IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 26, 2020, accepted January 8, 2021, date of publication January 12, 2021, date of current version January 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3051155

A Deviation-Based Detection Method Against False Data Injection Attacks in Smart Grid

CHAO PEI[1,2,3,4,5], YANG XIAO[5], (Fellow, IEEE), WEI LIANG[1,2,3,6], (Senior Member, IEEE), AND XIAOJIA HAN[2,3,4,6]

[1]State Key Laboratory of Robotics, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China
[2]Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China
[3]Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China
[4]University of Chinese Academy of Sciences, Beijing 100049, China
[5]Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290, USA
[6]Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China

Corresponding authors: Yang Xiao (yangxiao@ieee.org) and Wei Liang (weiliang@sia.cn)

The work of Chao Pei and Wei Liang was supported in part by the National Key Research and Development Program of China under Grant 2017YFE0101300, in part by the National Natural Science Foundation of China under Grant 62022088, in part by the Liaoning Revitalization Talents Program under Grant XLYC1902110, in part by the Liaoning Provincial Natural Science Foundation of China under Grant 2020JH2/10500002 and Grant 2019-YQ-09, and in part by the International Partnership Program of Chinese Academy of Sciences under Grant 173321KYSB20180020 and Grant 173321KYSB20200002. This research was supported by the China Scholarship Council.

ABSTRACT State estimation plays a vital role to ensure safe and reliable operations in smart grid. Intelligent attackers can carefully design a destructive and stealthy false data injection attack (FDIA) sequence such that commonly used weighted least squares estimator combined with residual-based detection method is vulnerable to the FDIA. To effectively defend against an FDIA, in this paper, we propose a robust deviation-based detection method, in which an additional Kalman filter is introduced while retaining the original weighted least squares estimator, so that there are two state estimators. Moreover, an exponential weighting function is also applied to the introduced Kalman filter in our proposed method. When an FDIA occurs, the estimation results of weighted least squares estimator depend only on meter measurements at each time slot, but there is an adjustment process of estimated states for the Kalman filter based on historical states' transitions. Meanwhile, based on the exponential weighting function, estimated measurements in the Kalman filter can be adaptively suppressed for different attack strengths of FDIAs, and then the difference of the results of these two estimators increases. Subsequently, FDIAs can be effectively detected by checking the deviation of estimated measurements about the two estimators with a detection threshold. Experimental results validate the effectiveness of the proposed detection method against FDIAs. The impact of different attack strengths and noise on detection performance is also evaluated and analyzed.

INDEX TERMS State estimation, false data injection attacks, smart grid, cyber security, Kalman filter, cyber physical system.

I. INTRODUCTION

Smart grid is a typical Cyber-Physical Systems (CPS) which combines the physical world and the cyber world via seamless integration of sensing, communication, computation, and control. Compared to traditional power systems, smart grid generates a large amount of data due to the continuous two-way information interaction, demand response applications [1], etc. Bidirectional information exchange among customers, operators, and control devices provides an efficient way of energy supplying and consumption [2]. However, the strong coupling between cyber and physical operations also makes smart grid vulnerable to various malicious cyber attacks [3]. During data transmission process of power emergency control services, rapid response demands cause a lack of encryption and detection ability in smart measurement devices [4]. Successful cyber attacks may cause regional blackouts, significant financial losses, and even endangering of human lives. For instance, on 23 Dec. 2015, a synchronized and coordinated cyber attack compromised three Ukrainian regional electric power distribution companies, resulting in power outages affecting approximately 225,000 customers

The associate editor coordinating the review of this manuscript and approving it for publication was Zhitao Guan.

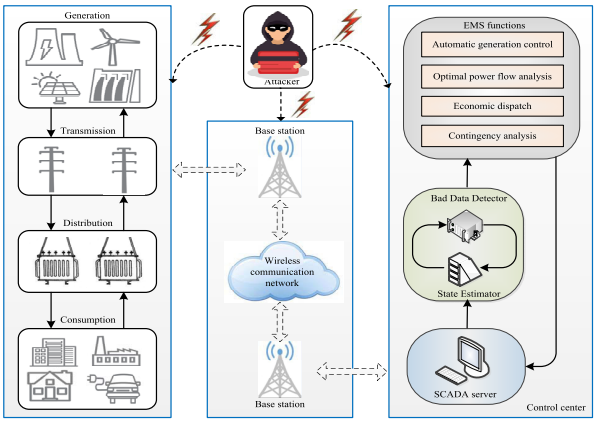

FIGURE 1. The vulnerabilities of the smart grid under the occurrence of FDIAs.

for several hours [6]. Also, it has been reported that there are about 2000 premeditated attacks on provincial power utilities in China every month [4].

FDIAs in smart grid target to state estimation. The accurate state estimation obtained from state estimators plays a vital role for the purpose of establishing the basis for subsequent controls and analysis. The real-time monitoring of smart grid is of critical importance to guarantee steady and secure operations. As shown in Fig. 1, remote terminal units such as smart meters, smart sensors, or actuators are used through the communication networks to monitor real-time measurements. The state estimator in the control center then uses these received redundant readings from supervisory control and data acquisition (SCADA) system and other available information such as topology information to estimate the electrical states. The electrical states are usually voltage amplitudes and voltage phase angles. These critical parameters must be accurately estimated in energy management system so that other applications such as optimal power flow analysis, automatic generation control, economic dispatch, and contingency analysis can be controlled. All these decisions in the control center are used to ensure the balance of power supply and demand in smart grid. The FDIAs can be launched through hacking some smart meters and sensors, interfering communication links, or damaging the database and the control center directly [5].

The widely used static state estimation in smart grid is based on the weighted least squares estimation method. A detector, either the ℓ_2-norm measurement residual-based $J(x)$ detector or the largest normalized residual-based (LNR) detector, can effectively detect bad data which is caused by random noise [8]. It has been shown that FDIAs can circumvent conventional normalized measurement residual-based bad data detection and can insert any bias into the value of estimated states stealthily [9], [10]. Recently, the possible false data injection attacks have also been considered in dynamic systems, especially in stochastic systems. In [11], a new necessary and sufficient condition for the insecurity is derived in the case that all communication channels are compromised by an adversary. In [7] and [12], an optimal linear deception attack strategy is proposed to successfully inject false data without being detected and the FDIA for cyber-physical system with resource constraint is also considered.

In response to FDIAs, defense mechanisms are either to protect the smart grid from attackers in advance or to detect and identify FDIAs during the process of state estimation. From the perspective of protection-based defense, FDIAs can be defended by protecting some strategically selected meter measurements such that these protected measurements cannot be tampered by attackers anymore. Another way of protection is to deploy advanced measurement units, such as phasor measurement units (PMUs). Since PMUs have the capability of providing accurate synchronous phasor measurements for geographically dispersed nodes in power grids by synchronizing to the global positioning system (GPS), PMUs are typically robust against data injection attacks and have measurements secured [13]. However, the deployment cost in this way is very high. Moreover, the protection-based defend methods are only applicable to power systems with specific topologies and they are unavailable to changing grid topologies.

Commonly used ℓ_2-norm-based measurement residual detection methods based on static state estimation have been verified to have good performance in dealing with bad data except for FDIAs [23]. For the real-time detection and identification of FDIAs in smart grid, adopting a state-space model enables a dynamic state estimator to combine present and past measurements so that the system state can be inferred in an accurate and robust way [25]. In [26], a cosine similarity matching approach is proposed to detect FDIAs by comparing estimated state values of a Kalman filter and measurements from PMUs. The authors in [27] present a Euclidean detector to determine the difference between the estimated measurements and the actual measurements. These actual measurements are usually obtained from smart sensors. However, these measurement residual-based detection methods [26], [27] generally rely on trustworthy and reliable measurements from advanced measurement devices such as PMUs. To manage and utilize large, high-density data streams with nanosecond time stamping of PMUs is a challenging task [35].

Based on above mentioned issues, the main motivations of this paper are illustrated as follows. Under normal operations of smart grid, fast dynamics of power systems can be well damped and sudden load changes are infrequent so that system states change gradually over time. Moreover, since loads in smart grid vary according to the temperature and weather, there exists temporal correlation of system states with the evolution of system changes. Based on historical state variables' transitions, bad effects of attacks can be introduced to these estimated state variables in a Kalman filter [28] when compared with the case that under normal condition. While the state estimation result of the original weighted least squares estimator under attacks is realtime at each time slot, if we introduce an additional estimator of a Kalman

filter based on the state-space model, it enables the FDIAs' detection by considering the difference of estimation results about the two estimators. Instead of hardware deployment with expensive PMUs equipment, we are concentrating on solving the problem of FDIAs detection only through the software implementation of the proposed effective detection method. Therefore, in this paper, we propose a deviation-based detection method against FDIAs by adopting an additional estimator of Kalman filter, which can conduct dynamic state estimation based on historical states' transition. There is an adjustment process of estimated states in the Kalman filter when FDIAs occur, while the estimation result of the weighted least squares estimator to FDIAs is realtime. With the weighted least square estimator, the discrepancy between estimation results of these two estimators allows FDIAs to be effectively detected. Moreover, the exponential weighting function is applied to enhance the robustness of the introduced additional Kalman filter. Therefore, the difference of the two estimators increases because the impact of estimation performance in the Kalman filter under attacks is mitigated. The main contributions of this paper are summarized as follows:

- A low-cost deviation-based detection method against FDIAs is firstly proposed considering the integration of an additional Kalman filter.
- An robust strategy using exponential weighting function is applied to enhance the robustness of introduced additional Kalman filter such that the detection performance of our proposed detection method is effectively improved.
- The proposed deviation-based detection method has strong scalability. It can also detect other types of attack scenarios, such as step attacks and random attacks.
- The reliable response and efficiency of the proposed detection method against FDIAs is demonstrated through experiments. The impact of different attack strengths and noise to the detection performance is also evaluated and analyzed.

The rest of the paper is organized as follows. Related works about defense methods against FDIAs are presented in Section II. Section III presents the model of system framework and FDIAs. In Section IV, the impact of FDIAs on estimation performance target to the Kalman filter is analyzed and the deviation-based detection method is proposed. Section V provides experiments and performance evaluation results. Finally, we conclude this paper with some future research directions in Section VI. Nomenclature of the paper is given in Table 1.

TABLE 1. Nomenclature.

$\boldsymbol{z}_k$	Measurement vector at time k
$\boldsymbol{x}_k$	State variables vector at time k
$\boldsymbol{v}_k$	Measurement error vector at time k
$\boldsymbol{R}$	Error covariance matrix of $\boldsymbol{v}$
$\boldsymbol{H}$	Jacobian matrix
$\boldsymbol{z}_k^f$	Measurement vector which is under FDIA at time k
$\boldsymbol{a}_k$	Nonzero injected false attack vector at time k
$\hat{\boldsymbol{x}}_k$	Estimated state vector when no attack
$\hat{\boldsymbol{z}}_k$	Estimated measurement vector when no attack
$\boldsymbol{r}_k$	Measurement residual vector at time k
τ	Detection threshold
$\hat{\boldsymbol{x}}_k^f$	Estimated state vector when under FDIA
$\boldsymbol{c}$	Introduced error to the correct state vector
$\boldsymbol{r}_k^f$	Measurement residual vector when under FDIA
$\boldsymbol{A}$	State transition matrix
$\boldsymbol{w}_k$	Process noise vector at time k
$\boldsymbol{Q}$	Error covariance matrix of $\boldsymbol{w}$
$\hat{\boldsymbol{x}}_{k\|k-1}$	Priori minimum mean square error estimation of state $\boldsymbol{x}$
$\boldsymbol{K}_k$	Kalman gain at time k
$\boldsymbol{P}_{k\|k-1}$	Priori state error covariance
$\boldsymbol{P}_k$	Posteriori state error covariance

II. RELATED WORKS

For the protection-based defense, the authors in [12] propose that FDIAs can be defended by protecting a set of strategically selected measurements. A greedy strategy-based method is presented in [14] to find the minimum measurements set that need to be protected. Moreover, since phasor measurement units (PMUs) have the capability of providing accurate synchronous phasor measurements for geographically dispersed nodes in power grids by synchronizing to the global positioning system (GPS), PMUs are typically robust against data injection attacks and have measurements secured [13]. The state information can be monitored directly by the placement of PMUs. In [19], [20], low complexity secure PMU placement algorithms are proposed based on a fast greedy strategy. A mixed integer programming model for optimal PMU placement is developed to defend FDIAs in [21]. However, since PMUs are expensive devices in practice, it is not feasible to deploy enough PMUs to secure all the measurements. Hence, deploying PMUs is more suitable for power systems that have great social and economic impacts [20].

Due to insufficiency of the protection-based defense and invalidation of traditional residual-based bad data detection methods against FDIAs, real-time detection and identification of such attacks are important to guarantee stable operations in smart grid. A generalized likelihood ratio test is presented to detect weak FDIAs (the adversary controls only a small number of meters and cannot perform the unobservable attack) in [22]. By taking the power measurements of two sequential data collection slots into account in short-term sampling range, an FDIA together with some non-stealthy attacks can be detected by monitoring the measurement variance and state changes. A state change vector, which can be estimated from the measurement change vector, is compared with a pre-defined threshold to detect FDIAs [13]. The authors in [23] propose a short-term state forecasting-aided method to detect false data injection attacks based on the fact that there exists temporal correlation between state variables. An auto-regressive (AR) model is adopted to obtain the forecasted measurements, and the normalized residual between original received measurements and forecasted measurements is used as an indicator of the detector. The authors in [24] adopt an adaptive cumulative sum (CUSUM) based

method to detect mean distribution change of the residual vector under the occurrence of FDIAs, and the state estimation is based on the conventional weighted least squares method. Given corrupted measurements matrix under FDIAs, the false data can be identified by performing low rank and sparse decomposition in the robust principal component analysis(RPCA) [14]. The authors in [15] propose to detect FDIAs in realtime by utilizing load forecasts, generation schedules, and synchrophasor data. These leveraged online information is independent with traditional SCADA measurements such that anomalies can be identified. Based on the fact that normal measurements and attacked measurements can be statistically distinguished, the authors in [16] adopt a distributed support vector machine (SVM) algorithm for training and principal component analysis (PCA) for feature selection. The authors in [17] propose a detection mechanism using a reinforcement learning algorithm and formulate the stealthy FDIAs detection problem as a partially observable Markov decision process. In [18], a data driven machine learning based scheme, which employs ensemble learning, is proposed to detect stealthy false data injection attacks on state estimation. Both supervised and unsupervised classification methods are used and decisions by individual classifiers are further classified [18].

For the real-time detection of FDIAs by adopting state-space models and dynamic state estimators, a diffusion strategy based on distributed Kalman filters is proposed by using the neighboring state information to form an optimal state for every meter [29]. As for distributed quickest detection of FDIAs, a CUSUM-based detection scheme is proposed [25]. The average false alarm rate of the CUSUM-based detection scheme is lower compared with the Euclidean detector because there is an accumulation of change statistics.

III. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a steady-state and lossless power transmission system with N buses and M meters, where $M \gg N$. The steady-state of a power system is usually defined as an operating condition of a power system in which all the operating quantities that characterize it can be considered to be constant for the purpose of analysis. It is usually difficult for a control center to directly obtain all state variables, such as phase angles of all buses, by sensors in smart grid. Therefore, state estimation plays an important role to estimate operation states. Even though the relationship between state variables and measurements in an actual power system is based on a nonlinear function, due to simplicity and robustness of the direct current (DC) model, a linear equation which compactly associates the state variables and measurements is widely used [10], [14], [19] as follows:

$$z_k = \boldsymbol{H}\boldsymbol{x}_k + \boldsymbol{v}_k, \tag{1}$$

where $k \in \mathbb{N}$ is the time index, $z_k \in \mathbb{R}^M$ is the vector of measurements obtained from meters, $\boldsymbol{x}_k \in \mathbb{R}^N$ is the vector of system states (bus phase angles in the DC model), $\boldsymbol{H} \in \mathbb{R}^{M\times N}$ is the measurement Jacobian matrix, and $\boldsymbol{v}_k \in \mathbb{R}^M$ is the zero-mean Gaussian white measurement noise with a known error covariance matrix $\boldsymbol{R}$, i.e., $\boldsymbol{v}_k \sim \mathcal{N}(\boldsymbol{0}, \sigma_v^2 \boldsymbol{I}_M)$, where $\boldsymbol{I}_M$ represents the $M \times M$ identity matrix. The target of the attacker is to inject additive malicious data to a subset of measurements by the ways shown is Fig. 1, such that the measurement model under FDIAs can take the following form:

$$z_k^f = \boldsymbol{H}\boldsymbol{x}_k + \boldsymbol{a}_k + \boldsymbol{v}_k, \quad k \geq k_0 \tag{2}$$

where $\boldsymbol{a}_k = [a_{1,k}, a_{2,k}, \ldots, a_{M,k}]^T$ is the injected false data at time k, k_0 represents the time that the attack is started to be launched. Not all the meters can be compromised in smart grid, such that if meter $i \in [1, M]$ is not under attack, we have $a_{i,k} = 0$; otherwise $a_{i,k} \neq 0$ holds.

The state estimation and the formulation of false data injection attacks in smart grid are stated as follows. The widely used weighted least squares state estimation is formulated as an optimization problem in which the weighted least squares error is minimized to obtain the estimated state variables. Suppose that the power system is under normal operation condition, the optimal solution can be obtained as $\hat{\boldsymbol{x}}_{\boldsymbol{k}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}z_k$ in the DC model. Naturally, the estimated measurement vector can be derived, i.e., $\hat{z}_k = \boldsymbol{H}\hat{x}_k = \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}z_k$. Intuitively, measurements from normal meters usually produce state variables that are close to the actual values. There exist inconsistence between normal measurements and bad measurements. The traditional bad data detection method is usually based on the residual-based detector and then the residuals between observed measurements z_k and estimated measurements $\hat{z}_k$ are compared with predetermined detection threshold τ. The residual is defined as $\boldsymbol{r}_k = z_k - \hat{z}_k = z_k - \boldsymbol{H}\hat{\boldsymbol{x}}_k = (\boldsymbol{I} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1})z_k$. In order to carry out the detection process, if the ℓ_2-norm of residual $\boldsymbol{r}_k$ is large than the predetermined threshold, i.e., $||z_k - \boldsymbol{H}\hat{\boldsymbol{x}}_k||_2 > \tau$, there exists bad measurements. On the contrary, if $||z_k - \boldsymbol{H}\hat{\boldsymbol{x}}_k||_2 \leq \tau$, the measurement vector $\boldsymbol{z}$ is regarded as a normal one. The predetermined threshold τ is usually obtained by the hypothesis test problem of $\Pr(\|\boldsymbol{r}_k\|_2 > \tau) = \alpha$ for a given false alarm probability α.

When attackers start to manipulate measurements, the estimated state variables $\hat{\boldsymbol{x}}_k^f$ under FDIAs can be represented as:

$$\begin{aligned}\hat{\boldsymbol{x}}_k^f &= (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}(z_k + \boldsymbol{a}_k) \\ &= \hat{\boldsymbol{x}}_k + (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{a}_k = \hat{\boldsymbol{x}}_k + \boldsymbol{c},\end{aligned} \tag{3}$$

where $\boldsymbol{c}$ represents the introduced error to original state variables and the dimension of $\boldsymbol{c}$ is the same as $\boldsymbol{x}_k$. The measurement residual under the attacks then can be expressed as follows:

$$\begin{aligned}\boldsymbol{r}_k^f &= ||z_k^f - \boldsymbol{H}\hat{\boldsymbol{x}}_k^f||_2 = ||z_k + \boldsymbol{a}_k - \boldsymbol{H}(\hat{\boldsymbol{x}}_k + \boldsymbol{c})||_2 \\ &= ||z_k - \boldsymbol{H}\hat{\boldsymbol{x}}_k + (\boldsymbol{a}_k - \boldsymbol{H}\boldsymbol{c})||_2.\end{aligned} \tag{4}$$

Therefore, if original normal measurements can bypass the measurement residual-based bad data detector and if the

injected attack vector $\boldsymbol{a}_k$ satisfies the condition $\boldsymbol{a}_k = \boldsymbol{Hc}, \boldsymbol{r}_k^f = ||\boldsymbol{z}_k^f - \boldsymbol{H}\hat{\boldsymbol{x}}_k^f||_2 \leq \tau$ holds. In other words, the compromised measurements can also circumvent the detector. Attackers need to obtain the Jacobian matrix $\boldsymbol{H}$ and have the capability to modify some meters. To sum up, this carefully designed FDIAs could inject any bias to the state estimation $\hat{\boldsymbol{x}}_k$ while circumventing the alarm of the bad data detector in the control center.

IV. PROPOSED DEVIATION-BASED DETECTION METRIC

As explained before, under normal operations of smart grid, there exists temporal correlation of the system states since loads are varying according to changes in weather and temperature. On the other hand, the influence of introduced attacks and disturbance can be propagated to future system states through state's transition. When attacks occur, the deviation of estimated states will break down the temporal correlation, and launched attacks can be easily detected. Therefore, besides the measurement equation, we further introduce the state transition equation to construct the state space model. Thus, a discrete-time linear time-invariant process is considered:

$$\boldsymbol{x}_{k+1} = \boldsymbol{A}\boldsymbol{x}_k + \boldsymbol{w}_k,\ \boldsymbol{z}_k = \boldsymbol{H}\boldsymbol{x}_k + \boldsymbol{v}_k, \tag{5}$$

where $k \in \mathbb{N}$ is the time index, $\boldsymbol{x}_k \in \mathbb{R}^N$ and $\boldsymbol{z}_k \in \mathbb{R}^M$ are the vectors of system states and measurements, $\boldsymbol{A} \in \mathbb{R}^{N\times N}$ is the state transition matrix. Process noise $\boldsymbol{w}_k \in \mathbb{R}^N$ and measurement noise $\boldsymbol{v}_k \in \mathbb{R}^M$ are assumed to be mutually uncorrelated zero-mean Gaussian signals with known error covariance $\boldsymbol{Q}$ and $\boldsymbol{R}$, i.e., $\boldsymbol{w}_k \sim \mathcal{N}(\boldsymbol{0}, \sigma_w^2\boldsymbol{I}_N)$, $\boldsymbol{v}_k \sim \mathcal{N}(\boldsymbol{0}, \sigma_v^2\boldsymbol{I}_M)$, where $\boldsymbol{w}_k$ represents the external disturbance of dynamic systems. The Kalman filter is known as an optimal linear estimator which can minimize the mean-squared error and can provide a recursive calculation of the state variables. The estimation process are represented as follows:

$$\hat{\boldsymbol{x}}_{k|k-1} = \boldsymbol{A}\hat{\boldsymbol{x}}_{k-1}, \tag{6}$$
$$\boldsymbol{P}_{k|k-1} = \boldsymbol{A}\boldsymbol{P}_{k-1}\boldsymbol{A}^T + \boldsymbol{Q}, \tag{7}$$
$$\boldsymbol{K}_k = \boldsymbol{P}_{k|k-1}\boldsymbol{H}^T[\boldsymbol{H}\boldsymbol{P}_{k|k-1}\boldsymbol{H}^T + \boldsymbol{R}]^{-1}, \tag{8}$$
$$\hat{\boldsymbol{x}}_k = \boldsymbol{A}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[\boldsymbol{z}_k - \boldsymbol{H}\hat{\boldsymbol{x}}_{k|k-1}], \tag{9}$$
$$\boldsymbol{P}_k = [\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{H}]\boldsymbol{P}_{k|k-1}, \tag{10}$$

where $\hat{\boldsymbol{x}}_{k|k-1}$ and $\hat{\boldsymbol{x}}_k$ are the priori and posteriori minimum mean squared error estimates of state $\boldsymbol{x}_k$ in the estimator, $\boldsymbol{P}_{k|k-1}$ and $\boldsymbol{P}_k$ are the corresponding priori and posteriori state error covariances, $\boldsymbol{K}_k$ is the Kalman gain at time k. The recursion starts from $\hat{\boldsymbol{x}}_0 = \boldsymbol{0}$ and $\boldsymbol{P}_0 = \boldsymbol{\pi}_0$, where $\boldsymbol{\pi}_0$ is the covariance matrix of the initial state $\hat{\boldsymbol{x}}_0$.

Moreover, the innovation of Kalman filter is defined as $\boldsymbol{\xi}_k = \boldsymbol{z}_k - \boldsymbol{H}\hat{\boldsymbol{x}}_{k|k-1}$. The innovation has following properties: (1) $\boldsymbol{\xi}_k$ is zero-mean Gaussian; (2) $\boldsymbol{\xi}_k$ and $\boldsymbol{\xi}_j$ are independent, $\forall j \neq k$; (3) The covariance of $\boldsymbol{\xi}_k$ satisfies $\mathbb{E}[\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T] = \boldsymbol{H}\boldsymbol{P}_{k|k-1}\boldsymbol{H}^T + \boldsymbol{R}$, where $\mathbb{E}$ represents the expectation [31].

Assume that the power system is operating in normal condition until FDIAs are launched at time k, from the estimation process of Equations (6)-(10), attackers can only change the measurement vector $\boldsymbol{z}_k$ into $\boldsymbol{z}_k^f$. Equation (9) becomes

$$\begin{aligned}\hat{\boldsymbol{x}}_k &= \boldsymbol{A}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[\boldsymbol{z}_k^f - \boldsymbol{H}\hat{\boldsymbol{x}}_{k|k-1}] \\ &= \boldsymbol{A}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[\boldsymbol{z}_k + \boldsymbol{a}_k - \boldsymbol{H}\hat{\boldsymbol{x}}_{k|k-1}].\end{aligned} \tag{11}$$

The estimated states after FDIAs at time k can be represented as $\hat{\boldsymbol{x}}_k^f = \hat{\boldsymbol{x}}_k + \boldsymbol{K}_k\boldsymbol{a}_k$, where $\hat{\boldsymbol{x}}_k^f$ is the estimated state vector after attacks. We define the injected bias of estimated states at time k as $\Delta\hat{\boldsymbol{x}}_k^f = \hat{\boldsymbol{x}}_k^f - \hat{\boldsymbol{x}}_k$. Then for the next time slot $k+1$, there exists the following relationships:

$$\begin{aligned}\hat{\boldsymbol{x}}_{k+1}^f &= \boldsymbol{A}\hat{\boldsymbol{x}}_k^f + \boldsymbol{K}_{k+1}[\boldsymbol{z}_{k+1}^f - \boldsymbol{H}\boldsymbol{A}\hat{\boldsymbol{x}}_k^f] \\ &= \boldsymbol{A}\hat{\boldsymbol{x}}_k^f + \boldsymbol{K}_{k+1}[\boldsymbol{z}_{k+1} + \boldsymbol{a}_{k+1} - \boldsymbol{H}\boldsymbol{A}\hat{\boldsymbol{x}}_k^f] \\ &= \hat{\boldsymbol{x}}_{k+1} + [\boldsymbol{I} - \boldsymbol{K}_{k+1}\boldsymbol{H}]\boldsymbol{A}\Delta\hat{\boldsymbol{x}}_k^f + \boldsymbol{K}_{k+1}\boldsymbol{a}_{k+1}.\end{aligned} \tag{12}$$

Thus the injected bias of estimated states at time $k+1$ is $\Delta\hat{\boldsymbol{x}}_{k+1}^f = \hat{\boldsymbol{x}}_{k+1}^f - \hat{\boldsymbol{x}}_{k+1} = [\boldsymbol{I} - \boldsymbol{K}_{k+1}\boldsymbol{H}]\boldsymbol{A}\Delta\hat{\boldsymbol{x}}_k^f + \boldsymbol{K}_{k+1}\boldsymbol{a}_{k+1}$.

Through the analysis mentioned above, we can see that injected bias is affected by current injected false data and the previous bias of estimated states. The injected bias to the estimated states is gradually accumulated to the real system states. Therefore, due to the adoption of state transition equation, based on historical estimated states, there exists an adjustment process of estimated states when FDIAs occur in the Kalman filter. However, the response of weighted least squares estimator to FDIAs is realtime at every current time slot. While retaining the weighted least squares estimator, the existence of discrepancy and inconsistency about the response of two estimators allows FDIAs to be effectively detected.

On the other hand, to mitigate the impact of injected bias to the estimation performance in the Kalman filter [30], some countermeasures can be applied to enhance the robustness. From the measurement update step of Kalman filter, if the Kalman gain can be adaptively reduced when the innovation becomes large due to injection of FDIAs. Then the estimation performance can be preserved to a certain extent, such that the final estimation results will have a larger weight on the results of prediction step. Inspired from [32], the measurement weighting function $\boldsymbol{W}_k$, which is the inverse of measurement noise covariance $\boldsymbol{R}$, can be replaced by the following equation:

$$(\boldsymbol{W}_k^{new})^{-1} = (\boldsymbol{W}_k)^{-1} * \exp(\left|\boldsymbol{z}_k - \boldsymbol{H}\hat{\boldsymbol{x}}_{k|k-1}\right|). \tag{13}$$

By this method, the influence leading to the deterioration of estimation performance can be better suppressed. When the predicted measurements and the received measurements have a large deviation, the increase of absolute residual vector makes measurement noise larger, leading to the decrease of the Kalman gain. On the contrary, the measurement noise will change a little if the deviation of predicted measurements and received measurements is very small. Estimation results will not be affected too much. At the same time, the robust state estimation of the Kalman filter can improve the detection capability of FDIAs because the estimated measurements of

Algorithm 1 The Deviation-Based Detection Method

Require: State transition matrix $\boldsymbol{A}$; noise error covariance $\boldsymbol{Q}$ and $\boldsymbol{R}$; initial state $\hat{\boldsymbol{x}}_0$ and state error covariance $\boldsymbol{P}_0$; predefined threshold τ;

Ensure: Declare the occurrence of FDIA.

1: **for** $k = 1$ to N_0, where N_0 represents the number of time slots **do**
2: Collect measurement vector z_k from all meters and identify measurement Jacobian matrix $\boldsymbol{H}$;
3: Traditional static state estimation using weighted least squares method to compute estimated state vector $\hat{\boldsymbol{x}}_{\boldsymbol{ks}}$, $\hat{\boldsymbol{x}}_{\boldsymbol{ks}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}z_k$;
4: Compute estimated measurement vector $\hat{\boldsymbol{z}}_{\boldsymbol{ks}}$, $\hat{z}_{ks} = \boldsymbol{H}\hat{x}_{ks} = \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}z_k$;
5: Implement the state prediction step of the Kalman filter using Equations (6)-(7);
6: Update measurement noise covariance by the exponential weighting function using Equation (13), where $\boldsymbol{R} = (\boldsymbol{W}_k)^{-1}$;
7: Implement the measurement update step of Kalman filter using Equations (8)-(10) to obtain estimated state vector $\hat{\boldsymbol{x}}_{kd}$, $\hat{\boldsymbol{x}}_{kd} = \boldsymbol{A}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[z_k - \boldsymbol{H}\hat{\boldsymbol{x}}_{k|k-1}]$;
8: Compute the estimated measurement vector $\hat{z}_{kd}$ from the Kalman filter, $\hat{z}_{kd} = \boldsymbol{H}\hat{x}_{kd}$;
9: Calculate deviations of the two estimated measurement vectors as $\boldsymbol{e}_k = \left|\hat{z}_{ks} - \hat{z}_{kd}\right|$;
10: **if** $\boldsymbol{e}_k$ is larger than τ **then**
11: Report FDIA and trigger an alarm;
12: **else**
13: Continue the state estimation process;
14: **end if**
15: **end for**

the enhanced Kalman filter is smaller than original results leading the difference of responses of weighted least squares estimator and the Kalman filter become apparent. The proposed deviation-based detection metric targeted to FDIAs is shown in Algorithm 1.

In the power grid, the state variables are usually voltage values and phase angles of all buses. The phase angles usually cannot be directly obtained. Since PMUs have the capability to measure voltage angles, the cost for a large scale deployment of these advanced devices is very expensive. Therefore, compared with these trustworthy measurements-based detection methods, our proposed detection method against FDIAs is designed to be effective with a low cost.

V. EXPERIMENTS AND RESULTS

In this section, the effectiveness of our proposed method against FDIAs is evaluated through experiments. Typically, the variation of amplitude and phase always changes with an attack or a fault in the power system [33]. Without loss of generality, we adopt the sinusoidal wave model of power grid voltage signal in which the basic simulation and experimental settings are the same with [26], [27], [29] and the state variables such as voltage magnitudes and angles are included. The commonly used three-phase sinusoidal voltage signal can usually be generalized to the power grid measurements because the state variables are constrained by power flow functions. Basically, we assume that the angular frequency is relatively constant over time so that the amplitude and phase are considered as state variables in the measurement equation. Moreover, the voltage value can be measured real-time by smart meters. In this paper, the measurement noise for these meters is assumed to be normally distributed with zero mean and variance 0.01. All experiments are conducted using MATLAB with a computer of 3.2 GHz Intel Core i5 processor and 4GB memory on a Windows 7 system.

The power system is assumed to operate under normal conditions and the sinusoidal voltage signal can be represented as $z_k = A_v\cos(\omega k+\phi) = A_v*\cos\phi*\cos\omega k - A_v*\sin\phi*\sin\omega k$, where A_v is the amplitude, ω is the angular frequency, and ϕ is the phase at discrete time k. Equivalently, the observation equation of actual sinusoidal voltage signal can be rewritten as: $\boldsymbol{z}_k = [\cos\omega k \;\; -\sin\omega k][x_1(k)\;\; x_2(k)]^T + \boldsymbol{v}_k$, where $x_1 = A_v * \cos\phi$ and $x_2 = A_v * \sin\phi$ are defined as state variables, and they are integrated indicators about amplitude and phase. As mentioned earlier, under normal operations of smart grid, the system is assumed to be operated under quasi static conditions, then fast dynamics of the system can be well damped, and system states change gradually over time. Thus the state transition matrix is diagonal and constant [34]. On the other hand, due to loads in smart grid can vary according to temperature and weather, there exists temporal correlation of system states with the operation of the system. Therefore, the system matrix is chosen to be an identity matrix, and the state transition equation can be formulated as: $\boldsymbol{x}_{k+1} = diag[1\;1]\boldsymbol{x}_k + \boldsymbol{w}_k$, where $\boldsymbol{x}_k = [x_1(k)\;\; x_2(k)]^T$, and $\boldsymbol{w}_k$ is the process noise representing the disturbance input and model error. Experimental parameters in our experiments are set as follows: the sampling frequency is 2 kHz, the nominal value of amplitude is 1 volt, the frequency is 50 Hz, the initial state vector is $\hat{\boldsymbol{x}}_0 = \boldsymbol{0}$, and the initial state covariance matrix is $\boldsymbol{P}_0 = \boldsymbol{I}$ representing identity matrix. Moreover, based on the analysis about stealthy condition of FDIAs in Section III, the launched attack vector $\boldsymbol{a}_k$ needs to satisfy $\boldsymbol{a}_k = \boldsymbol{Hc}$ at each time slot k, where $\boldsymbol{H}$ represents the Jacobian matrix and $\boldsymbol{c}$ is the injected bias to the state variables. Therefore, attackers need to know the Jacobian matrix $\boldsymbol{H}$ and have the capability to modify some meters. To launch FDIAs with different attack strengths, we can obtain the injected attack vector $\boldsymbol{a}$ by adjusting the value of injected bias $\boldsymbol{c}$. Therefore, measurement vectors under FDIAs can be obtained by the normal measurements plus the injected attack vectors. The carefully designed false data injection attacks are launched at time 0.06s.

Next, we first verify that the traditional used weighted least squares based estimator combined with the residual-based detection mechanism fails to detect false data injection attacks. Then, the detection performance of the proposed deviation-based method against FDIAs is illustrated.

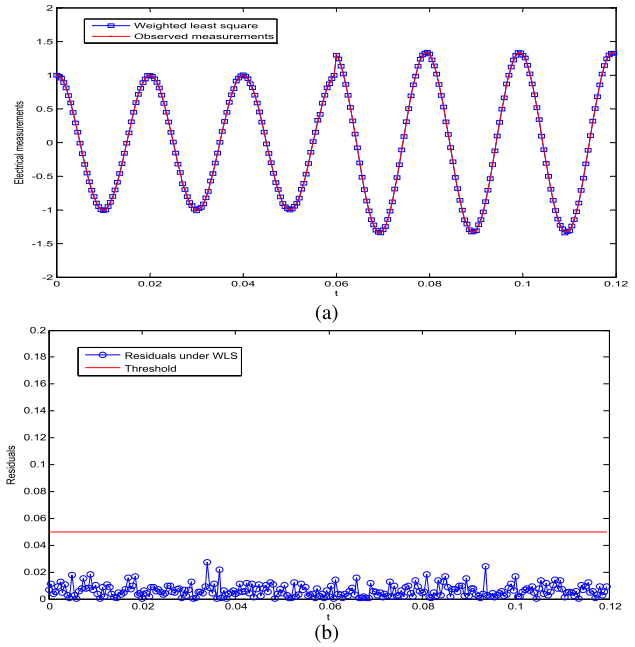

FIGURE 2. (a) Observed measurements and estimated measurements by the weighted least squares estimator under an FDIA. (b) Detection performance of the traditional residual-based detector under an FDIA.

The influence of noise and strength of attacks towards the detection performance are also discussed. Finally, we evaluate the detection performance of the proposed detection method to other attacks, such as random attacks and step attacks.

Based on aforementioned experimental setup, Fig. 2(a) shows that estimated measurements based on the weighted least squares estimator are almost the same with observed meter measurements before the occurrence of the FDIA at time 0.06s. The observed measurements refer to the values that can be directly measured by smart meters or smart sensors. In our experiments, the observed measurements are voltage amplitudes. In the second half of observation period, since the carefully designed FDIA satisfies the stealthy condition, which is $\boldsymbol{a}_k = \boldsymbol{Hc}$, where $\boldsymbol{H}$ is the measurement Jacobian matrix, $\boldsymbol{c}$ is the bias that the attacker attempts to inject to the state variables. We can see that the observed measurements tampered by attackers are almost consistent with the estimated measurements although the real measurements of the power system are not changed. The injected bias to the state variables is 0.5. Fig. 2(b) shows that the measurement residual-based bad data detector cannot detect the launched FDIA. The experiment results demonstrate that the FDIA can inject any bias to the state estimation while circumventing the detection of the bad data detector in the control center. This is very serious and harmful, and could endanger other subsequent modules of control and decision in the power grid.

While retaining the weighted least squares estimator in power system, Fig. 3 shows that there is an adjustment process of state variables in the introduced Kalman filter when the FDIA occurs in the second half of the observation period.

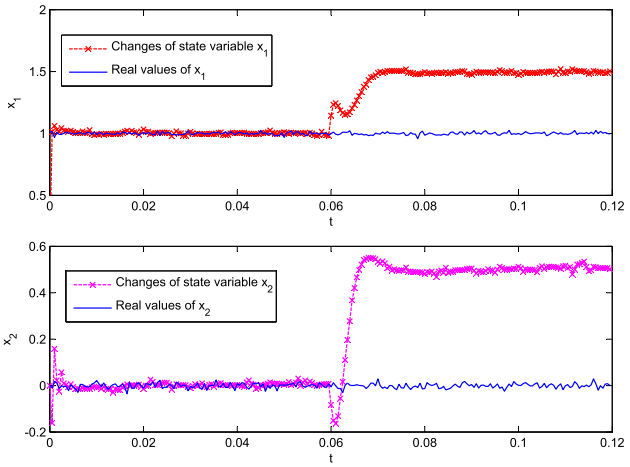

FIGURE 3. The response of state variables with the Kalman estimator under the FDIA.

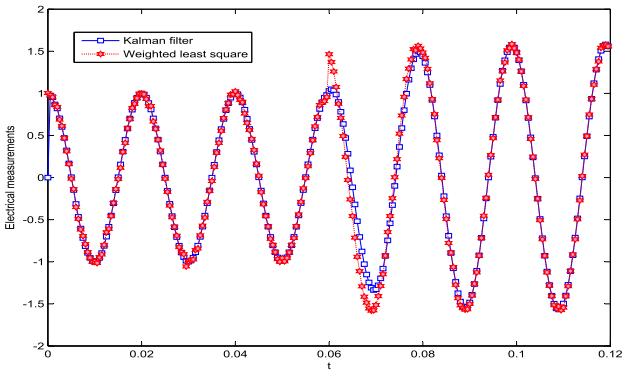

FIGURE 4. The inconsistency between the response of the Kalman filter and the weighted least squares estimator under the FDIA.

From the derivation of weighted least squares estimation, the response of the estimated state variables is immediate at each time slot. But from Equation (12), we observe that the influence of the attack vector at the current and previous time slots is coupled together. When the FDIA occurs at the first time, the state transition based on the accurate history state variables cause the variation of estimated state variables by the Kalman filter changing a little. Clearly, there is an adjustment process until the Kalman filter estimator reaches the steady state. The period of sinusoidal voltage signal is 0.02s. However, the adjustment process is more than half of the signal period under normal process noise until estimated state variables reach stable states. With a smaller process noise, the adjustment process becomes longer.

Fig. 4 shows the variance of estimated results about the Kalman filter estimator and the weighted least squares estimator. In the first half of the observation period, there is no FDIA launched in meter measurements. The estimated states from the two estimators are almost the same, and the difference of estimated states from the two estimators is smaller than the predefined threshold. This result can be observed from Fig. 5(a), and this implies that there is no FDIA occurring. For the second half of observation period, the FDIA is

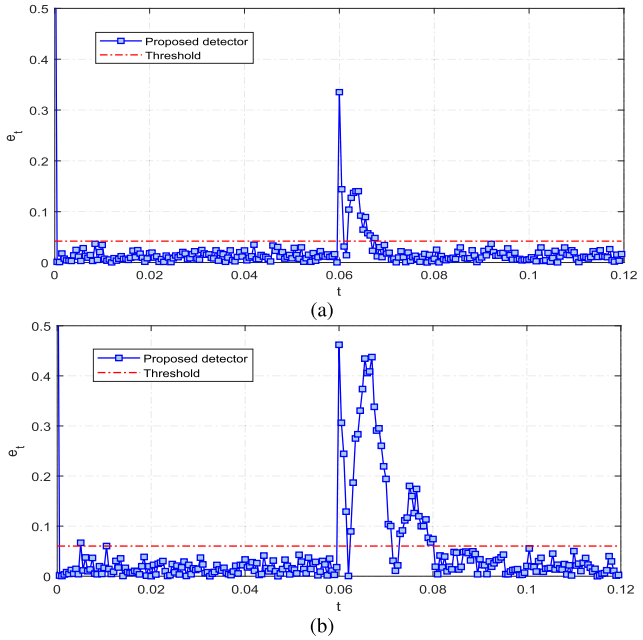

FIGURE 5. Detection performance of the proposed detection method under the FDIA with (a) large process noise. (b) small process noise.

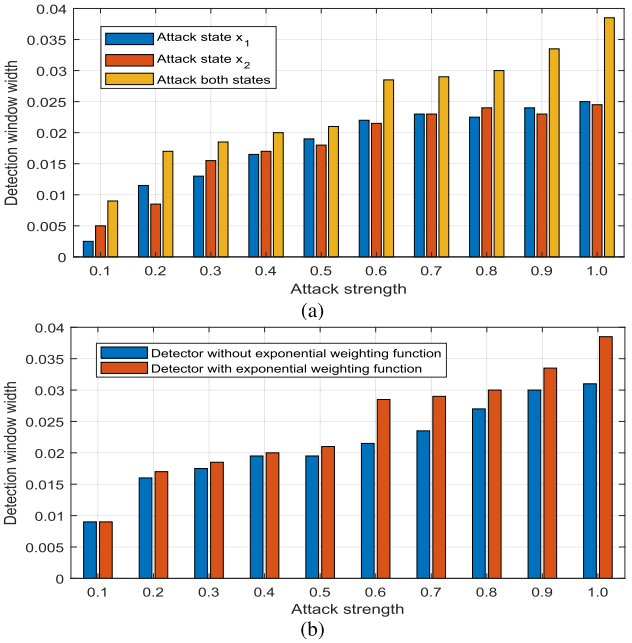

FIGURE 6. (a) Attack detection performance for different state variables under different attack strength. (b) Detection performance of the proposed detector considering exponential weighting function.

launched. The response of the estimated electrical measurements from the weighted least squares estimator immediately reaches the maximum value, while there is a slow adjustment process of the estimated electrical measurements from the Kalman filter. The inconsistency about the response of the two estimators allows the FDIA to be detected effectively. Fig. 5(a) shows the detection performance. When the FDIA occurs, the $\boldsymbol{e}_k$ exceeds the given threshold, which allows it to be detected quickly. Note that the threshold can be obtained through the normal historical state information.

Fig. 5(b) shows the detection performance of the proposed detection method with small process noise under the occurrence of the FDIA. The process noise is set to be ten times smaller than the normal process noise. Compared with results in Fig. 5(a), the values of detection indicators are significantly changed and the available FDIA detection time is increased.

The injected false data can usually cause a large perturbation on system states, while the detection rate may suffer from a slightly increase so that the sensitivity and reliability of attack detection should be carefully considered. Our proposed deviation-based FDIA detection algorithm can be completed within every state estimation and has good computational efficiency. Usually, in order to reduce false alarms, when e_k exceeds the threshold value τ for three consecutive time slots, an alarm is triggered to report FDIA. The detection threshold τ is chosen based on the historical observations and the tradeoff of detection probability and false alarm probability. The attack detection performance for different state variables under different attack strengths is shown in Fig. 6(a). We define a detection window width to describe the detection performance of our proposed detector. The detection window width is the time interval between the beginning and end of alarms. The time when an alarm ends is defined as the start time when $\boldsymbol{e}_k$ is less than the threshold τ for three consecutive time slots. Since state variables x_1 and x_2 are integrated indicators about amplitude and phase, in order to launch FDIAs with different attack strengths, we change the injected bias to the state variables. The bias injected into the state variables ranges from 0.1 to 1. We observe that the detection performance increases with the increase of attack strength. It is because when the injected attack vector increases, the robustness of the Kalman filter and the exponential weighting function can adaptively suppress the increased attack strengths of FDIAs while the response of the weighted least squares estimator is real-time. Therefore, the deviation of the two estimators becomes larger and the detection index also increases. For example, if the introduced state errors to both state variables x_1 and x_2 are the same, FDIA can be easily detected when both state variables are simultaneously attacked, compared with cases that only one state variable is attacked as shown in the Fig. 6(a). It is reasonable that not all the state variables are attacked thus that the influence of FDIA is not significant. The detection performance is about the same when only one state variable is attacked with the increase of the attack strength. Fig. 6(b) shows the amount of improvement of the proposed detector by using the exponential weighting function. Compared with the case without the exponential weighting function in the introduced Kalman filter, we can observe that when the attack strength of FDIAs is smaller than 0.4, the detection performance of our proposed detector with the exponential weighting function is slightly improved. It is because a smaller false data injection to meter measurements does not lead a large

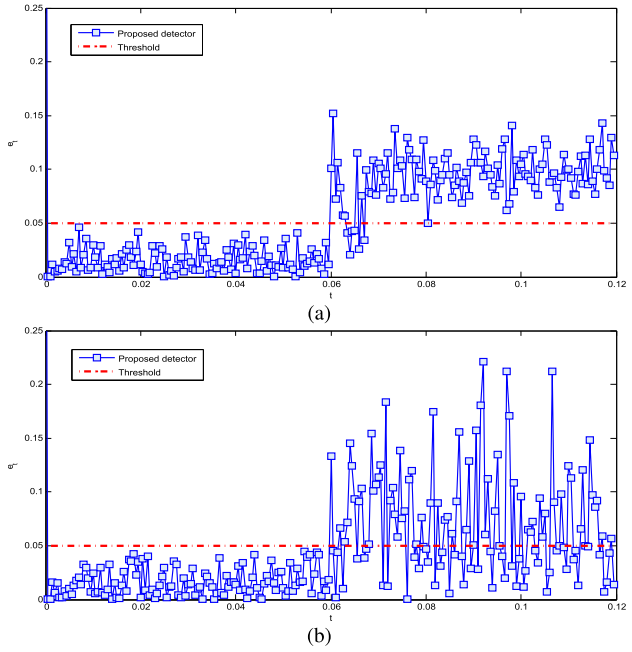

FIGURE 7. Detection performance of proposed deviation-based detection method for (a) step attacks. (b) random attacks.

deviation to the estimated states. However, when the attack strength of FDIAs is bigger than 0.4 and with the increase of attack strength, the influence leading to the deterioration of estimation performance can be better suppressed by the exponential weighting function in the Kalman filter. The improvement of detection performance by using exponential weighting function can be obviously reflected. Specifically, when attack strength of FDIAs is smaller than 0.4, the power of the exponential weighting function in Equation (13) does not change too much. Then, after the update of measurement noise covariance $\boldsymbol{R}$ in Equation (8), the Kalman gain $\boldsymbol{K}$ becomes slightly smaller. Subsequently, the estimated measurements of the Kalman filter also decrease a little and the difference between the Kalman filter and the weighted least squares estimator becomes larger. However, the difference does not increase too much compared with the case without the exponential weight function in our proposed detector. When the attack strength of FDIAs is bigger than 0.4, the power of the exponential weighting function in Equation (13) becomes large and the measurement noise covariance thus has a big change. Then the Kalman gain and the estimated measurements become much smaller. Finally, the difference between two estimators becomes more obvious. Overall, the detection performance of our proposed detector is better than that without using the exponential weight function.

The estimation results of the weighted least squares estimator are obtained at every current time slots, and when FDIAs occur, the estimation results are incorrect. The estimation results of the weighted least squares estimator are obtained at every current time slots, and when FDIAs occur, the estimation results are incorrect. But the estimation results of the Kalman filter have an adjustment process of state variables when the FDIA occurs. Finally, the estimation results of Kalman filter are also incorrect as shown in Fig. 5(a) and Fig. 5(b). The reason is that as the sampling and estimation proceed, the estimation results of two estimators are both incorrect and the small lag of the two estimators makes the FDIA undetected.

Although the stealthy FDIA is difficult to detect, there are still some other types of attacks in smart grid, such as step attacks and random attacks. A step attack involves adding a positive or negative value to the original measurements. A random attack usually adds random interference to real measurements. Despite these attacks can be detected by traditional residual-based methods, our proposed deviation-based detection method can also detect these attacks effectively. The results are shown in Fig. 7(a) and Fig. 7(b), in which these attacks are also launched at the second half of the observation period.

VI. CONCLUSION AND FUTURE WORK

In this paper, from the perspective of detection-based defense against coordinated FDIAs, we propose a deviation-based robust detection method in smart grid. To monitor state variables and estimated measurements more effectively, an additional Kalman filter estimator is introduced for real-time dynamic state estimation with the historical states' transitions. The impact of FDIAs incurs an adjustment process in the Kalman filter based on state space model, while the response of the traditional weighted least squares estimator is realtime at each time slot. The existence of the discrepancy of the proposed two estimators allows FDIAs to be effectively detected. We have also applied the exponential weighting function to enhance the robustness of the Kalman filter against attacks, and the detection performance is improved. Moreover, the proposed detection method can also detect other types of attacks, such as random attacks and step attacks and the detection performance is very good. Finally, experimental results have demonstrated the effectiveness and reliable response of proposed deviation-based detection method. In future work, since there exists continuous variations of loads and generation fluctuations in smart grid, the time-variant state transition matrix updating methods will be studied. Faults can cause the transmitted meter measurements lose in the transmission process. The new introduced Kalman estimator can obtain priori estimation of states and measurements based on normal historical data and prior information. If some meter measurements are lost, these missing measurements can be replaced by estimated measurements to improve the reliability of state estimation. Furthermore, we will study the identification of the attack strength and the time occurrence of attacks in smart grid.

REFERENCES

[1] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," *Future Gener. Comput. Syst.*, vol. 28, no. 2, pp. 391–404, Feb. 2012.

[2] P. Lynggaard, "Using neural networks to reduce sensor cluster interferences and power consumption in smart cities," *Int. J. Sens. Netw.*, vol. 32, no. 1, pp. 25–33, 2020.
[3] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 4th Quart., 2012.
[4] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *Int. J. Electr. Power Energy Syst.*, vol. 104, pp. 169–177, Jan. 2019.
[5] L. Chen, J. Liu, and W. Ha, "Cloud service security evaluation of smart grid using deep belief network," *Int. J. Sens. Netw.*, vol. 33, no. 2, pp. 109–121, 2020.
[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.
[7] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.
[8] A. Abur and A. G. Expoisito, *Power System State Estimation: Theory and Implementation*, 1st ed. New York, NY, USA: Marcel Dekker, Mar. 2004.
[9] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, Chicago, IL, USA, 2009, pp. 21–32.
[10] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
[11] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, Jan. 2018.
[12] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Syst. (CPSWeek)*, Stockholm, Sweden, Apr. 2010, pp. 1–9.
[13] J. Jiang and Y. Qian, "Defense mechanisms against data injection attacks in smart grid networks," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 76–82, Oct. 2017.
[14] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.
[15] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.
[16] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.
[17] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.
[18] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101994.
[19] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.
[20] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal PMU placement-based defense against data integrity attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1735–1750, Jul. 2017.
[21] A. Giani, R. Bent, and F. Pan, "Phasor measurement unit selection for unobservable electric power data integrity attack detection," *Int. J. Crit. Infrastruct. Protection*, vol. 7, no. 3, pp. 155–164, Sep. 2014.
[22] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
[23] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.
[24] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.
[25] M. N. Kurt, Y. Yilmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.
[26] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.
[27] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.
[28] B. B. Alagoz, M. Erturkler, and C. Yeroglu, "A theoretical investigation on moving average filtering solution for fixed-path map matching of noisy position data," *Int. J. Sensor Netw.*, vol. 29, no. 4, pp. 213–225, 2019.
[29] Y. Jiang and Q. Hui, "Kalman filter with diffusion strategies for detecting power grid false data injection attacks," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, Lincoln, NE, USA, May 2017, pp. 254–259.
[30] Z. Shen, G. Yao, Q. Xie, and F. Jiang, "Optimisation of delay tolerance in wireless sensor networks based on unscented Kalman filter estimation," *Int. J. Sens. Netw.*, vol. 33, no. 2, pp. 63–73, 2020.
[31] B. D. O. Anderson and J. Moore, *Optimal Filtering*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1979.
[32] Q. Yang, L. Chang, and W. Yu, "On false data injection attacks against Kalman filtering in power system dynamic state estimation," *Secur. Commun. Netw.*, vol. 9, no. 9, pp. 833–849, Jun. 2016.
[33] H. Qi, X. Wang, L. M. Tolbert, F. Li, F. Z. Peng, P. Ning, and M. Amin, "A resilient real-time system design for a secure and reconfigurable power grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 770–781, Dec. 2011.
[34] M. B. Do Coutto Filho and J. C. S. de Souza, "Forecasting-aided state estimation—Part I: Panorama," *IEEE Trans. Power Syst.*, vol. 24, no. 4, pp. 1667–1677, Nov. 2009.
[35] R. Arghandeh, "Micro-synchrophasors for power distribution monitoring, a technology review," May 2016, *arXiv:1605.02813*. [Online]. Available: http://arxiv.org/abs/1605.02813

CHAO PEI is currently pursuing the Ph.D. degree in control theory and control engineering with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China. He is also pursuing the Ph.D. degree with the Department of Computer Science, The University of Alabama. His research interests include cyber physical security of smart grid, power system state estimation, PMU deployment, and signal processing.

YANG XIAO (Fellow, IEEE) received the B.S. and M.S. degrees in computational mathematics from Jilin University, Changchun, China, and the M.S. and Ph.D. degrees in computer science and engineering from Wright State University, Dayton, OH, USA. He is currently a Full Professor with the Department of Computer Science, The University of Alabama, Tuscaloosa, AL, USA. He has published over 290 SCI-indexed journal articles (including over 50 IEEE/ACM transactions papers) and over 250 EI indexed refereed conference papers and book chapters related to these research areas. His current research interests include cyber-physical systems, the Internet of Things, security, wireless networks, smart grid, and telemedicine. He was a Voting Member of the IEEE 802.11Working Group, from 2001 to 2004, involving the IEEE 802.11 (WIFI) standardization work. He is an IET Fellow (previously IEE) (FIET). He currently serves as the Editor-in-Chief for *Cyber-Physical Systems* (Journal). He had (s) been an Editorial Board or Associate Editor for 20 international journals, including the IEEE TRANSACTIONS ON CYBERNETICS, since 2020, the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, from 2014 to 2015, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, from 2007 to 2009, and the IEEE COMMUNICATIONS SURVEY AND TUTORIALS, from 2007 to 2014. He has served (s) as a Guest Editor for over 20 times for different international journals, including the IEEE NETWORK, the IEEE WIRELESS COMMUNICATIONS, and ACM/Springer *Mobile Networks and Applications* (MONET).

WEI LIANG (Senior Member, IEEE) received the Ph.D. degree in mechatronic engineering from the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China, in 2002. She is currently a Professor with the Shenyang Institute of Automation, Chinese Academy of Sciences. As a Primary Participant/a Project Leader, she developed the WIA-PA and WIA-FA standards for industrial wireless networks, which are specified by IEC 62601 and IEC 62948, respectively. Her research interests include industrial wireless sensor networks and wireless body area networks. She received the International Electrotechnical Commission 1906 Award, in 2015, as a Distinguished Expert of industrial wireless network technology and standard.

XIAOJIA HAN is currently pursuing the Ph.D. degree in measurement technology and automatic equipment with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China. She is also visiting The University of Alabama. Her research interests include sensor and actuator fault detection methods, smart grid, and signal processing.