Intelligent Defense Simulation of High Efficient Internet of Things False Data Injection Attack

Juxia Xiong[1,2,3,a,*], Jinzhao Wu[1,2,3,b]

[1]Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu, Sichuan, 610041, China

[2]Chengdu Institute of Computer Application, University of Chinese Academy of Sciences, Beijing, 100049, China

[3]School of Mathematics and Physics, Guangxi University for Nationalities, Nanning, Guangxi, 53006, China

[a] email: xiongjuxia1107@163.com, [b] email: wjzgxun@163.com

*corresponding author

Keywords: Efficient Internet of Things, False Data Injection Attack, Intelligent Defense

Abstract: False data injection attack is a new attack method for power system state estimation in smart grid. That's a typical data integrity attack. FDIA avoids the existing bad data detection mechanism by tampering with the estimated state of transmission network. In addition, the wrong decision was made to the control center, which resulted in significant physical failure. It is very important to study the efficient and executable fdias detection method for building a safe and stable smart grid network physical system. For fdias, this paper focuses on those detection methods. Through the analysis of the principle and current research status of FDI as at home and abroad, the existing detection methods are compared and analyzed from the two perspectives of central detection and decentralized detection. Most of the existing detection methods ignore the influence of fdias on the physical characteristics of power system and the relationship between them. After detecting fdias, in order to restore the system measurement and make the system return to normal, a method of restoring the system in a short time is proposed. In order to solve this problem, the detection method based on the voltage stability index of nodes and the two-level detection method based on the matrix partition of zero space mapping are decentralized.

1. Introduction

With the development of modern communication, network, computing and control technology, the application of information technology is expanding. As a combination of advanced information technology and power technology, the new smart grid is an advanced measurement technology based on the comprehensive high-speed two-way communication network using advanced mechanical technology. In addition, advanced control methods and decision support system technology as well as rules for further improvement of energy and power [1]. The information network is closely coupled with the physical grid system, and interacts with each other to form a typical network physical system. The system has been applied in smart grid, smart transmitter, telemedicine, aerospace and other fields. The security of power system is divided into two levels: physical security and information security. The former aims to maintain normal operation in case of disturbance, while the latter is to protect communication network and computer system.

2. Smart Grid Security Overview

The safe and stable operation of electric power is the direct basis of national economy, which directly affects the national economy and people's life. Since the reform and opening up, China's economic structure has made great progress [2]. As the main project of national economic construction, transmission network construction has been greatly changed and reformed. Smart grid is a traditional grid. In order to understand the use of modern technologies such as unified

  DOI: 10.25236/ictmic.2020.077

technology and communication technology, the stability, security and reliability of the grid are high. The demand of people in the conference, the demand of people in the new era, and the important role of the state and the world's power industry in driving. The emergence of smart grid is of great significance to the development of global power and is the leader of global power. As the world's largest economy, the United States has the world's largest power industry. The U.S. government plays an important role in power system security. It has long been included in reports issued by the National Institute of standards and Technology (NIST). The logic structure and information security elements of smart grid are analyzed in detail, and the information security protection strategy of smart grid is formulated. Most of the information security related work, such as information security project research, standard preparation, offensive training simulation, etc., have been formed [3]. These standards provide a good guarantee for large grid reliability and important information assets.

Table 1 Number of state variables and measurements in IEEE test system

Standard Test System	Number of state variables	Number of measurements
IEEE 14-bus	13	54
IEEE 30-bus	29	112
IEEE 118-bus	117	490

3. False Data Injection Attack

With the continuous improvement of automation and interconnection level of intelligent power grid industry control system, the operation mode of power system is becoming more and more complex [4]. An important part of energy management system (EMS) of modern power system is the core module of online security analysis function of power system. The state estimation of power system obtains the measurement data through SCADA system and performs the estimation process. Measurement noise, remote error and communication noise often lead to incorrect state estimation results. Early power system researchers, during the state estimation, acknowledged the existence and threat of bad data, and realized the problem. Bad data usually produce huge standard measurement residuals, and researchers are studying the corresponding processing methods [5]. Among them, objective function extreme value J (x), measurement mutation detection method, weighted residual method and standard residual method are commonly used detection methods. The common feature of these methods is to detect bad data first.

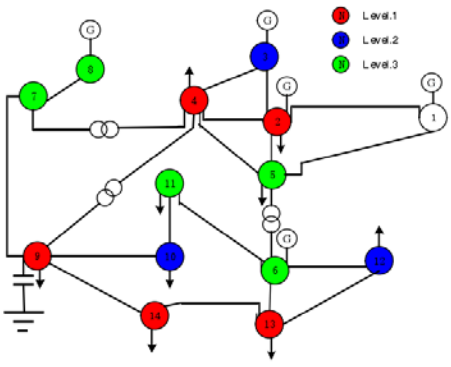

Figure 1 Clustering results of IEEE 14 bus system nodes

4. Analysis of Attack Principle and Detection Method of False Data Injection

4.1 Energy Management System

The traditional power grid is based on one-way thinking of generation, transformation, transformation, distribution and power consumption [6]. As the smart grid is built on a unified high-speed two-way communication network, all aspects of operation information flows in two

directions. In order to facilitate real-time data collection and timely release of control instructions. Energy management system (EMS) is a comprehensive automation system for modern power system.

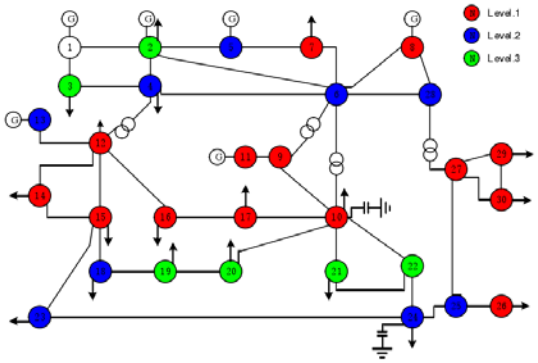

Figure 2 Clustering results of IEEE 30 bus system nodes

4.2 False Data Injection Attack Mode

Transmission system is a power network composed of power station, substation and transmission line. The power that users use at any time must be equal to the power generated by generators. Redundant transmission lines allow power generated by any power station in a widely distributed grid to be undisturbed [7]. The distribution principle provided to each user is to minimize the necessary operating costs.

4.3 Detection Method Based on Node Voltage Stability

Fdias causes grid defects by state estimation. Most of the existing detection methods consider the physical characteristics of fdias grid and the impact on the relationship between them[8]. Effective analysis of the physical characteristics of power grid is an effective way to improve the detection and protection ability of fdias. By analyzing the physical characteristics of power system, the voltage stability index (nvsi) of nodes is introduced, the relationship between FDI and nvsi is established, and the vulnerability level of nodes under different levels of attack is determined. In order to obtain the interdependence of different nodes, the cfpso optimization algorithm is based on the improved k-means easy to be classified algorithm. For different classes of system nodes, in order to be used, the detection method of vulnerability expression level in each class is to detect the implementation of fdias which will be used first. The simulation experiment is installed in IEEE 14 bus, IEEE 30 bus, IEEE 118 bus and other three standard test systems. The proposed method detects fdias and verifies its feasibility and effectiveness.

4.4 Introduction of Voltage Stability Index of Nodes

The concept of voltage stability index is not clear to power system operators [9]. Other scholars have defined voltage stability: the ability to maintain acceptable voltage after normal activity or the ability of all nodes after power system failure; after given initial operating conditions, the ability to maintain acceptable voltage continuously, and voltage collapse is a series of events, such as causing power failure in most areas of the system or voltage instability of low voltage. The node voltage stability index (nvsi) in power system is the scale of critical stable operation point, and is one of the important indexes of system stability. It is usually divided into two categories: status indicator and margin indicator. It can reflect the real-time state of the system and prevent the occurrence of voltage collapse. Voltage stability analysis usually includes static analysis and dynamic analysis. Among them, the static analysis method has the ability of simple calculation and qualitative voltage stability standard, so it becomes the main method to study voltage stability. The static grid voltage stability calculation of transmission network needs to consider the influence of line charging capacitor. One of the main advantages of nvsi is its simplicity and the accuracy of its modeling and calculation. The calculation of VSI and nvsi only requires electrical measurement of the current

system operation state, and the values can be obtained easily and quickly. The result is straightforward and easy to understand. Therefore, regular and systematic staff, the index is the weak link of the system, the online monitoring stability of the system, in order to prevent the timely and effective processing of the system monitoring and prediction, and effectively prevent the collision of the system, in order to help is regarded as the auxiliary analysis index[10]. According to the nvsi value, the system staff can not only determine the cause of system instability, but also determine the voltage collapse point when the system is close to the critical threshold. In fdias, the system staff must be more sensitive to the node voltage stability to avoid the system affected by the system instability.

5. Conclusion

Power system is a complex control system which combines physical system and information system. As the main foundation of a country, its safe and stable operation is the key foundation for the stable development of society and the rapid and healthy development of national economy. In the smart grid, there are great security risks in the power system. For example, an attacker may hide behind the attack conditions and wait for a better time to cause a fatal attack on the power system. In this paper, the research focus of the pseudo data injection attack in the power system, the research progress of the pseudo data injection attack in the power system, and the analysis of the principle of EMS and fdias and the influence of the power system. From the perspective of the system staff, the research on the detection method of the false data injection attack first, the security risk of the smart grid, the importance of the security of the smart grid, emphasized. This paper introduces the research status and trend analysis of fdias data integration attack on state estimation data of smart grid power system. This paper introduces the principle of false data injection attack and its influence on system state estimation. This paper summarizes the research situation of false data injection attack detection method from two points of view. Almost all the existing researches ignore the impact of attacks on the physical characteristics of the system.

Acknowledgements

1) This research has been financed by the National Natural Science Foundation of China “Error analysis and control of semi-algebraic model detection method” (61772006);

2) The Science and Technology Major Project of Guangxi “Research and Application Demonstration of Key Technologies for Intelligent Ship Networking in Beibu Gulf” (AA17204096);

3) The Key Research and Development Project of Guangxi “DPA-proof full asynchronous RSA security crypto chip: design methods, tools and prototypes” (AB17129012);

4) The Special Fund for Bagui Scholars of Guangxi “Control system design and verification” (2017);

5) The Promotion Project of Basic Faculties for Young and Middle-aged College Teachers in Guangxi “Research on Formal Analysis Method of Hybrid System Based on Polyhedron Projection and Segmentation” (2017KY0174);

6) The Promotion Project of Basic Faculties for Young and Middle-aged College Teachers in Guangxi “Common Sense Dynamic Logic Reasoning and Its Application” (2018KY0164).

References

[1] Alex Brito, Dmitry Grapov, Johannes Fahrmann,. The Human Serum Metabolome of Vitamin B-12 Deficiency and Repletion, and Associations with Neurological Function in Elderly Adults. Journal of Nutrition, vol. 147, no. 10, pp. jn248278, 2017.

[2] Kelsey Mathieu, Zhen Lu, Hailing Yang,. Abstract 1864: Feasibility of magnetic relaxometry for early ovarian cancer detection: preliminary evaluation of sensitivity and specificity in cell culture and in mice. Cancer Research, vol. 77, no. 13 Supplement, pp. 1864-1864, 2017.

[3] Dan Li, You-Gang Chen, Cui-Juan Zhang,. Safflower Extract and Aceglutamide Injection Promoting Recovery of Peripheral Innervations via Vascular Endothelial Growth Factor-B Signaling in Diabetic Mice, vol. 130, no. 23, pp. 2829-2835, 2017.

[4] Fei Miao, Quanyan Zhu, Miroslav Pajic,. Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injection Attacks. IEEE Transactions on Control of Network Systems, vol. 4, no. 1, pp. 106-117, 2017.

[5] Ying Chen, Shaowei Huang, Feng Liu,. Evaluation of Reinforcement Learning Based False Data Injection Attack to Automatic Voltage Control. IEEE Transactions on Smart Grid, no. 99, pp. 1-1, 2018.

[6] Zhisheng Wang, Ying Chen, Feng Liu,. Power System Security Under False Data Injection Attacks with Exploitation and Exploration Based on Reinforcement Learning. IEEE Access, no. 99, pp. 1-1, 2018.

[7] Mostafa Mohammadpourfard, Ashkan Sami, Alireza Seifi. A Statistical Unsupervised Method Against False Data Injection Attacks: A Visualization-Based Approach. Expert Systems with Applications, vol. 84, 2017.

[8] Jiandong Zhang, Xiaoyu Qu, Arun Kumar Sangaiah. A Study of Green Development Mode and Total Factor Productivity of the Food Industry Based on the Industrial Internet of Things. IEEE Communications Magazine, vol. 56, no. 5, pp. 72-78, 2018.

[9] Zheng, Qing-Hua, Li, Xiao-Li, Mei, Zhi-Gang,. Efficacy and safety of puerarin injection in curing acute ischemic stroke: A meta-analysis of randomized controlled trials. Medicine, vol. 96, no. 1, pp. e5803, 2017.

[10] Jubaer Ahmed, Zainal Salam. An Enhanced Adaptive P&O MPPT for Fast and Efficient Tracking Under Varying Environmental Conditions. IEEE Transactions on Sustainable Energy, no. 99, pp. 1-1, 2018.