Bad Data Detection Method for Smart Grids based on Distributed State Estimation

Yun Gu, Ting Liu*, Dai Wang, Xiaohong Guan, Zhanbo Xu
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
{ygu, tliu, daiwang, xhguan, zbxu}@sei.xjtu.edu.cn

***Abstract*—Bad Data Injection (BDI) in Smart Grid is considered to be the most dangerous cyber attack, as it might lead to energy theft on the end users, false dispatch on the distribution process, and device breakdown on the power generation. State Estimation and Bad Data Detection, which are applied to reduce the observation errors and detect false data in the traditional power grid, could not detect the bad data in smart grid. In this paper, three BDI attack cases in IEEE 14-bus system are designed to bypass the traditional bad data detection. The potential risks on economy and security are analyzed exploiting the MATPOWER. A new method based on Distributed State Estimation (DSE) is proposed to detect BDI, named as DSE-based bad data detection. The power system is divided into several subsystems, and a Chi-squares test is applied to detect the bad data respectively in each subsystem. Simulation results demonstrate that the DSE-based bad data detection can detect all bad data in three attack cases. Moreover, it can locate the bad data in specific subsystem which is helpful for the further identification.**

***Keywords* — Smart Grid; security; bad data detection; distributed state estimation; bad data injection.**

I. INTRODUCTION

In smart grids, the information techniques are applied to the power system to provide a desirable infrastructure for real-time measurement, transmission, decision and control. Various attacks (such as eavesdropping, information tampering and malicious programs) that have almost ruined the Internet would impose great threat on security and stability of smart grids. Since the data in smart grid can easily be monetized, the bad data injection is extremely attractive for hackers (e.g. the hackers can manipulate their energy costs by modifying the smart meter readings). Furthermore, the bad data would mislead the control center to take erroneous actions, thus it is extremely dangerous for smart grids. For example, in 2010, Iran's Bushehr nuclear plant was cracked by Stuxnet worm which updated the false system state to SCADA to stop the system protection strategies.

Power system state estimation and bad data detection is considered as a good solution to detect injection data, which is applied to reduce the observation errors and detect false data in the SCADA. Schweppe [1] firstly introduced the concept of power system state estimation and employed Weighted Least Squares (WLS) method to solve this problem in 1969. Xiang et al. [2] presented an approach for detection and identification of multiple bad data. This approach was developed in order to improve the performance of static state estimators of power systems. Cutsem and Pavella [3] presented an identification method which attempts to alleviate some difficulties, such as multiple and interacting bad data. Two identification techniques were derived and further investigated and assessed by means of a realistic illustrative example. It is believed that these techniques are sufficient to detect and recover from sensor measurement manipulation.

However, Liu et al. [4] demonstrated that an adversary, armed with the knowledge of the network configurations, can accomplish malicious data attack on state estimation that uses DC power flow models without being detected. Since Liu et al. firstly addressed the existence of "undetectable" cyber-attack on power system state estimation which has attracted a lot of research efforts in recent years. Some new methods have been proposed to solve the above problem which cannot be detected by traditional bad data detection. Kosut and his colleagues [5] divided malicious attacks into two regimes: the strong attack regime and the weak attack regime. They studied the parameter which is the size of the smallest unobservable malicious data attack. They also studied the generalized likelihood ratio test as a detector and provided residue energy heuristic to find particularly damaging attacks in this regime. Xie et al. [6] presented a potential class of cyber-attack against the state estimation in deregulated electricity markets and showed that such attacks will lead to profitable financial misconduct. Pasqualetti [7] proposed an attack model which generalizes the prototypical stealth, false-data injection and replay attacks. To solve the problem, they designed provably-correct detection and identification procedures based on tools from geometric control theory. The studies above have successfully proved the existence of "undetectable" attacks and the limitations of state estimation in smart grids.

In this paper, we present several bad data injection cases in IEEE 14-bus system, which cannot be detected by the traditional state estimation. The potential risks, such as energy theft and cracking economic dispatch, are analyzed to calculate the possible harms. The distributed state estimation (DSE) method proposed in this paper is applied to detect bad data. With the proposed method, the power system is divided

*Corresponding author
This work was supported by the National Natural Science Foundation (91118005, 91218301, 61221063, 61203174), Doctoral Fund of Ministry of Education of China (20110201120010), the Fundamental Research Funds for the Central Universities and the Cisco University Research Program Fund, a corporate advised fund of Silicon Valley Community Foundation.

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

into several subsystems according to the physical topology or using clustering algorithms. Chi-squares test is applied to detect whether there is any bad data respectively in each subsystem. The testing results demonstrate that all bad data can be detected in three attack cases and located in a specific subsystem with the proposed DSE-based bad data detection. In summary, the main contribution of this paper is twofold:

1. Several bad data injection cases are simulated in IEEE 14-bus system. It is the first time to demonstrate such attacks, and calculate the potential risks for smart grids.

2. DSE is firstly applied in cyber-attack detection. The experiments prove that DSE-based bad data detection present higher detection accuracy and much lower computation cost than them with the traditional methods.

The rest of this paper is organized as follows. The background of state estimation and bad data detection are introduced in Section II. In Section III, a cyber-attack scenario is illustrated to show the potential motivations and risks. The methodology of cyber-attack detection based on distributed state estimation is introduced in Section IV. In Section V, the proposed method is tested with IEEE 14-bus system. The results and analysis are also shown in this section. The concluding remarks then follow.

II. PRELIMINARIES

The notations are listed in TABLE I.

TABLE I. NOTATIONS IN THIS PAPER

Notation	Definition
p^{sub}	The number of subsystems after decomposition
$subsys\_k$	The label of subsystem after decomposition ($1 \le k \le p^{sub}$)
N	The number of buses in a power system
M	The number of transmission lines in a power system
M^{TIE}	The number of tie lines
N^k	The number of buses in $subsys\_k$
M^p	The number of transmission lines in $subsys\_k$
bus_i	Load Bus/Generators in power system, labeled according to the definition in IEEE standard case ($1 \le i \le N$)
$L_{i,j}$	The transmission line connecting bus_i and bus_j
$P_{i,j}$	The real line power flow from bus_i to bus_j, observed on bus_i
$\mathbf{x}$	State variables in power system, $\mathbf{x} = [x_1, x_2, ..., x_n]^T$
$\mathbf{z}$	Measurements in power system, $\mathbf{z} = [z_1, z_2, ..., z_m]^T$
$\mathbf{e}$	Measurements noise $\mathbf{e} = [e_1, e_2, ..., e_m]^T$
$\mathbf{R}$	The diagonal measurement covariance matrix
$h(x)$	The nonlinear function relating measurements z to state variables x
o	The degree of freedom in power system
$T_{o,p}$	The threshold of o degree of freedom corresponding to a detection confidence with probability p.
$\mathbf{x}^k$	States variables in $subsys\_k$, $\mathbf{x}^k = [x_1^k, x_2^k, ..., x_n^k]^T$
$\mathbf{z}^k$	Measurements in $subsys\_k$, $\mathbf{z}^k = [z_1^k, z_2^k, ..., z_m^k]^T$
$h^k(x^k)$	The nonlinear function relating measurements z_k to states variables x_k in $subsys\_k$
o^k	The degree of freedom in $subsys\_k$
$\mathbf{a}^k$	The false data injection attack (if exists) in $subsys\_k$

A. WLS State Estimation

Power system state estimation is widely used to ensure the safety and economy of operation of power system. The state variables are related to the measurements as shown in (1)

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

where $\mathbf{x}$ is the state variables and $\mathbf{z}$ is the meter measurements. $\mathbf{h}(\mathbf{x}) = [h_1(x_1, x_2, ..., x_n), ..., h_m(x_1, x_2, ..., x_n)]^T$ where $h_1(x_1, x_2, ..., x_n)$ is a function of $x_1, x_2, ..., x_n$. $\mathbf{e} = [e_1, e_2, ..., e_m]^T$ is the measurement noise which is assumed to follow Gaussian distribution of zero mean. This assumption is generally accepted in power system state estimation formulation [8].

Essentially, power system state estimation is a process which uses real-time redundant measurements to improve data accuracy and automatically excluded from the error message caused by random interference. The objective is to find an estimate $\hat{\mathbf{x}}$ of $\mathbf{x}$ that is the best fit of the measurement $\mathbf{z}$ according to (1). The problem is usually solved by the WLS Algorithm [8]. The state estimation can be formulated as a quadratic optimization problem:

$$J(\mathbf{x}) = [\mathbf{z} - \mathbf{h}(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \tag{2}$$

where $\mathbf{R}^{-1}$ is the measurement inverse covariance matrix. Newtown's method can be applied to solve the quadratic optimization problem.

B. Bad Data Detection

There are several common methods for bad data detection, such as Chi-squares test and normalized residuals method [8]. The most common method, Chi-squares test, is used for detecting bad data in this paper. It is assumed that all the state variables are mutually independent and the meter errors follow the normal distribution. It can be shown that $\sum_{i=1}^{m} \frac{(z_i - h_i(\hat{\mathbf{x}}))^2}{\sigma_i^2}$ follows a $\chi^2_{(m-n)}$ distribution, where m-n is the degree of freedom.

The steps of the Chi-squares test are given as follows:

1) Solve the WLS estimation problem and compute the objective function:

$$J(\hat{\mathbf{x}}) = \sum_{i=1}^{m} \frac{(z_i - h_i(\hat{\mathbf{x}}))^2}{\sigma_i^2} \tag{3}$$

2) Look up the value from the Chi-squares distribution table corresponding to a detection confidence with probability *p (e.g. 95%)* and *(m-n)* degrees of freedom. Let this value be $\chi^2_{(m-n),p}$. Here, $p = \Pr(J(\hat{\mathbf{x}}) \le \chi^2_{(m-n),p})$. The threshold in this paper is a value which corresponds to a detection confidence with 95% and *(m-n)* degrees of freedom.

3)Test $J(\hat{\mathbf{x}}) \ge \chi^2_{(m-n),p}$. If yes, then bad data will be suspected. Else, the measurements will be assumed to be free of bad data.

III. ATTACK CASE

An attack case on IEEE 14-bus system is shown in Fig.1 to explain how the injected bad data avoid detection and the potential risks of the attack. The original load on bus_5 and bus_7 are 7.60MW and 47.80MW, repectively. The power flow on the transmission line $L_{5,4}$ is 61.15MW. In the attack case, the hackers try to move 60.96MW of power load from bus_5 to bus_4. Thus, the load on bus_5 and bus_7 and the power flow on the transmission line $L_{5,4}$ are modified to -53.56 MW, 108.96MW and 122.32MW respectively to keep the power balance of these buses. The revised data is analyzed with the state estimation and $J(\hat{x})$ is equal to 67.5471 by solving (3), which is less than the threshold 72.1532. So traditional bad data detection fails to detect this attack and the measurements will be assumed to be free of bad data.

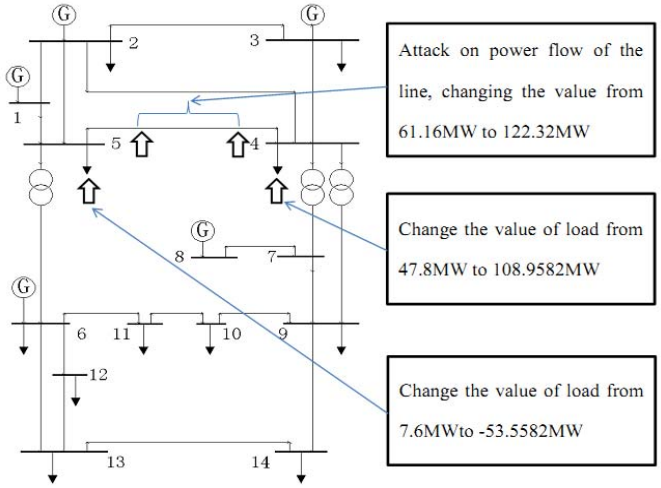

Fig. 1. IEEE 14-bus system

And then the potential risks of the attack will be presented as follows.

Risk1: Energy Theft

Energy theft may be the most common and attractive motivations for hackers to design the bad data injection. In common senses, it is ridiculous to change the load from a positive value to a negative value. However, in the paradigm of smart grids, it becomes a normal thing. Demand response plays an indispensable role in the smart grid. For some energy-intensive industries, such as iron & steel enterprise and cement enterprise, they always have their captive power plants and energy storage devices [9]. When the energy is enough for production, they can participate in the demand side bidding and demand response for their economic benefits. So these energy-intensive enterprises may falsify the value of the smart meter to mislead the power company to believe that the electrical energy is fed into the grid from these enterprises. The enterprises thus can obtain the economic benefits of the aforementioned electrical energy. According to the current tariff published by PG&E, the electricity price is 0.18590$/kW•h. If this attack lasts for one hour, it may bring the customer on bus 5 unjust enrichment about 11369.644$.

Risk2: Cracking Economic Dispatch

Economic dispatch is the short-term determination about the optimal output of a number of electricity generation facilities, which is to minimize the overall operating cost while satisfying the power load of system according to a robust and reliable manner. To achieve the goal of economic dispatch, the Optimal Power Flow (OPF) is applied to solve the load flow and determine a new set of values for generator's output that reduces the generation cost [10]. We calculate the total generation cost of this region with MATPOWER, a toolbox which is developed by the Cornell University [11]. In the normal situation, the optimal generation cost is 8081.5 $/h. If the attack illustrated in figure 1 is launched, the loads of bus_4 and bus_5 and the power flow on the line will change. The control center will be misled to generate a new strategy for all generators [12]. The new optimal generation cost considered the attack is 8128.96 $/h, increasing with 47.46 $/h, about 0.59% of the cost without the attack.

Moreover, there are other serious harms caused by bad data injection. With the bad data injection, the economic dispatch program cannot get feasible solution, and the erroneous actions may be taken by the control center such as cutting off transmission line to avoid the overload and blackout.

IV. DSE-BASED BAD DATA DETECTION

As shown in (3), the threshold of measurements is set to tolerate the unpredictable and inevitable errors in state estimation and bad data detection. The attackers can elaborately construct an attack vector hidden in the normal observation errors. When the number of measurements grows, the threshold has to rise to tolerate the higher accumulated error. Thus, it is difficult to detect the injected data in a large system. If the redundancy of measurements can be reasonably reduced, the threshold will be dropped and the detection will be more sensitive. In DSE-based bad data detection, the DSE is applied to divide the complex and large system into several subsystems and Chi-squares test is used to detect bad data in each subsystem. Since the threshold of each subsystem is expected to be lower than that of the entire system, it is more sensitive to detect the bad data in each subsystem. The main procedure of DSE-based method consists of following steps:

1) Divide the power system into several subsystems;
2) State Estimation in each subsystem;
3) Bad Data Detection in each subsystem.

A. Power System Decomposition

The decomposition of power system is shown in Fig.2. The power system is divided into a specific number p_{sub} of non-overlapping subsystems connected with each other by tie lines. There is a slack bus in each subsystem for state estimation. Lines in original power system are divided into 2 categories:

1) Internal Lines ($L_{i,j}^{INT}$): the lines connect the buses in the same subsystem. Their power flow will be used for state estimation in the corresponding subsystem.

2) Tie Lines ($L_{i,j}^{TIE}$): the lines which connect the buses in different subsystems. The power flow of the tie lines will be added to the load of their node bus.

Through decomposition, the power system is divided into p_{sub} subsystems connected by M^{TIE} tie lines. In the subsystem k described by *subsys_k (k = 1... p_{sub})*, there are N_k buses and M_k lines, let n_k denote the number of state variables and m_k denote the number of measurements, they should satisfy the following equations:

$$N = \sum_{k=1}^{p_{sub}} N_k, \quad M = \sum_{k=1}^{p_{sub}} M_k + M^{TIE}, \quad n_k = 2N_k - 1 \tag{4}$$

Noted that there must be ensured a sufficient redundancy of measurements in each subsystem to carry out the state estimation, i.e. $m_k > n_k$. The method of decomposition will be adjusted in accordance with different situations:

- Self-feature: when the bus and lines represent specific features, such as geographic location and system structure, it is recommended to divide the power system according to its physical information.
- Clustering algorithms: in general, a power system can be divided into a number of subsystems by using some clustering algorithms, e.g. K-Means.

B. Subsystem State Estimation

Each subsystem is assigned with its own estimator. The state estimator of each subsystem can be run in parallel and separately with the respect of their own slack bus respectively. The state estimation of *subsys_k* can be formulated as follows:

$$\mathbf{z}^k = \mathbf{h}^k(\mathbf{x}^k) + \mathbf{e}^k + \mathbf{a}^k \tag{5}$$

where $\mathbf{z}^k$ is the measurement vector which describes the line power flow in each subsystem; $\mathbf{x}^k$ denotes state variables in *subsys_k*; $\mathbf{h}^k(\mathbf{x}^k)$ is a non-linear vector function indicating the relationship between the measurements and the state variables in the subsystems k; $\mathbf{e}^k$ is the random Gaussian error; and $\mathbf{a}^k$ is a sparse vector of which the non-zero elements are injected attacking values on specific measurements.

C. Subsysten Bad Data Detection

The bad data detection is carried out in each subsystem by traditional Chi-squares test. Referring to (3), the local threshold $T_{o,p}^k$ of bad data in *subsys_k* is determined by the local degree of freedom o_k for χ^2 distribution of the objective function $J(\hat{x})$ and $o_k = m_k - n_k$.. Since the local degree of freedom o_k is obviously lower than the global one, the threshold of bad data could be less than it in entire system. Therefore, it is easy to detect the bad data from the errors.

V. Experiment And Analysis

In this section, IEEE 14-bus system is selected to simulate the bad data injection attacks. The comparison of detection result between the proposed method and the traditional Chi-squares test is also shown.

The decomposition of IEEE 14-bus system is carried out by clustering algorithm, since the system is not large-scaled and does not have special geographical constraints. The topological location of IEEE 14-bus system after decomposition is shown in Fig.2 and the detailed data of each subsystems is listed in TABLE II.

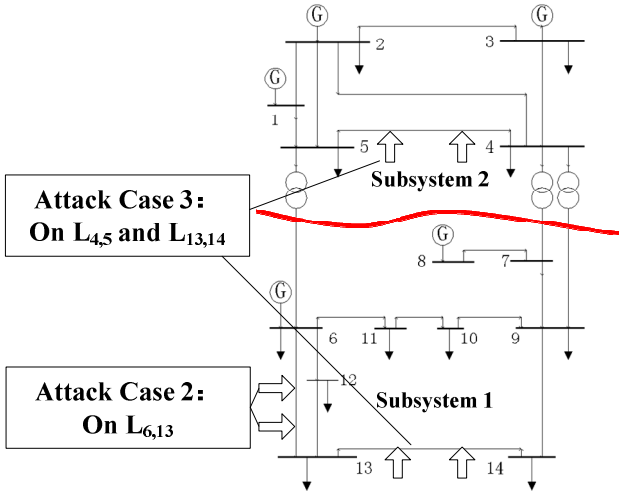

Fig. 2. Decomposition of IEEE 14-bus system

TABLE II. Decomposition of the IEEE 14-Bus System.

	bus	n_states	n_measurements	D.F.	threshold
subsys_1	1,2,3,4,5	9	28	19	31.41
subsys_2	6,7,8,9,10, 11,12,13,14	17	40	23	35.17
Global	All	27	80	53	72.15

As shown in Table II, the IEEE14-bus system is divided into two subsystems, "*subsys_1*" and "*subsys_2*". In *subsys_1*, there are 5 buses labeled from No.1 to No.5. The number of state variables is 9 and the number of measurements is 28. "D.F." represents the degree of freedom in the subsystem .*D.F. = m - n*. According to the property of χ^2 distribution in (3), the threshold of bad data suspicion is 31.41 in *subsys_1*. In *subsys_2*, there are 9 buses, 17 state variables, and 40 measurements, and the threshold is 35.17. To test the performance of DSE-based bad data detection, three attack cases are constructed as shown in Table III. $L_{i,j}$ denotes the transmission line where the modified measurements located. $P_{i,j}$ denotes the real line power flow from bus_i to bus_j, observed on bus_i . The real power flow $P_{i,j}$ and $P_{j,i}$ are modified at the same time to guarantee the balance of line power flow. In *Attack Case 1*, bad data is only injected into *subsys_1*. The $P_{4,5}$ is modified from -

61.16MW to -122.32MW and $P_{5,4}$ is modified from 61.67MW to 122.34MW. In *Attack Case 2*, bad data is only injected into *subsys_2*. The $P_{6,13}$ is modified from 17.75MW to 53.24MW and $P_{13,6}$ is modified from -17.54MW to 52.61MW. In *Attack Case 3*, a pair of bad data is injected both into *subsys_1* and *subsys_2*. The $P_{4,5}$ is modified from -61.16MW to -122.32MW and $P_{5,4}$ is modified from 61.67MW to 122.34MW. The $P_{13,14}$ is modified from 5.65MW to 22.58MW and $P_{14,13}$ is modified from -5.59MW to 22.36MW.

TABLE III. INJECTION ATTACK ON IEEE 14-BUS SYSTEM

	Modified Measurement	$P_{i,j}$ (MW)		$P_{j,i}$ (MW)	
		Original Value	Injected Value	Original Value	Injected Value
Attack Case 1	$L_{4,5}$	-61.16	-122.32	61.67	122.34
Attack Case 2	$L_{6,13}$	17.75	53.24	-17.54	-52.61
Attack Case 3	$L_{4,5}$	-61.16	-122.32	61.67	122.34
	$L_{13,14}$	5.65	22.58	-5.59	-22.36

As shown in TABLE IV, "*T*" denotes the threshold of suspicion of bad data. Global values of $J(\hat{x})$ are 67.5471, 65.0776 and 63.3993 in three attack cases respectively. Obviously, they are lower than the threshold. Thus the injected bad data could not be detected. When we adopt DSE-based method to deal with the *Attack Case* 1, we find that: in *subsys_1*, the $J(\hat{x})$ is 34.67, which is higher than the local threshold (31.41); in *subsys_2*, the $J(\hat{x})$ is 9.2276, which is below the local threshold (36.415). It implies that there is bad data in *subsys_1*. Similarly in *Attack Case 2*, the DSE-based method can detect the bad data in *subsys_2*. In *Attack Case 3*, the values of $J(\hat{x})$ in the two subsystems are lower than their threshold respectively. It is found that the DSE-based bad data detection could be able to detect the multiple bad data.

TABLE IV. DETECTION RESULT OF TRADITIONAL METHOD AND DSE-BASED METHOD

	Global		subsys_1		subsys_2	
value	***T***	$J(\hat{x})$	***T***	$J(\hat{x})$	***T***	$J(\hat{x})$
Attack Case 1	72.15	67.55	31.41	34.67	36.42	9.23
Attack Case 2		65.08		1.90		40.93
Attack Case 3		63.40		33.78		38.04

VI. CONCLUSION

In this paper, three bad data injection attack cases are designed to explain how the hackers modify the data in smart grids and avoid the traditional bad data detection in power system. We discuss the potential risks of Bad Data Injection in smart grids, and evaluate the loss of energy theft and cracking economic dispatch in IEEE 14-bus system.

To solve the problem, the DSE-based method is proposed to detect bad data injection attack. The basic idea of this method is to improve the sensitivity of bad data detection by dividing a complex system into several subsystems. The main procedure of DSE-based method consists of following steps: 1) Divide the power system into a certain number of subsystems according to the system's physical topology or using some clustering algorithms; 2) State Estimation in each subsystem; and 3) Bad Data Detection in each subsystem.

In the experiments, the traditional method cannot detect bad data in three attack cases. However, the DSE-based method can detect all bad data and locate the bad data into the subsystem correctly.

REFERENCES

[1] F. C. Schweppe and J. Wildes, "Power System Static-State Estimation, Part I: Exact Model," *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-89, pp. 120-125, 1970.

[2] N. Xiang, S. Wang and E. Yu, "A New Approach for Detection and Identification of Multiple Bad Data in Power System State Estimation," *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-101, pp. 454-462, 1982.

[3] T. Van Cutsem, M. Ribbens-Pavella and L. Mili, "Hypothesis Testing Identification: A New Method For Bad Data Analysis In Power System State Estimation," *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-103, pp. 3239-3252, 1984.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proc. ACM Conf. Computer Communication Security, 2009, pp. 21–32.

[5] O. Kosut, J. Liyan, R. J. Thomas, and T. Lang, "Malicious Data Attacks on the Smart Grid," *IEEE Transactions on Smart Grid,* vol. 2, pp. 645-658, 2011..

[6] Le Xie, Yilin Mo and Bruno Sinopoli, "False Data Injection Attacks in Electricity Markets," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 226-231.

[7] 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*, 2011, pp. 2195-2201.

[8] Ali Abur, Antonio Gomez Exposito, Power System State Estimation,Theory and Implementation, CRC Press. 2004

[9] Zhaojie Wang, et al., "A gradient information based real time pricing mechanism for microgrid in energy intensive enterprise", in the 10th World Congress on Intelligent Control and Automation, Beijing, 2012.

[10] G.F. Reid and L. Hasdorff, "Economic Dispatch Using Quadratic Programming", *IEEE Transactions on Power Apparatus and Systems*, PAS-92(6): p. 2015-2023,1973

[11] R. D. Zimmerman, C. E. Murillo-S´ anchez, and R. J. Thomas, "MAT-POWER's extensible optimal power flow architecture," in IEEE Power and Energy Society General Meeting, July 2009, pp. 1–7.

[12] H.W. Dommel and W.F. Tinney, "Optimal Power Flow Solutions, " *IEEE Transactions on Power Apparatus and Systems,* 1968. PAS-87(10): p. 1866-1876.