Research Article

Data-Driven and Low-Sparsity False Data Injection Attacks in Smart Grid

Jiwei Tian , Buhong Wang, and Xia Li

Information and Navigation College, Air Force Engineering University, Xi'an, Shanxi Province 710077, China

Correspondence should be addressed to Jiwei Tian; tianjiwei2016@163.com

Received 5 April 2018; Accepted 10 September 2018; Published 26 September 2018

Guest Editor: Jin Wei

Copyright © 2018 Jiwei Tian et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Recent researches on data-driven and low-sparsity data injection attacks have been presented, respectively. To combine the two main goals (data-driven and low-sparsity) of research, this paper presents a data-driven and low-sparsity false data injection attack strategy. The proposed attacking strategy (EID: Eliminate-Infer-Determine) is divided into three stages. In the first step, the intercepted data is preprocessed by sparse optimization techniques to eliminate the outliers. The recovered data is then exploited to learn about the system matrix based on the parallel factorization algorithm in the second step. In the third step, the approximated system matrix is applied for the design of sparse attack vector based on the convex optimization. The simulation results show that the EID attack strategy achieves a better performance than the improved ICA-based attack strategy in constructing perfect sparse attack vectors. What is more, data-driven implementation of the proposed strategy is also presented which ensures attack performance even without the prior information of the system.

1. Introduction

Driven by the smart grid, various emerging information and communication technologies are being integrated into the electric power grid, such as advanced metering infrastructures (AMI), intelligent electronic devices, and IEC 61850 based substations [1]. The in-depth integration of information technologies and communication networks enables the system operators to monitor the real-time operation and take emergency control measures to alleviate risks. However, modern power systems are also subject to numerous cyber-attacks on account of the vulnerabilities of the information technologies and communication networks.

State estimation is used to acquire power system state's best estimate by analyzing meter measurements. The output of state estimation is used by the control center operators as they perform security-constrained economic dispatch (SCED), optimal power flow (OPF), contingency analysis (CA), etc. Liu et al. [2] demonstrate that the power system state estimators are at present greatly vulnerable to the cyber-attacks. Liu et al. reveal that the Bad Data Detection (BDD) algorithm cannot detect the attack if certain strategies are adopted and the new class of attacks is called false data

injection attacks (FDIA). So far, numerous research works have been carried out due to the hiddenness of FDIA and the serious consequences of the attacks, discussed below.

The FDIA proposed by Liu et al. requires two conditions in order to achieve the purpose of arbitrarily tampering state estimation results: one is that attackers have preceding knowledge of the system structure matrix; the other is that attackers need to control all of the meter readings. However, the two conditions above are difficult to achieve in the actual attacks for two reasons. First, the system structure matrix is usually unknown to the attacker. In fact, it is often safeguarded by the system operator. Second, as the attacker has access to only a small quantity of meter measurements typically, it is quite hard to control all of the meter measurements in practice. To facilitate real-world attacks, there are two main lines of research on the construction of false data injection attack vectors as discussed below.

The first line of research is on implementing a successful attack based on prior knowledge of the system structure matrix by controlling only a few meter measurements. Kim and Poor [3] proposed a general optimization scheme to construct low-sparsity attack vectors when a subset of meter sensors are safeguarded, while Ozay et al. [4] extended

the low-sparsity attack vector construction scheme to a distributed one. Sandberg et al. [5] thought about sparse attacks that target crucial sensors, which are sensitive to attacks and crucial for the observability of the power system. Hao et al. [6] proposed an effective attack vector construction algorithm generating highly sparse attack vectors rapidly. Another line of research is on carrying out FDI attacks without prior knowledge of the system structure matrix. Esmalifalak et al. [7] proposed to identify a mixing matrix based on independent component analysis (ICA) from which an undetectable attack is launched. In this work, Esmalifalak presumed that the prior information of the system is unknown to the attacker and the attacker can carry out stealthy attacks based on the measurement matrix. Yu and Chin [8] proposed a blind FDI attack construction strategy based on principal component analysis (PCA), which stealthily and successfully attacks the system by the meter measurements. Kim et al. [9] proposed a similar approach for attack construction in view of both partial measurements and full measurements. The above data-driven strategies all presume that the meter measurements are noiseless or involve random noise following Gaussian distribution. However, gross errors (e.g., errors that do not follow Gaussian distribution), which are prevalent in other applications (e.g., bioinformatics, image processing), are also omnipresent in power grid measurements owing to communication errors, data losses, or sensor malfunctions. Theoretically, as long as the data include gross errors, the PCA's accuracy will be affected [10]. Anwar et al. [11] demonstrated that PCA based attack schemes are invalid in the presence of gross errors and proposed a technique to overcome this limitation.

The research of the two lines has a relatively independent development. This paper attempts to combine the two main lines of research; that is, this paper attempts to solve the problem of carrying out low-sparsity attacks through estimating system structure matrix without prior knowledge of the system information. Moreover, this paper will provide a data-driven and low-sparsity false data injection attack strategy which is more suitable for real-world attacks. The main contributions of this paper are threefold:

(1) In the data-driven approach, the attack vector is determined based on the measurement signals only based on PARAFAC (parallel factor analysis) method. In the low-sparsity approach, the attack vector can be constructed based on the convex optimization as a sparse term where only few components are nonzeros, which indicates that a small number of sensors need to be controlled. We combine the data-driven blind attack strategy and low-sparsity attack strategy in order to provide a more practical attack strategy: EID (Eliminate-Infer-Determine) attack strategy.

(2) We consider the existence of gross errors and propose a technique based on sparse optimization overcoming this limitation by extracting the outliers from the data, which successfully generates stealthy FDI attacks in the presence of outliers. The proposed EID attack strategy using Augmented Lagrange Multiplier (ALM) approach can carry out stealthy FDI attacks successfully with the existence of gross errors.

(3) We provide a comprehensive consideration of the situations of the attack process and propose a pragmatic

three-stage attack strategy. In the first step, the intercepted data is preprocessed by sparse optimization techniques to eliminate the outliers. The recovered data is then exploited to learn about the system matrix based on the parallel factorization algorithm in the second step. In the third step, the approximated system matrix is applied for the design of sparse attack vector based on the convex optimization.

The rest of this paper is ordered as follows: The preliminaries are given in Section 2. The attack disclosure analysis is explored in Section 3. A three-stage data-driven attack strategy is demonstrated in Section 4. Experimental outcomes and analyses using the IEEE 14-bus, 30-bus, 118-bus, and 300-bus systems are given in Section 5. The conclusions are provided in Section 6.

2. Preliminaries

2.1. System Model. Here, a typical formulation of the state estimation problem is presented using a DC power flow model.

$$z = Hx + e \quad (1)$$

In (1), $z = [z_1, z_2, \dots, z_m]^T$ represents the sensor measurements, $x = [x_1, x_2, \dots, x_n]^T$ denotes the state variables of the system to be estimated, H is an $m \times n$ measurement matrix, and $e = [e_1, e_2, \dots, e_m]^T$ is random errors in measurement.

In reality, there are more sensor measurements in the power system than those needed for observability; i.e., $m > n$. When m is greater than n , as is in the representative case, state estimation involves figuring out an overdetermined system of linear equations. The issue is usually worked out by the weighted least squares (WLS) algorithm.

$$\hat{x} = (H^T W H)^{-1} H^T W z \quad (2)$$

Due to device misconfiguration, device failures, or other errors, meter measurements used for state estimation may be inaccurate. Thus, it is extremely necessary to detect the presence of bad measurements. Prevailing power systems use BDD to compare the measurement residual with a threshold τ .

$$r = z - H(\hat{x}) \quad (3)$$

If $\|r\| > \tau$, the system identifies bad data measurements. Differently, z is regarded as a regular measurement.

2.2. Undetectable False Data Injection Attacks. In [2], Liu et al. present undetectable false data injection attacks that can bypass BDD as discussed below.

Let $a = [a_1, a_2, \dots, a_m]^T$ represent an attack vector added to original measurement vector $z = [z_1, z_2, \dots, z_m]^T$. Let $z_{bad} = z + a$ be the resulting compromised measurement vector. $\hat{x}$ and x_{bad} represent the estimated state corresponding to the original measurement z and manipulated measurement z_{bad} , respectively. Let $c = [c_1, c_2, \dots, c_n]^T$ represent the estimation error introduced by the attack, so that $x_{bad} = x + c$.

Theorem 3 ensures that the above attack is undetectable. What is more, the attack is irreducible which means that a minimum set of attack sensors is required in an undetectable attack. The theorem proves in theory that the undetectable attack with low-sparsity can be implemented using the incomplete system matrix $H(S_i, \cdot)$ and corresponding sensors S_i . As a matter of fact, the information of $H(S_i, \cdot)$ is usually well protected and unknown to the attacker. In the following part, we will provide a three-stage data-driven attack strategy to demonstrate that the incomplete system matrix can be inferred and used to perform an undetectable attack with low-sparsity.

4. Data-Driven and Low-Sparsity Attack Strategy

Li et al. [13] have pointed out that the interception of the unprotected sensor meters during the transmission of meter measurement can be utilized for attack. In this case, it is assumed that the eavesdropping data is used to design low-sparsity undetectable attacks. Based on observation above, a three-stage data-driven attack strategy (EID (Eliminate-Infer-Determine) attack strategy) is presented as follows:

(1) First, the intercepted meter data are preprocessed to eliminate the outliers. Gross errors (e.g., outliers) are omnipresent in power grid measurements on account of sensor failures or communication errors so that the traditional data-driven based attack strategies are often invalid. Therefore, it is necessary that the intercepted data should be preprocessed based on sparse optimization techniques to eliminate the outliers in the first stage.

(2) At the second stage, an identification method to infer the system's incomplete knowledge is adopted. Besides, a necessary model transformation is required to guarantee the system matrix's identifiability.

(3) At the third stage, sparse attack vector is determined based on inferred information of the system matrix. An approach for designing sparse attack vector is proposed applying the obtained linear structure matrix.

4.1. First Step: Eliminating the Outliers. Assume that the measurement matrix that contains outliers is written as

$$Z_{outlier} = Z + E \quad (10)$$

where Z stands for the original matrix needed to be restored, which is of low rank; E stands for outliers, which is a sparse matrix. Z and E need to be separated from the raw measurement matrix containing outliers $Z_{outlier}$ before generating attack vectors. This is a matrix recovery issue that can be expressed as below.

$$\begin{aligned} \min \quad & \|Z\|_* + \lambda \|E\|_1 \\ \text{s.t.} \quad & Z_{outlier} = Z + E \end{aligned} \quad (11)$$

In the convex optimization issue above, $\|\bullet\|_*$ represents a matrix's nuclear norm, $\|\bullet\|_1$ represents a matrix's l_1 norm, and λ denotes the positive weighting parameter [14]. To deal with this trouble, the Augmented Lagrange Multiplier (ALM) [15] approach is used as follows.

The ALM approach can be applied for common constraint optimization issues as discussed below.

$$\begin{aligned} \min \quad & f(x) \\ \text{s.t.} \quad & h(x) = 0 \end{aligned} \quad (12)$$

With the ALM method, we can express the objective function as a Lagrangian function:

$$L(x, Y, \mu) = f(x) + \langle \gamma, h(x) \rangle + \frac{\mu}{2} \|h(x)\|_F^2 \quad (13)$$

where γ stands for the LaGrange multiplier and μ represents a positive scalar.

Considering $x = (Z, E)$, $f(x) = \|Z\|_* + \lambda \|E\|_1$, and $h(x) = Z_{outlier} - Z - E$, we can write the Lagrangian function as follows.

$$\begin{aligned} L(A, E, \gamma, \mu) &= f(x) \\ &= \|Z\|_* + \lambda \|E\|_1 \\ &\quad + \langle \gamma, (Z_{outlier} - Z - E) \rangle \\ &\quad + \frac{\mu}{2} \|Z_{outlier} - Z - E\|_F^2 \end{aligned} \quad (14)$$

The optimization process is worked out by two update stages.

$$Z_{K+1} = \arg \min L(Z, E_k, \gamma_k, \mu_k) \quad (15)$$

$$E_{K+1} = \arg \min L(Z_{K+1}, E, \gamma_k, \mu_k) \quad (16)$$

Equation (16) is solvable from the soft shrinkage formula [16], using an iterative method which employs the matrix's singular value decomposition ($Z_{outlier} - E_k + \mu_k^{-1} \gamma_k$). Thereafter, we can obtain the rectangular diagonal matrix S and unitary matrix U, V . Then, update Z .

$$Z_{k+1} = U \xi_{\mu_k^{-1}}[S] V^T \quad (17)$$

And update E .

$$E_{k+q} = \xi_{\lambda \mu_k^{-1}}[Z_{outlier} - Z_{k+1} + \mu_k^{-1} \gamma_k] \quad (18)$$

Here $\lambda = 1/\sqrt{\max(m, t)}$ and ξ represents a soft-thresholding operator. It is defined as follows [14].

$$\xi_\varepsilon[x] = \begin{cases} x - \varepsilon, & \text{if } x > \varepsilon \\ x + \varepsilon, & \text{if } x < -\varepsilon \\ 0, & \text{otherwise} \end{cases} \quad (19)$$

γ and μ are updated throughout each iteration as discussed below:

$$\gamma_{k+1} = \gamma_k + \mu_k (Z_{outlier} - Z_{k+1} - E_{k+1}) \quad (20)$$

$$\mu_{k+1} = \Psi \mu_k \quad (21)$$

where Ψ represents a positive constant. The optimization process proceeds till the convergence standards are satisfied. The method's convergence is checked over based on the relative error using (22) against a tolerance, τ .

$$c_k^{ite} = \frac{\|Z_{outlier} - Z_{k+1} - E_{k+1}\|}{\|Z_{outlier}\|_F} \quad (22)$$

The original measurement matrix Z is restored, once the algorithm has converged. A stealthy attack vector that is based on recovered measurement matrix can be then constructed.

4.2. Second Step: Inferring the System's Incomplete Knowledge. Similar to the research of [17, 18], based on the load variables, model (1) can be firstly transformable into a linearly independent model. Let $L = [l_1 \cdots l_d]^T$ represent the system load variables, where l_d is the loads number ($l_d < n$). As the state variable x is associated with the load variable L , the relationship can be expressed as a nonlinear function $x = f(L)$. Without generality's loss, the elements of L are statistically independent, and $f(0) = 0$. We can approximately have

$$x = f(0) + \Gamma(L - 0) + o(\|L - 0\|_F^2) = \Gamma L + o(\|L\|_F^2) \quad (23)$$

where the matrix Γ represents the Taylor expansion's first-order coefficient matrix of $f(L)$ at 0, and $o(\|L\|_F^2)$ is the remainder term. Generally speaking, the remainder term $o(\|L\|_F^2)$ is negligible. Model (1) correspondingly is transformable into

$$z = NL + e \quad (24)$$

where $N = [n_1 \cdots n_{l_d}] = H\Gamma \in R^{m \times l_d}$ represents a new system matrix. Due to the load variables' independence, (24) is a linearly independent system.

The subsystem matrix's unknown knowledge needs to be identified using the eavesdropped data, as stated in Theorem 3. The estimation issue is in essence equal to identification of the matrix $N(S_i, \cdot) = H(S_i, \cdot)\Gamma$ that is based on (24). To simplify the symbol, the new matrix N in place of $N(S_i, \cdot)$ is addressed. The necessary explanations will be provided at the section's end for completeness. In particular, a new system matrix with eavesdropping meter data can be inferred using a multiway decomposition approach such as PARAFAC [19, 20]. Here, it is assumed that a series of sensor data with T samples are intercepted. We can calculate the intercepted data as a high order cumulant, such as a fourth order tensor:

$$\hat{\Phi}_{\sigma_1, \sigma_2, \sigma_3, \sigma_4} = \text{cum}(z_{\sigma_1}, z_{\sigma_2}, z_{\sigma_3}, z_{\sigma_4}) \quad (25)$$

where $\sigma_1, \sigma_2, \sigma_3, \sigma_4 = 1, 2, \dots, m$ and $\text{cum}(\bullet)$ denotes the moments of the distribution. The tensor in (25) can be decomposed as follows:

$$\Phi = \sum_{k=1}^{l_d} \xi_k \times n_j \circ n_j \circ n_j \circ n_j \quad (26)$$

where ξ_k is the kurtosis of the k -th load variable; i.e., $\xi_k = \text{cum}(l_j, l_j, l_j, l_j)$. In [21], the authors have shown that the decomposition as in (26) is generally unique if $(m+1)(m+2)(m+3)/(4!) \geq l_d$. Based on the condition, the minimal eavesdropped measurements $f_{\min}$ is determined when the load number l_d is given, which is shown in Table 1.

Generally, we can model the decomposition of equation (26) as a constraint minimization issue as follows.

$$\begin{aligned} \min_{\Phi} \quad & \left\| \hat{\Phi} - \Phi \right\|_F^2 \\ \text{s.t.} \quad & \Phi = \sum_{k=1}^{l_d} \xi_k \times n_j \circ n_j \circ n_j \circ n_j \end{aligned} \quad (27)$$

TABLE 1: The relation between the minimal intercepted meters and the load number.

l_d	5	8	14	21	30	41
$f_{\min}$	3	4	5	6	7	8

The optimal solution can be obtained by the alternative least squares (ALS) approach [17]. Let $\hat{N}$ represent the estimated new matrix of N with the result of (27). These matrices are intercorrelated:

$$\hat{N} = N\Pi\Lambda \quad (28)$$

where Π denotes the permutation matrix and Λ denotes the diagonal matrix. In [17], it is stated that these insignificant uncertainties have no effect on new matrix recognition.

4.3. Third Step: Determining the Sparse Attack Vector. In this step, based on the inferred matrix $\hat{N}$, our goal is to design the sparse attack vector that is corresponding to the attack sensors. Using the new system model of (24), we can write the attack vector in terms of (9) as

$$a_i = \hat{N}l \quad (29)$$

where $l \in R^{l_d}$ denotes the load variables' perceived change. Notice that l must be calculated to guarantee the attack vector's sparsity elaborately.

Taking into account the above situation, we illustrate that the attack vector construction issue is transformable as a constraint minimization optimization problem. For convenience, we denote $u = (\hat{N}(i, \cdot))^T$, and $V_i = [v_1^T \cdots v_m^T]^T = \hat{N}(I_i, \cdot)$, where $I_i = M \setminus \{i\}$. With an appropriate reordering of the rows, a_i can be represented as follows.

$$a_i = \begin{bmatrix} u^T l \\ V_i l \end{bmatrix} \quad (30)$$

In (30), we restrict $u^T l = 1$. This constraint implies that we can fix the i -th bus meter; that is, the attack meter set corresponds to S_i . Taking into account (29) and (30), we can express the attack vector construction issue as a constraint cardinality min problem as follows.

$$\begin{aligned} \min_l \quad & \|a_i\|_0 = \left\| \hat{N}l \right\|_0 \\ \text{s.t.} \quad & u^T l = 1 \iff \\ \min_l \quad & \|a_i\|_0 = \|V_i l\|_0 \\ \text{s.t.} \quad & u^T l = 1 \end{aligned} \quad (31)$$

Note that the optimization (31) is a NP-hard issue, and an alternative method can be resorted, e.g., the one that is based on l_1 minimization model.

$$\begin{aligned} \min_l \quad & \|a_i\|_1 = \|V_i l\|_1 \\ \text{s.t.} \quad & u^T l = 1 \end{aligned} \quad (32)$$

Input: Z_{outlier} =intercepted data matrix;
 (1) Eliminate the outliers: $Z = \text{ALM}(Z_{\text{outlier}})$;
 (2) Infer the system's incomplete knowledge: $\hat{N} = \text{PARAFAC}(Z)$;
 (3) Determine the sparse attack vector: $a = \hat{N} l$
 (4) $z' = z + a$;
Output: attack vector z'

ALGORITHM 1: The proposed EID (Eliminate-Infer-Determine) attack strategy.

The proposed three-step attack strategy is summarized in Algorithm 1. Notice that owing to the designed attack vector's sparsity, there is no need to acquire the system matrix's total knowledge. Instead, we should infer a subsystem matrix $N(E_i, :)$, where E_i represents the eavesdropped meter set satisfying $S_i \subset E_i$, $|E_i| < m$. We can select the number of E_i as comparatively larger than the number of loads. Accordingly, the reduced meter data set $Z(E_i, :)$ is considered to be eavesdropped. In addition, we can express the designed sparse attack vector as follows:

$$a_i^* = \begin{bmatrix} a_i^*(E_i) \\ 0 \end{bmatrix} \quad (33)$$

where $a_i^*(E_i) = N(E_i, :)y^*$.

5. Experiments and Analysis

5.1. Experiment Settings. In this part, we evaluated the proposed attack strategy through experiments using four IEEE power systems. Figure 2 demonstrates the topology of the IEEE 14-bus system and the topology of the IEEE 30-bus system, respectively. The state estimation can be obtained based on MATPOWER [22]. All buses and branch lines are measured by corresponding sensors. In addition, the loads are at random modified to produce experimental measurements to simulate a practical power condition. Suppose that the loads on each bus in the power system are uniformly distributed between 50% and 150% of its base load and the meter data are produced correspondingly [17]. We select the data length as 5000. Next, signal-to-noise ratio (SNR) has been considered between 5 and 40 dB during the simulation.

5.2. Results Analysis. As is shown in Figure 2, we evaluated the proposed data-driven attack strategy in the case of the 5-sparse undetectable attack case [12]. For 14-bus system, we select sensor set $S_{11} = \{B_{11}, F_{11}\}$ as 5-sparse undetectable attack case. For 30-bus system, we select sensor set $S_{19} = \{B_{19}, F_{19}\}$ as the 5-sparse undetectable attack case. In the proposed attack scheme's first stage, the intercepted data is preprocessed based on ALM method to eliminate the outliers. In the second stage, the recovered measurement is exploited to infer the system information based on the parallel factorization algorithm. In the third step, the calculated system matrix is employed for the sparse attack vector construction based on the convex optimization. Since the attack vector constructed by the traditional ICA-based method has no

sparse terms, we introduced the improved ICA-based method to replace the traditional method for a better comparison. The improved ICA-based method is similar to the EID strategy which includes three stages. The only difference is that the second phase of the proposed method is ICA. We call this strategy an improved ICA-based strategy.

First of all, we evaluated the validity of linearity assumptions and its performance with different levels of noises. The required subsystem matrices to be estimated are selected as $N(E_i, :)$ where $i = 11$ is as shown in Figure 2(a) and $i = 19$ is as shown in Figure 2(b). To ensure designed attack vector's sparsity, the number of sensors is usually advised to be larger than the number of loads; e.g., $|E_i| = 2l_d$. We define the Mean Square Errors (MSEs) as the residuals between the estimated measurements and the meter measurements. Figure 3(a) shows the MSEs of the PARAFAC method and ICA method under various SNRs noises in IEEE 14-bus and 30-bus system, respectively. As is illustrated in Figure 3(a), the PARAFAC method achieves a lower MSEs performance than that of the ICA method, especially in the lower SNRs cases. The result implies that the PARAFAC method takes advantage of the non-Gaussian load variables' higher-order statistics to infer the system matrix. Therefore, the PARAFAC method is less sensitive to Gaussian noises of the system than the ICA method. However, in the presence of outliers, the PARAFAC method and ICA method will both present a relatively large MSEs, as is shown in Figure 3(b). In this case, the estimated system matrix will seriously deviate from the actual state of the power system. If we preprocess the intercepted data based on ALM method to eliminate the outliers and use the PARAFAC method or ICA method on intercepted data to learn about the system matrix, the MSEs will be greatly reduced and the estimated system matrix is able to reflect the system condition more precisely, as is shown in Figure 3(c). As is illustrated in Figure 3(c), the PARAFAC method also achieves a lower MSEs performance than ICA method does even if the data is preprocessed.

Applying the estimated system matrix, the sparse attack vector construction performance was next evaluated. Figure 4 illustrates the attack vector construction under two different systems. Take Figure 4(a) as an example; the attack vector (blue line) based on the EID attack strategy is almost identical to the attack vector (red line) when the complete system information is known to the attacker (it is named as perfect FDI attack). The yellow line represents the sparse attack vector based on the improved ICA-based method. Although the red line and yellow line are very similar, there are subtle

Ⓜ GENERATORS
Ⓢ SYNCHRONOUS
CONDENSERS

Ⓜ GENERATORS
Ⓢ SYNCHRONOUS
CONDENSERS

(b)

FIGURE 2: (a) IEEE 14-bus case, the attack sensor set S_{11} is selected for the 5-sparse undetectable attack case; (b) IEEE 30-bus case, the attack sensor set S_{19} is selected for the 5-sparse undetectable attack case.

FIGURE 3: Comparison of the validity of linearity assumptions with varying levels of SNRs. (a) With only Gaussian noise; (b) with Gaussian noise and outliers; (c) with Gaussian noise and outliers (outliers eliminated).

differences in two different systems especially in IEEE 30-bus system (in Figure 4(b), the 10th measurement for the yellow line is nonzero, while the 10th measurement for the red line is nonzero). It means that the improved ICA-based attack may be more easily detected than the EID attack. In other words, the EID attack strategy achieves a better performance than the improved ICA-based attack strategy in constructing perfect sparse attack vectors. Due to sensor failures, communication errors, or data loss, gross errors are ubiquitous in power grid measurements, so we considered both Gaussian noise and outliers in the experiment. The

intercepted data was first preprocessed by ALM method to remove the outliers (Figure 5 is the approximation of the real measurement matrix by separating the outliers in only a single sparse error case).

Then, the attack performance by the missed detection probability (MDP) was evaluated. We set the whole numbers of Monte Carlo runs as 10000. In every Monte Carlo experiment, the Bad Data Detection approach is applied to discover the missed detection cases. A missed detection event happens if $\max_j (|r_j| / \sqrt{\text{cov}(r_j)}) \leq \nu$, where τ is a predefined threshold changing from 0.1 to 1.0. It can be seen from Figure 6 that

FIGURE 4: Comparison of designed sparse attack vectors in different cases. (a) 14-bus; (b) 30-bus.

FIGURE 5: The ALM approach estimates the real measurement matrix by dividing the gross errors. (a) The corrupted measurements with gross errors; (b) low-rank original matrix; (c) sparse error matrix.

the MDP rises as the threshold increases in both IEEE 14-bus and 30-bus systems under 3 different attack cases. Take IEEE 14-bus system as an example; when the EID attack strategy is used, the MDP is very close to the no attack case. In other words, it is difficult to distinguish the EID attack case from the no attack case, which implies that the EID attack is stealthy and undetectable to the Bad Data Detection. However, when the improved ICA-based attack strategy is used, the MDP is quite different from the no attack case as shown in Figure 6(a). It means that the Bad Data Detection has a high probability of detecting the attack based on the improved ICA-based attack strategy. Overall, the EID attack strategy has better performance than the improved ICA-based strategy. Similar results can also be observed in the IEEE 30-bus system.

Finally, we also evaluated the scalability of our work by using larger-scale test systems, including IEEE 118-bus system and 300-bus system, which have been widely used in research community. Since larger systems can cause longer execution time of the algorithm, we set the whole numbers of Monte Carlo runs as 10000 in test systems and record the execution time for carrying out the EID attack strategy. Table 2 shows the average execution time (total time of the three phases) in different test systems (regarding other

TABLE 2: The execution time of EID attacks in different test systems.

Test systems	Execution time (s)
IEEE 14-bus	2.3286
IEEE 30-bus	3.6167
IEEE 118-bus	5.1015
IEEE 300-bus	9.6467

indicators, the simulation results of the large systems and the above small systems are similar, and it is inconvenient to use figures to represent the simulation results of the large systems, so they are omitted). For all test systems, the attacker can construct corresponding sparse attack vectors based on the EID strategy with average execution time ranging from 2.3286 s to about 9.6 s. In fact, in the three stages of the EID attack strategy, the first stage (Eliminate: ALM method) takes up most of the execution time. From Table 1, we can conclude that even with larger-scale test systems, the average execution time is also acceptable for attackers. Of course, the EID attack strategy, especially the first stage of the strategy, still needs to be optimized to obtain sparse attack vectors faster.

FIGURE 6: Missed detection probability with the proposed attack strategy in different cases. (a) 14-bus; (b) 30-bus.

6. Conclusions and Future Work

In this paper, a data-driven sparse false data injection attack strategy was proposed. The proposed attack strategy can solve the problem of implementing the sparse attack without the system information matrix. The experimental results show that the strategy can successfully implement sparse attacks even in the presence of outliers. The next step is to study the defense strategy against this type of attack to deal with the threat of sparse false data injection attacks to improve the security of the power system.

Data Availability

The datasets used or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61272486).

References

- [1] N. Liu, J. Zhang, and X. Wu, "Asset analysis of risk assessment for IEC 61850-Based power control systems - Part II: Application in substation," *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 876–881, 2011.
- [2] 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. 21–32, 2011.
- [3] 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.
- [4] 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.
- [5] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proceedings of the Preprints of the First Workshop on Secure Control Systems (CPSWeek '10)*, Stockholm, Sweden, April 2010.
- [6] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 11, pp. 1–12, 2015.
- [7] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proceedings of the IEEE 2nd International Conference on Smart Grid Communications (SmartGridComm '11)*, pp. 244–248, Brussels, Belgium, October 2011.
- [8] Z. Yu and W. Chin, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 2015.
- [9] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: a data driven approach," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1102–1114, 2015.
- [10] E. J. Candes, X. Li, Y. Ma, and J. Wright, "Robust principal component analysis?" *Journal of the ACM*, vol. 58, no. 3, article 11, 2011.

- [11] A. Anwar and A. N. Mahmood, "Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors," in *Proceedings of the IEEE Power and Energy Society General Meeting (PESGM '16)*, pp. 1–5, July 2016.
- [12] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.
- [13] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 476–486, 2011.
- [14] Z. Lin, M. Chen, and Y. Ma, "Fast convex optimization algorithms for exact recovery of a corrupted low-rank matrix," UIUC Technical Report UILU-ENG 09-2214, 2009.
- [15] Z. Lin, M. Chen, and Y. Ma, "The augmented Lagrange multiplier method for exact recovery of corrupted low-rank matrices," IUC Technical Report UILUENG 09-2214, 2009.
- [16] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.
- [17] Y. Huang, M. Esmalifalak, H. Nguyen et al., "Bad data injection in smart grid: Attack and defense mechanisms," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 27–33, 2013.
- [18] T. JiWei, W. BuHong, S. FuTe, and L. Shuaiqi, "Stealthy false data injection attacks using matrix recovery and independent component analysis in smart grid," *IOP Conference Series: Materials Science and Engineering*, vol. 199, no. 1, 2017.
- [19] T. G. Kolda and B. W. Bader, "Tensor decompositions and applications," *SIAM Review*, vol. 51, no. 3, pp. 455–500, 2009.
- [20] P. Comon, X. Luciani, and A. L. F. de Almeida, "Tensor decompositions, alternating least squares and other tales," *Journal of Chemometrics*, vol. 23, no. 7-8, pp. 393–405, 2009.
- [21] L. De Lathauwer, J. Castaing, and J.-F. Cardoso, "Fourth-order cumulant-based blind identification of underdetermined mixtures," *IEEE Transactions on Signal Processing*, vol. 55, no. 6, part 2, pp. 2965–2973, 2007.
- [22] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER's extensible optimal power flow architecture," in *Proceedings of the Power & Energy Society General Meeting*, pp. 1–7, Calgary, AB, Canada, July 2009.