IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 March 2023, accepted 28 April 2023, date of publication 8 May 2023, date of current version 11 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3273730

RESEARCH ARTICLE

Detection of False Data Injection Attacks in Smart Grid Based on Joint Dynamic and Static State Estimation

PENGFEI HU, WENGEN GAO, YUNFEI LI, FENG HUA, LINA QIAO, AND GUOQING ZHANG
School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China
Key Laboratory of Advanced Perception and Intelligent Control of High-end Equipment, Chinese Ministry of Education, Wuhu 241000, China

Corresponding author: Wengen Gao (ahpuchina@ahpu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant U21A20146, in part by the Natural Science Foundation of Anhui Province under Grant 1908085MF215, in part by the Open Research Fund of Anhui Province Key Laboratory of Detection Technology and Energy Saving Devices under Grant JCKJ2022C02, and in part by the Open Research Fund of Key Laboratory of Advanced Perception and Intelligent Control of High-end Equipment of Ministry of Education under Grant GDSC202208.

ABSTRACT Power system state estimation is an essential component of the modern power system energy management system (EMS), and accurate state estimation is an indispensable basis for subsequent work. However, the attacker can inject biases into measurements to launch false data injection attacks (FDIAs) in smart grids, which ultimately cause state estimates to deviate from security values. This paper proposed the joint use of static state estimation and dynamic state estimation to detect the FDIA, i.e. the joint use of weighted least squares (WLS) and extended Kalman filter (EKF) with exponential weighting function (WEKF), which improves the robustness of state estimation. Since the WLS estimation considers only the measurements at the current moment, the recursive feature of the WEKF enables the estimation process to involve both historical state and current measurements. Therefore, consistency tests and residual tests were performed using the estimations of WLS and WEKF to effectively detect FDIA. In addition, a cluster partitioning approach with approximate equal redundancy of subsystems is proposed to locate the FDIA. The detection of FDIA triggers the partitioning of the network system, and then the chi-square test is used separately in each sub-network to determine the location of FDIA. Finally, the experimental results in the IEEE-14 bus system and the IEEE-30 bus system demonstrate that the approach can effectively detect and locate FDIAs.

INDEX TERMS Cyber security, AC state estimation, false data injection, WEKF, attack detection, smart grids.

I. INTRODUCTION

State estimation is also called filtering. It uses the redundancy of the real-time measurement system to improve the estimation accuracy and automatically filter out the error information caused by random interference [1]. Power system state estimation first selects different system physical quantities as the system state variables to be determined, such as voltage amplitude, voltage phase angle, line current and line power phases, etc. Then, real-time measurement, pseudo measurement and virtual measurement are estimated using the selected estimation algorithm, and finally the operating state of the system is estimated with high accuracy and integrity [2]. Therefore, state estimation is of great significance for monitoring the secure operation of power system [3]. With the development of smart grids and access to various distributed energy sources making the structure and operation of power systems more complicated, so the automation level of power system scheduling centers needs to be further improved [4]. Modern power dispatching system requires fast, accurate and comprehensive acquisition of real-time operation status of power system, while it needs to accurately analyze and predict the operating trend of the power system [5]. This makes state estimation play an important role in the

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

operation of power system and provides basis for the next operation of dispatcher. The state estimation of power system can be divided into static state estimation and dynamic state estimation. Dynamic state estimation takes the measured data at one moment as the initial value, and then estimates the operating state of the system at the next moment according to the motion equation. The state of the static state estimation at a certain time is determined from the measured data at that time. Dynamic state estimation can better predict and track the operation state of power grid [6], [7].

With the construction of energy internet and smart grid, a large number of devices are connected through communication and network to form a complex, mostly heterogeneous system, i.e., cyber-physical system (CPS). Due to the randomness of sensor nodes in the sensing layer of CPS and the openness of data interaction communication channels, the system is vulnerable to network attacks [8], [9], [10], [11], such as false data injection attacks (FDIAs) [12]. Attackers can attack the communication devices of the smart grid or the remote terminal units (RTU) remotely accessed through the network [13]. False data injection attacks change the state estimation in the smart grid to that expected by the attacker, while corrupting the validity of the data to some extent, leading to wrong decisions in the control center, which will eventually lead to a greater degree of electrical security incidents [14]. Attackers can initiate FDIAs by destroying the measurements obtained by the SCADA system or phasor measurement units (PMUs), such as attacking the power flow between different buses and the power injected by the bus, et al. Classical bad data detection (BDD) system can detect bad data caused by random noise, but cannot detect well-designed FDIAs. It has been shown that classical methods based on maximum normalized residuals are unable to detect well-designed false data injection attacks. Therefore, an attacker can inject the expected attack into the measurement and eventually corrupt the results of state estimation [15], [16].

Both the classical chi-square test and the maximum normalized residual test are based on the results of the state estimation of the WLS, and the test results are then compared with the corresponding thresholds to determine the existence of bad data. Today, network attacks have become more sophisticated and stealthy, so detection methods using WLS alone cannot detect FDIAs, especially when the attacker knows the topology information of the network [17]. In addition, the estimates obtained using WLS are based on current measurement data only and do not contain any historical information, so they cannot predict the operational state of the system [18], [19]. However, the EKF estimates are based on current measurement data and historical information, and the EKF can also predict the operating state of the system.

Considering the cost and effectiveness of detection methods, this paper proposes a method that jointly uses static state estimation and dynamic state estimation to detect FDIAs. In particular, this paper introduces an exponential weighting function in the EKF, which makes the state estimation more robust. WEKF can adaptively reduce the weight of the current measurements in the face of FDIAs while increasing the weight of the predicted estimated measurements, which can ultimately maintain excellent estimated performance. When FDIAs occurs, the estimate obtained by WLS at the next moment jumps, but the estimate obtained by WEKF at the next moment remains stable. The estimates obtained from the two estimation methods were then used to effectively detect FDIAs using a consistency test. To localize FDIAs, we propose a system partitioning method that maintains the approximate equality of redundancy. Since the division of the system makes the subsystems less redundant, this makes the chi-square test more effective. Finally, the chi-square test is used in each subsystem to locate FDIAs. The main contributions of this paper can be summarized as follows:

- In response to the problem that the extended Kalman filter suffers from degraded estimation performance in the face of the FDIA, an extended Kalman filter with the introduction of an exponential weighting function is proposed. This enables the WEKF to maintain excellent state estimation performance in the face of the FDIA with different attack strengths.
- A WEKF-based detection approach is proposed for the FDIA, which is used for the first time in conjunction with WLS state estimation.
- To maintain the detection performance, the method for determining the dynamic detection threshold is proposed.
- To further locate the location of FDIA, a system partitioning approach that maintains the redundancy of subsystems approximately equal is proposed. Finally the FDIA is detected in each subsystem separately to determine the location of the FDIA attack.
- The experimental results demonstrate that the approach maintains excellent detection and localisation performance in the face of the FDIA with different attack strengths.

The rest of this paper is organized as follows. Section II describes the related work. Section III presents the principles of FDIA and the model for state estimation. Section IV describes the methods used in this paper to detect and localize FDIA. Section V presents the results of simulation and numerical examples. Section VI concludes the paper and future research directions.

II. RELATED WORKS

The FDIA based on the DC state estimation model has been extensively used in many researches. However, constructing FDIAs using the DC model produces larger residuals in the AC state estimation, which are more readily detected [20]. FDIAs based on AC state estimation models were constructed in [21] to attack the distribution network. An attacker can approximate the system state through power flow or power injection measurements without knowing the system state, and eventually deviate the state estimate from the security value without being detected. In order to decrease the number of measurements that need to be modified when constructing an attack, a false data injection attack model is proposed in [22] to modify the network parameters, which ultimately leads to a better coordination between the state change of the system and the modification of the network parameters. In [23], an attack model based on nonlinear physical constraints was proposed to achieve the hiding effect and successfully bypass the detection.

In models with AC state estimation, it is difficult for an attacker to achieve perfect FDIAs, and imperfect attacks lead to changes in the probability distribution of the measurement residuals. Therefore, a detection method based on the statistical consistency of the measurement residuals is proposed in [24]. Although this method can effectively detect FDIAs, it cannot find the specific location of FDIAs. In the face of FDIAs in the dynamic model of smart grid, a fast intrusion detection algorithm is proposed in [25]. The algorithm distinguishes between FDIAs and systematic mutations by analyzing the estimated statistical properties. At the same time, the method can detect or eliminate FDIAs with very low latency. In [26], the method based on Kullback-Leibler distance (KLD) is used to detect FDIAs. This method determines the existence of FDIAs by comparing the difference in probability distributions between historical and current measurements. The disadvantage of this detection method is that it requires a large amount of historical measurement data, and the detection efficiency may be compromised in the face of trapezoidal attacks. In [27], a detection method based on the measured data of PMUs is proposed. This method takes the state estimates obtained by PMUs and SCADA and performs a consistency check to detect FDIAs. However, the assumption that the measurements obtained by PMUs are always secure does not always hold.

III. PRELIMINARIES

A. AC STATE ESTIMATION

Power system state estimation is one of the core functions of the Energy Management System (EMS) of the power system dispatch center. Its function is to estimate the current operating status of the power system based on various measurement information of the power system. Assume that the power system has m measurements and n state variables. In AC power systems, the nonlinear relationship between measurements and state variables is as follows:

$$z = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{v} \tag{1}$$

where $z \in \mathbb{R}^{m\times 1}$ is the vector of measurements; $\boldsymbol{x} \in \mathbb{R}^{n\times 1}$ represents the vector of state variables to be estimated; $\boldsymbol{v} \in \mathbb{R}^{m\times 1}$ is the measurement error vector, which is a Gaussian white distribution with zero mean and error covariance matrix $\boldsymbol{R}$, i.e., $\boldsymbol{R} = diag(\sigma_1^2, \ldots, \sigma_m^2)$; $\boldsymbol{h}(\cdot)$ represents the nonlinear relationship between the measurement vector z and the state estimation vector $\boldsymbol{x}$.

The nonlinear relationship $\boldsymbol{h}(\cdot)$ between the state vector and the measurement vector is as follows [1]:

$$P_i = V_i \sum_{j\in\Omega_i} V_j(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \tag{2}$$

$$Q_i = V_i \sum_{j\in\Omega_i} V_j(G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}) \tag{3}$$

$$P_{ij} = V_i{}^2(g_{si} + g_{ij}) - V_iV_j(g_{ij}\cos\theta_{ij} + b_{ij}\sin\theta_{ij}) \tag{4}$$

$$Q_{ij} = -V_i{}^2(b_{si} + b_{ij}) - V_iV_j(g_{ij}\sin\theta_{ij} - b_{ij}\cos\theta_{ij}) \tag{5}$$

where P_i and Q_i are the active and reactive power injection of bus i, respectively; P_{ij} and Q_{ij} are the real and reactive power flow from bus i to bus j, respectively; V_i is the voltage at bus i; θ_i is the phase angle at bus i; θ_{ij} is the phase angle difference between buses i and j; $G_{ij}+jB_{ij}$ is the line admittance between buses i and j; $g_{ij} + jb_{ij}$ is admittance of the shunt branch at bus i; Ω_i is the set of buses associated with bus i.

The WLS method is the most basic method to obtain the state estimation [28]. The method to obtain state estimation using WLS is as follows:

$$\hat{\boldsymbol{x}} = \arg\min\,[z - \boldsymbol{h}(\boldsymbol{x})]^T \boldsymbol{R}^{-1}[z - \boldsymbol{h}(\boldsymbol{x})] \tag{6}$$

where $\hat{\boldsymbol{x}}$ is the vector of state estimates for the best-fit measure z.

The solution of Equation (6) can be obtained by Newton iteration method [1]:

$$\begin{aligned}
\Delta z^{(l)} &= z - \boldsymbol{h}(\hat{\boldsymbol{x}}^{(l)}) \\
\Delta\hat{\boldsymbol{x}}^{(l)} &= [\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H}]^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\Delta z^{(l)} \\
\hat{\boldsymbol{x}}^{(l+1)} &= \hat{\boldsymbol{x}}^{(l)} + \Delta\hat{\boldsymbol{x}}^{(l)}
\end{aligned} \tag{7}$$

where l is the l-th iteration index; $\hat{\boldsymbol{x}}^{(l)}$ is the result of the l-th iteration of the state estimation vector; $\boldsymbol{H}$ is the Jacobian matrix.

B. BAD DATA DETECTION AND FALSE DATA INJECTION ATTACK

The classical BDD detection algorithm compares the objective function value of the WLS with the threshold value of the chi-square test. The objective function $J(\hat{\boldsymbol{x}})$ of the WLS-based state estimation results is

$$J(\hat{\boldsymbol{x}}) = \sum_{i=1}^{m} [z_i - h_i(x)]^2 \Big/ \sigma_i^2 \tag{8}$$

where m is the number of measurements; σ_i^2 represents the measurement error of the ith meter; z_i represents the measured value of the ith meter.

The detection of bad data using the objective function (8) can be achieved by hypothesis testing.

$$\begin{cases} H_0 : J(\hat{\boldsymbol{x}}) \le \chi^2_{(m-n),p}, \text{ No bad data, Accept } H_0 \\ H_1 : J(\hat{\boldsymbol{x}}) > \chi^2_{(m-n),p}, \text{ Bad data, Reject } H_0 \end{cases} \tag{9}$$

where H_0 is called original hypothesis, i.e., there is no bad data; H_1 is called alternative hypothesis, i.e., there is bad data.

$\chi^2_{(m-n),p}$ is the chi-square test threshold with confidence level p and degree of freedom $(m-n)$.

Let $\boldsymbol{a} \in \mathbb{R}^{m\times 1}$ denote the attack vector that the attacker attempts to inject into the meter. Then normal measurement $\boldsymbol{z}$ changes to $\boldsymbol{z}_{bad} = \boldsymbol{z} + \boldsymbol{a}$ after being attacked. Let $\hat{\boldsymbol{x}}_{bad} = \hat{\boldsymbol{x}} + \boldsymbol{c}$ denote the state estimation variable after being attacked, i.e., $\boldsymbol{c} = [c_1, \ldots c_n]^T$, where $\boldsymbol{c}$ is the deviation of state estimation caused by FDIAs. The residual vector of the attacked measurement $\boldsymbol{z}_{bad}$ is

$$\boldsymbol{r}_{bad} = \boldsymbol{z}_{bad} - \hat{\boldsymbol{z}}_{bad} = \boldsymbol{z} + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}). \tag{10}$$

Therefore, the L_2-norm of the measurement residual under normal conditions is

$$\|\boldsymbol{r}\|_2 = \left\|\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})\right\|_2 \tag{11}$$

If $\|\boldsymbol{r}\|_2$ is less than the threshold τ, the measurement is considered to have no bad data; otherwise, the measurement is considered to have bad data.

If the attacker constructs a well-designed attack vector as $\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}})$ [15], the residuals of the attacked measurement become

$$\begin{aligned} \boldsymbol{r}_{bad} &= \boldsymbol{z} + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) \\ &= \boldsymbol{z} + \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) \\ &= \boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}}) \\ &= \boldsymbol{r} \end{aligned} \tag{12}$$

where $\boldsymbol{r}$ is the residual of the normal measurement. Equation (12) shows that the measurement residuals of attacked and unattacked are equal. Therefore, classical bad data detection methods are unable to detect the above-constructed false data injection attacks.

C. MODEL FOR DYNAMIC STATE ESTIMATION

The power information physical system is a highly multi-dimensional non-linear system, and the AC power flow equation of the power system presents a non-linear relationship. The state equation and measurement equation of dynamic state estimation are as follows [29]:

$$\boldsymbol{x}_{k+1} = \boldsymbol{f}(\boldsymbol{x}_k) + \boldsymbol{w}_k \tag{13}$$

$$\boldsymbol{z}_k = \boldsymbol{h}(\boldsymbol{x}_k) + \boldsymbol{v}_k \tag{14}$$

where $\boldsymbol{x}_k$ and $\boldsymbol{x}_{k+1}$ represent the state vectors at time k and $k+1$, respectively; $\boldsymbol{f}$ is the state transition equation of state vector $\boldsymbol{x}_k$ to $\boldsymbol{x}_{k+1}$; $\boldsymbol{w}_k$ is the systematic error at time k; $\boldsymbol{z}_k$ and $\boldsymbol{v}_k$ represent the measurement vector and measurement error at time k, respectively; $\boldsymbol{h}$ represents the nonlinear relationship between the state vector $\boldsymbol{x}$ and the measurement vector $\boldsymbol{z}$. Suppose $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ are uncorrelated and obey white Gaussian noise with zero mean, and their error covariance matrices are $\boldsymbol{Q}$ and $\boldsymbol{R}$, respectively.

The Kalman filter is a linear optimal estimator. However, the power information physical system is a highly multi-dimensional and non-linear system. Therefore, we consider the use of extended Kalman filter (EKF) for dynamic state estimation. The linearization model of the extended Kalman filter is as follows [29]:

$$\boldsymbol{x}_{k+1} = \boldsymbol{F}_k\boldsymbol{x}_k + \boldsymbol{G}_k + \boldsymbol{w}_k \tag{15}$$

$$\boldsymbol{z}_k = \boldsymbol{H}_k\boldsymbol{x}_k + \boldsymbol{v}_k \tag{16}$$

where $\boldsymbol{F}_k = \partial \boldsymbol{f}/\partial \boldsymbol{x}|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_k}$ is the Jacobian of the equation of state at time k; $\boldsymbol{G}_k$ is denoted as the input matrix at time k; $\boldsymbol{H}_k = \partial \boldsymbol{h}/\partial \boldsymbol{x}|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_k}$ is the Jacobian of the measurement equation at time k.

The power information physical system is a network with complexity, multidimensionality and load variability. The state transition matrix at each moment is difficult to determine, and using the method of linearizing the state equation will introduce errors. Therefore, the method of Holt's two-parameter exponetial smoothing method is used in this paper to predict the state value of the next moment. This method has the advantage of storing few variables and fast calculation, so it is suitable for short-term load forecasting. It is an online identification method rather than a linearization. The equation of state can be written as

$$\begin{aligned} \hat{\boldsymbol{x}}_{k+1|k} &= \boldsymbol{a}_k + \boldsymbol{b}_k \\ \boldsymbol{a}_k &= \alpha\hat{\boldsymbol{x}}_k + (1-\alpha)\hat{\boldsymbol{x}}_{k|k-1} \\ \boldsymbol{b}_k &= \beta(\boldsymbol{a}_k - \boldsymbol{a}_{k-1}) + (1-\beta)\boldsymbol{b}_{k-1} \end{aligned} \tag{17}$$

where $\hat{\boldsymbol{x}}_k$ and $\hat{\boldsymbol{x}}_{k|k-1}$ denote the state estimate vector and predicted state vector at time k, respectively; α and β are both expressed as smoothing parameters, where $\alpha = 0.85$, $\beta = 0.05$.

Thus, the linearized equation of state can be expressed as

$$\begin{aligned} \hat{\boldsymbol{x}}_{k+1|k} = \alpha(1+\beta)\hat{\boldsymbol{x}}_k + (1+\beta)(1-\alpha)\hat{\boldsymbol{x}}_{k|k-1} \\ -\beta\boldsymbol{a}_{k-1} + (1-\beta)\boldsymbol{b}_{k-1} \end{aligned} \tag{18}$$

IV. DETECTION AND LOCALIZATION OF FDIAs

A. EKF WITH ADAPTIVE CHANGE OF MEASUREMENT WEIGHTS

In order to better detect false data injection attacks with different attack strengths, this paper adds an exponential weighting function to the EKF. The EKF with the introduction of an exponential weighting function maintains excellent estimation performance in the face of FDIA with different attack strengths. The specific state estimation process is

(1) Forecasting steps

$$\hat{\boldsymbol{x}}_{k|k-1} = \boldsymbol{F}_{k-1}\hat{\boldsymbol{x}}_{k-1} \tag{19}$$

$$\boldsymbol{P}_{k|k-1} = \boldsymbol{F}_{k-1}\boldsymbol{P}_{k-1}\boldsymbol{F}_{k-1}^T + \boldsymbol{Q}_{k-1} \tag{20}$$

(2) Updating steps

$$\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_{k|k-1} + \boldsymbol{K}_k\left[\boldsymbol{z}_k - \boldsymbol{h}\left(\hat{\boldsymbol{x}}_{k|k-1}\right)\right] \tag{21}$$

$$\boldsymbol{K}_k = \boldsymbol{P}_{k|k-1}{\boldsymbol{H}_k}^T(\boldsymbol{H}_k\boldsymbol{P}_{k|k-1}{\boldsymbol{H}_k}^T + \boldsymbol{R}_k)^{-1} \tag{22}$$

$$\boldsymbol{P}_k = (\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{H}_k)\boldsymbol{P}_{k|k-1} \tag{23}$$

where $\boldsymbol{P}_{k|k-1}$ and $\boldsymbol{P}_k$ are denoted as the covariance matrix of the prior estimation error and the covariance matrix of the posterior estimation error at time k, respectively; $\boldsymbol{K}_k$ denotes the Kalman gain at time k. The initial state values and the covariance matrix of the estimation errors are set to $\hat{x}_0 = 0$ and $\boldsymbol{P}_0 = \boldsymbol{I}$, respectively. Furthermore, we define the residuals of the prediction estimates at time k as $\tilde{\boldsymbol{r}} = z_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})$.

Suppose false data injection attacks are launched into the power system at time k. The attacker can only inject bias into the measurement, so the measurement changes from z_k to z_k^a. Equation (21) can be written as

$$\begin{aligned}\hat{\boldsymbol{x}}_k^a &= \boldsymbol{F}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[z_k^a - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})]\\ &= \boldsymbol{F}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[z_k + \boldsymbol{a}_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})]\\ &= \hat{\boldsymbol{x}}_k + \boldsymbol{K}_k\boldsymbol{a}_k \end{aligned} \tag{24}$$

where $\hat{\boldsymbol{x}}_k^a$ denotes the vector of state estimates after being attacked at time k. We assume that the bias of the state estimate caused by the false data injection attack at time k is $\Delta\hat{\boldsymbol{x}}_k^a = \hat{\boldsymbol{x}}_k^a - \hat{\boldsymbol{x}}_k$. Therefore, the state estimate obtained after being attacked at time $k+1$ can be written as

$$\begin{aligned}\hat{\boldsymbol{x}}_{k+1}^a &= \boldsymbol{F}\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}[z_{k+1}^a - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}^a)]\\ &= \boldsymbol{F}\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}[z_{k+1} + \boldsymbol{a}_{k+1} - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}^a)]\\ &= \boldsymbol{F}\Delta\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}[\Delta\boldsymbol{h}^a(\hat{\boldsymbol{x}}_{k+1|k}) + \boldsymbol{a}_{k+1}] + \hat{\boldsymbol{x}}_{k+1} \end{aligned} \tag{25}$$

We define the injection bias of the estimated measurements predicted at time k as $\Delta\boldsymbol{h}^a(\hat{\boldsymbol{x}}_{k+1|k}) = \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}^a)$. Therefore, the bias of the state estimate caused by the false data injection attack at time $k+1$ is

$$\hat{\boldsymbol{x}}_{k+1}^a - \hat{\boldsymbol{x}}_{k+1} = \boldsymbol{F}\Delta\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}\Delta\boldsymbol{h}^a(\hat{\boldsymbol{x}}_{k+1|k}) + \boldsymbol{K}_{k+1}\boldsymbol{a}_{k+1} \tag{26}$$

From the above calculation, it can be concluded that the state estimation bias at the current time is not only affected by the state estimation bias at the previous time, but also by the injection attack at the current time. When using the EKF for state estimation, the state transfer equation and process noise will have some influence on the state estimation, so there is a transition process of convergence in the EKF [30]. However, when using WLS for state estimation, the state values will converge and update accelerated. This enables us to efficiently detect FDIAs using discrepancies and inconsistencies in the estimated responses.

When FDIAs are injected, the prediction residual $\tilde{\boldsymbol{r}} = z_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})$ increases. To enable the EKF to excellent good estimation performance despite the existence of FDIAs, this paper adaptively decreases the filter gain of the EKF using the prediction residuals, which allows the attacked measurements to have a lower weight in the state estimation process. Meanwhile, the weights of the predicted estimated measurements are increased. The relationship between the weighting matrix $\boldsymbol{W}_k$ of the measurements and the covariance matrix $\boldsymbol{R}$ of the measurement noise is $\boldsymbol{W}_k = \boldsymbol{R}^{-1}$. The weighting matrix of the measurements can be updated as

$$(\boldsymbol{W}_k^{new})^{-1} = \boldsymbol{W}_k^{-1} * e^{|z_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})|} \tag{27}$$

The above method can effectively suppress the degradation of state estimation performance due to the increase in attack strength. When the predicted estimated measurement $\boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})$ deviates significantly from the current measurement z_k, the increase in the mode of the predicted residual vector makes the measurement noise increase and ultimately decreases the Kalman gain. Conversely, minor deviations between the predicted and current measurements lead to minor changes in the measurement noise, which further leads to minor changes in the Kalman gain and ultimately to minor changes in the estimated values. When FDIAs are existing, the WEKF can better suppress the effects of attacks, ultimately increasing the difference between the WEKF and WLS estimation.

B. DETECTION METHOD BASED ON STATE DEVIATION

The power flow calculation is performed for the power system at the moment of k, and then the calculation results are added the perturbation error conforming to the Gaussian distribution as the measurement data of the current system. Then, two state estimation methods proposed above are used to estimate the state of the system. Firstly, consistency tests are used to compare the deviations between the two estimates. The formula is as follows:

$$\left\| \hat{\boldsymbol{x}}_k^s - \hat{\boldsymbol{x}}_k^d \right\|_2 \le \tau_a \tag{28}$$

where $\hat{\boldsymbol{x}}_k^s$ and $\hat{\boldsymbol{x}}_k^d$ represent the predicted state estimates from WEKF and WLS, respectively. τ_a is the consistency check threshold, and its value is determined by the measurement error and the accuracy of the state estimation result.

Since the predicted values are calculated using Holt's two-parameter method, the system with sudden changes in generator and load is no longer applicable [31]. Therefore, the consistency test may not be satisfied even if the system is not under attack. To eliminate false detections caused by sudden generator changes or sudden load changes, the residuals between the predicted estimates and the actual measurements are further checked. The method of residual test is

$$\left\| z_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_k^s) \right\|_2 \le \tau_b \tag{29}$$

where $\boldsymbol{h}(\hat{\boldsymbol{x}}_k^s)$ is the estimated measurement obtained using the WEKF; τ_b is the detection threshold for bad data, and its value is determined by the error tolerance of the chi-square distribution.

When bad data are exist in the power grid, the consistency test results of the state estimates obtained by the two estimation methods are much larger than the threshold values. Next, the existence of mutational interference or the existence of FDIAs needs to be determined. Finally, the prediction estimates obtained using WEKF are subjected to residual tests to determine whether FDIAs actually exist. When the result of the residual test was also greater than the threshold of the chi-square test, the existence of FDIA was determined. Conversely, when the result of the residual test is less than the threshold of the chi-square test, the result of the consistency test is disturbed by mutations and should ultimately be judged as non-existent attack.

C. LOCALIZATION OF FDIAs

To locate the FDIA, the existence of FDIA is first detected using Equation (28) and Equation (29). If FDIA does not exist, then no system partitioning is triggered, otherwise the complete system $\boldsymbol{G}$ is divided into multiple subsystems $\boldsymbol{G}_1$, $\boldsymbol{G}_2, \ldots$ and $\boldsymbol{G}_n$ based on the principle of approximate equal redundancy of subsystems. When the system is divided into subsystems, the redundancy of each subsystem is decreased and the threshold of the chi-square test is decreased making the chi-square test more effective. Finally, the chi-square test is performed on the subsystems until the location of FDIA is found.

Therefore, the proposed method for detecting and locating the FDIA is shown in Algorithm 1.

Algorithm 1 Detection Methods Based on Dynamic and Static State Estimation

```
Input: Smoothing parameters $\alpha$ and $\beta$; noise error covariance $\boldsymbol{Q}$ and $\boldsymbol{R}$; initial state $\hat{\boldsymbol{x}}_0$ and state error covariance $\boldsymbol{P}_0$; consistency test threshold $\tau_a$ and residual test threshold $\tau_b$;
Output: Declare the occurrence of FDIA.
for $k = 1$ to $N$, where $N$ represents the number of time slots do
    Acquire the measurement vector $z_k$ and determine the Jacobi matrix $\boldsymbol{H}$;
    The exponential smoothing method of Equation (17) is used to predict the state vector $\hat{\boldsymbol{x}}_{k|k-1}$ at the next moment.
    Classical state estimation using weighted least squares method to calculate the predicted state estimate vector $\hat{\boldsymbol{x}}_k^d$; $\hat{\boldsymbol{x}}_k^d = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}z_k$;
    $\boldsymbol{P}_{k|k-1}$ is acquired by the state prediction step of Equation (20);
    The measurement noise covariance matrix was updated by using Equation (27), where $\boldsymbol{W}_k = \boldsymbol{R}^{-1}$;
    The update steps of Equations (21)-(23) are used to acquire the state estimate $\hat{\boldsymbol{x}}_k^s$, $\hat{\boldsymbol{x}}_k^s = \hat{\boldsymbol{x}}_{k|k-1} + \boldsymbol{K}_k[z_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})]$;
    if $\left\|\hat{\boldsymbol{x}}_k^s - \hat{\boldsymbol{x}}_k^d\right\|_2 \geq \tau_a$ then
        The FDIA and bad data may be existing;
    else if $\left\|z_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_k^s)\right\|_2 \geq \tau_b$ then
        The FDIA is existing and the alarm is triggered. At the same time, the system is divided;
        The chi-square test was performed on the divided subsystems using Equation (9);
        If the objective function of the subsystem obtained by Equation (8) is still greater than the threshold value;
        Divide the subsystem into smaller subsystems until it is positioned at the FDIA attack location;
    else
        The FDIA is not existing and the process of state estimation continues;
    end if
end for
```

V. SIMULATION RESULTS

In this paper, MATLAB R2018b was used for the simulation. The power flow is calculated using the relevant data from the MATPOWER 7.1 power simulation package. Finally, measurement noise is added to the results of the power flow to serve as measurement data. At the same time, the measurement noise obeys the Gaussian distribution with the mean value of 0 and the variance of 0.015.

In this section, the detection performance of the proposed algorithm is demonstrated by simulation results. Firstly, this paper uses the construction method of the attack vector in [32] to inject false data into the IEEE-14 bus system. The results of state estimation using WLS, EKF and WEKF are compared for the smart grid after an attack. Secondly, the detection method proposed in this paper is used to detect the existence of FDIA in the IEEE-14 bus system and the IEEE-30 bus system, respectively. Finally, the FDIA injected into the IEEE-30 bus system is located through experimental simulations.

A. PERFORMANCE COMPARISON BETWEEN WEKF AND EKF

To compare the robustness of state estimation when the WEKF and EKF are affected by the FDIA, this paper uses the root mean square error (RMSE) to determine the estimation performance of the two estimators. The RMSE calculates the estimation error for both estimators by using the difference between the predicted estimate and the actual value. The estimated predicted voltage of the bus is compared with the actual value when the grid is under attack. RMSE is defined as follows:

$$RMSE = \sqrt{\frac{1}{N}\sum_{j=1}^{N}(\hat{\boldsymbol{x}}_j - \boldsymbol{x}_j)^2} \tag{30}$$

where N represents the number of buses; $\hat{\boldsymbol{x}}_j$ is the predicted voltage estimate for the jth bus; $\boldsymbol{x}_j$ represents the actual voltage of the jth bus.

The voltage estimation errors for each bus after the grid has been attacked are shown in Table 1. As seen in Table 1, the estimation error of WEKF is minimal when the grid is attacked by false data injection. At the same time, the error of state estimation using WLS is the largest. In short, the WEKF has a better estimation performance than the EKF when the smart grid is under attack. The RMSE calculated from the estimated error for each bus is shown in Table 2. As shown in Table 2, the RMSE of the WEKF estimates is significantly less than the RMSE of the EKF estimates. Therefore, when FDIA is existing, the WEKF has better estimation performance than the EKF and WLS.

TABLE 1. Estimated error of each bus.

Bus	WLS	EKF	WEKF
1	8.23×10^{-2}	1.71×10^{-2}	-3.1×10^{-3}
2	10.20×10^{-2}	2.80×10^{-2}	5.3×10^{-3}
3	9.94×10^{-2}	2.23×10^{-2}	4.2×10^{-3}
4	12.14×10^{-2}	2.2×10^{-2}	5.1×10^{-3}
5	12.16×10^{-2}	2.50×10^{-2}	6.2×10^{-3}
6	11.47×10^{-2}	1.75×10^{-2}	7.5×10^{-3}
7	10.90×10^{-2}	2.50×10^{-2}	5.5×10^{-3}
8	11.44×10^{-2}	2.64×10^{-2}	5.8×10^{-3}
9	10.96×10^{-2}	1.87×10^{-2}	3.9×10^{-3}
10	10.94×10^{-2}	2.42×10^{-2}	6.1×10^{-3}
11	11.75×10^{-2}	2.37×10^{-2}	5.2×10^{-3}
12	11.64×10^{-2}	2.41×10^{-2}	3.7×10^{-3}
13	11.71×10^{-2}	1.97×10^{-2}	4.1×10^{-3}
14	12.05×10^{-2}	3.31×10^{-2}	7.2×10^{-3}

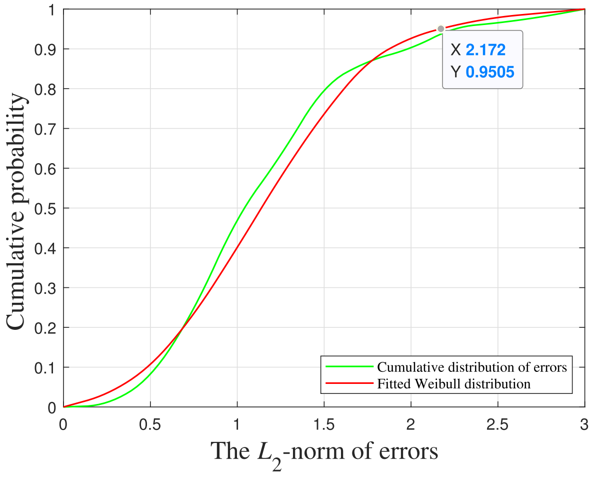

FIGURE 1. The fitted cumulative distribution function with the L_2-norm of errors.

TABLE 2. RMSE of voltage amplitude.

Algorithm	RMSE
WLS	0.1116
EKF	0.0575
WEKF	0.0054

B. DETERMINING DYNAMIC DETECTION THRESHOLD AND DETECTING FDIA

In this paper, the sum of squared errors (SSE) method is used to determine τ_a. The error is the difference between the estimates of WLS and WEKF in the absence of FDIA. Specifically, the steps for determining τ_a are as follows:

- Firstly, estimates were obtained using WLS and WEKF respectively in the absence of FDIA. Then the errors of the two estimates were calculated and finally the L_2-norm of the error was obtained.
- Secondly, the sample values of the L_2-norm of the error were fitted using the Weibull distribution.

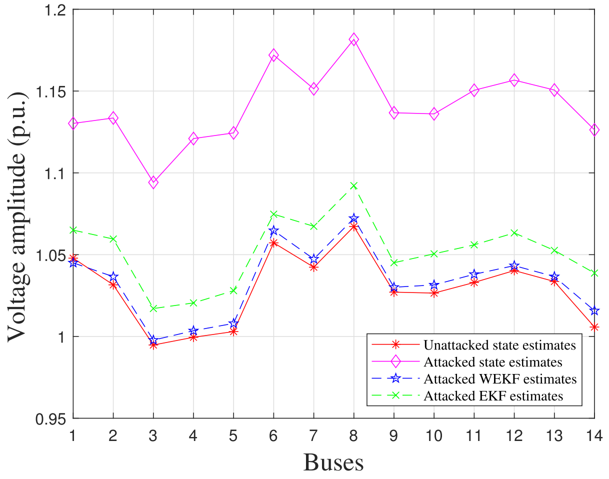

FIGURE 2. The voltage amplitude of each bus before and after the attack.

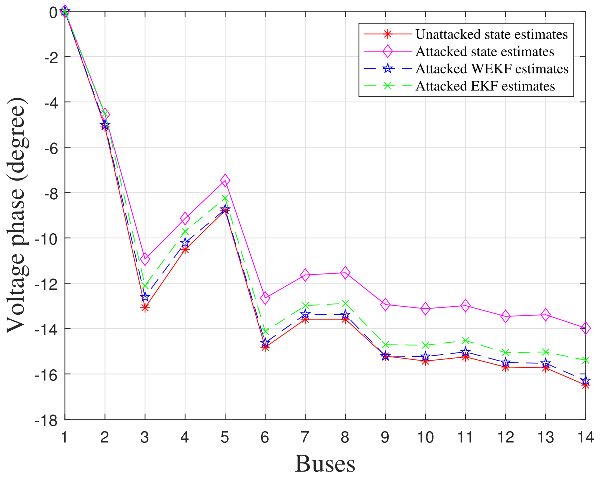

FIGURE 3. The voltage phase of each bus before and after the attack.

- Finally, the false alarm rate is used to determine the corresponding threshold value.

Fig. 1 gives an illustration of the approach to determining the detection threshold τ_a in the IEEE-14 bus system. The false alarm rate, i.e. the false positive rate (FPR), was first determined. Then (1−FPR), i.e. 0.95, was used as the value of the vertical coordinate for fitting the Weibull distribution. Finally the value of the horizontal coordinate corresponding to the Weibull distribution was taken as the detection threshold, i.e. $\tau_a = 2.172$.

In this paper, the attack vector is constructed by modifying the measurement data of the local subnet. At the same time, the attack vector is made to achieve concealment [17].

Assume that the power system is continuously affected by the false data injection attack from the third hour, while the power system is unaffected in the first two hours. At the same time, the EMS is sampled every 30 seconds. As can be seen in Fig. 2 and Fig. 3, the amplitude and phase angle of the bus voltage changed both before and after the attack. The residuals of the estimates before and after the attack using

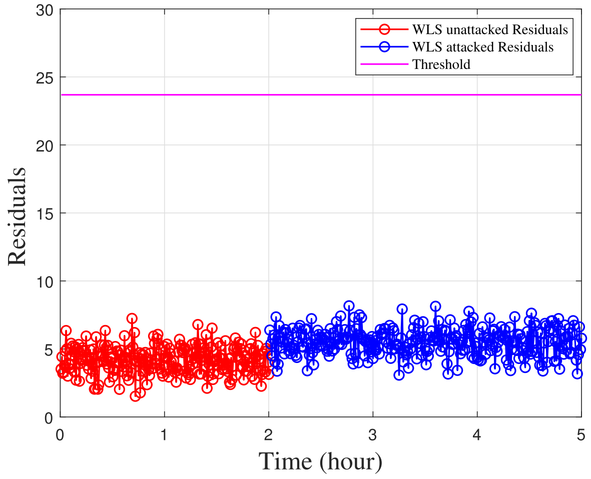

FIGURE 4. Residuals of WLS estimates before and after the attack.

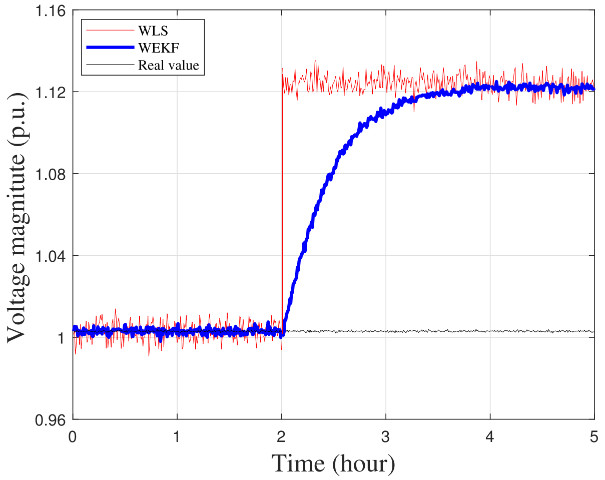

FIGURE 5. The change in voltage phase of bus 5 before and after the attack.

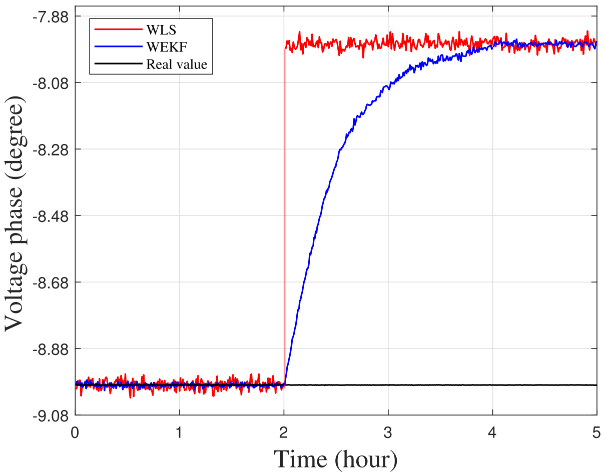

FIGURE 6. The voltage phase change of bus 5 before and after being attacked.

weighted least squares are shown in Fig. 4. The estimated residual of the weighted least squares method when not under attack was calculated to be 4.1572. However, the estimated residual after being attacked was 5.5671. Therefore, the variation in the estimated residuals before and after the attack is minimal. Suppose we set the confidence level to 0.95. The IEEE-14 bus system has 41 measurements and 27 state variables. Therefore, the redundancy is $k = m - n = 14$. The detection threshold obtained by looking up the chi-square table was 23.685. The residuals calculated after the attack are less than the threshold, but the voltage amplitude and phase angle change after the attack, so this FDIA cannot be detected by the WLS-based method.

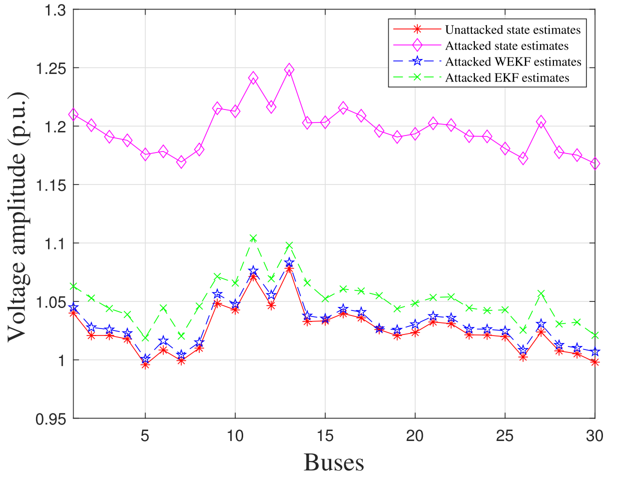

FIGURE 7. The voltage amplitude of each bus before and after the attack.

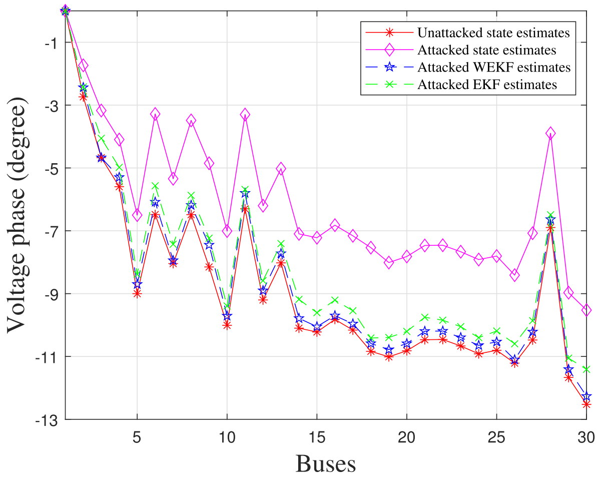

FIGURE 8. The voltage phase of each bus before and after the attack.

Suppose the power system operates normally for the first two hours and then is subject to a continuous false data injection attack from the third hour onwards. Based on these two methods of state estimation, Fig. 5 and Fig. 6 show the changes in the state estimates of the voltage amplitude and phase angle of bus 5 before and after the attack, respectively. Traditional weighted least squares estimation (WLSE) is a static state estimation method based on the current measurements, so the WLSE will react quickly when the FDIA occurs at the third hour. However, the WEKF is a recursive method. The current state estimate is determined by a combination of historical data and current measurements. Therefore, there is a process of state adjustment in the WEKF when the FDIA occurs. Therefore, the deviations from the state estimates obtained by the two methods can be used to detect the FDIA.

When FDIAs were not existing, the result of the consistency test using Equation (28) was 0.7426. However, the result of the consistency test in the existence of the FDIA was 19.361. Meanwhile, the threshold of the consistency test was set at 2.172, so the result of the consistency test after the attack was significantly greater than the threshold. In order to eliminate false detections caused by sudden changes in the generator or load, the estimation results of the WEKF were further tested for residuals using Equation (29). The result of the residual test for the WEKF estimate is 31.614, which is greater than the threshold value of 23.685 and does not satisfy Equation (29). Therefore, it can be determined that FDIA is existed rather than the effect of mutation disturbance. When FDIA is existing in the power system, the results of both the consistency test and the residual test are greater than the corresponding thresholds, and finally the existence of FDIA can be determined.

In order to further verify the validity and applicability of the method, simulations were carried out in the IEEE-30 bus system in this paper. The simulation results in Fig. 7 and Fig. 8 show the estimates obtained for each bus using different estimation algorithms before and after the attack. Simulation results show that the WEKF maintains excellent estimation performance after an attack on the smart grid, but that the state estimates of the classical WLS deviate from the security values. Suppose we set the confidence level to 0.95 and the IEEE-30 bus system has 93 measurements and 59 state variables. Therefore, the redundancy is $k = m - n = 34$. The detection threshold obtained by querying the chi-square table was 48.602. After the attack, the estimated residual of WLS changes from 4.624 to 5.867, so it is below the threshold. As a result, classical BDD detection algorithms are unable to detect such attacks. To test for the FDIA, the consistency test is first carried out using Equation (28). The result of the consistency test was 1.844 when FDIA is not exist, but the result of the consistency test after the injection attack was 20.961. As the threshold for the consistency test is 3.216, the result of the consistency test after the attack is larger than the threshold. To eliminate the interference caused by external conditions, the residual test is continued using Equation (29). The result of the residual test for the WEKF estimate is 54.622, which is greater than the threshold value of 48.602 and does not satisfy Equation (29). Therefore it can be determined that FDIA is existed rather than the effect of mutation disturbance. Thus, by using Equations (28) and Equation (29), the FDIA can be effectively detected.

C. LOCATING THE FDIA

To further find the location of the FDIA, this paper conducts simulation experiments in an IEEE-14 bus system. When the FDIA is not exist, the objective function $J(\hat{x})$ is less than the detection threshold of the IEEE-14 bus system. At this point, the deviations in the state estimates of the WLS and WEKF are so minimal that no partitioning of the system is triggered.

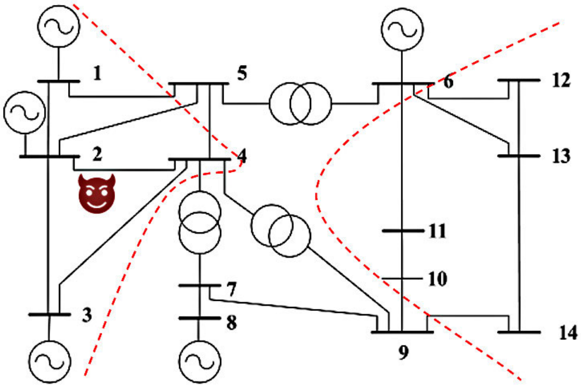

FIGURE 9. The partitioning of the IEEE-14 bus system.

TABLE 3. Subsystem chi-square detection.

Subsystem	$J(\hat{x})$	Threshold χ^2
1	20.145	12.592
2	6.473	9.488
3	7.811	9.488

In this paper, we use the construction approach of the attack vector in [21] to minimise the power increment of the bus and to decrease the modal length of the attack vector as much as possible. Firstly, use Equations (28) and Equations (29) to determine the existence of an FDIA. After that, the system triggers partitioning to divide the whole system into three subsystems. This partitioning approach allows for better maintenance of almost equal redundancy in each subsystem. The system is divided into three sections, I, II and III, as shown in Fig. 9. System partitioning decreases the redundancy of each subsystem, which results in lower thresholds for the chi-square test and ultimately makes the chi-square test more valid. The chi-square test was then performed in each subsystem, where the objective function value $J(\hat{x})$ and the detection threshold χ^2 for each subsystem are shown in Table 3. Since subsystems 2 and 3 are not under attack, the objective function value $J(\hat{x})$ is less than the chi-square test threshold χ^2. The objective function values for subsystems 2 and 3 were $J(\hat{x}) = 6.473$ and $J(\hat{x}) = 7.811$, respectively, which were both less than the chi-square test threshold of $\chi^2 = 9.488$. The objective function value of $J(\hat{x}) = 20.145$ for subsystem 1 is greater than the chi-square detection threshold of $\chi^2 = 12.592$, indicating the existence of FDIA in this subsystem.

Locating attacks in large scale power systems can be very difficult due to the very large redundancy. The simulation results show that the method proposed in this paper can effectively detect and locate area attacks.

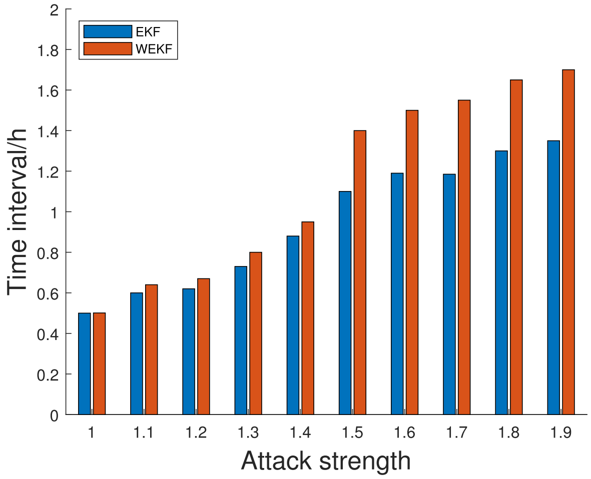

FIGURE 10. The comparison of detection performance with different attack strengths.

When Equation (28) is greater than the corresponding threshold and Equation (29) is less than the corresponding threshold, an alarm is triggered and the existence of FDIA is reported. To validate the detection performance of the WEKF and the conventional EKF under different attack intensities, we defined the length of the interval between starting and stopping the alarm to measure the detection performance. As shown in Fig. 10, as the attack intensity increases, the WEKF detection method proposed in this paper has better detection performance than the classical EKF detection method. The main reason for this is that the WEKF adaptively suppresses the FDIA as the attack intensity increases, thus making the difference between the estimates obtained by the two estimation methods larger. The increased discrepancy between the state estimates of the WLS and WEKF makes the FDIA more readily detectable.

VI. CONCLUSION AND FUTURE WORK

Considering that the conventional WLS and EKF cannot effectively detect and locate the FDIA, this paper proposes a method based on state deviation and system partitioning to effectively detect and locate the FDIA. By introducing an exponential weighting function to the conventional EKF, the degradation of detection performance due to the increased strength of the FDIA attack can be better suppressed. The consistency test of the WEKF and WLS estimates was performed to initially determine if there was false data injection attack in the system. In order to decrease the error detection rate, a residual test was then added to the consistency test, which ultimately made the test more robust. In order to further localise the detected FDIAs, the system partitioning method is proposed that maintains an almost equal degree of redundancy. This paper takes advantage of the fact that the redundancy of subsystems decreases, resulting in more efficient chi-square test for each subsystem. Finally, the experimental results demonstrate the excellent performance of the method proposed in this paper in detecting and locating the FDIA. In future work, we will detect other types of attacks in the power system, such as synchronous and immediate attacks. Simultaneously, detect and locate multi-point attacks in multiple areas of the power system.

REFERENCES

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

[2] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[3] J. Zhao, A. Gómez-Expósito, M. Netto, L. Mili, A. Abur, V. Terzija, I. Kamwa, B. Pal, A. K. Singh, J. Qi, Z. Huang, and A. P. S. Meliopoulos, "Power system dynamic state estimation: Motivations, definitions, methodologies, and future work," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3188–3198, Jul. 2019.

[4] M. Hasheminamin, V. G. Agelidis, V. Salehi, R. Teodorescu, and B. Hredzak, "Index-based assessment of voltage rise and reverse power flow phenomena in a distribution feeder under high PV penetration," *IEEE J. Photovolt.*, vol. 5, no. 4, pp. 1158–1168, Jul. 2015.

[5] X. Dou, J. Wang, Z. Wang, L. Li, L. Bai, S. Ren, and M. Gao, "A dispatching method for integrated energy system based on dynamic time-interval of model predictive control," *J. Mod. Power Syst. Clean Energy*, vol. 8, no. 5, pp. 841–852, 2020.

[6] M. A. M. Ariff, B. C. Pal, and A. K. Singh, "Estimating dynamic model parameters for adaptive protection and control in power system," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 829–839, Mar. 2015.

[7] Y. Yu, Z. Wang, and C. Lu, "A joint filter approach for reliable power system state estimation," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 1, pp. 87–94, Jan. 2019.

[8] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.

[9] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[10] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Atlanta, GA, USA, Dec. 2010, pp. 5991–5998.

[11] J. Farquharson, A. Wang, and J. Howard, "Smart grid cyber security and substation network security," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Washington, DC, USA, Jan. 2012, pp. 1–5.

[12] S. Cui, Z. Han, S. Kar, T. T. Kim, H. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[13] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.

[14] M. Du, G. Pierrou, X. Wang, and M. Kassouf, "Targeted false data injection attacks against AC state estimation without network parameters," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5349–5361, Nov. 2021.

[15] J. Zhao, G. Zhang, J. Y. Dong, and K. P. W. Davoudi, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Trans. Smart Grid.*, vol. 7, no. 1, pp. 6–8, Jan. 2016.

[16] 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.

[17] 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.

[18] C. Pei, Y. Xiao, W. Liang, and X. Han, "A deviation-based detection method against false data injection attacks in smart grid," *IEEE Access*, vol. 9, pp. 15499–15509, 2021.

[19] 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.

[20] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Vancouver, BC, Canada, Jul. 2013, pp. 1–5.

[21] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[22] C. Liu, H. Liang, and T. Chen, "Network parameter coordinated false data injection attacks against power system AC state estimation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1626–1639, Mar. 2021.

[23] N. N. Tran, H. R. Pota, Q. N. Tran, and J. Hu, "Designing constraint-based false data-injection attacks against the unbalanced distribution smart grids," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9422–9435, Jun. 2021.

[24] G. Cheng, Y. Lin, J. Zhao, and J. Yan, "A highly discriminative detector against false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2318–2330, May 2022.

[25] S. Nath, I. Akingeneye, J. Wu, and Z. Han, "Quickest detection of false data injection attacks in smart grid with dynamic models," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1292–1302, Feb. 2022.

[26] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[27] J. Zhao, G. Zhang, and R. A. Jabr, "Robust detection of cyber attacks on state estimators using phasor measurements," *IEEE Trans. Power Syst.*, vol. 32, no. 3, pp. 2468–2470, May 2017.

[28] M. Majdoub, J. Boukherouaa, B. Cheddadi, A. Belfqih, O. Sabri, and T. Haidi, "A review on distribution system state estimation techniques," in *Proc. 6th Int. Renew. Sustain. Energy Conf. (IRSEC)*, Rabat, Morocco, Dec. 2018, pp. 1–6.

[29] X. Kong, X. Zhang, X. Zhang, C. Wang, H.-D. Chiang, and P. Li, "Adaptive dynamic state estimation of distribution network based on interacting multiple model," *IEEE Trans. Sustain. Energy*, vol. 13, no. 2, pp. 643–652, Apr. 2022.

[30] R. Zhang, Q. Zhang, Z. Wang, and H. Sun, "Detection of false data injection attack in smart grid based on iterative Kalman filter," in *Proc. China Autom. Congr. (CAC)*, Beijing, China, Oct. 2021, pp. 6083–6088.

[31] H. Hossein and S. M. T. Bathaee, "Designing three indicators to detect false data injection attacks on smart grid by dynamic state estimation," *J. Intell. Fuzzy Syst.*, vol. 35, no. 5, pp. 5593–5604, Nov. 2018.

[32] K. Khanna, S. K. Singh, B. K. Panigrahi, R. Bose, and A. Joshi, "On detecting false data injection with limited network information using transformation based statistical techniques," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Chicago, IL, USA, Jul. 2017, pp. 1–5.

PENGFEI HU received the bachelor's degree in electrical engineering and automation from Chuzhou College, China, in 2020. He is currently pursuing the M.S. degree with the School of Electrical Engineering, Anhui Polytechnic University, China. His research interests include cyber security and power system state estimation.

WENGEN GAO received the Ph.D. degree from Jiangnan University, China. He is currently a Professor with the School of Electrical Engineering, Anhui Polytechnic University, China. He has published a considerable number of articles in international conferences. His research interests include microgrids control and energy optimization algorithms.

YUNFEI LI received the B.S. degree in communication engineering and the master's degree in automatic engineering from Anhui Polytechnic University, in 2012 and 2015, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Macau, Macau. He is currently with the Key Laboratory of Advanced Perception and Intelligent Control of High-End Equipment, Ministry of Education, Anhui Polytechnic University. His research interests include localization robust algorithm, secure localization algorithm, and statistical signal processing.

FENG HUA received the bachelor's degree from Anhui Polytechnic University, in 2021, where he is currently pursuing the master's degree. His research interests include attack defense and state estimation of smart grids, and the optimal placement of PMUs.

LINA QIAO received the bachelor's degree in electrical engineering and automation from the Wanjiang University of Technology, China, in 2021. She is currently pursuing the M.S. degree with the School of Electrical Engineering, Anhui Polytechnic University, China. Her research interest includes power system state estimation.

GUOQING ZHANG received the bachelor's degree in electrical engineering and automation from Anhui Polytechnic University, China, in 2022, where he is currently pursuing the M.S. degree with the School of Electrical Engineering. His research interests include cyber security and power system state estimation.