Research on False Data Injection Attack in Smart Grid

Aidong Xu1*, Tengyue Zhang2, Liang Chen3, Qing Li2, Yunan Zhang1, Haojie Lin2, Peiyao Wang2, Sihui Wu2, Runhui Zhao2 and Yixin Jiang1

1Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
2School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China
3Science & Technology Department of Sichuan Province, Chengdu, China
Email: xud@csg.cn; uestczyt@163.com; rsyzch@163.com; zhangyn@csg.cn; jiangyx@csg.cn; Corresponding Author Email: xud@csg.cn

Abstract. The concealed false data injection (FDI) attack in the smart grid can successfully pass the power system state estimation commonly used in the residual bad data test without being detected by the existing algorithms, resulting in the state estimation error of the control center and disturbing the normal operation of the power system. In this paper, false data injection attack and attack detection are carried out in the actual power edge security protection system, microgrid control system and intelligent energy security protection system. Among them, the false data attack part simulates the attack of the voltage phase angle, and compares it with the ordinary attack method, and demonstrates the success of these attacks in the actual power grid system.

1. Introduction

As the next generation power system, smart grid can realize on-line monitoring and real-time information control of important operation parameters in each link of power grid by using advanced digital information and communication technology. However, the access of communication facilities also makes smart grid face potential network attack risk[1-12]. In particular, the false data injection (FDI) attack can bypass the traditional bad data detection (BDD) mechanism in the power system. By tampering with the measured data, the state estimation of the power system is not accurate, and then the decision-making of the control center is interfered to disturb the normal order of the power market. There are significant economic and security risks[1]. Since FDI attack was proposed, it has been widely concerned by scholars. The research results mainly focus on protection strategy, attack strategy and attack detection.

In the aspect of attack detection, Liu et al. [13] used the time correlation of state measurement and the sparsity of FDI attacks to detect generalized FDI attacks [14]. In reference [15], a distributed state estimation method was proposed, which can judge whether FDI attacks are suffered according to the deviation of estimation results, and can accurately locate the tampered state variables. For the hidden FDI attack with special structure, reference [16] regard it as a statistical learning problem. Taking historical data as training samples, according to the feature that the attack vector will make the normal measurement value and the attacked measurement value produce a "distance" change[16], the machine learning method is used to classify the measured value to achieve the purpose of detecting hidden FDI attack. This paper mainly focuses on the successful implementation of concealed false data injection attacks in three actual scenarios of power grid edge security protection system,
microgrid control system and smart energy system, and then considers the application of concealed attack detection methods in actual systems.

2. Principles of Hidden FDI Attacks for the Smart Grid

State estimation in the grid system refers to estimating the state of the system based on the measurement data of the meters on each bus. The measurement includes bus voltage, bus active and reactive power, and state variables include bus voltage and voltage phase angle, and its alternating current (AC) power flow model can be expressed as

\[ z = h(x) + n \]  
(1)

Where \( x \in R^P \) is the state variable of the power grid, which is the node voltage and phase angle variable. \( z \in R^N \) is the measurement vector, which is the measurement data of the sensor, \( n \in R^N \) is the measurement noise, and \( h(x) \) is the nonlinear relationship between the measurement value and the state variable, and its form is The topology of the power grid and the parameters on the bus are determined. Assuming that the noise obeys a Gaussian distribution with a mean value of 0 and a covariance matrix of \( \Lambda \), and the state of the system changes slowly over a period of time, the nonlinear AC model can be approximated linearly by Taylor expansion near the operating point, Get the direct current (DC) power flow model, its mathematical description is

\[ z = Hx + n \]  
(2)

Where \( H \in R^{N \times D} \) is the measurement Jacobian matrix, the state vector estimation can be obtained by the weighted least squares estimation

\[ \hat{x} = (H^T \Lambda H)^{-1} H^T \Lambda z \]  
(3)

FDI attack means that the attacker tampered with the measurement data in the terminal to make the equipment produce wrong state estimation, and then make the wrong decision. When the terminal is attacked, the measurement equation (2) becomes

\[ \tilde{z} = Hx + a + n \]  
(4)

Where \( a \in R^N \) is the attack vector. For attack vector \( a \), the commonly used detection method is bad data detection (BDD)

\[ \gamma = \|\tilde{z} - H\hat{x}\|_2 \]  
(5)

When the measurement residual exceeds a certain threshold \( \gamma > \varepsilon_0 \), it is judged to be attacked, where \( \varepsilon_0 \) is the threshold that needs to be set.

BDD is used to guarantee the integrity of state estimation to filter the error metrics introduced due to device failure or malicious attacks. However, when constructing a false data injection attack vector, if the attacker has complete understanding of the power grid topology and transmission on-line admittance, under the condition of fully understanding the topology Jacobian matrix \( H \), the attacker can inject a hidden attack vector \( a = Hc \) to generate a new measurement value. The attack has the same residual error as the non attack, but the system state estimation changes. Therefore, the attack is covert. When encountering a hidden FDI attack, equation (5) can be obtained

\[ \gamma = \|\tilde{z} - H\hat{x}\|_2 = \|\tilde{z} - H(H^T \Lambda H)^{-1} H^T \Lambda z\|_2 = \|n - H(H^T \Lambda H)^{-1} H^T \Lambda n\|_2 \]  
(6)
It can be seen from the above formula that the measured residual $\gamma$ is only affected by noise, and traditional BDD methods cannot detect hidden and false data injection attacks.

3. System Implementation of False Data Attack
Firstly, the attack of voltage phase angle is simulated in Figure 1. Data destruction based on time seed random number is a common attack method, so that the authenticity of the data is lost, which will change the system state estimation. The bad data detection based on residual detection is used to detect it. Figure 1 shows that the common attack can be detected. And related business integration is carried out on the power system edge computing security protection management platform.

Then the hidden false data injection is carried out to attack the voltage phase angle, and the contrast diagram with the original voltage phase angle is obtained in Figure 1. Finally, it is verified that the common residual detection method can not detect the hidden data attack. Therefore, the traditional BDD method can not detect the hidden false data injection attack. The experimental results verify this. And related business integration is carried out on the power system edge computing security protection management platform.

Three versions of the power edge safety protection system (metering system), microgrid control system, and smart energy safety protection system (charging piles) have been integrated with related businesses. In the system integration of the power edge computing security protection system, the attack on the voltage phase angle of thirty analog meters has been completed. The common attack method can be used to achieve common attacks on different meters by switching the meters. Figure 1 is a schematic diagram of randomly selecting attackers. Residual detection shows which meters are under attack. By calculating the Jacobian matrix of the power flow from the measurement information, a hidden attack vector is constructed to attack the state information.

![Figure 1. Schematic diagram of data attack business under metering system and charging piles.](image-url)
The smart energy system (micro grid control) adopts the same covert attack method as the metering system. Under the smart energy system, attacking the data of wind power generation, solar power generation and load power consumption in the smart energy system will affect the electricity trading behavior. The interface is shown in Figure 2. By selecting the attack object as the microgrid device, the normal and covert attacks are carried out, and the power generation situation after the two attacks is displayed, and the current time of being attacked is displayed by residual detection.

![Figure 2. Schematic diagram of device attack service under microgrid control.](image)

4. Conclusion
In this paper, the hidden false data injection attack and attack detection are carried out in the actual power metering system, micro-grid control system and intelligent energy security protection system, and compared with common attack methods. It is verified that the bad data detection based on residual detection can detect common attacks, but can not detect hidden data injection attacks. In the future, designing an effective detection method for hidden FDI attacks in actual systems is worthy of further study.

5. Acknowledgments
This work is supported by the National major R & D program (No. 2018YFB0904900, 2018YFB0904905).

6. References
[1] Zhao J H, Liang G Q, Wen F S and Dong Y C 2016 Lessons learnt from Ukrainian blackout: protecting power grids against false data injection attacks Automation of Electric Power Systems vol 40 pp 149-151
[2] Liao R F, Wen H, Wu J, Song H, Pan F and Dong L 2018 The rayleigh fading channel prediction via deep learning Wireless Communications and Mobile Computing 2018
[3] Wen H, Ho P H, Qi C and Gong G 2010 Physical layer assisted authentication for distributed ad hoc wireless sensor networks *IET information security* vol 4 pp 390-396

[4] Wen H, Ho P H and Wu B 2014 Achieving secure communications over wiretap channels via security codes from resilient functions *IEEE Wireless Communications Letters* vol 3 pp 273-276

[5] Chen S, Wen H, Wu J, Lei W, Hou W, Liu W and Jiang Y 2019 Internet of things based smart grids supported by intelligent edge computing *IEEE Access* vol 7 pp 74089-74102

[6] Ji B, Li Y, Zhou B, Li C, Song K and Wen H 2019 Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting *IEEE Access* vol 7 pp 38738-38747

[7] Wen H, Tang J, Wu J, Song H, Wu T, Wu B and Sun L M 2014 A cross-layer secure communication model based on Discrete Fractional Fourier Transform (DFRFT) *IEEE Transactions on emerging topics in computing* vol 3 pp 119-126

[8] Hu L, Wen H, Wu B, Tang J, Pan F and Liao R F 2017 Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers *IEEE Transactions on Vehicular Technology* vol 67 pp 2108-2117

[9] Liu X and Li Z 2016 False data attacks against AC state estimation with incomplete network information *IEEE Transactions on smart grid* vol 8 pp 2239-2248

[10] Wen H, Wang Y, Zhu X, Li J and Zhou L 2013 Physical layer assist authentication technique for smart meter system *IET Communications* vol 7 pp 189-197

[11] Xie Y, Wen H, Wu B, Jiang Y and Meng J 2019 A modified hierarchical attribute-based encryption access control method for mobile cloud computing *IEEE Transactions on Cloud Computing* vol 7 pp 383-391

[12] Xiao J, Wen H, Wu B, Jiang X, Ho P H and Zhang L 2013 Joint design on DCN placement and survivable cloud service provision over all-optical mesh networks *IEEE Transactions on Communications* vol 62 pp 235-245

[13] Liu L C, Esmalifalak M, Han Z. 2013 Detection of false data injection in power grid Exploiting Low Rank and Sparsity. *International Conference on Communications*, Budapest, Hungary.

[14] Liang G Q, Zhao J H, Luo F J, Weller S R, Dong Z Y. 2017 A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid* vol 8 pp1630-1638

[15] Shan Ke-Meng, Qi Dong-Lian 2017 Distributed detection of false data injection in smart grid and location of error estimation. *Proceedings of the 36th Chinese Control Conference*. Dalian, China.

[16] Ozay M, Esnaola I, Vural F T Y, Kulkarni S R, Poor H V. 2015 Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems* vol 27 pp 1773-1786