Hindawi
Complexity
Volume 2018, Article ID 8503825, 16 pages
https://doi.org/10.1155/2018/8503825

WILEY | Hindawi

Research Article

A Novel Sparse False Data Injection Attack Method in Smart Grids with Incomplete Power Network Information

Huixin Zhong,[1] **Dajun Du**,[1] **Chuanjiang Li**,[2] **and Xue Li**[1]

[1]*School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China*
[2]*School of Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai, China*

Correspondence should be addressed to Chuanjiang Li; licj@shnu.edu.cn and Xue Li; lixue@i.shu.edu.cn

Received 8 June 2018; Revised 5 September 2018; Accepted 16 September 2018; Published 1 November 2018

Guest Editor: Liang Hu

The paper investigates a novel sparse false data injection attack method in a smart grid (SG) with incomplete power network information. Most existing methods usually require the known complete power network information of SG. The main objective of this paper is to propose an effective sparse false data injection attack strategy under a more practical situation where attackers can only have incomplete power network information and limited attack resources to access the measurements. Firstly, according to the obtained measurements and power network information, some incomplete power network information is compensated by using the power flow equation approach. Then, the fault tolerance range of bad data detection (BDD) for the attack residual increment is estimated by calculating the detection threshold of the residual L2-norm test. Finally, an effective sparse imperfect strategy is proposed by converting the choice of measurements into a subset selection problem, which is solved by the locally regularized fast recursive (LRFR) algorithm to effectively improve the sparsity of attack vectors. Simulation results on an IEEE 30-bus system and a real distribution network system confirm the feasibility and effectiveness of the proposed new attack construction method.

1. Introduction

The traditional power systems operate in an isolated physical environment, where their security mainly focuses on the random failures of the system components [1]. With the deep integration of electricity infrastructure and modern information and communication technology, a smart grid (SG) uses two-way flows of electricity and information to create a widely distributed automated energy delivery network [2–10], leading to the great improvement of the comprehensive level of automation and management. However, SG has been found vulnerable to cyberattacks as a large number of smart devices are deployed over unencrypted cyber communication environments [11–15]. Malicious cyberattacks are one type of the most popular cyberattacks, which may trigger the catastrophic damage to power supplies and widespread power outages [16, 17]. For example, during the Christmas of 2015, a synchronized and coordinated cyberattack compromised three Ukrainian regional electric power distribution companies, resulting in power outages and further affecting approximately 225,000 customers for several hours [18]. Moreover, the US PJM system received 4090 cyberattacks in one month in 2015, which was equivalent to 5.5 times per hour [19]. Moreover, the Israeli power supply system was hit by a major cyberattack in 2016, forcing a large number of computers in the power supply system to run offline [20]. Therefore, cyber security of SG is an important and open problem, which has attracted great interests from the government, industry, and academia. Cyber security can be studied from two perspectives to improve the system reliability. The remote state estimation was investigated from the perspective of defense [21] under possible false data injection attacks, where the whole knowledge of the system model must be known. However, this paper is aimed at finding the vulnerability of the power system with incomplete power grid information by developing an effective sparse false data injection attack strategy from the attackers' perspective.

State estimation is usually employed to estimate or predict the system operational states, which provides real-time information and effective supervision of SG. The traditional

state estimation based on the least squares (LS) method and the fast decoupling method derived from the LS has been applied for many years [22]. As the scale of the power system continues to increase, the dispatch center puts higher and higher requirements on the accuracy and stability of state estimation. Some power grids use a weighted least squares method based on a fixed Jacobian matrix and introduce orthogonalization [23]. This state estimation method has better numerical stability and faster calculation speed. Others use a two-level distributed state estimation method [24], which makes full use of a large amount of redundant measurement information in the substation: the first step is to perform high-precision local estimation and the second one is to perform global coordination, so that a more reliable real-time state estimation result of the whole network can be obtained. Moreover, the distributed state estimation has also been employed for a large-scale power system to support the system operation [25].

False data injection attacks (FDIAs), as one typical type of malicious cyberattacks, can purposely manipulate measurements to perturb the results of state estimation without posing any anomalies to the bad data detection (BDD) while producing a serious threat or damage to SG operations [26, 27]. A common assumption on FDIAs in most works is that the attacker must obtain complete knowledge of the power network information [8, 26–28], i.e., topology information and transmission line parameters of the power grid. However, a practical attacking situation needs to be usually considered from two aspects: (1) it is difficult for an attacker to know all power network information of a power grid due to the strict protection of the control center and the lack of knowledge of real-time grid parameters such as the position of circuit breaker switches and transformer tap changers and (2) the attacker may access only a part of smart meters due to the limited attack resources and the physical protection of some important smart instruments.

For the first case, an attacker cannot gain the complete network information; i.e., the Jacobian matrix $\mathbf{H}$ is an incomplete matrix, but it is critical for the construction of a perfect FDIA strategy [26]. To overcome the strong requirement of knowing the full topology and parameter information of a power grid, the first attempt is made successfully to design false data injection attacks with incomplete power information [29]. Here, the limited parameter information obtained by the attacker is expressed as $\bar{\mathbf{H}} = \mathbf{H} + \boldsymbol{\delta}$, where $\boldsymbol{\delta}$ represents the difference between the complete parameter information $\mathbf{H}$ and the obtained partial parameter information $\bar{\mathbf{H}}$. Then, two cases of perfect attacks and imperfect attacks are studied, and the residual increments caused by perfect attacks and imperfect attacks are zero and nonzero, respectively. Furthermore, the range of residual increments caused by the undetectable imperfect FDIAs is given as $0 \le \tau_a \le \|\mathbf{a}\|_2 \cdot \cos\gamma$ in [30], where τ_a denotes the residual increments caused by the attacks and γ represents the angle between the null space of the real Jacobian transpose matrix $\mathbf{H}^T$ and the image space of the inaccurate Jacobian matrix $\bar{\mathbf{H}}$. The attackers only need to obtain the power network information of the local attacking region to inject false data into smart meters in the local region of the power grid without being detected [31], and a strategy is designed to determine the optimal attacking region of a single load bus by obtaining less power network information [32]. The phenomenon of intermittent faults is described by Bernoulli distribution in [33], as the intermittent faults in the nonuniformly sampled multirate systems occur randomly. However, the incomplete power network information in this paper is the incomplete power information of the system parameter; i.e., the parameter information of the whole power network is known well. The above works do not consider the compensation for the incomplete information in the measurement Jacobian matrix to reduce the estimation error of the predesigned false data to be injected into certain measurements. Furthermore, the fault tolerance range of the BDD unit for the residual increment caused by an imperfect false data is not analyzed in detail, which cannot ensure the high success rate for an attack to avoid the BDD.

For the second case, the attackers always tend to compromise as fewer measurements as possible to implement successful attacks, namely, constructing sparse attack vectors. It has stimulated several research works [34–37]. These sparse attack models still require the full-power network information. Moreover, to the best of our knowledge, there is no feasible algorithm that can efficiently construct highly sparse undetectable attack vectors with incomplete power network information.

It seems to be much more difficult to launch an undetectable sparse attack when considering both aspects of the practical attacking situation. However, to improve the robustness of SG, it is very necessary to find the system vulnerability by developing a new and practical FDIA strategy. However, the following challenges and difficulties need to be addressed:

(1) The first challenging problem is how to compensate unknown power information in the measurement Jacobian matrix and distinguish the secure measurement set and the attackable measurement set after the compensation

(2) How to estimate the fault tolerance range of the BDD unit for the attack residual increment is another difficult problem

(3) The third difficult problem is how to design and solve a sparse imperfect attack model to obtain an effective sparse imperfect strategy

To address these difficulties, this paper investigates a novel sparse imperfect FDIA construction method by modifying only a much smaller number of measurements. The main contributions of the paper include: (1) according to the obtained measurements and power network information, some unknown information in the measurement Jacobian matrix is compensated by solving the power flow equation, and the secure measurement set and the attackable measurement set are constructed by determining whether the attackers can inject false data. (2) To ensure that the attack can bypass the BDD with a high success rate, the fault tolerance range of the BDD unit for the attack residual increment is estimated by calculating the detection threshold of the

residual L2-norm test based on the largest normalized residual (LNR) test. (3) Based on the attackable measurement set, an effective sparse imperfect strategy is proposed by regarding the choice of measurements as a subset selection problem of a linear regression model with noise. This can then be solved by the locally regularized fast recursive (LRFR) algorithm, which can effectively improve the sparsity of the attack vector.

The rest of the paper is organized as follows. Section 2 describes the problem formulation of the sparse imperfect attack strategy. In Section 3, the LRFR algorithm is used for the smallest subset selection of attack vector elements. Simulation results are provided in Section 4, followed by concluding remarks in Section 5.

2. Problem Formulation

Considering the practical attacking situation, the schematic block diagram of a power network control system under FDIAs is shown in Figure 1. The attacker can only inject false data into certain measurements. That is, the system contains an attackable measurement set z^F and a secure measurement set z^S, which will be defined in detail in the later section. Then, the contaminated measurements $z_a = \{z^S, z_a^F\}$ are transmitted to the state estimator for the identification of state variables. Furthermore, the bad data detector is used to identify and detect anomaly data based on the results of state estimation. If the attack cannot be detected by the BDD, the misleading state estimate results will be transmitted to the control system, which may pose seriously potential threats to system security and economic operation. Therefore, for SG with unknown power information, how to design a new sparse imperfect attack strategy is the following work. It will lay the foundation for finding system vulnerabilities and designing the corresponding protection strategies.

2.1. State Estimation in a DC System Model. We focus on a steady-state and lossless power transmission system with a set $N = \{0, 1, 2, \dots, n\}$ of buses and a set $L = \{1, 2, \dots, l\}$ of transmission lines. Each bus $i \in N$ corresponds to an active power injection p_i (generator active power minus load) and a bus phase angle θ_i. Each branch $k = \{i, j\} \in L$ connects two buses and corresponds to an active power flow f_{ij}. Then, the branch active power flow is defined as positive if it is in the direction of the branch; otherwise, it is negative if it is in the opposite direction. Therefore, $f_{ji} = -f_{ij}$ for $\forall\{i, j\} \in L$ [38]. To describe the network topology and transmission line parameters of the electricity grid better, let $\mathbf{A} \in \{-1, 0, 1\}_{l\times n}$ denote the branch-bus connection matrix; i.e.,

$$A_{ki} = \begin{cases} 0, & \text{if the branch } k \text{ is not connected to bus } i, \\ 1, & \text{if the direction of branch } k \text{ begins from bus } i, \\ -1, & \text{if the direction of branch } k \text{ ends towards bus } i. \end{cases} \tag{1}$$

Then, let the diagonal matrix $\mathbf{D} \in \mathbb{R}^{l\times l}$ describe the physical properties of the transmission lines, and the k^{th} diagonal element of $\mathbf{D}$ (i.e., D_k) is the negative admittance of branch $k = \{i, j\}$, i.e., $D_k = -b_{ij}$. Therefore, the power network information matrix $\mathbf{H}$ is constructed as

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}^T\mathbf{D}\mathbf{A} \\ \mathbf{D}\mathbf{A} \\ -\mathbf{D}\mathbf{A} \end{bmatrix}_{m\times n}. \tag{2}$$

According to the DC power flow model, the relationship between measurements $\mathbf{z}$ and state variables $\mathbf{x}$ can be expressed as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{v}, \tag{3}$$

where $\mathbf{z} \in \mathbb{R}^{m\times 1}$ is the measurement vector consisting of branch active power flow measurements and bus active power injection measurements, m is the total number of measurements, $\mathbf{x} \in \mathbb{R}^{n\times 1}$ is the state vector of bus phase angles except for the reference angle fixed as $\theta_o = 0$, $n + 1$ is the total number of buses, and $\mathbf{v} \sim N(\mathbf{0}, \mathbf{R})$ is the Gaussian measurement noise vector with a diagonal covariance matrix $\mathbf{R} = \text{diag}\{\sigma_1^2, \sigma_2^2, \dots, \sigma_m^2\}$ [39].

Real-time state information is important to provide operation supports such as ensuring system stability. However, we consider that the power system is static and the measurement equation is linear. For the system, the weighted least square (WLS) method [39] is used for state estimation because it is able to handle regression situations in which data points are of varying quality. The state of system $\mathbf{x}$, which is estimated by the WLS method, follows

$$\hat{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z}. \tag{4}$$

Remark 1. A recursive filter algorithm to deal with dynamic state estimation problem for power systems with quantized nonlinear measurements is proposed in [40], which is for dynamic nonlinear systems. However, the main objective of this paper is to design an effective sparse attack strategy so that the attackers can compromise as fewer measurements as possible to destroy the measurement information accuracy. This paper considers that the power system is static and the measurement equation is linear, where the weighted least square (WLS) method is employed to estimate the system state. Thus, an attack regression model can be obtained and the choice of measurements can be treated as a subset selection problem, which can be solved by the locally regularized fast recursive (LRFR) algorithm to effectively improve the sparsity of attack vectors.

Further, the measurement estimates can be obtained as

$$\hat{\mathbf{z}} = \mathbf{H}\hat{\mathbf{x}} = \mathbf{H}\left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z}. \tag{5}$$

When the system is attacked, false data in measurements may mislead the results of state estimation. Traditional BDD methods identify and detect bad data by testing

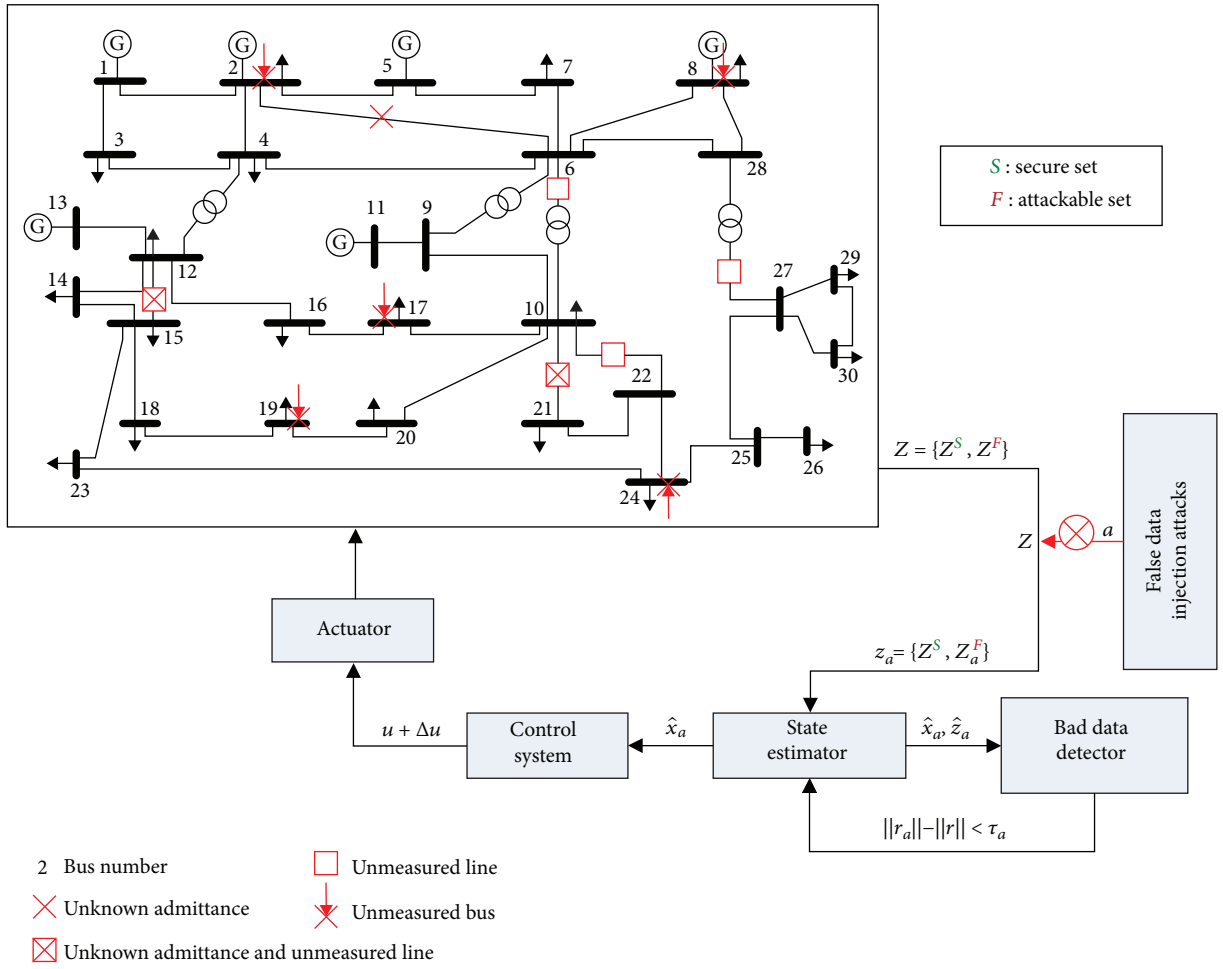

Figure 1: Power network control system under false data injection attacks.

the measurement residual, which is denoted as the difference between the observed measurements $\mathbf{z}$ and the estimated measurements $\hat{\mathbf{z}}$, i.e., $\mathbf{r} \triangleq \mathbf{z} - \hat{\mathbf{z}} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$. Generally, if the L2-norm of the residual vector $\mathbf{r}$ exceeds a certain threshold (i.e., $\|\mathbf{r}\|_2 > \tau$), bad data may exist in the measurements $\mathbf{z}$.

Remark 2. The selection of threshold τ is a key issue for BDD based on residual L2-norm, which can be determined according to the LNR test [39]. The process is as follows:

The normalized residuals [41] are defined as

$$r_{N,i} = \frac{r_i}{\sqrt{\sum_{ii}}}, \quad i = 1, \ldots, m, \tag{6}$$

where $\sum_{ii}$ is the i^{th} diagonal element of $\boldsymbol{\Sigma}$ and $\boldsymbol{\Sigma} = \text{diag}[\mathbf{WR}]$, $\mathbf{W} = \mathbf{I} - \mathbf{H}(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}$, is called the sensitivity matrix. Referring to the literature [39], the normalized residual threshold τ_N can be chosen, where the normalized residual generally follows the standard normal distribution, i.e., $r_{N,i} \sim N(0,1)$, and τ_N is determined by looking up the standard normal distribution table. For example, if the probability of false detection is set as $P_e = 0.005$, i.e., $P\{|r_{N,i}| < \tau_N\} = 1 - 0.005$, the range of the normalized residuals is expressed as

$$\left| r_{N,i} = \frac{r_i}{\sqrt{\sum_{ii}}} \right| < \tau_N = 2.81, \quad i = 1, \ldots, m. \tag{7}$$

Then, the range of normal residuals can be obtained as $|r_i| < 2.81\sqrt{\sum_{ii}}$, $i = 1, \ldots, m$, and the threshold τ of the residual L2-norm test is further solved as

$$\|\mathbf{r}\|_2 = \sqrt{r_1^2 + \cdots + r_m^2} < \sqrt{2.81^2(\Sigma_{11} + \cdots + \Sigma_{mm})} = \tau. \tag{8}$$

With the wide application of the communication technology in SG, the attackers can access the SCADA system through a communication network. If the attackers can obtain the full network information of the power grid and enough measurements, they can then inject purposely the predesigned false data into some measurements without posing any anomalies to the traditional BDD based on the residual L2-norm test, which will inevitably bring serious security threats to SG.

2.2. Undetectable Attacks with Complete Power Network Information. Generally, the attackers intrude into the power system by compromising the readings of certain smart devices intentionally. That is, the original measurements $\mathbf{z}$ are manipulated by the false data $\mathbf{a}$, i.e., $\mathbf{z_a} = \mathbf{z} + \mathbf{a}$. The state estimation deviation caused by the attack is denoted as $\hat{\mathbf{x}}_\mathbf{a} = \hat{\mathbf{x}} + \mathbf{c}$, where $\mathbf{c} \in \mathbb{R}^{n\times 1}$ is the arbitrary error vector injected into state estimation. Thus, the attack residual L2-norm can be expressed as

$$\begin{aligned}\|\mathbf{r_a}\| &= \|\mathbf{z_a} - \mathbf{H}\hat{\mathbf{x}}_\mathbf{a}\| = \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c})\| = \|(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}) \\ &\quad + (\mathbf{a} - \mathbf{Hc})\| \le \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| + \|\mathbf{a} - \mathbf{Hc}\| = \|\mathbf{r}\| + \Delta_a < \tau,\end{aligned} \tag{9}$$

where $\Delta_a = \|\mathbf{a} - \mathbf{Hc}\|$ is defined as the attack residual increment. There are two cases for an attack to bypass the BDD. In the first case, the attack vector is carefully constructed to satisfy $\mathbf{a} = \mathbf{Hc}$, namely, $\Delta_a = 0$. Then, the attack will not be detected by the traditional BDD because the injected false data no longer affect the original residual L2-norm, i.e., $\|\mathbf{r_a}\| = \|\mathbf{r}\|$. Such attacks are thus called perfect FDIAs. In the second case, there is $\mathbf{a} \neq \mathbf{Hc}$, namely, $\Delta_a \neq 0$, but the condition $\Delta_a < \tau - \|\mathbf{r}\| \triangleq \tau_a$ must be met. Such attacks can also successfully bypass the traditional BDD, which are called imperfect FDIAs.

Remark 3. For the first case, the perfect FDIAs depend on a strong assumption that the attackers have complete knowledge about the network information of the power grid and are capable of accessing all measurements. However, it is more practical for the attackers to obtain incomplete power network information and limited measurements, which makes the attackers unable to launch perfect FDIAs successfully in the practical attack situation. Therefore, how to design a new attack strategy with limited network information and attack resources is an interesting and open problem.

Remark 4. For the second case, the threshold τ_a represents the fault tolerance ability of the BDD, which is related to the measurement noises contained in the original measurements $\mathbf{z}$. If the measurement noises are smaller, the original residual L2-norm $\|\mathbf{r}\|$ is smaller and then the threshold τ_a is larger; otherwise, if the measurement noises are larger, the original residual L2-norm $\|\mathbf{r}\|$ is larger and then the threshold τ_a is smaller. When the measurement noises are given, the fault tolerance ability of the BDD τ_a is determined. Therefore, if the attack residual increment is set within the range of τ_a, the attack can bypass the BDD with a high success rate.

Remark 5. Recent researches have shown that an undetectable false data injection attack can still be accomplished even with the incomplete power network information. However, there is shorting of the more practical FDIA strategies with both incomplete power network information and limited attack resources considered.

2.3. Sparse Imperfect FDIA Strategy with Incomplete Power Network Information and Measurements. It is analyzed above that the attackers cannot have complete power network information and measurements due to the practical issues. However, we find that some unknown information, i.e., transmission line admittances D_k, can be calculated according to the obtained measurements and power network information. Thus, more information about the measurement Jacobian matrix $\mathbf{H}$ can be known indirectly. In terms of the unknown D_k, we have the following theorem.

Theorem 1. *When the phase angle difference $\theta_i - \theta_j$ between the two buses of the branch $k = \{i, j\}$ can be calculated indirectly and the branch power flow f_{ij} is known, the unknown element $D_{kk} = -b_{ij}$ in the branch admittance matrix $\mathbf{D}$ can be calculated by using the branch active power flow equation $f_{ij} = -b_{ij}(\theta_i - \theta_j)$.*

Proof 1. Firstly, a generator bus needs to be selected as the reference bus o, and the adversary needs partial knowledge of the network topology to find the paths from bus o to bus i and bus j separately (at least one path can be found according to the network topology connectivity). Assuming that the path $(o \to i)$ passes through a sequence of intermediate buses $\{o_1, o_2, \ldots, o_q\}$, the attacker needs to know the branch admittances $\{b_{oo_1}, b_{o_1o_2}, \ldots, b_{o_qi}\}$ and the branch power flows $\{f_{oo_1}, f_{o_1o_2}, \ldots, f_{o_qi}\}$. Then, the phase angle θ_i can be calculated as

$$\begin{aligned}\theta_i &= \theta_i - \theta_o = \left(\theta_i - \theta_{o_q}\right) + \cdots + \left(\theta_{o_1} - \theta_o\right) \\ &= -\frac{f_{io_q}}{b_{io_q}} - \cdots - \frac{f_{o_1o}}{b_{o_1o}}.\end{aligned} \tag{10}$$

Next, the phase angle θ_j can be calculated in a similar way, and the adversary needs to further know the branch power flow f_{ij}. Then, the unknown element D_k in the branch admittance matrix $\mathbf{D}$ can be obtained finally by $D_k = -b_{ij} = f_{ij}/(\theta_i - \theta_j)$. Therefore, the proof is completed.

Remark 6. According to Theorem 1, some unknown information in $\mathbf{H}$ can be mathematically compensated. But there is still some unknown power information that cannot be compensated. Thus, according to the sufficient condition $\mathbf{a} = \mathbf{Hc}$ for constructing false data inject attacks, namely, $a_i = \sum_{j=1}^{n} h_{ij}c_j$, when the i^{th} row of the Jacobian matrix $\mathbf{H}$ contains unknown elements due to the incomplete power network information after the compensation, set $a_i = 0$. Meanwhile, when the measurement z_i cannot be obtained, set $a_i = 0$ similarly. Thus, we can divide all the measurements into the secure set S (or $\mathbf{z}^S$) and the attackable set F (or $\mathbf{z}^F$), where $a_i = 0$, $\forall i \in S$.

Assume that the number of elements in the set F is M; i.e., an attacker can tamper with M smart devices at most.

Thus, an attack vector $\mathbf{a}$ with at most M nonzero elements can be expressed as

$$\mathbf{a} = \left(\dots, a_{i_1}, 0, \dots, 0, a_{i_2}, 0, \dots, 0, a_{i_M}, \dots \right)^T. \tag{11}$$

By removing the zero elements from $\mathbf{a}$, it gets $\bar{\mathbf{a}} = (a_{i_1}, a_{i_2}, \dots, a_{i_M})^T$ with M elements. Then, we have

$$\Delta_a = \|\mathbf{a} - \mathbf{H}\mathbf{c}\| = \left\| \begin{bmatrix} \mathbf{a}^S \\ \bar{\mathbf{a}} \end{bmatrix} - \begin{bmatrix} \mathbf{H}^S \\ \bar{\mathbf{H}} \end{bmatrix} \mathbf{c} \right\| = \left\| \begin{bmatrix} \mathbf{a}^S - \mathbf{H}^S\mathbf{c} \\ \bar{\mathbf{a}} - \bar{\mathbf{H}}\mathbf{c} \end{bmatrix} \right\|, \tag{12}$$

where $a_i^S = 0,\ \forall i \in S$.

Remark 7. The reason that the Jacobian matrix $\mathbf{H}$ can be divided into two parts $\mathbf{H}^S$ and $\bar{\mathbf{H}}$ is as follows. After the compensation for some unknown information in $\mathbf{H}$, if the i^{th} row of the Jacobian matrix $\mathbf{H}$ contains unknown elements, set $a_i = 0$. Meanwhile, if the measurement z_i cannot be obtained, set $a_i = 0$ similarly. Thus, we can divide all the measurements into the secure set S and the attack set F, where $a_i = 0,\ \forall i \in S$. Then, the attack vector $\mathbf{a}$ can be divided into the secure section $\mathbf{a}^S$ and the attack section $\bar{\mathbf{a}}$. Correspondingly, the Jacobian matrix $\mathbf{H}$ can be divided into two parts $\mathbf{H}^S$ and $\bar{\mathbf{H}}$ by the row.

Suppose that there exists a vector $\mathbf{c}$ satisfying $\mathbf{H}^S\mathbf{c} = \mathbf{0} = \mathbf{a}^S$, but there is no guarantee that $\bar{\mathbf{a}} = \bar{\mathbf{H}}\mathbf{c}$ will be met. According to (12), we thus have

$$\Delta_a = \left\| \begin{bmatrix} \mathbf{a}^S - \mathbf{H}^S\mathbf{c} = \mathbf{0} \\ \bar{\mathbf{a}} - \bar{\mathbf{H}}\mathbf{c} \neq \mathbf{0} \end{bmatrix} \right\| = \left\| \bar{\mathbf{a}} - \bar{\mathbf{H}}\mathbf{c} \right\| \neq \mathbf{0}, \tag{13}$$

where $\bar{\mathbf{H}} = [\mathbf{h}_{i_1}^T, \mathbf{h}_{i_2}^T, \dots, \mathbf{h}_{i_M}^T]^T$ is known completely by the attacker and $\mathbf{h}_{i_j} = [h_{i_j,1}, h_{i_j,2}, \dots, h_{i_j,n}] (1 \le j \le M)$ is the i_j^{th} row of the matrix $\mathbf{H}$. According to (13), the construction of an imperfect attack needs to be considered. Therefore, considering the attackable set F, we formulate the imperfect attack subvector as

$$\bar{\mathbf{a}} = \bar{\mathbf{H}}\mathbf{c} + \boldsymbol{\varepsilon}, \tag{14}$$

where $\boldsymbol{\varepsilon}$ is defined as an attack deviation vector. According to the BDD detection mechanism, if $\|\boldsymbol{\varepsilon}\|_2 = \Delta_a < \tau_a$ is satisfied, the attack can bypass the BDD well.

Remark 8. Calculating the test threshold τ and the fault tolerance range of the BDD τ_a requires the complete Jacobian matrix $\mathbf{H}$ and all the measurements $\mathbf{z}$, which cannot be obtained completely by the attackers in the practical situation. Thus, we take the obtained measurements and parameter information to calculate the approximation thresholds $\bar{\tau}$ and $\bar{\tau}_a$. We can have $\bar{\mathbf{W}} = \mathbf{I} - \bar{\mathbf{H}}(\bar{\mathbf{H}}^T\bar{\mathbf{R}}^{-1}\bar{\mathbf{H}})^{-1}\bar{\mathbf{H}}^T\bar{\mathbf{R}}^{-1}$ by using $\bar{\mathbf{H}}$ and $\bar{\mathbf{R}}$ and calculate $\bar{\tau}$ by (8). Furthermore, due to $\|\bar{\mathbf{r}}\| = \|\mathbf{z}^F - \bar{\mathbf{H}}\hat{\bar{\mathbf{x}}}\|$, the approximation fault tolerance range of the BDD $\bar{\tau}_a = \bar{\tau} - \|\bar{\mathbf{r}}\|_2$ is then calculated by (9). If $\|\boldsymbol{\varepsilon}\|_2 < \bar{\tau}_a$ is satisfied, the attack can bypass the BDD well.

For the convenience of subsequent calculation, define the attack vector as $\bar{\mathbf{a}} = (a_1, a_2, \dots, a_M)^T$. The state error vector $\mathbf{c}$ is unknown, so the attack vector $\bar{\mathbf{a}}$ cannot be calculated directly. However, the attackers can find an attack vector $\bar{\mathbf{a}}$ as follows. Let $\boldsymbol{\Psi} = \bar{\mathbf{H}}(\bar{\mathbf{H}}^T\bar{\mathbf{H}})^{-1}\bar{\mathbf{H}}^T$ and $\mathbf{B} = \boldsymbol{\Psi} - \mathbf{I}$. It is easy to see that $\boldsymbol{\Psi}\bar{\mathbf{H}} = \bar{\mathbf{H}}$ [28]. The attackers can simply multiply $\boldsymbol{\Psi}$ to both left sides of the relation $\bar{\mathbf{a}} = \bar{\mathbf{H}}\mathbf{c} + \boldsymbol{\varepsilon}$ to obtain a sequence of equivalent equations as

$$\begin{aligned} \bar{\mathbf{a}} = \bar{\mathbf{H}}\mathbf{c} + \boldsymbol{\varepsilon} &\Leftrightarrow \boldsymbol{\Psi}\bar{\mathbf{a}} = \boldsymbol{\Psi}\bar{\mathbf{H}}\mathbf{c} + \boldsymbol{\Psi}\boldsymbol{\varepsilon} = \bar{\mathbf{H}}\mathbf{c} + \boldsymbol{\Psi}\boldsymbol{\varepsilon} \Leftrightarrow \boldsymbol{\Psi}\bar{\mathbf{a}} \\ &= (\bar{\mathbf{a}} - \boldsymbol{\varepsilon}) + \boldsymbol{\Psi}\boldsymbol{\varepsilon} \Leftrightarrow \mathbf{B}\bar{\mathbf{a}} = \mathbf{B}\boldsymbol{\varepsilon}, \end{aligned} \tag{15}$$

where $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_M] \in \mathbb{R}^{M\times M}$ and $\mathbf{b}_i = [b_{1,i}, \dots, b_{M,i}] \in \mathbb{R}^{M\times 1}$, $i = 1, \dots, M$. For constructing an attack vector $\bar{\mathbf{a}}$, it is the first step to determine an exploitable measurement such as the i^{th} measurement in the attackable set F and inject the predesigned false data a_i into it. According to $\mathbf{B}\bar{\mathbf{a}} - \mathbf{B}\boldsymbol{\varepsilon} = \mathbf{b}_1 a_1 + \cdots + \mathbf{b}_m a_m - \mathbf{B}\boldsymbol{\varepsilon} = \mathbf{0}$, we move the term $\mathbf{b}_i a_i$ to the right of the equation. Then, we have $\mathbf{b}_1 a_1 + \cdots + \mathbf{b}_{i-1} a_{i-1} + \mathbf{b}_{i+1} a_{i+1} + \cdots + \mathbf{b}_m a_m - \mathbf{B}\boldsymbol{\varepsilon} = -\mathbf{b}_i a_i$.

Next, the attack vector can be constructed by using the identification estimation method. Let $-\mathbf{b}_i a_i = \mathbf{Y}$, and the attack regression model is obtained as

$$\mathbf{Y} = \mathbf{B}'\mathbf{a}' + \boldsymbol{\Xi}, \tag{16}$$

where $\mathbf{B}' = (\mathbf{b}_1, \dots, \mathbf{b}_{i-1}, \mathbf{b}_{i+1}, \dots, \mathbf{b}_M) \in \mathbb{R}^{M\times(M-1)}$, $\mathbf{a}' = (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_M)^T \in \mathbb{R}^{(M-1)\times 1}$, and $\boldsymbol{\Xi} = -\mathbf{B}\boldsymbol{\varepsilon}$ is defined as the residual error vector. $\boldsymbol{\varepsilon}$ is the system residual increment caused by an attack, which is time-varying and usually regarded as Gaussian white noise; thus, $\boldsymbol{\Xi}$ is treated as the Gaussian noise. And if $\|\boldsymbol{\Xi}\| = \|\mathbf{B}\| \cdot \|\boldsymbol{\varepsilon}\| < \|\mathbf{B}\| \cdot \bar{\tau}_a$ is satisfied, the attack can bypass the BDD well. For convenience, define the vectors again as $\mathbf{a}' = (a_1', a_2', \dots, a_{M-1}')^T$, $\mathbf{B}' = [\mathbf{b}_1', \mathbf{b}_2', \dots, \mathbf{b}_{M-1}']$, and $\mathbf{b}_j' = [b_{1,j}', b_{2,j}', \dots, b_{M,j}']^T$, $j = 1, \dots, M-1$.

Remark 9. Based on the attack regression model with noise, the fast stepwise forward algorithms, i.e., the fast regression algorithm (FRA) [42], can be used to choose the nonzero attack vector elements one by one, each time maximizing the model error reduction ratio. However, the existence of the residual error vector $\boldsymbol{\Xi}$ can lead to overfitting of the attack model with more measurements selected, which is inconsistent to attackers' wish that as few measurements as possible need to be manipulated for an undetectable attack with the limited resources. To improve the sparsity of attack vectors and the generalization performance of the attack model, the locally regularized fast recursive (LRFR) algorithm [43] is used next to choose significant attack vector elements by associating each candidate attack vector element with an

individually regularized parameter, which is optimized within the Bayesian evidence framework.

3. The Locally Regularized Fast Recursive Algorithm

When the LRFR algorithm is used to construct the attack vector, each attack vector element corresponds to a candidate (i.e., the column vector $\mathbf{b}_i'$) in the regression matrix $\mathbf{B}'$. Then, identifying the smallest set of attacked measurements is equivalent to the selection of the significant model candidates in the regression matrix $\mathbf{B}'$. In this paper, a regularization technique is used to bind a regularization parameter to each candidate, and the Bayesian evidence framework is used to optimize the regularization parameters. Next, the significant candidates are directly selected according to the model error reduction contribution of each candidate term with a regularization parameter, leading to the construction of a compact regression model. To reduce the computational complexity, some proper regression contexts are further defined which allows fast implementation of the proposed method.

3.1. Generalization of Sparse Attack Vectors. The regularization technique, which introduces a decay term into the cost function, has been proposed to overcome the overfitting problem. A regularized cost function J based on the attack regression model (16) is shown as

$$J = \Xi^T\Xi + \sum_{i=1}^{M-1}\lambda_i\left(a_i'\right)^2 = \left(\mathbf{Y}-\mathbf{B}'\mathbf{a}'\right)^T\left(\mathbf{Y}-\mathbf{B}'\mathbf{a}'\right) + \left(\mathbf{a}'\right)^T\mathbf{\Lambda}\mathbf{a}', \tag{17}$$

where $\boldsymbol{\lambda} = [\lambda_1, \ldots, \lambda_{M-1}]^T$ is the regularization parameter vector that has the same dimension as the column vectors in the regression matrix $\mathbf{B}'$ and $\mathbf{\Lambda} = \text{diag}\,(\lambda_1, \ldots, \lambda_{M-1})$ is a diagonal matrix. To ensure that the attack can bypass the BDD well, the value of J needs to satisfy the corresponding condition (e.g., $J < (\|\mathbf{B}\| \cdot \overline{\tau}_a)^2$) by $\|\Xi\| = \|\mathbf{B}\| \cdot \|\boldsymbol{\varepsilon}\| < \|\mathbf{B}\| \cdot \overline{\tau}_a$. Thus, to guarantee that the condition is established, the appropriate termination criterion needs to be set. Then, the least-squares estimate of the attack vector elements that minimizes (17) is given as

$$\widehat{\mathbf{a}}' = \left(\left(\mathbf{B}'\right)^T\mathbf{B}' + \mathbf{\Lambda}\right)^{-1}\left(\mathbf{B}'\right)^T\mathbf{Y}. \tag{18}$$

Remark 10. As can be seen from (18), each attack vector element $\widehat{a}_i{}'$ is bound to a regularization parameter λ_i. It has been demonstrated that Bayesian evidence framework inference can be used to optimize the regularization parameter vector $\boldsymbol{\lambda}$. During the optimization process, if the values of some regularization parameters are getting larger and larger, the corresponding attack vector elements will become smaller and smaller and approach zero. That is, the corresponding measurements will not be selected to attack as the false data injected into them approach zero. This provides an effective way to guarantee the sparsity of attack vectors.

In forward subset selection, suppose that k out of $M-1$ attack regression vectors $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_k$ has already been selected. The remaining vectors (corresponding to the candidate attack vector elements) from the regression matrix $\mathbf{B}'$ are $\{\mathbf{p}_{k+1}, \mathbf{p}_{k+2}, \ldots, \mathbf{p}_{M-1}\}$. For an attack regression model with k elements, it follows that

$$\mathbf{S}_k \triangleq \left(\mathbf{B}_k'\right)^T\mathbf{B}_k' + \mathbf{\Lambda}_k, \tag{19}$$

$$\widehat{\mathbf{a}}_k' = \mathbf{S}_k{}^{-1}\left(\mathbf{B}_k'\right)^T\mathbf{Y}, \tag{20}$$

$$J\left(\widehat{\mathbf{a}}_k'\right) = \mathbf{Y}^T\left(\mathbf{I} - \mathbf{B}_k'\mathbf{S}_k^{-1}\left(\mathbf{B}_k'\right)^T\right)\mathbf{Y}, \tag{21}$$

where $\mathbf{B}_k' = [\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_k]$ and $\mathbf{\Lambda}_k = \text{diag}\,\{\lambda_1', \ldots, \lambda_k'\}$. The latter contains the corresponding k regularization parameters from the full vector $\boldsymbol{\lambda}$ in terms of the original indexing of $\mathbf{p}_i$ $(1 \le i \le k)$ in $\mathbf{B}'$.

If a new attack vector element $\mathbf{b}_j' \in \{\mathbf{p}_{k+1}, \ldots, \mathbf{p}_{M-1}\}$ is selected, the selected regression matrix increases by one column, becoming $\mathbf{B}_{k+1}{}' = [\mathbf{B}_k', \mathbf{b}_j']$. The corresponding $\lambda_j' \in \{\lambda_{k+1}{}', \ldots, \lambda_{M-1}{}'\}$ is also selected for $\mathbf{b}_j'$, producing the new regularization parameter matrix $\mathbf{\Lambda}_{k+1} = \text{diag}\,\{\mathbf{\Lambda}_k, \lambda_j'\}$. The regularized cost function is then updated as

$$J\left(\widehat{\mathbf{a}}_{k+1}{}'\right) = \mathbf{Y}^T\left(\mathbf{I} - \mathbf{B}_{k+1}{}'\mathbf{S}_{k+1}^{-1}\left(\mathbf{B}_{k+1}{}'\right)^T\right)\mathbf{Y}, \tag{22}$$

and the contribution of $\mathbf{b}_j'$ as the $(k+1)^{\text{th}}$ attack vector element is given as

$$\Delta J_{k+1}\left(\mathbf{b}_j'\right) = J_k\left(\widehat{\mathbf{a}}_k'\right) - J_{k+1}\left(\widehat{\mathbf{a}}_{k+1}{}'\right). \tag{23}$$

To select a new attack vector element, the contribution in (23) has to be computed for each of the $M-k-1$ remaining candidate elements as $\Delta J_{k+1}(\mathbf{b}_j')$, $\forall \mathbf{b}_j' \in \{\mathbf{b}_{k+1}{}', \ldots, \mathbf{b}_{M-1}{}'\}$. The one that produces the largest error reduction to the cost function is then chosen as the $(k+1)^{\text{th}}$ attack vector element.

In this way, the compact attack regression model is constructed in a forward selection way; i.e., the attack vector elements are selected to attack, one at a time according to the size of their contributions. The selection of the attack vector element continues until some attack vector construction criterion is satisfied.

The use of the LRFR will generate an initial subset of measurements to be attacked. To further reduce the number of the measurement subsets, the level 2 inference of the Bayesian evidence framework will be used to optimize the regularization parameters.

3.2. Optimization of the Regularization Parameters. Define $\mathbf{h} = [h_1, \ldots, h_{M-1}]^T$ as the vector of hyperparameters and β as the noise parameter, i.e., the inverse of the variance of the noise Ξ. The regularization parameters are equivalent to the ratio of the hyperparameters to the noise parameter explained by the level 1 inference of the Bayesian evidence framework [41]; i.e.,

$$\lambda_i = \frac{h_i}{\beta}, \quad 1 \le i \le M-1. \tag{24}$$

The second level of inference can determine the values of $\mathbf{h}$ and β by maximizing the posterior distribution. To further optimize the regularization parameters by the level 2 inference of the Bayesian evidence framework, the Hessian matrix $\mathbf{G}$ is given as

$$\mathbf{G} = \beta\left(\mathbf{B}'\right)^T\mathbf{B}' + \mathbf{\Lambda}_\mathbf{h}, \tag{25}$$

where $\mathbf{\Lambda}_\mathbf{h} = \text{diag}\,(h_1, \ldots, h_{M-1})$. From (16) and (21), it is clearly shown that $\mathbf{G} = \beta\mathbf{S}$.

Defining quantities $\gamma_i = 1 - V_{ii}h_i$, where V_{ii} is the i^{th} diagonal element of $\mathbf{G}^{-1}$, yields

$$h_i^{\text{new}} = \frac{\gamma_i}{\left(a_i'\right)^2}. \tag{26}$$

Then, define $\gamma = \sum_{i=1}^{M-1}\gamma_i$; it follows that

$$\beta^{\text{new}} = \frac{M-\gamma}{\Xi^T\Xi}. \tag{27}$$

Substituting (23) and (24) into $\lambda_i = h_i/\beta$, the updating formulas for the regularization parameters can be given as

$$\lambda_i^{\text{new}} = \frac{\gamma_i}{M-\gamma}\frac{\Xi^T\Xi}{\left(a_i'\right)^2}, \quad 1 \le i \le M-1. \tag{28}$$

3.3. Reduction of the Computational Complexity. To reduce the computational complexity, the following two steps need to be achieved: firstly, the updating of the regularization parameters $\lambda_i (1 \le i \le M-1)$ is relieved by using a recursive formula derived below and, secondly, some proper regression contexts are defined to significantly reduce the computation effort of the updating process (23).

Before further reducing the computational complexity, two steps are achieved as follows.

For the first step, suppose that the inverse of $\mathbf{S}_{k+1}^{-1}$ is defined as

$$\mathbf{S}_{k+1}^{-1} \triangleq \begin{bmatrix} \mathbf{F}_k & \mathbf{g}_k \\ \mathbf{g}_k^T & u_k \end{bmatrix}, \tag{29}$$

where $\mathbf{F}_k \in \Re^{k\times k}$, $\mathbf{g}_k \in \Re^{k\times 1}$, and $u_k \in \Re$. Also, another two definitions are introduced: $b'^{j}_{\lambda} \triangleq (\mathbf{b}_j')^T\mathbf{b}_j' + \lambda_j'$ and $\mathbf{B}'^{j}_{k} \triangleq (\mathbf{B}_k')^T\mathbf{b}_j'$. Then, (29) can be computed by using the following recursive formulas:

$$\begin{aligned} \mathbf{F}_k &= \mathbf{S}_k^{-1} + \frac{\mathbf{S}_k^{-1}\mathbf{B}'^{j}_{k}\left(\mathbf{B}'^{j}_{k}\right)^T\mathbf{S}_k^{-1}}{b'^{j}_{\lambda} - \left(\mathbf{B}'^{j}_{k}\right)^T\mathbf{S}_k^{-1}\mathbf{B}'^{j}_{k}}, \\ \mathbf{g}_k &= -\frac{\mathbf{F}_k\mathbf{B}'^{j}_{k}}{b'^{j}_{\lambda}}, \\ u_k &= \frac{b'^{j}_{\lambda} + \left(\mathbf{B}'^{j}_{k}\right)^T\mathbf{F}_k\mathbf{B}'^{j}_{k}}{\left(b'^{j}_{\lambda}\right)^2}. \end{aligned} \tag{30}$$

According to (25) and (29), it is obvious that the inverse of the Hessian matrix can be updated using the recursive formula $\mathbf{G}_{k+1}^{-1} = \beta^{-1}\mathbf{S}_{k+1}^{-1}$.

For the second step, define a residual matrix series as

$$\mathbf{R}_k \triangleq \mathbf{I} - \mathbf{B}_k'\left(\left(\mathbf{B}_k'\right)^T\mathbf{B}_k' + \mathbf{\Lambda}_k\right)^{-1}\left(\mathbf{B}_k'\right)^T = \mathbf{I} - \mathbf{B}_k'\mathbf{S}_k^{-1}\left(\mathbf{B}_k'\right)^T, \tag{31}$$

where $\mathbf{R}_k$, $1 \le k \le M-1$ is of full-column rank and $\mathbf{R}_0 \triangleq \mathbf{I}$. Then, $\mathbf{R}_{k+1}$ can be expressed using the following recursive formula:

$$\mathbf{R}_{k+1} = \mathbf{R}_k - \frac{\mathbf{R}_k\mathbf{p}_{k+1}\left(\mathbf{p}_{k+1j}\right)^T\mathbf{R}_k}{(\mathbf{p}_{k+1})^T\mathbf{R}_k\mathbf{p}_{k+1} + \lambda_j'}. \tag{32}$$

According to (32), (23) can be computed as

$$\Delta J_{k+1}\left(\mathbf{b}_j'\right) = \mathbf{Y}^T\mathbf{R}_k\mathbf{Y} - \mathbf{Y}^T\mathbf{R}_{k+1}\mathbf{Y} = \frac{\mathbf{Y}^T\mathbf{R}_k\mathbf{p}_{k+1}(\mathbf{p}_{k+1})^T\mathbf{R}_k\mathbf{Y}}{(\mathbf{p}_{k+1})^T\mathbf{R}_k\mathbf{p}_{k+1j} + \lambda_j'}. \tag{33}$$

To further simplify the computation of (33), another quantity involving $\mathbf{b}_j' \in \{\mathbf{p}_{k+1}, \ldots, \mathbf{p}_{M-1}\}$ is now introduced:

$$\mathbf{R}_k^j \triangleq \mathbf{R}_k\mathbf{b}_j'. \tag{34}$$

From (32), $\mathbf{R}_k^j$ can be recursively updated as

$$\begin{aligned} \mathbf{R}_k^j = \mathbf{R}_k\mathbf{b}_j' &= \left(\mathbf{R}_{k-1} - \frac{\mathbf{R}_{k-1}\mathbf{p}_k\mathbf{p}_k^T\mathbf{R}_{k-1}}{\mathbf{p}_k^T\mathbf{R}_{k-1}\mathbf{p}_k + \lambda_k'}\right)\mathbf{b}_j' \\ &= \mathbf{R}_{k-1}^j - \frac{\mathbf{R}_{k-1}^k\left(\mathbf{R}_{k-1}^k\right)^T\mathbf{b}_j'}{\mathbf{p}_k^T\mathbf{R}_{k-1}^k + \lambda_k'}. \end{aligned} \tag{35}$$

Substituting (34) into (33), the reduction contribution of $\mathbf{b}'_j$ to the cost function can be explicitly expressed as

$$\Delta J_{k+1}\left(\mathbf{b}'_j\right) = \frac{\left(\mathbf{Y}^T\mathbf{R}_k^j\right)^2}{\left(\mathbf{b}'_j\right)^T\mathbf{R}_k^j + \lambda'_j}. \tag{36}$$

3.4. Complete Algorithm. The procedure for the proposed attack strategy can be summarized in Figure 2.

4. Simulation and Results

To verify its effectiveness and feasibility, the proposed new sparse imperfect attack strategy is tested on a IEEE 30-bus system as shown in Figure 3. Firstly, the sparsity of the imperfect attack vectors constructed by FRA and LRFR is compared. Then, from the operator's viewpoint, the probability that the attackers can successfully construct an attack vector bypassing the BDD is calculated. Finally, a practical coastal area distribution network system is tested to further demonstrate the effectiveness of the proposed approach in practical systems.

4.1. Case 1. The IEEE 30-bus system consists of 30 buses and 41 transmission lines. Bus 1 is selected as the reference bus with the reference phase angle $\theta_1 = 0$. The unknown admittances and the unknown measurements by attackers are summarized in Table 1.

4.1.1. The Feasibility of the New Attack Strategy. There are a total of 112 measurements in the IEEE 30-bus system, where the 1^{st}–30^{th} measurements are bus active power injections, the 31^{st}–71^{st} measurements are power flows at "from" buses, and the 72^{nd}–112^{th} measurements are power flows at "to" buses. However, the system is assumed to be measured with 97 measurements except for 15 unknown measurements in Table 1, and the noise of each measurement follows $v_i \sim N(0, 0.05^2)$. It is assumed that the attackers are able to obtain the topology information but unable to acquire 3 admittances shown in Table 1. According to Theorem 1, an attacker can take the line flow measurements $f_{1-2}, f_{1-3}, f_{3-4}, f_{4-6}$ and the line parameters $b_{1-2}, b_{1-3}, b_{3-4}, b_{4-6}$ to calculate the phase angle difference between buses 2 and 6; i.e.,

$$\begin{aligned}\theta_2 - \theta_6 &= (\theta_2 - \theta_1) - (\theta_6 - \theta_1) = \left(-\frac{f_{2-1}}{b_{2-1}}\right) \\ &\quad - \left(-\frac{f_{6-4}}{b_{6-4}} - \frac{f_{4-3}}{b_{4-4}} - \frac{f_{3-1}}{b_{3-1}}\right) = \left(-\frac{0.0880}{16.67}\right) \\ &\quad - \left(-\frac{0.1458}{5.263} - \frac{0.1188}{25} - \frac{0.2133}{25}\right) = 0.0357.\end{aligned} \tag{37}$$

Then, the unknown element $D_6 = -b_{2-6}$ in the branch admittance matrix $\mathbf{D}$ can be calculated according to the branch active power flow equation $f_{2-6} = -b_{2-6}(\theta_2 - \theta_6)$.

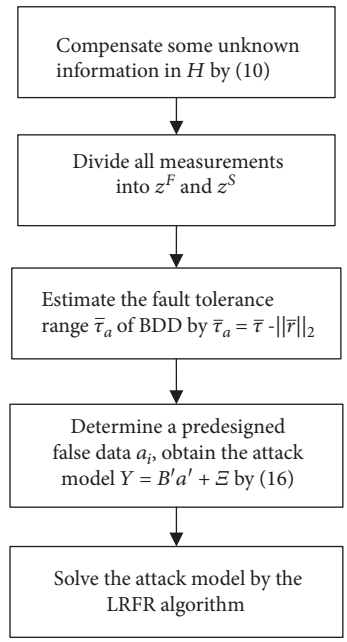

Figure 2: The procedure for the proposed attack strategy.

That is,

$$D_6 = -b_{2-6} = \frac{f_{2-6}}{\theta_2 - \theta_6} = \frac{0.1925}{0.0357} = 5.392. \tag{38}$$

However, the unknown elements $D_{27} = -b_{10-21}$ and $D_{18} = -b_{12-15}$ cannot be calculated by Theorem 1 as the line flow measurements f_{10-21} and f_{12-15} are unknown. The 10^{th}, 12^{th}, 15^{th}, 21^{st}, 48^{th}, 57^{th}, 89^{th}, and 98^{th} rows of the Jacobian matrix $\mathbf{H}$ contain unknown elements due to the unknown line parameters b_{10-21} and b_{12-15}. Thus, set $a_{10}, a_{12}, a_{15}, a_{21}, a_{48}, a_{57}, a_{89}, a_{98} = 0$. Moreover, since the measurements p_2, p_8, p_{17}, p_{19}, p_{24}, and $f_{6-10}, f_{10-6}, f_{12-15}, f_{15-12}, f_{10-21}, f_{21-10}, f_{10-22}, f_{22-10}, f_{28-27}, f_{27-28}$ cannot be obtained due to the attacker's limited resources or the physical protection of some smart meters, set $a_2, a_8, a_{17}, a_{19}, a_{24}, a_{42}, a_{48}, a_{57}, a_{58}, a_{66} = 0$ and $a_{83}, a_{89}, a_{98}, a_{99}, a_{107} = 0$ similarly. According to (8) and (9), we can calculate the approximation threshold $\overline{\tau} = 1.1063$ and $\overline{\tau}_a = 1.1063 - 0.0198 = 1.0865$.

The proposed new sparse imperfect attack strategy based on LRFR is used to construct the sparse attack vector. The 10^{th} measurement in the attackable set F is set as the initial attacked measurement, and the corresponding attack vector element (i.e., injected false data) is set as $a_{10} = 0.0970$. Each element of the residual error vector Ξ is set to follow $\Xi_i \sim N(0, 0.25^2)$. The initial value of ρ for terminating the attack vector element selection is chosen to be as small as possible such that in the first iteration of regularization parameter optimization, a large measurement subset is produced. This ensures that the significant measurements are not missed when $\boldsymbol{\lambda}$ is far from its optimal value, and the attack can bypass the BDD well.

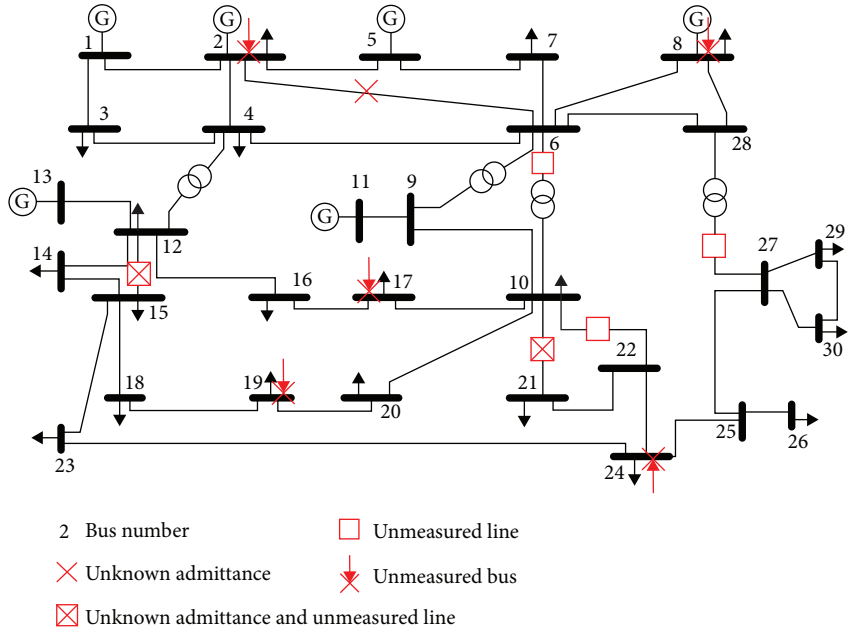

Figure 3: The modified IEEE 30-bus system.

Table 1: Unknown admittances and unknown measurements.

Unknown measurements	$f_{6-10}, f_{10-6}, f_{12-15}, f_{15-12}, f_{10-21}$ $f_{21-10}, f_{10-22}, f_{22-10}, f_{27-28}, f_{28-27}$ $p_2, p_8, p_{17}, p_{19}, p_{24}$
Unknown admittances	$b_{2-6}, b_{10-21}, b_{12-15}$

Table 2: Regularization parameters and false data for selected measurements.

Number l	False data a_l	Regularizer λ_l
21	−0.0164	15.9775
22	−0.0047	72.3036
23	0.0029	97.5222
24	0.0122	119.5453
25	−0.0123	144.3983
26	$-4.5797e-04$	151.0655
27	$-2.5728e-04$	145.7458
28	$2.6321e-04$	398.5669
29	$2.1098e-04$	863.9326
30	$1.1179e-04$	$1.0191e+03$
31	$1.2722e-04$	$4.7434e+03$
32	$-1.2481e-04$	$1.0839e+04$
33	$7.0177e-06$	$1.7708e+04$
34	$1.3973e-05$	$1.9152e+04$
35	$-1.3771e-05$	$3.1378e+04$
36	$1.6981e-06$	$3.8401e+04$
37	$4.6776e-07$	$5.7022e+04$
38	$-1.1456e-06$	$6.6393e+04$
39	$-5.0220e-07$	$1.0695e+05$
40	$9.5805e-07$	$3.8948e+05$

After the first iteration, there are 40 candidate attack vector elements. The attack model is then refined until the regularization parameter $\boldsymbol{\lambda}$ converges at the 114th iteration. Some values of the regularization parameters and false data are listed in Table 2. It is shown that all attack vector elements added after the 25th measurement have very large regularization parameters and their corresponding values (i.e., the false data injected into the measurements) are very close to zero. Therefore, the final attack vector is constructed by this new method effectively with only 25 nonzero elements.

The change of the resultant attack model error is shown in Figure 4 and Table 3, respectively. The parameter estimation process when 25 measurements are selected is shown in Figure 5. Table 4 shows the final selection order of the measurements and the estimation values of the attack vector elements.

4.1.2. The Sparsity Comparison of the Attack Vectors Constructed by LRFR and FRA. The sparse attack strategy based on FRA is used firstly to construct the sparse attack vector. Then, the sparsity of attack vectors constructed by LRFR and FRA is compared. It can be seen from Figure 6 that the strategy based on FRA selected 55 measurements and the new proposed strategy based on LRFR only selected 25 measurements. Thus, the proposed new attack strategy is able to produce a sparser attack vector.

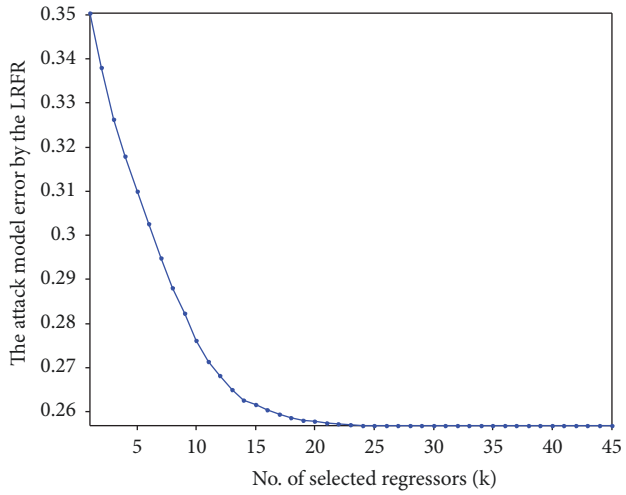

Figure 4: The change of the attack model error by the LRFR.

Table 3: The change value of the attack model error by the LRFR.

Number l	Model errors	Number l	Model errors
1	0.3502	16	0.2604
2	0.3380	17	0.2594
3	0.3261	18	0.2586
4	0.3179	19	0.2580
5	0.3100	20	0.2577
6	0.3026	21	0.2575
7	0.2948	22	0.2572
8	0.2881	23	0.2570
9	0.2823	24	0.2569
10	0.2760	25	0.2567
11	0.2714	26	0.2567
12	0.2681	27	0.2567
13	0.2650	28	0.2567
14	0.2627	29	0.2567
15	0.2615	30	0.2567

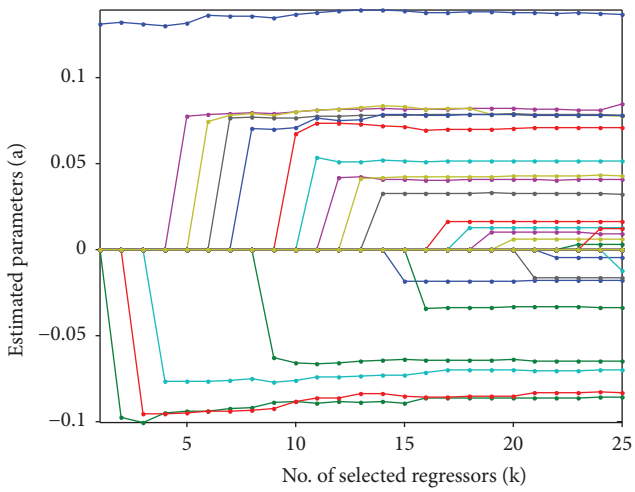

Figure 5: Parameter estimation process when 25 measurements are selected.

Table 4: Final selection order and estimation values of attack vector elements.

Initial number in set F	Estimation $\hat{a}_i'$	Initial number in set F	Estimation $\hat{a}_i'$
82	0.1366	55	0.0322
68	−0.0854	58	−0.0176
60	−0.0828	71	−0.0337
32	−0.0699	66	0.0162
16	0.0847	53	0.0127
75	0.0774	11	0.0093
12	0.0780	70	0.0062
54	0.0779	25	−0.0164
24	−0.0646	43	−0.0047
61	0.0705	15	0.0029
64	0.0514	39	0.0122
89	0.0405	49	−0.0123
27	0.0429	—	—

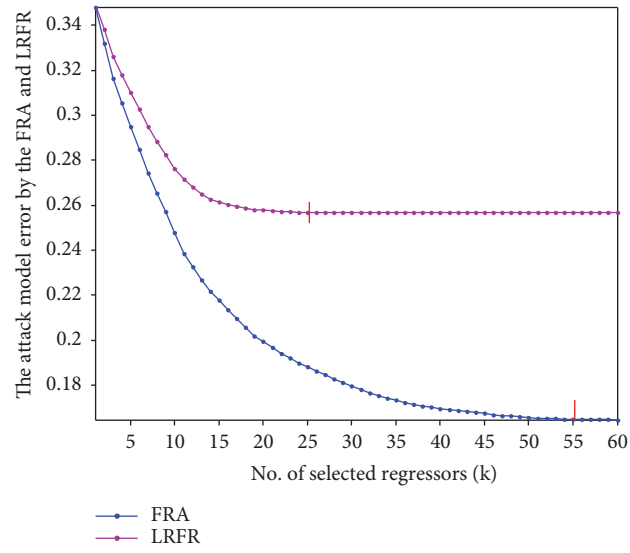

Figure 6: The change of the attack model error based on the FRA and LRFR.

4.1.3. The Probability of Constructing Attack Vectors Successfully from the Operator's Viewpoint. The full Jacobian matrix $\mathbf{H}$ and the full measurements $\mathbf{z}$ are known for the operators. Then, the detection threshold can be calculated as $\tau = 1.2771$. The distribution of the measurement noise vector $\mathbf{v}$ and the distribution of the residual error vector $\boldsymbol{\Xi}$ are the same as in Section 4.1. Firstly, a measurement $z_i \in F$ is randomly selected and a random false data a_i is injected into it to construct an imperfect attack regression model; 500 groups of imperfect attack regression models are then generated repeatedly in the same way. For each attack regression model, the LRFR method is used to solve the attack vectors and the attack residual is calculated to determine whether the attack vectors can successfully bypass the BDD.

The attack residuals calculated in the 500 simulations are shown in Figure 7, which indicates that 15 residuals exceed the threshold τ. Thus, the success rate of constructing attack vectors P_s is calculated as

$$P_s = \frac{500 - N_F}{500} \times 100\% = \frac{500 - 15}{500} \times 100\% = 97\%, \quad (39)$$

where N_F represents the number of detected attacks.

This shows that the proposed novel attack strategy can effectively construct the attack vectors with high success rate while ensuring the sparsity of attack vectors.

4.2. Case 2. The proposed new sparse attack strategy is next tested on a practical coastal area distribution network system [44] as shown in Figure 8. The distribution network system consists of 23 buses, 12 transformers, and 15 transmission lines (including overhead lines and underground cables). It covers 4 voltage levels containing one 110 kV/35 kV substation, two 35 kV/10 kV substations, and five 10 kV/0.4 kV substations. All branch impedance parameters (named values) are given in Table 5. Table 6 shows the active requirements of all 15 loads C1~C15 in the system.

There are a total of 67 measurements in the coastal area distribution network system. The acquisition of the measurements used in this simulation is from "Matpower" [45] directly, which is modified by [44]. Firstly, we can get the topology and parameter in [44] (i.e., all branch impedance parameters and the active demand of loads and voltage levels). And the distribution network system has 23 nodes and 22 branches. Then, we set the settings (e.g., system MVA base, bus data, generator data, and branch data) of the "Matpower case" according to the information of the distribution system. Finally, we set the number of measurements $m = 23 + 22 \times 2 = 67$, and the measurements are got by power flow calculation for the modified "Matpower case." Therefore, the simulation can be performed well by using the sufficient measurements. Moreover, if only a small number of measurements are available, the state estimation can still be used. For example, a new state estimation method referred to as the "mean squared estimator" (MSE) [46] is proposed, which is accurate with a limited number of measurements with guaranteed convergence.

However, considering the practical attacking situation where only partial topology and parameter information of the power grid are available and the attackers can only have access to limited smart meters, the system is assumed to be measured with 54 measurements except for the 13 secure measurements p_6, p_9, p_{19} and $\pm f_{2-4}, \pm f_{8-11}, \pm f_{8-16}, \pm f_{12-14}, \pm f_{20-21}$. Thus, set $a_6, a_9, a_{19} = 0$ and $a_{26}, a_{32}, a_{34}, a_{39}, a_{44}, a_{48}, a_{54}, a_{56}, a_{62}, a_{66} = 0$. According to (10), we can then calculate the approximation threshold $\overline{\tau} = 0.7948$ and $\overline{\tau}_a = 0.7948 - 0.0160 = 0.7788$. The distribution of the measurement noise vector $\mathbf{v}$ and the distribution of the residual error vector $\boldsymbol{\Xi}$ are the same as in Section 4.1.

The proposed new sparse attack strategy is then used to construct the sparse attack vector against the practical coastal area distribution network system. The 40th measurement is selected from the attackable set F as the initial attack measurement, and the corresponding attack vector element (i.e., injected false data) is set as $a_{40} = 0.1873$. The candidate measurement set after the first iteration contained 36 candidate measurements. The regularization parameters and the elements of the attack vector (injected false data) after $\boldsymbol{\lambda}$ converges at the 155th iteration are listed in Table 7. According to Table 7, the regularization parameters relating to the false data from the 23rd to the 36th are all very large and the associated attack vector elements are effectively close to zero. Thus, the final attack vector with 22 nonzero elements is produced. The parameter estimation process when 22 measurements are selected is shown in Figure 9. Table 8 shows the final selection order of the measurements and the estimation values of the attack vector elements.

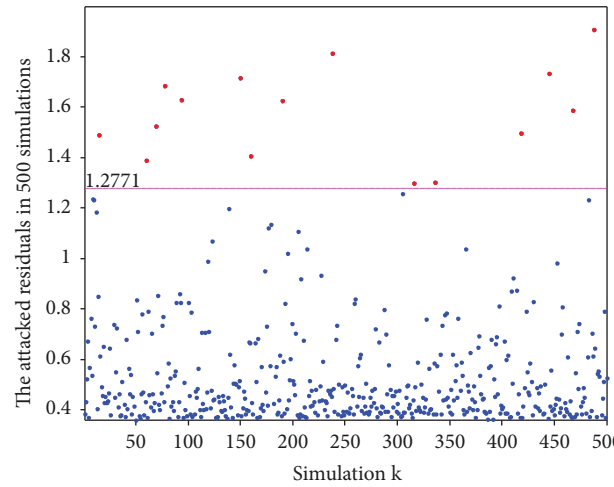

Figure 7: The attacked residuals calculated in 500 detection experiments.

Compared to the attack strategy based on FRA, Figure 10 shows that the LRFR algorithm produced a sparser attack vector with a reduction of 8 nonzero elements. The results confirm that the proposed method can produce a smaller number of measurements to attack again.

The full Jacobian matrix $\mathbf{H}$ and the full measurements $\mathbf{z}$ are known for the operators. Then, the detection threshold can be calculated as $\tau = 0.9425$. The LRFR method is tested on a separate set of 500 imperfect attack regression models generated by the same way in Section 4.1.3. The attack residuals calculated in the 500 simulations are shown in Figure 11, which indicates that 30 residuals exceed the threshold τ. Thus, the success rate of constructing attack vectors is calculated as

$$P_s = \frac{500 - N_F}{500} \times 100\% = \frac{500 - 30}{500} \times 100\% = 94\%, \quad (40)$$

where N_F represents the number of detected attacks.

This shows that the proposed novel attack strategy can effectively construct the attack vectors with high success rate while ensuring the sparsity of attack vectors again.

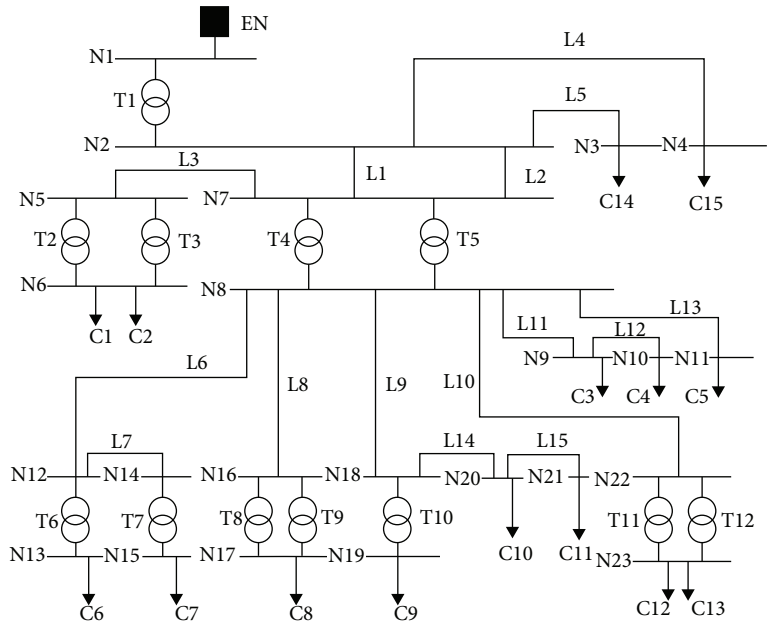

Figure 8: Topology diagram of the generic distribution network (N: node, T: transformer, L: line, and C: customer).

Table 5: Impedance parameters of network lines.

Branches	Resistance (ohm)	Reactance (ohm)
N1~N2	10.380	6.4740
N2~N3	0.4704	0.2163
N2~N4	0.4704	0.2163
N2~N7	0.3750	0.1781
N5~N6	9.6300	0.9125
N5~N7	0.4704	0.2163
N7~N8	2.4030	0.5360
N8~N9	0.0721	0.1126
N8~N11	0.2424	0.3789
N8~N12	0.1231	0.1925
N8~N16	0.2603	0.1511
N8~N18	0.1231	0.1925
N8~N22	0.1231	0.1925
N9~N10	0.0706	0.0410
N12~N13	28.500	0.0800
N12~N14	0.1129	0.0655
N14~N15	28.500	0.0800
N16~N17	14.250	0.0400
N18~N19	28.500	0.0800
N18~N20	0.1207	0.0701
N20~N21	0.1333	0.0774
N22~N23	35.910	0.0635

Table 6: The active demand of loads.

Load name	Network level (kV)	P (MW)
C1	10	4.200
C2	10	7.267
C3	10	3.840
C4	10	21.36
C5	10	2.950
C6	0.4	1.752
C7	0.4	3.306
C8	0.4	3.600
C9	0.4	0.280
C10	10	1.424
C11	10	1.088
C12	0.4	0.742
C13	0.4	2.039
C14	35	7.723
C15	35	12.46

5. Conclusion

The paper has proposed a novel sparse false data injection attack method in SG with incomplete power network information. Firstly, according to the obtained measurements and network information, some incomplete network information is compensated by the power flow equation. Then, the fault tolerance range of the BDD for the attack residual increments is estimated by calculating the detection threshold of the residual L2-norm test. Finally, an effective sparse imperfect strategy is proposed by treating the choice of measurements as a subset selection problem, which is solved by the LRFR algorithm to effectively improve the sparsity of the attack vector. The effectiveness of the proposed attack strategy is verified by the two cases

Table 7: The values of attack vector elements when converged at the 155th iteration.

Number l	False data a_l	Regularizer λ_l
18	0.0097	4.3561
19	−0.0061	7.4107
20	−0.0153	22.7431
21	0.0021	52.6785
22	0.0054	$2.1333e+03$
23	$-5.2091e-04$	$2.6064e+03$
24	$1.3981e-05$	$4.5212e+03$
25	$9.1153e-06$	$3.4857e+04$
26	$1.1554e-06$	$8.5604e+05$
27	$4.2074e-08$	$7.2734e+05$
28	$9.2636e-09$	$3.1392e+06$
29	$2.2372e-07$	$3.7652e+06$
30	$-1.6126e-08$	$3.5070e+07$
31	$8.6451e-10$	$3.9174e+07$
32	$2.6888e-09$	$1.9947e+08$
33	$-2.0263e-10$	$1.8797e+08$
34	$-1.6745e-10$	$2.2747e+08$
35	$-1.3460e-10$	$3.6586e+08$
36	$-3.8601e-10$	$8.3411e+08$

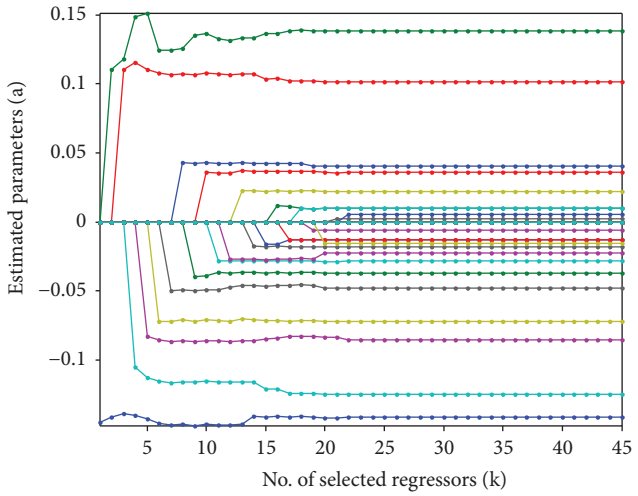

Figure 9: The parameter estimation process when 22 measurements are selected.

studied. For further work, considering that the attack does not rely on any prior power system network information but only uses the measurements, this will save attack resources and bring more complex effects on the smart grid. Thus, a blind sparse attack construction strategy is important and meaningful for finding the vulnerabilities of the power system.

Table 8: Final selection order and estimation values of attack vector elements.

Initial number in set F	Estimation $\widehat{a}$	Initial number in set F	Estimation $\widehat{a}$
32	−0.1418	35	−0.0225
6	0.1387	30	0.0218
22	0.1016	11	−0.0179
23	−0.1252	4	−0.0128
1	−0.0854	18	0.0097
26	−0.0722	2	−0.0128
45	−0.0480	17	0.0097
47	0.0405	8	−0.0060
25	−0.0370	51	−0.0153
37	0.0357	53	0.0021
24	−0.0285	38	0.0054

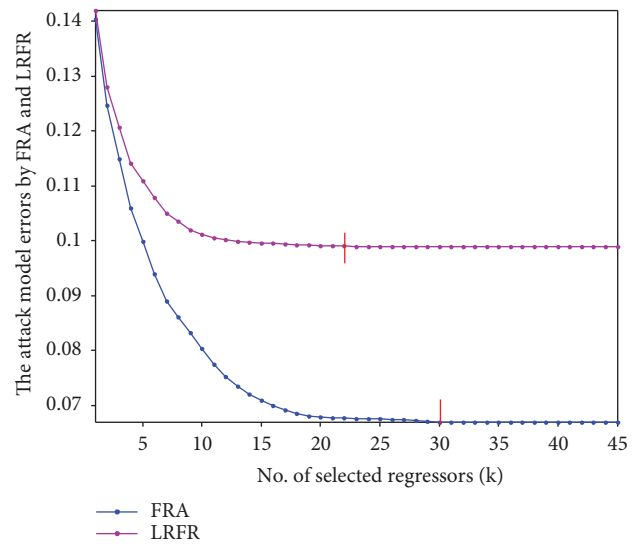

Figure 10: The change of the attack model error based on the FRA and LRFR.

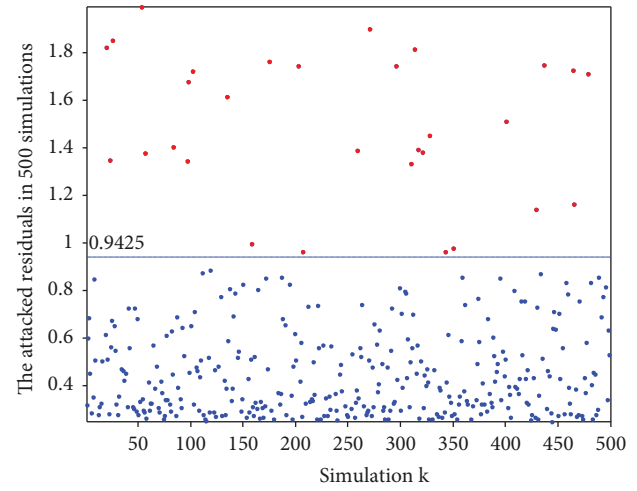

Figure 11: The attacked residuals calculated in 500 detection experiments.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This research was supported in part by the National Science Foundation of China (61773253, 61633016, and 61533010) and Science and Technology Commission of Shanghai Municipality (15JC1401900, 14JC1402200, and 17511107002).

References

[1] X. Zhang and C. K. Tse, "Assessment of robustness of power systems from a network perspective," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 3, pp. 456–464, 2015.

[2] C. Peng and J. Zhang, "Delay-distribution-dependent load frequency control of power systems with probabilistic interval delays," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3309–3317, 2016.

[3] Q. Sun, C. C. Lim, P. Shi, and F. Liu, "Design and stability of moving horizon estimator for Markov jump linear systems," *IEEE Transactions on Automatic Control*, p. 1, 2018.

[4] C. Peng, J. Zhang, and H. Yan, "Adaptive event-triggering H_∞ load frequency control for network-based power systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 2, pp. 1685–1694, 2018.

[5] C. Peng, J. Li, and M. Fei, "Resilient event-triggered H_∞ load frequency control for networked power systems with energy-limited DoS attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 4110–4118, 2017.

[6] K. F. Krommydas and A. T. Alexandridis, "Modular control design and stability analysis of isolated PV-source/battery-storage distributed generation systems," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 3, pp. 372–382, 2015.

[7] P. Singh and B. Khan, "Smart microgrid energy management using a novel artificial shark optimization," *Complexity*, vol. 2017, Article ID 2158926, 22 pages, 2017.

[8] D. Du, R. Chen, M. Fei, and K. Li, "A novel networked online recursive identification method for multivariable systems with incomplete measurement information," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 4, pp. 744–759, 2017.

[9] C. Han, L. Jia, and D. Peng, "Model predictive control of batch processes based on two-dimensional integration frame," *Nonlinear Analysis: Hybrid Systems*, vol. 28, pp. 75–86, 2018.

[10] D. Du, R. Chen, X. Li, L. Wu, P. Zhou, and M. Fei, "Malicious data deception attacks against power systems: a new case and its detection method," *Transactions of the Institute of Measurement and Control*, 2018.

[11] Y. L. Wang and Q. L. Han, "Network-based modelling and dynamic output feedback control for unmanned marine vehicles in network environments," *Automatica*, vol. 91, pp. 43–53, 2018.

[12] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.

[13] D. Du, C. Zhang, H. Wang, X. Li, H. Hu, and T. Yang, "Stability analysis of token-based wireless networked control systems under deception attacks," *Information Sciences*, vol. 459, pp. 168–182, 2018.

[14] D. Du, B. Qi, M. Fei, and Z. Wang, "Quantized control of distributed event-triggered networked control systems with hybrid wired-wireless networks communication constraints," *Information Sciences*, vol. 380, pp. 74–91, 2017.

[15] D. Du, B. Qi, M. Fei, and C. Peng, "Multiple event-triggered H_2/H_∞ filtering for hybrid wired–wireless networked systems with random network-induced delays," *Information Sciences*, vol. 325, pp. 393–408, 2015.

[16] W. Wang and Z. Lu, "Cyber security in the smart grid: survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[17] M. L. Tuballa and M. L. Abundo, "A review of the development of smart grid technologies," *Renewable & Sustainable Energy Reviews*, vol. 59, pp. 710–725, 2016.

[18] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2017.

[19] R. Marsh, "Congressman: national power grid frequently attacked," 2015, https://edition.cnn.com/2015/10/21/politics/national-power-grid-cyber-attacks/index.html.

[20] D. Goodin, "Israel's electric authority hit by "severe" hack attack," 2016, https://arstechnica.com/information-technology/2016/01/israels-electric-grid-hit-by-severe-hack-attack/.

[21] L. Hu, Z. Wang, Q. L. Han, and X. Liu, "State estimation under false data injection attacks: security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, 2018.

[22] L. Holten, A. Gjelsvik, S. Aam, F. F. Wu, and W. H. E. Liu, "Comparison of different methods for state estimation," *IEEE Transactions on Power Systems*, vol. 3, no. 4, pp. 1798–1806, 1988.

[23] A. Monticelli, "Fast decoupled state estimator," *IEEE Transactions on Power Systems*, vol. 5, no. 2, pp. 556–564, 1999.

[24] A. Gomez-Exposito and A. de la Villa Jaen, "Two-level state estimation with local measurement pre-processing," *IEEE Transactions on Power Systems*, vol. 24, no. 2, pp. 676–684, 2009.

[25] A. Primadianto and C. N. Lu, "A review on distribution system state estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3875–3883, 2017.

[26] L. Yao, N. Peng, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[27] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[28] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[29] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power

grids," in *2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 3153–3158, Anaheim, CA, USA, 2012.

[30] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *49th IEEE Conference on Decision and Control (CDC)*, pp. 5991–5998, Atlanta, GA, USA, 2010.

[31] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.

[32] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 2015.

[33] Y. Zhang, Z. Wang, and F. E. Alsaadi, "Detection of intermittent faults for nonuniformly sampled multi-rate systems with dynamic quantisation and missing measurements," *International Journal of Control*, pp. 1–12, 2018.

[34] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[35] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: centralized and distributed models," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306–1318, 2013.

[36] K. C. Sou, H. Sandberg, and K. H. Johansson, "Computing critical κ-tuples in power networks," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1511–1520, 2012.

[37] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194–3208, 2014.

[38] R. Deng, P. Zhuang, and H. Liang, "CCPA: coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.

[39] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, CRC Press, Boca Raton, FL, USA, 2004.

[40] L. Hu, Z. Wang, and X. Liu, "Dynamic state estimation of power systems with quantization effects: a recursive filter approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1604–1614, 2016.

[41] A. Monticelli, "State estimation in electric power systems: a generalized approach," *Power Electronics and Power Systems*, vol. 20, no. 4, pp. 553–556, 1999.

[42] D. Du, K. Li, X. Li, and M. Fei, "A novel forward gene selection algorithm for microarray data," *Neurocomputing*, vol. 133, no. 8, pp. 446–458, 2014.

[43] D. Du, X. Li, M. Fei, and G. W. Irwin, "A novel locally regularized automatic construction method for RBF neural models," *Neurocomputing*, vol. 98, no. 18, pp. 4–11, 2012.

[44] V. L. Strugar, V. A. Katic, and J. V. Milanovic, "Generic model of coastal distribution network for power system harmonics studies," *Przegląd Elektrotechniczny*, vol. 2013, no. 123, pp. 149–155, 2013.

[45] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.

[46] H. Bilil and H. Gharavi, "MMSE-based analytical estimator for uncertain power system with limited number of measurements," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5236–5247, 2018.