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.