

Efficient Detection Method for Data Integrity Attacks in Smart Grid

Peixiu An and Zhitao Guan^(✉)

School of Control and Computer Engineering, North China Electric Power University,
Beijing 102206, China
{anpeixiu14717, guanzhitao}@126.com

Abstract. With the developing of the Smart Grid, false data injection attacks (FDIAs) as a typical data integrity attack successfully bypass the traditional bad data detection and identification, has a serious influence on the power system safe and reliable operation. State estimation, which is an important process in smart grid, is used in system monitoring to get optimally estimate the power grid state through analysis of the monitoring data. However, FDIAs compromising data integrity will lead to wrong decision makings in power dispatch or electric power market transactions. In this paper, focusing on the power property, we introduce an index to quantitatively measure the node voltage stability and reflect the influence of FDIAs on the power system. Then, we use an improved clustering algorithm to identify the node vulnerability level, which helps operators take measures and detect the false data injection attacks timely. Besides, one effective state forecasting detection method is proposed, which is meaningful for real-time detection of false data injection attacks. Finally, the simulation result verifies the effectiveness and performance of the proposed method.

Keywords: Smart grid · Voltage stability · False data injection attacks · Cyber security · State estimation

1 Introduction

In recent years, the industrial control system and the power system automation, intelligent level continuous improvement make the power system rapidly develop. It also makes the grid security defense face more severe challenges at the same time [1–3]. By tampering the estimated value of power system state estimation, the false data injection attacks (FDIAs) would mislead control center to make wrong decisions and consequently impact severely on the grid's stability and reliability. Unconsciously, the FDIAs become one of the focuses of current researchers [4–8]. For this serious vulnerability, how to detect and identify the FDIAs has attracted a lot of attention among researchers. Although there are lots of articles about the FDIAs, most of the existing FDIAs detection methods rarely consider the impact of false data injection attacks on the power system. They ignore the connection of the FDIAs and the power system physical properties. However, for the system operators, it is an effective way that analysis the physical properties of power system to improve the detection and protection ability for FDIAs.

For a given initial operating condition, the voltage stability reflect the ability of power system that regaining state operating equilibrium after being subjected to a physical disturbance [9]. It is very convenient that system operators use fast, simple and correct methods to monitor the proximity of voltage collapse of a power system. Moreover, the node voltage stability can quantitatively measure the stability and reflect the impact of false data injection attacks on the power grid. So, we study and analyze this physical property of power system. We also construct the relationship between the false data injection attack and the node voltage stability to identify the vulnerability level of each node in the complex system, which can help power operators to targeted detection and take the corresponding protective measures timely.

In this paper, we present an efficient detection method against FDIAs. And the main contributions of this paper can be summarized as the following:

We study and analyze the physical property of power system and introduce an index to quantitatively measure the impact of false data injection attacks on the power system. We also construct the relationship between the false data injection attacks and the node voltage stability to identify the vulnerability of each node in the complex system;

According to the value of the node voltage stability, we use the improved clustering method to cluster the nodes into three different clusters. As the result of clustering, the nodes with similar vulnerability level get together for a cluster;

We use the effective state forecasting method to obtain state prediction and detect the false data injection attacks. Besides, we simulate the tests on the IEEE 30-bus systems to verify the effectiveness and performance of the proposed method.

2 Related Work

False data injection attacks (FDIAs), a new typical data integrity attack which is one of the most threatening cyber-attacks in smart grids, is presented firstly in [10]. For this serious vulnerability, many smart algorithms are applied to detect the FDIAs [11], such as geometrically designed residual filter, the generalized likelihood ratio test [4]. And the cumulative sum (CUSUM) test-based detection mechanism introduced in [12–14] is also designed for these stealth attacks. The researchers of [15] use the machine learning method to deal with the stealth false data. Moreover, how to economically deploy PMUs to facilitate the state estimator and detect the FDIAs has become an interesting problem [16, 17]. In [18], a detection method based on the PMU is proposed, the authors assume that the measuring of a portion in the system is absolute secure under the protection of the secure physical parts, and the attackers couldn't tamper the protected meters, otherwise it will be detected as an attack and carry on a limit to the attackers' behavior. Later, with the power systems increasingly interconnected in the smart grid, distributed state estimate (DSE) becomes an important alternative to centralized and hierarchical solutions [19, 20]. In [21], two new methods of distributed state estimation are proposed, one is using the incremental mode of cooperation, and the other is based on diffusive interaction pattern. The authors of [22, 23] apply the distributed state estimation (DSE) into the fully distributed power system for attack detection. In [24], a bad data detection method based on an extended distributed state estimation (EDSE) is presented. A power

system is decomposed into several subsystems using graph partition algorithms. For each subsystem, buses are classified into three groups: internal bus, boundary bus and adjacent bus. Simulation results demonstrate that the detection accuracy of the EDSE-based method is much higher than the traditional method on average, and its computation complexity is significantly lowered.

Nowadays, various methods have been proposed to address the problems of false data injection attacks in Smart Grid. However, the study of the physical property and analyzing networks data to detect the false data injection attacks is very meager. So, we study the corresponding work in this paper.

The rest of this paper is organized as follows. In Sect. 3, the system model and background are discussed. The proposed node vulnerability level identification is shown in Sect. 4. The state forecasting method is discussed in Sect. 5. We simulate the test and the effectiveness and performance of the proposed model and detection method are evaluated in Sect. 6. Finally, the paper is concluded in Sect. 7.

3 System Model and Background

In this section, we briefly discuss the state estimation in power system and the node voltage stability index.

3.1 Notations

In order to check the convenience, some important notations used in our paper are listed in the Table 1.

3.2 Problem Formulation

In our work, we present a common formulation of the state estimation problem when using a DC power flow. The measurements vector z is an $m \times 1$ vector in a power system such as power flows at transmission lines, and power injections and loads at buses. The power flow measurements can be taken at one or both ends of a transmission line. In the progress of state estimation, we are interested in using the collected set of measurements to estimate an $n \times 1$ vector x of unknown state variables, where $m \geq n$. The unknown state variables are the voltage angles or voltage magnitudes at different nodes. H denotes the $m \times n$ measurements Jacobian matrix.

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

Where, the e is the measurement noise. And the noise is normally Gaussian distributed with zero mean, then the estimated state variables can be express as:

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

Where the W is a diagonal matrix whose diagonal elements are given by $W_{ii} = \delta_i^{-2}$, and δ_i^2 is the variance of e_i , for $i = 1, 2, \dots, n$.

Table 1. Some important notations

Notation	Description
z	The $m \times 1$ vector of measurements
x	The $n \times 1$ vector of state variables
H	The $m \times n$ Jacobian matrix denoting the power system topology
e	Random errors of measurements
m	The number of measurements
n	The number of state variables
\hat{x}	The estimated value of state variables
W	The diagonal matrix
z_f	The $m \times 1$ measurements vector with false data
a	The $m \times 1$ attacked vector
c	The $n \times 1$ vector of estimated errors
\hat{x}_f	The estimated value of state variables with false data
τ	The threshold
r	The measurement residuals
$NVSI(N_i)$	The voltage stability index at the node i
U_j	The voltage magnitude of node j
R	The resistance of branch
X	The reactance of branch
P_i	The real power of node i
Q_i	The reactive power of node i
s	The population size of the CFPSO
K	The number of the centroids
F_{sum_dis}	The total sum of the distance of each particle to the centroid
G_{t-1}	The state transition matrix at time sample $t - 1$
Q_{t-1}	The nonzero diagonal matrix at time sample $t - 1$
\widehat{z}_t	The forecasting measurements at sample t

In the FDIAs, an adversary try his/her best to hack the readings of sensors such that the vector of measurement z is replaced by a compromised vector $z_f = z + a$, where the a is a $m \times 1$ attack vector. The attacker constructs the attacked vector a to be a linear combination of the rows in matrix H , i.e., $a = Hc$ for some arbitrary $n \times 1$ vector c , then the traditional detection methods based on residue test will not be able to detect the attack since the injected false data will no longer affect the residue:

$$\begin{aligned}
\| r \| &= \| z_f - H\hat{x}_f \| \\
&= \| z + a - H(\hat{x} + c) \| \\
&= \| (z - H\hat{x}) + (a - Hc) \| \\
&= \| z - H\hat{x} \| < \tau
\end{aligned} \tag{3}$$

and

$$\begin{aligned}\hat{x}_j &= \hat{x} + (H^T WH)^{-1} H^T WHc \\ &= \hat{x} + c\end{aligned}\quad (4)$$

By using the knowledge of the line admittances and the power topology, the adversary can successfully implement false data injection attacks which not be detected by the traditional detection methods. But the attacked vectors to the measurements cause the deviation of the state estimation, and this will lead to the grid power collapse or paralysis.

3.3 Node Voltage Stability Description

As we all know, many methods and techniques have been reported for voltage stability analysis and voltage collapse prediction. A number of static voltage stability index have been widely used for evaluating and predicting the proximity of the system to voltage stability. In our paper, we introduce the node voltage stability index (*NVSI*) presented by the authors in [25], as follows,

$$NVSI(N_i) = 4U_j^{-4}(RQ_i - XP_i)^2 - 4U_j^{-2}(XQ_i + RP_j) \quad (5)$$

where the $NVSI(N_i)$ is the voltage stability index at the node i , U_j is the voltage magnitude of node j . R and X are the resistance and reactance of branch respectively, which can be obtained from the power network electric topological database. Besides, P_i , Q_i are the summation of the real power and reactive power. After a successful power flow solution of system, all parameters of Eq. (5) are known, and the $NVSI(N_i)$ index of each node can be calculated. This index can provide important information about the proximity of the system stability, which enables us to set an index threshold to monitor and predict system stability on-line so that a proper action can be taken to prevent the system from collapse timely and detect the false data in smart grid.

4 Node Vulnerability Level Identification

For real-time or extended real-time operation, the electricity operator collects power data from the SCADA. If an attacker has access to any or all of the measurements, he will manipulate the power data by injecting false data. When the measurements under FDIAs, the corrupted real and reactive power measurements, P_i , Q_i and U_j will be changed. Any higher value of the *NVSI* indicates that the system is highly likely to voltage collapse. So, the system operators should become concerned about keeping the system with instability margin.

In the light of the *NVSI* values of all monitored nodes, we can identify the weakest nodes of the system. The *NVSI* at the weakest node will be very large when the system approaches its voltage collapse point. Therefore, a threshold of *NVSI* can be easily set up to trigger an emergency remedial action scheme to remind the operator to detect the FDIAs and take appropriate measures protecting the system from voltage collapse.

Clustering algorithms are often used to measure the similarity between different data sources and to classify the data sources into different clusters. K-means++ algorithm is an efficient and well know unsupervised clustering algorithm which has a wide range of applications. However, a major problem of K-means++ is that it may trap in one of the local minima algorithm. In our work, we use the CFPSO algorithm to optimize that imperfection. At the beginning, we set the K-means++ algorithm is replicated $s/2$ times, where s is the population size of the CFPSO. We obtain the cluster centroids from the replicated K-means++ algorithm and use them as half of the initial population of the swarm. Besides, the remaining half swarm population are initialized randomly based on the solution space. In this way, the remaining half input vectors of the swarm still be capable to produce enough diversity in the velocities of the particles to reach to a better solution. In order to identify the nodes vulnerability level, we set $K = 3$. So the nodes will be clustered into 3 clusters, which indicates three vulnerability levels, the most vulnerable level, the vulnerable level and the stable level separately. In our analysis, we formulate the total sum of the distance of each particle to the centroids considered as a objection function F_{sum_dis} .

At the beginning of identifying the nodes vulnerability level, it is a key problem that how to get the best quality clustering centroid. The step-by-step procedure of the proposed solution is described briefly in Fig. 1.

Then the following steps describe the vulnerability identification procedure:

- Read the system data and calculate of each node;
- Obtain the best quality clustering centroid from above progress, and cluster the nodes into three swarm according the value;
- Identify the nodes vulnerability level of three swarms. The most vulnerability level, the vulnerability level and the stable level separately.

We simulate experiment at the IEEE 30-bus at one moment, and the result of node vulnerability level in Table 2.

Table 2. The node vulnerability level of IEEE 30-bus system

The number of swarm	Vulnerability level	The number of node
Swarm 1	The most vulnerability level	7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 26, 27, 28, 29, 30
Swarm 2	The vulnerability level	4, 5, 6, 23, 24, 25
Swarm 3	The stable level	2, 3, 19, 20, 21, 22

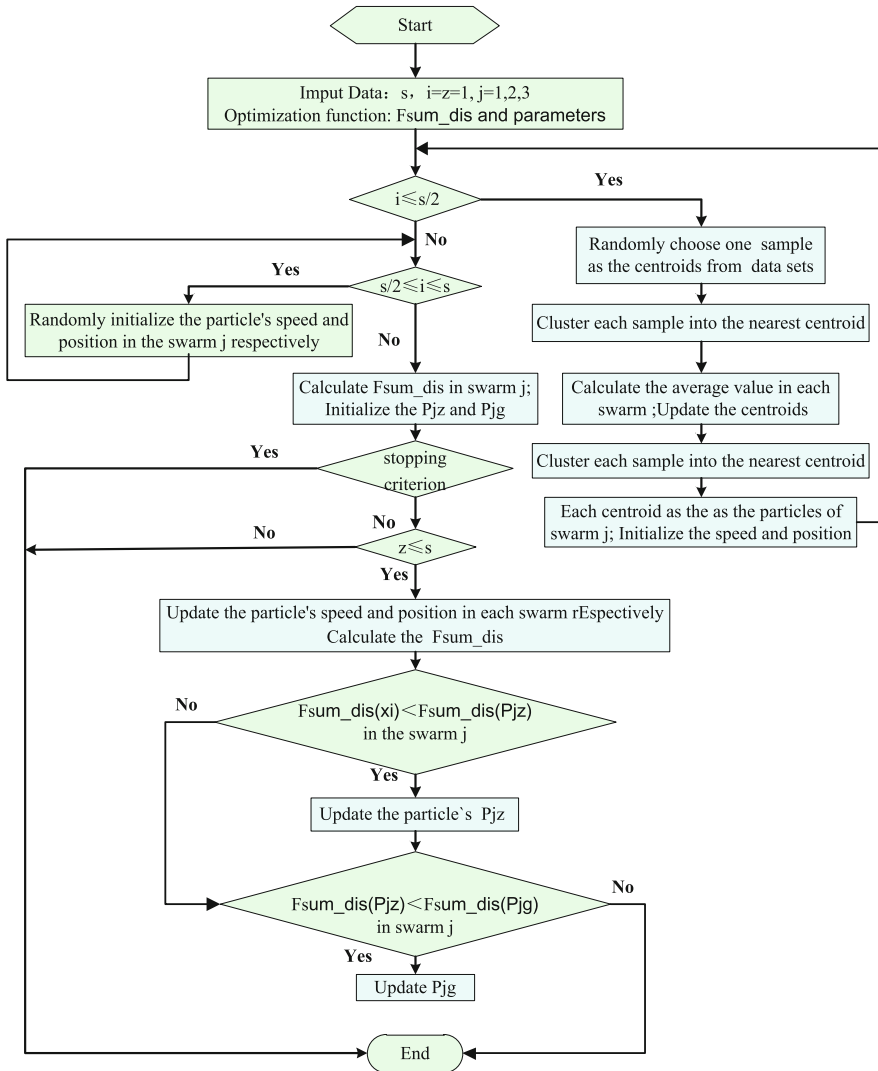


Fig. 1. The procedure of obtaining the centroids

5 State Forecasting Method

The main advantages of identifying the nodes vulnerability level are convenient in modeling and calculations, and ease in real time or on-line applications. The clustering results show that the nodes vulnerability level can reflect the weakest nodes causing system instability, but also help the operators detect the FDIAs. Combining this feature, we propose a new detection method considering two consecutive time frames from to forecast the state of power system and detect the FDIAs.

In the quasi steady state operation of the power system, we can obtain the prediction model by using the historical data and the state estimation. And the forecasting model is

$$x_t = G_{t-1}x_{t-1} + Q_{t-1} \quad (6)$$

Where G_{t-1} is state transition matrix, x_{t-1} is state estimated value at time sample $t - 1$ and the Q_{t-1} is nonzero diagonal matrix. Sampling time is at $t - 1$ and t separately. Hence, we can calculate the forecasting measurements as:

$$\widehat{z}_t = Hx_t \quad (7)$$

The measurement residuals at is

$$r = Hx - \widehat{z}_t = z - \widehat{z}_t \quad (8)$$

where z is estimated value at t , the \widehat{z}_t is the forecasting measurements using the data at t . In order to simplify the complexity of the formula, we will omit time scale t in the following work.

6 Simulation

In this paper, the proposed method is tested on IEEE 30-bus. The experiment model is constructed in the MATPOWER [26], and the test data is obtained from it. We use the $J(x)$ detector and LNR detector with our power system physical property for detecting the FDIAs to prove the performance. We construct the attacked vectors using the similar way in [12, 13].

We compare the $J(x)$ detector and the LNR detector with our method to see the effectiveness at different false alarm. In the Fig. 2, the ROC shows the trade-off between the probability of attack detection at different probability of false alarms. In our method, if the historical state data is available, the state forecasting is performed.

From the Fig. 2, we can find that the detection rate is gradually increased with the change of false alarm. The $J(x)1$ indicates the detection rate of traditional detect method, and the $J(x)2$ shows the detection rate of our method. Similarly, $LNR1$ and $LNR2$ denote the traditional and our method respectively. On the other hand, we can see that the detection rate of the LNR detector is higher than the $J(x)$ detector.

In a word, according to the node voltage stability index, we can identify the node vulnerability level. After that, we focus on the most vulnerability level firstly, and it help operators take efficient measures timely. State forecasting make operators determine whether exist any false data at time sample t . Finally, the simulation result verifies that the proposed mechanism can effectively detect FDIAs in the smart grid.

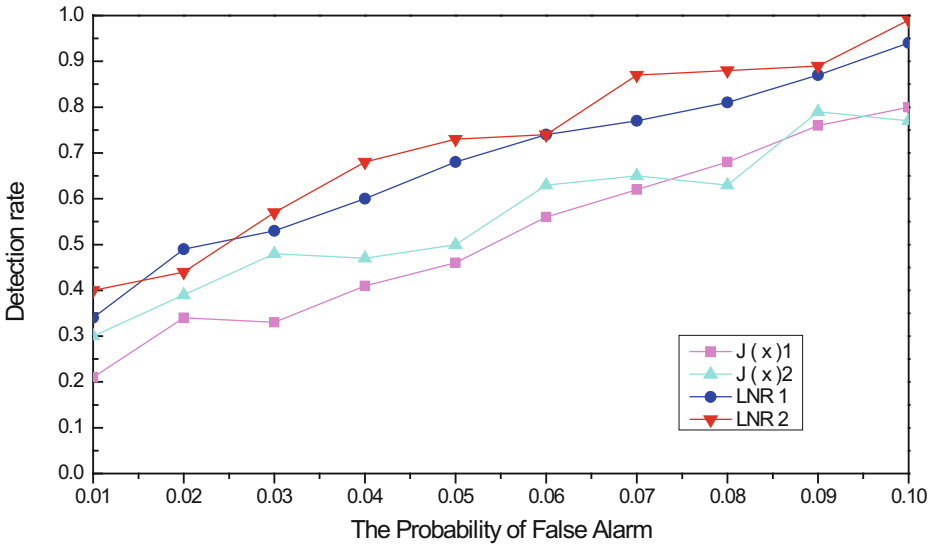


Fig. 2. The detecting results in IEEE 30-bus system

7 Conclusion

To deal with the problem of data integrity in smart grid, which may lead to wrong decision makings in power dispatch or electric power market operations, we propose an efficient FDIAs detection scheme based on power system physical property. Firstly, we analysis the power system and introduce the node voltage stability index to identify the vulnerability level of nodes in power system. As the result, we define three levels to cluster the system nodes into three swarms. In the progress of clustering, we use the improved cluster algorithm and realize the nodes clustering. This step help us to find the suspected false data injection points easily. Then we use the state forecasting method to obtain the states of power system. In addition, the and test methods are used to find the sensitive measurement vectors. In the simulation, we built different types of attack vectors, which makes an abundant experimental results. Finally, the simulation result verifies that the proposed mechanism can effectively detect FDIAs in the smart grid.

Acknowledgments. This work is partially supported by Natural Science Foundation of China under grant 61402171, Central Government University Foundation under grant JB2016045.

References

1. Fang, X., Misra, S., Xue, G., et al.: Smart grid—the new and improved power grid: a survey. *IEEE Commun. Surv. Tutorials* **14**(4), 944–980 (2012)
2. Kayastha, N., Niyato, D., Hossain, E., et al.: Smart grid sensor data collection, communication, and networking: a tutorial. *Wirel. Commun. Mob. Comput.* **14**(11), 1055–1087 (2014)

3. Liu, T., Sun, Y., Liu, Y., et al.: Abnormal traffic-indexed state estimation: a cyber–physical fusion approach for Smart Grid attack detection. *Future Gener. Comput. Syst.* **49**, 94–103 (2015)
4. Pasqualetti, F., Dörfler, F., Bullo, F.: Cyber-physical attacks in power networks: models, fundamental limitations and monitor design. In: 2011 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), pp. 2195–2201. IEEE (2011)
5. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: *ACM Conference on Computer and Communications Security*, pp. 21–32. ACM (2009)
6. Guan, Z., An, P., Yang, T.: Matrix partition-based detection scheme for false data injection in smart grid. *Int. J. Wirel. Mob. Comput.* **9**(3), 250–256 (2015)
7. Guan, Z., Sun, N., Xu, Y., et al.: A comprehensive survey of false data injection in smart grid. *Int. J. Wirel. Mob. Comput.* **8**(1), 27–33 (2015)
8. Asada, E.N., Garcia, A.V., Romero, R.: Identifying multiple interacting bad data in power system state estimation. In: 2005 IEEE Power Engineering Society General Meeting, pp. 571–577. IEEE (2005)
9. Zabaoui, T., Dessaint, L.A., Kamwa, I.: Preventive control approach for voltage stability improvement using voltage stability constrained optimal power flow based on static line voltage stability indices. *IET Gener. Transm. Distrib.* **8**(5), 924–934 (2014)
10. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **14**(1), 13 (2009)
11. Cui, S., Han, Z., Kar, S., et al.: Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions. *Sig. Process. Mag. IEEE* **29**(5), 106–115 (2012)
12. Kosut, O., Jia, L., Thomas, R.J., et al.: Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2**(4), 645–658 (2011)
13. Huang, Y., Esmalifalak, M., Nguyen, H., et al.: Bad data injection in smart grid: attack and defense mechanisms. *IEEE Commun. Mag.* **51**(1), 27–33 (2013)
14. Li, S., Yilmaz, Y., Wang, X.: Quickest detection of false data injection attack in wide-area smart grids. *IEEE Trans. Smart Grid* **6**(6), 2725–2735 (2015)
15. Esmalifalak, M., Nguyen, N.T., Zheng, R., et al.: Detecting stealthy false data injection using machine learning in smart grid. In: 2013 IEEE Global Communications Conference (GLOBECOM), pp. 808–813. IEEE, (2013)
16. Bi, S., Zhang, Y.J.: Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Trans. Smart Grid* **5**(3), 1216–1227 (2014)
17. Bobba, R.B., Rogers, K.M., Wang, Q., et al.: Detecting false data injection attacks on dc state estimation. In: *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010* (2010)
18. Giani, A., Bitar, E., Garcia, M.A., et al.: Smart grid data integrity attacks. *IEEE Trans. Smart Grid* **4**(3), 1244–1253 (2013)
19. Kim, T.T., Poor, H.V.: Strategic protection against data injection attacks on power grids. *IEEE Trans. Smart Grid* **2**(2), 326–333 (2011)
20. Kekatos, V., Giannakis, G.: Distributed robust power system state estimation. *IEEE Trans. Power Syst.* **28**(2), 1617–1626 (2013)
21. Ozay, M., Esnaola, I., Vural, F.T.Y., et al.: Distributed models for sparse attack construction and state vector estimation in the smart grid. In: 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp. 306–311. IEEE (2012)

22. Yang, J., Yu, R., Liu, Y., et al.: A two-stage attacking scheme for low-sparsity unobservable attacks in smart grid. In: 2015 IEEE International Conference on Communications (ICC), pp. 7210–7215. IEEE (2015)
23. Gu, Y., Liu, T., Wang, D., et al.: Bad data detection method for smart grids based on distributed state estimation. In: 2013 IEEE International Conference on Communications (ICC), pp. 4483–4487. IEEE, (2013)
24. Cramer, M., Goergens, P., Schnettler, A.: Bad data detection and handling in distribution grid state estimation using artificial neural networks. In: 2015 IEEE Eindhoven PowerTech, pp. 1–6. IEEE (2015)
25. Jasmon, G.B., Lee, L.: New contingency ranking technique incorporating a voltage stability criterion. In: IEEE Proceedings of C-Generation, Transmission and Distribution, vol. 140, no. 2, pp. 87–90. IET (1993)
26. MATPOWER (2015). <http://www.pserc.cornell.edu/matpower/>