xIlkogretim Online - Elementary Education Online,2021; Vol 20 (Issue 1): pp.2283-2289
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.254

A Novel State Estimation Based Shield Mechanism Thwarting SIoT Attacks

R. Subash, Department of CSE, College of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, 603203, Kanchipuram, Chennai, Tamil Nadu, India. subashr@srmist.edu.in
R. Jebakumar, Department of CSE, College of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, 603203, Kanchipuram, Chennai, Tamil Nadu, India
Authors E-mail: jebakumr@srmist.edu.in

Abstract- Adopting social networking concepts in the Internet of Things (IoT) paradigm, establishes a new interesting field called Social Internet of Things (SIoT). Under this, devices socially communicate with each other to solve similar problems using IoT. One of the major areas of such an arena is Smart Grid (SG) power system. SG is an intelligent, efficient but complex Cyber-Physical System (CPS) of the Power Internet of Things (PIOT). The smart grid integrates the power grid (PG) with IOT. Smart Grid (SG) system is operated by its center of control called as the Supervisory Control and Data Acquisition System (SCADA) which has a built-in ICT. SCADA has a State Estimator which screens the real time power states and decides the respective control actions. SG basically facilitates the exchange of 2-way information between the customers and the energy providers through the public IP- based communication protocols. Therefore, the SCADA in SG is highly vulnerable to several cyber-attacks. One such severe threat for the State Estimator in SCADA is the cyber attacks caused by the False Data Injection (FDI). In order to pose a solution for such a challenging attack, this paper introduces a novel scheme for detecting bad data injection in State Estimation. This technique detects both the stealthy and non-stealthy attacks by using the Continuous Prevention and Detection (CPD) algorithm, which does the mechanism of either protecting the SG from attacks in advance or continuously detecting the FDI attacks. The proposed algorithm is initiated by the attack classification which proceeds by the defense mechanisms of the control center in the IOT based electric grid.

Keywords: Social Internet of Things; Smart Grid; Cyber-Physical System; Power Internet of Things; Supervisory Control and Data Acquisition System; False Data Injection attack

I. INTRODUCTION

Internet of Things (IOT) is the most emerging technology changing our day to day life rapidly. IOT has started to reshape the future of internet through "anytime-anywhere-anyone-connected to anything" era. With the IOT technologies, virtual and smart physical things are able to communicate with each other and various intelligent services in the physical world can be easily created without any human intervention. In IoT, the devices can only observe, whereas SIoT gives the freedom for the devices to interact among them without any human intervention which makes them smarter than before. Hence, SIoT provides device socialization rather than uplifting their smartness. Power Internet of Things (PIOT) is one such application of SIOT technology in the energy sector. PIOT is applied widely across the fields of generating, transmitting, distributing the power and finally its consumption by users. Smart Grid (SG) is a modern electricity delivery system using PIOT technology. SG implies IOT + traditional power grid system (i.e.) it integrates physical system (power grid) and cyber-system (IOT). SG is capable of monitoring and controlling the grid remotely. The key elements of SG power system are the following: The control centre called the Supervisory Control and Data Acquisition System (SCADA), Advanced Metering Infrastructure of the grid (AMI), Phasor Measurement Unit (PMU), Fault Detectors, Plug-in Electric Vehicles. Since SG is the integration of a physical traditional power grid system and an IOT based cyber- system, it questions about the enormous risk in the cyber security which results in the endangered electric grid regarding the cyber-physical hacks. Therefore, the need for security is important in SG power systems. This SG is operated by a built-in ICT control center called the SCADA. This ICT provides power state estimator which results the SG to face critical cyber-attacks through the public internet-based communication protocols. Also, these security threats damages transformers in the SG power system. The following are the types of security threats in SG: threats in smart metering- attacks occur in Smart Meter and in AMI, threats in monitoring and measurement- attacks occur in SCADA and threats in information transmission- attacks occur in communication networks.

The organization of this paper is structured as the following: section 2 briefs about the related works, section 3 deals about the attacks regarding the False Data Injection, section4 discusses the real time shield

mechanism for detecting FDI attacks using Continuous Prevention and Detection (CPD) Algorithm, section 5 discuss about the performance evaluation and the conclusions are under section 6.

II. Related Works

Following are the related works carried out in cyber security of SCADA of the smart grid power system. Power readings of the progressive information are detected by using adaptive detection algorithm. Effective action strategies for continuous attack are needed [1]. Euclidean distance defense mechanism is used to deal with a novel kind of FDI attack [2]. FDI attacks are detected using a Kalman filter (KF) based method for better accuracy [3]. Power anomalies are detected using machine learning algorithms like Support Vector Machine (SVM) [4]. A State Vector Estimator (SVE) and a Deep – Learning Based Identification (DLBI) scheme which employs Conditional Deep Belief Network (CDBN) that exploits Conditional Gaussian – Bernoulli RBM (CGBRBM) is proposed [5].

Deep neural network systems are extended to detect such attacks efficiently [5]. Dynamic Encryption Key (DEK) is used for detecting the FDI attacks, but the threats and counter measures to validate of SEDEA are not analyzed and tested [6]. When reviewing the various FDI attacks against the detection methods, AC model power system is found to be desirable [7]. Graph models for power network and graphical characterization of state estimation is introduced to rectify the threats in the security of the grid. Application oriented security analysis in higher application level to be done [8]. A Mechanism for detecting intrusion in cyber security for IEC based substations is implemented. A method for control detection, listing protocol is introduced. Prediction for model-based scenario and multi parameter methods is needed [9]. Designed an interval observer to predict the state of internally physical system using dynamic grid system [10]. A mechanism for practical FDI attack against state estimation is proposed, it indicates that the system states can be guessed certainly by calculating the local state measurement equations [11]. A game theory-based attack identification strategy is proposed by considering the topological branch chain graphs of a dispatch power system without considering the electrical characteristics of the system [12].

III. False Data Injection Attacks

The following section illustrates about the false Data Injection attacks, its types and its effects on smart grid. By knowing the value of Jacobin matrix and state estimation as load profiles, the attack vector is added for an FDI attacker by an attacker in a smart grid power system. Based on the detection of bad data attack by conventional residual test, the FDI attacks are of two types which are as follows, Stealthy and Non stealthy data injection attacks.

Non stealthy Data Injection Attack: Such attacks are recognized by the usual residual test method of conventional analysis (i.e.) through Bad Data Detection mechanism. Here the attackers are unaware of the value in measurement vector. They are randomly injecting some bad vector into the readings of the smart meter and hack the smart grid system.

Stealthy Data Injection Attack: These attacks are not recognized by the usual residual test method of conventional analysis. Here either the structure of grid or measurement matrix is familiar to the attacker. Hence it is easy for the attacker to inject the malicious data into the smart grid system. Attackers overcome the conventional normal residual test method. Therefore, the control center does not have any knowledge about the bad data vector and believes that it is the normal state vector.

IV. Continuous Prevention and Detection (CPD) Shield Method for Finding FDI Attacks

In the following section, the proposed Continuous Prevention and Detection (CPD) algorithm is discussed with the further performance evaluation of the proposed mechanism in the standard IEEE buses for better results**.** Power will be generated in the various type of the power generating unit. The Figure 1 in architecture diagram.

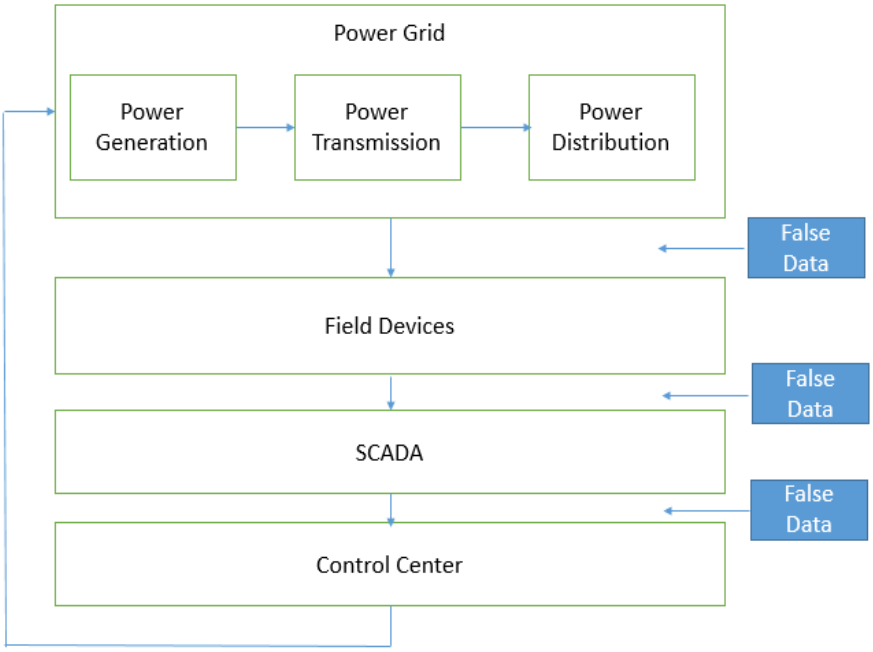

Figure 1. Architecture Diagram

It follows the various IEEE bus standards for generating of power in the power grid. There may be two types of power grid exist in the real environment. One will be the manual power grid and another one will be the smart power grid. In the SG all the activities are monitored and controlled by the system. In our architecture first stage will be the power grid, it consists of power generation, power transmission and power distribution will be combined to form as a power grid.

Power generation will be done in various types of power generating methodology will be used to generate the power in the system. It comprises of all the power generation methods and form as grid. It may also consist of the power transmission in the grid will be provided by various type of the lines used to transmit the power from one region to another region. It carries the power and also data in the smart power grid system. Through the data prediction of availability of the power will be easily calculated by the system. Control centre is used to observe the PS in the grid, it consists of the SCADA and various sensing units to observe the power measures of the various units and transferred to the unit. The remote sensing consists of the meter or sensors to observe the data produced in the various sensing units in the bus. Once data is observed from the sensing unit it will be transferred to control centre for further actions. Transferring of data can be done by using the wired or wireless mode of transmission using WiMAX or using the available cellular networks through the wireless mode of transfer of data. The state estimator to construct the real time power network. In the data injection may happen to alter the measurement of transmission in the power network.

State Estimation: Voltage phase angle from the IEEE bus will be noted by operating persons in the control centre, it is very difficult to measure the phase angle from the power transmission. State estimation mechanism used to find the states of the power system through the power measurements collected from the various sensor nodes of the grid system. Power transmissions through the buses relay on the amplitudes of the voltages and phase angles of the measurements. Data injection attacks will have the take the wrong decision in the system will lead to the blackout in the whole area. There should be some defence mechanism to protect the system from irrelevant vectors added to the estimation. The process of state estimation is used to find whether the power grid is in safer hands. Deference mechanism has Phase Measurements units (PMU) in various location of the grid to monitor the attackers in advance in the system.

Phase Measurements units will be placed in the various centre for the power measurements in the power grid using the uniquely assigned position in the globe to obtain the reading the power in the grid. Placing of PMU in all the place are very expensive do deploy in the power grid. Usage of the graphical methods to study the defence mechanism to protect the system from the various types of the attacks is done. Residual test method is used to alarm the data injection in power grid, power estimation measurements would not

change when the system is in the no – attack state in the system and no abnormality in the grid. Machine learning algorithms will be used to protect from the stealthy attack in the system.

The SCADA in SG is highly vulnerable to various cyber attacks. One such severe threat for the State Estimator in SCADA is the FDI attack. In order to solve this challenging attack, a novel scheme for detecting bad data injection in State Estimation is proposed in this work. This technique detects both stealthy and non-stealthy attacks by using the Continuous Prevention and Detection (CPD) algorithm, which does the mechanism of protecting the SG from attacks in advance and continuously detecting the FDI attacks. If an attack is being detected, it is immediately reported to the control centre of the smart grid system. The proposed algorithm is initiated by the prevention detection attack classification which proceeds by the defence mechanisms of the control centre in the IOT based electric grid.

The equations of the received measurement value can be written in the form of state space equation. When the state space matrix is represented by using time index 'i', is given by the equation 1, where M_i denotes the measurement vector, H represents the measurement matrix, y_i represents the system state vector and u_i denotes the Gaussian noise

$$M_i = Hy_i + u_i \quad (1)$$

Initially collect the value of matrix until the n value of the state estimation vector matrix. For each and every step increment the time index to get the next state vector matrix, get the current value of matrixM_i, y_i, u_i, to compute the value ofM_i. Compute the value $m_i$of $r_i$and based on the above-mentioned formula as given by the equations 2 and 3.

$$m_i = M_i - Hy_i \quad (2)$$

$$r_i = m_i - Hy_i \quad (3)$$

Based on the below results we can check whether attack is present in the system or not. Since FDI attacks are stealthy or non- stealthy attack both these attacks are detected by our proposed shield mechanism. If m_i is less thanT_1, then there does not exist any attack in the system, further m_i is greater than thenT_2, stealthy FDI attack exist in the system. If false data injection attack is predicted it is further reported to the control centre to make the further action to avoid the future attacks in the system. After the type of attack is known the power system prioritizes the corresponding actions to protect the grid system. If any of these attacks are found, then the respective false data vectors are deleted from the system equation of state estimation as shown in the algorithm 1.

Algorithm 1: Continuous Prevention and Detection (CPD)

Inputs: state estimation vector matrix,
Output: Updated W_i and b_i

1. **begin**
2. Initialize counter $i = 0$and get 'n' value.
3. Collect the state estimation vector matrix.
4. Repeat the procedure continuously until $i < n$
5. For each step increment $i = i + 1$
6. Get the current value of the measurement vector M_i, y_i, u_i to compute $M_i = Hy_i + u_i$
7. Compute the values of measurement change vector $m_i = M_i - Hy_i$
8. Compute the value of residual vector $r_i = m_i - Hy_i$
9. If $W_i \leq T_1$, then no FDI attack
10. If else$W_i > c$, then Stealthy FDI attack
11. Else$r_i > T_1$, then Non-Stealthy FDI attack,$T_1, T_2$are predetermined residual value
12. Continue the above steps until FDI attack is found
13. If FDI attack is found, report to the control center

V. Performance Evaluation

In this paper, MATPOWER of MATLAB is used for simulation of the power grid system. The performance evaluation of the the proposed CPD algorithm for detection of FDI attacks is done on the basis of IEEE bus system.

The Attack Noise Ratio (ANR) is used to specify the brutality level of the witnessed attack in any network. It is defined as the ratio of attack power level to the noise power level. Receiver Operating Characteristic (ROC) curve is generated by plotting the probability of detection against the probability of false alarm at various threshold settings. The probability of detection indicates the probability of occurrence of an attack

that has been truly witnessed. The probability of false alarm is the probability of absence of an attack that has been truly witnessed. The proposed scheme is validated for the detection performance even for a higher attack level. Several simulations are done using IEEE 9, 14 and 39 bus systems by incorporating various values of ANR like 10,12, 6 dB for both non-stealthy and stealthy attacks.

Here for FDI attacks, both the stealthy as well as non -stealthy attacks are considered, the probability of detection vs. indicates probability of FDI attacks is presented. The probability of FDI attacks represents the number of attacks occurred and the probability of detection represents the number of attacks that are detected by our proposed Continuous Prevention and Detection CPD algorithm. For the comparison of the performance of proposed algorithm compared to the existing method to detect both stealthy and non-stealthy attacks based on the IEEE 39,14,9 bus System.

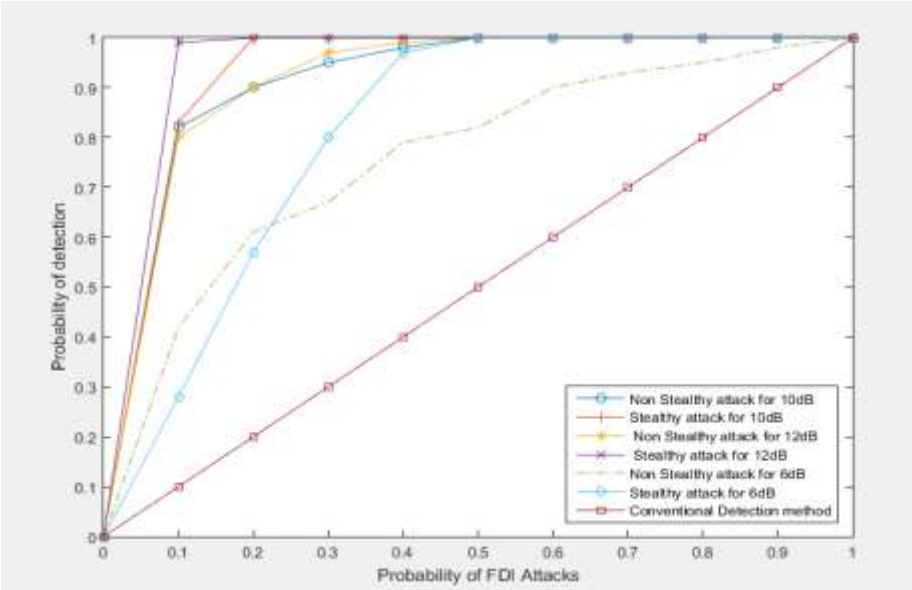

Figure 2. Performance comparison of CPD algorithm with conventional method for IEEE 9 bus system

s

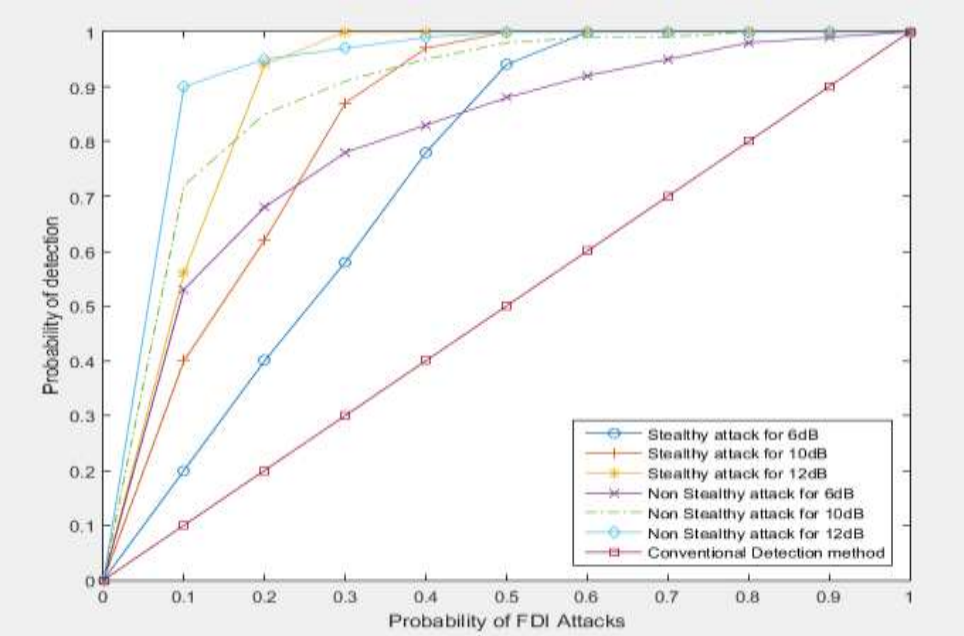

Figure 3. Performance comparison of CPD algorithm with conventional method for IEEE 14 bus system

In Figure 3, the probability of FDI attacks are estimated using IEEE 14 bus system by incorporating various values of ANR like 10,12, 6 dB for both non-stealthy and stealthy attacks. Even when the ANR is increased, the proposed system detects both the stealthy and non-stealthy attacks with a higher detection

probability, exponentially increasing. The random prediction line is obtained using the conventional detection approach. The ROC curve obtained using the proposed scheme are all above the random prediction line, which means that the system performs well in classifying and detecting attacks. The proposed CPD approach successfully detects stealthy attacks around 90% and non-stealthy attacks around 92%.

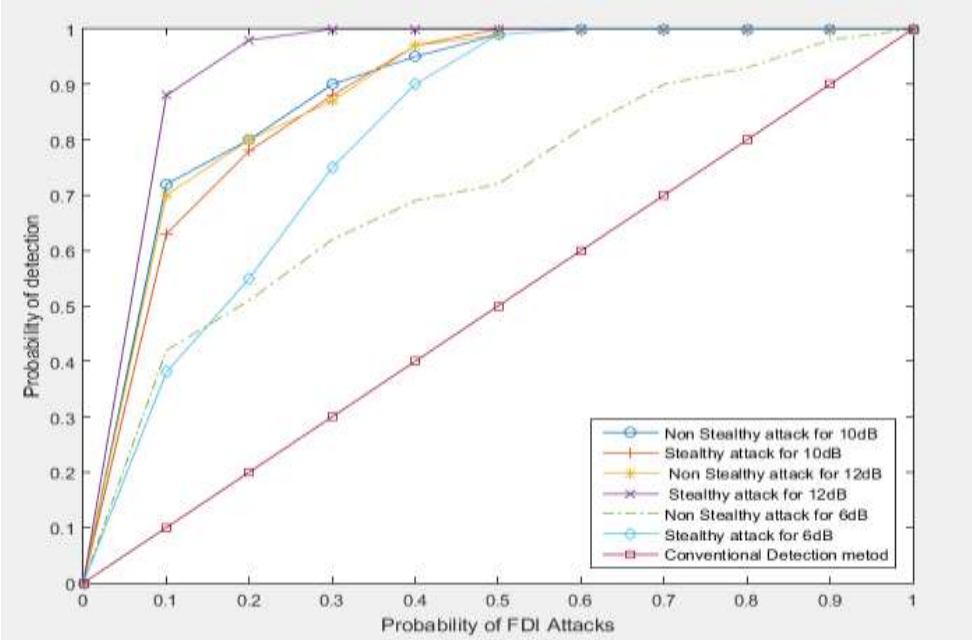

Figure 4. Performance comparison of CPD algorithm with conventional method for IEEE 39 bus system

In Figure 4, the probability of FDI attacks are estimated using IEEE 39 bus system by incorporating various values of ANR like 10,12, 6 dB for both non-stealthy and stealthy attacks. Even when the ANR is increased, the proposed system detects both the stealthy and non-stealthy attacks with a higher detection probability, exponentially increasing. The proposed CPD approach successfully detects stealthy attacks around 89% and non-stealthy attacks around 70%.The proposed detection mechanism achieves the better detection probability for detecting the stealthy and non stealthy FDI attacks compared with the conventional method.

VI. CONCLUSION

In this paper, Smart Grid's security issues are discussed along with the basis and the types of false data which occur in the state estimation of the SCADA. For detecting the cyber security attacks in SG, novel shield mechanism constructed on the Continuous Prevention and Detection (CPD) algorithm which does the mechanism of either protecting the SG from attacks in advance or continuously deleting the FDI tacks. The proposed algorithm is initiated by the attack classification which proceeds by the defence mechanism of the control centre of the electric grid.

REFERENCES

1. Jing Jiang and Yi Qian, "Defense Mechanisms against Data Injection Attacksin Smart Grid Networks," IoT and Information Processing in Smart Energy Applications, IEEE Communications Magazine, October 2017.
2. Wen-Long Chin, Wan Li, and Hsiao-Hwa Chen, "Energy Big Data Security Threats in IoT-Based Smart Grid Communications," IoT and Information Processing in Smart Energy Applications, IEEE Communications Magazine, October 2017.
3. Md Masud Rana, Li Li, and Steven W. Su, "Cyber Attack Protection and Control of Microgrids," IEEE/CAA Journal Of AutomaticaSinica, October 2017.
4. Mohammad Esmalifalak, Student Member, IEEE, Lanchao Liu, Student Member, IEEE, Nam Nguyen, Student Member, IEEE, Rong Zheng, Senior Member, IEEE, and Zhu Han, Fellow, IEEE, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid," IEEE Systems Journal, Vol. 11, No. 3, September 2017.

5. Youbiao He, Student Member, IEEE, Gihan J. Mendis, Student Member, IEEE, and Jin Wei, Member, IEEE, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," IEEE Transactions on Smart Grid, Vol. 8, No. 5, September 2017.
6. Ting Liu, (Member, IEEE), Jue Tian, YuhongGui, Yang Liu, and Pengfei Liu, "SEDEA: State Estimation-Based Dynamic Encryption and Authentication in Smart Grid," Special Section on Security Analytics and Intelligence for Cyber Physical Systems, August 22, 2017.
7. Gaoqi Liang, Student Member, IEEE, Junhua Zhao, Member, IEEE, Fengji Luo, Member, IEEE, Steven R. Weller, Member, IEEE, and Zhao Yang Dong, Senior Member, IEEE, "A Review of False Data Injection Attacks Against Modern Power Systems," IEEE Transactions on Smart Grid, Vol. 8, No. 4, July 2017.
8. Suzhi Bi and Ying Jun (Angela) Zhang, "Graph-based Cyber Security Analysis of State Estimation in Smart Power Grid," IEEE Communications Magazine, April 2017.
9. Yi Yang, Member, IEEE, Hai-Qing Xu, Lei Gao, Yu-Bo Yuan, Kieran McLaughlin, and SakirSezer,"Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks," IEEE Transactions on Power Delivery, Vol. 32, No. 2, April 2017.
10. Xinyu Wang, XiaoyuanLuo,Yuyan Zhang, and XinpingGuan,"Detection and Isolation of False Data Injection Attacks in Smart Grids via Nonlinear Interval Observer", IEEE Internet of Things, vol. 6, no. 4, august 2019.
11. Ruilong Deng, Peng Zhuang and Hao Liang, "False Data Injection Attacks Against State Estimation in Power Distribution Systems", IEEE TransactionsonSmart Grid, vol. 10, n0. 3, May 2019.
12. Da-Tian Peng,JianminDong, and Qinke Peng, "Overloaded Branch Chains Induced by False Data Injection Attack in Smart Grid", IEEE Signal Processing Letters, vol. 27, 2020.