A Novel Method to Detect Bad Data Injection Attack in Smart Grid

Ting Liu, Yun Gu, Dai Wang, Yuhong Gui, Xiaohong Guan
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
{tliu, ygu, daiwang, yhgui, xhguan}@sei.xjtu.edu.cn

Abstract — **Bad data injection is one of most dangerous attacks in smart grid, as it might lead to energy theft on the end users and device breakdown on the power generation. The attackers can construct the bad data evading the bad data detection mechanisms in power system. In this paper, a novel method, named as Adaptive Partitioning State Estimation (APSE), is proposed to detect bad data injection attack. The basic ideas are: 1) the large system is divided into several subsystems to improve the sensitivity of bad data detection; 2) the detection results are applied to guide the subsystem updating and re-partitioning to locate the bad data. Two attack cases are constructed to inject bad data into an IEEE 39-bus system, evading the traditional bad data detection mechanism. The experiments demonstrate that all bad data can be detected and located within a small area using APSE.**

***Index Terms*—smart grid; security; detection; bad data injection; adaptive partitioning state estimation**

I. Introduction

The smart grid (SG) is a highly open network, where numerous sensors are deployed at millions of buildings and streets, connected with information network and applied the uniform public protocols and standards. Various attacks, such as information tampering and system intrusion, would impose great threat on security and stability of SG, which have almost ruined the Internet. Moreover, the data in SG is one of most attractive targets for various attackers. For the hackers, the bad data injection attack in SG can easily be monetized, e.g. the hackers can manipulate the energy costs by modifying the smart meter readings. For the military, the bad data could mislead the control center to take erroneous actions in power system. For example, in 2010, Iran's Bushehr nuclear plant was cracked by Stuxnet worm which tamper the system state to disable the system protection strategies of SCADA (Supervisory Control and Data Acquisition).

State estimation is applied to monitor the running status of the power system and widely used to reduce the impact of observation errors. In state estimation, measurements are usually the values that can be observe easily, such as the line power flow, bus power injections, bus voltage magnitudes, line current flow magnitudes and etc. The state variables are usually complex phasor voltages which cannot be measured conveniently. Both of the measurements and state variables follow the same constraints, such as power balance theory, Kirchhoff's Law, etc. which can be applied to estimate each other. In general, the measurements are more than state variables, since there are more lines than buses and more kinds of measurements than state variables. Thus, the measurements are used to estimate the state variables, detect and eliminate the error caused by random interference.

Most bad data detection methods tests in state estimation are based on Chi-squares test or normalized residuals test. In our paper, Chi-squares test is used for detecting bad data. This method makes use of the correlation between measurements and the great impact of bad data on the weighted sum-squared residual[1]. Assuming that all the state variables are mutually independent and the meter errors follow the normal distribution, it can be shown that weighted sum-squared residual $J(\hat{x})$ follows a $\chi^2_{(m-n)}$ distribution, where *m* is the number of measurements, *n* is the number of state variables, and *m-n* is the degree of freedom. Then we consider the following composite binary hypothesis:

$$\begin{cases} H_0 : J(\hat{x}) \geq \chi^2_{(m-n),p} & \textit{there is bad data} \\ H_1 : J(\hat{x}) \leq \chi^2_{(m-n),p} & \textit{there is not bad data} \end{cases} \tag{1}$$

where $\chi^2_{(m-n),p}$ is the threshold corresponding to a detection confidence with *p*. In this paper, the detection confidence *p* is 95%. The details about the state estimation and Chi-squares test are shown in Appendix.

However, recent works demonstrate that an adversary, armed with the knowledge of the power system configurations, can accomplish bad data injection attack against state estimation without being detected [2]-[5]. Many cases are constructed in our work to prove the existence of bad data injection. These attacks hide the bad data among the normal observation errors. According to (1), when the number of measurements grows, the threshold has to rise to tolerate the higher accumulated error. Thus, it is possible for attackers to inject bad data into a large power system evading the bad data detection.

As shown in Fig.1, an attack case is constructed to inject bad data into IEEE 39-bus system, which demonstrate how the bad data evade the detection. In the standard case, the output of generator on bus 34 is 508MW, the load on bus 20 is 680MW, and the power flow on the transmission line $L_{20,34}$ is 508MW. In the attack case, the hackers try to falsify the generated

This project is supported in parts by a gift fund from the Cisco University Research Program, National Natural Science Foundation of China (91118005, 91218301, 61221063, 61203174), Doctoral Fund of Ministry of Education of China (20110201120010) and the Fundamental Research Funds for the Central Universities.

978-1-4673-1017-8/13/$31.00 ©2013 IEEE

output with an increase of 152.4MW. To keep the power balance, the power load on bus 20 and the power flow on the transmission line $L_{20,34}$ are modified to 832.4 MW, and 660.4MW respectively. The $J(\hat{x})$ of revised measurements is 120.77, which is less than the threshold $\chi^2_{(184-77),95\%} = 133.26$. Thus, the injected data could not be detected by Chi-squares test, and misguide the control center making wrong control decisions. According to the current tariff published by PG&E, the electricity price is 0.18590$/kW•h. If this attack lasts for one week, it may bring the generation company on bus 34 unjust enrichment for more than 4.7 million dollars. Moreover, the bad data injection may cause that 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.

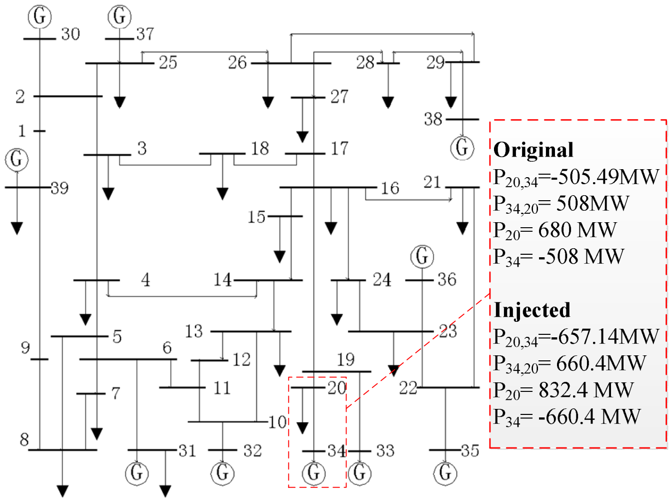

Fig.1 Attack case in IEEE 39-bus system

In this paper, an adaptive partitioning state estimation (APSE) is proposed to detect bad data injection attacks and locate the attacks within a small area. In this method, the power system is transformed to a weighted undirected graph. Clustering algorithms are applied to partition the large graph into several subgraphs that correspond to subsystems in power system. Chi-squares test is used to detect bad data in each subsystem. Since the threshold of subsystem is expected to be lower than that of the entire system, it is more sensitive to detect the bad data in each subsystem. If the bad data is detected, the result will work as a feedback and guide the graph update. Then the suspicious subgraphs will be updated and partitioned into several smaller subgraphs. Through multiple graph-updating and partitioning, the bad data will be located within a small area. In the experiments, two bad data injection cases are constructed in IEEE 39-bus system, which cannot be detected using the Chi-squares test. The testing results demonstrate that all bad data can be detected and located within a small area using the APSE.

The rest of this paper is organized as follows. The related work is introduced in Section II. We present the methodology and experiments of APSE in Section III and IV. Section V is the conclusions and future work.

II. Related Work

After Schweppe [6] firstly introduced the concept of power system state estimation in 1969, bad data detection caught many researchers attention. Xiang et al [7] 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 [8] presented an identification method which attempts to alleviate some difficulties, such as multiple and interacting bad data. Two identification techniques were further investigated and derived by many scholars. It was believed that these techniques are sufficient to detect and recover from falsified measurements.

Liu et al. [2] firstly demonstrated the existence of “undetectable” cyber-attack on power system state estimation in the SG paradigm. Then, bad data injection attracted a lot of research efforts. Hug and Giampapa [3] assessed the vulnerability of AC state estimation with respect to false data injection cyber-attacks. Kosut and his colleagues [4] 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. Xie et al. [5] 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. These studies have successfully proved the existence of “undetectable” attacks and the limitations of state estimation in SG.

Some new methods have been proposed to solve such kind of attacks which cannot be detected by traditional bad data detection. Bobba et al. [9] explored the detection of false data injection attacks proposed by Liu et.al [2] through protecting a strategically selected set of sensor measurements and by having a way to independently verify or measure the values of a strategically selected set of state variables. They showed that it is necessary and sufficient to protect a set of basic measurements to detect such attacks. Pasqualetti et al. [10] designed provably-correct detection and identification procedures based on tools from geometric control theory to detect false-data injection. Nevertheless, no specific testing case with AC power flow model is presented in these papers.

III. Methodology

In this section, the framework of APSE is introduced, as shown in Fig 2. Firstly, the graph of the SG is established according to the structure of power system. Then, the graph will be partitioned into several subgraphs and each subgraph corresponds to a subsystem. Afterwards, the bad data detection is performed on each subsystem. If bad data exists, the iteration of Graph Update, Graph Partition and Bad Data Detection will be repeated until the bad data is located within a small region.

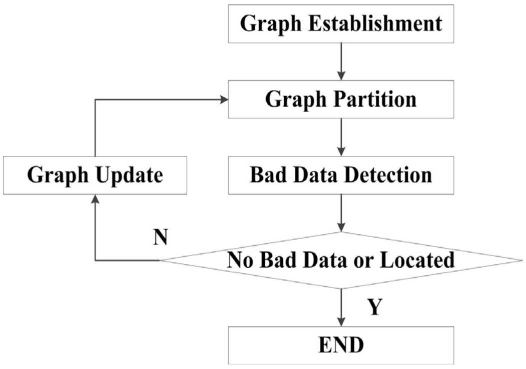

Fig.2 Framework of APSE

a) Graph Establishment

Assuming a SG with *n* buses connected by *m* transmission lines, a graph of power system can be established as follows

$$G = \{V, A\} \tag{2}$$

where V is a set of vertices representing load buses or generators, and A is the graph adjacency matrix $A=\{a_{i,j}\},i,j=1,2,...n.$ The weighted-edge $a_{i,j}$ is nonzero when bus i and bus j is directly connected and it also indicates the physical properties between the two buses. Given a specified power system, many methods are available to determine the weight of edges including:

- The basic topology of the power system ($a_{i,j}$ =1 if bus *i* and bus *j* are connected);
- The impedance of transmission lines;
- The line power flow at each sampling time.

In present paper, the impedance of transmission lines is adopted for the weight of edges. Let $Z = R + jX$ denote the impedance of transmission line, where R represents the resistance and X represents the reactance. In power transmission system, the value of reactance part has more obvious effect on electricity transmission. So we take $|X|$ as the weight of edge in this paper.

Consider an acyclic path $P = \{V_{i,1}, V_{i,2}, ..., V_{i,p}\}$ in the graph. The path length is not the sum of edges' weight but the value of mutual impedance [11] between $V_{i,1}$ and $V_{i,p}$ because of the special characteristic in power system.

b) Graph Partition

As shown in Section I, attackers can elaborately construct a bad data injection hidden in normal observation errors. When the power system is divided into several subsystems, the redundancy of measurements can be reasonably reduced. The threshold of bad data is expected to be lower than the global one. As a result, the sensitivity of Chi-squares detection in each subsystem will rise.

Many methods have been proposed to partition the power system. In traditional distributed state estimation, the power system will be divided into several subsystems according to its physical features, such as geographic location and system structures. In our work, the clustering algorithms are applied to partition the graph of power system, such as K-Medoid, K-Means and Chameleon, etc. The former methods are easy to understand while our methods are convenient to be developed as a software and partition the complex power systems.

In this paper, L-bounded Graph Partition Method (LGPM), an efficient algorithm [12], is adopted for graph partitioning. The result of this method is relatively stable while the K-Medoid algorithm is affected by the choice of initial clustering centers. The main process of LGPM is illustrated as follows:

Algorithm 1: LGPM

```
Data: The adjacency matrix $A = \{a_{i,j}\}$ for graph $G$ ;The number of subgraphs. $N$
Result: Subgraphs $G_i$ ( $\iota = 1,2,...,$N)
    1.Initialization;
    2.Normalize a nonnegative symmetric matrix $A'$ from $A$ and make it doubly stochastic;
    3.Spectural Partition: Calcuate the $N$ largest eigenvectors $U_i$ ( $\iota = 1,2,...,$N) ;
    4.A general clustering algorithm (k-means or EM) using $\{U_i\}$ and $N$ as input s is adopted to get the arrtibution of each vertexs;
    5.Generate the adjacency matrix for each subgraphs
```

c) Bad Data Detection

After the graph partitioning, the power system graph is divided into several subgraphs. The global power system is divided into subsystems in accordance with the graph partionting.

State Estimation and Bad Data Detection will be carried out in each subsystems. 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 *Subsystem_k* can be formulated as follows:

$$z^k = h^k(x^k) + e^k + a^k \tag{3}$$

where z^k is the measurement vector which describes the line power flow in each subsystem and $z^k = [z_1^k, z_2^k, ..., z_{m_k}^k]^T$; x^k denotes state variables in the subsystem k and $x^k = [x_1^k, x_2^k, ..., x_{n_k}^k]^T$.

In this paper, the Chi-squares test is selected to detect the bad data in each subsystem. The threshold of bad data could be less than it in entire system. Therefore, it is easier to detect the bad data from the errors.

If no bad data are detected in all subsystems, the APSE comes to the termination. Otherwise, an iteration of Graph Update, Graph Partition and Bad Data Detection will be repeated until the suspected range of bad data injection is limited into a small-scaled subsystem.

d) Graph Update

The stage of Graph Update is to make some adjustment to the original graph according to the result of last-round bad data detection. If the bad data is detected in a specific subsystem , the graph will be updated to generate a new scheme of graph partition which guides the bad data identification. Subsystem-

Extension and Tie-Line-Fusion are two strategies for Graph Update.

Subsystem-Extension(SSE): The main idea of SSE strategy is to divide the subsystem with bad data injection into several smaller-scaled systems so that the suspected range of bad data can be limited. Noted that the state estimation in subsystem should be ensured with sufficient redundancy of measurements. For a subsystem with bad data, the buses which are connected to the original subsystems will be included to the new subsystem. In the process of Graph Partition, the new subsystem will be divided with the clustering algorithm.

Tie-Line-Fusion (TLF): The main idea of TLF strategy is to use the intersection of detection result from different partitioning schemes. For the result of last Graph Partition, make the fusion of the vertices/buses which are connected with the same edge but partitioned into different subsystems. In the process of Graph Partition, the updated graph will be adopted to generate a new scheme of partition and run state estitmaiton and then bad data detection will be performed. If bad data is detected, get the intersection of subsystems with bad data from different partitioning scheme. With multiple round of iteration with TLF, Graph Partition and Bad Data Detection, the suspected range of bad data can be narrowed down.

In this paper ,the SSE strategy is adopted in Graph Update. It is more efficient and easier for implementation.

IV. Experiments and Analysis

In this section, two attack cases on IEEE 39-bus system are constructed, as shown in TABLE I. The traditional bad data detection and APSE are applied to detect the false data.

A. Attack Case Constructing

As shown in Table I, the power flow on the transmission lines between bus 20 and 34 ($L_{20,34}$) are revised in Attack Case I. The power flow from bus 20 to bus 34, observed on bus 20 ($P_{20,34}$) is modified from -505.49MW to -657.14MW; the $P_{34,20}$ is modified from 508MW to 660.4MW. (Generally, the $P_{i,j}$ is not equal to $P_{j,i}$, because of the line losses.) The Chi-square test is applied to detect the bad date from all measurements. In our work, Chi-squares test is solved by MATPOWER [13]. The weighted sum-squared residual $J(\hat{x})$ is 120.77, which is lower than the threshold of IEEE 39-bus system $\chi^2_{(m-n),p} = \chi^2_{(168-77),0.95} = 133.26$. Thus the bad data in Attack Case I could not be detected using the traditional state estimation and bad data detection method.

In Attack Case II, the power flow on $L_{2,25}$ ($P_{2,25}$ and $P_{25,2}$) are modified; and the $J(\hat{x})$ is also lower than the threshold.

TABLE I. Attacks and the Result of the Traditional Method

	Bus		Power Flow (MW)		Global	
	From	To	Original	Injected	*Threshold*	$J(\hat{x})$
Attack Case I	20	34	-505.49	-657.14	133.26	120.77
	34	20	508.00	660.40		
Attack Case II	2	25	-244.59	-317.97		132.44
	25	2	248.93	323.61		

B. APSE vs. Attack Case I

The APSE is applied to detect the bad data from Attack Case I. The processes of detection are described as following:

1) The graph of IEEE 39-bus system is generated firstly. And then it could be divided into three subsystems using the L-bounded Graph Partition Algorithm, as shown in Fig.3.

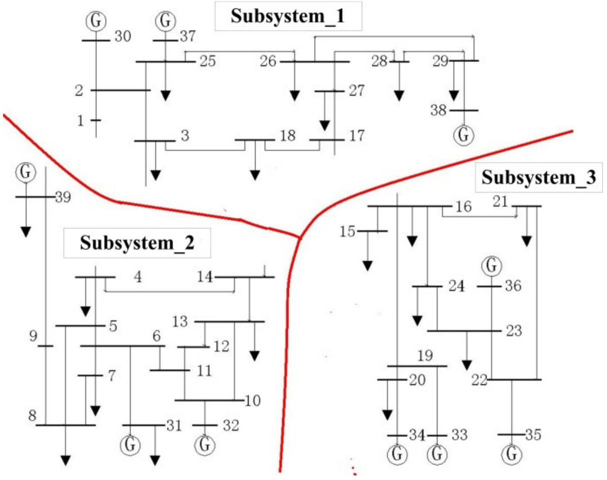

Fig.3 Partition of IEEE 39-bus System

2) The Chi-squares test is applied to analyze the measurements of each subsystem. As shown in TABLE II, the local $J(\hat{x})$ is higher than the local threshold in Subsystem_3. It conducts that there are bad data in Subsystem_3

TABLE II. Bad Data Detection Result (First Round, Case I)

	Number of Measurements (m)	Number of State Variables (n)	Threshold	$J(\hat{x})$
Subsystem_1	56	25	46.19	16.41
Subsystem_2	64	27	53.38	21.61
Subsystem_3	**48**	**23**	**38.89**	**63.06**

3) The subgraph of Subsystem_3 is updated with SSE strategy. Bus 14 and 17 are added into updated subsystem_3, which are directly connected to Subsystem_3. In the second round partitioning, the updated Subsystem_3 is divided into Subsystem_3_1 and Subsystem_3_2, as shown in Fig.4.

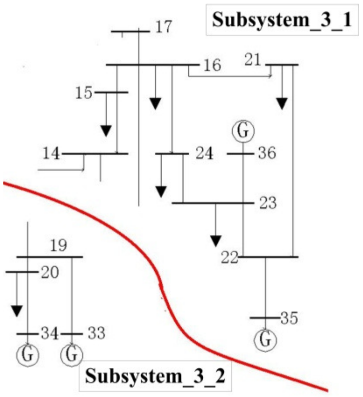

Fig.4 Partition of Subsystem3

4) The bad data detection is taken for the second time. As shown in TABLE III, it is found that the local $J(\hat{x})$ is higher than the local threshold in Subsystem_3_2.

TABLE III. BAD DATA DETECTION RESULT (SECOND ROUND, CASE I)

	Number of Measurements (m)	Number of State Variables (n)	Threshold	$J(\hat{x})$
Subsystem_3_1	40	19	33.92	23.24
Subsystem_3_2	**12**	**7**	**12.59**	**48.68**

Consequently, we can identify that the malicious injected data is in the Subsystem_3_2 which contains only 3 transmission lines ($L_{19,20}$, $L_{20,34}$ and $L_{19,33}$). The bad data in attack case I is detected and located successfully.

C. APSE vs. Attack Case II

Similarly to Case I, the IEEE 39-bus is initially divided into three subsystems after the first round partitioning as shown in Fig.3. Then the Chi-squares test is performed on each subsystems and the result is shown in TABLE IV.

TABLE IV. BAD DATA DETECTION RESULT (FIRST ROUND, CASE II)

	Number of Measurements (m)	Number of State Variables (n)	Threshold	$J(\hat{x})$
Subsystem_1	**56**	**25**	**46.19**	**85.82**
Subsystem_2	64	27	53.38	33.71
Subsystem_3	48	23	38.89	16.18

It is found that the local $J(\hat{x})$ is higher than the local threshold in Subsystem_1. Bus 39, Bus 4 and Bus 16 are added into updated Subsystem_1. In the second round partitioning, the updated subsystem_1 is divided into 2 subsystems, as shown in Fig.5.

The Chi-square test is applied to calculate the $J(\hat{x})$ of each subsystem. As shown in TABLE V, none exceeds the local threshold of subsystems. It infers that the bad data are on the tie-lines which are the lines between the subsystems and cut off in the second round partitioning. Thus, two lines: $L_{2,25}$ and $L_{17,18}$, are classified as suspicious. Obviously, the bad data injected into $L_{2,25}$ is detected successfully.

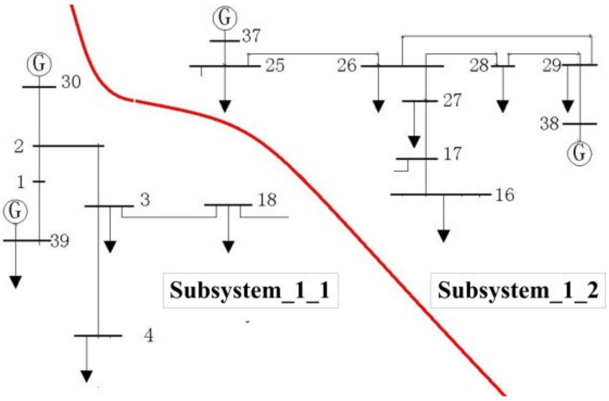

Fig.5 Partition of Subsystem1

TABLE V. BAD DATA DETECTION RESULT (SECOND ROUND, CASE II)

	Number of Measurements (m)	Number of State Variables (n)	Threshold	$J(\hat{x})$
Subsystem_1_1	24	13	31.41	20.33
Subsystem_1_2	36	17	21.03	6.79

V. CONCLLUSIONS AND FUTURE WORK

The APSE is proposed to detect the bad data injection attack in SG. The basic idea of this method is to improve the sensitivity of bad data detection by dividing a complex system into several subsystems, and the testing result works as a feedback to guide the subsystem update and repartition to locate the bad data within a small area. The main procedure of APSE consists of following steps: 1) The power system is transformed into a weighted undirected graph; 2) The graph is partitioned into a certain number of subgraphs exploiting the L-bounded Graph Partition Method; 3) the Chi-squares method is applied to detect the bad data in each subsystem; and 4) Subsystem-Extension is proposed to update the graph to narrow the suspicious region of bad data.

In the experiments, two bad data injection attack cases are constructed on IEEE 39-bus system to explain how the hackers inject bad data and evade the traditional bad data detection. These attacks make use of the tolerance of chi-squares testing threshold and hide in the normal observation errors. However, the APSE method can detect all bad data and locate the bad data within a small area.

In the future work, the algorithms of graph updating and partitioning will be further investigate. And current APSE could detect the bad data on one transmission line. The method to detect multiple bad data will be studied. Moreover, we will develop our method to locate the bad data within an accurate position with low computation cost.

VI. APPENDIX

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 (4)

$$z = h(\mathrm{x}) + e \tag{4}$$

where $x=[x_1,x_2,\ldots,x_n]^T$ is the state variables and $z=[z_1,z_2,\ldots,z_m]^T$ is the meter measurements. $h(x)=[h_1(x_1, x_2,\ldots, x_n),\ldots, h_m(x_1, x_2,\ldots, x_n)]^T$ where $h_i(x_1, x_2,\ldots, x_n)$ is a function of $x_1, x_2,\ldots, x_n$. $e=[e_1,e_2,\ldots,e_m]^T$ is the measurement noise which is assumed to follow Gaussian distribution of zero mean, i.e. $e \sim N(0,R)$ where $R=Eee^T$ is the diagonal measurement covariance matrix.

In the power system, the state variables are usually complex phasor voltages at every bus. When using the polar coordinates for a system containing N buses, the state vector will have ($2N$-1) elements, N bus voltage magnitudes and (N-1) phase angles. Measurements can be the line power flow, bus power injections, bus voltage magnitudes, and line current flow magnitudes. So, there are usually more measurements than state variables (*m*>*n*). 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 $\hat{x}$ of x that is the best fit of the measurement *z* according to (4). The problem is usually solved by the WLS Algorithm [1]. The state estimation can be formulated as a quadratic optimization problem:

$$J(x) = [z - h(x)]^T R^{-1} [z - h(x)] \tag{5}$$

Newtown's method is applied to solve the quadratic optimization problem. The increment can be calculated by

$$\Delta x^{(k)} = G(x^{(k)})^{-1} H^T(x^{(k)}) \cdot R^{-1} \cdot [z - h(x^{(k)})] \tag{6}$$

where $H(x^{(k)}) = \left.\frac{\partial h(x)}{\partial(x)}\right|_{x=x^{(k)}}$ is the Jacobi matrix and $G(x^{(k)})$ = $H^T(x^{(k)})\ R^{-1}\ H(x^{(k)})$ is the gain matrix. The convergence criterion of IPM is the following:

$$\max(\left|\Delta x^k\right|) < \varepsilon_x \tag{7}$$

where ε_x is a predefined threshold.

B. Bad Data Detection

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

$$J(\hat{x}) = \sum_{i=1}^{m} \frac{(z_i - h_i(\hat{x}))^2}{\sigma_i^2} \tag{8}$$

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, $p = \Pr(J(\hat{x}) \le \chi^2_{(m-n),p})$. The threshold in this paper is a value which corresponds to a detection confidence with 95% and *(m-n)* degrees of freedom.

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

REFERENCES

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

[2] 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*, pp. 21–32, 2009.

[3] 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.

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

[5] Le Xie, M. Yilin and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 226-231, 2010.

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

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

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

[9] Rakesh B. Bobba, et al., detecting false data injection attacks on dc state estimation. *CPSWEEK2010*, Stockholm Switzerland, April 12th, 2010.

[10] F. Pasqualetti, F. Dorfler and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pp. 2195-2201, 2011.

[11] J. D. Glover, M. S. Sarma, T. J. Overbye, *Power System Analysis &Design,* Cengage Learning, 2010

[12] J. P. Haspenha, An Efficient MATLAB Algorithm For Graph Partitioning, Citeseer, 2004

[13] R. D. Zimmerman, et al., "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education, " *Power Systems, IEEE Transactions on*, vol.26, pp. 12-19, 2011.