False Data Injection Attacks

Subjects: Engineering, Electrical & Electronic
Contributor: Zhengwei Qu

False data injection attacks (FDIAs), as a covert cyber-attack method, pose a huge challenge to the safe and stable operation of smart grids by illegally hacking into power systems to tamper with measurement data and thus undermine data integrity.

Keywords: false data injection attacks (FDIAs)

1. Introduction

In recent years, sensing, communication, and control technologies have been able to realize the seamless integration in smart grids. Hence, the physical and network fields of the power system are deeply integrated to form a cyber-physical system [1]. After collecting measurement data through remote terminal units (RTUs), the smart grid relies on the state estimation algorithm to achieve its regulation. Thus, the main purpose of cyberattacks is to undermine or to mislead the state estimation mechanism, leading to incorrect decision-making in the energy management system (EMS). In a highly complex and automated environment, a cyber-attack may propagate to the entire system, triggering grid paralysis, mass outage incidents, and so on, such as the massive power outage that occurred in Venezuela on 7 March 2019 [2].

False data injection attacks (FDIAs), as a covert cyber-attack method, pose a huge challenge to the safe and stable operation of smart grids by illegally hacking into power systems to tamper with measurement data and thus undermine data integrity [3][4][5]. In [6], Liu et al. first proposed the concept of FDIAs and mentioned that attackers can use power system topology and parameter information to construct a well- designed attack vector that bypasses traditional bad data detections (BDDs) and destroys the integrity of smart grid information. Since attackers can construct extremely hidden FDIAs without relying on system configuration information, it is difficult for traditional model-based detection methods and boundary protection systems to handle such FDIAs. In order to run the power grid safely and steadily, an effective FDIAs testing scheme needs to be studied and developed, which has been intensively studied by many researchers.

From the perspective of defenders, some methods have been improved for the state estimation algorithm in the study of FDIAs detection. The improved state estimation methods mainly include residual detection method [7], measurement transformation detection method [8], and some detection methods related to the use of Kalman filters [9][10]. The FDIAs detection method based on state estimation is mainly used for static analysis and detection of attacks at specific moments. When the power system fluctuates, it is prone to missed detection and false detection [11].

The increase in the deployment of wide-area measurement system provides massive data for the analysis of power system data. Therefore, artificial intelligence technology should be gradually increased in the FDIAs detection, mainly including support vector machine [12], extreme learning machine [13], fuzzy c-means clustering [14], deep learning [15][16], integrated learning [17], etc. The advantages of such methods are that they do not need to solve complex power system time domain equations and their calculation speed is fast. However, the disadvantage is that the test results are highly dependent on the training process of the model. Improper selection of training samples can directly affect detection performance.

Since the power system is in continuous dynamic operation and a space-time correlation exists between different measurement data or state variables, most attacks are continuous. Therefore, it is feasible to consider using historical data for trajectory prediction analysis to detect FDIAs, which mainly includes statistical consistency detection, sequence consistency detection and sensor trajectory prediction.

Kurt et al. [18] used the generalized cumulative sum (CUSUM) algorithm for quickest detection of FDIAs. This method is robust to time-varying state, attack and attacked instruments in both centralized and distributed environments. Similarly, Li et al. [19] proposed a sequence detector based on a broad analogy for sequential detection of FDIAs in the smart grid. This detector is significantly superior to first order CUSUM detector in terms of robustness and average detection delay

performance. In [20], Malhotra et al. proposed a stacked LSTM prediction network to effectively detect time series anomalies or failures, modeling the prediction error as a multivariate Gaussian distribution to evaluate abnormal behavior. By analyzing and learning the original measurement data, [21][22] used different methods to detect abnormal data which did not conform to the historical measurement distribution, which however failed to detect false data matching the historical measurement distribution. Khalid et al. [23] proposed multi- sensor track fusion-based model prediction for malicious attacks in PMUs, which can use smoothing algorithm based on Kalman particle filter to detect attacks at each monitoring node. The online FDIAs detection process of SCADA and PMU hybrid measurement is proposed in [24], which can effectively find the spatial hidden FDIAs based on multi-matching state prediction. However, when conditions such as load mutation or equipment failure occur, the state prediction results are seriously misaligned and thus affect the detection results.

Considering the time correlation of node measurement, Zhao et al. [25] compared prediction data with collected data based on short-term state prediction method, and further built detection index in combination with traditional measurement residual analysis. In order to solve the problem that it is impossible to detect attacks similar to historical data, Gu et al. [26] considered the characteristics of measured data variation and proposed a detection method based on Kullback-Leibler distance (KLD). However, the method failed to detect attacks on some nodes. A real-time detection scheme of FDIAs based on joint transformation is proposed in [27], but the detection accuracy is reduced when the attack is less intense.

The detection method based on trajectory prediction analysis is mainly used to predict the distribution of state variables according to the operation law of the system state and of the historical database. By comparing the running track, various types of FDIAs can be detected effectively. However, there are two problems when the probability density function is used to represent the data running track. One is the problem of overlapping distributions, and the other is the difficulty of detecting historical data replay attacks.

2. System Model

Assuming that the grid has N+1 nodes and M measurement devices. Based on the common linear DC model, measurement equation and state equation of discrete linear power system are given as follows:

$$z_t = h\left(x_t\right) + e_t \tag{1}$$

$$x_t = f\left(x_{t-1}\right) + v_t \tag{2}$$

In (1) and (2), between each time interval $t-1$ and t, $\lambda \in \{1,2,3,\ldots\}$ is usually small. Therefore, the collected measurement data between time $t-1$ and t needs to be processed at time t.

3. Bad Data Detection and Identification

System with data acquisition and monitoring control can collect real-time measurement data and make state estimation. In order to eliminate the error caused by non-human factors [28] and ensure the reliability of the state estimation results, there is a built-in BDD scheme in EMS for bad data detection and identification. The essence of the traditional method of detecting and identifying bad data can be summed up as residual method. The residual vector r is first determined by calculation, and then different detection standards are used for judgment. In other words, bad data can be detected by calculating r as follows:

$$\begin{aligned} r &= z - \hat{z} = h\left(x\right) + e - \left(h\left(x\right) + H\left(x - \hat{x}\right)\right) \\ &= e - H\left(H^T R^{-1} H\right)^{-1} H^T R^{-1} e \\ &= \left(I - H\left(H^T R^{-1} H\right)^{-1} H^T R^{-1}\right) e \\ &= Se \end{aligned} \tag{3}$$

Taking the extremum detection method of objective function [29] as an example. The extremum of objective function established by residual vector is as follows:

$$J\left(\hat{x}\right) = \left[z - h\left(\hat{x}\right)^T\right] R^{-1} \left[z - h\left(\hat{x}\right)\right] = r^T R^{-1} r \tag{4}$$

$$D_{J(\hat{x})}(z)=\begin{cases}1 & J\left(\hat{x}\right)>\gamma_0, \quad \text{bad data}\\ 0 & J\left(\hat{x}\right)\le\gamma_0, \quad \text{no bad data}\end{cases} \tag{5}$$

In order to further eliminate bad data by identifying them, the generally adopted criterion is the "3σ" principle. When the system has bad data, the measurement corresponding to the maximum residual should be corrected and the above detection process should be repeated until all elements in the residual vector are within the threshold.

4. Principle of False Data Injection Attack

Attacker can successfully inject into measurement data by constructing the effective attack vector. Traditional FDIAs are typically given as follows:

$$z_a=z+a=h\left(x\right)+a+e \tag{6}$$

where a is the injected false data attack vector; z_a is the attacked measurement vector; x is the estimation vector of original measurement vector z without attack.

If z can bypass the traditional bad data detector based on residuals, then a can also bypass BDD, satisfying the following equation:

$$a=Hc \tag{7}$$

$$z_a=Hx+Hc+e=H\left(x+c\right)+e=Hx_a+e \tag{8}$$

$$r_a=z_a-Hx=z+a-H\left(x+c\right)=z-Hx \tag{9}$$

At this point, the traditional method of bad data detection and identification fails to FDIAs, which allows attacker to tamper with the measurement data at will.

References

1. Tang, Y.; Chen, Q.; Mengya, L.I.; Wang, Q.; Ming, N.I.; Liang, Y. Overview on cyber-attacks against cyber physical power system. Autom. Electr. Power Syst. 2016, 40, 59–69.
2. Xian, G. Analysis of Venezuela's blackouts and suggestions on network security of critical infrastructure. Inf. Technol. Netw. Secur. 2019, 38, 1–2.
3. Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False data injection on state estimation in power systems attacks, impacts, and defense: A survey. IEEE Trans. Ind. Inform. 2017, 13, 411–423.
4. Li, Q.; Sun, H.; Sheng, T.; Zhang, B.; Wu, W.; Guo, Q. Injection attack analysis of transformer false data in substation state estimation. Autom. Electr. Power Syst. 2016, 40, 79–86.
5. Qi, W.; Wei, T.; Yi, T.; Ming, N. A review of the false data injection attack against the cyber physical power system. Acta Autom. Sin. 2019, 45, 74–85.
6. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 2011, 14, 1–33.
7. Kosut, O.; Jia, L.; Thomas, R.; Tong, L. Limiting false data attacks on power system state estimation. In Proceedings of the 44th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, USA, 17–19 March 2010; pp. 1–6.
8. Hu, Z.; Yong, W.; Tian, X.; Yang, X.; Fan, R. False data injection attacks identification for smart grids. In Proceedings of the Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), Beirut, Lebanon, 29 April–1 May 2015; pp. 139–143.

9. Qu, Z.; Dong, Y.; Wang, Y.; Chen, L. Improved robust unscented Kalman filtering algorithm for dynamic state estimation of power systems. Autom. Electr. Power Syst. 2018, 42, 87–92.
10. Chen, B.; Li, H.; Li, B. Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network. Power Syst. Technol. 2019, 43, 3226–3236.
11. Wang, D.; Guan, X.; Gu, T.; Shen, C.; Xu, Z. Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids. Energies 2014, 7, 1517–1538.
12. Ahmed, S.; Lee, Y.; Hyun, S.-H.; Koo, I. Feature selection-based detection of covert cyber deception assaults in smart grid communications networks using machine learning. IEEE Access 2018, 6, 27518–27529.
13. Xue, D.; Jing, X.; Liu, H. Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework. IEEE Access 2019, 10, 31762–31773.
14. Mostafa, M.; Ashkan, S.; Seifi, A.R. A statistical unsupervised method against false data injection attacks: A visualization-based approach. Expert Syst. Appl. 2017, 10, 1016–1035.
15. Li, Y.; Zeng, J. Detection method of false data injection attack on power grid based on improved convolutional neural network. Autom. Electr. Power Syst. 2019, 43, 97–104.
16. Ahmed, S.; Lee, Y.; Hyun, S.; Koo, I. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. IEEE Trans. Inf. Forensics Secur. 2019, 14, 2765–2777.
17. Wang, D.; Wang, X.; Zhang, Y.; Jin, L. Detection of power grid disturbances and cyber-attacks based on machine learning. J. Inf. Secur. Appl. 2019, 46, 42–52.
18. Kurt, M.N.; Yilmaz, Y.; Wang, X. Distributed quickest detection of cyberattacks in smart grid. IEEE Trans. Inf. Forensics Secur. 2018, 13, 2015–2030.
19. Li, S.; Yilmaz, Y.; Wang, X. Quickest detection of false data injection attack in wide-area smart grids. IEEE Trans. Smart Grid 2015, 6, 2725–2735.
20. Malhotra, P.; Vig, L.; Shroff, G.; Agarwal, P. Long short term memory networks for Anomaly detection in time series. In Proceedings of the 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, Bruges, Belgium, 22–24 April 2015; pp. 89–94.
21. Liu, L.; Esmalifalak, M.; Ding, Q.; Emesih, V.A.; Han, Z. Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans. Smart Grid 2014, 5, 612–621.
22. Mestav, K.R.; Tong, L. Universal Data Anomaly Detection via Inverse Generative Adversary Network. IEEE Signal Process. Lett. 2020, 27, 511–515.
23. Khalid, H.M.; Peng, J. Immunity toward data-injection attacks using multisensor track fusion-based model prediction. IEEE Trans. Smart Grid 2017, 8, 697–707.
24. Liu, X.; Wu, Z. Online defense research of spatial-hidden malicious data injection attacks in smart grid. Proc. Chin. Soc. Electr. Eng. 2020, 13, 1520–1534.
25. Zhao, J.; Zhang, G.; Scala, M.L.; Dong, Z.Y.; Chen, C.; Wang, J. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. IEEE Trans. Smart Grid 2017, 4, 1580–1590.
26. Gu, C.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in ac state estimation. IEEE Trans. Smart Grid 2015, 5, 2476–2483.
27. Singh, S.K.; Khanna, K.; Bose, R.; Panigrahi, B.K.; Joshi, A. Joint-transformation-based detection of false data injection attacks in smart grid. IEEE Trans. Ind. Inform. 2018, 14, 89–97.
28. Cheng, G.; Lin, Y.; Chen, Y.; Bi, T. Adaptive State Estimation for Power Systems Measured by PMUs With Unknown and Time-Varying Error Statistics. IEEE Trans. Power Syst. 2021, 36, 4482–4491.
29. Abur, A.; Exposito, A.G. Power System State Estimation: Theory and Implementation, 3rd ed.; CRC Press: Boca Raton, FL, USA, 2004.