SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:833–849
Published online 27 August 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.835

SPECIAL ISSUE PAPER

On false data injection attacks against Kalman filtering in power system dynamic state estimation

Qingyu Yang[1], Liguo Chang[1] and Wei Yu[2]*

[1] Xi'an Jiaotong University, Xi'an, China
[2] Towson University, Towson, MD, U.S.A.

ABSTRACT

State estimation is a very critical component in smart grid, a typical energy-based cyber-physical system. Kalman filter has been widely used in the dynamic state estimation of power systems. Although a large number of research efforts have been made on the robustness and filtering effectiveness, little effort has been conducted on cyber attacks against Kalman filtering. To address this issue, in this paper we systematically compare three representative Kalman filtering techniques and formalize the problem of anomaly detection against false data injection attacks in Kalman filter. On the basis of our modeling results, we investigate five novel attack approaches that can bypass the anomaly detection. To defend against those attacks, we develop two countermeasures: the enhancement of Kalman filtering and the temporal-based detection algorithm. We conduct extensive performance evaluation and our data validates our theoretical finding well. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS

smart grid; Kalman filter; dynamic state estimation; false data injection attack; countermeasures

***Correspondence**

Wei Yu, Towson University, Towson, MD, U.S.A.
E-mail: wyu@towson.edu

1. INTRODUCTION

Smart grid is a typical cyber physical system (CPS) [1,2] which integrates a physical power transmission system with the cyber process of network computing and communication. It supplies electric power from generators through power transmission and distribution networks to large geographical areas. In a power grid, *supervisory control and data acquisition (SCADA) systems* collect the real time information of power field and report the collected information to the control center. To provide reliable and secured electricity service operations, real-time monitoring is essential for both system operators and customers, as it provides rich and pertinent information on the condition of a power-grid based on the measurements of meters deployed at critical locations of power grid.

State estimation is a very critical component in smart grids that monitor and control the grid operation. The traditional state estimation mainly reflects the static state characteristics of power systems, denoted as the static state estimation. The static state estimation uses telemetered data from the supervisory control and data acquisition system per several seconds and applies the weighted least squares (WLS) to obtain the best fit estimation of static state variables, for example, bus voltage magnitudes and phase angles. One shortcoming of these static estimation techniques is the accuracy, posing the missing detection of abnormal behaviors. Differently, dynamic state estimation can obtain complete, coherent, and real-time dynamic states, including the generator speeds, rotor angles, and others.

Kalman filtering techniques have been widely used in the dynamic state estimation of power systems. The traditional state estimation of power systems is based on the steady system state model [3] that only reflects static states. With Kalman filtering, the dynamic state estimation can be used to dynamically predict system states and control the system. Kalman filter can not only provide the prediction through the dynamic system model and previous estimation of system states but also obtain the optimal estimate of power systems through meter measurements deployed in the field. In particular, measurements can be conducted through phasor measurement units (PMU) and processed by the dynamic state estimator to filter measurement noise and detect gross errors. The output of dynamic state estimation can be used by other grid applications at the control

center, including the contingency analysis, optimal power flow, economic dispatch, and others [4].

The dynamic state estimation was initially developed in 1970s [5] when Kalman filtering was applied to improve the computational performance of steady state estimation in power systems. After that, a number of techniques to conduct the dynamic state estimation in power systems have been developed [3,6–14]. In particular, the linear extended Kalman filter (EKF) [10] is a popular one that provides the optimal state estimation for power systems. However, once the system is encountered, measurement errors or large load changes, the performance of EKF could decline noticeably. To overcome this limitation, the enhanced EKF [15] and M-estimation and unscented Kalman filter (UKF) [12] were proposed to incorporate with nonlinear measurement functions. We would like to point out that although a number of research efforts have been made on improving the performance of Kalman filtering such as robustness to deal with random noise [15], little effort has been conducted on cyber attacks such as false data injection attacks against Kalman filtering.

To address this issue, in this paper we investigate false data injection attacks against Kalman filtering in the dynamic state estimation of power systems and develop countermeasures to defend against those attacks. Note that the adversary can inject false measurement reports to the controller through compromised nodes and disrupt system operation. Those attacks that are generally denoted as false data injection threats could pose dangerous threats to the smart grid. To this end, we first review and compare several representative Kalman filter techniques and formalize the anomaly detection problem in the Kalman filter. Based on our modeling results, we then investigate five attack approaches that can bypass the anomaly detection. In addition, we discuss the impact of false data injection attacks on other key functional modules of smart grid.

We conduct extensive experiments on IEEE 14-bus, 30-bus, and 118-bus systems to validate the effectiveness of our investigated attacks. Our data shows that our proposed attacks can effectively reduce the performance of Kalman filtering. To mitigate such attacks, we develop two defensive mechanisms: one is enhancing UKF technique to improve the resilience of Kalman filter, and the other is adopting the temporal-based detection algorithm. We implement our proposed countermeasures on IEEE 14-bus, 30-bus, and 118-bus systems. Our experimental data shows that the enhanced UKF technique achieves the best performance than other Kalman filtering techniques to deal with random benign noise and reduce the impact of attacks to some extent. Our experimental data show that our temporal-based detection can identify compromised meters accurately and quickly.

To the best of our knowledge, our research is the first on studying the impact of false data injection attacks on Kalman filtering in the dynamic state estimation of power systems. The remainder of this paper is organized as follows: In Section 2, we review the related work. In Section 3, we briefly discuss smart grid and state estimation and introduce threat model. In Section 4, we review and compare the three representative Kalman filtering techniques. In Section 5, we formalize the anomaly detection problem in the Kalman filter and investigate five attack approaches that can bypass the anomaly detection. In Section 6, we analyze the deviation of state estimation under these attacks. In Section 7, we develop two countermeasures against false data injection attacks. In Section 8, we show the experimental results of those attacks and corresponding countermeasures. Finally, we conclude the paper in Section 9.

2. RELATED WORK

We now briefly review some of the research efforts related to our study, including the smart grid security, cyber attacks against state estimation, and Kalman filter techniques. With the development of the smart grid, a number of efforts have been paid on the cyber security of smart grid [16–19]. For example, Teixeira *et al*. [16] analyzed the cyber security of state estimators in SCADA system operation in power grids and proposed the stealthy deception attacks under perturbed linear and nonlinear estimators and developed a protection tool against such attacks in SCADA. Xie *et al*. [19] analyzed the potential financial misconduct in electricity markets under false data injection attacks against the state estimation in deregulated electricity markets.

State estimation is a very critical component in smart grid, which monitors and controls the smart grid operation in desired states. In the recent past, there are some research efforts on false data injection attacks against the static state estimation in power systems. For example, Liu *et al*. [20] showed that the adversary with the knowledge of grid system configuration can bypass the traditional bad data detection and identification algorithms so that the results of static state estimation can be manipulated. Using the developed attack schemes, the adversary can construct the attack vector and change the results of static state estimation arbitrarily. After this work, a number of research efforts have been conducted to study the false data injection attacks against power system static state estimation and countermeasures [18,19,21–24].

Different from the static state estimation, the dynamic state estimation can obtain complete, coherent, and real-time dynamic states such as generator speeds, rotor angles, and others. In the past, a number of research efforts have been conducted to improve the performance of dynamic state estimate in power systems [10–12,15]. Note that Kalman filtering techniques were initially proposed to use for the dynamic state estimation by Debs *et al*. [5]. After that, a number of research efforts have been conducted to improve its performance in power systems to conduct the dynamic state estimation [10–12,15]. For example, based on the EKF technique, Mandal *et al*. [11] proposed two algorithms for conducting the dynamic state estimation

DOI: 10.1002/sec

that incorporate the nonlinearity of measurement functions in the EKF technique. Shih *et al*. [15] proposed an improved technique using the exponential function to increase the robustness of the EKF technique. Valverde *et al*. [12] introduced the UKF technique to deal with a highly nonlinear model of network equations in power systems. Ghahremani *et al*. [10] developed an EKF technique for dynamic state estimation for a synchronous machine by using PMU quantities and proposed an EKF with unknown inputs to identify and estimate the states and unknown inputs of the synchronous machine simultaneously.

Although a number of research efforts have been conducted on improving the performance of the Kalman filtering, little effort has been conducted on cyber attacks against Kalman filtering in the dynamic state estimation of power systems. Different from the existing research efforts, our research is the first on studying the impact of false data injection attacks on the performance of Kalman filtering in the dynamic state estimation of power systems.

3. PRELIMINARIES

In this section, we first introduce the smart grid and discuss dynamic state estimation. After that, we introduce the attack model.

3.1. Smart grid

The smart grid is a completely modernized electricity delivery system that uses modern information, communications, and control technology to detect, protect and optimize the operation of interconnected elements. Smart grid is designed to improve the electric system's reliability, security, and efficiency through the two-way communication of both electricity and information [25]. To transform the existing power grid to the one that functions more intelligently, the smart grid not only takes advantage of modern communication and sensing/measurement technologies but also incorporates renewable energy resources. For example, to improve the electricity distribution and management, the modern measurement technologies such as PMUs are considered. To provide better situation awareness of the grid, PMUs can collect 30 to 60 data points per second, whereas the traditional SCADA systems collect one data point per second. Through the aid of communication, signal processing, control, and computation technologies, the smart grid enables the power grid to be smarter.

3.2. State estimation

State estimation has been widely used by the energy management systems (EMS) to monitor and control the power grid and make it operate in desired states. State estimation plays an important role in the monitoring and controlling of the grid. As the input of other modules, the results of state estimation can affect the grid operation significantly. For example, on August 14, 2003, the power grid failure in northeastern America resulted in the largest blackout in history, affecting around 50 million people in major US and Canadian cities, including New York, Cleveland, Detroit, Toronto, and Ottawa [26]. The direct reason of this accident is that bushes beneath the 345-KV line fired, leading to line short-circuit disconnection. The other main reason of this power outage is due to an error in state estimation in the regional grid dispatch center. The dispatcher could not recognize the short circuit of the line and the error led to a series of chain reactions and expanded the affect of accident.

Another example is the Portugal blackout on May 10, 2000 [27]. A stork's nest tangled in power lines was thought plunged Lisbon and the southern half of Portugal into darkness. In this accident, because of the error in state estimation at the control center, the automatic protection system at a major substation in *Rio Maior*, 50 miles north of Lisbon, did not function and the short circuit led to a domino effect that knocked out other substations further south.

3.3. Attack model

The smart grid is under the serious risk of cyber attacks because of its dependence on cyber infrastructure [28]. An adversary may launch cyber attacks by compromising the meter or sensor and hacking the communication networks in the smart grid [20,29–31]. For example, the Stuxnet worm found in July 2010 that targeted the SCADA system in the process control system raises new questions about power grid security [32].

We assume that the measurements of power systems are conducted through a sensor network that consists of m sensors with a measurement vector $y_k = \{y_{k,1}, \cdots, y_{k,m}\}$. Here $y_{k,i}$ is the measurement from sensor i at time k. All sensors should have a range that defines the bound of y_i for all k. That is, all sensors have minimum and maximum values $\forall k, y_{k,i} \in \left[y_i^{min}, y_i^{max}\right]$. Let $\Gamma_i = \left[y_i^{min}, y_i^{max}\right]$. We assume the sensor measurement $y_{k,i}$ is bounded by Γ_i.

Denote $z(k) \in \mathbb{R}^p$ as received measurements at the state estimator at time k. Based on these measurements, the state estimator approximates the power system states. If some of the sensors are under attack, $z(k)$ may be different from the real measurement y_k. We assume that the element in received measurement $z_{k,i}$ is bounded by Γ_i. Note that signals beyond this bound can be easily detected.

Denote $K_a = \{K_b, \cdots, K_s\}$ as the attack duration that begins with the time of K_b and ends at the time of K_s. A general model for received measurements is defined by the following:

$$z_{k,i} = \begin{cases} y_{k,i} & \text{for } k \notin K_a \\ y_{k,i} + c_{k,i} & \text{for } k \in K_a, y_{k,i} + c_{k,i} \in \Gamma_i \end{cases} \quad (1)$$

Table I. Notation.

k	Time slot.
x_k	State variable vector at time k.
y_k	Measurement vector in a sensor at time k.
z_k	Received measurement vector at the state estimator at time k.
u_k	Measurable input at time k.
w_k	Process (state) noise at time k.
v_k	Measurement noise at time k.
f	The system function.
h	The output function.
Q_k	Model error variance.
R_k	Measurement error variance.
$\hat{x}_k^-$	The prediction of x_k.
P_k^-	The prediction of P_k.
K_k	Kalman gain matrix.
$\hat{x}_k^+$	The estimation of x_k.
$\mathbf{a}_k$	Malicious errors that are added to the original estimates $\hat{x}_k^+$ at time k.
$\mathbf{c}_k$	Nonzero attack vector at time k.
$\hat{x}_k^{++}$	State estimation at time k after the attack is included.

where $c_{k,i}$ is the attack signal. This generic attack model can be used to represent false data injection attacks in this paper. In terms of false data injection attacks, we assume that if adversaries compromise sensors, they can inject arbitrary values that can bypass the detection by the anomaly detection algorithms. Hence, $c_{k,i}$ is an arbitrary nonzero value.

4. KALMAN FILTERING TECHNIQUES

In this section, we review and compare the three representative Kalman filtering techniques, including the EKF [10], the UKF [12], and the enhanced EKF [15]. The notations in this paper are listed in Table I.

4.1. Extended Kalman filter technique and enhanced extended Kalman filter technique

In the following, we first review the EKF technique [10] and then review the enhanced EKF technique [15,33].

4.1.1. Extended Kalman filter technique.

The EKF technique [10] considers both incoming measurements and predicted states to obtain the optimal estimates of system states. The EKF technique consists of a two-stage recursive process of prediction and filtering. The state equations and measurement equations in power systems are as follows

$$\begin{cases} x_k = f(x_{k-1}, u_{k-1}, w_{k-1}) \\ z_k = h(x_k, u_k, v_k) \end{cases} \tag{2}$$

where z_k and x_k are the measurable output and state variable vector at time k (subscript k represents time slots), respectively, u_k is the measurable input, w_{k-1} the process (state) noise, v_k the measurement noise, f the system function, and h the output function. Assume that measurements from PMU use the discrete sampling time instant k. The noise sequences v_k and w_k are supposed to be white Gaussian and independent with a zero mean and covariance matrices R_k and Q_k, respectively. Here Q_k and R_k are model error variance and measurement error variance, respectively. With the knowledge of the power system model, steps in EKF algorithm can be listed as follows:

Step 1: prediction step.

$$\begin{cases} \hat{x}_k^- = f\left(\hat{x}_{k-1}^+, u_{k-1}, 0\right) \\ P_k^- = F_{k-1} P_{k-1}^+ F_{k-1}^T + L_{k-1} Q_{k-1} L_{k-1}^T \end{cases} \tag{3}$$

where $F_{k-1} = \frac{\partial f}{\partial x}\left(\hat{x}_{k-1}^+, u_{k-1}, 0\right)$ and $L_{k-1} = \frac{\partial f}{\partial w}\left(\hat{x}_{k-1}^+, u_{k-1}, 0\right)$.

Step 2: Filtering step.

$$\begin{cases} K_k = P_k^- H_k^T \left(H_k P_k^- H_k^T + M_k R_k M_k^T\right)^{-1} \\ \hat{x}_k^+ = \hat{x}_k^- + K_k \left[y_k - h\left(\hat{x}_k^-, 0\right)\right] \\ P_k^+ = (I - K_k H_k) P_k^- \end{cases} \tag{4}$$

where $H_k = \frac{\partial h}{\partial x}\left(\hat{x}_k^-, u_k, 0\right)$ and $M_k = \frac{\partial h}{\partial v}\left(\hat{x}_k^-, u_k, 0\right)$. The detailed description of EKF algorithm can be found in [34].

The EKF technique is effective and applicable to linear systems. We can approximate the power system through a linear system in the normal operation condition. Then EKF technique is applied to achieve an accurate prediction. Nevertheless, EKF technique ignores the nonlinearity of measurement functions. When the system load or generator output power mutates, ignoring the second-order and higher order terms can have impact on the accuracy of estimation. In addition, the distribution of the power system state may not follow the Gaussian distribution and the EKF technique can incur errors as it assumes that the distribution of states follows the Gaussian distribution.

4.1.2. Enhanced extended Kalman filter technique.

The enhanced EKF technique [15,33] incorporates the nonlinearity of the measurement function and embeds the exponential weight function in the filtering process. The enhanced EKF technique consists of the following two steps: prediction and filtering. The state equation in the enhanced EKF is linear, different from the linear state equation in EKF. The form of prediction step in the enhanced EKF is the same as it in EKF. In the filtering step, it formulates an objective function, replaces W_k (W_k representing k^{th} diagonal element in the diagonal matrix W and W is the diagonal matrix of weighting factors for each measurement) by $W_k \times \exp\left(-\left|z_k - h\left(\hat{x}_k^-\right)\right|\right)$, and minimizes the

objective function in terms of the state vector. After that, it then uses the Taylor series to expand $h(\hat{x}^+)$ in term of $\hat{x}^-$ while ignoring the high-order terms. Hence, we can take the second-order term into account [33] and the nonlinearity of measurement function can be well incorporated. After that, the result can be substituted into the derivative of objective function and the results of filtering step can be obtained.

The enhanced EKF technique can effectively improve the performance and robustness in comparison with the EKF technique. First, it improves the performance by incorporating the nonlinearity of measurement functions, especially when sudden large load and/or generation changes occur [11]. Second, the enhanced EKF technique replaces the weight function of W by $W * exp(-|z - h(x)|)$. Once a raw measurement encounters a significant deviation that results in the increase of absolute residual vector, the inversion of absolute of residual vector can suppress the impact. In this way, the estimation performance can be maintained.

4.2. Unscented Kalman filter technique

The UKF technique [12] is based on the application of the unscented transformation along with the Kalman filter. The state equations and measurement equations in the power system are the following:

$$\begin{cases} x_k = f(x_{k-1}, k-1) + q_{k-1} \\ z_k = h(x_k, k) + r_k \end{cases} \tag{5}$$

where z_k and x_k are the measurable output and state variable vector at time k, respectively, q_{k-1} and r_k are the system noise and measurement Gaussian noise, with zero mean and uncorrelated covariance matrices Q and R. Note that functions f and h are nonlinear equations that represent the system and measurements models in terms of the state variables and other system inputs. The UKF technique consists of the following three steps:

Step 1: sigma points calculation. It creates a set of $2n+1$ sigma points by using the state vector x at time $k-1$ and the corresponding covariance matrix P_{k-1}

$$\begin{aligned} X_{k-1} = &\left[x^+_{k-1} \ \cdots \ x^+_{k-1}\right] \\ &+ \sqrt{c}\left[0 \ \sqrt{P^+_{k-1}} \ -\sqrt{P^+_{k-1}}\right] \end{aligned} \tag{6}$$

where $c = n + \lambda$, $\lambda = \alpha^2(n + \kappa) - n$, and $\kappa = 0$. For the purpose of the estimation initialization (i.e., when $k = 0$), the initial state vector and the initial covariance matrix have to be defined in advance according to a priori knowledge of the system.

Step 2: Kalman filter state prediction. It evaluates the set of sigma points computed in step 1 through the state-update function,

$$\hat{X}^i_k = f\left(X^i_{k-1}, k-1\right) \ i = 0, \ldots, 2n \tag{7}$$

where X^i_{k-1} is the $(i+1)^{th}$ column of matrix X_{k-1} and $\hat{X}^i_k$ is a $n \times (2n+1)$ matrix that contains the propagated sigma points. Next, it computes the predicted state mean vector $\hat{x}^-_k$ and the predicted covariance matrix P^-_k as follows:

$$\begin{cases} \hat{x}^-_k = \sum_{i=0}^{2n} W^m_i \hat{X}^i_k \\ P^-_k = \sum_{i=0}^{2n} W^c_i \left[\left(\hat{X}^i_k - \hat{x}^-_k\right)\left(\hat{X}^i_k - \hat{x}^-_k\right)^T\right] + Q_{k-1} \end{cases} \tag{8}$$

where $W^m_0 = \frac{\lambda}{n+\lambda}$, $W^c_0 = \frac{\lambda}{n+\lambda} + (1 - \alpha^2 + \beta)$, $W^m_i = \frac{1}{2(n+\lambda)}$, and $W^c_i = \frac{1}{2(n+\lambda)}$.

Step 3: Kalman filter state correction. It calculates the sigma points corresponding to the mean vector and covariance matrix of the predicted state. We have

$$X^-_k = \left[\hat{x}^-_k \ \cdots \ \hat{x}^-_k\right] + \sqrt{c}\left[0, \ \sqrt{P^-_k}\sqrt{P^-_k}\right] \tag{9}$$

It propagates the sigma points through the measurement-update function

$$Y^-_k = h\left(X^-_k, k\right) \tag{10}$$

The mean of propagated points is derived by

$$\mu_k = \sum_{i=0}^{2n} W^m_i Y^-_k \tag{11}$$

It obtains the measurement covariance matrix and the cross-covariance of state and measurement on the basis of

$$S_k = \sum_{i=0}^{2n} W^c_i \left[\left(Y^i_k - \mu_k\right)\left(Y^i_k - \mu_k\right)^T\right] + R_k \tag{12}$$

$$C_k = \sum_{i=0}^{2n} W^c_i \left[\left(X^i_k - x^-_k\right)\left(Y^i_k - \mu_k\right)\right] \tag{13}$$

It then computes the filter gain K_k, state mean $\hat{x}^+_k$, and covariance P^+_k by

$$\begin{cases} K_k = C_k S^{-1}_k \\ \hat{x}^+_k = \hat{x}^-_k + K_k[z_k - \mu_k] \\ P^+_k = P^-_k - K_k S_k K^T_k \end{cases} \tag{14}$$

The detailed description of UKF technique can be found in [35].

In the UKF technique, the nonlinear equations are not linearized as the EKF technique does. Differently, the statistical distribution of states is propagated through nonlinear equations. Hence, it can provide a better estimate of actual states and the posterior covariance matrix. In

Table II. Comparison of Kalman filtering techniques.

Techniques	EKF	UKF	Enhanced EKF
Filtering capacity	High	Highest	Higher
Time complexity	High	Highest	Higher
Jacobian matrix	Need	Not need	Need
Robustness	Common	Weaker	Stronger

EKF, extended Kalman filter; UKF, unscented Kalman filter.

Table III. Performance of mean value of performance index.

Systems	14-bus	30-bus	118-bus
EKF	0.3280	0.3372	0.3987
Enhanced EKF	0.3046	0.3133	0.3751
UKF	0.2903	0.3016	0.3629
Enhanced UKF	0.2739	0.2871	0.3561

EKF, extended Kalman filter; UKF, unscented Kalman filter.

Table IV. Computation time(s).

Systems	14-bus	30-bus	118-bus
EKF	0.103243	0.405167	10.120152
Enhanced EKF	0.114964	0.576307	17.304385
UKF	0.467665	2.999628	345.539882
Enhanced UKF	0.492641	3.042560	346.684631

EKF, extended Kalman filter; UKF, unscented Kalman filter.

addition, the UKF technique can improve the convergence speed and the robustness [12].

The comparison of those three Kalman filtering techniques is summarized in Table II. Note that the detailed evaluation of filtering capacity and time complexity can be found in Tables III and IV in Section 8, and the detailed evaluation of robustness can be found in Figures 6, 7, 8, and 9 in Section 8, which show the results of performance index under false data injection attacks. For the observation of Jacobian matrix, we can simply obtain through the principle of Kalman filtering techniques described previously.

5. ATTACK APPROACHES

In this section, we first formalize the anomaly detection in the Kalman filter and then represent five attacks to bypass the anomaly detection, followed by the discussion of those attacks.

5.1. Anomaly detection in Kalman filter

On the basis of the principle of the EKF technique in Section 4.1, we can see that the predicted state vector can be obtained after the step of prediction. From the predicted state vector, system measurements can be predicted and an innovation vector defined as the difference between the actual and predicted measurements can be determined. The innovation vector $\mathbf{v}$ can be derived by the following:

$$\mathbf{v}_k = \mathbf{y}_k - \mathbf{h}\left(\hat{\mathbf{x}}_k^-, 0\right) \tag{15}$$

where $\mathbf{y}_k$ is the original measurement vector, $\mathbf{h}\left(\hat{\mathbf{x}}_k^-, 0\right)$ is the predicted measurements, and $\hat{\mathbf{x}}_k^-$ is the predicted state. Note that $\mathbf{v}$ can be approximated by a white Gaussian process.

The benefit of using an innovation vector for time k is helping to identify the presence of anomalies through the normalized innovation vector λ_k. For the i^{th} measurement, the normalized innovation process [36] in the EKF technique is as follows:

$$\lambda_{k,i} = v_{k,i}/\rho_{k,i} \qquad i = 1, 2, \cdots, m \tag{16}$$

$$\boldsymbol{\rho}_{k,i}^2 = \mathbf{H}_{k,i}\mathbf{P}_k^-\mathbf{H}_{k,i}^T + \mathbf{M}_{k,i}\mathbf{R}_k\mathbf{M}_{k,i}^T, \qquad i = 1, 2, \cdots, m \tag{17}$$

$$\mathfrak{R}_k = \mathbf{H}_k\mathbf{P}_k^-\mathbf{H}_k^T + \mathbf{M}_k\mathbf{R}_k\mathbf{M}_k^T \tag{18}$$

where $\mathbf{H}_k = \frac{\partial \mathbf{h}}{\partial \mathbf{x}}\left(\hat{\mathbf{x}}_k^-, \mathbf{0}\right)$ and $\mathbf{M}_k = \frac{\partial \mathbf{h}}{\partial \mathbf{v}}\left(\hat{\mathbf{x}}_k^-, \mathbf{0}\right)$, $v_{k,i}$ is the i^{th} component of $\mathbf{v}_k$, $\mathbf{H}_{k,i}$ and $\mathbf{M}_{k,i}$ is the i^{th} row of $\mathbf{H}_k$ and $\mathbf{M}_k$, respectively; $\mathbf{P}_k^-$ is the error covariance matrix of prediction step, $\mathbf{R}$ is the error covariance matrix of measurement. When the anomaly exists, the hypothesis $|\lambda_{k,i}| \leq \lambda_{max}\ \forall i(i \in m)$ will not hold. Note that the selection of λ_{max} is based on the diagonal entries of $\mathfrak{R}_k$.

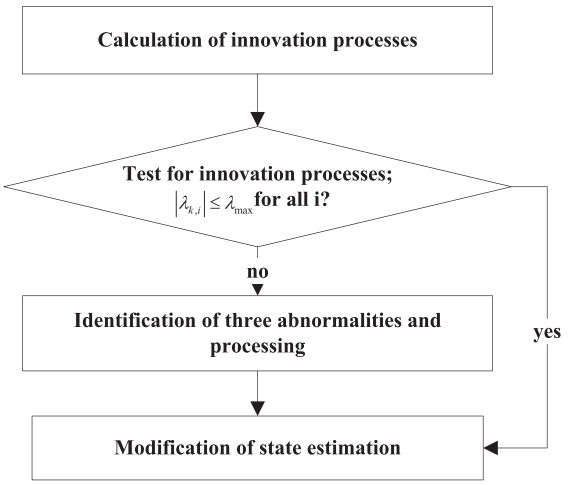

Figure 1. Workflow of anomaly detection.

Figure 1 illustrates the workflow of anomaly detection. As we can see that once the anomaly is detected, the next step is to identify three abnormalities (e.g., occurrence of bad data, sudden variation of states, and changes in network configuration) and take the corresponding action. If the first step in the anomaly detection can be bypassed (i.e., if $|\lambda_{k,i}| \leq \lambda_{max}\ \forall i(i \in m)$), the anomaly detection algorithm cannot issue alert and Kalman filter can continue to

execute. The detailed steps of anomaly detection algorithm is shown in Algorithm 1.

Algorithm 1 Anomaly Detection Algorithm

```
Input:
  y_k: Original measurement vector at time k;
  h(x̂_k^-, 0): Predicted measurement vector at time k.
Parameters:
  λ_max: Determined by the diagonal entries of ℜ_k;
  ρ_{k,i}: The i^th diagonal element of ℜ_k.
Output: Anomaly condition happened or not.
v_k ← y_k − h(x̂_k^-, 0)
for Each element v_{k,i} in the innovation vector v_k do
    λ_{k,i} ← v_{k,i}/ρ_{k,i}
    for All i (i ∈ m) do
        if |λ_{k,i}| ≤ λ_max then
            Anomaly condition does not occur and continue to execute
        end if
        if |λ_{k,i}| > λ_max then
            Anomaly condition occurs and the abnormality is detected
        end if
    end for
end for
```

For UKF and enhanced EKF techniques, because the structure of these two techniques is similar to the EKF technique, the innovation vector and the normalized innovation vector can be derived in the same way as the one in EKF technique, except that in UKF technique, the $\Re_k$ equal to S_k, and

$$\rho_{k,i}^2 = \sum_{j=0}^{2n} W_j^c \left(\mathbf{Y}_{k,i}^{-i} - \mu_{k,i}\right)^2 + r_{k,i}^2 \tag{19}$$

where $\mathbf{Y}_{k,i}^-$ is the i^{th} row of $\mathbf{Y}_k^-$ and $r_{k,i}^2$ is the i^{th} diagonal element of $\mathbf{R}_k$.

5.2. Novel attack approaches bypassing anomaly detection

Recall that the anomaly detection algorithm is based on $|\lambda_{k,i}| \leq \lambda_{\max}\ \forall i(i \in m)$. When sophisticated false data injection attacks are used, the adversary can attack the power system effectively with the non-zero attack vector $\mathbf{c}_k$. From the anomaly detection algorithm, we have

$$\left|\frac{z_{k,i} - h_i\left(\hat{\mathbf{x}}_k^-, 0\right)}{\rho_{k,i}}\right| \leq \lambda_{\max} \tag{20}$$

where $h_i\left(\hat{\mathbf{x}}_k^-, 0\right)$ is the i^{th} element of $h\left(\hat{\mathbf{x}}_k^-, 0\right)$, and $z_{k,i}$ is the malicious measurements. We obtain the range of $z_{k,i}$ by

$$h_i\left(\hat{\mathbf{x}}_k^-, 0\right) + \lambda_{\max}\rho_{k,i} \geq z_{k,i} \geq h_i\left(\hat{\mathbf{x}}_k^-, 0\right) - \lambda_{\max}\rho_{k,i} \tag{21}$$

That is, the malicious measurement $z_{k,i}$ can be a value within the limitation and the attack vector is $\mathbf{c}_k = \mathbf{z}_k - \mathbf{y}_k$. In addition, every malicious measurement can approach its threshold at the same time. On the other hand, $\lambda_{\max}$, $\rho_{k,i}$ and $h_i\left(\hat{\mathbf{x}}_k^-, 0\right)$ can be derived between time $k-1$ and k. That is, the range of malicious measurement $z_{k,i}$ can be acquired before time k, which will pose a great threat to the estimate at time k.

We assume that the adversary knows about the anomaly detection algorithm that relies on $|\lambda_{k,i}| \leq \lambda_{\max}\ \forall i(i \in m)$. The adversary has the knowledge, including the exact nonlinear model that is used (i.e., f and h), parameters (Q and R), state estimation $\hat{x}$, error covariance matrix P and original measurements $\mathbf{y}$. In the following, we present five attack approaches in detail.

5.2.1. Maximum magnitude-based attack.

In a maximum magnitude-based attack, the adversary tends to achieve the maximum deviation of original measurements that equals to the maximum magnitude of the attack vector $|c_{k,i}|$. To achieve this goal, the received measurement $z_{k,i}$ should be manipulated furthest from the original measurement $y_{k,i}$ after adding the false data. To be drifted from the original measurement $y_{k,i}$, $z_{k,i}$ should be as follows:

$$z_{k,i} = \begin{cases} h_i\left(\hat{\mathbf{x}}_k^-, 0\right) - \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} \geq 0 \\ h_i\left(\hat{\mathbf{x}}_k^-, 0\right) + \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} < 0 \end{cases} \tag{22}$$

Based on Equation (15), the attack vector $\mathbf{c}_k$ can be derived by the following:

$$c_{k,i} = z_{k,i} - y_{k,i} = \begin{cases} -v_{k,i} - \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} \geq 0 \\ -v_{k,i} + \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} < 0 \end{cases} \tag{23}$$

We have

$$|c_{k,i}| = |z_{k,i} - y_{k,i}| = \lambda_{\max}\rho_{k,i} + |v_{k,i}| \tag{24}$$

Then, the magnitude of attack vector $|c_{k,i}|$ is maximum.

The detailed steps of maximum magnitude-based attack is shown in Figure 2. As we can see, after we acquire the power system parameters such as the model, the current estimation and error covariance matrix at time $k-1$, we compute the predicted measurements h_i, λ_{max} and $\rho_{k,i}$ at time k. Then for the next time step when the original measurement $y_{k,i}$ is received at time k, the innovation vector $v_{k,i}$ is computed and the decision of $v_{k,i} \geq 0$ can be determined. If it holds, the adversary would manipulate the received measurement $z_{k,i}$ and makes it $h_i - \lambda_{\max}\rho_{k,i}$ at time k. Otherwise, the adversary would manipulate the received measurement $z_{k,i}$ and make it $h_i + \lambda_{\max}\rho_{k,i}$. Then, the power system state at time k is obtained using the received measurements. If the adversary wants to continue the attack, the above process repeats over different times.

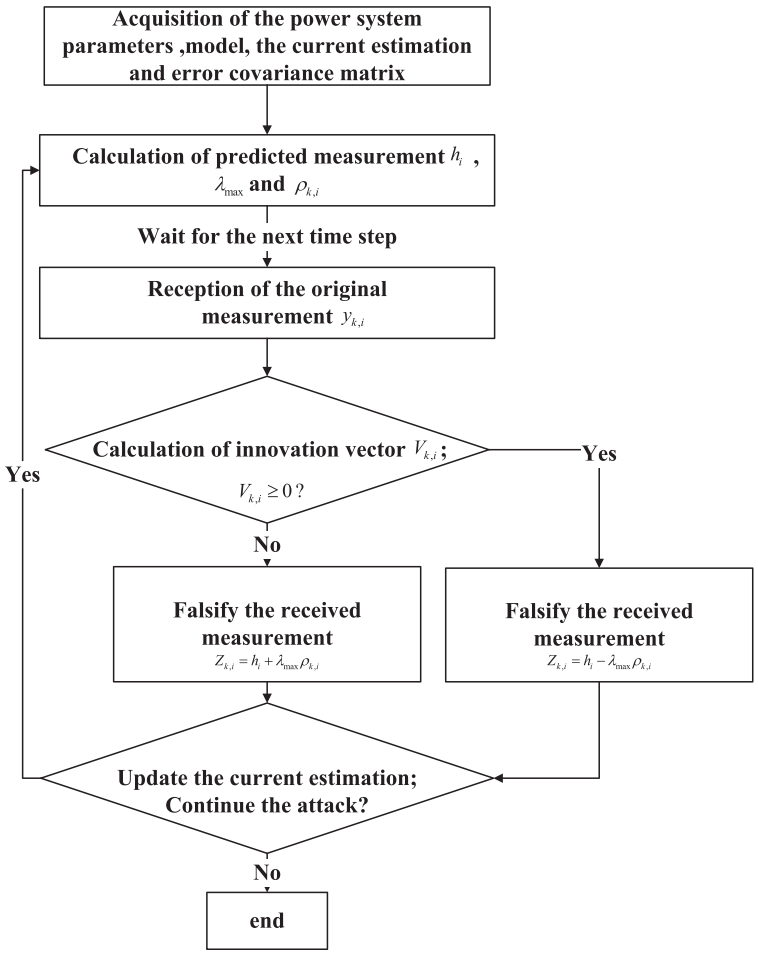

Figure 2. Workflow of maximum magnitude-based attack.

5.2.2. Wave-based attack.

Opposite to the maximum magnitude-based attack, in the wave-based attack, regardless of whether $v_{k,i}$ is positive or negative, the malicious measurements $z_{k,i}$ will be the reverse direction of injected attack data at time $k-1$.

To this end, $z_{k,i}$ is as follows:

$$z_{k,i} = \begin{cases} h_i\left(\hat{\mathbf{x}}_k^-, 0\right) - \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} < 0 \\ h_i\left(\hat{\mathbf{x}}_k^-, 0\right) + \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} \geq 0 \end{cases} \tag{25}$$

The attack vector $\mathbf{c}_k$ is as follows:

$$c_{k,i} = z_{k,i} - y_{k,i} = \begin{cases} -v_{k,i} - \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} < 0 \\ -v_{k,i} + \lambda_{\max}\rho_{k,i} & \text{if } v_{k,i} \geq 0 \end{cases} \tag{26}$$

Then, the absolute value of the element in attack vector $\mathbf{c}_k$ is as follows:

$$|c_{k,i}| = |z_{k,i} - y_{k,i}| = \lambda_{\max}\rho_{k,i} - |v_{k,i}| \tag{27}$$

The detailed steps of wave-based attack is the same as the one in the maximum magnitude-based attack, except that if $v_{k,i} < 0$, the received measurement will be set to $h_i - \lambda_{\max}\rho_{k,i}$; otherwise, the received measurement will be set to $h_i + \lambda_{\max}\rho_{k,i}$.

5.2.3. Positive deviation attack.

In the positive deviation attack, the adversary tends to achieve the maximum deviation of original measurements along with the direction of increase; that is, the malicious measurements $z_{k,i}$ are always maximum in the range of its value. Positive deviation attack can be described as

$$z_{k,i} = h_i\left(\hat{\mathbf{x}}_k^-, 0\right) + \lambda_{\max}\rho_{k,i} \tag{28}$$

The attack vector $\mathbf{c}_k$ is as follows:

$$c_{k,i} = z_{k,i} - y_{k,i} = -v_{k,i} + \lambda_{\max}\rho_{k,i} \tag{29}$$

The absolute value of the element in the attack vector $\mathbf{c}_k$ is as follows:

$$|c_{k,i}| = |z_{k,i} - y_{k,i}| = \lambda_{\max}\rho_{k,i} - v_{k,i} \tag{30}$$

DOI: 10.1002/sec

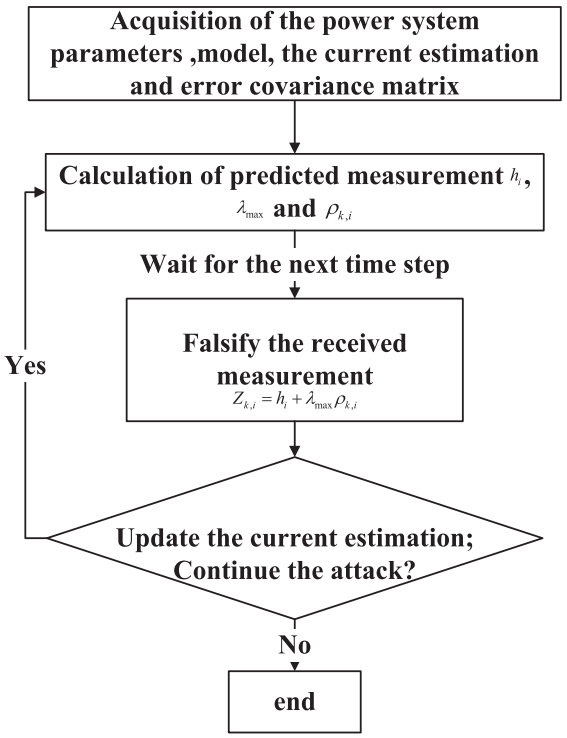

Figure 3. Workflow of positive deviation attack.

The detailed steps of positive deviation attack is shown in Figure 3.

5.2.4. Negative deviation attack.

In the negative deviation attack, the adversary tends to achieve the maximum deviation of original measurements along with the direction of decrease, that is, the malicious measurements $z_{k,i}$ are always minimum in the range of its value. In the negative deviation attack, $z_{k,i}$ should be

$$z_{k,i} = h_i\left(\hat{\mathbf{x}}_k^-, 0\right) - \lambda_{\max}\rho_{k,i} \tag{31}$$

The attack vector $\mathbf{c}_k$ is as follows:

$$c_{k,i} = z_{k,i} - y_{k,i} = -v_{k,i} - \lambda_{\max}\rho_{k,i} \tag{32}$$

The absolute value of the element in the attack vector $\mathbf{c}_k$ is as follows:

$$|c_{k,i}| = |z_{k,i} - y_{k,i}| = \lambda_{\max}\rho_{k,i} + v_{k,i} \tag{33}$$

The detailed steps in the negative deviation attack is the same as the ones in the positive deviation attack, except that the updated measurement will be set to $h_i - \lambda_{\max}\rho_{k,i}$.

5.2.5. Mixed attacks.

On the basis of the four attacks described previously as primitives, the adversary can develop other attacks by mixing those attack primitives. Taking the wave-based attack and positive deviation attack as an example, the adversary launches the wave-based attack at time k, the positive deviation attack at time $k + 1$, the wave-based attack again at time $k + 2$, and positive deviation attack at time $k + 3$ and so on. In addition, we have other alternatives such as negative/positive-mixed attack that mixes the negative deviation attack and positive deviation attack, wave/negative-mixed attack that mixes the wave-based attack and negative deviation attack, wave/positive-mixed attack that mixes the wave-based attack and positive deviation attack, and so on.

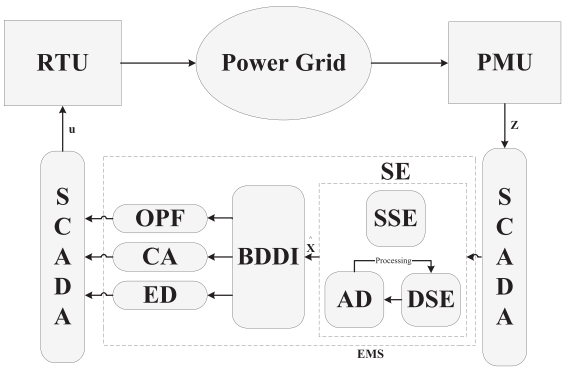

Figure 4. Workflow of smart grid system operation.

5.3. Discussion

We now discuss the false data injection attacks on smart grid. Note that results of state estimation have a great impact on other modules in power grid, including the contingency analysis (CA), optimal power flow (OPF,) economic dispatch (ED), and others. State estimation and other modules are shown in Figure 4. As we can see, PMUs measure the output data of the power grid, SCADA collects data and transfers it to the state estimator in EMS. The state estimator can be either a static state estimator or a dynamic state estimator. Note that he dynamic state estimator consists of the dynamic state estimation algorithm and the anomaly detection algorithm.

In the dynamic state estimator, the raw measurements are first processed by the dynamic state estimation algorithm to output state estimation. Then, the results of state estimation can be processed by detection algorithm. In detection algorithm, the model and data of power system can be adapted if anomaly condition is detected, and the adapted model and data will be returned to the dynamic state estimation algorithm that conduct the estimate again. If the anomaly condition does not occur, the state estimation results of dynamic state estimation algorithm will be used by other modules directly. Depending on outputs of the state estimator, the BDDI module processes the raw measurements on the basis of the estimated states and determine whether raw measurements can be used or not.

The output of BDDI will be the input of modules such as CA, OPF, and ED. After that, control decisions based on the output of these modules will be reached. In other words, if the result of state estimation is manipulated, it incurs a great impact on other modules.

State estimation is used for the case in which we have redundant equations for the system. Differently, power flow control is used for handling the case in which we have nonredundant equations. The power flow computation is based on the measurements processed by BDDI. The measurements after processing by BDDI will be the input for the power flow computation. Note that power flow computation is subject to the assumption that inputs is absolutely accurate, and as a matter of fact it is impossible in real-world practice. If the deviation of state estimation appears, the measurement processed by BDDI can have a large deviation from the true value, posing errors of power flow computation as well.

State estimation can estimate the actual switching (or connection) state in power grid based on remote measurements, and correct the occasional error switch state information to ensure the correctness of the power grid. Contingency analysis uses the outputs of state estimation. As an example, the power grid failure in northeastern America [26] discussed in Section 3.2 is a typical case in which the network topology analysis error in state estimation leads to the error in contingency analysis.

Under the circumstance of guaranteeing the safety and high quality of power production and meeting customer demand for electricity, the economic dispatch takes a variety of techniques and management measures to ensure power production equipments in a good condition and transmission electricity power in the lowest cost. To this end, the economic dispatch is a critical module in the power grid. It tends to reduce line loss of power grid and achieve the lowest cost of power generation or fuel costs. The line loss also depends on the accuracy of state estimation as its computation is based on bus voltage phasor and bus current phasor as well. If state estimation is manipulated, the computation of line loss can be misled and the economic dispatch functional modules can then be disrupted.

6. ANALYSIS OF STATE DEVIATION

In this section, we conduct the theoretical analysis of state deviation caused by attacks. We first show our analysis on the linear model of power system and then extend it to a nonlinear model of power system.

6.1. State deviation in linear model

Taking the linear model into consideration, we have the following:

$$\begin{cases} x_k = F_{k-1}x_{k-1} + G_{k-1} + w_{k-1} \\ z_k = H_k x_k + v_k \end{cases} \tag{34}$$

where F_{k-1} is an n-dimensional nonzero diagonal matrix, G_{k-1} is an n-dimensional column vector, w_{k-1} is a white Gaussian sequence with zero mean and covariance matrix Q_{k-1}, H_k is an m-dimensional nonzero measurement matrix, and v_k is a white Gaussian measurement noise error vector with zero mean and covariance matrix R_k. The parameter matrix F_{k-1} and G_{k-1} can be identified online by using a linear exponential smoothing technique for forecasting [13]. We also assume that the adversary attacks the power system between time $k-1$ and k. At this time, we have the prediction step listed in the later text.

$$\begin{cases} \hat{x}_k^- = F_{k-1}\hat{x}_{k-1}^+ + G_{k-1} \\ P_k^- = F_{k-1}P_{k-1}^+ F_{k-1}^T + Q_{k-1} \end{cases} \tag{35}$$

Then the filtering step can be described as follows:

$$\begin{cases} K_k = P_k^- H_k^T \left(H_k P_k^- H_k^T + R_k\right)^{-1} \\ \hat{x}_k^+ = \hat{x}_k^- + K_k\left(z_k - H_k\hat{x}_k^-\right) \\ P_k^+ = (I - K_k H_k)P_k^- \end{cases} \tag{36}$$

Note that the system parameters F, G, and H unchanged continuously in this case. In addition, P^-, P^+ and K are always unchanging due to the changeless of P_{k-1}^+, so only y_k can be manipulated after being attacked, that is, the state deviation that the adversary manipulates in the next step is denoted as follows:

$$\mathbf{a}_k = K_k \mathbf{c}_k \tag{37}$$

where $\mathbf{a}_k$ is malicious errors that are added to the original estimates $\hat{x}_k^+$ at time k, K_k is the Kalman gain at time k, $\mathbf{c}_k$ is the nonzero attack vector that the adversary adds to the original sensor measurement vector y_k at time k.

With the attack vector $\mathbf{c}_k$, the state at time k is as follows:

$$\hat{\mathbf{x}}_k^{++} = \hat{\mathbf{x}}_k^+ + \mathbf{a}_k \tag{38}$$

where $\hat{\mathbf{x}}_k^{++}$ is the state estimation after the attack is launched. At the next time $k+1$, we have the following:

$$\hat{\mathbf{x}}_{k+1}^{++} = F_k\hat{\mathbf{x}}_k^{++} + G_k + \mathbf{K}_{k+1}\left[\mathbf{z}_{k+1} - H_{k+1}\left(F_k\hat{\mathbf{x}}_k^{++} + G_k\right)\right] \tag{39}$$

where $\mathbf{z}_{k+1}$ is the received measurement at time $k+1$ and $\mathbf{z}_{k+1} = \mathbf{y}_{k+1} + \mathbf{c}_{k+1}$.

Then, we have the following:

$$\mathbf{z}_{k+1} = \mathbf{y}_{k+1} + \mathbf{c}_{k+1} \tag{40}$$

$$\hat{\mathbf{x}}_{k+1}^{+} = F_k\hat{\mathbf{x}}_k^{+} + G_k + \mathbf{K}_{k+1}\left[\mathbf{y}_{k+1} - H_{k+1}\left(F_k\hat{\mathbf{x}}_k^{+} + G_k\right)\right] \tag{41}$$

$$\hat{\mathbf{x}}_{k+1}^{++} = F_k\hat{\mathbf{x}}_k^{++} + G_k + \mathbf{K}_{k+1}\left[\mathbf{z}_{k+1} - H_{k+1}\left(F_k\hat{\mathbf{x}}_k^{++} + G_k\right)\right] \tag{42}$$

Substituting Equations (38), (40), and (41) into Equation (42), we have the following:

$$\hat{\mathbf{x}}_{k+1}^{++} = \hat{\mathbf{x}}_{k+1}^{+} + \mathbf{K}_{k+1}\mathbf{c}_{k+1} + (\mathbf{I} - \mathbf{K}_{k+1}H_{k+1})F_k\mathbf{a}_k \tag{43}$$

That is,

$$\mathbf{a}_{k+1} = \mathbf{K}_{k+1}\mathbf{c}_{k+1} + (I - \mathbf{K}_{k+1}H_{k+1})F_k\mathbf{a}_k \quad (44)$$

Similarly, we have the following:

$$\mathbf{a}_{k+2} = \mathbf{K}_{k+2}\mathbf{c}_{k+2} + (I - \mathbf{K}_{k+2}H_{k+2})F_{k+1}\mathbf{a}_{k+1} \quad (45)$$

and so on.

From the previous analysis, we conclude that when the attack is launched between the time $k-1$ and k, we can obtain the state deviation $\mathbf{a}_k = K_k\mathbf{c}_k$ when the adversary first launches the attack at time sample k, then the state deviation can be changed in according to following:

$$\mathbf{a}_{k+m} = \mathbf{K}_{k+m}\mathbf{c}_{k+m} + (I - \mathbf{K}_{k+m}H_{k+m})F_{k+m-1}\mathbf{a}_{k+m-1} \quad (46)$$

6.2. State deviation in nonlinear model

The linear model is useful in power system application. However, the nonlinear model fits the actual power system better. We now analyze the state deviation in the nonlinear model of the power system. From the principle of EKF techniques in Section 4.1, we have the following:

$$\begin{aligned}\hat{x}_k^+ &= \hat{x}_k^- + K_k\left[y_k - h\left(\hat{x}_k^-, 0\right)\right] \\ &= f\left(\hat{x}_{k-1}^+, 0\right) + K_k\left[y_k - h\left(f\left(\hat{x}_{k-1}^+, 0\right), 0\right)\right] \\ &= K_k y_k + f\left(\hat{x}_{k-1}^+, 0\right) - K_k h\left(f\left(\hat{x}_{k-1}^+, 0\right), 0\right)\end{aligned} \quad (47)$$

We assume that the adversary attacks the power system between time $k-1$ and k. From the principle in Section 4.1, we can see that system parameters F_{k-1}, L_{k-1}, H_k, and M_k unchanged due to the unchange of the filtering process at time $k-1$. In addition, P_k^- and K_k are not changed, so only y_k can be changed at time k, that is, the state deviation that the adversary make in the next step can be denoted as follows:

$$\mathbf{a}_k = K_k\mathbf{c}_k \quad (48)$$

where $\mathbf{a}_k$ is malicious errors that are introduced into the original estimates $\hat{x}_k^+$ at time k, K_k is Kalman gain at time k, and $\mathbf{c}_k$ is the nonzero attack vector that the adversary adds to the original sensor measurement vector y_k at time k.

With the attack vector $\mathbf{c}_k$, the state at time k is as follows:

$$\hat{\mathbf{x}}_k^{++} = \hat{\mathbf{x}}_k^+ + \mathbf{K}_k\mathbf{c}_k \quad (49)$$

where $\hat{\mathbf{x}}_k^{++}$ is the state estimation after the attack is added. At the next time $k+1$, we have the following:

$$\hat{\mathbf{x}}_{k+1}^{++} = f\left(\hat{\mathbf{x}}_k^{++}, 0\right) + \mathbf{K}_{k+1}\left[\mathbf{z}_{k+1} - h\left(f\left(\hat{\mathbf{x}}_k^{++}, 0\right), 0\right)\right] \quad (50)$$

where $\mathbf{z}_{k+1}$ is the received measurement at time $k+1$ and $\mathbf{z}_{k+1} = \mathbf{y}_{k+1} + \mathbf{c}_{k+1}$. However, the parameter $\mathbf{K}_{k+1}$ has changed as the state estimation at time k becomes $\mathbf{x}_k^{++}$.

7. COUNTERMEASURES

In this section, we investigate two countermeasures. First, we consider to enhance the resilience of the UKF technique because the UKF technique achieves the best performance in the three Kalman filtering techniques discussed in Section 4. In this way, we can reduce the impact of false data injection attacks. As this approach cannot solve the problem completely, we propose a detection algorithm to detect false data injection attacks.

7.1. Principle of the enhanced unscented Kalman filter technique

To enhance the resilience of the UKF technique, we replace the measurement noise R by $R * exp(|z - h(x)|)$. When the predicted measurement and received measurement have a large deviation, the increase of absolute residual vector makes the measurement noise larger, leading to the decrease of Kalman gain K. This will reduce the weight of received measurement in the estimation and the estimation performance can be preserved. Conversely, when the deviation between the predicted measurement and the received measurement is small, the decrease of absolute residual vector will make the measurement noise change marginally, leading to a very small impact on estimation results.

7.2. Temporal-based detection algorithm

To detect the previous attacks, we propose the temporal-based detection that uses the on-line nonparametric cumulative sum (CUSUM) change detection mechanism [37]. Generally speaking, the CUSUM change detection algorithm defines the two hypotheses: H_0 (normal condition) and H_1 (being attacked). The CUSUM change detection algorithm assumes that the observation $y(i)$ begins with H_0, and at time k_s, it changes to hypothesis H_1. The goal of this algorithm is to detect such a change as early as possible. Given a suppressed false positive rate, the CUSUM algorithms tend to minimize the time N ($N \geq k_s$), for which the test stops and determines whether a change occurs or not.

The classical CUSUM statistic is updated on the basis of the following:

$$S(k) = \left(\log\frac{p_1(y(k-1))}{p_0(y(k-1))} + S(k-1)\right)^+ \quad (51)$$

where $S(0) = 0$, $(a)^+ = a$ if $a \geq 0$ and zero otherwise, $p_1(y(k-1))$ and $p_0(y(k-1))$ is the probability distribution of $y(k-1)$ under H_1 and H_0, respectively.

The detection time can be computed by the following:

$$N = \inf_n\{n : S(n) \geq \tau\} \quad (52)$$

where τ is the threshold selected on the basis of the false positive rate.

In our experiment, the probability distribution $p_1(y(k-1))$ and $p_0(y(k-1))$ are not known. Hence, we adopt the nonparametric statistics mechanism that can avoid making assumptions about the probability distribution of attacks. Let $z_i(k)$ be the measurement of i^{th} meter at time k. We define the observation $y_i(i)$ as the following:

$$y_i(k) = \left\| z_i(k) - h_i(\hat{\mathbf{x}}_k^-, 0) \right\| - \eta_i \tag{53}$$

where η_i is determined by $E_0 \left\| z_i(k) - h_i\left(\hat{\mathbf{x}}_k^-, 0\right) \right\|$ (the expected value of $\left\| z_i(k) - h_i\left(\hat{\mathbf{x}}_k^-, 0\right) \right\|$ under H_0). The nonparametric CUSUM statistics for i^{th} measurement is as follows:

$$S_i(k) = (S_i(k-1) + y_i(k))^+, S_i(0) = 0 \tag{54}$$

Then, a decision rule can be made by the following:

$$S_i(k) \underset{H_1}{\overset{H_0}{\lessgtr}} \tau_i \tag{55}$$

where τ_i is the threshold determined on the basis of the false positive rate for the i^{th} measurement. Algorithm 2 shows the the detailed steps of temporal-based detection.

Algorithm 2 Temporal-based Detection Algorithm

1: Input:
   $z_i(k)$: Observed measurement of the i^{th} meter at time k;
   $h_i(\hat{\mathbf{x}}_k^-, 0)$: Pre-measurement of the i^{th} meter at time k.
2: Parameters:
   τ_i: Detection threshold for the i^{th} measurement;
   η_i: Determined by $E_0 \left\| z_i(k) - h_i\left(\hat{\mathbf{x}}_k^-, 0\right) \right\|$.
3: Output: i^{th} meter is compromised by attacks or not.
4: $S_i(0) = 0$
5: **for** Each measurement at time k **do**
6: $S_i(k) \leftarrow S_i(k-1) + \left\| z_i(k) - h_i\left(\hat{\mathbf{x}}_k^-, 0\right) \right\| - \eta_i$
7: **if** $S_i(k) < 0$ **then**
8: $S_i(k) \leftarrow 0$
9: **end if**
10: **if** $S_i(k) \geq \tau_i$ **then**
11: The i^{th} meter is compromised by attacks and the detection stops
12: **else**
13: Wait for measurement at next time
14: **end if**
15: **end for**

To measure the effectiveness of temporal-based detection, we consider two metrics: false positive rate and detection time. The false positive rate is defined as the probability of falsely rejecting the null hypothesis H_0 and the detection time is the average time that it takes to detect attack. Obviously, the smaller the values of both metrics, the higher performance of detection is. We show the evaluation results of the temporal-based detection by using these two metrics in Section 8.

8. PERFORMANCE EVALUATION

In this section, we conduct experiments to investigate the effectiveness of the attacks and the corresponding countermeasures.

8.1. Experimental setup

The performance of proposed attack techniques and countermeasures in Sections 5 and 7 have been validated on IEEE 14-bus, IEEE 30-bus, IEEE 118-bus systems, respectively. Note that although we conducted all experiments on IEEE 14-bus, 30-bus, and 118-bus systems, we only show the results of IEEE 14-bus and 30-bus systems in the evaluation of attack approaches and the results of IEEE 30-bus system in the evaluation of detection algorithm as the similar results on other IEEE buses can be drawn. We simulated our approaches by using MATLAB R2011b. All parameters used in our experiments, including the real value of state variables, sensor measurements, and the Jacobian matrix, are based on the MATLAB package MATPOWER [38]. We first evaluate four Kalman filtering techniques (including the enhanced UKF proposed in Section 7) under the normal condition and then evaluate the impact of attack approaches. Lastly, we evaluate the effectiveness of the temporal-based detection algorithm.

The performance comparison of four Kalman filtering was conducted based on the following performance index [12,15,39] that has been widely used to measure the filtering capacities and is defined by the following:

$$\mathbf{J_k} = \frac{\sum \left| \hat{\mathbf{Z}}_\mathbf{k}^\mathbf{i} - \mathbf{Z}_\mathbf{k}^\mathbf{i+} \right|}{\sum \left| \mathbf{Z}_\mathbf{k}^\mathbf{i} - \mathbf{Z}_\mathbf{k}^\mathbf{i+} \right|} \tag{56}$$

where $\hat{\mathbf{Z}}_\mathbf{k}^\mathbf{i}$ is the estimated measurement vector, $\mathbf{Z}_\mathbf{k}^\mathbf{i}$ is the noisy (real) measurement vector, and $\mathbf{Z}_\mathbf{k}^\mathbf{i+}$ is the true vector of measurements. Obviously, the lower performance index $\mathbf{J_k}$, the more effective the filtering algorithm is.

8.2. Evaluation results

8.2.1. Results under normal conditions.

Figure 5 shows the performance index $\mathbf{J}$ of the four Kalman filtering techniques for IEEE 14-bus, 30-bus, and 118-bus systems. Table III shows the mean value of performance index of those four filtering techniques. From Figure 5 and Table III, we can see that under the normal operation, the descending order of the performance index $\mathbf{J}$ is EKF, enhanced EKF, UKF, and enhanced UKF. This confirms that in the normal condition to handle random noise, the enhanced UKF achieves the highest filtering capacity. In Table IV, we show the computation time of those four filtering techniques. From Table IV, we can see that the computation time increases as the improvement of filtering capacity. In each recursive operation, EKF needs to compute the *Jacobian* matrix and the state equation once

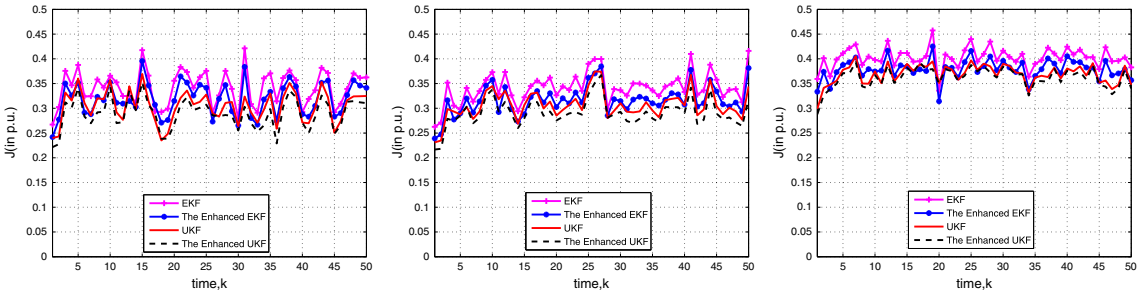

Figure 5. Performance index **J** (in per unit) under normal conditions in IEEE 14-bus, 30-bus, and 118-bus systems.

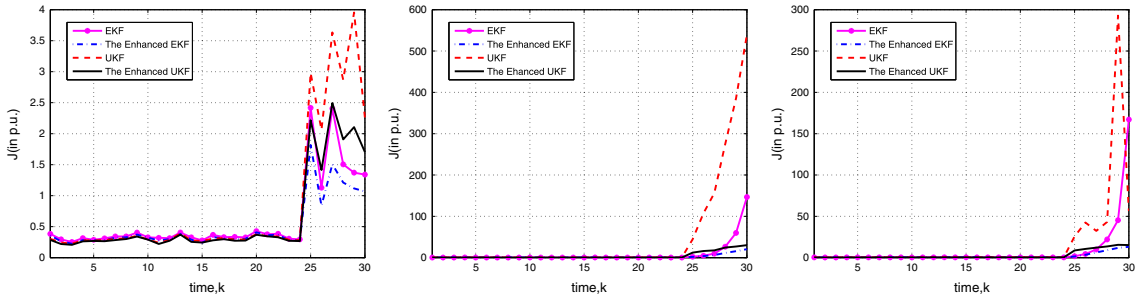

Figure 6. Performance index **J** under wave-based attack, positive deviation attack, and negative deviation attack in IEEE 14-bus system.

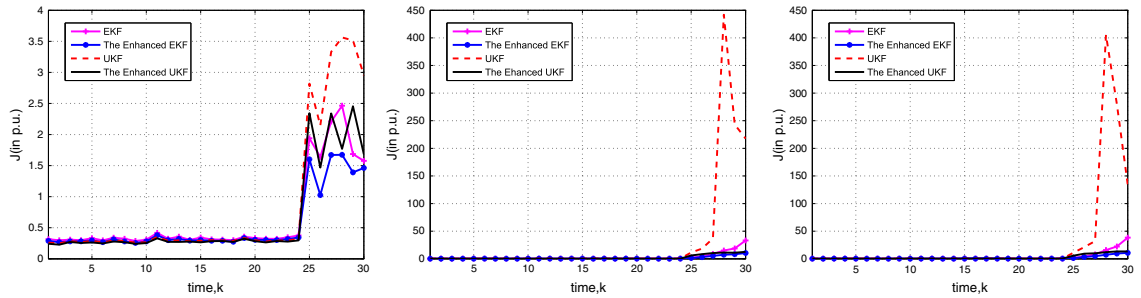

Figure 7. Performance index **J** under wave-based attack, positive deviation attack, and negative deviation attack in IEEE 30-bus system.

at every time, but UKF needs to conduct $2n+1^{\text{th}}$ computations of the state equation at every time. This makes UKF take more time to compute the state equation and a longer time in the entire process. As expected, the enhanced EKF and the enhanced UKF revised parameters in EKF and UKF that makes them take a longer time than EKF and UKF.

8.2.2. Results under false data injection attacks.

We investigate the performance index **J** under different attacks discussed in Section 5, which can bypass the anomaly detection. In the maximum magnitude-based attack, the Jacobian matrix **H** will change greatly after several steps, posing a negative innovation vector error covariance matrix $\mathfrak{R}_k$. Our experiment results indicate that the maximum magnitude-based attack can elevate performance index **J** to 10^5 after a 10-step attack, posing a substantial reduction of performance.

To verify the impact of the wave-based attack, positive deviation attack, negative deviation attack and mixed attack, we assume that the adversary launches attacks at $t \geq 25$. The curves in Figures 6, 7, 8, and 9 represent the performance index **J** of four Kalman filtering techniques after adding attacks in IEEE 14-bus and IEEE 30-bus systems, respectively. Note that after a few steps attack, Cholesky decomposition appears not positive definite in UKF. In comparison with the three curves in Figure 6, we can see that the performance index under the wave-based attack can reach 1 – 4, the performance index under the positive deviation attack and the negative deviation attack approach 10 – 600 and 10 – 300, respectively. In comparison with the three curves in Figure 7, we can see that the

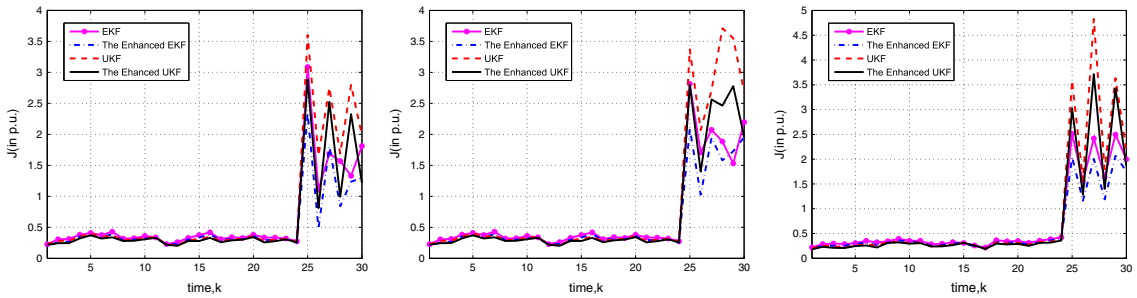

Figure 8. Performance index **J** under negative/positive-mixed attack, wave/negative-mixed attack, and wave/positive-mixed attack in IEEE 14-bus system.

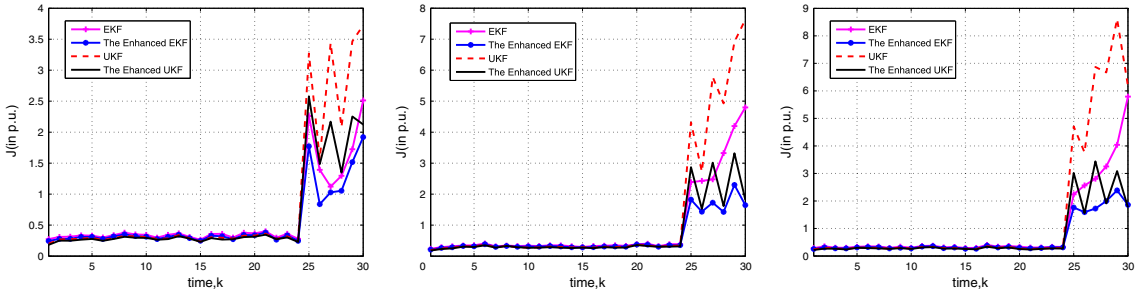

Figure 9. Performance index **J** under negative/positive-mixed attack, wave/negative-mixed attack, and wave/positive-mixed attack in IEEE 30-bus system.

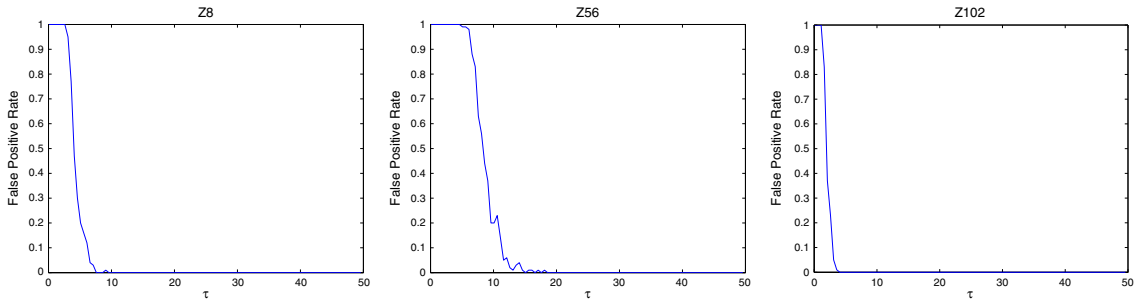

Figure 10. False positive rate versus τ for z_8, z_{56}, and z_{102} in IEEE 30-bus system.

performance index under the wave-based attack is 1–4, the performance index under the positive deviation attack and negative deviation attack are 10–450 and 10–450, respectively. Our data shows that the positive deviation attack and negative deviation attack can reduce the performance more seriously than the wave-based attack. In addition, if the adversary has enough information about the power system, the performance of Kalman filter would be reduced noticeably.

In comparison with the three curves in Figure 8, we can see that the performance index under the negative/positive-mixed attack is 0.5 – 4, the performance index under the wave/negative-mixed attack and wave/positive-mixed attack are 1 – 4 and 1 – 5, respectively. Comparing with three curves in Figure 9, we can see that the performance index under the negative/positive-mixed attack is 0.5 – 4, the performance index under the wave/negative-mixed attack and wave/positive-mixed attack are 1 – 8 and 1 – 9, respectively. Our data shows that these three mixed attacks can reduce the performance of Kalman filtering to the similar level as the wave-based attack does, more slightly than the positive deviation attack and negative deviation attack. The reason is that the measurements in the mixed attack and the wave-based attack are changed toward two directions, but the measurements in positive deviation attack and negative deviation attack are changed toward only one direction.

From the results in Figure 6, 7, 8, and 9, we can see the performance index **J** of both enhanced UKF and EKF are smaller than that of UKF, indicating that the enhanced UKF achieves a better performance than that of UKF and the performance of EKF is better than that of UKF after

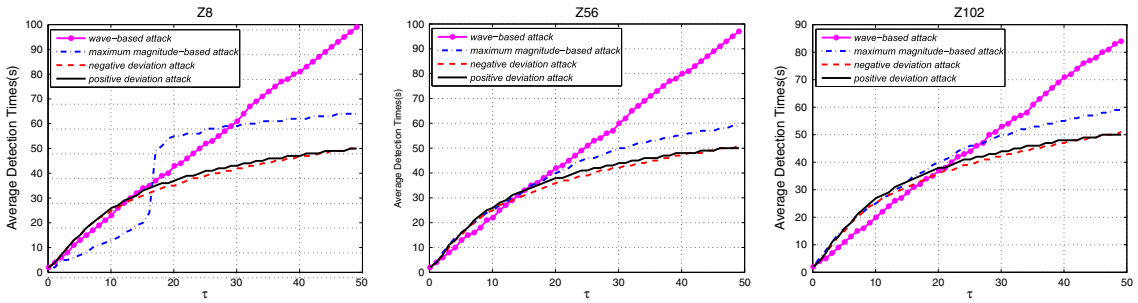

Figure 11. Detection time versus τ for z_8, z_{56}, and z_{102} in IEEE 30-bus system.

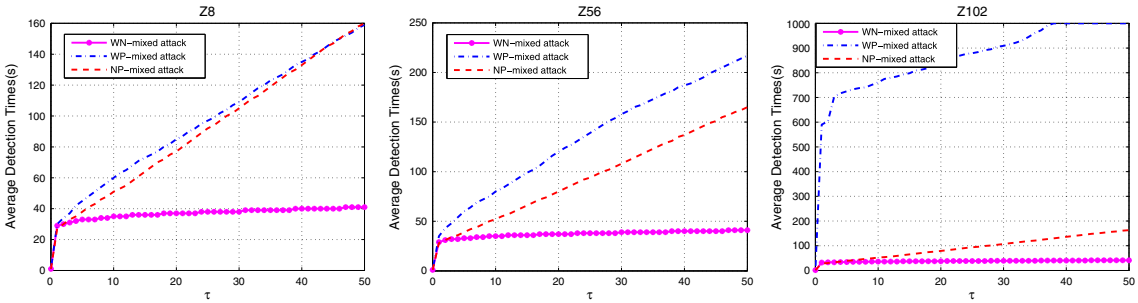

Figure 12. Detection time of mixed attack versus τ for z_8, z_{56}, and z_{102} in IEEE 30-bus system.

the attack is launched. We can also see that the performance index **J** of the enhanced EKF are the smallest after the attack is introduced, indicating that the enhanced EKF achieves the best performance after the attack is launched. These results indicate that the enhanced EKF achieves the best performance and UKF achieves the worst performance in terms of robustness.

8.2.3. Results of temporal-based detection.

To validate the temporal-based detection algorithm, we implemented the detection algorithm in IEEE 14-bus, IEEE 30-bus, and IEEE 118-bus systems. Here, we only show the results of IEEE 30-bus in the evaluation of the detection algorithm as similar observations on other IEEE bus systems can be drawn. In our experiments, we take the EKF technique as an example and choose the meters of z_8, z_{56}, and z_{102} in IEEE 30-bus system, which measure the node voltage of V_8, the power injections of P_{26}, and the power flow of $P_{6\text{–}10}$, respectively. We run simulations for 10,000 times without attacks and compute the mean value of $\left\| z_i(k) - h_i\left(\hat{\mathbf{x}}_k^-, 0\right)\right\|$ under H_0: $E_0^i = E_0\left\| z_i(k) - h_i\left(\hat{\mathbf{x}}_k^-, 0\right)\right\|$. We then obtain $E_0^8 = 0.7348$, $E_0^{56} = 1.5825$, and $E_0^{102} = 0.3534$ in IEEE 30-bus system. After that, we round up the two most significant units and obtain $\eta_8 = 0.74$, $\eta_{56} = 1.6$, $\eta_{102} = 0.36$ in IEEE 30-bus system.

We run simulations for 1000 times without attacks and compute the total number of false positives for different values of τ. The false positive rate, P_F can be defined as $P_F = \frac{\#false\ alarms}{1000}$. Figure 10 show the results for z_8, z_{56}, and z_{102} in IEEE 30-bus system. For z_{56} in IEEE 30-bus system, we can see the false positive rate become very low when we set $\tau_{56} > 20$. Figures 11 and 12 show the average detection time by conducting 1000 times experiments based on our proposed temporal-based algorithm in terms of thresholds: z_8, z_{56}, z_{102} in IEEE 30-bus system. As we can see, the detection time increases as the threshold τ increases. As we know that τ is selected based on the false positive rate and there is a tradeoff between the detection time and false positives. From Figure 10, we can see that selecting τ as high as possible for each sensor can reduce false positives. Nevertheless, increasing τ leads to more time to detect attacks.

9. CONCLUSION

In this paper, we investigated the false data injection attacks against Kalman filtering and developed countermeasures to mitigate such attacks. We first systematically compared the three representative Kalman filtering techniques for the dynamic state estimation for power systems. We then formalized the anomaly detection in Kalman filtering and investigated five types of attacks to avoid the anomaly detection. We discussed the false data injection attacks on other modules in the smart grid in addition to the state estimation. To evaluate the effectiveness of those attacks, we implemented those attacks and evaluated the impact of those attacks on the performance reduction of Kalman filtering on IEEE 14-bus, 30-bus, and 118-bus systems, respectively. To mitigate attacks, we developed countermeasures through enhancing the

resilience of Kalman filtering and developing a temporal-based detection scheme. Our experimental data shows that enhancing the resilience of Kalman filtering technique can maintain the performance to some extent and our developed temporal-based detection technique can detect attacks accurately and quickly.

ACKNOWLEDGEMENTS

The work was supported in part by the Fundamental Research Funds for the Central Universities (xjj2011078) in China, the National Natural Science Foundation of China under grant 61075001, and the US National Science Foundation under grants CNS-1117175. Any opinions, findings, conclusions, and/or recommendations expressed in this material, either expressed or implied, are those of the authors and do not necessarily reflect the views of the sponsor listed previously.

REFERENCES

1. *Report: Cyber-physical systems submit*. http://varma.ece.cmu.edu/Summit/.
2. Morris T, Srivastava AK, Reaves B, Pavurapu K, Abdelwahed S, Vaughn R, McGrew W, Dandass Y. Engineering future cyber-physical energy systems: Challenges, research needs, and roadmap. In *Proceedings of North American Power Symposium (NAPS)*, Starkville, MS, USA, October 2009; 1–6.
3. Huang Z, Schneider K, Nieplocha J. Feasibility studies of applying Kalman filter techniques to power system dynamic state estimation. In *Power Engineering Conference, 2007. IPEC 2007. International*, Singapore, December 2007; 376–382.
4. Albur A, Exposito AG. *Power System State Estimation: Theory and Implementation*. CRC Press: Boca Raton, Florida, 2004.
5. Debs A, Larson R. A dynamic estimator for tracking the state of a power system. *IEEE Transactions on Power Apparatus and Systems* 1970; **PAS-89** (7): 1670–1678.
6. Xue H, quan Jia Q. A dynamic state estimation method with PMU and SCADA measurement for power systems. In *Power Engineering Conference, 2007. IPEC 2007. International*, Singapore, December 2007; 848–853.
7. Bian X, Li X. Joint estimation of state and parameter with synchrophasors – part I: state tracking. *IEEE Transactions on Power Systems* 2011; **26** (3): 1196–1208.
8. Sinha AK, Mondal JK. Dynamic state estimator using ANN based bus load prediction. *IEEE Transactions on Power Systems* 1999; **14**(4): 1219–1225.
9. Lin J-M, Huang S-J, Shih K-R. Application of sliding surface-enhanced fuzzy control for dynamic state estimation of a power system. *IEEE Transactions on Power Systems* 2003; **18**(2): 570–577.
10. Ghahremani E, Kamwa I. Dymamic state estimation in power system by applying the extended Kalman filter with unknown inputs to phasor measurements. *IEEE Transactions on Power Systems* 2011; **26** (4): 2556–2566.
11. Mandal J, Sinha A, Roy L. Incorporating nonlinearity of measurement function in power system dynamic state estimation. *IEE Proceedings - Generation, Transmission and Distribution* 1995; **142**(3): 289–296.
12. Valverde G, Terzija V. Unscented Kalman filter for power system dynamic state estimation. *IET Generation, Transmission and Distribution* 2011; **5** (1): 29–37.
13. da Silva AML, Filho MBDC, de Queiroz JF. State forecasting in electric power systems. *Generation, Transmission and Distribution, IEE Proceedings C* 1983; **130**(5): 237–244.
14. da Silva AML, Filho MBCC, Cantera JMC. An efficient dynamic state estimation algorithm including bad data processing. *IEEE Transactions on Power Systems* 1987; **2**(4): 1050–1058.
15. Shih KR, Huang SJ. Application of a robust algorithm for dynamic state estimation of a power system. *IEEE Transactions on Power Systems* 2002; **17**(1): 141–147.
16. Teixeira A, Amin S, Sandberg H, Johansson KH, Sastry SS. Cyber security analysis of state estimators in electric power systems. In *Proceedings of 49th IEEE Conference on Decision and Control*, Atlanta, GA, United States, December 2010; 5991–5998.
17. Teixeira A, Dan G, Sandberg H, Johansson KH. A cyber security study of a scada energy management system: stealthy deception attacks on the state estimator. In *Proceedings of 18th IFAC World Congress*, Milano, Italy, 2011; 11271–11277.
18. Mo YL, Sinopoli B. False data injection attacks in control systems. In *Preprints of the 1st Workshop on Secure Control Systems*, Stockholm, Sweden, 2010; 1–6.
19. Xie L, Mo YL, Sinopoli B. False data injection attacks in electricity markets. In *Proceedings of 1st IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, October 2010; 226–231.
20. Liu Y, Reiter MK, Ning P. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, IL, United States, November 2009; 21–32.
21. Sandberg H, Teixeira A, Johansson KH. On security indices for state estimators in power networks.

In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, 2010.

22. Bobba RB, Rogers KM, Wang Q, Khurana H, Nahrstedt K, Overbye TJ. Detecting false data injection attacks on dc state estimation. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, 2010; 1–6.
23. Pasqualetti F, Carli R, Bullo F. A distributed method for state estimation and false data detection in power networks. In *IEEE SmartGridComm*, Brussels, Belgium, October 2011; 469–474.
24. Kim T, Poor H. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid* 2011; **2**(2): 326–333.
25. Khurana H, Hadley M, Lu N, Frincke D. Smart-grid security issues. *Security and Privacy, IEEE* 2010; **8**(1): 81–85.
26. Walsh B. *The power grid: from rickety to resilient*, 2012.
27. *Bird's nest suspected in portugal blackout may 10, 2000 web posted at: 12:31 pm edt (1631 gmt)*, 2000.
28. Cui S, Han Z, Kar S, Kim T, Poor H, Tajer A. Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions. *Signal Processing Magazine, IEEE* 2012; **29**(5): 106–115.
29. McLaughlin S, Podkuiko D, McDaniel P. Energy theft in the advanced metering infrastructure. *Critical Information Infrastructures Security of Lecture Notes in Computer Science* 2010; **6027**: 176–187.
30. Song K, Seo D, Park H, Lee H, Perrig A. OMAP: One-way memory attestation protocol for smart meters. In *2011 Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW)*, Busan, Korea, 2011; 111–118.
31. Cleveland F. Cyber security issues for advanced metering infrastructure (AMI). In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, PA, United States, 2008; 1–5.
32. Chen TM. Stuxnet, the real start of cyber warfare? [Editor's Note]. *Network, IEEE,* November 2010; **24**(6): 2–3.
33. Huang S-J, Shih K-R. Dynamic-state-estimation scheme including nonlinear measurement-function considerations. *IEE Proceedings-Generation, Transmission and Distribution* 2002; **149**(6): 673–678.
34. Welch G, Bishop G. *An Introduction to the Kalman Filter*. University of North Carolina at Chapel Hill, Department of Computer Science: Chapel Hill, NC, USA, 1995.
35. Julier S, Uhlmann J. Unscented filtering and nonlinear estimation. *Proceedings of the IEEE* 2004; **92**(3): 401–422.
36. Nishiya K, Hasegawa J, Koike T. Dynamic state estimation including anomaly detection and indentification for power systems. *Generation, Transmission and Distribution, IEE Proceedings C* 1982; **129** (5): 192–198.
37. Cardenas AA, Amin S, Lin ZS, Huang YL, Huang CY, Sastry S. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of ACM Symposium on Information, Computer and Communications Security, AsiaCCS 2011*, Hong Kong, China, March 2011; 355–366.
38. Zimmerman RD, Murillo-Sanchez CE, Gan D. *MATPOWER, a MATLAB power system simulation package*, 2007.
39. Chun-Lien S, Chan-Nan L. Interconnected network state estimation using randomly delayed measurements. *IEEE Transactions on Power Systems* 2001; **16** (4): 870–878.