Customized Attack Detection Under Power Industrial Control System

Bin Wang[1], Ling He[1], Huiting Yang[1], Feng Li[1], and Jie Fan[2(✉)]

[1] State Grid XinJiang Electric Power Co. Ltd., Electric Power Research Institute, Xinjiang, China
331657859@qq.com, 355080044@qq.com, 731613043@qq.com, 252491552@qq.com
[2] Global Energy Interconnection Research Institute Co. Ltd., Nanjing, China
fanjie@geiri.sgcc.com.cn

Abstract. With the rapid development of information technology, the power system already has the typical characteristics of the information physical fusion system. The power industrial control system is widely used in the power industry. While improving the efficiency, the economic benefits have also been greatly improved. However, the dependence on information technology has also increased the vulnerability to malicious attacks. Power industry control system is facing a more serious threat. In this paper, we combine anomaly detection and data dimensionality reduction to propose a feature extraction method for iForest power measurement data, which not only ensures the targeting of attack detection in the data processing stage, but also takes into account the data quality of feature extraction. In addition, we use deep learning techniques to identify attack behavior characteristics and use captured features to detect attack behavior in real time. We prove the availability of the method through simulation of the IEEE 118-bus power systems.

Keywords: Power industrial control system · Deep learning · iForest

1 Introduction

With the deep integration of informatization and the rapid development of the Internet of Things, more and more information technology is applied to the industrial field, and the power industrial control system is facing the threat of cyber attacks [1].

The power industry control system is an important part of the country's critical infrastructure, covering power monitoring systems such as power plants, substations, and distribution automation systems [2]. However, the existing security protection methods cannot meet the new trend of intelligent and interactive development of industrial control systems [3–5]. Some provincial power companies have begun to introduce new methods and ideas in some production processes to build an industrial control system security system, forming a complete

Supported by organization State Grid XinJiang Electric Power Co. Ltd., Electric Power Research Institute.

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2020
Published by Springer Nature Switzerland AG 2020. All Rights Reserved
D.-J. Deng et al. (Eds.): SGIoT 2019, LNICST 324, pp. 96–106, 2020.
https://doi.org/10.1007/978-3-030-49610-4_8

set of security early warning mechanisms for industrial control systems. However, in order to fundamentally solve the problem of network security of power industrial control systems, it is necessary to model for network intrusion and attack behavior [6]. It is also necessary to combine the operational characteristics of the power industrial control system to build a well-featured network intrusion behavior signature database.

The research on network intrusion of power industrial control system is divided into two aspects [7]. One is for the typical vulnerabilities in the power industrial control protocol, and the other is to analyze the types of industrial control protocols involved in the business in combination with the business scenario. Among them, the threat of attack is a possible factor or event that has potential damage to the organization or assets. Generally speaking, the attack methods for power industrial control systems, including distributed data tampering, forgery control commands, and other advanced and customized attacks closely integrated with business logic, have strong concealment and complexity [8,9].

In 2009, Yao Liu et al. [10] first proposed the basic concepts and related theories of False Data Injection Attacks (FDIA) and conducted simulation experiments. Literature [11–13] studied how to launch FDIA attacks through local parameter information of local power systems. In addition to FDIA attacks based on DC power systems, literature [14] studied the false data injection attacks based on AC power systems. The above research is mainly aimed at the false data attack in static state estimation. Literature [15] studied the false data attack in the dynamic Kalman filter algorithm, proposed an effective attack model, and analyzed the impact of the attack on the state estimation result.

In this paper, we comprehensively consider the above situation, combine anomaly detection and data dimensionality reduction, and propose a feature extraction method for iForest power measurement data. It not only ensures the targeting of attack detection in the data processing stage, but also takes into account the data quality of feature extraction [16]. In addition, we use deep learning techniques to identify attack behavior characteristics and use captured features to detect attack behavior in real time. The main contributions of this paper are listed as follows.

- We use the advantages of isolated forest (iForest) and local linear embedding (LLE) in anomaly detection and data dimensionality reduction, and innovatively combine abnormal score extraction and data dimensionality reduction.
- We design a real-time Deep Learning Based Identification (DLBI) based on deep learning mechanism to detect false data bypassing the traditional bad data detection mechanism.
- In response to our proposed false data attack detection mechanism, we conduct a simulation experiment. Then we compare them with ANN-based and SVM-based false data attack detection mechanisms to test the detection accuracy and efficiency.

The remainder of this paper is organized as follows. In Sect. 2, we briefly introduce a unified preprocessing method for power measurement data. In Sect. 3, we introduce an attack detection mechanism based on deep learning. In Sect. 4, we deploy IEEE 118-bus system in the environment and carry out simulation experiments. Finally, in Sect. 5, we conclude this work and make plans for the future.

2 Uniform Preprocessing of Measurement Data

In this section, we consider that the power system, especially the large complex network, has a high measurement data dimension and the data structure is mostly non-linear. Although the linear dimension reduction method is simple to implement, the effect is not good [17]. At the same time, the individual data dimension reduction will ignore the change of data distribution and abnormal characteristics after the injection attack, resulting in the lack of pertinence of feature extraction [18]. Therefore, we propose an abnormal score extraction method based on Isolation Forest (iForest) as an independent feature, and then use the nonlinear feature extraction scheme of Locally Linear Embedding (LLE).

2.1 Outlier Extraction Based on Isolated Forest

A well-designed false data injection attack can successfully evade the state estimation detection mechanism and invalidate the traditional anomaly detection algorithm. In addition, the power measurement data is increasing rapidly and is already in the category of big data. If we directly use clustering and correlation algorithms to detect abnormal data, it will generate a huge amount of computation, and real-time and accuracy cannot be guaranteed. Based on the iForest algorithm, this paper establishes the iForest anomaly score equation of physical data to realize the feature extraction of the physical system. It has the characteristics of shorter calculation time and higher detection stability, and is suitable for large-scale and high-complexity power measurement data, which meets the requirement of all-weather real-time performance of attack detection.

Building iTree and iForest For the power measurement data set D_p containing n data samples x and φ features f, the establishment of iForest is composed of multiple isolated trees iTree. As a random binary tree, the establishment process of iTree is as follows:

Step1: Select a feature P randomly from the power measurement data set D_p;

Step2: Randomly selecting a single value Q in feature P;

Step3: According to the feature P, binary log segmentation is performed for each record. If any record in the attribute P is $R < Q$, the record is placed in the left child node, and if $R \geq Q$, it is placed on the right child node;

Step4: Recursively construct the left child node and the right child node to construct a binary tree until each sample is isolated or the height of the tree reaches a defined height to form an iTree.

Isolated Forest iForest consists of a large number of iTree trees. The establishment process is a random sampling process. The establishment process is to sample the measurement data set D_p multiple times, and obtain a plurality of sub data sets, and respectively establish multiple iTree according to the sub data sets to form iForest.

Output Outlier Feature After the establishing of iTree and iForest, the abnormal score of each measurement data can be output. For a power measurement data sample x, the calculation principle of the abnormal score is the average traversal depth of all iTrees. For the quantification of the detection sample x at each iTree traversal depth, define the following anomaly score quantization equation:

$$c(\mu) \begin{cases} 2H(\mu-1) - (2(\mu-1)/n), & \mu > 2 \\ 1, & \mu = 2 \\ 0, & \mu < 2 \end{cases} \tag{1}$$

$$H(t) = \ln(t) + \xi \tag{2}$$

The iForest exception score for each physical data x can be expressed as:

$$iscore(x) = 2^{\frac{-E[h(x)]}{c(\mu)}}, \tag{3}$$

where ξ is the Euler constant, $h(x)$ is the path length of x, that is, the sum from the root node to the edge of the isolated node, and $E[h(x)]$ is the mean of the path lengths on all iTrees. When iscore(x) approaches 0.5, the higher the normality, the higher the degree of abnormality when it tends to 1. In the detection of false data injection attacks, we use the abnormal score iscore(x), which is quantized by outliers, as an independent feature of attack detection. The power measurement data after extracting the abnormal score still has high latitude and strong noise. The problem requires further feature extraction.

2.2 Power Measurement Data Dimensionality Reduction Method

After extracting the abnormal score of the measured data in the previous section, it is regarded as an independent feature, and further data reduction is needed for the high-dimensional measurement data. In this paper, we use nonlinear local linear embedding and linear principal component analysis to measure feature data.

Nonlinear Local Linear Embedding. Local linear embedding (LLE) is an unsupervised dimensionality reduction method for nonlinear structural data. For global nonlinear structures, LLE considers each data point in its neighboring data points in a local linear structure, constructing a local reconstruction weight matrix. While maintaining the nonlinear structure of the global high-dimensional space, the low-dimensional mapping of high-dimensional data is sought to achieve data dimensionality reduction. The implementation process is as follows:

(1) In the original high-dimensional data, for each data point x_i, artificially specify the nearest k ($k < N$) points as the neighboring points, and calculate the distance between x_i and the adjacent points in turn, as follows:

$$d_{ij} = \sqrt{\sum \left(x_{ik} - x_{jk}\right)^2} \tag{4}$$

(2) Define the local reconstruction weight matrix W. In each local range, the sample point and the adjacent point can be approximated as a linear structure, then there is an error $P(W)$, and the following objective function is established to minimize the error:

$$\begin{array}{l} \min P(W) = \sum_{i=1}^{N} \left| x_i - \sum_{j=1}^{k} w_{ij} x_{ij} \right|^2, \\ j = (1, 2, \cdots, k) \end{array} \tag{5}$$

where x_{ij} is the neighboring point of x_i, $\mathcal{W}ij$ is the weight between the sample points, and satisfies $\sum_{j=1}^{k} w_{ij} = 1$. The error for any point x_i is:

$$e = \left| x_i - \sum_{j=1}^{k} w_{ij} x_{ij} \right|^2 = \left| \sum_{j=1}^{k} w_{ij} \left(x_i - x_j\right) \right|^2 = \sum_{j=1}^{k} \sum_{m=1}^{k} w_{ij} w_{in} Q_{jm}^{i} \tag{6}$$

$$Q_{jm}^{i} = \left(x_i - x_j\right)^T \left(x_i - x_m\right) \tag{7}$$

Using the Lagrangian multiplier method, we obtain the following partial reconstruction weight matrix:

$$w_{ij} = \frac{\sum_{m=1}^{k} \left(Q^i\right)_{jm}^{-1}}{\sum_{p=1}^{k} \sum_{q=1}^{k} \left(Q^i\right)_{pq}^{-1}} \tag{8}$$

When Q^i is a singular matrix, regularize it:

$$Q^i = Q^i + rI, \tag{9}$$

where r is the regularization parameter and I is the identity matrix.

(3) Define the data points x_i and x_j in the high-dimensional space, and find the y_i and y_j projected to the low-dimensional space. The local weight matrix $\mathcal{W}ij$ remains unchanged to maintain the nonlinear structure of the high-dimensional space. The following objective function is established:

$$\min P(Y) = \sum_{i=1}^{N} \left| y_i - \sum_{j=1}^{k} w_{ij} y_{ij} \right|^2 = \sum_{i=1}^{N} \sum_{j=1}^{N} M_{ij} y_i^T y_j \tag{10}$$

Among them, the definition of M is as follows:

$$M = (I - W)^T (I - W) \tag{11}$$

At the same time, the objective function satisfies the following:

$$\begin{cases} \sum_{i=1}^{N} y_i = 0 \\ \frac{1}{N} \sum_{i=1}^{N} y_i y_i^T = I \end{cases} \tag{12}$$

Using the Lagrange multiplier method, we get:

$$MY^T = \lambda Y^T \tag{13}$$

As shown in the above formula, the solution of the high dimensional space in the low dimensional space can be obtained by means of feature decomposition, wherein the low dimensional solution Y is the eigenvector corresponding to the smallest eigenvalue in the M matrix.

iForest-LLE Feature Extraction Method. The feature data extraction for the false data injection attack, using the iForest method to extract the abnormal score, can detect most of the random tampering and part of the injection attack in the measured data. However, the well-designed false data injection attack will bypass the traditional state estimation of bad data identification. Therefore, it is necessary to further determine whether or not FDIAs are accepted by the machine learning classification method. This requires further data reduction for high-dimensional nonlinear power measurement data.

This paper combines the advantages of iForest in dealing with anomaly detection and LLE in dealing with dimensionality reduction of high-dimensional data attributes, and proposes the iForest-LLE power measurement data feature extraction method for false data injection attack detection. Figure 1 shows the algorithm flow.

For the power measurement data x, first extract the abnormal score iscore(x) of each data and use it as an independent feature, and then use LLE to perform dimensionality reduction on the high-dimensional measurement data with the specified dimension r. When the attack detection is performed, two characteristics are comprehensively calculated to perform classification decision, thereby defining the attack detection measurement data feature P:

$$P = [ID, iscore(x), f_1, f_2, \cdots, f_r], \tag{14}$$

where ID is the data sample number and iscore(x) is the iForest exception score, $[f_1, f_2, \cdots, f_r]$ is a new attribute of the power measurement data based on LLE dimension reduction.

3 Attack Detection Based on Deep Learning

In this section, we propose a false data detection mechanism based on deep learning mechanism (Deep Learning Based Identification (DLBI) to detect spurious data that bypasses traditional bad data detection mechanisms [19].

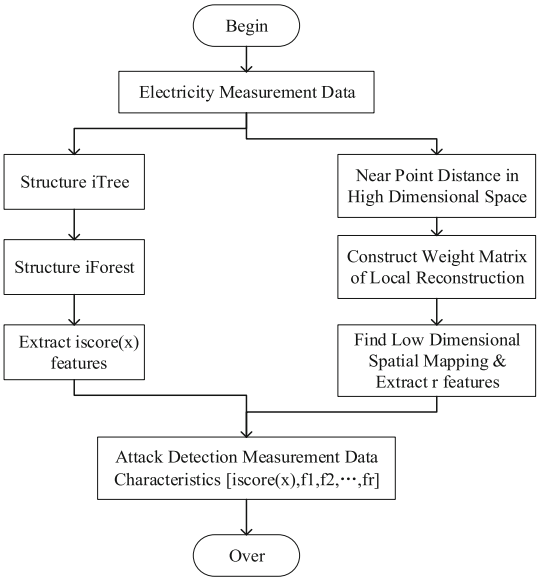


Fig. 1. The iForest-LLE feature extraction method.

3.1 DLBI Detection Method Design

The detection method flow is shown in Fig. 2. The proposed detection mechanism is mainly composed of the traditional State Data Estimator (SVE) and the Deep Learn Based Identification (DLBI) scheme [20]. As described in Eq. (15), the traditional bad data detection compares the critical value with the real-time data, and when the processing result exceeds the critical value (n $>$ τ), the attack alarm is triggered, and the collected data is considered to be infused with false data.

$$\begin{cases} \|z - Hx\|_2 > \tau \\ \|z - Hx\|_2 \leq \tau \end{cases} \tag{15}$$

When the processing result is within the critical value (n $<$ τ), the obtained measurement data is transmitted to the DLBI for further detection. In theory, the critical value τ should be within an appropriate range [21]. If τ is too small, the robustness of the traditional bad data detection system to environmental noise will be reduced to some extent, which may lead to excessive unobjectionable attack alarms [22]. On the other hand, if the value of τ is too large, it may have a large impact on the effectiveness of the traditional bad data detection system, and it will also cause a large load pressure on the subsequent DLBI system [23].

Based on Eq. (15), the measured value Z_a injected into the attack vector cannot be found by the traditional bad data detection mechanism, as described below:

$$\|z_a - Hx_{bad}\|_2 = \|z+a-H(x+c)\|_2 = \|z-Hx+(a-Hc)\|_2+\|a-Hc\|_2 \leq \tau \tag{16}$$

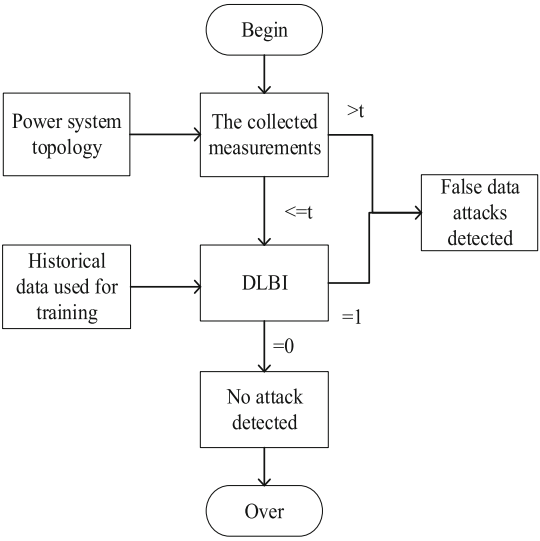


Fig. 2. Attack detection mechanism.

Let $\tau_a = \tau - \|z - Hx\|_2$, if $\|a - Hc\| \leq \tau_a$, false data attacks can bypass traditional bad data detection mechanisms [24]. Therefore, we can describe the sufficient conditions for a false data attack to bypass the traditional bad data detection mechanism as follows:

$$a = Hc + t, \tag{17}$$

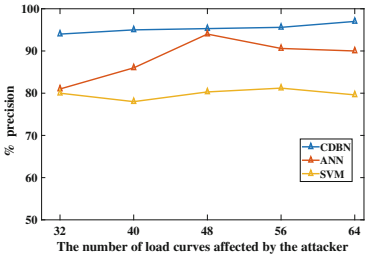
where H is the measured Jacobian matrix provided to the attacker, c and t are the measured values designed by the attacker, and $\|t\|_2 \leq \tau_a$. A false data attack that can be detected by the traditional bad data detection mechanism is called an observable false data attack, and a false data attack that cannot be detected by the traditional bad data detection mechanism is called an unobservable false data attack. In our proposed mechanism, DLBI is used to detect undetectable false data attacks.

4 Experiment Analysis

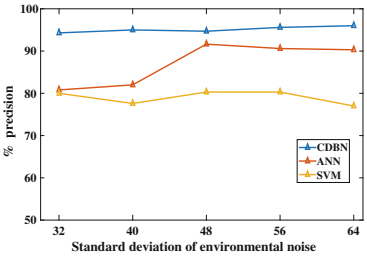
In this section, we evaluate the performance of DLBI through the IEEE-118 bus test system. In the 118 bus system, the state vector $x \in R^{118}$ consists of the voltage phase angle of each individual bus, and the measurement vector $z \in R^{490}$ consists of the measured values of the bus and the branch that are actually injected into the power system. In our simulation, we use complex load curves collected from real-world environments, only a portion of which was verified false data. In order to train enough false data to train the CBDN model in our proposed DLBI mechanism, we use Fourier transform and principal component

analysis to analyze the pattern of the confirmed false data. Considering that the attacker has limited resources under actual conditions, an attacker who can reasonably launch a false data attack can only tamper with a limited load curve. We assume that an attacker of a false data attack can only tamper with 64 bus of the IEEE-118 bus systems.

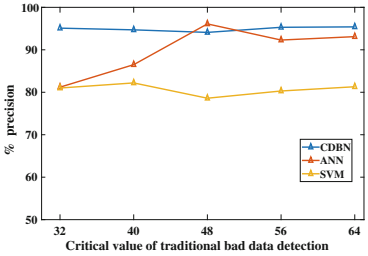
In order to verify the validity of our proposed CDBN structure, we compared the mechanism of using ANN and SVM as false data identification with our proposed CDBN mechanism. In the simulation experiment, the ANN consists of a hidden layer with 25 cells, and the SVM algorithm uses a Gaussian kernel function. In order to ensure fairness of comparison, we use the same amount of tag data in the training process of these three methods.



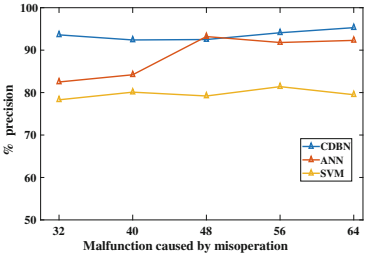
(a) The number of tamper-evident load curves.



(b) Environmental noise.



(c) Traditional bad data.



(d) Malfunction caused by misoperation.

Fig. 3. Comparison of experimental results of three algorithms.

We model the ambient noise as Gaussian white noise $\sim N(0, 0.5)$, set the threshold τ to 10, and consider the number of tamper-evident load curves $k = 32$, 40, 48, 56, 64. Our load curve is made up of 360 samples obtained by collecting power measurements every 4 min on the load bus. From each load curve consisting of 360 samples, we obtain 50 labeled data samples and 200 unmarked data samples for training the DLBI mechanism using CDBN. Figure 3 compares the detection accuracy of ANN-based and SVM-based detection mechanisms. From Fig. 3 we can see that our proposed detection mechanism achieves the highest detection accuracy among three different detection mechanisms. Our proposed

test solution has a strong environmental noise robustness. In addition, to a certain extent, it can avoid the detection impact caused by misuse.

5 Conclusion

In this paper, we aim at the problem that the depth of abnormal behavior detection in the power industrial control system is not high enough, and the ability to monitor the customized network attack combined with the industrial control business logic is insufficient. We propose a feature extraction method based on iForest, which realizes high-speed acquisition of real-time data of power industrial control system and unified preprocessing of different structures, dimensions and format data. And we also use the knowledge of deep learning to propose a DBN-based attack detection method to achieve accurate identification of network attacks in specific attack scenarios.

In order to test the attack detection mechanism, we deploy IEEE 118-bus system in the environment and carry out simulation experiments. The final results show that our proposed method has excellent performance.

The future work is mainly to strengthen the integration of power industrial control systems and detection mechanisms, and how to effectively detect advanced and customized attacks that are closely integrated with business logic, including distributed data tampering and forgery control commands.

References

1. Wang, K., Xu, C., Guo, S.: Big data analytics for price forecasting in smart grids. In: IEEE GLOBECOM 2016, Washington, USA, December 2016
2. Wang, X.Z., Ge, Z.Q., Ge, M.H., Wang, L., Li, L.: The research on electric power control center credit monitoring and management using cloud computing and smart workflow. In: 2018 China International Conference on Electricity Distribution (CICED), Tianjin, China, September 2018
3. Wang, Y., Wang, K., Huang, H., Miyazaki, T., Guo, S.: Traffic and computation co-offloading with reinforcement learning in fog computing for industrial applications. IEEE Trans. Industr. Inf. **15**(2), 976–986 (2019)
4. He, H., Liu, J.D., Jin, Y.K., Li, Z. Zhang, Z.R., et al.: Research on power quality control method of active distribution network with microgrids. In: 2018 3rd International Conference on Smart City and Systems Engineering (ICSCSE), Xiamen, China, December 2018
5. Wang, K., Ouyang, Z., Krishnan, R., Shu, L., He, L.: A game theory based energy management system using price elasticity for smart grids. IEEE Trans. Industr. Inf. **11**(6), 1607–1616 (2015)
6. Zhang, J., Chen, R., Xiao, L.S., Guo, X.C., Liu, B.: Optimal control for AC and DC power quality of VSC-HVDC. In: 2017 International Conference on Computer Systems, Electronics and Control (ICCSEC), Dalian, China, December 2017
7. Dong, X.M., Sun, H., Wang, C.F., Yun, Z.H., Wang, Y.M., et al.: Power flow analysis considering automatic generation control for multi-area interconnection power networks. IEEE Trans. Ind. Appl. **53**(6), 5200–5208 (2017)

8. Yu, J., Wang, K., Zeng, D., Zhu, C., Guo, S.: Privacy-preserving data aggregation computing in cyber-physical social systems. ACM Trans. Cyber Phys. Syst. **3**(1), 1–23 (2018). Article 8
9. Wang, Y., et al.: Coordinated recovery strategy of AC and UHVDC interconnected system considering the power grid strength. In: 2017 IEEE Conference on Energy Internet and Energy System Integration, Beijing, China, November 2017
10. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. **14**(1), 1–33 (2011)
11. Li, S., Yang, Y.M., Wang, X.: Quickest detection of false data injection attack in wide-area smart grids. IEEE Trans. Smart Grid **6**(6), 2725–2735 (2017)
12. Wang, K., Du, M., Yang, D., Zhu, C., Shen, J., Zhang, Y.: Game theory-based active defense for intrusion detection in cyber-physical embedded systems. ACM Trans. Embed. Comput. Syst. **16**(1), 1–21 (2016). Article 18
13. Liu, X., Li, Z.: Local load redistribution attacks in power systems with incomplete network information. IEEE Trans. Smart Grid **5**(4), 1665–1676 (2014)
14. Yang, L., Ding, C., Wu, M., Wang, K.: Robust detection of false data injection attacks for the data aggregation in Internet of things based environmental surveillance. Comput. Netw. **129**(2), 410–428 (2017)
15. Liu, X., Bao, Z., Lu, D.: Modeling of local false data injection attacks with reduced network information. IEEE Trans. Smart Grid **6**(4), 1686–1696 (2017)
16. Wang, K., et al.: Wireless big data computing in smart grid. IEEE Wirel. Commun. **24**(2), 58–64 (2017)
17. Hug, G., Giampapa, J.A.: Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid **3**(3), 1362–1370 (2012)
18. He, Y.B., Mendis, G.J., Jin, W.: Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans. Smart Grid **8**(5), 2505–2516 (2017)
19. Wang, K., Du, M., Maharjan, S., Sun, Y.: Strategic honeypot game model for distributed denial of service attacks in the smart grid. IEEE Trans. Smart Grid **8**(5), 2474–2482 (2017)
20. Ashrafuzzaman, M., Chakhchoukh, Y., Jillepalli, A.A., Tosic, P.T., et al.: Detecting stealthy false data injection attacks in power grids using deep learning. In: 2018 14th International Wireless Communications Mobile Computing Conference, Limassol, Cyprus, June 2018
21. Wei, L., Gao, D.H., Cheng, L.: False data injection attacks detection with deep belief networks in smart grid. In: 2018 Chinese Automation Congress (CAC), Xian, China, December 2018
22. Niu, X.Y., Li, J.N., Sun, J.Y., Tomsovic, K.: Dynamic detection of false data injection attack in smart grid using deep learning. In: 2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, February 2019
23. Wang, K., Du, M., Sun, Y., Vinel, A., Zhang, Y.: Attack detection and distributed forensics in machine-to-machine networks. IEEE Netw. **30**(6), 49–55 (2016)
24. Ding, Y.M., Li, K., Meng, Z.X.: CPS optimal control for interconnected power grid based on model predictive control. In: 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, October 2018