A Survey on Bad Data Injection Attack in Smart Grid

Dai Wang, Xiaohong Guan, Ting Liu*, Yun Gu, Yanan Sun, Yang Liu
Ministry of Education Key Lab for Intelligent Networks and Network Security,
School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi, China
{daiwang, xhguan, tliu, ygu, ynsun, yliu }@sei.xjtu.edu.cn

***Abstract*— Bad data injection (BDI) is one of the most threatening attacks in smart grid, as it may cause energy theft of end users, false dispatch on the distribution process, and device breakdown during power generation. In this paper, the BDI attack is defined as a cyber-physical attack which is a combination of two aspects: 1) on the cyber side, modern attack techniques are exploited to intrude and inject bad data into the information system; 2) on the physical side, attackers construct the bad data to bypass the traditional error detection in power systems. Related work on BDI construction and implementation are reviewed. An attack simulation is constructed to illustrate how to launch a BDI attack. The countermeasures against the BDI are also summarized from the views of cyber-orientation, physical-orientation. Finally, our work on cyber-physical fusion detection is presented.**

***Index Terms*-- smart grid; security; bad data injection; cyber-physical fusion.**

I. INTRODUCTION

Smart grid provides a desirable infrastructure for efficient energy consumption and transmission, by integrating traditional power grids with information networks. Since state measurements, price information and control actions are transmitted via information network, various attacks (such as eavesdropping, information tampering and malicious programs) which have almost ruined the Internet would impose great threats on the security and stability of smart grid.

Bad Data Injection (BDI) attack has drawn wide concerns in smart grid, which is firstly proposed by Liu and Ning [1]. They proved that attackers can introduce bad data into certain state variables and bypass the existing techniques for bad measurement detection in power system, exploiting the knowledge of the power system configurations. After that, researchers further proposed many physics-law-based algorithms to detect the well-designed bad data [2-10].

Unlike the traditional power grid, in which control centers are relatively isolated and protected, the advanced metering infrastructures (AMI) in smart grid is large in amount, widely distributed and inter-connected to the communication network. With modern cyber-attack technologies, it is not difficult to control the electrical terminals and intrude into the communication network [11-13]. The hackers can modify the smart meter readings to fool the billing systems [14]. In industrial field, the BDI attack can disturb the balance between demand and supply, increase the cost for energy distribution, and mislead the control center to make erroneous decisions [4, 15]. For the terrorists, the BDI attack can result in massive damage on local or national power infrastructure [14].

In our work, we define the BDI attack as a cyber-physical attack which is a combination of two aspects: 1) on the cyber side, information techniques are exploited to intrude and inject bad data into the information system; 2) on the physical side, the attackers carefully construct the bad data to bypass traditional error detection system. An attack case which combines technologies from two sides is constructed to show how to falsify meter readings and launch a BDI attack.

Attack technologies on the cyber side are the foundation of the BDI attack. Attackers get access to smart meters and revise meter readings through some cyber techniques like password cracking, authentication evading and historical data replay. Bad data construction on the physical side does not refer to physically modify the electric circuits. It focuses on the construction of false measurements against the bad data detection mechanism in power systems. A BDI attack requires cyber intrusion into the communication networks and modification on measurements bypassing bad data detection simultaneously.

Since cyber side and physical side are both crucial to the BDI attack, the countermeasures can be proposed from these two perspectives. Many efforts have been devoted to defend the system from BDI attacks on the physical side [4, 5, 8] [16-19], utilizing the information from historical data, the installation of Phasor Measuring Unit (PMU) and the topology of power grid. From another perspective, to ensure the correct functioning of smart grid, it is essential that communications are secured [12, 20]. Some cyber technologies such as authentication [21-22] and dynamic key [23] are used to protect the information security. However, the countermeasures simply from the view of cyber-orientation or physical-orientation are inadequate for complex cyber-physical attacks. The tight coupling between communication network and power grid introduces the rethinking of traditional objective of countermeasures. Once BDI attack is launched, both cyber network and power grids will present interactive reaction in different forms. The cyber-physical fusion strategies should be a better solution to detect BDI attacks.

The rest of this paper is organized as follows: In Section II, we review related work on BDI techniques on both cyber side

Ting Liu is the corresponding author of this paper.
This project was supported by National Natural Science Foundation of China (Grant Nos. 60921003, 61203174, 91018011, 91118005, 912183001), Key Projects in the National Science & Technology Pillar Program (Grant No.2011BAK08B02), Doctoral Fund of the Ministry of Education in China (Grant No. 20110201120010), and Fundamental Research Funds for the Central Universities.

and physical side. In Section III, an attack case is constructed to show how to launch a BDI attack. In Section IV, the countermeasures against BDI are presented from the views of cyber-orientation and physical-orientation. Our works on fusion detection are also introduced in this section. The concluding remarks on the BDI attack then follow in Section V.

II. BAD DATA INJECTION ATTACK

A BDI attack in smart grid is a combination of cyber side (for network intrusion and data injection) and physical side (for the bad data construction). In this section, the related methods for the BDI attack are summarized.

A. Cyber Side

Techniques on the cyber side are the foundation of the BDI attack. The basic target for cyber attack is to obtain the authorization to make invalid operations on smart meters or network communication.

- **Device-failure attack** aims to make the smart meters or communication network out of response through DoS (Denial of Service)/DDoS (Distributed Denial of Service) attack. The maximum capacity of connection for smart meters, especially the infrastructures deployed in Home Area Networks (HAN), is extremely limited (usually fewer than 20 connections [24]). The attack will result in the delay or failure of data communication. Since the compromised meters may be out of work in a short duration, the attacker can disguise as a host which has the IP address or MAC of the compromised smart meters to send the false data package to the control center.
- **Password-cracking attack** is a classical method to get the access to devices. The modification of smart meter settings often requires authentication. However, considering the limited computational resource and storage, smart meters are not equipped with complex password mechanisms. We know that for smart meters, the password is made up of four numerical digits and only several seconds are needed to crack it.
- **Authentication-identifying attack** is another way to get the access for smart meters. Some smart meters [24] are equipped with complex password mechanisms. However, for most smart meters, communication protocol is Modbus/TCP or DNP 3.0/TCP, in which information is transmitted as plaintext. Attackers can monitor the traffic flow to identify critical operations on smart meters requiring authentication, such as modifications of system time, IP addresses and firmware updates. If the package including authentication information is identified, attackers can seize the password and obtain access to smart meters.
- **Worm attack** makes use of the package sending/receiving function of smart meters. For large-scale deployed smart meters, manual firmware update for every terminal user is inconvenient and impractical. An aggregator server will provide the update service for directly connected meters. Attackers can get control of the server and inject a worm into the firmware to be updated. The injected worm will change the authentication mechanism of the meter and even send update commands to other meters which lead to a large-scale spread of the worm [25].
- **(Hybrid) Attack graph** is to struggle against the Intrusion Detection System (IDS) system deployed in communication networks in smart grid [26]. Compared with the traditional attack graph, hybrid attack graph includes both cyber and physical parameters and helps the attackers quickly identify the key sensors in cyber networks. The difficulty against this attack is the limitation of the investments on secure meters and the variety of the attack paths.

Cyber attack on communication networks in smart grid is currently based on the limited computational resource and the vulnerability on transmission protocols. Since it is not possible to equip the household smart meters with high-performance hardware, the cyber-security for smart grid is still critical and dangerous.

B. Physical Side

With the cyber attack intruding into the communication network, attackers can change the meter readings and feed the tampered data back to the control center. When attackers are armed with the knowledge of power system configurations, they can construct bad data according to the physical model of smart grid, bypassing the bad data detection. Supposing a smart grid with N buses, a model-based view of the power grid is shown as follows:

$$z = h(x) + e \tag{1}$$

where x denotes the states variables including the voltage magnitude and phase angle; z denotes the measurements including the injected active or reactive power flow for each bus, active or reactive power flow on transmission lines, etc. h presents the physical relationship between state variables and measurements; e is the measurement noise which is a Gaussian noise with mean value of 0 and covariance R. In smart grids, measurements are collected and uploaded to the control center State variables are estimated from the measurements with Weighted Least Squares (WLS) in practice [27].

On the physical side, the measurements are maliciously tampered by attackers as follows:

$$z = h(x) + e + a \tag{2}$$

where a is the attack vector. The traditional bad data detection in power system is based on the residual between the real values of measurements and the estimated ones. Since the measurement noise is a Gaussian noise with mean value of 0 and covariance R, if the difference between estimated measurements $\hat{z}$ and the real measurements z exceeds the tolerance threshold, i.e. $|\hat{z} - z| > \tau$, the bad data will be detected [28]. A stealth BDI aims to construct an attack vector a free from the bad data detection in power systems.

1) Undetectable BDI

Liu [1] firstly proposed the undetectable BDI against the traditional detection. The basic idea of the undetectable BDI is to construct the attack vector a on DC model as follows:

$$z = Hx + e + a = H(x + c) + e \tag{3}$$

where H is the Jacobian Matrix of $h(x)$ since there is an approximate linear relationship between state variables and measurements in DC model. The attack vector satisfies $a = Hc$ so that the residual between the injected measurements and the true value will never exceed the detection threshold.

Since the number of devices cracked by the adversary is usually limited, Sandberg [2, 29] proposed the BDI with minimum number of compromised sensors. Hug and Giampapa [30] presented an algorithm based on graph theory which allows determining how many and which measurement signals an attacker will attack in order to minimize his efforts in keeping the attack hidden from bad data detection. Kosut [16] considered the smallest set of attacked measurements capable of the network unobservability using a graphic theory. Giani [13] proposed an algorithm to find all unobservable attacks involving the compromise of exactly two power injection meters. Ozay [31] introduced two distributed sparse attack models including the Distributed Sparse Attacks, in which attackers modified local measurements, and Collective Sparse Attacks, in which attackers will gain extra topology information to realize a sparse attack. Mohammad [5] assumed that the attackers are with no topology information and ICA analysis is introduced to construct the attack vector. Jia [32] examined the effects of nonlinearity in the power systems on the effectiveness of malicious data attack on state estimation and demonstrated that attack algorithms designed for DC model may not be effective when they are applied to nonlinear system with nonlinear state estimators. Liu [4] studied the BDI for AC model based on the tolerance of transmission errors of traditional bad data detection mechanism in power grid. In addition, undetectable BDI attacks have a great influence on the electric market. Detailed analysis is made on the electric market with the impact of the undetectable BDI in smart grid [6, 18, 33-35].

2) Network Topology BDI

The basic idea of undetectable BDI is based on the static model of the power grid. It means that the function model $h(x)$ is time-invariant. However, the operation of smart grid is a dynamic process which contains the change of switch status. In this case, the control centers will receive two types of measurements, one is the meter measurement and the other is status of breakers. Kim [36] proposed the BDI scheme on network topology by modifying both meter data and breaker status simultaneously.

3) Time Stamp/Synchronization BDI

PMU (Phasor Measuring Unit) is deployed in smart grid to collect the measurements more precisely. Thus, a new idea for BDI is to crack the time synchronization mechanism in smart grid. Gong [37] proposed a time stamp attack by spoofing the GPS. By sending a forged signal to the GPS receiver, hackers can implement the attack even without get access into the communication networks. This attack scheme leads to the failure of the basic application of PMU system including transmission line fault detection, voltage stability monitoring and regional distributed event location.

Bad data constructions on the physical side are mostly based on the physical model of the power grid. Moreover, it is a significant difference from the conventional attack on Internet. The adversary not only aims at stealing user's private information but also create a physical consequence such as energy theft, system failure and erroneous dispatch. Therefore, a combination of cyber side and physical side will lead to serious threats on smart grid.

III. ATTACK SIMULATION

In this section, an attack case which combines technologies from both cyber and physical sides is constructed to show how to intrude into smart meters and launch a BDI attack.

A. Smart Meter Intrusion

Cyber techniques are the foundation of the BDI. The basic target for cyber-attacks is to obtain the authorization to make invalid operations on smart meters or network communications. An experimental platform on vulnerability assessment shown in Fig. 1 is built to illustrate that attackers can obtain access to smart meters through cyber techniques and change measurement values bypassing the energy conservation test. Three smart meters (I-III) are deployed to monitor power parameters. All of them are connected to the same switcher (IV) and wireless router (V). The consumption of electric kettle (VI) and desk lamp (VII) are measured by Meter (I) and (II) respectively. The total energy is measured by Meter (III). An attack tool (VIII) is developed for the adversary.

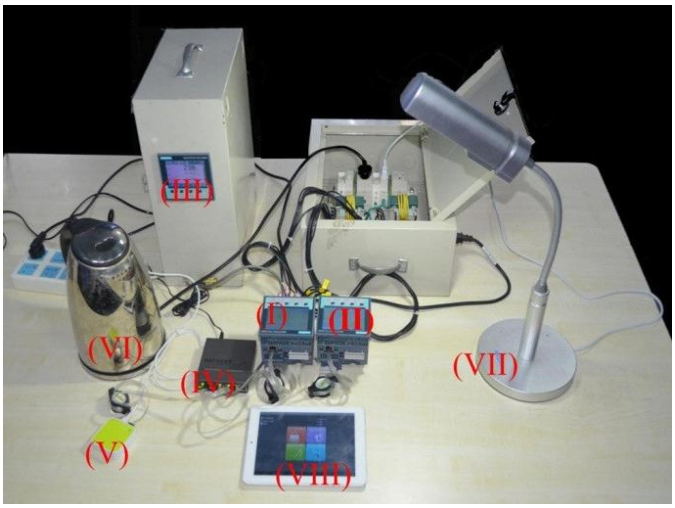

Fig.1 Experimental platform on vulnerability assessment

For most smart meters, communication protocol is Modbus/TCP or DNP 3.0/TCP. The port of Modbus/TCP is 502 and the port of DNP3.0/TCP is 20000 by default. In the attack simulation, we first scan all hosts in the network segment, trying to find devices with opened Port 502 or 20000. Next, two special hosts are found and marked to be suspicious. We further communicate with these devices to obtain their product types and make sure they are smart meters.

Then we exploit the vulnerability on plaintext transmission to intrude into smart meters. As mentioned in Section II, for most smart meters, communication protocol is Modbus/TCP or DNP 3.0/TCP, in which information is transmitted as

plaintext. We monitor the traffic flow to identify critical operations on smart meters requiring authentication, such as modifications of system time, IP addresses and firmware updates. If the package including authentication information is identified, we can seize the password and obtain access to smart meters.

With successful intrusion, we try to change measurement values bypassing the energy conservation test. For most smart meters, measurement values such as active power and reactive power are read-only. However, some settings such as time and current transformer (CT) ratio are writable. A CT is used for measurement of alternating electric currents. The CT ratio *K* is defined as: $K = I_1 / I_2$, where I_1 is the primary current and I_2 is the secondary current. The values of active power and reactive power will increase or decrease in proportion to the change of *K*.

In this simulation, the proper CT ratio of the three meters is 5:1. The active power measurements of smart meters (I-III) are 2,000W, 20W and 2,020W. We falsify CT ratios of Meter I and Meter II to be 5:100 and 500:1 respectively, which will reverse the measurement values of Meter I and Meter II. The active power measurement of Meter III is still 2,020W, which is the sum of Meter (I) and Meter (II). This falsification successfully evades the test of energy balance. Simulation on smart meter intrusion shows that attackers can change the measurements through revising CT ratios of smart meters.

B. A BDI Attack on IEEE 14-bus System

A simulation is constructed to inject bad data into the IEEE 14-bus system as shown in Fig. 2. Measurements of active power are changed by falsifying the CT ratio of smart meters. This attack case is illustrated to prove that it is possible to bypass traditional bad data detection through hiding the injected data among the normal observation errors.

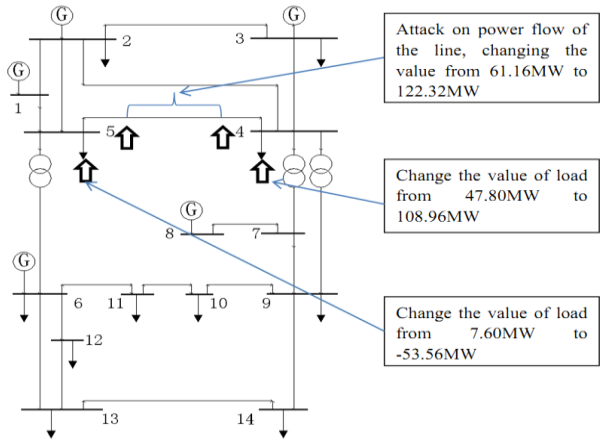

Fig. 2. An attack case on IEEE 14-bus system

The original load on bus_5 and bus_4 are 7.60MW and 47.80MW, respectively. The power flow on the transmission line $L_{5,4}$ is 61.16MW. In the attack case, the hacker tries to move 60.96MW of power load from bus_5 to bus_4. Thus, the load on bus_5 and bus_4 and the power flow on the transmission line $L_{5,4}$ are modified to -53.56 MW, 108.96MW and 122.32MW respectively to maintain the power balance of these buses. The revised data is analyzed with the state estimation and the weighted sum-squared residual (WSSR) is 67.5471, which is less than the chi-squares test threshold 72.1532. This shows that the traditional bad data detection method is inadequate and unable to detect this attack, and measurements will be assumed to be free of bad data.

IV. COUNTERMEASURES AGAINST BAD DATA INJECTION

Defending BDI attacks in smart grid has drawn a lot of efforts in recent years. This section begins with the work on detecting the cyber attack with the help of information technologies. For physical side, the study on bad data detection in power systems will be summarized. Our work on the Cyber-Physical fusion detection will also be introduced.

A. Cyber Defense

Cyber Defense against BDI mainly focuses on data transmission and access authentication.

- **Strict authentication** is required in communication networks of smart grid. Access to critical meters and the data fed to the control center should be authenticated to confirm that a communication entity is the claimed one. A lot of information techniques are available for this problem. IEC62351 deals with the cyber security for power systems management. Time stamps are used to prevent the replay attack .The secure protocols such as Transport Layer Security Protocol (TLS) or Secure Sockets Layer (SSL) and hashed keys such as Secure Hash Algorithm (SHA) or Hash Message Authentication Code (HMAC) are adopted in this standard to prevent the invalid access and forged messages in communication networks [21-22].
- **Dynamic key management** is a good solution to protect the system from traffic monitoring and replay attack in smart grid. Liu [23] proposed a dynamic secret-based encryption method which makes use of the package loss and retransmission in data exchange. The status of retransmission will be hashed and adopted for dynamic key between the valid users and smart meters. Gharavi [38] proposed a dynamic key refreshment mechanism to enhance the security of IEEE 802.11s standards against the DoS/DDoS attack in smart grid.
- **WSN-featured defense** has drawn huge concern for the wide use of wireless sensor networks (WSN) in smart grid. Wang [39] investigates the physical-layered security for WSN against the BDI. For wireless adapters, the basic actions such as SLEEP, RECEIVE and AWAKE follow a regular sequence in normal cases. Kher [40] proposed a model for monitoring the smart grid against malicious activities or attacks using machine learning techniques.

B. Physical Defence

Since Liu [1] firstly proposed the undetectable BDI attack, a lot of efforts have been devoted to prevent such attack schemes in smart grid [7-10]. The conventional detection model is inadequate in smart grid.

1) Quickest Detection

Conventional bad data detection mechanism in power grid use measurements for state estimation and bad data detection at each sampling time. In smart grid, smart meters are often equipped with the storage for historical data which can be used to detect the abrupt changes in measurements. Huang [3] proposed a defense mechanism against the stealth BDI based

on CUSUM Test. Since the statistical model of adversary attacks is unknown, the generalized likelihood ratio test (GLRT) is used to replace the estimated parameters in Cumulative Sum (CUSUM) Test. The proposed work demonstrated a minimum detection delay in comparison with other detection method based on sequence data.

2) Dynamic Model based Detection

In classical research on power systems, the power grid is often described as a load-flow equation for the power flow through different buses. State estimation and the bad data detection are based on this static model. However, in smart grid, the dynamic features of the physical model should be further concerned since the smart meters can obtain sufficient power parameters. Pasqualetti [17] modeled the smart grid as a linear time-invariant system and analyzed the detectability and identifiability of BDI under a Kron-presentation. Moreover, a dynamic detection method for BDI is proposed. Huang [19] introduced the Kalman Filter and Artificial Neural Network (ANN) into bad data detection. The state estimation is carried out with Extended Kalman Filter and the trained ANN to detect the bad data from the raw measurements.

3) Correlation Analysis based Detection

Optimal Power Flow (OPF) has been widely used to make real-time decisions for energy dispatch. In normal cases, the input measurements and the output of OPF can be considered following a regular relationship. Valezunela [41] used Principal Component Analysis (PCA) to separate the power flow variability into regular space and irregular space. The further analysis on irregular space indicates the existence of compromised measurements in smart grid.

4) Distributed Detection

In a large-scaled smart grid, attackers can make use of the detector's tolerance on normal cumulative observation noises and construct the injected bad data evading bad data detection in power grid [4]. Moreover, the computational complexity and storage consumption should also be taken into account. Zhang [18] proposed a distributed intrusion detector in which by developing and deploying an intelligent module, the analyzing modules are embedded at each level of the smart grid. The use of the support vector machine helps to detect and classify malicious data and possible cyber attacks.

C. Cyber-Physical Fusion Defence

BDI in smart grid introduces interactive reaction both in cyber network and power grid. Invalid access to some infrastructures, anomaly traffic or alarm triggers will be emerged by cyber attacks. And for attacks on the physical side, the power conservation may be violated according to the meter readings. Therefore, cyber-physical fusion strategies are considered to be better solutions to BDI attacks.

In our work, a cyber-physical fusion strategy is proposed. The basic idea is to make a fusion of consistency check of power measurements and abnormality detection on traffic flows. As shown in Fig.3, the framework consists of three modules: for the cyber network, Snort is deployed to monitor the network traffic and detect abnormal packets; for the physical system, an Energy Conservation module is exploited to check the consistency of smart meter readings; and the Fusion module detects the attacks by fusing the alerts of information network and physical inconsistent measurement.

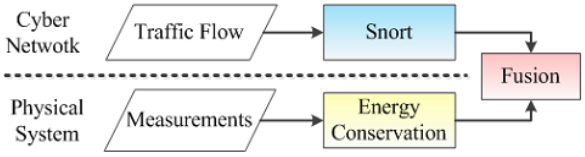

Fig. 3. Main Framework of Cyber-Physical Fusion

In cyber network, Snort is exploited to monitor the network traffic. In our work, several rules are designed to detect the packets that are used to read or write the important and sensitive states of smart meters. The Snort alerts are recorded in an alarm log with attack type and priority, which is indexed by IP and Timestamp.

For physical system, all the physical restrictions including the system topology, Kirchhoff's current/voltage law and energy conservation can be exploited for power data consistency check. Considering the imprecise synchronism of different devices, the entire system model is built by adopting energy conservation that can mitigate the synchronization problem. This model is suitable for a neighbor-area network, where multiple home-area networks (HAN) or business-area networks (BAN) are hosted. For either of them, the total injection energy is measured, as well as the consumption nodes of different electric appliances. Therefore, the system consistency can be verified according to the physical topology by applying energy conservation check within HANs or BANs.

Finally, a physical-directed fusion method is introduced to correlate the alerts of cyber and physical systems. The fusion module will trace the cyber alerts for correlation analysis to detect attacks once triggered by the physical alarms. In our work, physical data consistency is verified every T_{phy}, while a moving timing channel is applied to the cyber network to retrieve the Snort alarm log within T_{cyber} considering the duration extension of the cyber attacks. IP address is selected to build the connection between the inconsistent data and Snort alerts. Once the measurements of power system is inconsistent, the fusion module will refer to the Snort alarm log using IP address and timing window to locate the victim physical HANs or BANs, trace the malicious attackers and identify the attack purpose.

V. CONCLUSION

In this paper, we define the BDI as a cyber-physical attack. Basic attack methods and countermeasures are summarized from both cyber side and physical side. A simulation is presented to illustrate how attackers intrude into smart meters and launch BDI attacks. We believe that current countermeasures solely derived from the view of physical-orientation or cyber-orientation are inadequate. For cyber defense, the inherent properties of electrical parameter in smart grid have not been concerned. For physical defense, the integrity and validity of power grid data cannot be ensured. Therefore, we conclude that the cyber-physical fusion is a

better solution, which combining the features of cyber network and the physical models of power system. Finally, a brief introduction about our work on fusion detection is presented.

REFERENCES

[1] Y. Liu, P. Ning and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids,", *Proceedings of the 16th ACM conference on Computer and communications security*, 2009.

[2] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. Smart Grid Communications (SmartGridComm), 2010.*

[3] Y. Huang, H. Li, K. A. Campbell and Z. Han, "Defending false data injection attack on smart grid network using adaptive cusum test," in *Proc. 2011 Information Sciences and Systems (CISS)*, 2011.

[4] T. Liu, Y. Gu, D. Wang, X. Guan and Y. Gui, "A Novel Method to Detect Bad Data Injection Attack in Smart Grid," in *Proc. IEEE INFOCOM Workshop on CCSES*, 2013.

[5] Y. Huang, et al., "Bad data injection in smart grid: attack and defense mechanisms," *Communications Magazine, IEEE*, vol.51, pp. 27-33, 2013.

[6] M. Esmalifalak, G. Shi, Z. Han and L. Song, "Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study", *IEEE Transactions on Smart Grid*, vol.4 , pp:106-169, 2012.

[7] A. Tarali and A. Abur, "Bad data detection in two-stage state estimation using phasor measurements," in *Proc. Innovative Smart Grid Technologies (ISGT Europe), 2012*.

[8] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Proc. Preprints of the First Workshop on Secure Control Systems*, 2010.

[9] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang and W. Zhao, "On False Data Injection Attacks against Power System State Estimation: Modeling and Countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, 2013.

[10] B. Gou and R. Kavasseri, "A pre-procedure of bad data detection for smart grid monitoring," in *Power and Energy Society General Meeting, IEEE*, 2012.

[11] H. Khurana, M. Hadley, N. Lu and D. A. Frincke, "Smart-grid security issues," *Security & Privacy, IEEE*, vol.8, pp. 81-85, 2010.

[12] R. Q. Hu, Y. Qian, H. Chen and H. T. Mouftah, "Cyber security for smart grid communications: part II [Guest Editorial]," *Communications Magazine, IEEE*, vol.51, pp. 16-17, 2013.

[13] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and K. Poolla, "Smart Grid Data Integrity Attacks,", *IEEE Transactions on Smart Grid*, vol.4 , pp:1244-1253, 2013.

[14] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *Security & Privacy, IEEE*, vol.7, pp. 75-77, 2009.

[15] J. Lin, W. Yu, X. Yang, G. Xu and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *IEEE/ACM Third International Conference on Cyber-Physical Systems (ICCPS)*, , 2012.

[16] O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious data attacks on the smart grid," *Smart Grid, IEEE Transactions on*, vol.2, pp. 645-658, 2011.

[17] F. Pasqualetti, F. Dorfler and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, 2011.

[18] Y. Zhang, L. Wang, W. Sun, R. C. Green and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *Smart Grid, IEEE Transactions on*, vol.2, pp. 796-808, 2011.

[19] C. Huang, K. Shih, C. Lee and Y. Wang, "Application of Kalman Filter to Bad-Data Detection in Power System," InTech , 2010.

[20] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol.100, pp. 210-224, 2012.

[21] D. von Oheimb, "IT Security architecture approaches for Smart Metering and Smart Grid," *Smart Grid Security. Springer Berlin Heidelberg*, pp. 1-25, 2013.

[22] C. Rosinger and M. Uslar, "Smart Grid Security: IEC 62351 and Other Relevant Standards," *Standardization in Smart Grids. Springer Berlin Heidelberg*, pp. 129-146, 2013.

[23] L. Ting, L. Yang, S. Yao, M. Yashan and G. Xiaohong, "A dynamic secret-based encryption method in smart grids wireless communication," *IEEE Transactions on Smart Grid*, pp. 1-5, 2013.

[24] G. D. E. Inc., EPM 9800 Instruction Manual (Rev. A3), 2008.

[25] D. Seo, H. Lee and A. Perrig, "Secure and Efficient Capability-Based Power Management in the Smart Grid," in *IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011*.

[26] P. J. Hawrylak, M. Haney, M. Papa and J. Hale, "Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid," in *5th International Symposium on Resilient Control Systems (ISRCS), 2012*.

[27] E. Handschin, F. C. Schweppe, J. Kohlas and A. Fiechter, "Bad data analysis for power system state estimation," *Power Apparatus and Systems, IEEE Transactions on*, vol.94, pp. 329-337, 1975.

[28] A. G. E. Ali Abur, Power System State Estimation Theory and Implementation, CRC Press, 2004.

[29] K. C. Sou, H. Sandberg and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *IEEE Conference on Decision and Control and European Control Conference, 2011*.

[30] G. Hug and J. A. Giampapa, "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks," *Smart Grid, IEEE Transactions on*, vol.3, pp. 1362-1370, 2012.

[31] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni and H. Vincent Poor, "Distributed models for sparse attack construction and state vector estimation in the smart grid," in *IEEE Third International Conference on Smart Grid Communications, 2012*.

[32] L. Jia, R. J. Thomas and L. Tong, "On the nonlinearity effects on malicious data attack on power system," in *Proc. 2012 Power and Energy Society General Meeting, 2012 IEEE*, pp. 1-8.

[33] L. Xie, Y. Mo and B. Sinopoli, "False data injection attacks in electricity markets," in *2010 First IEEE International Conference on Smart Grid Communications, 2010*.

[34] M. Esmalifalak, Z. Han and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Proc. 2012 Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, pp. 2468-2472.

[35] L. Jia, R. J. Thomas and L. Tong, "Impacts of Malicious Data on Real-Time Price of Electricity Market Operations," in *45th Hawaii International Conference on System Science (HICSS), 2012*.

[36] J. Kim and L. Tong, "On Topology Attack of a Smart Grid," *2013 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2013.

[37] S. Gong, Z. Zhang, H. Li and A. D. Dimitrovski, "Time stamp attack in smart grid: Physical mechanism and damage analysis," arXiv preprint arXiv:1201.2578, 2012.

[38] H. Gharavi and B. Hu, "Dynamic key refreshment for smart grid mesh network security," in *Proc. 2013 Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pp. 1-6.

[39] X. Wang, Q. Liang, J. Mu, W. Wang and B. Zhang, "Physical layer security in wireless smart grid," *Security and Communication Networks*, 2013.

[40] S. Kher, V. Nutt, D. Dasgupta, H. Ali and P. Mixon, "A detection model for anomalies in smart grid with sensor network," in *Proc. 2012 Future of Instrumentation International Workshop (FIIW)*, 2012, pp. 1-4.

[41] J. Valenzuela, J. Wang and N. Bissinger, "Real-Time Intrusion Detection in Power System Operations," *Power Systems, IEEE Transactions on* , vol.28, pp. 1052-1062, 2013.