Detecting False Data Injection Attacks in AC State Estimation

Gu Chaojun, *Student Member, IEEE*, Panida Jirutitijaroen, *Senior Member, IEEE*, and Mehul Motani, *Member, IEEE*

***Abstract*—Estimating power system states accurately is crucial to the reliable operation of power grids. Traditional weighted least square (WLS) state estimation methods face the rising threat of cyber-attacks, such as false data injection attacks, which can pass the bad data detection process in WLS state estimation. In this paper, we propose a new detection method to detect false data injection attacks by tracking the dynamics of measurement variations. The Kullback–Leibler distance (KLD) is used to calculate the distance between two probability distributions derived from measurement variations. When false data are injected into the power systems, the probability distributions of the measurement variations will deviate from the historical data, thus leading to a larger KLD. The proposed method is tested on IEEE 14 bus system using load data from the New York independent system operator with different attack scenarios. We have also tested our method on false data injection attacks that replace current measurement data with historical measurement data. Test results show that the proposed approach can accurately detect most of the attacks.**

***Index Terms*—False data injection, Kullback–Leibler distance (KLD), state estimation.**

I. Introduction

State ESTIMATION is an important function in power grid energy management system (EMS) [1]. To perform the state estimation, the power system control center gathers measurement data from remote terminal units (RTUs). These data generally include real and reactive power injections, real and reactive power flow in the transmission lines, and voltage magnitude at generator buses. The measurement data are converted to system state (bus phase angle and voltage magnitude) using dc state estimation or ac state estimation.

Accurately estimating system states is important because the system state information from the state estimation is used in other functions of EMS, such as transmission stability analysis, load shedding, etc. The measurement data gathered from the RTUs may contain small random measurement errors, which can be caused by noise or inaccuracy of measurement equipment [2], [3]. These small measurement errors are generally independent from each other. Weighted least square state estimation can estimate the system state accurately when the variances of these small measurement errors are known.

Apart from the small measurement errors caused by the noise and inaccuracy of measurement, it is possible that measurement data contain larger errors caused by biased meters or telecommunication failure [2]. These larger measurement errors are considered independent and can be detected using residual analysis of traditional bad data detection method [2], [3].

In recent years, cyber-attacks are emerging threats to the secure operation of power systems [4]–[6]. It is found in [7] that a new type of cyber-attack called false data injection attack can pass the traditional bad data detection in power system state estimation. A successful false data injection attack was initially illustrated by dc state estimation which relies on linear measurement function $\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}$ where $\mathbf{z}$, $\mathbf{x}$, and $\mathbf{e}$ are the vectors of measurements, system states, and errors, respectively. A manipulated measurement vector $\mathbf{z}_{\text{bad}} = \mathbf{H}\mathbf{x}_{\text{bad}} + \mathbf{e}$ will not be detected by the traditional bad data detection process because the measurement residuals with false data injection attacks are the same as the measurement residuals with no false data injection attacks. Results from [8] show that an attack using a dc model may trigger the bad data detector in an ac state estimation, but attackers can still inject false data into the ac state estimation. Both dc state estimation and ac state estimation are prone to the false data injection attacks.

Several methods have been proposed to alleviate false data injection attacks. These methods can be divided into two categories: 1) protection-based; and 2) detection-based [9]. The protection-based methods [9]–[13] which defend against the false data injection attacks by protecting certain sensors have two drawbacks. The first drawback is the decrease of redundancy. This is because only the protected measurements are trusted and used. The second drawback is that the protection may not be secure all of the time. The state estimation would be in danger if attackers can penetrate the protection and manipulate the measurements. The detection-based methods [14]–[16], by analyzing the raw measurements, are able to detect those abnormal ones that do not fit the distribution of historical measurements. However, these methods do not have the ability to detect false data that fits the distribution of historical measurements, such as previous measurement data.

In [17]–[19], there are many time series anomaly detection methods. Most of these methods have specific applications and have not been used in power system analysis. In this

Manuscript received May 16, 2014; revised September 21, 2014; accepted December 28, 2014. Date of publication February 6, 2015; date of current version August 19, 2015. Paper no. TSG-00463-2014.

The authors are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore (e-mail: a0040186@nus.edu.sg; elejp@nus.edu.sg; elemm@nus.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2015.2388545

paper, a new detection-based method is proposed to address the limitations of the existing methods. The key idea of the proposed method is to track the dynamics of the measurements by calculating distance indices between adjacent steps. Distance indices can be calculated from historical measurements using the Kullback-Leibler distance (KLD) [20]. A threshold of the distance index, calculated from historical data, will be used to detect potential false data injection attacks. The distance index between the current time step k and the previous step $k-1$ should fall within the threshold when there are no false data injection attacks. If the distance index is significantly different from historical distance values, the newly received measurements are likely to be manipulated.

The remaining parts of this paper are organized as follows. Section II explains the background of state estimation, bad data detection, and false data injection attacks. Section III discusses the existing methods and our proposed method to detect false data injection attacks. Section IV explains how to build the test system and calculate the distance index. Section V shows the test results of different attacking scenarios. The conclusion is drawn in Section VI.

II. Background

Based on the measurement function that models the measurement and system state, there are two ways to perform state estimation: 1) dc state estimation; and 2) ac state estimation. It is possible to inject false data in both dc and ac state estimation.

A. DC State Estimation

DC state estimation is based on the following linear measurement function:

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

where $\mathbf{z} \in \mathbb{R}^{m\times 1}$ is the measurement vector that contains m measurements. These m measurements include real power injection at buses and real power flow in transmission lines. $\mathbf{x} \in \mathbb{R}^{n\times 1}$ is the system state vector. In dc state estimation, $\mathbf{x}$ consists of phase angles at all the buses except the slack bus where the phase angle is set to be zero. $\mathbf{H} \in \mathbb{R}^{m\times n}$ is the linear measurement function. $\mathbf{H}$ is determined according to the physical structure of the power grid. $\mathbf{e} \in \mathbb{R}^{m\times 1}$ is a vector of measurement errors. $\mathbf{R}$ is the diagonal matrix representing the covariance matrix of the measurement errors.

DC state estimation assumes that bus voltage magnitudes are all equal to one. All shunt elements and branch resistances are negligible. The real power flow between buses i and j is given by $P_{ij} = (\theta_i - \theta_j)/x_ij$, where x_{ij} is the reactance of the branch between buses i and j, θ_i and θ_j are the phase angles at bus i and j, respectively.

The estimated system state $\hat{\mathbf{x}}$ from dc state estimation is calculated by minimizing the objective function

$$F(\mathbf{x}) = (\mathbf{z} - \mathbf{H}\mathbf{x})^T\mathbf{R}^{-1}(\mathbf{z} - \mathbf{H}\mathbf{x}). \tag{2}$$

The $\hat{\mathbf{x}}$ that minimizes (2) is given by

$$\hat{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z}. \tag{3}$$

B. Bad Data Detection and False Data Injection Attacks

Traditional bad data detection is based on the residual analysis of $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$. If the measurement errors are independent and follow normal distribution, then the residual $||r||$ follow a chi-square distribution. To detect the existence of bad data, the residual is compared with a threshold value calculated with a certain confidence interval. However, this way of detecting bad data faces a threat from an newly discovered attack.

According to [7], an attacker can pass the bad data detection test if the attacker has knowledge of the system structure ($\mathbf{H}$) and can manipulate multiple measurements at the same time. Mathematically, the manipulated measurement $\mathbf{z}_{\text{bad}} = \mathbf{z} + \mathbf{a}$, can pass the bad data detection test if $\mathbf{a} = \mathbf{H}\mathbf{c}$ where $\mathbf{a}$ is the malicious data added to the original measurements, and $\mathbf{c}$ is the injected error on the system state. After the false data injection, dc state estimation will get an erroneous system state $\hat{\mathbf{x}}_{\text{bad}} = \hat{\mathbf{x}} + \mathbf{c}$ from the manipulated measurement data.

False data injection attacks can pass the traditional bad data detection tests because the residual from the false data injection attacks, $\mathbf{r}_{\text{bad}} = \mathbf{z}_{\text{bad}} - \mathbf{H}\hat{\mathbf{x}}_{\text{bad}} = \mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c}) = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} = \mathbf{r}$. This means that the measurement residual will not increase after the false data have been injected to the system. Thus traditional bad data detection methods cannot detect the false data injection attacks.

C. AC State Estimation False Data Injection

Different from dc state estimation, ac state estimation uses a nonlinear function between measurements and system state. The nonlinear measurement function is shown

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

where $\mathbf{h}()$ is a nonlinear function between the measurement vector $\mathbf{z}$ and the system state vector $\mathbf{x}$.

In ac state estimation, system state variables include not only bus phase angles, but also bus voltage magnitudes. Reference [8] expands the dc false data injection into ac false data injection. In that research, it is found that in order to pass the ac state estimation bad data detection, the attacker needs to know the value of the system state and the system configuration. In ac state estimation, the false data added to the measurement $\mathbf{a}$ can pass bad data detection if $\mathbf{a} = \mathbf{h}(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{h}(\hat{\mathbf{x}})$.

In this paper, we focus our analysis on false data injection attacks on ac state estimation. The proposed method is also applicable for dc state estimation. When the attacker wants to inject false data into ac state estimation, there are generally two targets. One is to manipulate certain system state variables; another is to manipulate certain measurements.

1) Targeting System State Variables: In ac state estimation, there are two types of state variables: 1) bus phase angle (θ); and 2) bus voltage magnitude (V). If the attacker targets a specific state variable, all the measurements that depend on this state variable will be affected. The measurement values are related to the system state by the following equations [2].

1) Real and reactive power injection at bus i

$$P_i = V_i \sum_{j\in\Omega_i} V_j\left(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}\right) \tag{5}$$

$$Q_i = V_i \sum_{j \in \Omega_i} V_j \left(G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}\right). \quad (6)$$

2) Real and reactive power flow from bus i to bus j

$$P_{ij} = V_i^2 \left(g_{si} + g_{ij}\right) - V_i V_j \left(g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij}\right) \quad (7)$$

$$Q_{ij} = -V_i^2 \left(b_{si} + b_{ij}\right) - V_i V_j \left(g_{ij} \sin\theta_{ij} - b_{ij} \cos\theta_{ij}\right) \quad (8)$$

where

V_i	voltage at bus i;
θ_i	phase angle at bus i;
θ_{ij}	$\theta_i - \theta_j$;
$G_{ij} + jB_{ij}$	line admittance between bus i and j;
$g_{si} + jb_{si}$	admittance of the shunt branch at bus i;
Ω_i	set of buses connected to bus i.

From (5)–(8), it is clear that to target one state variable, for example V_i, the measurements that need to be manipulated are P_i, Q_i, P_{ij}, and Q_{ij} where $j \in \Omega_i$. If the attacker intends to change multiple states at the same time, then the attacker needs to manipulate even more measurements. For example, if the attacker wants to change V_k where $k \in \mathbf{U}_a$ is a set of bus numbers, then the measurements that need to be manipulated are P_k, Q_k, P_{kj}, and Q_{kj} where $k \in \mathbf{U}_a$, $j \in \Omega_k$.

2) Targeting Certain Measurements: A specific measurement in the state estimation is determined by system structure and at least two system variables. To change a specific measurement, an attacker needs to change at least one state variable that controls the targeted measurement. To pass the bad data detection, an attacker needs to manipulate all the measurements that are affected by the manipulated state variable.

III. Methodology

A. Current Defending Methods

The existing countermeasures can be categorized into: protection-based approaches and detection-based approaches [9].

1) Protection-Based Approaches: References [9]–[13] proposed to prevent false data injection attacks by protecting measurements from certain sensors. It is possible to calculate the minimal set of measurements that needs to be protected for both dc and ac state estimation. However, there are two drawbacks of the protection-based approach. The first drawback is that measurement redundancy drops since only the protected measurements can be trusted. The second drawback is that protecting of measurement may not work 100% of the time. If the attacker is capable of penetrating the protection, then state estimation is still in great danger.

2) Detection-Based Approaches: Another type of countermeasure proposed by [14]–[16] is to detect potential false data injection attacks using Bayesian framework. The Bayesian framework assumes that the vector of system states is a random vector with Gaussian distribution $\mathcal{N}(\boldsymbol{\mu}_x, \boldsymbol{\Sigma}_x)$. The distribution is estimated from the historical data. The estimated distribution is used as a reference in the hypothesis test for the new state. This method will capture the attacks that lead to extreme abnormal system states. The drawback of Bayesian framework method is that it cannot detect attacks that inject measurement data that fit the distribution of historical data. For example, if an attacker replaces the current measurement data with previous measurement data which fall in the distribution, the Bayesian-based method cannot detect the attack.

In this paper, we propose a new method that can overcome the above drawbacks.

B. Proposed Method

The proposed method detects false data injection attacks by tracking the dynamics of the measurement data. To quantify the measurement variation, we use two distance indices: 1) absolute distance; and 2) KLD. For both distance indices, there are two probability distribution p and q. The probability distribution q is the distribution of measurement variation from the historical data. p is the distribution of measurement variation between the current time step and the previous time step. When there is no false data injection, the distance index would be relatively small. When false data are injected into the power systems, the distance index will increase. By comparing the distance index of current time step with the historical distance index values, we can determine if false data are injected in to the power systems.

1) Absolute Distance: This is a naive way of comparing the difference between two probability distributions. We call it absolute distance in this paper. The distance is defined as follows:

$$A(p||q) = \sum_x |p(x) - q(x)|. \quad (9)$$

2) KLD: The KLD calculates the difference between two probability distributions $p(x)$ and $q(x)$ [20]. The distance is defined as follows:

$$D(p||q) = \sum_x p(x) \ln \frac{p(x)}{q(x)} \quad (10)$$

$$= E_p \ln \frac{p(X)}{q(X)}. \quad (11)$$

In the above definition, we use the convention that $0 \ln 0/q = 0$ and $p \ln p/0 = \infty$. The KLD is also called the relative entropy. The KLD is not a true distance metric as it is not symmetric ($D(p||q)$ may not be equal to $D(q||p)$), and it does not satisfy a triangle inequality. It is always nonnegative and is zero if and only if $p = q$.

The KLD was introduced by Solomon Kullback and Richard Leibler in 1951. It has been used in many applications. Reference [21] uses the KLD to retrieve texture. In [22], the KLD is used to help improve the audio search. The KLD can even indicate nonstationarity change of neurological signals [23]. In our problem, we use the KLD to detect potential cyber-attacks on power system.

IV. Case Studies

A. Test System

In this section, we discuss how to prepare a test system to test the performance of our proposed method. The test system

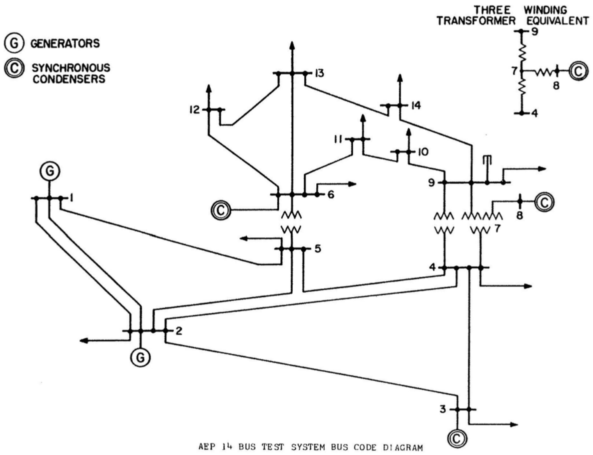
THREE WINDING TRANSFORMER EQUIVALENT
G GENERATORS
C SYNCHRONOUS CONDENSERS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
AEP 14 BUS TEST SYSTEM BUS CODE DIAGRAM

Fig. 1. IEEE 14 bus test system.

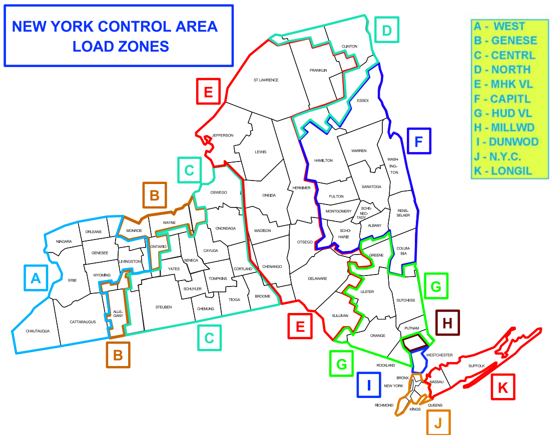

Fig. 2. NYISO map of 11 electric power grid regions in New York State, USA.

used in this paper is based on the IEEE 14 bus system, as shown in Fig. 1.

The load data used in the test system are based on the New York independent system operator (NYISO) from 2012. There are 11 load regions in the NYISO data as shown in Fig. 2. The time interval of the load data is five minutes.

Due to the lack of five minutes system state data, we perform the following procedures to generate the system state data from NYISO load pattern.

1) Link each load bus of IEEE 14 bus system with one region of NYISO using the following matrix:

$$\begin{pmatrix} 2 & 3 & 4 & 5 & 6 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{pmatrix}.$$

The first row of the matrix is the bus number of IEEE 14 bus system. The second row is the corresponding NYISO region number.

2) Normalize the load of NYISO to the initial real and reactive load of the corresponding IEEE 14 bus, so that the test system operates near the initial state of the IEEE 14 bus system. After this step, we will have real and reactive load data for the IEEE 14 bus system. Due to lack of reactive load information, we assume that the system load has a constant power factor so only real power prediction is needed. This assumption can be relaxed if the historical data of reactive power is available.

3) Add up the new real power load. Find the ratio of the new total load to the IEEE 14 bus initial total load. Multiply this ratio to the generations of all the generators. Here, we assume that generations from the generators increase at the same rate as the total load. This assumption can be adjusted according to system operators since the system operators know the generation plan ahead of the time [24].

4) Repeat the previous step for the reactive power.

5) Calculate the system state ($\mathbf{x}$) using power flow analysis.

6) Calculate the system measurement value $\mathbf{z} = \mathbf{h}(\mathbf{x})$, where $\mathbf{h}()$ is the power flow equation derived from the system structure.

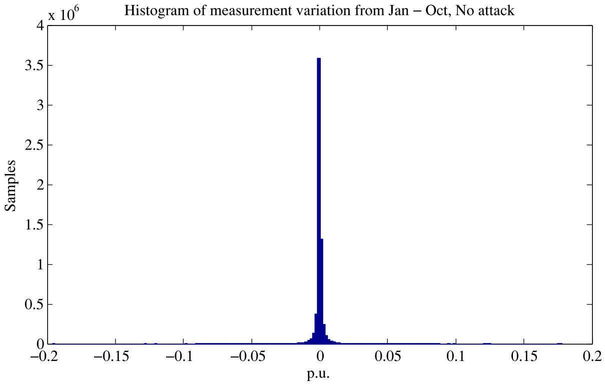

Fig. 3. Histogram of measurement variation from January to October 2012.

B. Simulate False Data Injection Attacks

To test the proposed method, we simulate false data injection attacks by targeting different system state variables. The manipulated system state after the attack is denoted by $\mathbf{x}_{\text{bad}} = \mathbf{x} + \mathbf{c}$. The corresponding measurement for the manipulated system state is $\mathbf{z}_{\text{bad}} = \mathbf{h}(\mathbf{x}_{\text{bad}})$.

For ac state estimation in IEEE 14 bus system, there are 27 state variables (13 bus phase angles and 14 voltage magnitudes). We simulate false data injection attacks on each of these 27 state variables.

C. Measurement Variation

Power systems are considered as quasi-static systems. The power system state changes constantly but slowly. This means that measurements gathered from the RTUs should vary slowly. The measurement data gathered from RTUs at time step k is denoted by $\mathbf{z}(k)$. The measurement variation is defined as $\mathbf{z}(k) - \mathbf{z}(k-1)$. Fig. 3 shows the histogram of measurement variation from January 2012 to October 2012 with no false data injection attacks. From Fig. 3, we can see that most of the measurement variations are small and close to zero. This histogram is converted to probability density function q in (10).

When there are no false data injection attacks, the distributions of measurement variation are similar between different

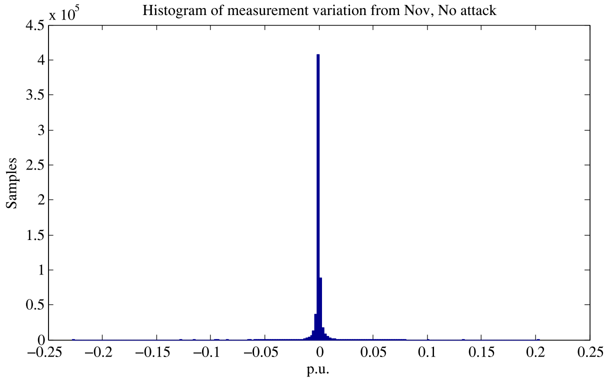

Fig. 4. Histogram of measurement variation in November 2012.

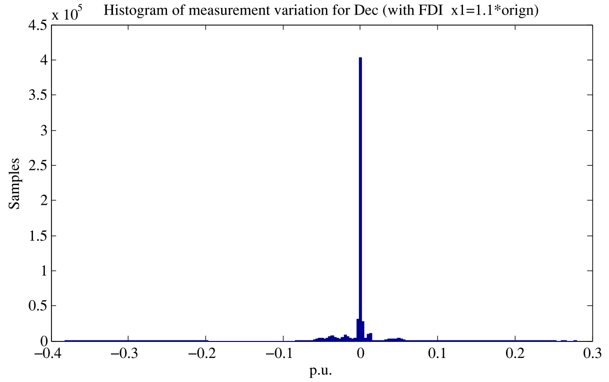

Fig. 5. Histogram of measurement variation with false data injection attacks.

months. Fig. 4 is the histogram of measurement variation in November 2012 with no false data injection attacks. Comparing Fig. 3 with Fig. 4, we can see that two histograms are quite similar.

However, when false data are injected to the power system, the histogram of the measurement variation will be different. To illustrate the impact of false data injection on measurement variation, we simulate 10% incremental attack on the first variable of the system state (θ_2), $\mathbf{c} = (0.1 * \theta_2, 0, \ldots, 0)$. We simulate this attack for each time step of December. Fig. 5 is the histogram of measurement variation $(\mathbf{z}_{\mathrm{bad}}(k) - \mathbf{z}(k-1))$ when false data are injected into the system. From Figs. 4 and 5, we can see that false data injection will affect the distribution of measurement variation.

D. Distance Index

To quantify the difference between two distributions, we test two difference indices. For both indices, there are two probability distributions p and q. In this paper, q is derived from the historical data of measurement variations (Fig. 3). p is derived at each time step. For the IEEE 14 bus system, there are 70 measurements at each time step. It includes real and reactive power injection, real and reactive power flow in the transmission line and voltage magnitude at generator buses. The variation of these 70 measurements at each time step is used to derive p.

1) Absolute Distance: We firstly test absolute distance between p and q using (9).

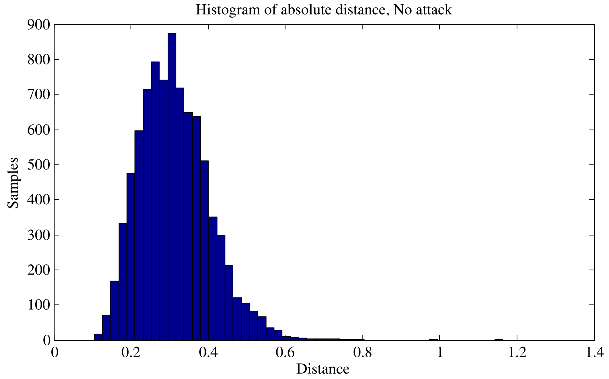

Fig. 6. Histogram of absolute distance on November with no false data injection attacks.

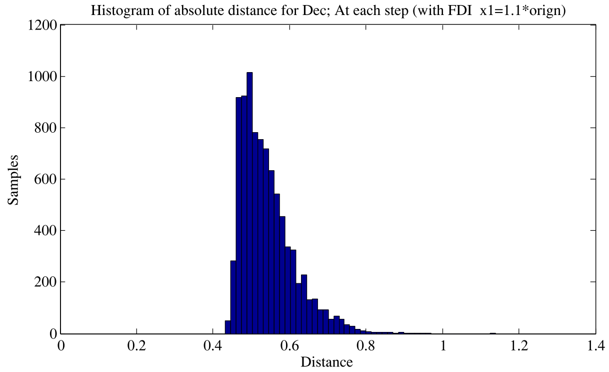

Fig. 7. Histogram of absolute distance on December with false data injection attacks.

Fig. 6 is the histogram of absolute distances for November with no false data injection attacks. The absolute distances range from 0.1 to 0.6.

Fig. 7 is the histogram of absolute distance for December with false data injection attacks. Compared with absolute distance with no attack in Fig. 6, the absolute distances with false data injection attacks are mostly larger. However, there is some overlapping between Figs. 6 and 7 around 0.4 to 0.6. This means that when we get a measurement sample with absolute distance between 0.4 and 0.6, this sample can be from either no attack or with attack. Thus absolute distance is not an ideal candidate to test false data injection attacks.

2) KLD: KLD is calculated based on (10). Fig. 8 is the histogram of KLD for November with no false data injection attacks. The histogram shows that the KLD of most samples in November are less than 0.45. Fig. 9 is the histogram of KLD for December with false data injection attacks. In Fig. 9, KLD of all samples are larger than 0.45. By comparing Fig. 8 with Fig. 9, we can see that false data injection attacks will increase KLD.

Unlike the absolute distance, there is much less overlapping in the histograms with the KLD. To detect false data injection attacks, we set a KLD threshold from the previous data (Fig. 8). This threshold is then compared with every sample during runtime (Fig. 9). If the runtime KLD is larger than the threshold, it is likely that false data have been injected into the system.

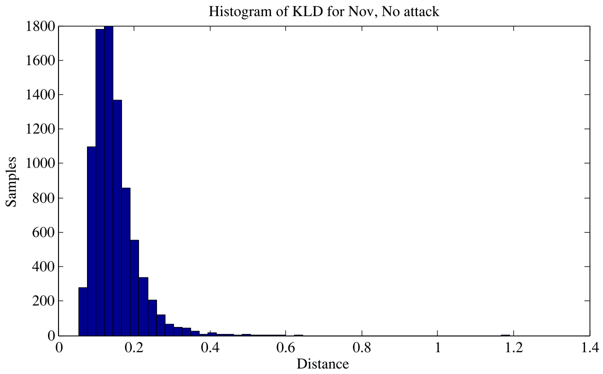

Fig. 8. Histogram of KLD on November with no false data injection attacks.

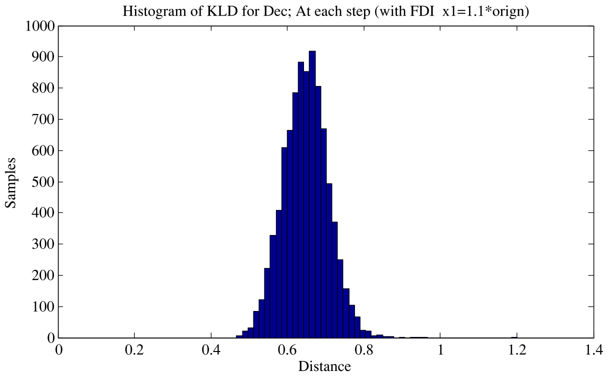

Fig. 9. Histogram of KLD on December with false data injection attacks.

Selecting the proper threshold affects the accuracy of detection. Threshold represents the tolerance of measurement variation for the detection algorithm. When the threshold is set to high, the proposed method will potentially not be able to detect certain attacks. When the threshold is set to low, some true measurement data may be classified as false data.

It is possible to use the maximum historical distance as the threshold. However, the maximum distance may be too large. In Fig. 8, the maximum KLD is 1.19 which is higher than most of the samples in Fig. 9. If we use 1.19 as the threshold, we cannot detect the false data injection attacks. Please note that the extreme large historical distance may be caused by the measurement error in the test system data.

To solve this problem, in this paper, we use a maximum KLD from historical data with certain confidence level. For example, the 99% confidence level means that the threshold value is larger than 99% of the historical data. In Fig. 8, the 99% confidence maximum KLD is 0.35 which is smaller than most of the samples in Fig. 9. This 99% confidence maximum is used as threshold to detect potential false data injection attacks.

V. Results and Discussion

In this section, the proposed method is tested with two different types of false data injection attacks.

1) *Attack on State Variable:* One system variable is targeted and all measurements linked to that system variable are replaced with false data.

TABLE I
Summary of Test Results For Data Injection Attacks

Inject	Org*0.9		Org*0.95		Org*1		Org*1.05		Org*1.1	
	UD	%	UD	%	UD	%	UD	%	UD	%
θ_2	0	0%	118	1%	8848	99%	141	2%	0	0%
θ_3	2004	22%	4894	55%	8848	99%	5004	56%	2885	32%
θ_4	0	0%	0	0%	8848	99%	0	0%	0	0%
θ_5	0	0%	0	0%	8848	99%	0	0%	0	0%
θ_6	0	0%	0	0%	8848	99%	0	0%	0	0%
θ_7	5192	58%	6225	70%	8848	99%	6271	70%	5438	61%
θ_8	8527	96%	8529	96%	8848	99%	8520	95%	8515	95%
θ_9	0	0%	0	0%	8848	99%	0	0%	0	0%
θ_{10}	0	0%	1	0%	8848	99%	3	0%	0	0%
θ_{11}	0	0%	0	0%	8848	99%	1	0%	0	0%
θ_{12}	0	0%	111	1%	8848	99%	175	2%	0	0%
θ_{13}	0	0%	0	0%	8848	99%	0	0%	0	0%
θ_{14}	0	0%	418	5%	8848	99%	634	7%	0	0%
V_1	0	0%	0	0%	8848	99%	0	0%	0	0%
V_2	0	0%	0	0%	8848	99%	0	0%	0	0%
V_3	0	0%	137	2%	8848	99%	179	2%	0	0%
V_4	0	0%	0	0%	8848	99%	0	0%	0	0%
V_5	0	0%	0	0%	8848	99%	0	0%	0	0%
V_6	0	0%	0	0%	8848	99%	0	0%	0	0%
V_7	0	0%	1764	20%	8848	99%	1756	20%	1	0%
V_8	8539	96%	8539	96%	8848	99%	8544	96%	8544	96%
V_9	0	0%	0	0%	8848	99%	0	0%	0	0%
V_{10}	0	0%	0	0%	8848	99%	0	0%	0	0%
V_{11}	0	0%	0	0%	8848	99%	0	0%	0	0%
V_{12}	0	0%	0	0%	8848	99%	0	0%	0	0%
V_{13}	0	0%	0	0%	8848	99%	0	0%	0	0%
V_{14}	0	0%	0	0%	8848	99%	0	0%	0	0%

2) *Attack Using Previous Measurement Data:* The intruder replaces the current measurement data with older measurement data.

A. Attack State Variable

To test the performance of the proposed method, we simulate false data injection attacks on each system state variable. For each attack, one system state variable is decreased or increased by certain percentage of its original value. Table I summarizes the test results.

Each row of Table I represents one system state variable that is targeted. For each targeted state variable, we simulate five injection amounts, which are 90%, 95%, 100%, 105%, and 110% of the original value. Ninety percentage means that the manipulated system state variable is 10% smaller than the true value. Hundred percentage means that there is no attack.

Result for each targeted state variable and injected amount is shown in two formats, UD and %. UD stands for undetected samples. Percentage indicates the percentage of samples that are not detected, which is equal to UD divided by total samples. In the case study, there are 8927 samples for each attacking scenario.

The second and third columns of Table I show that when the manipulated state variable is 90% of the original value, our proposed method can detect most of attack scenarios with no undetected sample. When the manipulated state variable is 95% of its variable, there are slightly more samples that cannot be detected. This is because 95% is closer to the original value than 90%, thus the attacks have smaller impact on the measurements.

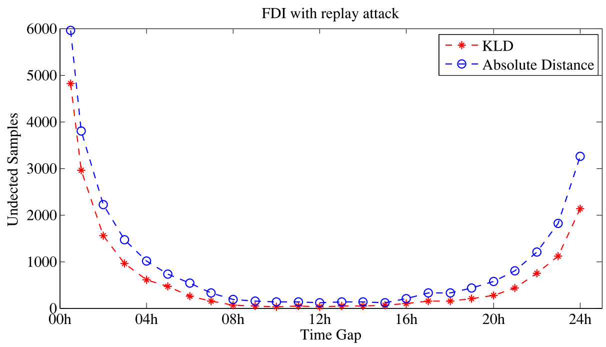

Fig. 10. False data injection attacks with replay attacks. Tested on 8927 samples.

Table I also shows that it is difficult to detect false data injection attacks for certain state variables. In our case study, manipulating state variables at buses 3, 7, and 8 are difficult to detect. This is because these buses have fewer connections to the remaining parts of the grid. Manipulating these state variables affect fewer measurements.

The seventh and eighth columns of Table I are the test results when there is no false data injection attacks. The test results show that our method will classify 99% of these test samples as no attack. This means that our method is not likely to classify a good measurement (no attack) as false data.

B. Attack Using Previous Measurement Data (Replay Attack)

Another type of false data injection attacks is to replace the current measurement data with previous measurement data. $\mathbf{z}_{\text{bad}}(k) = \mathbf{z}(k - \delta)$ where k is the current time step, δ is the time gap. Please note that we are not looking at continuous replay attack where $\mathbf{z}_{\text{bad}}(k - 1) = \mathbf{z}(k - 1 - \delta)$, $\mathbf{z}_{\text{bad}}(k) = \mathbf{z}(k - \delta)$, and $\mathbf{z}_{\text{bad}}(k + 1) = \mathbf{z}(k + 1 - \delta)$. The proposed method is meant to detect injection attack at time step k where there is no attack before time step k.

This type of replay attack does not require the system configuration information as long as the system configuration has not been changed during δ. The manipulated measurements and system states will still fit the distribution of historical records. This makes it is difficult to detect using existing detection methods.

However, our method is based on the variation of the measurement, not the measurement itself. This means if the time gap δ is significant, our method will be able to detect the attack. We have tested our method using different time gaps. The results from the testing are shown in Fig. 10.

The time gaps that have been tested vary from 30 m to 24 h. Fig. 10 shows that the number of undetected samples decreases using KLD when the time gap increases for the first 12 h. After 12 h, the number of undetected samples increases. This phenomenon is caused by the periodicity of the power system. For example, the load at 9 A.M. today is likely to be more similar to the load at 9 A.M. yesterday than 9 P.M. yesterday. This is the reason why the detection is more accurate when δ equals 12 h than 24 h.

The test results also show that when the time gap is small, our method may not be able to detect the attack. However, a smaller time gap means that the impact on the measurement is also smaller. Comparing KLD approach and absolute distance approach, we can see that the KLD approach outperforms the absolute distance approach.

VI. Conclusion

False data injection attacks threaten the secure operation of power grids. In this paper, a new detection method is proposed to detect false data injection attacks. The detection method is based on the KLD which calculates distance between two distributions, p and q. In this paper, measurement variation from the historical data is used to derive the q. For each time step, p is derived from the measurement variation between the current time step and the previous time step. Under normal conditions with no false data injection attacks, the KLD is quite small. When false data are injected into the system, the KLD will be larger than normal, allowing for detection of the attack.

We have tested our method using different attacking scenarios. Test results show that the proposed method can accurately detect most of the attacks. The proposed method is also capable of detecting false data injection attacks that use previous measurements.

During the case study, we found it difficult to detect false data injection attacks on certain state variables. Besides, the proposed method will not work very well for continuous small-scale attacks and continuous replay attacks. Detecting these attack scenarios is a clear direction for future research.

References

[1] S. W. Blume, "System control centers and telecommunications," in *Electric Power System Basics*. Hoboken, NJ, USA: Wiley, Sep. 2007.

[2] A. Abur and A. G. Expsito, *Power System State Estimation: Theory and Implementation*, 1st ed. New York, NY, USA: Marcel Dekker, Mar. 2004.

[3] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. New York, NY, USA: Springer, May 1999.

[4] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[6] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Feb. 2012.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security (CCS)*, New York, NY, USA, 2009, Art. ID 21C32. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653666

[8] G. Hug and J. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[9] Q. Yang *et al.*, "On false data injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[10] R. B. Bobba *et al.*, "Detecting false data injection attacks on DC state estimation," in *Proc. Preprints 1st Workshop Secure Control Syst. (CPSWEEK)*, Stockholm, Sweden, 2010.

[11] M. Talebi, C. Li, and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in *Proc. IEEE 7th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Hoboken, NJ, USA, Jun. 2012, pp. 393–396.

[12] S. Bi and Y. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Houston, TX, USA, Dec. 2011, pp. 1162–1167.

[13] S. Bhattarai, L. Ge, and W. Yu, "A novel architecture against false data injection attacks in smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 907–911.

[14] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. 44th Annu. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, 2010, pp. 1–6.

[15] O. Kosut, L. Jia, R. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Proc. 45th Int. Univ. Power Eng. Conf. (UPEC)*, Cardiff, U.K., 2010, pp. 1–6.

[16] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[17] A. Khatkhate, A. Ray, E. Keller, S. Gupta, and S. Chin, "Symbolic time-series analysis for anomaly detection in mechanical systems," *IEEE/ASME Trans. Mechatronics*, vol. 11, no. 4, pp. 439–447, Aug. 2006.

[18] D. Dasgupta and S. Forrest, "Novelty detection in time series data using ideas from immunology," in *Proc. 5th Int. Conf. Intell. Syst.*, Reno, NV, USA, 1996.

[19] S. Salvador, P. Chan, and J. Brodie, "Learning states and rules for time series anomaly detection," in *Proc. 17th Int. FLAIRS Conf.*, Miami, FL, USA, 2004, pp. 306–311.

[20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 1991.

[21] M. Do and M. Vetterli, "Wavelet-based texture retrieval using generalized Gaussian density and Kullback–Leibler distance," *IEEE Trans. Image Process.*, vol. 11, no. 2, pp. 146–158, Feb. 2002.

[22] H. Lin, Z. Ou, and X. Xiao, "Generalized time-series active search with Kullback–Leibler distance for audio fingerprinting," *IEEE Signal Process. Lett.*, vol. 13, no. 8, pp. 465–468, Aug. 2006.

[23] S. Tong, Z. Li, Y. Zhu, and N. Thakor, "Describing the nonstationarity level of neurological signals based on quantifications of time-frequency representation," *IEEE Trans. Biomed. Eng.*, vol. 54, no. 10, pp. 1780–1785, Oct. 2007.

[24] M. Nejati, N. Amjady, and H. Zareipour, "A new stochastic search technique combined with scenario approach for dynamic state estimation of power systems," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 2093–2105, Nov. 2012.

Gu Chaojun (S'12) received the B.Eng. degree from the National University of Singapore, Singapore, in 2011, where he is currently pursuing the Ph.D. degree from the Department of Electrical and Computer Engineering.

His current research interests include power system cyber security, reliability, and forecasting.

Panida Jirutitijaroen (S'05–M'08–SM'13) received the B.Eng. degree from Chulalongkorn University, Bangkok, Thailand, and the Ph.D. degree from Texas A&M University, College Station, TX, USA, in 2002 and 2007, respectively, both in electrical engineering.

She was a Post-Doctoral Researcher with the Department of Electrical and Computer Engineering, Texas A&M University, in 2007. She is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. Her current research interests include power system reliability and optimization.

Mehul Motani (S'92–M'98) received the B.E. degree from Cooper Union, New York, NY, USA; the M.S. degree from Syracuse University, Syracuse, NY; and the Ph.D. degree from Cornell University, Ithaca, NY; in 1992, 1995, and 2000, respectively, all in electrical and computer engineering.

He was a Research Scientist at the Institute for Infocomm Research, Singapore, for three years, and was a Systems Engineer at Lockheed Martin, Syracuse, for four years. He was a Visiting Fellow at Princeton University, Princeton, NJ, USA. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore (NUS), Singapore. His current research interests include wireless networks, information theory, and communications, with applications to mobile computing, underwater communications, sustainable development, and societal networks.

Dr. Motani was the recipient of the Intel Foundation Fellowship for Ph.D. Research, the NUS Faculty of Engineering Innovative Teaching Award, and the NUS Faculty of Engineering Teaching Honors List Award. He has served as an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY and an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS. He has also served on the Organizing Committees of the IEEE International Symposium on Information Theory, the IEEE Wireless Network Coding Conference, the IEEE International Conference on Communication Systems, and on the Technical Program Committees of the Association for Computing Machinery (ACM) International Conference on Mobile Computing and Networking; the IEEE International Conference on Computer Communications; the IEEE International Conference on Network Protocols; the IEEE Conference on Sensor, Mesh, and *Ad Hoc* Communications and Networks; and several other conferences. He actively participates in the IEEE and the ACM, and has served as the Secretary of the IEEE Information Theory Society Board of Governors.