Title	System-state-free false data injection attack for nonlinear state estimation in smart grid
Author(s)	Wang, J; Hui, LCK; Yiu, HSM
Citation	International Journal of Smart Grid and Clean Energy, 2015, v. 4 n. 3, p. 169-176
Issued Date	2015
URL	http://hdl.handle.net/10722/217773
Rights	Creative Commons: Attribution 3.0 Hong Kong License

International Journal of Smart Grid and Clean Energy

System-state-free false data injection attack for nonlinear state estimation in smart grid

Jingxuan Wang, Lucas C. K. Hui, S. M. Yiu*

Department of Computer Science, The University of Hong Kong, Hong Kong

Abstract

Cyber-physical security of smart grid under attacks is a serious issue today. The technique of state estimation has been employed in such a large-scale system to ensure the reliability. Successful attacks on tampering these readings were shown for ***linear*** state estimation. For the more realistic ***nonlinear*** state estimation are used in real systems, the attack that requires the knowledge of system states (which are difficult to obtain, even for insiders) was proposed. Up to our best knowledge, there are no research results that are able to give an attack to any buses without the knowledge of system states. This research paper provides such an attack. Demonstrations on IEEE test system show that the smart grid can be exploited by launching such attacks even without system state information. The strategy to generate such an attack is simple and easy to implement. Thus, the results in this paper show that a more realistic threat to the smart grid system. Hopefully the community could revisit the tampered reading detection algorithms to come up with a more sophisticated solution to avoid this vulnerability.

Keywords: False data injection attack, state estimation, cyber-physical system, smart grid, information security

1. Introduction

Cyber Physical System (CPS) is an integrated system in which computational elements collaborate to control physical entities. CPS was regarded as a top-priority research area since 2007 [1]. Being a critical infrastructure, smart grid is a typical example of CPS (e.g. with the sensors and smart meters as the physical entities, the SCADA (Supervisory Control and Data Acquisition) control system as one of the computational elements). The current trend of smart grid is to provide *on-demand* power supply according to *real-time* user requirements [2]. One of the major security concerns of a smart grid system is on the communications of the cyber components (i.e. software in the SCADA system) and the physical components (i.e. sensors/meters). Several attacks indicate that the physical components, such as smart meters, can be compromised in order to misuse private customer data or manipulate meter readings [3].

To ensure the reliability of such a system, the following system monitoring procedure is being used. Meters (sensors) are placed at different (critical) points of the system and the status of the system can be computed/predicted to make sure that the system is in a secure state. Example readings from these meters include bus voltages, bus power injections, and branch power flows [4]. The readings are transmitted from the meters to the SCADA system and the state of the system will be estimated (this process is called "state estimation"). In the computation of the state estimation, the electricity flows in the smart grid are needed to be modeled. There are two approaches: Alternating Current (AC) model and Direct Current (DC) model. The AC model is more realistic and the flow is usually modeled by a set of *nonlinear* equations while the DC model is a simplified model to approximate the AC model. The DC model is not as accurate as the AC model and the flow is only modeled by linear equations. The state of the system (i.e., the output of the state estimation) is usually represented by a vector of state variables (e.g. voltage

* Manuscript received March 30, 2015; revised August 21, 2015.
Corresponding author. Tel.: +852 69063778; *E-mail address*: jxwang@cs.hku.hk.
doi: 10.12720/sgce.4.3.169-176

magnitudes and angles for different buses). The values of these state variables are used to control or adjust the smart grid components.

The bad news is that existing hacking techniques are able to compromise meters with malicious attacks. In view of this, there exist methods to detect whether the readings have been tampered (or are incorrect due to other reasons). These methods are referred as "bad data detection methods (algorithms)" [5]. Most, if not all, of these methods rely on the same principle: if the readings (measurements sent back from the meters) are bad (e.g. being tampered), the difference between these observed readings and the computed readings based on the estimated state variables. This difference is called "residual" and this observation is referred as the "residual principle".

Recently, a new class of man-in-the-middle attacks, namely *false data injection attacks* (FDIAs) was first proposed in [6]. They successfully showed that FDIAs could bypass existing bad data detection algorithms for the DC power flow model. Such an attack, if successful, would mean a big loss to the system [7]. For example, [7] illustrated that for the IEEE 14-bus system, if the output of the generator on one bus was modified and this attack lasted for one week, it would bring more than 4.7 million dollars benefits to the generation company.

While FDIAs were widely explored in DC model [6], the proposed adversary models could not be applied to AC power flow model [8]. Paper works towards constructing FDIAs in AC power flow model were very few [9]-[11]. [9], [10] concentrated on how many and which measurement should be tampered in the AC model with the knowledge of **system states**. These system states were usually stored in the secure part of the SCADA system and were difficult to access (even for insiders). [11] followed the work in [9] and proposed a feasible approach to obtain those system states. Their analysis can only cover some of the buses which they called "injection-bus", but not all. So up to our best knowledge, there are no research results that are able to give an attack to any buses. This research paper provides such an attack.

The difficulty for constructing stealthy errors in AC model lied on the complexity of the set of nonlinear equations. It is not easy to construct a set of tampered readings to satisfy the equations so that it can bypass the bad data detection algorithm. Also, for AC model, the number of measurements is also more than that of DC model, which increases the difficulty of the problem.

The **main contribution** of this paper is to present a simple strategy to launch FDIA against nonlinear state estimation from the attacker's perspective. This strategy can be applied to any types of buses without the knowledge of system states. One theorem is introduced to show that it is likely to find such an attack vector when satisfying a simple rule. Two realistic attack goals are considered: *random false data injection attacks*, in which the attacker wants to inject any attack vectors as long as leading some wrong state variables in AC power flow model and *specific false data injection attacks*, in which the attacker wants to inject specific error into state variables in AC power flow model. This paper then proposes a procedure to generate such attack and illustrates that it is possible to construct attack vectors against nonlinear systems through simulations on several IEEE test systems (IEEE 14-bus, 30-bus, and 118-bus).

The rest of this paper is organized as follows. Some preliminaries of nonlinear state estimation in a smart grid system are given in Section 2. In Section 3, models of launching FDIAs in nonlinear system are introduced. Section 4 presents the evaluations on the proposed attacks and Section 5 concludes the paper.

2. Nonlinear State Estimation

Consider a set of measurements given by the vector $z = h(x) + e$, where x is state vector, $h(x)$ is a function vector relating z to x and $e = [e_1, e_2, ..., e_m]^T$ is the vector of measurement errors. In an AC power flow model, there are $2l-1$ elements in a state vector, which can be represented as

$$x = [\theta_2, \theta_3, ..., \theta_l, \mathrm{V}_1, \mathrm{V}_2, ..., \mathrm{V}_l]^T \quad (1)$$

where θ_i, V_i is voltage angle and voltage magnitude at bus i .Without loss of generality, bus 1 is chosen as the reference $(\theta_1 = 0)$. Furthermore, measurements include real/reactive power injections and real/reactive power flows. More details about measurements can be found in [4].

When given measurement vector z , state variables are often estimated by weighted least-square criterion (WLS), maximum likelihood criterion and minimum variance criterion. These criterions are the most popular methods when dealing with state estimation problem, thus are used in this paper. The WLS estimator is used to minimize the following objective function:

$$J(x) = \sum_{i=1}^{m} (\mathrm{z}_i - \mathrm{h}_i(\mathrm{x}))^2 \Big/ R_{ii} = [\mathrm{z} - \mathrm{h}(\mathrm{x})]^T R^{-1} [\mathrm{z} - \mathrm{h}(\mathrm{x})] \tag{2}$$

where:

(1) $E[e_i] = 0$,where $i = 1, 2, ..., m$;

(2) Measurement errors are independent (i.e. $E[e_i e_j] = 0$);

(3) $R = E[e \cdot e^T] = diag\{\mathrm{R}_{11}, \mathrm{R}_{22,} ..., \mathrm{R}_{nn}\}$ and R_{ii} is the variance of the error in measurement i .

2.1. Bad data detection(BDD)

State variables in control center will be re-estimated when the system is injected by either minor physical errors or malicious attacks. Most BDD programs use "residual principles" to detect the presence of bad measurements. Upon detection of bad data in smart meters, the identification can be accomplished by further processing residuals. Measurement residuals (differences between observed measurements and estimated measurements) can be represented as,

$$r = z - h(\hat{\mathrm{x}}) \tag{3}$$

Mostly, χ^2 Test is used to test whether there exists bad measurements, $J(x) < \chi^2_{(m-n),(1-\alpha)}$, where $\chi^2_{(m-n),(1-\alpha)}$ denotes the value in χ^2 distribution table with a significance level α and the degree of freedom $v = m - n$.

3. False Data Injection Attacks in AC Model

Since intruding the control center is quite difficult, system states (x) cannot be easily obtained in reality, the assumptions in the smart grid environment are summarized as follows:

- Control center cannot be read or falsified by anyone, including system operators;
- Attacker needs to know the topology of the system;
- Attacker only has resources to intrude (read/modify) at most f meters among all meters (knowledge about complete measurement information is not necessary).

It needs to be pointed out that in previous works [9], [10], which constructing FDIAs in nonlinear systems, do pose strong requirements for the attackers. They require the attackers to know the topology of the targeted system. Moreover, the attackers need to get the knowledge of the system states, which is in general not easy to obtain, even for insiders. Notwithstanding, it is important for security researchers to derive one kind of attack without the knowledge of system states, which can inject errors on any buses in nonlinear system. The rest of this section first gives basic principles on adversary models in nonlinear systems. Then two kinds of attacks are addressed: random false data injection attacks and specific false data injection attacks. Both attacks are under the realistic attack scenarios that the attacker is limited to modify any f meters. The first attack is to generate an attack vector without considering the impacts on estimated state variables (system states) in the control center. The whole system may be disordered when

launching this kind of attack. The second kind of attack is more focused and it tries to generate specific errors on targeted state variables. In this case, the attacker does not need to concern if his attack impacts other state variables when attacking the chosen one(s).

3.1. Basic principle

It is noted that there are m measurements $(z_1, z_2, ... z_m)^T$ and n state variables $(x_1, x_2, ..., x_n)^T$ in a smart grid system. The relationship characterized between z_i and x is the function $h_i(x)$, as is discussed in Section 2. Let $z_a = z + a$ be the measurements after attacks, where z is the current measurements and a is referred as the stealthy attacks [12]. The L_2 norm of the measurement residual after an attack, can be represented by

$$r_a = \left\| z_a - h(\hat{x}_{bad}) \right\| = \left\| z + a - h(\hat{x}_{bad}) \right\| \tag{4}$$

where $h(\hat{x}_{bad})$ is denoted as the vector of estimated state variables obtained from z_a .

As discussed above, BDD computes the difference between z_a and $h(\hat{x}_{bad})$. Theorem 1 shows a simple criterion that makes z_a bypass BDD based on residual principle when all measurement information can be collected by the attacker. In details, the attack vector a can be computed as $a = a_0 - r_0$, where a_0 is an arbitrary vector and r_0 is its residual. In other words, there exists a way of calculating an attack vector that can bypass the detection quite easily.

Theorem 1: Assume that the meter errors are very small (in the parameters given by IEEE test systems, it is about 10^{-4}), there always exists a stealthy attack a that can bypass the bad data detection scheme without detected when there exists a vector a_0 , which can make the nonlinear system observable.

Proof: When there exists a malicious vector a_0 that can lead to an estimation of state estimation in the nonlinear system, it is easy to compute the system residual r_0 by Equations (3). Based on the assumption that the meter errors are very small, we can have

$$0 = z + a_0 - r_0 - h(\hat{x}_0) \tag{5}$$

where $h(\hat{x}_0)$ is the state variables estimated by $z + a_0 - r_0$.

Considering if an attack $a = a_0 - r_0$, the measurement residual r_a (after attack a) can be described as,

$$r_a = z + a_0 - r_0 - h(\hat{x}_0) \tag{6}$$

Since observability is defined as the ability to uniquely estimate the system states using the given measurements [13], a will have a unique vector of state variables (denoted as $\hat{x}_0$). That is, $r_a = 0$. The attack $a = a_0 - r_0$ can bypass the bad data detection scheme. Therefore, the proof is complete.

3.2. Random false data injection attack

In a random FDIA, the attacker intends to find any attack vector a as long as it can result in a wrong estimation of state variables [6]. As discussed earlier, the attacker can get the knowledge of system topology $h(\cdot)$. When considering the network parameters are time invariant, it is feasible to perform the process of constructing random FDIAs based on THEOREM 1. Assume that the attacker can read/modify at most any f meters in a smart grid system. Let $z = (z_{i_1}, ..., z_{i_f})^T$ and $z_a = (z_{a_{i1}}, ..., z_{a_{if}})^T$. And let $count(z_a - z)$ denotes the number of meters need to be modified in set S_p , where S_p is the meter set

includes all critical meters [14] and at least one meter exists in every critical k-tuple within the system.

Algorithm 1 is the pseudocode of constructing random false data injection attacks on behalf of an attacker. The input of this algorithm is the topology information (i.e. admittance matrixes). The output of this algorithm is to return an attack vector (a). Step 3-18, it tests whether there exists a solution x_0^k based on z and $h(\cdot)$, where k is the iteration index. The iteration index k is closely based on a_0 since z is fixed. When considering Step 16, if $count(a) < f$, the attack vector does exist. Specifically, in each iteration, the measurement function $h(x_0^k)$ and measurement Jacobian $\mathrm{H}_{x=x_0^k}$ are calculated based on equations of different measurement types [4]. Furthermore, gain matrix $G(x_0^i)$ can be computed as:

$$G(x_0^i) = \mathrm{H}_{x=x_0^k} R^{-1} \mathrm{H}_{x=x_0^k} \tag{7}$$

Algorithm 1 Random FDIA of Nonlinear SE

Input:

Admittance matrixes $h(\cdot)$;

A set of current measurements $\{\mathrm{z}_i\}$;

Number of meters that can be read/modified, f.

Output:

Random false data injection attack z_a.

1: Initialize a random nonzero attack vector $(\mathrm{a}_0)_{m\times 1}$;
2: Initialize $x_0^1 = (0,0,...0,1,1,...,1)^T$;
3: **for** $i = 1{:}100$ **do**
4: Compute $g(\mathrm{x}_0^i)$ based on $g(x) = \partial J(x)/\partial x = -[\partial h(x)/\partial x]^T R^{-1}[\mathrm{z}-\mathrm{h}(x)]$;
5: Compute $G(\mathrm{x}_0^i) = \partial g(\mathrm{x})/\partial \mathrm{x}$;
6: **if** $G(\mathrm{x}_0^i)$ is positive definite && $i < 100$ **then**
7: Compute Δx_0^i by $G(x_0^i)\Delta x_0^i = [\partial h(x)/\partial x]^T R^{-1}[\mathrm{z}-\mathrm{h}(x)]|_{x=x_0^i}$;
8: **if** $\Delta x_0^i < \varepsilon$ then
9: $a = h((\mathrm{H}^{iT}\mathrm{R}^{-1}\mathrm{H}^i)^{-1}\mathrm{H}^{iT}\mathrm{R}^{-1}(\mathrm{z}+\mathrm{a}_0)) - \mathrm{z}$;
10: Go to Step 16;
11: **end if**
12: **else**
13: Go to Step 1;
14: **end if**
15: **end for**
16: **if** $count(a) < f$; **then**
17: return a;
18: **end if**

Measurements can be modified by intruding the smart meters. By launching such attacks, arbitrary or specific errors (c) can be successfully injected on state variables (in control center).

3.3. Specific false data injection attack

The specific FDIAs are the attacks that can generate specific errors on state variables without being

detected. As is discussed earlier in this paper, the attacker does not need to consider the impacts on other state variables when attacking the targeted ones. To construct an attack vector with specific errors on x, the attacker needs to find a p-sparse vector $x = x^k$, which satisfies

$$(H^{kT}R^{-1}H^k)x^k = H^{kT}R^{-1}(z + a_0) \tag{8}$$

Noted that z is the current measurement vector and a_0 is a non-zero random selected attack vector. Equation (8) can be reformulated as a NP-Complete problem [15]: The computation of non-zero elements of $(\hat{x}^k - \hat{x})$ satisfying $Ax^k = b$ are at most q.

Note that attacker cannot obtain state variables by accessing the control center. This paper gives a heuristic method to construct a set of attack vectors with their corresponding estimated state variables. The attacker can then pick up ideal attacks by using the least smart meters (when injecting specific errors c onto state variables). If there are multiple attacks that can fulfill the requirements above, the attacker can select a vector a with the smallest number of modified meters. This enables the attacker to inject an attack with meters as few as possible.

4. Experimental Results

In this section, the proposed FDIAs are validated through experiments based on IEEE test systems, including 14-bus, 30-bus and 118-bus systems. The dataset used in this section can be found in [16]. This paper primarily focuses on the feasibility of generating FDIAs against AC power flow model as well as the efforts needed for a successful attack. The information of state variables and measurements within various IEEE test systems is given in Table 1 and τ is set to be 2.0.

Table 1. Number of state variables and measurements in the IEEE test systems

IEEE Bus System	14-bus	30-bus	118-bus
No. of voltage measurements	2	2	4
No. of real power inject measurements	7	15	39
No. of reactive power inject measurements	7	15	39
No. of real power flow measurements	8	23	111
No. of reactive power flow measurements	8	23	111
No. of total measurements	32	78	304
No. of state variables	27	59	235

4.1. Time and probability

The performance of probability of constructing random FDIAs is first evaluated when f is not fixed. The experiments are performed as follows. Let the parameter f varies from 1 to maximum number of meters in each system. For each f, randomly choose f meters to attempt an attack vector construction. Repeat this process *1000* times and estimate the success probability p_f = *# successful trials/1000*.

Fig. 1(a) shows the relationship between the probability of finding proposed attacks and the percentage of modified meters. It can be seen that the probability increases as the number of modified measurements increases. Attack can be constructed with the probability close to *100%* when f is large. For example, probability is *100%* when f is set to *59.38%, 76.92%, 80.26%* of the whole measurements for IEEE 14-bus, 30-bus and 118-bus respectively. For example, the attacker can always find a random FDIA in IEEE 14-bus system, when he can modify at least *19* smart meters.

As is shown in Fig. 1(b), constructing specific FDIA is more challenging for the attacker. The aim of specific FDIAs is to inject specific errors on state variables. Monte Carlo method is used to perform the experiments. These experiment results demonstrate that FDIAs in nonlinear systems can be systematically constructed by algorithms proposed in this paper. Also the results show that it is possible and practical to

launch FDIAs in nonlinear system with the knowledge of system's topology but without the knowledge of system states.

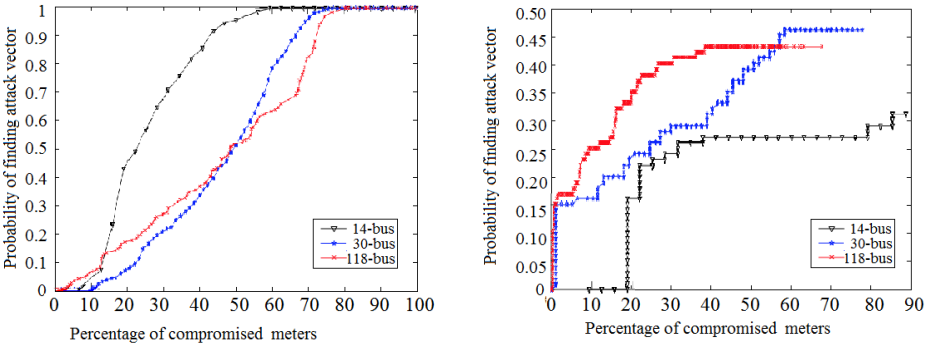

Fig. 1. Probability of finding an attack: (a) random FDIAs and (b) specific FDIAs.

Table 2. Time and Probability on Random FDIAs

IEEE Bus System	Timing Cost(s)	Probability
14-bus	0.164-1.513	47.43%
30-bus	0.395-2.207	55.40%
118-bus	2.946-6.955	61.73%

When f is set to be $f = 0.3\times$ *(# of meters)*, based on evaluation objectives, two indices are analyzed: *timing cost* that constructs an attack vector and *probability* that the attack can be successfully constructed among *1000* trials for each test system, which is shown in Table 2. When the attack is feasible, the speed for generating such an attack is fairly quick. Moreover, the time is mainly spent on Cholesky factorization. Despite the fact that the topology of nonlinear system is more complex, the execution time of our method (*2946-6955* ms) is comparable to that of [8] (*0.55-8549.6* ms).

4.2. Impacts on state variables

The impacts after random FDIAs are analyzed. A good attack is defined as successful injecting large errors on x.

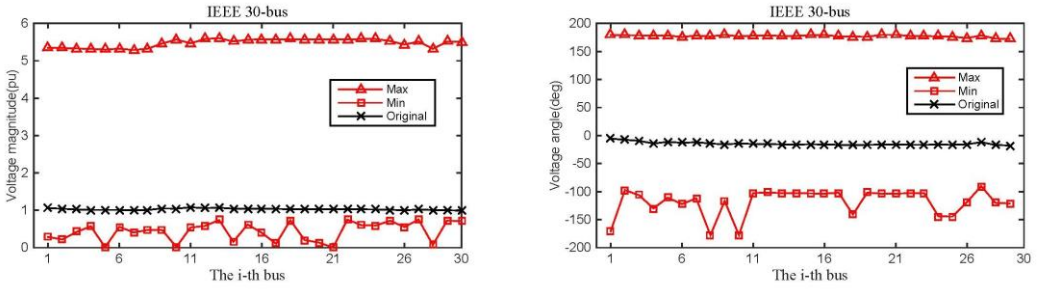

Fig. 2. State variables (voltage magnitudes and angles) range after attacks in IEEE 30-bus system.

Fig. 2. shows the maximum and minimum values of voltage magnitudes and angles of all buses among *1000* times attacked by random FDIA in IEEE-30 bus system. From analyzing our results, FDIA can inject errors at most 5 times larger than original estimated magnitudes (for example, the range of voltage magnitude at bus 11 is $[0.5411, 5.4699]$ and the original estimated voltage magnitude at bus 11 is 1.0820), and can inject errors that change the angle to nearly 180. Since these results are based on *1000*

trails, reinforce these conclusions are very convincing.

5. Conclusion

This paper proposes a false data injection attack against nonlinear state estimation in a cyber-adversarial system (i.e. smart grid). The innovative idea of this algorithm is that it does not need the knowledge of system state and can inject errors into an AC power flow system without being detected. This paper strengthens the attacks to cyber-adversarial systems, and therefore research on protections in with cyber-adversarial systems will be in a greater need in near future. Furthermore, this work focuses on the smart grid environment, the general application and infrastructure work can be extended to other domains, such as aviation cyber-physical systems or smart micro-grids.

Acknowledgements

The work described in this paper was partially supported by the HKU Seed Funding's for Applied Research 201409160030, and HKU Seed Funding's for Basic Res 201311159149 and 201411159122.

References

[1] Bush PGW. Leadership Under Chal-lenge: Information Technology R & D in a Competitive World, August 2007.
[2] Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 2012; 100(1): 210-224.
[3] Widl E, Palensky P, Siano P, Rehtanz C. Guest editorial: modeling, simulation, and application of cyber-physical energy systems. *IEEE Transactions on Industrial Informatics*, 2014; 10(4):2244–2246.
[4] Abur A, Gomez Exposito A. *Power System State Estimation: Theory and Implementation*. CRC Press; 2004.
[5] Chen J, Abur A. Placement of pmus to enable bad data detection in state estimation. *IEEE Transactions on Power Systems*, 2006; 21(4):1608–1615.
[6] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 2011; 14(1):13.
[7] Liu T, Gu Y, Wang D, Gui YH, Guan XH. A novel method to detect bad data injection attack in smart grid. In: *Proc. Proceedings IEEE INFOCOM*, 2013:3423–3428.
[8] Jia LY, Thomas RJ, Tong L. On the nonlinearity effects on malicious data attack on power system. In: *Proc. IEEE Power and Energy Society General Meeting*, 2012:1–8.
[9] Hug G, Giampapa JA. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on Smart Grid*, 2012; 3(3):1362–1370.
[10] Rahman M, Mohsenian-Rad H, *et al*. False data injection attacks against nonlinear state estimation in smart power grids. In: *Proc. Power and Energy Society General Meeting*, 2013:1–5.
[11] Liang JW, Kosut O, Sankar L. Cyber attacks on ac state estimation: unobservability and physi-cal consequences. In: *Proc. PES General Meeting— Conference & Exposition*, 2014:1–5.
[12] Wang S, Ren W. Stealthy false data injection attacks against state estimation in power systems: switching network topologies. In: *Proc. American Control Conference*, 2014:1572-1577.
[13] Expsito AG, Abur A. Generalized observability analysis and measurement classification. In: *Proc. 20th International Conference on Power Industry Computer Applications*, 1997:97-103.
[14] Clements KA, Davis PW. Multiple bad data detectability and identifiability: a geometric approach. *IEEE Transactions on Power Delivery*, 1986; 1(3):355-360.
[15] Michael RG, David SJ. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. San Francisco: WH Freeman & Co.; 1979.
[16] Christie RD. Power systems test case archive. Electrical Engineering dept., University of Washington; 2000.