Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 2, No. 2, 2022

Research on the defense mechanism based on FDIA in smart grid

Ronghua Yi *

Department of Computer Science, North China Electric Power University, BaoDing 07100, Hebei China

Abstract: With the extensive application of communication and information technology in power grid, the physical fusion system of power information develops rapidly, which makes the realization of every link in smart power grid rely on the support of information network. Although smart grid information can greatly enhance the performance of the power system, it also brings new security risks to the power system. FDIA (False Data Injection Attacks), as one of the most harmful Attacks to the stability of the power system, has attracted the attention of information security researchers. Therefore, this paper aims at the defense mechanism of power grid FDIA to discuss the protection strategy of power grid information security.

Keywords: Power information physical fusion system; Power system stability; FDIA defense mechanism.

1. Introduction

In recent years, attacks on smart grid through network and sabotage have occurred from time to time. As an important critical infrastructure, most countries are paying more and more attention to the information security of smart grid, and China has also included it in the national security strategy. In this paper, we analyze the threats to smart grid from the perspective of grid system security, and then summarize the attack methods and defense strategies of the typical attack form - false data injection.

Information security consists of five basic requirements: information integrity, confidentiality, non-repudiation, availability and controllability. The domestic smart grid information security research mainly involves transmission grid information security, distribution grid information security, power monitoring system and energy management system information security, power enterprise information security, substation information security and power consumption information collection system information security .

According to the basic attributes of information security, attacks on power grids can be divided into three categories in addition to physical damage: confidentiality attacks, availability attacks and integrity attacks. Confidentiality attack is an attacker who performs unauthorized access or eavesdrops on the confidential information and data of the power system. Availability attacks affect the stable operation of the power system by blocking the measurement data or control commands, which may lead to catastrophic consequences for the power system without effective control. Abdallah Farraj et al studied the effects of denial of service attacks (DoSA) and communication delays on the transient stability of the smart grid, and proposed a delay adaptive design using parametric feedback linearization (PFL) control feature. As for the integrity attack, it is by the attacker to tamper with the content of control or measurement signals, which can seriously affect the reliability and security of the grid. False data injection attacks (FDIA) is a typical integrity attack because of its covert nature and potential danger, which can affect the analysis and decision making of the upper control center and cause serious consequences, and is one of the high threat attacks on the power system. In this paper, we summarize the key issues and research status of FDIA construction, detection and defense mechanisms.

2. FDIA principle and process analysis

2.1. FDIA principle

The principle of FDIA can be expressed using the DC current equation for power system operation.

$$z = Hx + e \tag{1}$$

where z is the quantity measurement, H is the measurement Jacobi matrix, x is the state quantity to be estimated, and e is the measurement error. The state estimation is based on redundant measurements, of which the measurements may contain spurious data, which requires data detection to ensure the reliability of the state estimation results. To eliminate the influence of bad data on state estimation, residual-based spurious data detection methods are widely used. The expression of the residuals is given by

$$r = z - H(\hat{x}) \tag{2}$$

The basis for detecting false data is: $\|r\| < \tau$， τ is the threshold value for judgment, if $\|r\| < \tau$, then the system can be considered as not containing false data, otherwise the corresponding false data should be eliminated and the state estimation should be performed again until it passes the false data detection.

However, if the attacker uses $a = [a_1, a_2, \dots, a_m]^T$ to represent the false data vector injected in the volume measurement. The actual measurement becomes $z_{bad} = z + a$, at which point the estimated state variable also becomes $x_{bad} = x + c$, where c denotes the error vector introduced in the state variable due to the injection of the a vector. At this point the expression for the residuals also becomes

$$\|r\| = \|z_{bad} - Hx_{bad}\|$$
$$= \|z + a - H(\hat{x} + c)\| = \|z - H(\hat{x}) + a - Hc\| \tag{3}$$

Obviously, when $a = Hc$, $\|r\| = \|z_{bad} - Hx_{bad}\| = z - H(\hat{x})$. At this point, the residual-based bad data detection method is unable to detect the false data, and the attacker is able to change the quantity measurement and state change quantity at will, which seriously endangers the security stability of the power system.

False data injection attacks can be divided into many categories depending on the variant type, such as load

redistribution attacks that tamper with the load sent from power plants to control centers and branch currents, blind false data injection attacks that are data-driven by principal component analysis of the power system, topology attacks that can achieve state maintenance by only having local topology information and related measurement information of a specific attack line, and so on.

2.2. FDIA process analysis

In addition to a series of physical devices such as generators, transformers, circuit breakers, etc., the Cyber physical system (CPS) also contains heterogeneous intelligent terminal devices such as Remote terminal unit (RTU), synchronous phase measurement unit (PMU), etc., which realize the information collection and sensing of the power system.

As shown in Figure 1, from the attacker's point of view, FDIA can be conducted for two aspects of the communication sensing network and power control system of the power CPS.

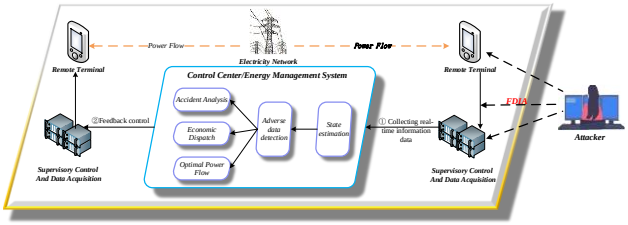

Figure .1 FDIA attack location

(1) The first step of the false data injection attack for the communication sensing network is to obtain the accessibility of the information side of the power information physical fusion system, and the intrusion process is usually realized during the data collection and transmission process. When the data is transmitted over the communication link, based on the principle of intrusion, it can be mainly divided into interaction and implantation system, where the interaction includes attacks such as masquerade, bypass control, man-in-the-middle and interception replay, and the implantation system includes attacks such as virus Trojan, trapdoor and service spoofing. For the prevention of FDIA on the power grid during communication, information security can be ensured by means of encryption technology and digital signature authentication, such as Luo Zhao et al introduced the domestic SM2 cryptosystem instead of the RSA algorithm of the original public key cryptosystem, and designed a power grid information security support platform based on the national secret SM2, which is based on Elliptic curve cryptography (ECC). SM2 cryptography system is an encryption algorithm based on Elliptic curve cryptography (ECC), which is more efficient than RSA algorithm, and it can ensure the integrity and confidentiality of measurement information in the communication process to a certain extent.

In the data acquisition process, FDIA can mainly target remote terminal units and synchronous phase measurement units. For example, an attacker can use the GPS vulnerability in the PMU to conduct a time synchronization attack and forge GPS signals to flood the correct data. When an attacker successfully injects the incorrect data into the information layer, he can achieve the goal of manipulating the physical processes of the power based on the full knowledge of the power system operation, control and protection operations.Kumar et al a novel ECC-based authentication protocol (ECCAuth) aims to preserve the demand response in SG systems. Compared to existing proposals that use only device-to-device communication in the local domain for authentication, the proposed protocol supports dynamic SG device authentication and UC addition in the SG environment at any time in both local and global domains.

(2) When an attacker targets FDIA as a power control system, first of all, we all know that sensor measurement data in the grid is not completely accurate, and naturally bad data can be caused by accidental factors such as device failure, sensor offset, incorrect connection, and communication interference. These inaccurate data are transmitted to the state estimator in the control system (e.g., energy management system EMS), and the estimated real-time system state is contaminated. So in order to remove such accidental random bad data, the Largest normalized residual (LNR) can be mainly used for detection, but if an attacker is familiar with the power system topology and state estimation algorithm, he can tamper with the measurement matrix by hijacking and distorting the output of the sensors, thus destroying the integrity of the state estimator. Then he can, like the FDIA principle described in the previous section, elaborate false data to satisfy the line topology and tide constraints, avoid bad data identification, improve the success rate, and subsequently lead to control decision failures.

3. FDIA impact analysis on the system

FDI attack is a great threat to the power system due to its stealthy nature, which can lead to serious consequences such as system load shedding, line overload, and disruption of the power market. For different power businesses, FDIA has a huge impact on the system not only in terms of security control, but also in terms of economic dispatch.

3.1. FDIA's impact on economic scheduling

In FDIA with the objective of financial gain, the attacker can falsify the system unit output plan or load forecast data, thus causing the system to misjudge the constraints of load balance, unit operation and grid security, and ultimately increasing the system energy consumption and equipment losses. When the attacker aims to gain economic benefits, he can falsify the line blockage level to profit from the tariff difference or theft in the power market. Xie L et al simulated the attacker to exploit the flaw of malicious data detection algorithm to falsify two line blockages for virtual bidding against IEEE14 node system by simulation and finally gained $6.0/MWh economic arbitrage. This has a huge harmful impact on the economic efficiency of both grid companies. Meanwhile, in the power demand response auction activity, malicious users can participate in the auction activity by faking the identity of legitimate users, and malicious bidding can lead to the demand response auction cannot be carried out smoothly.

3.2. Impact of FDIA on security control

In terms of power system security control, the consequences of the attack can be divided into the impact on system observability and controllability and the impact on security stability.

If FDIA fails to evade bad data detection, the tampered quantity measurements will be rejected as bad data, thus causing a certain area of the system to be unobservable, resulting in the power system dispatch control center not being able to grasp the actual operating status of the unobservable area in a timely manner, thus triggering subsequent system operation risks.

When FDIA successfully interferes with the estimated value of the quantity measurement, for example, by falsifying the node voltage magnitude over the limit, it may lead to load shedding or even system voltage collapse; by falsifying the line overload, it may lead to line fault and change of power topology.

4. FDIA defense mechanism principle and defense scheme

4.1. Principle of FDIA defense mechanism

The power CPS contains a large number of power primary equipment, communication equipment and information processing and control equipment. Since the power primary equipment side is a time-varying continuous system, while the information side is a discrete system and information changes are triggered by events, the spatio-temporal characteristics and description methods of the two are essentially different in terms of the principles of FDIA defense mechanism. Qi Wang et al analyzed the spatio-temporal dimensions of the power information-physical fusion system and studied the defense mechanisms according to different dimensions, and provided an insightful overview of the FDIA attack and defense means in the power CPS.

(1) In the temporal dimension, taking the analysis of power business data as an example, the sampling frequency and delay requirements of the data are different due to the different sources and business importance of the data, so the redundancy and reasonableness of the measurement data from different sources and time scales need to be verified, the interrelationships between the data are explored, the wrong data are eliminated by mutual verification, the data quality is improved, and the information security defense mechanism of multiple time scales is formed.

(2) In the spatial dimension, it is necessary to ensure the confidentiality, integrity and availability of information space on the one hand, and the stability of power space voltage, frequency, load supply and other indicators on the other. It is necessary to establish the correlation matching rules of both operational characteristics through the cross-space propagation mechanism of risk from information to physical for collaborative defense.

Based on the above defense mechanism principles, we need to establish a defense system covering the whole process of transient, steady-state and medium- and long-term dynamics in time, and a multi-layer defense architecture containing power layer, information layer and coupling layer in space, so as to establish a multi-dimensional synergistic defense model in time and space. The power CPS network security protection process is an evolving and dynamic process that requires a cyclical process of security management, implementation, deployment and evaluation.

The division of the organizational structure of the power CPS in turn explores the principle of each layer's defense means against FDIA is also different. The basic principle of information layer defense is to identify the correctness of data protocols and logic based on information security knowledge; the principle of power layer defense is to identify the reasonableness of data content based on power expertise. The intersection of the two is in the control application equipment, which is the highest layer of the information infrastructure and contains the database and high-level business applications covering the flow of measurement and command data for the physical grid. Fraudulent data injected at the information layer is collected in the control application, so ensuring the correctness of data content based on power knowledge is the last line of defense to prevent FDIA from disrupting the physical grid.

4.2. Analysis of FDIA defense methods and existing defense schemes

Today's smart grid information-physical convergence system defense methods against FDIA mainly contain detection and protection links. The protection method focuses on the planning of protection resources before the attack, and the detection method focuses on the identification of the attack behavior after the attack. The two types of links are usually applied in the initial stage of the attack, and if properly arranged, they can eliminate the attack in the nascent stage and minimize the impact of the attack, thus playing an important role in the overall defense process.

4.2.1. FDIA-oriented detection methods and related program analysis

Detection methods focus on detecting the presence of erroneous data and can be broadly classified into two categories: model-based detection methods and data-driven detection methods.

(1) Model-based detection method

This method models the smart grid by real-time measurements and by using static system data (e.g., system parameters and substation configuration). This detection method can be classified according to the operating conditions as a modeling detection method based on state estimation with quasi-static nature and a modeling detection method with trajectory prediction.

From the state estimation-based detection method, the constructed quasi-static model assumes that the system state changes in a smooth and slow manner, and the transient response generated by the system is negligible and easy to construct. And through the continuous improvement of the state estimation algorithm by researchers, it contains residual detection method, quantitative mutation detection method, and quantitative correlation detection method, etc. Dai Wang et al is the simulation experiment conducted by the FDIA method of detection based on state estimation, Dai Wang et al constructed a new FDI attack method - -tolerable false data injection (TFDI). This attack exploits the tolerance of conventional detectors to observation errors and bypasses the conventional bad data detection. Then a smart grid TFDI detection method based on extended distributed state estimation (EDSE) is proposed. The method uses a graph partitioning algorithm to decompose the power system into multiple subsystems, and the buses are divided into three groups: internal buses, boundary buses, and neighboring buses. Each subsystem is extended outward, including adjacent buses and contact lines to make generate extended subsystems. And the SE test and Chi-squares test are used to detect whether each subsystem contains spurious data. After the simulation results show that the system using EDSE detection method detects TFDI with much higher accuracy and reduces the computational effort by more than 90%.

The advantage of the detection method based on state estimation is that it utilizes proven algorithms, detects quickly, and also reduces the impact of general algorithms on detection accuracy.

In addition to the above detection methods based on state estimation of the power system to build a quasi-static model there are also detection methods based on trajectory

prediction to build a dynamic model. Because in the process of continuous dynamic operation of the power system, there is a strong spatio-temporal relationship between multiple state quantities. At this time, the quasi-static model is not suitable for use. Therefore, trajectory analysis using historical data can be considered to predict the current state of the power grid and compare it with the current actual quantity measurements to analyze the areas in which may be under attack. This method can effectively detect various types of false data by predicting the distribution pattern of state variables based on the operation law of system state and historical database, and by matching the operation trajectory, but the high computational complexity and slow detection speed are not suitable for complex systems.

(2) Data-based detection method

Unlike the model-based detection algorithm, the data-based detection algorithm is model-free. Therefore, such FDI detection methods do not involve system parameters or models.

Yi Wang et al proposed a data-centric paradigm to detect FDI attacks in large-scale smart grids. In this detection method, the Margin Setting Algorithm (MSA) is used to process large amounts of real-time data from large-scale smart grids. The simulation dataset for this literature is generated from a MATLAB/Simulink model that uses a six-bus power system in a WAMS network. The real-world dataset is based on hourly data input from a synchronous phase volume network in Texas. And two FDIA attack schemes, replay attack and temporal attack, are investigated. The final experimental results show that the algorithm has higher accuracy and minimum error in detecting FDIAs than the traditional SVM and ANN algorithms.

The significant advantages of this FDIA detection method using artificial intelligence are the powerful computational power and clear framework. However, due to the complexity of the power system operation mechanism, the interpretability of this type of method is usually poor.

4.2.2. FDIA-oriented protection methods and related program analysis

Due to the massive measurement and control data and complex operation mode of the power grid, the calculation of the impact of different combination types of attacks on the operation mode of the power system is very large, so it is difficult to meet the requirements of the decision time by using real-time decision making and real-time control. It is necessary to adopt the idea of offline decision making and online matching. Before the attack, in the offline static analysis stage, the idea of planning is used to locate the critical area and analyze the attack-fault mapping relationship, so as to determine the decision table in advance; in the online matching decision stage, the idea of game is used to analyze the attack and defense behavior in advance, filter out the possible attack methods and determine the optimal defense strategy.

Chen Yulin et al conducted a study on FDIA defense under distributed cooperative control of microgrids. For the effect of constant value attack of FDI on distributed cooperative control, a distributed controller that can completely eliminate constant value attack is designed by using the property of constant value differentiation to zero. The method does not require the design of complex parameters to evaluate the trustworthiness of neighbor information, does not rely on additional estimators and communication networks, is able to completely eliminate the impact of the attack, and is highly practical as it can cope with all cases in which the distributed generator (DG) is attacked. The protection method can be found to provide great help for transient stability of power systems.

Qi Wang et al proposed a two-layer defense model including detection and protection from the perspective of defense against FDIA, where the upper layer model implements detection-based defense and the lower layer model implements protection-based defense. It uses the measurements within the phase measurement units (PMUs) as the attack and defense targets, and quantifies the attack results using the load reduction caused by line failure. The measurement redundancy is enhanced using an extra-domain additional protection approach.

The advantage of this approach is that game theory provides a more practical and sophisticated understanding of the game process between attackers and defenders. It not only analyzes the priority defense deployment in the grid from a holistic perspective, but also takes into account the opponent's choices to optimize its own offensive and defensive resource deployment as much as possible.

5. Conclusion

This paper presents a theoretical analysis of the attack process in terms of attack invasion methods, attack conditions, attack impacts, and defense aspects such as protection and detection, and introduces the FDIA attack and defense mechanism for power CPS. The analysis and summary of FDIA for smart grid defense are based on several research cases.

References

[1] Jie Cheng,Zhijie Sang,Wei Hu,ShuLin Zhang. Smart Grid Information System Security Hazards and Response Strategies [J]. Electrotechnical Application,2020,39(04):99-102.

[2] A.K.Farraj, E.M.Hammad, and D.Kundur, “A Cyber-Physical Control Framework for Transient Stability in Smart Grids,” IEEE Trans. Smart Grid, vol.9 , no.2 , pp.1205-1215 , Mar.2018.

[3] JiWei Tian,BuHong Wang . Research Progress and Prospects of False Data Injection Attack on Smart Grid [J]. Cyberspace Security,2019,10(09):73-84.

[4] Zhao Luo,JiHua Xie,Wei Gu. Development of a power grid information security support platform based on SM2 cryptosystem[J]. Automation of Electric Power Systems,2014,38(6):68-74.

[5] N. Kumar, G. S. Aujla, A. K. Das and M. Conti, "ECCAuth: A Secure Authentication Protocol for Demand Response Management in a Smart Grid System," in IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6572-6582, Dec. 2019.

[6] Xie L, Mo Y L, Sinopoli B. Integrity data attacks in power market operations. IEEE Transactions on Smart Grid,2011,2(4):659−666.

[7] Qi Wang,Yi Tang,Ming Ni. A Review of Research on False Data Injection Attacks for Power Information Physical Systems [J]. IEEE/CAA Journal of Automatica Sinica,2019,45(01):72-83.

[8] Dai Wang, Xiaohong Guan, Ting Liu, Yun Gu, Chao Shen, Zhanbo Xu. Extended Distributed State Estimation: A Detection Method against Tolerable False Data Injection Attacks in Smart Grids[J]. Energies,2014,7(3).

[9] Wang, Y., et al., A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids[J]. IEEE Access, 2017. 5: p. 26022-26033.

[10] YuLin Chen,DongLian Qi ,ZhenYu Wang. Distributed Cooperative Control of Microgrids under False Data Injection Attack [J]. Automation of Electric Power Systems,2021,45(05):97-103.

[11] Qi Wang, Wei Tai, Yi Tang, Ming Ni, Shi You. A two-layer game theoretical attack-defense model for a false data injection attack against power systems[J]. International Journal of Electrical Power and Energy Systems,2019,104.