaviors and highlight the cyber risk of power systems, as an attacker is possible to launch a successful false data injection attack after obtaining a limited amount of network information.

Acknowledgments This work was supported by National Natural Science Foundation of China (No. 51777062), National key research and development program (No. 2018YFB0904200) the Fundamental Research Funds for the Central Universities, and Hunan science and technology project (No. 2017XK2014).

References

[1] Carreras BA, Lynch VE, Dobson I et al (2002) Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos Interdiscip J Nonlinear Sci 12(4):985–994
[2] U.S.-Canada Power System Outage Task Force (2004) Final report on the August 14, 2003 blackout in the United State and Canada: causes and recommendations. https://reports.energy.gov/. Accessed 1 January 2004
[3] Ma R, Chen HH, Huang YR et al (2013) Smart grid communication: its challenges and opportunities. IEEE Trans Smart Grid 4(1):36–46
[4] National Institute of Standards and Technology (2011) NISTIR 7628 revision 1: guidelines for smart grid cyber security. https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf. Accessed August 2010
[5] Abur A, Exposito A (2004) Power system state estimation: theory and implementation. CRC Press, Boca Raton. https://doi.org/10.1201/9780203913673
[6] Liu Y, Ning P, Reiter MK (2009) False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM conference on computer and communications security, Chicago, USA, 9–13 November 2009, pp 21–32
[7] Hug G, Giampapa JA (2012) Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 3(3):1362–1370
[8] Yuan Y, Li Z, Ren K (2011) Modeling load redistribution attacks in power systems. IEEE Trans Smart Grid 2(2):382–390
[9] Liu X, Li Z, Shuai Z et al (2017) Cyber attacks against the economic operation of power systems: a fast solution. IEEE Trans Smart Grid 8(2):1023–1025
[10] Liu X, Li Z (2017) Trilevel modeling of cyber attacks on transmission lines. IEEE Trans Smart Grid 8(2):720–729
[11] Che L, Liu X, Shuai Z et al (2018) Cyber cascades screening considering the impacts of false data injection attacks. IEEE Trans Power Syst. https://doi.org/10.1109/TPWRS.2018.2827060
[12] Che L, Liu X, Li Z (2018) Mitigating false data attacks induced overloads using a corrective dispatch scheme. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2018.2817515
[13] Xie L, Mo Y, Sinopoli B (2011) Integrity data attacks in power market operations. IEEE Trans Smart Grid 2(4):659–666
[14] Ye H, Ge Y, Liu X et al (2016) Transmission line rating attacks in two settlement markets. IEEE Trans Smart Grid 7(3):1346–1355
[15] Jia L, Kim J, Thomas RJ et al (2014) Impact of data quality on real-time locational marginal price. IEEE Trans Power Syst 29(2):627–636
[16] Mo Y, Kim THJ, Brancik K et al (2012) Cyber-physical security of a smart grid infrastructure. Proc IEEE 100(1):195–208
[17] Mo Y, Sinopoli B (2010) False data injection attacks in control systems. In: Proc. 1st workshop secure control syst., Stockholm, Sweden
[18] Kim J, Tong L (2013) On topology attack of a smart grid: undetectable attacks and countermeasures. IEEE J Sel Areas Commun 31(7):1294–1304
[19] Liu X, Li Z (2017) Local topology attacks in smart grids. IEEE Trans Smart Grid 8(6):2617–2626
[20] Liu X, Li Z (2016) Masking transmission line outage detection via false data attacks. IEEE Trans Inf Forensics Secur 11(7):1592–1602
[21] Jiang X, Zhang J, Harding B et al (2013) Spoofing GPS receiver clock offset of phasor measurement units. IEEE Trans Power Syst 28(3):3253–3262

[22] Zhang Z, Gong S, Dimitrovski A et al (2013) Time synchronization attack in smart grid: impact and analysis. IEEE Trans Smart Grid 4(1):87–98
[23] Liu X, Shahidehpour M, Li Z et al (2017) power system risk assessment in cyber attacks considering the role of protection systems. IEEE Trans Smart Grid 8(2):572–580
[24] Liu X, Shahidehpour M, Cao Y et al (2017) Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. IEEE Trans Smart Grid 8(3):1330–1339
[25] Huang T, Satchidanandan B, Kumar PR et al (2018) An online detection framework for cyber-attacks on automatic generation control. IEEE Trans Power Syst. https://doi.org/10.1109/TPWRS.2018.2829743
[26] Tan R, Nguyen HH, Foo EY et al (2017) Modeling and mitigating impact of false data injection attacks on automatic generation control. IEEE Trans Inf Forensics Secur 12(7):1609–1624
[27] Zimmerman RD, Murillo-Sánchez CE, Thomas RJ (2011) MATPOWER: steady-state operations, planning and analysis tools for power systems research and education. IEEE Trans Power Syst 26(1):12–19
[28] Liu X, Li Z (2014) Local load redistribution attacks in power systems with incomplete network information. IEEE Trans Smart Grid 5(4):1665–1676
[29] Xiang Y, Ding Z, Zhang Y et al (2017) Power system reliability evaluation considering load redistribution attacks. IEEE Trans Smart Grid 8(2):889–901
[30] Ding Z, Xiang Y, Wang L (2016) Quantifying the influence of local load redistribution attack on power supply adequacy. In: Proceedings of 2016 IEEE power and energy society general meeting (PESGM), Boston, USA, 17–21 July 2016, pp 1–5
[31] Li Z, Shahidehpour M, Alabdulwahab A et al (2018) Analyzing locally coordinated cyber-physical attacks for undetectable line outages. IEEE Trans Smart Grid 9(1):35–47
[32] Sun Y, Li WT, Song W et al (2015) False data injection attacks with local topology information against linear state estimation. In: Proceedings of 2015 IEEE innovative smart grid technologies—Asia (ISGT ASIA), Bangkok, Thailand, 3–6 November 2015, pp 1–5
[33] Ly K, Kwiat K, Kamhoua C et al (2017) Approximate power grid protection against false data injection attacks. In: Proceedings of 2017 IEEE 15th intl conf on dependable, autonomic and secure computing, 15th intl conf on pervasive intelligence and computing, 3rd intl conf on big data intelligence and computing and cyber science and technology congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, USA, 6–10 November 2017, pp 527–533
[34] Zhang J, Chu Z, Sankar L et al (2018) Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? IEEE Trans Power Syst. https://doi.org/10.1109/TPWRS.2018.2818746
[35] Zhang J, Chu ZG, Sankar L et al (2016) False data injection attacks on power system state estimation with limited information. In: Proceedings of 2016 IEEE power and energy society general meeting (PESGM), Boston, USA, 17–21 July 2016, pp 1–5
[36] Liu X, Bao Z, Lu D et al (2015) Modeling of local false data injection attacks with reduced network information. IEEE Trans Smart Grid 6(4):1686–1696
[37] Liu X, Li Z (2017) False data attacks against AC state estimation with incomplete network information. IEEE Trans Smart Grid 8(5):2239–2248
[38] Anwar A, Mahmood AN (2016) Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors. In: Proceedings of 2016 IEEE power and energy society general meeting (PESGM), Boston, USA, 17–21 July 2016, pp 1–5
[39] Wu D, Lesieutre BC, Ramanathan P et al (2016) Preserving privacy of AC optimal power flow models in multi-party electric grids. IEEE Trans Smart Grid 7(4):2050–2060
[40] Yu ZH, Chin WL (2016) Blind false data injection attack using PCA approximation method in smart grid. IEEE Trans Smart Grid 6(3):1219–1226
[41] Chin WL, Lee CH, Jiang T (2017) Blind false data attacks against AC state estimation based on geometric approach in smart grid communications. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2017.2708114
[42] Xie S, Yang J, Xie K et al (2017) Low-sparsity unobservable attacks against smart grid: attack exposure analysis and a data-driven attack scheme. IEEE Access 5:8183–8193
[43] Chen Y, Huang S, Liu F et al (2018) Evaluation of reinforcement learning based false data injection attack to automatic voltage control. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2018.2790704
[44] Anwar A, Mahmood AN, Pickering M (2016) Data-driven stealthy injection attacks on smart grid with incomplete measurements. In: Intelligence and security informatics. Springer International Publishing, pp 180–192
[45] Kim J, Tong L, Thomas RJ (2015) Subspace methods for data attack on state estimation: a data driven approach. IEEE Trans Signal Process 63(5):1102–1114
[46] Kim J, Tong L, Thomas RJ (2013) Data framing attack on state estimation with unknown network parameters. In: Proceedings of 2013 Asilomar conference on signals, systems and computers, Pacific Grove, USA, 3–6 November 2013, pp 1388–1392
[47] Esmalifalak M, Nguyen H, Zheng R et al (2011) Stealth false data injection using independent component analysis in smart grid. In: Proceedings of 2011 IEEE international conference on smart grid communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011, pp 244–248
[48] Mengis M, Tajer A (2017) Data injection attacks on electricity markets by limited adversaries: worst-case robustness. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2017.2695120
[49] Tajer A (2017) False data injection attacks in electricity markets by limited adversaries: stochastic robustness. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2017.2733346
[50] Xue M, Tajer A (2016) Robust false data injection attacks in electricity markets by limited adversaries. In: Proceedings of 2016 50th Asilomar conference on signals, systems and computers, Pacific Grove, USA, 6–9 November 2016, pp 1370–1374
[51] Bi S, Zhang YJ (2014) Using covert topological information for defense against malicious attacks on DC state estimation. IEEE J Sel Areas Commun 32(7):1471–1485
[52] Deng R, Zhuang P, Liang H (2018) False data injection attacks against state estimation in power distribution systems. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2018.2813280
[53] Che L, Liu X, Li Z (2017) A mixed integer programming model for evaluating hidden probabilities of $N-k$ line contingencies in smart grids. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2017.2758389
[54] Che L, Liu X, Li Z (2018) An intra-interval security risk regarding regulation burden due to wind variation in high-wind-penetrated power systems. IEEE Trans Power Syst 33(3):3213–3216

Yufei SONG received the B.S. degree from Taiyuan University of Technology, China, in 2017. He is working towards his Ph.D. degree in the College of Electrical and Information Engineering at Hunan University, China. His research interest is smart grid cyber security.

Xuan LIU received the B.S. and M.S degrees from Sichuan University, China, in 2008 and 2011, and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, in 2015, all in electrical engineering. He is currently a Professor in the College of Electrical and Information Engineering at Hunan University, China. His research interests include smart grid security, operation and economics of power systems.

Zhiyi LI received the B.S. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2011, and the M.S. degree from Zhejiang University, Hangzhou, China, in 2014, and Ph.D. degree from Illinois Institute of Technology, USA, in 2017. He is a postdoc researcher at the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA. His current research interests include cyber-physical power system and power system optimization.

Mohammad SHAHIDEHPOUR received the Honorary Doctorate degree in electrical engineering from the Polytechnic University of Bucharest, Bucharest, Romania. Professor Shahidehpour is the Bodine Chair Professor and the Director of the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA, and a Research Professor with King Abdulaziz University, Jeddah, Saudi Arabia. He is an IEEE Fellow, a member of the U.S. National Academy of Engineering. His current research interests include power system operation and planning, microgrids and energy hubs, sustainable energy integration.

Zuyi LI received the B.S. and M.S. degrees from Shanghai Jiao Tong University, Shanghai, China, in 1995 and 1998, respectively, and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, in 2002, all in electrical engineering. Presently, he is a Professor in the Electrical and Computer Engineering Department at IIT. His research interests include economic and secure operation of electric power systems, cyber security in smart grid, renewable energy integration, electric demand management of data centers, and power system protection.