Electrical Power and Energy Systems 57 (2014) 156–163

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

State summation for detecting false data attack on smart grid

Yuancheng Li, Yiliang Wang *

School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, PR China

ARTICLE INFO

Article history:
Received 30 August 2012
Received in revised form 24 November 2013
Accepted 26 November 2013

Keywords:
Smart grid
Power system state estimation
False data attack
Cyber security

ABSTRACT

The SE (state estimation) is an essential part of future smart grid for estimating its running state based on meter measurements. While it has been presented that the attacker can conduct a type of FDA (false data attack) which bypasses bad data detectors recently. In the paper general analysis about protection strategy and how to find a sparse attack, secure meters are discussed. Then by considering the impact of injection data, two detectors are proposed to detect the attack using state variables' distributions. In addition, we formalize the problem as a hypothetical test of standard normal distribution with empirical data. Finally, we demonstrate the effectiveness of our detectors comparing with classical detectors.

1. Introduction

The future Smart Grid will be an upgrade to current power grid that runs on more complex environment and makes intelligent decision to maintain a stable system. While the electric power system transmits electricity from local electric power generator to remote customs through power transmission and distribution network, it will be essential for Smart Grid to be composed of networks to communicate and manage users and suppliers. However, it will introduce some cyber security risks into the system [1,2]. To maintain a stable system, the control center has to monitor and identity the accurate running state of power system. SE (State Estimation) is widely used by the energy management system (EMS) to process the real-time data collected via Supervisory Control And Data Acquisition (SCADA) system and analyze the current power system state. For most SE, they make use of sets of redundant data and measurement residue to deal with gross errors, such as measurement errors and telemetry failures that affect the accuracy of SE [3–7]. However, these approaches may not efficiently detect the multiple interacting measurement errors.

It seems not likely that random interacting measurements noise could evade detection [8,9], while it has been proven that a new class of attacks could be constructed under several mild conditions, bypass the security guard and bring arbitrary errors into system state variables [10]. With the development of Smart Gird, an attacker could corrupt some smart measurement devices and access the power system configuration information through network to launch an successful malicious bad data attack in a way Liu et al. [10] presents, causing power grid to be perturbed arbitrarily. For this serious vulnerability, much work has been put into studying malicious FDAs and protecting power grid against these attacks [11–17]. Bobba et al. [11] proposed a strategy of selecting a set of measurements and verified state variables against the attack. Similarly, Sandberg et al. [13] introduced two security indices quantifying the least effort for the attack to achieve its goals without triggering bad-data alarm. Kosut et al. [12] limited FDAs by capturing the prior information of the likely state of the power system with introducing a Bayesian formulation of the bad data problem. For the large size of power system, Kim and Poor [14] proposes a fast greedy algorithm to address the complexity issue of selecting a subset of measurements. Even though some false attacks cannot be successfully injected, they still can bring errors into the system. As well as computing the smallest set of measurements capable of causing network unobservability, Kosut et al. [15] proposes a weak regime to detect unsuccessful attack. There exists another different approach [16] that applying known perturbations to the system and measuring the changes elsewhere to detect the attack.

There are mainly two strategies to consider making sure the functionality of SE against FDA in recent work. The first intuition is to protect the meters from being compromised by attackers. These work has largely been studied by [14,18,19]. In the beginning of their work, they study how to construct a successful attack and analyze the least number of compromised meter needed. Then the problem is usually equivalently converted to l_0 and l_1 relaxation optimization problem and by linear programming methods it can be solved under some system constraints. The l_1 relaxation has been proven to show more effective than l_0 relaxation [18].

* Corresponding author. Address: School of Control and Computer Engineering, North China Electric Power University, 2 Beinong Road, Huilongguan Town, Beijing, China. Tel.: +86 (0)10 6177 2757.
E-mail address: wangyiliang206@163.com (Y. Wang).

0142-0615/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijepes.2013.11.057

Some other methods try to solve the problem with graph theory and power network [15,19]. Even though the least number can be computed and specific meters do, the issue still remains about practically effectiveness and latent risk to power grid. The other strategy is trying to use historical data and statistics against FDA [12,15]. The two strategies can both be implemented to defend against FDA.

In this paper, we first analyze the general principle about how to find a sparse attack and then study the properties of measurement residual with empirical data, and formalize the problem as a hypothetic test of norm distribution. Based on the observation, we propose our detector versus the conventional detector against the FDA. We also study the FDA in worse scenario the attacker can hide attack data more secretly and present a heuristic strategy to construct an average energy attack vector. By analyzing the relationship between attack energy and detection probability, our detector outperforms other detectors.

The rest of the paper is organized as follows. Section 2 presents the vulnerability of SE and gives the basic principle and general analysis of FDAs. In Section 3, we introduce our proposed approach against the attacks in different conditions, respectively. We show the effective experimental results of the approach in defending the system in Section 4. Section 5 concludes and discusses future research directions.

2. False data attack

2.1. Basic principles

We consider a linearized dc power flow model derived from complex ac power flow model. For accurate state estimation, the relationship between measurements and state variables can be expressed in a linear matrix form.

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{1}$$

where $\mathbf{z}$ is the $m \times 1$ vector of measurements, $\mathbf{x}$ is the $n \times 1$ vector of power system state variables and $\mathbf{e}$ is the vector of measurements noise distributed according to a Gaussian distribution with a zero mean and covariance diagonal matrix $\mathbf{R}$ and $\mathbf{W} = \mathbf{R}^{-1}$ [3]. $\mathbf{H}$ is a $m \times n$ measurement jacobian matrix, that depends on the topology of power grid. It is efficacious that use redundant measurements to obtain high estimation accuracy and protect against bad measurements, which means the number of measurement is always larger than state variables', and $\mathbf{H}$ is a full column rank matrix.

The basic FDA, as presented in Ref. [10], is supposed to construct an attack vector injected into measurements by satisfying

$$\mathbf{a} = \mathbf{H}\mathbf{c} \tag{2}$$

It is common that analysis process of bad data of State Estimation adopts the measurements residual strategy, based on their properties and expected probability distribution. Taking $J(x)$ detection of the weighted least squares state estimation (WLS) into consideration, the 2-norm of measurements residual while an attack vector has been injected is

$$\begin{aligned} \|\mathbf{z}_a - \widehat{\mathbf{z}}_a\|_2^2 = & \ \|(\mathbf{z} + \mathbf{a}) - \mathbf{K}(\mathbf{z} + \mathbf{a})\|_2^2 \\ = & \ \|(\mathbf{I} - \mathbf{K})\mathbf{z} + (\mathbf{I} - \mathbf{K})\mathbf{H}\mathbf{c}\|_2^2 \\ = & \ \|(\mathbf{I} - \mathbf{K})\mathbf{z}\|_2^2 \leqslant \tau \end{aligned} \tag{3}$$

where $\mathbf{K}$ is the hat matrix of SE and $\mathbf{K} = \mathbf{H}(\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}$, and τ is threshold determined by the system. It would be noticed the adversary can manipulate measurements values without triggering the alarm defense system since the attack vector bypasses the measurement residual detection.

We assume that the attacker could have hacked into the power grid network and got the system configure information. He could contaminate the state variable with the error

$$\widehat{\mathbf{x}}_{bad} - \widehat{\mathbf{x}} = (\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{a} = \mathbf{c} \tag{4}$$

Note that $\mathbf{c}$ is an arbitrary nonzero vector. Traditional bad data detectors and Hypothesis Testing Identification (HTI) can not deal with the special interacting bad data that has been intentionally generated in FDA.

2.2. General analysis on FDA

To construct a success FDA, the attacker has to intrude the metering infrastructure and injects highly correlated false data to deceive the system center controller. Not only does he have to know the topology and configuration information, he also need keep the false data under low profile. Considering the practical that some measurements cannot be compromised and specific goals of the attacker, the problem about how to construct a meaningful attack is transformed into following formulation:

$$\begin{aligned} \underset{\mathbf{c}}{\text{minimze}} \quad & \|\mathbf{a}\|_2 \\ \text{s.t.} \quad & \mathbf{H}^S(\mathbf{c}) = 0 \\ & \mathbf{H}^k(\mathbf{c}) = 1 \\ & \|\mathbf{c}\|_2 \geqslant \tau_c \end{aligned} \tag{5}$$

where $\mathbf{H}^S$ denotes that meters cannot be reached by attacker and are safe whether are protected or not. $\mathbf{H}^k$ denotes the meter the attacker wants to intrude and change to a particular value. The last constraint means the false data takes effect and brings meaningful loss into system. The formulation can be solved by nonlinear program methods or many intelligent optimization methods such as GA, and ABC [20]. However, it is not easy to find the optimal solution and these methods take lots of iterations to approximate the optimal solution. Nevertheless, it is worth trying because the attacker may prepare within enough time before attacking the system. It has been studied that a small set of meters could be chosen to set up an unobservable attack. The number of meters is more interesting to the attacker than attack energy. So taking the scenario the attacker need to intrude less meters, the problem can be transformed into following form:

$$\begin{aligned} \underset{\mathbf{c}}{\text{minimze}} \quad & \|\mathbf{a}\|_0 \\ \text{s.t.} \quad & \mathbf{H}^S(\mathbf{c}) = 0 \\ & \mathbf{H}^k(\mathbf{c}) = 1 \\ & \|\mathbf{c}\|_2 \geqslant \tau_c \end{aligned} \tag{6}$$

It is pointed out that finding a k-sparse attack vector is an NP-complete problem [21]. So mostly the attacker try to find a solution that may not be the sparsest and we can evade the NP hardness. Then he solves the following formulation:

$$\begin{aligned} \underset{\mathbf{c}}{\text{minimze}} \quad & \|\mathbf{H}^{\bar{S}}(\mathbf{c})\|_1 \\ \text{s.t.} \quad & \mathbf{H}^S(\mathbf{c}) = 0 \\ & \mathbf{H}^k(\mathbf{c}) = 1 \\ & \mathbf{c}_i = 1 \end{aligned} \tag{7}$$

where $\mathbf{H}^{\bar{S}}$ corresponds to those meters compromised and $\mathbf{c}_i$ means some state variable the attacker wants to change specifically. Many papers have been presented on solving the equation or its equivalent forms for achieving better computational ability and optimal solution [14,18,22,23]. These meters are more vulnerable to attackers and suggest they need protecting to keep the system functions normally.

3. State summation strategy against FDA

3.1. Critical meters and secure measurements

The sufficient condition that an unobservable attack can be found is the number of meters can be accessed by attacker is more that $m - n$ [21]. So it means we at least need to protect n meters to absolutely prevent FDA. If the cardinality of S which is a set of meters cannot be reached by attacker is more than n, the **c** is equal to zero and there is no solution for Eqs. (5)–(7). Then a secure subset of meters can be chosen and protected against FDA. Let N_τ denote the number of secure set to be protected at last and $N_\tau \geqslant n$. Let $N_c = \|S\|_0$ and a^* denote the meters the attacker compromise every time. So we can formulate the problem into choosing critical meters and add them into secure set until $N_c \geqslant N_\tau$. The following is the procedure of secure measurements (see Fig. 1).

3.2. State summation strategy and formulation

In this section, we propose our State Summation Detection (SSD), which is compatible with the conventional measurements residual detection for FDAs, and discuss it relation with secure measurements. For bad data detection, the measurements residual is most widely proposed to calculate the difference between measurements and estimated values. Here we assume that the state variables in State Estimation are independently given, and are not necessarily identically distributed and then analyze the properties of the sum of large measurements in power system. At last, we give our detector and show its effectiveness in section 4.

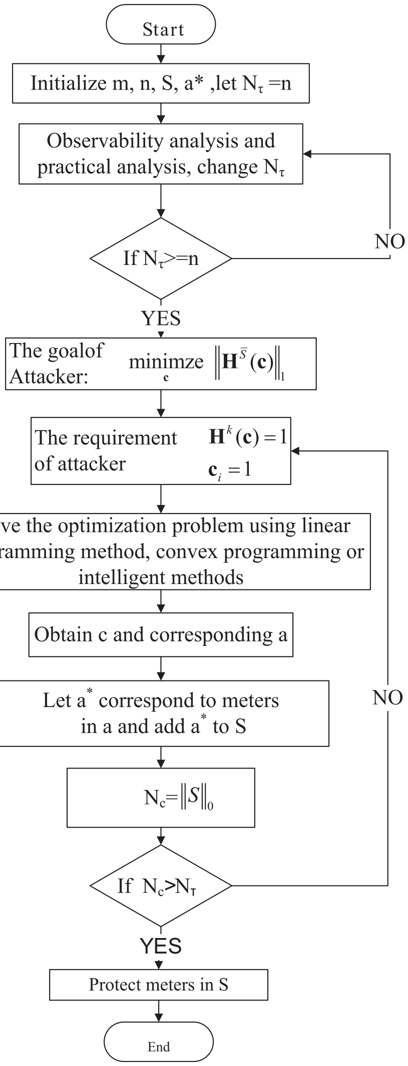
Start
Initialize m, n, S, a* ,let N_τ =n
Observability analysis and practical analysis, change N_τ
If N_τ>=n
NO
YES
The goalof Attacker:
$\underset{c}{\text{minimze}} \left\|\mathbf{H}^{\bar{S}}(\mathbf{c})\right\|_1$
The requirement of attacker
$\mathbf{H}^k(\mathbf{c}) = 1$
$\mathbf{c}_i = 1$
Solve the optimization problem using linear programming method, convex programming or intelligent methods
Obtain c and corresponding a
Let a^* correspond to meters in a and add a^* to S
$N_c = \|S\|_0$
If N_c>N_τ
NO
YES
Protect meters in S
End

Fig. 1. The flowchart of determining critical meters and a set of secure measurements.

3.2.1. Our solution formulation

In order to maintain a stable system, the control center has to make moderate decision according the current running state which is estimated by the state estimation. The state estimation has to filter error data and find an optimal estimation. Considering the WLS, most widely proposed estimation, the bad data is processed with 2-norm measurements residual, namely $J(x)$ that is given below,

$$J(\hat{x}) = \mathbf{r}^T\mathbf{W}\mathbf{r}, \qquad \mathbf{W} = \mathbf{R}^{-1} \tag{8}$$

where $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$ is the measurements residual and $\hat{\mathbf{x}}$ is estimated vector of dimension n. Assuming that meter errors are the normally distributed and state variables follow independent random distribution, the $J(\hat{x})$ can be mathematically proven that it follows Chi-squares distribution of $m - n$ degree of freedom. So we can desire a hypothetical test based on χ^2 distribution to detect bad data.

As showed in Ref. [10], there exist FDAs that could bypass the measurement residual detection and introduce into state variables. So it is spontaneous for us to think of an enviable approach against the attack with state variable changes. Consider the following formulation

$$S_x = \mathbf{z}^T\mathbf{W}\mathbf{z} - J(\hat{x}) \tag{9}$$

The S_x represents the true measurement square sum in the formula. When the estimation is correct and no FDA, we can lead it to a simple form with the following solution,

$$J(\hat{x}) = \mathbf{r}^T\mathbf{W}\mathbf{r} = (\mathbf{z} - \hat{\mathbf{z}})^T\mathbf{W}(\mathbf{z} - \hat{\mathbf{z}}) \tag{10}$$

With the formula $\hat{\mathbf{z}} = \mathbf{K}\mathbf{z}$ [3], so we can simplify S_x by the transformation,

$$\begin{aligned} S_x = &\ 2\mathbf{z}^T\mathbf{W}\hat{\mathbf{z}} - \hat{\mathbf{z}}^T\mathbf{W}\hat{\mathbf{z}} \\ = &\ \mathbf{z}^T(2I - \mathbf{K}^T)\mathbf{W}\mathbf{K}\mathbf{z} \\ = &\ \mathbf{z}^T\mathbf{K}_W\mathbf{z} \end{aligned} \tag{11}$$

where we let $\mathbf{K}_W$ equal to $(2I - \mathbf{K}^T)\mathbf{W}\mathbf{K}$. Then we substitute $\mathbf{z} = \mathbf{H}\mathbf{x}_0$ for measurements vector **z**, while $\mathbf{x}_0$ represents the real state variables correspondent to every measuring. Having $\mathbf{KH} = \mathbf{H}$, S_x can be written

$$\begin{aligned} S_x = &\ \mathbf{x}_0^T\mathbf{H}^T\mathbf{K}_W\mathbf{H}\mathbf{x}_0 \\ = &\ \mathbf{x}_0^T\mathbf{H}^T\mathbf{W}\mathbf{H}\mathbf{x}_0 \\ = &\ \mathbf{x}_0^T\mathbf{G}\mathbf{x}_0 \end{aligned} \tag{12}$$

where **G** is the gain matrix, generally non-negative definite and could be Cholesky factorized. From the observation of (14), we can conclude that S_x is the value of true state variables sum. Conspicuously, S_x is real quadratic form and can be brought to a diagonal form.

While an adversary constructs a FDA, he would inject errors into the system as large as he can to achieve his purpose. So we consider the changes of S_x under conditions of FDAs. Given a specific attack vector **a**, then we could rewrite the S_x as

$$\begin{aligned} S_{xbad} = &\ (\mathbf{z} + \mathbf{a})^T\mathbf{K}_W(\mathbf{z} + \mathbf{a}) \\ = &\ \mathbf{x}_0^T\mathbf{G}\mathbf{x}_0 + 2\mathbf{x}_0^T\mathbf{G}\mathbf{c} + \mathbf{c}^T\mathbf{G}\mathbf{c} \\ = &\ S_x + f(\mathbf{c}) \end{aligned} \tag{13}$$

where **c** is an arbitrary nonzero injection attack vector and **a** = **Hc**. Note that if we could determine the S_x, then the attack vector can be distinguished. The Eq. (12) is composed of non-central chi-squared distribution which can be derived and solved [24]. When the freedom of chi-squared distribution is larger than 30, it is usually dealt as norm distribution. In this case, S_x approximates to norm distribution according to Central Limit Theorem. And it is treated as norm distribution when the power system is larger than 30 bus system.

Considering the power system is operating regularly, we assume that the state variables are independently random distributed with mean μ_x and covariance σ_x [15]. With large numbers of state variables in current power system, S_x follows normal distribution. $S_x \sim N(\mu_{sx}, \sigma_{sx}^2)$ according to Central Limit Theorem. So far we can desire a detector against false attacks. It is essential for control center that a detector can identify errors and replace with correct data, but preliminarily we focus on protecting power system from the catastrophic impact of injection attacks. Here we consider the detector SSD distinguishing the following hypothetic test.

$$\begin{aligned} H_0 &: \ \mathbf{c}=\mathbf{0}\\ H_1 &: \ \left|\frac{S_x-\mu_{sx}}{\sigma_{sx}}\right|>\lambda, \quad \mathbf{c}\neq\mathbf{0}\end{aligned} \tag{14}$$

where λ is a threshold and determined by the significant level of the test. The detector makes decision based on the hypothetic test. In the small scale system, we can set a threshold for S_x according to historical data and when there is a FDA, the value will exceed the threshold. From problem formula (13), $f(\mathbf{c})$ denotes the deviance how large the false attacks could introduce into the state variables sum. So we consider this problem formulation in adversary's perspective.

$f(\mathbf{c})$ is a quadratic function that equals to zeros when **c** is zero vector, which means the attacker does not attack the system. So we consider the optimization problem

$$\begin{aligned} &\text{maximize } \|f(\mathbf{c})\|_1\\ &\text{s.t. } \Pr\,(H_0|\mathbf{c}) \leqslant \alpha, \quad \mathbf{a} \text{ is } k\text{-sparse}\end{aligned} \tag{15}$$

It means if the adversary knows the detector, he tries to find the largest error the detector could tolerate. Equivalently, he can resolve the problem in the form

$$\begin{aligned} &\text{maximize } \|\mathbf{c}^T\mathbf{G}\mathbf{c}\|_2^2\\ &\text{s.t. } \Pr\,(H_0|\mathbf{c}) \leqslant \alpha, \quad \mathbf{a} \text{ is } k\text{-sparse}\end{aligned} \tag{16}$$

Certainly, the adversary is more interested in introduce larger error into the system. It can be solved in an equivalent form

$$\begin{aligned} &\text{maximize } \|\mathbf{c}\|_2^2\\ &\text{s.t. } \Pr\,(H_0|\mathbf{c}) \leqslant \alpha \quad \mathbf{a} \text{ is } k\text{-sparse}\end{aligned} \tag{17}$$

In any case, the adversary could solve a series of linear functions if there exists an optimal solution. Note if the attacker can compromise up to k meters and there is no restriction on which meters are chosen, it is an NP-complete problem. All in all, it is necessary for a detector to alleviate the attack impact on the power system.

3.2.2. Relationship with critical measurements

The main purpose of state summation is analyzing the impact FDA imposes on SE. The change of the state variables injected by the attacker differentiates it form historic data. The attacker would not change all state variables under different goals. So it is feasible to choose a set of state variables and analyze their variation. While in the observability analysis, redundant measurements are found to make power system more reliable instead of critical measurements we try to obtain in Section 2. Considering the critical measurements in power system, their corresponding state variables are more vulnerable to FDA. In this case, we can take advantage of critical measurements to pinpoint the vulnerable state variables. Let S_c denote those state variables are directly related to meters in S and $n_c = \|S_c\|_0$. While $\|S\|_0 \geqslant n$, all state variables are included in S_c according to SE. Here the flowchart of choosing a subset is given following (see Fig. 2):

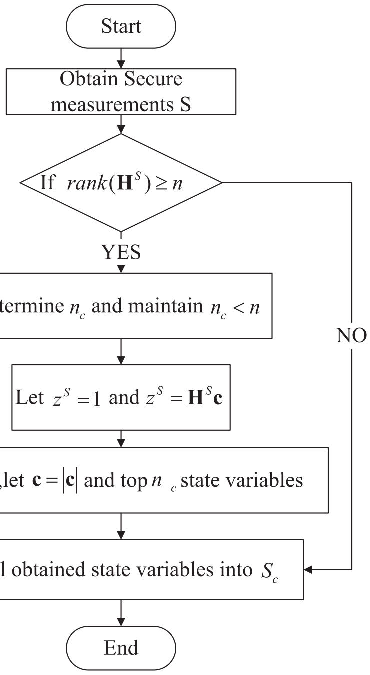
Start
Obtain Secure measurements S
If $rank(\mathbf{H}^S) \geq n$
YES
NO
Determine n_c and maintain $n_c < n$
Let $z^S = 1$ and $z^S = \mathbf{H}^S\mathbf{c}$
Obtain $\mathbf{c}$,let $\mathbf{c} = |\mathbf{c}|$ and top n_c state variables
Add all obtained state variables into S_c
End

Fig. 2. The flowchart of choosing a subset of state variables according to secure measurements.

Then we can simplify our formulation and lower computation when substitute the state variable in S_c for all state variables. The attacker's strategy (16) can be rewritten into:

$$\begin{aligned} &\text{maximize } \|\mathbf{c}\|_2^2\\ &\text{s.t. } \Pr\,(H_0|\mathbf{c}^S) \leqslant \alpha \quad \mathbf{a} \text{ is } k\text{-sparse}\end{aligned} \tag{18}$$

So the empirical prior of critical state variables can be used to detect FDA. The strategy of using state variables is complementary to secure measurements. Even we can pinpoint a set secure meters against FDA, updating and encrypting them face practical operation problems and accelerate computational needs for real-time SE. As with development of Smart Grid, these two strategies can be both put into effect and made against FDA.

3.2.3. Our detector

Considering the problem formulation (14), we can desire a detector against the false attack. The control center can estimate the mean and covariance $(\widehat{\mu}_{sx}, \widehat{\sigma}_{sx})$ of the distribution of S_x according to empirical data stored in the data center. The measurement residual is effective in dealing with bad data except the intentional false data, so we integrate the $J(x)$ detector with 2-norm in our detector. Our detector, SSD, is given as

$$L_2(\mathbf{x}) = \begin{cases} 1 & \text{if } J(x) > \tau \text{ or } \left|\frac{S_x-\widehat{\mu}_{sx}}{\widehat{\sigma}_{sx}}\right| > \lambda \\ 0 & \text{otherwise}\end{cases} \tag{19}$$

where the two threshold, τ and λ, mark the significant level of hypothetic test. We vary λ to test our detector and fix τ to a desired false alarm probability. The SSD is a detector based on summation of all state variables, the properties of normalized state variables for a single false data can be used to devise a test for identifying

FDA. The single state detector denoted by SiSD, can be written as following:

$$L(\mathbf{x}) = \begin{cases} 1 & \text{if } \left|\frac{x-u_x}{\sigma_x}\right| > \lambda_x \\ 0 & \text{otherwise} \end{cases} \quad (20)$$

In power system the state variables would converge in numeric range when the system maintains a stable state. It is more probable the detectors will detect FDA when the power system is running more stable and regularly. We test its influence on our detector on IEEE bus test system. Moreover we concentrate the relation between false data injection impact and the probability of being detected.

4. Experiment result and discussions

In this section, we implement our detector proposed on the Section 3 and use IEEE test systems to evaluate the performance, including 14-bus, 118-bus. We run our experiments using matlab 7.11 and extract the configuration (matrix H, real value of state variables) from MATPOWER 4.1 [25]. The state variables and measurements are the same as used in Ref. [10]. We plot the relationship between false data injection vector and detection probability with AOC and ROC curve, defined in Ref. [15]. Respectively, AOC depicts the relation between false data injection vector and detection probability and fixes the probability of false alarm, while the ROC curve fixes the false data injection vector and varies the probability of false alarm. We compare the $J(x)$ detector, LNR detector with our detector to see the effectiveness.

Without loss of general, we assume that the rate of variance to mean of S_x is 0.1, by that the normal state variables can fluctuate around 20%. Also, we generate diagonal matrix **R** by setting diagonal elements with number 625 [10], then introduce noise with norm distribution $(0, 0.04^2)$. We characterize the energy of FDA with 2-norm of attack vector **a**, Attack MSE, defined as $10\log_{10}\left(\|\mathbf{a}\|_2^2/m^*\sigma_{noise}^2\right)$. Considering large scale of bus system, we reiterate 300 times for 118-bus system in each experiments, while 500 times for 14-bus system.

4.1. Scenario 1 – Random false data attack detection

In this scenario, we implement random FDA against power system. In order to hide the attack from attacker's perspective, we distribute the attack's energy into every measurement. First, we evaluate the impact of noise on detectors. The results are showed in Fig. 3 for 14-bus system and Fig. 4 for 118-bus system. For the L_∞ detector or other single value test, it is because the probability of extraordinary noise is $1-(1-\alpha)^m$ (α and m are probability of significance test and measurements number), so the detection probability increases fast while the system is getting bigger. Our results show this property. For 118-bus system, we set the probability of false alarm $\alpha/10$ for LNR detector.

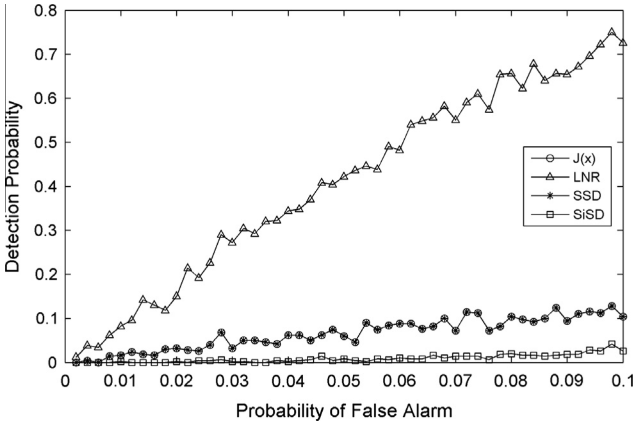

Fig. 3. Comparison of four detectors without FDA for 14-bus system.

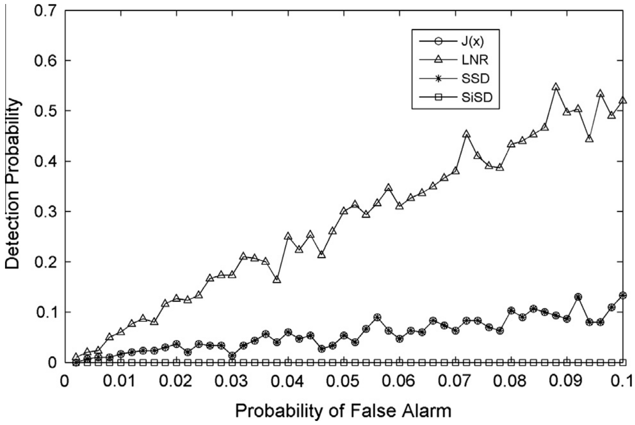

Fig. 4. Comparison of four detectors without FDA for 118-bus system, the *x*-axis of LNR is from 0 to 0.01.

From formula (15), the SSD detects the FDA through the impact on state variables. The problem of finding the max attack vector of being undetected is equivalent to find the min attack vector of being detected. More specifically, we resolve this problem as (17). Now, we consider the problem from adversary's perspective. A successful attack does more concern the attacker and is more dangerous. We substitute the Attack MSE for (17) to see how large the energy injected can arouse false alarm directly. Additionally, we evaluate the performance of our detector for worse scenario that the attacker can manipulate enough meters to inject a random attack data. So it can hide the attack more secret by reducing error in each meter to evade conventional detector. 20 m are corrupted for 14-bus system of 34 m, 230 m for 118-bus system of 304 m. Our heuristic strategy is dividing basis resolution of false attack into little standard energy block and adding to an attack vector little by little.

Figs. 5 and 6 show the AOC relationship between attack energy and detection probability under 0.05 false alarm rate. We can see that the detection probability of SSD and SiSD increase fast when the energy exceeds some values for both in power system. For large scale system, the detection rate of SiSD is better than SSD and the attack's energy ratio is higher than attacking 14-bus system. The reason is that SiSD is checking the most fluctuated state and it is

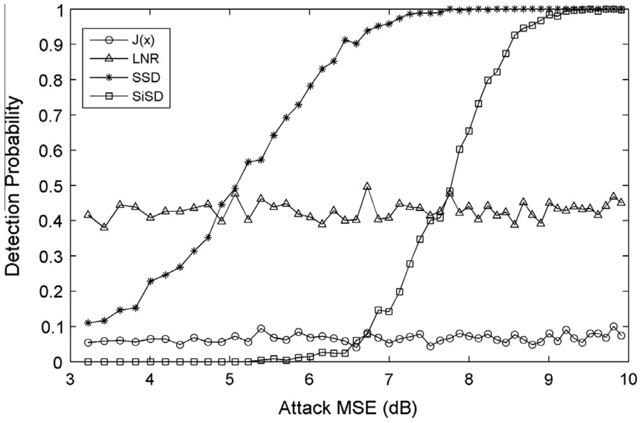

Fig. 5. AOC performance of SSD and SiSD under random attack with km = 20 for 14-bus system. False alarm rate is 0.05.

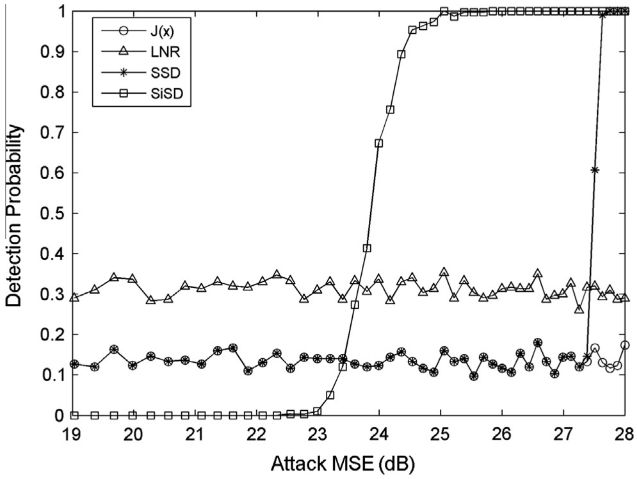

Fig. 6. AOC performance of SSD and SiSD under random attack with km = 230 for 118-bus system. False alarm rate is 0.05 for SSD, SiSD $J(x)$, and 0.005 for LNR.

not easy to make sure all state variables are in regular scope when implementing FDA. We also can derive from Fig. 5 and 6 that the SSD limits the attack's energy and is more sensitive in smaller power system.

Observe that the $J(x)$ detector and LNR detector cannot detect the FDA even the detection probability is not zero. Comparing with noise detection result, the detection probability of LNR does not increase due to our heuristic strategy to reduce each false data in meters. If the adversary cannot control enough meters, the energy concentrates on several measurements leading to be detected by single value detector.

Figs. 7 and 8 show the ROC performance of SSD and SiSD comparing with LNR and $J(x)$ detector. As we can see, the SSD outperforms other detectors in 14-bus system and SiSD does in 118-bus system. The false alarm decides the value of λ and τ in (19) and (20), specifically the rate is 0.05. As presented in (17), the attacker tries to find the largest impact on state variables under fixed energy. In unlimited source attack, the search for k meters of optimal solution is NP-hard problem. Therefore, we conduct random attacks, and iterate many times to approximate it.

It can be derived from (19) that if the FDA introduces very low energy and non-norm distributed errors into SE, the detector may not trigger FDA alarm and treat it as system variation. In the larger power system, it is difficult to find an FDA to make sure all the state variables change in its regular value scope. So it is easier to detect the FDA using single state variable detection in large power system, otherwise SSD does better. However, in this case this type attacker do not do more harm than that of FDA launched by attackers with special goals. Just like $J(x)$ detector, it is tolerated when the valve of error is low. Figs. 5–8 can reflect this characteristic. When the energy of FDA is low, the probability of detecting is as same as traditional detector. As the energy rises, we can see that the alarm is more probably triggered. The state summation strategy can be complementary to traditional bad data detector and protect power system against FDA.

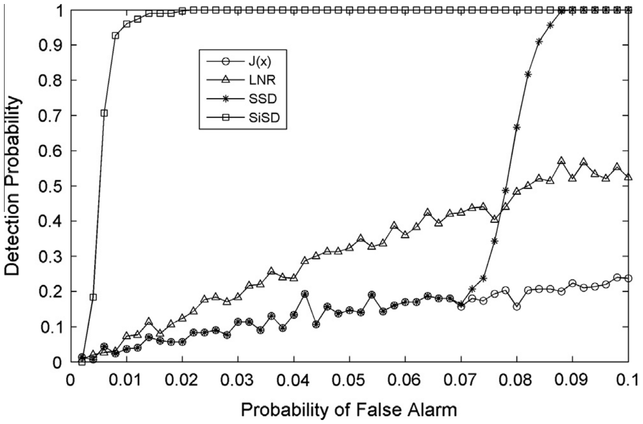

Fig. 8. ROC performance of SSD and SiSD under random attack with km = 230 for 118-bus system. Attack MSE is 27 dB. The x-axis of LNR is from 0 to 0.01.

4.2. Scenario 2 – Single and normal state variable attack detection

In this scenario, we first conduct FDA aiming to change a single state variable to check our detectors' performance. The single state variable in this experiment is set to be the phase degree on second bus. The other settings of power system are the same as scenario 1. We add 20% perturbation to power system and eliminate the noise of measurements for clear view. First, the non-attack scenario is simulated and the results are shown in Figs. 9 and 10 respectively for 14-bus system and 118-bus system. The false positive rate of SiSD is high in the 118-bus and the reason is the same as LNR detector in scenario 1. Then we conduct false state attack aiming at the second state variable. The attack energy is rising to change the state variable from 0.01 to 0.5 of its normal state value. Figs. 11 and 12, the x-axis is the ratio of attack energy to the value of the state variable, show the results

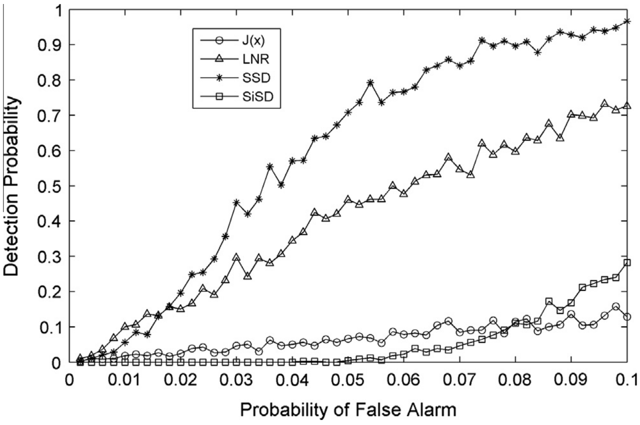

Fig. 7. ROC performance of SSD and SiSD under random attack with km = 20 for 14-bus system. Attack MSE is 5.703 dB.

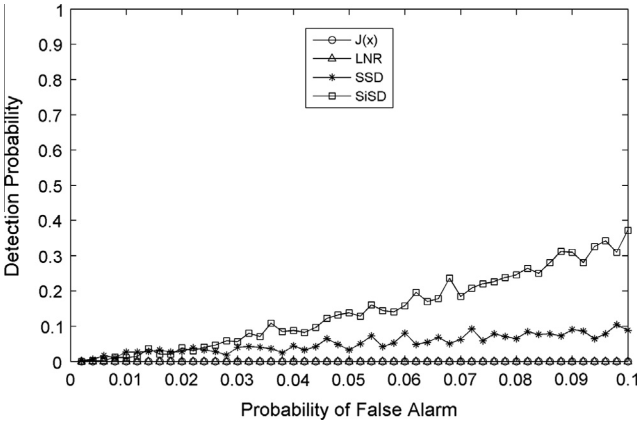

Fig. 9. Comparison of four detectors with 20% fluctuation of state variables and no noise for 14-bus system.

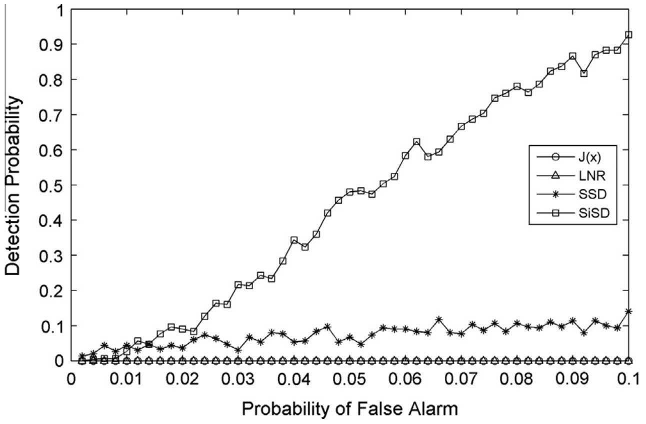

Fig. 10. Comparison of four detectors with 20% fluctuation of state variables and no noise for 118-bus system.

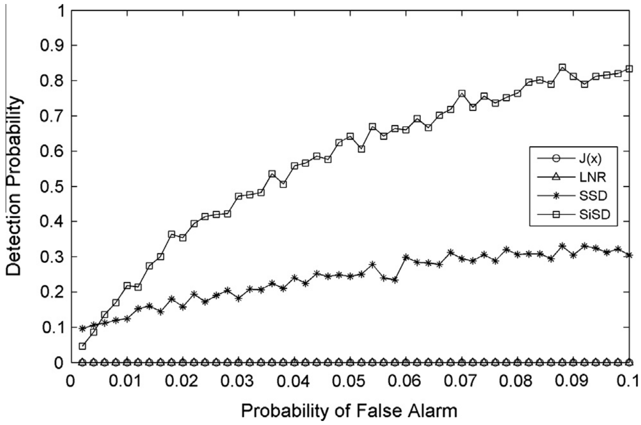

Fig. 13. Results of detection for normal state FDA for 14-bus system.

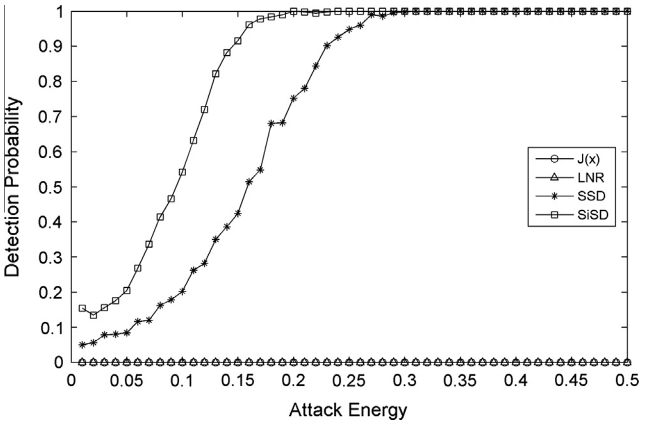

Fig. 11. Results of detection for single state FDA for 14-bus system.

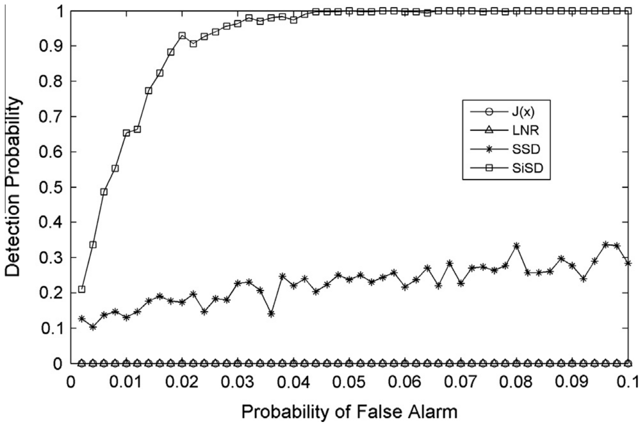

Fig. 14. Results of detection for normal state FDA for 118-bus system.

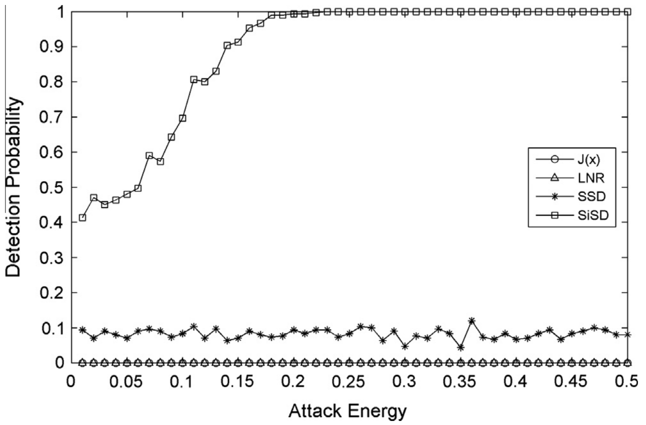

Fig. 12. Results of detection for single state FDA for 118-bus system.

and the SSD and SiSD detectors in 14-bus system work well and have little difference in detection probability. But in 118-bus system, the SSD cannot detect the single FDA because its impact on all state variables is too small to trigger the alarm while the SiSD has large false positive rate.

In the next experiment, we simulate the scenario that the attacker injects false data following the norm distribution as same as state variables. In this case, the meaning of this attack is to get specific view to know the essence of FDA. We formulate the attack following norm distribution with $xk \sim N(0, \sigma_x^2)$ where xk is attacker's aim. Even though we separate the FDA from ST in the experiment, the problem can be rewritten into $x \sim (u_x, 2\sigma_x^2)$ after the attacker injects false data. The results are shown in Figs. 13 and 14 respectively for 14-bus and 118-bus system. The formulation is demonstrated from the results. The performance of SSD in Figs. 13 and 14 can definitely show that the FDA is an attack that its data are in accord with power system network topology and are trying to staying in accord with normal data of historical running regular state of power system. If it causes relative perturbation or network topologic failure, it will be detected by our detectors. The principle of state detectors is trying to identify anomalous data according to historical and regular data of power system. If the power system is more stable or regular, FDA is more and more difficult to successfully implement.

5. Conclusions

In this paper, FDA which recently was found to have the ability to stealthily inject false data into SE was introduced and attracted lots of scientists' attention such as Henrik Sandberg and Kin Cheong Sou (KTH Royal Institute of Technology, Stockholm, Sweden). Its impact on power system has been analyzed from DC SE to AC SE. At the same time two strategies based on secure measurements and statistics of variables' value were developed to defend against FDA. General analysis about how to find an optimal attack from specific goal was studied in the paper. A set of critical meters was greedily chosen based on the analysis and can give instruct about which state variables are more vulnerable to FDA. Then we proposed a state summation strategy against the FDA. By studying the properties of measurement residual with empirical data, we formalized the problem as a hypothetic test of norm distribution. We also implemented our detector in MATLAB and validated its effectiveness on IEEE bus test system, including 14-bus system and 118-bus system in comparison with conventional detectors. Particularly, we studied the energy of false attack of being detected and provided a heuristic strategy of constructing an average energy attack in our experiments. In future research, we study detecting more realistic data attacks including unlimited resources scenario, and distinguish topology changes of network with high perturbation and its impact on AC power system.

The main contributions of this paper can be listed as following three points. (1) The strategy based on state variables of detecting FDA is proposed and validated effective. For different power systems, two methods are discussed and analyzed. The SSD and SiSD are suggested complementarily using at the same time. For Large power systems, it is effective to divide into small or median blocks to defend against FDA. (2) The historical data of power system can be used to detect FDA. Here we assume it is subject to norm distribution and discuss its function. It is more general and practical to treat these data with Bayesian methods in the future research. (3) The essence of FDA are discussed in the last experiments which disguises itself as normal running data of power system in accord with network topology. The more stable and regular power system is, the more difficult FDA is to hide itself. Also FDA is difficult to successfully implement for it needs large information about network configuration and running regularity of power system.

Acknowledgement

This paper is supported by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry ([2013]693).

References

[1] Baumeister T. Literature review on smart grid cyber security. Honolulu, HI, USA; 2010.
[2] Bompard E, Huang T, Wu Y, Cremenescu M. Classification and trend analysis of threats origins to the security of power systems. Int J Electr Power Energy Syst 2013;50:50–64.
[3] Abur A, Expsito AG. Power system state estimation: theory and implementation. New York: Marcel Dekker; 2004.
[4] Handschin E, Schweppe FC, Kohlas J, Fiechter A. Bad data analysis for power system state estimation. IEEE Trans Power Ap Syst 1975;94:329–37.
[5] Van Cutsem T, Ribbens-Pavella M, Li M. Hypothesis testing identification: a new method for bad data analysis in power system state estimation. IEEE Trans Power Ap Syst 1984;PAS-103:3239–52.
[6] Graven JH, van Amerongen RAM. Static state estimation with DC models and linear programming. Int J Electr Power Energy Syst 1986;8:241–7.
[7] Prieto F, Sarabia JM, Sáez AJ. Modelling major failures in power grids in the whole range. Int J Electr Power Energy Syst 2014;54:10–6.
[8] Asada EN, Garcia AV, Romero R. Identifying multiple interacting bad data in power system state estimation. Power engineering society general meeting. San Francisco, CA: IEEE; 2005. p. 571–7.
[9] Singh D, Misra RK, Singh VK, Pandey RK. Bad data pre-filter for state estimation. Int J Electr Power Energy Syst 2010;32:1165–74.
[10] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. In: The 16th ACM Conference on Computer and Communications Security (CCS'09). Chicago, IL, USA: ACM; 2009. p. 21–32.
[11] Bobba RB, Rogers KM, Wang Q, Khurana H, Overbye KNaTJ. Detecting false data injection attacks on DC state estimation. In: Proceedings of the first workshop on Secure Control Systems (SCS'10). Stockholm, Sweden; 2010. p. 226–31.
[12] Kosut O, Jia L, Thomas RJ, Tong L. Limiting false data attacks on power system state estimation. In: The 44th information sciences and systems (CISS) Conference. Princeton, NJ, USA; 2010. p. 1–6.
[13] Sandberg H, Teixeira A, Johansson KH. On security indices for state estimators in power networks. In: The first workshop on secure control systems. Stockholm Sweden; 2010.
[14] Kim TT, Poor HV. Strategic protection against data injection attacks on power grids. IEEE Trans Smart Grid 2011;2:326–33.
[15] Kosut O, Jia L, Thomas RJ, Tong L. Malicious data attacks on the smart grid. IEEE Trans Smart Grid 2011;2:645–58.
[16] Morrow KL, Heine E, Rogers KM, Bobba RB, Overbye TJ. Topology perturbation for detecting malicious data injection. In: The 45th System Science (HICSS) conference. Hawaii, USA; 2012. p. 2104–13.
[17] Esmalifalak M, Huy N, Rong Z, Zhu H. Stealth false data injection using independent component analysis in smart grid. In: 2011 IEEE international conference on Smart Grid Communications (SmartGridComm); 2011. p. 244–8.
[18] Kin Cheong S, Sandberg H, Johansson KH. On the exact solution to a smart grid cyber-security analysis problem. IEEE Trans Smart Grid 2013;4:856–65.
[19] Giani A, Bitar E, Garcia M, McQueen M, Khargonekar P, Poolla K. Smart grid data integrity attacks. IEEE Trans Smart Grid 2013;4:1244–53.
[20] Li Y, Wang Y, Li B. A hybrid artificial bee colony assisted differential evolution algorithm for optimal reactive power flow. Int J Electr Power Energy Syst 2013;52:25–33.
[21] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Trans Inf Sys 2011:14.
[22] Kin Cheong S, Sandberg H, Johansson KH. Electric power network security analysis via minimum cut relaxation. In: 2011 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC); 2011. p. 4054–9.
[23] Kin Cheong S, Sandberg H, Johansson KH. Computing critical k-Tuples in power networks. IEEE Trans Power Syst 2012;27:1511–20.
[24] Sheil J, O'Muircheartaigh I. Algorithm as 106: the distribution of non-negative quadratic forms in normal variables. J Roy Stat Soc: Ser C (Appl Stat) 1977;26:92–8.
[25] Zimmerman RD, Murillo Sanchez CE, Thomas RJ. MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans Power Syst 2011;26:12–9.