IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 November 2023, accepted 22 November 2023, date of publication 24 November 2023,
date of current version 1 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3336683

RESEARCH ARTICLE

Detection and Localization of False Data Injection Attacks in Smart Grid Based on Joint Maximum a Posteriori-Maximum Likelihood

GUOQING ZHANG, WENGEN GAO, YUNFEI LI, WENXIN HU, PENGFEI HU, AND FENG HUA

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 Open Research Fund of Anhui Province Key Laboratory of Detection Technology and Energy Saving Devices under Grant JCKJ2022C02 and Grant JCKJ2022A10, 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, and in part by the Open Research Fund of Anhui Province Key Laboratory of Electric Drive and Control under Grant DQKJ202103.

ABSTRACT State estimation plays a central role in ensuring the secure operation of the smart grid. However, deliberately designed false data injection attacks (FDIAs) can pass by conventional detections to manipulate the process of state estimation by injecting malicious data into measurements. Ultimately, FDIAs make the result of state estimation deviate from secure value and affect the security and stable operation of the power system. In this paper, we consider the different distribution characteristics between normal measurements and false measurements and build a Gaussian mixture model (GMM). Particularly, we focus on achieving joint detection and localization of FDIAs. To tackle these challenges, a model-based algorithm named Joint Maximum a Posteriori - Maximum Likelihood (JMAP-ML) is proposed to estimate the individual parameters of GMM and achieve joint detection and localization of FDIAs with high accuracy. Different testing scenarios in the IEEE-14-bus and IEEE-30-bus power systems are simulated to show the performance of the proposed algorithm on parameters estimation, FDIAs detection and localization. Numerical examples demonstrate the proposed algorithm achieves satisfactory results in detecting and localizing FDIAs compared to the other algorithms.

INDEX TERMS False data injection attacks, JMAP-ML, detection, localization, smart grid.

I. INTRODUCTION

Smart grid is a modern power system that uses advanced information and communication technologies to monitor, control and optimize the operation of the power system. While traditional power systems are mainly based on centralized energy generation and one-way energy transmission mode, the smart grid realizes digitalization, automation and intelligence of power systems by introducing advanced communication, sensing and control technologies [1], [2], [3]. However, the relations of modules in the smart grid cause it to be vulnerable to any intentional cyber-attacks [4]. If it is compromised by an adversary, the accident will cause significant damage, including prolonged power outages and electrical equipment damage [5], [6]. For example, the massive power outage in the northeastern United States in 2003 showed that even small failures in parts of the grid could end up costing billions of dollars [7]. A synchronized and coordinated cyber attack compromised three Ukrainian regional electric power distribution companies on 23 Dec.2015 which resulted in a significant effect on the lives of people of Ivano-Frankivsk, almost 1.4 million individuals lost electrical energy for 3 to 6 hours [8].

The cyber-physical system (CPS) mainly contains energy management system (EMS), supervisory control and data acquisition (SCADA) system, demand side management

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

system, etc. False Data Injection Attack (FDIA) is regarded as a means of attacking the integrity of state estimation data. The common attack strategies are shown in Figure 1: firstly, maliciously destroying the samples collected in the remote terminal units of the system; secondly, maliciously attacking the communication network; thirdly, attacking the SCADA system. The attacker can carefully design the attack vectors and inject false data through the above attack methods to damage the core equipment in the system, and ultimately interfere with the normal operation of the CPS [9], [10], [11].

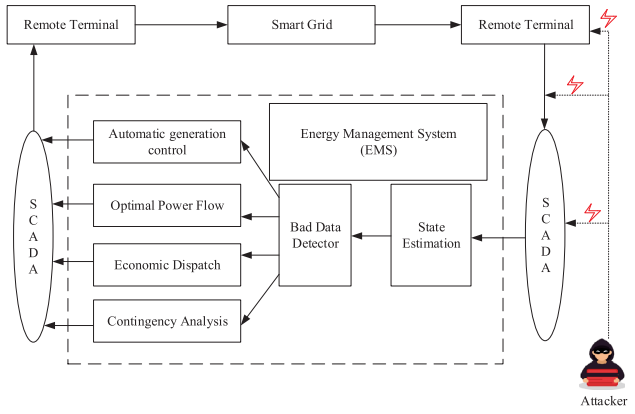

FIGURE 1. Schematic of false data injection attack in Smart Grid.

Liu et al. [12] first proposed the concept of grid false data injection attack and pointed out that the target of grid false data injection attack is the power system data, which poses a great threat to the state estimation link in the energy management system of the power system. Guo et al. [13] proposed an optimized attack strategy that can manipulate the estimation results without being detected. By exploring the impact of such an attack on the state estimation system, they analyze the vulnerabilities in the system and highlight the importance of developing robust defense mechanisms to counter malicious attacks. The FDIA in the power system is artificially orchestrated and highly covert, and can bypass the existing BDD mechanism such as the largest normalized residual (LNR) test and the Chi-square test [14], [15], [16] to destroy core equipment in the power CPS, leading to large-scale blackouts. Therefore, many researchers have worked on detecting false data injection attacks to secure the security of the smart grid.

This paper proposes the joint maximum a posteriori-maximum likelihood (JMAP-ML) detection algorithm which belongs to model-based detection. For model-based detection algorithms, the process of detection is relatively independent of each other. Additionally, in contrast to data-driven detection algorithms, it requires neither training data nor storing the training samples. Because the offset is introduced to the measurements after FDIAs, it brings about the differences in the model feature parameters between normal measurements and false measurements. Based on it, a Gaussian mixture model is built to approximate the error distribution. Hence, we use the JMAP-ML algorithm to estimate model parameters and eliminate the measurements affected by FDIAs. Finally, we can achieve the detection and localization of FDIAs. The main contributions of this paper are summarized as follows:

- Considering the joint detection and localization of the FDIAs problem, the paper proposes a JMAP-ML algorithm and achieves simultaneous detection and localization of FDIAs by modeling the hybrid measurements as a mixed Gaussian noise.
- Utilizing the proposed algorithm's iterative closed-form solution, we jointly localize the FDIAs and estimate the unknown parameters in the Gaussian mixture model with low computational complexity and high accuracy.
- Conducting numerical simulations on IEEE-14-bus and IEEE-30-bus test cases to verify the algorithm's performance, the results demonstrate that the proposed algorithm has a better performance in detecting and localizing the FDIAs than the other algorithms.

The rest of this paper is organized as follows. Section II introduces the related works about detection methods against FDIAs. Section III presents the model of the system framework and FDIAs. In Section IV, a Gaussian mixture model is used to approximate the distribution of the measurement errors. Section V presents the parameter estimation based on the JMAP-ML algorithm. Section VI presents the convergence and complexity analysis. Section VII provides simulation analysis. Finally, we conclude this paper in Section VIII.

II. RELATED WORKS

To achieve the goal of FDIAs detection in smart grid, many detection methods have been proposed by the researchers. Generally, they can be divided into two categories. One is model-based detection, the other is data-driven detection [16].

A. MODEL-BASED DETECTION

Nowadays, with the increasing degree of interconnection of power systems in smart grids, the simple use of the weighted least squares approach is no longer applicable and many variants have emerged, such as distributed state estimation [17], [18]. Ho et al. [19] proposed a great likelihood estimation-based network attack detection method that exploits the near chordal sparsity (NCS) of power grids to build an efficient framework for solving the associated great likelihood estimation problem, and then decomposes this detection method into several local ML estimation problems, which will ensure privacy and reduce the complexity of the potential problem. Chen et al. [20] propose a kernel density estimation-based method for FDIA detection. Based on historical records, this method can estimate the probability densities of measurements and control commands and give their confidence intervals at the significance level. Then, if a measurement (or a control command) fails its hypothesis test, it is replaced by the corresponding ML estimate. Shi et al. [21] proposed an efficient prediction-based FDIA detection and

localization scheme, which represents the state vectors of the smart grid as a multivariate time series and predicts them by intentionally exploiting the temporal and spatial correlation of the states through a vector autoregressive process (VAR). The consistency between predicted measurements and observations is utilized to detect and localize false data. Jorjani et al. [22] proposed FDIA detection method based on graph theory analysis. First, probability distributions of changes in the estimated state variables and measured values are used to detect outliers in the current state estimation results. Then, neighboring points in the identified outliers are found by constructing a graph. If there is sufficient evidence that the identified outliers are neighboring and related to each other, then the attack is detected and localized.

B. DATA-DRIVEN DETECTION

Unlike system model-based detection algorithms, data-driven detection algorithms are model-free. Therefore, the detection process of FDIAs does not involve system parameters and models, and it relies on a large amount of historical data from the smart grid as a way to speculate on future data [17]. Yu et al. [23] proposed a detection method based on wavelet transform and deep neural network for real-time detection of false data injection attacks. They first utilize wavelet transform for feature extraction of the data and then use RNN approach for FDIA detection. Zhang et al. [24] proposed a detection method based on semi-supervised deep learning, they used labeled and unlabeled data to achieve detection and classification of false data injection attacks. The method was able to automatically learn feature representations and perform the discrimination of false data injection attacks by deep neural networks. Aboelwafa et al. [25] performed FDIA detection using a deep neural network Autoencoder, which provides nonlinear compression (encoding) and expansion (decoding) of input samples. The detection scheme is based on the error between the decoded samples and the input of the network, and an anomaly is considered to exist when the error exceeds a certain level. Li et al. [26] proposed a distributed host-based collaborative detection method. Specifically, a majority voting algorithm based on a merging rule is used to collaboratively detect erroneous measurements inserted by damaged phase measurement units.

III. SYSTEM MODEL

The steady state of a power system is a basic requirement for power system operation, and it is essential for the quality and sustainability of power supply. Although the relationship between state variables and measurements in an actual power system is nonlinear, due to simplicity and robustness, a linear equation can be used based on the direct current (DC) model [15], [27], [28]. The following three assumptions are made to transform the nonlinear function into a linear function. First, when the power CPS operates normally, the bus voltage amplitudes are in the neighborhood of the rated voltage, i.e., $V_i = 1$; Second, for the UHV network, it is set to be a lossless circuit by neglecting the conductance; Third, in cyber-physical system, the phase difference between the buses of any two branches is not significant, i.e., $\theta_{ij} = 0$. An approximation can be obtained to get $\sin\theta_{ij} = 0$, $\cos\theta_{ij} = 1$.

The relationships between physical measurements and state variables are following:

$$P_i = \sum_{j \in T} B_{ij}\left(\theta_i - \theta_j\right) \tag{1}$$

$$Q_i = 0 \tag{2}$$

$$P_{ij} = -B_{ij}\left(\theta_i - \theta_j\right) \tag{3}$$

$$Q_{ij} = 0 \tag{4}$$

where P_i and Q_i represent the active and reactive power injection of bus i, respectively; P_{ij} and Q_{ij} denote active power flow and reactive power flow from bus i to bus j, respectively; B_{ij} denotes the susceptance of the line between from bus i to bus j; θ_{ij} denotes phase angle difference of the line voltage between from bus i to bus j; T denotes the set of adjacent buses of bus i.

We consider a power system with M measurements and F state variables. The relationships between measurements and state variables are following:

$$\boldsymbol{y_k} = \underbrace{\boldsymbol{H x_k}}_{=z_k} + \boldsymbol{e_k} \tag{5}$$

where $\boldsymbol{y}_k \in \mathbb{R}^{M\times 1}$ is the vector of original measurements; $\boldsymbol{z}_k \in \mathbb{R}^{M\times 1}$ is noise-free measurement vectors; $\boldsymbol{x}_k \in \mathbb{R}^{F\times 1}$ represents the vector of state variables; $\boldsymbol{e}_k \in \mathbb{R}^{M\times 1}$ is the measurement error vector and satisfies a Gaussian white distribution with zero mean and error covariance matrix $\boldsymbol{R}$, i.e., $\boldsymbol{R} = diag(\Sigma_1, \ldots, \Sigma_M)$; $\boldsymbol{H} \in \mathbb{R}^{M\times F}$ is the measurement Jacobian matrix. The attacker aims to inject malicious data into the measurements that are collected by SCADA in the way shown in Figure 1, the measurement model under FDIAs can be expressed as:

$$\boldsymbol{y_k^a} = \underbrace{\boldsymbol{H x_k}}_{=z_k} + \boldsymbol{e_k} + \boldsymbol{a_k} \tag{6}$$

where $\boldsymbol{a}_k \in \mathbb{R}^{M\times 1}$, $\boldsymbol{a_k} = [a_1, a_2, \cdots, a_M]^T$. When the meter $i \in [1, M]$ is not under attack, we have $a_i = 0$; otherwise $a_i \neq 0$ holds.

The presence of bad data is inevitably reflected in the objective function $\boldsymbol{J}(\hat{\boldsymbol{x}})$ and leads to $\boldsymbol{J}(\hat{\boldsymbol{x}})$ deviating significantly from its normal value; therefore, the general approach to detecting bad data boils down to some kind of hypothetical on the random variable $\boldsymbol{J}(\hat{\boldsymbol{x}})$. Weighted least squares is widely used to detect bad data, and the objective function $\boldsymbol{J}(\hat{\boldsymbol{x}})$ is expressed as:

$$\boldsymbol{J}(\hat{\boldsymbol{x}}) = (\boldsymbol{y}_k - \boldsymbol{H}\hat{\boldsymbol{x}_k})^T \boldsymbol{R}^{-1} (\boldsymbol{y}_k - \boldsymbol{H}\hat{\boldsymbol{x}_k}) \tag{7}$$

According to the minimum objective function $\boldsymbol{J}(\hat{\boldsymbol{x}})$, the state variables can be expressed as:

$$\hat{\boldsymbol{x_k}} = (\boldsymbol{H^T R^{-1} H})^{-1} \boldsymbol{H^T R^{-1} y_k} \tag{8}$$

thereby, we can obtain the estimated measurement vector

$$\hat{\boldsymbol{y}_k} = \boldsymbol{H}\hat{\boldsymbol{x}_k} = \boldsymbol{H}(\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}\boldsymbol{y_k} \tag{9}$$

After getting the measurement vector and the estimated measurement vector, the formula of residual is expressed as:

$$\boldsymbol{r_k} = \boldsymbol{y_k} - \hat{\boldsymbol{y}_k} = (\boldsymbol{I} - \boldsymbol{H}(\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}})\boldsymbol{y_k} \tag{10}$$

We can perform hypothesis testing to detect the bad data, the principle is that comparing the objective function $\boldsymbol{J}(\hat{\boldsymbol{x}})$ value of the WLS with the threshold value of the chi-square test [29], [30]. Specifically, the formula is expressed as:

$$\begin{cases} \boldsymbol{H_0} : \boldsymbol{J}(\hat{\boldsymbol{x}}) > \chi^2_{(M-F),p}, & \text{Bad data, Reject } \boldsymbol{H}_0 \\ \boldsymbol{H_1} : \boldsymbol{J}(\hat{\boldsymbol{x}}) \leq \chi^2_{(M-F),p}, & \text{No bad data, Accept } \boldsymbol{H}_0 \end{cases} \tag{11}$$

where $\boldsymbol{H}_0$ is on behalf of the original hypothesis, i.e., there exists no bad data; $\boldsymbol{H}_1$ is on behalf of the alternative hypothesis, i.e., there exists bad data. p and $M - F$ is the confidence level and the freedom of $\chi^2_{(M-F),p}$.

When attackers start to launch an FDIA, the form of the estimated state variables $\hat{\boldsymbol{x}^a_k}$ which is different from normal state variables can be expressed as:

$$\hat{\boldsymbol{x}^a_k} = (\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}(\boldsymbol{z_k} + \boldsymbol{a_k}) = \hat{\boldsymbol{x}_k} + \boldsymbol{c_k} \tag{12}$$

where $\boldsymbol{c}_k \in \mathbb{R}^{F\times 1}$ represents the introduced error to original state variables $\boldsymbol{x}_k$. The measurement residual under the attacks then can be expressed as follows:

$$\begin{aligned} \boldsymbol{r^a_k} &= \boldsymbol{z^a_k} - \boldsymbol{H}\hat{\boldsymbol{x}^a_k} = \boldsymbol{z_k} + \boldsymbol{a_k} - \boldsymbol{H}(\hat{\boldsymbol{x}_k} + \boldsymbol{c_k}) \\ &= \boldsymbol{z_k} - \boldsymbol{H}\hat{\boldsymbol{x}_k} + (\boldsymbol{a_k} - \boldsymbol{H}\boldsymbol{c_k}) \end{aligned} \tag{13}$$

Hence, if $\boldsymbol{a_k}$ satisfies the condition $\boldsymbol{a_k} = \boldsymbol{H}\boldsymbol{c_k}$, i.e., $\boldsymbol{r^a_k} = \boldsymbol{r_k}$, it means that the false measurements can bypass the measurement residual-based bad data detector. It is necessary for the attackers to obtain the Jacobian matrix $\boldsymbol{H}$ and have the ability to modify some meters. In a word, after the attackers obtain the Jacobian matrix $\boldsymbol{H}$, they could inject any bias into the state estimation $\boldsymbol{x_k}$. And they do not trigger the alarm of the bad data detector in the control center.

IV. MIXTURE MODEL FOR MEASUREMENTS

We assume N measurements of M measurements in the measurement vector $\boldsymbol{y}$ are continuously attacked. That is to say that N components in the attack vector a are not zero. The corresponding error samples come from two parts: one is the sample of N false measurements, and the other is the sample of $M - N$ normal measurements. In the subsequent measurements acquisition process, we identify whether the normal measurements are replaced with false measurements or not by the $K(K \geq 1)$ measurement vectors. To facilitate the analysis, the actual obtained component of the ith measurement of the kth measurement vector $\boldsymbol{y}_k$ can be expressed as:

$$\boldsymbol{y}_{i,k} = \boldsymbol{z}_{i,k} + \boldsymbol{e}_{i,k} \tag{14}$$

where $\boldsymbol{e}_{i,k}$ follows a Gaussian distribution, it can be divided into two cases: normal measurements errors distribution is expressed as ${p_e}^{(1)}(e;\, \mu_1, \sigma_1^2)$, conversely false measurements errors distribution is expressed as ${p_e}^{(2)}(e;\, \mu_2, \sigma_2^2)$.

For better understanding, a vector form which represents the measurement model is expressed as follows:

$$\boldsymbol{Y} = \boldsymbol{Z} + \boldsymbol{E} \tag{15}$$

where

$$\boldsymbol{Y} = \left[y_{1,1}, \ldots, y_{1,K}, \ldots, y_{M,1}, \ldots, y_{M,K}\right]^T \tag{16}$$

$$\boldsymbol{Z} = \left[z_{1,1}, \ldots, z_{1,K}, \ldots, z_{M,1}, \ldots, z_{M,K}\right]^T \tag{17}$$

$$\boldsymbol{E} = \left[e_{1,1}, \ldots, e_{1,K}, \ldots, e_{M,1}, \ldots, e_{M,K}\right]^T \tag{18}$$

Column vectors $\boldsymbol{Y}$, $\boldsymbol{Z}$ and $\boldsymbol{E}$ are all of dimension $MK \times 1$.

In this paper, we simplify the problem by using a Gaussian mixture model to represent the measurement errors.

$$p(e;\, \boldsymbol{\theta}) = \sum_{l=1}^{2} \alpha_l p_e^{(l)}(e;\, \mu_l, \sigma_l^2) \tag{19}$$

where α_l is an unknown parameter that represents the ratio of the components. It is assumed that N of M measurements are under attack. And $\alpha_1 = (M - N)/M$,$\alpha_2 = N/M$. It must satisfy a probability condition.

$$\sum_{l=1}^{2} \alpha_l = 1, \alpha_l \in [0, 1] \tag{20}$$

The main challenge of the Gaussian mixture distribution is to solve for the parameters of each part distribution $\boldsymbol{\theta} = \left[\alpha_1, \alpha_2, \mu_1, \mu_2, \sigma_1^2, \sigma_2^2\right]^T$. Hence, we can use the JMAP-ML algorithm to achieve our needs.

V. PARAMETERS ESTIMATION BASED ON JMAP-ML

Based on the measure model in (15) and Gaussian mixture distribution in (19), the cost function of $\boldsymbol{\theta} = \left[\alpha_1, \alpha_2, \mu_1, \mu_2, \sigma_1^2, \sigma_2^2\right]^T$ is given by

$$\begin{aligned} \mathcal{L}_I\left(\boldsymbol{\theta}; \boldsymbol{E}\right) &= \ln\left[p\left(\boldsymbol{E}; \boldsymbol{\theta}\right)\right] \\ &= \ln\left[\prod_{i=1}^{M}\prod_{k=1}^{K} p\left(e_{i,k}, \theta\right)\right] \\ &= \sum_{i=1}^{M}\sum_{k=1}^{K} \ln\left[\sum_{l=1}^{2} \alpha_l p_e^{(l)}\left(e_{i,k};\, \mu_l, \sigma_l^2\right)\right] \end{aligned} \tag{21}$$

The estimation of relevant parameters can be obtained by solving the following question

$$\begin{aligned} \arg\max_{\boldsymbol{\theta}} \quad & \mathcal{L}_I(\boldsymbol{\theta}; \boldsymbol{E}) \\ \text{subject to} \quad & \alpha_1 \geq 0,\ \alpha_2 \geq 0, \\ & \alpha_1 + \alpha_2 = 1 \end{aligned} \tag{22}$$

It is complicated for us to solve the cost function in (21), essentially, the JMAP-ML algorithm is an approximation to the maximum likelihood estimate (MLE). Therefore, to simplify the complexity of the cost function, we introduce the

latent variable $\boldsymbol{h} = \left[h_{1,1}, \ldots, h_{1,K}, \ldots, h_{M,1}, \ldots, h_{M,K}\right]^T$. By the value of $\boldsymbol{h}_{i,k}$, we can know which mixture component has generated the corresponding measurement error, with

$$h_{i,k} = \begin{cases} 1, & e_{i,k} \in p_e^{(1)}\left(e; \mu_1, \sigma_1^2\right) \\ 2, & e_{i,k} \in p_e^{(2)}\left(e; \mu_2, \sigma_2^2\right) \end{cases} \tag{23}$$

On the basis of the latent variable h, we set $\boldsymbol{o} = \{\boldsymbol{h}, \boldsymbol{E}\}$. To avoid ambiguity, we define $\{\boldsymbol{E}; \boldsymbol{\theta}\}$ as incomplete data and $\{\boldsymbol{E}, \boldsymbol{h}; \boldsymbol{\theta}\}$ as complete data. The complete data log-likelihood function is easily expressed as:

$$\begin{aligned} \mathcal{L}_C\left(\boldsymbol{\theta}; \boldsymbol{E}, \boldsymbol{h}\right) &= \ln\left[p\left(\boldsymbol{h}, \boldsymbol{E}; \boldsymbol{\theta}\right)\right] \\ &= \ln\left[\prod_{i=1}^{M}\prod_{k=1}^{K} p\left(e_{i,k}, h_{i,k}, \boldsymbol{\theta}\right)\right] \\ &= \sum_{i=1}^{M}\sum_{k=1}^{K} \ln\left(\alpha_{h_{i,k}} p_e^{(h_{i,k})}\left(e_{i,k}; \mu_{h_{i,k}}, \sigma_{h_{i,k}}^2\right)\right) \end{aligned} \tag{24}$$

the above equation holds provided that $e_{i,k}$'s are independent, consequently, $h_{i,k}$'s which are similar to $e_{i,k}$'s are also independent. It is obvious that the calculation method of the complete data log-likelihood function $\mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}, \boldsymbol{E})$ is simpler. The problem of solving MLE (22) becomes

$$\begin{aligned} \arg\max_{\theta} \quad & \mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}, \boldsymbol{E}) \\ \text{subject to} \quad & \alpha_1 \geq 0, \ \alpha_2 \geq 0, \\ & \alpha_1 + \alpha_2 = 1 \end{aligned} \tag{25}$$

Because of introducing latent variable h, it is not difficult to find that the complete data log-likelihood function has a more solution-friendly form.

As the mean of approximating the MLE, we adopt the idea of MLE to process the data, i.e., the complete data log-likelihood function $\mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}, \boldsymbol{E})$ is maximized directly with respect to both $\boldsymbol{\theta}$ and $\boldsymbol{h}$, that is,

$$\arg\max_{\boldsymbol{\theta}, \boldsymbol{h}} \mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}, \boldsymbol{E}) = \arg\max_{\boldsymbol{\theta}} \left\{\arg\max_{\boldsymbol{h}} \mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}, \boldsymbol{E})\right\} \tag{26}$$

The JMAP-ML algorithm which is divided into two steps is an iterative algorithm, the specific steps are as follows:

A. MAP STEP

The estimation of parameter $\boldsymbol{h}$ is the first step of JMAP-ML algorithm. To facilitate the solution, we need to transform the likelihood function as follows:

$$\mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}, \boldsymbol{E}) = \ln p(\boldsymbol{h}, \boldsymbol{E}; \boldsymbol{\theta}) = \ln p(\boldsymbol{h}|\boldsymbol{E}; \boldsymbol{\theta}) + \ln p(\boldsymbol{E}; \boldsymbol{\theta}) \tag{27}$$

where $\ln p(\boldsymbol{E}; \boldsymbol{\theta})$ is independent of $\boldsymbol{h}$. Therefore, the maximization of (27) can be replaced by maximization concerning the front conditional probability function as shown as follows:

$$\arg\max_{\boldsymbol{h}} \quad \ln p(\boldsymbol{h}|\boldsymbol{E}; \boldsymbol{\theta}) \tag{28}$$

Replacing $\boldsymbol{\theta}$ with the ηth iteration $\boldsymbol{\theta}^{(\eta)}$, and solving the MAP estimation of $\boldsymbol{h}$, yields

$$\boldsymbol{h}^{(\eta+1)} = \arg\max_{\boldsymbol{h}} \quad \ln p(\boldsymbol{h}|\boldsymbol{E}; \boldsymbol{\theta}^{(\eta)}) \tag{29}$$

which can be slashed into MK simpler pieces as follows:

$$h_{i,k}{}^{(\eta+1)} = \arg\max_{h_{i,k}} \quad \ln p(h_{i,k}|\boldsymbol{e}_{i,k}; \boldsymbol{\theta}^{(\eta)}) \tag{30}$$

$\forall (i,k) \in P \triangleq \{(1,1), \cdots, (1,K), \cdots, (1,M), \cdots, (M,K)\}$. With $p\left(h_{i,k} = l \middle| e_{i,k}; \boldsymbol{\theta}^{(\eta)}\right)$ being calculated by the following equation (31) which can be computed by means of Bayes'rule as follows:

$$p\left(h_{i,k} = l \middle| e_{i,k}, \boldsymbol{\theta}^{(\eta)}\right) = \frac{\alpha_l^{(\eta)} p_e^{(l)}\left(e_{i,k}; \mu_l, \sigma_l^{2,(\eta)}\right)}{p\left(e_{i,k}; \boldsymbol{\theta}^{(\eta)}\right)} \tag{31}$$

with

$$p\left(e_{i,k}; \boldsymbol{\theta}^{(\eta)}\right) = \sum_{l=1}^{2} \alpha_l^{(\eta)} p_e^{(l)}\left(e_{i,k}; \mu_l^{(\eta)}, \sigma_l^{2,(\eta)}\right) \tag{32}$$

Since $h_{i,k}$ is discrete-valued, the global optimal solution to (30) must be the one among $\{h_{i,k} = 1, 2\}$ that maximizes $\ln\left[p\left(h_{i,k} \middle| e_{i,k}, \theta^{(\eta)}\right)\right]$. By defining

$$\Gamma_{i,k,l}^{(\eta)} \triangleq \alpha_l^{(\eta)} p_e^{(l)}\left(e_{i,k}; \mu_l^{(\eta)}, \sigma_l^{2,(\eta)}\right), l = 1,2 \tag{33}$$

Because $\ln(.)$ is a monotonic function, we need only to compare the value of $\Gamma_{i,k,l}^{(\eta)}$ and give the MAP estimation as follows:

$$h_{i,k}^{(\eta)} = \begin{cases} 1, & \Gamma_{i,k,1}^{(\eta)} \geq \Gamma_{i,k,2}^{(\eta)} \\ 2, & \Gamma_{i,k,1}^{(\eta)} < \Gamma_{i,k,2}^{(\eta)} \end{cases} \tag{34}$$

B. ML STEP

The estimation of parameter $\boldsymbol{\theta}$ is the second step of JMAP-ML algorithm. By substituting the estimated $\boldsymbol{h}^{(\eta+1)}$ into the complete log-likelihood function $\mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}, \boldsymbol{E})$, the complete log-likelihood function can be reformulated as:

$$\begin{aligned} &\mathcal{L}_c\left(\boldsymbol{\theta}; \boldsymbol{E}, \boldsymbol{h}^{(\eta+1)}\right) \\ &= \ln\left[p\left(\boldsymbol{E}, \boldsymbol{h}^{(\eta+1)}; \boldsymbol{\theta}\right)\right] \\ &= \sum_{i=1}^{M}\sum_{k=1}^{K} \ln\left(\alpha_{h_{i,k}^{(\eta+1)}} p_e^{\left(h_{i,k}^{(\eta+1)}\right)}\left(e_{i,k}; \mu_l, \sigma_l^2\right)\right) \\ &= \sum_{i=1}^{M}\sum_{k=1}^{K}\sum_{l=1}^{2} \ln\left(\alpha_l p_e^{(l)}\left(e_{i,k}; \mu_l, \sigma_l^2\right)\right) \delta\left(l - h_{i,k}^{(\eta+1)}\right) \end{aligned} \tag{35}$$

where

$$\delta\left(l - h_{i,k}^{(\eta+1)}\right) = \begin{cases} 1, \textit{if} \ \ l = h_{i,k}^{(\eta+1)} \\ 0, \textit{otherwise} \end{cases} \tag{36}$$

is impulse function. In the subsequent step, we maximize $\mathcal{L}_c\left(\boldsymbol{\theta}; \boldsymbol{h}^{(\eta+1)}, \boldsymbol{E}\right)$ with respect to $\boldsymbol{\theta}$, and thus can obtain the $(\eta+1)$th iteration of the $\boldsymbol{\theta}$

$$\boldsymbol{\theta}^{(\eta+1)} = \arg\max_{\boldsymbol{\theta}} \mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{h}^{(\eta+1)}, \boldsymbol{E}) \tag{37}$$

To facilitate the calculation, we introduce the weighting function $\omega_{i,k,l}$. Hence, the cost function (35) can be transformed into another form as follows:

$$\begin{aligned}
&\mathcal{L}_c^{(\eta)}\left(\boldsymbol{\theta}; \boldsymbol{E}, \boldsymbol{h}^{(\eta+1)}\right) \\
&= \ln\left[p\left(\boldsymbol{E}, \boldsymbol{h}^{(\eta+1)}; \boldsymbol{\theta}\right)\right] \\
&= \sum_{i=1}^{M}\sum_{k=1}^{K}\sum_{l=1}^{2} \omega_{i,k,l}^{(\eta)} \ln\left[\alpha_l p_e^{(l)}\left(e_{i,k}; \mu_l, \sigma_l^2\right)\right] \\
&= \sum_{i=1}^{M}\sum_{k=1}^{K}\left(\omega_{i,k,1}^{(\eta)} \ln\alpha_1 + \omega_{i,k,2}^{(\eta)} \ln\alpha_2\right) \\
&\quad + \sum_{i=1}^{M}\sum_{k=1}^{K}(\omega_{i,k,1}^{(\eta)} \ln p_e^{(1)}\left(e_{i,k}; \mu_1, \sigma_1^2\right) \\
&\quad + \sum_{i=1}^{M}\sum_{k=1}^{K}(\omega_{i,k,2}^{(\eta)} \ln p_e^{(2)}\left(e_{i,k}; \mu_2, \sigma_2^2\right)
\end{aligned} \tag{38}$$

where the weighting function $\omega_{i,k,l}^{(\eta)}$ is defined by

$$\omega_{i,k,l}^{(\eta)} = \delta\left(l - h_{i,k}^{(\eta+1)}\right) \tag{39}$$

In (38), we can simplify this formula

$$\mathcal{L}_c^{(\eta)}\left(\boldsymbol{\theta}; \boldsymbol{E}, \boldsymbol{h}^{(\eta+1)}\right) = \mathcal{L}_0^{(\eta)}(\alpha_1, \alpha_2) + \sum_{l=1}^{2} \mathcal{L}_l^{(\eta)}\left(\mu_l, \sigma_l^2\right) \tag{40}$$

where

$$\mathcal{L}_0^{(\eta)}(\alpha_1, \alpha_2) \triangleq \sum_{i=1}^{M}\sum_{k=1}^{K}\left(\omega_{i,k,1}^{(\eta)} \ln\alpha_1 + \omega_{i,k,2}^{(\eta)} \ln\alpha_2\right) \tag{41}$$

and for $l = 1, 2$,

$$\mathcal{L}_l^{(\eta)}\left(\mu_l, \sigma_l^2\right) \triangleq \sum_{i=1}^{M}\sum_{k=1}^{K} \ln\left(p_e^{(l)}\left(e_{i,k}; \mu_l, \sigma_l^2\right)\right)\omega_{i,k,l}^{(\eta)} \tag{42}$$

First, we maximize $\mathcal{L}_c(\boldsymbol{\theta}; \boldsymbol{E}, \boldsymbol{h})$ concerning the mixture model parameters by following the route shown in (38). More precisely, we solve the following equations:

$$\frac{\partial}{\partial\alpha_l}\left[\mathcal{L}_0^{(\eta)}(\alpha_1, \alpha_2) + \lambda\left(\sum_{l=1}^{2}\alpha_l - 1\right)\right] = 0 \tag{43}$$

$$\frac{\partial}{\partial\mu_l}\left[\mathcal{L}_l^{(\eta)}\left(\mu_l, \sigma_l^2\right)\right] = 0 \tag{44}$$

$$\frac{\partial}{\partial\sigma_l^2}\left[\mathcal{L}_l^{(\eta)}\left(\mu_l^{(\eta+1)}, \sigma_l^2\right)\right] = 0 \tag{45}$$

where λ in (43) is the Lagrange multiplier. By solving the above equations which are in closed form, the estimation of α_l, μ_l and σ_l^2 are given by

$$\alpha_l^{(\eta+1)} = \frac{1}{MK}\sum_{i=1}^{M}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)} \tag{46}$$

$$\mu_l^{(\eta+1)} = \frac{\sum_{i=1}^{M}\sum_{k=1}^{K}\left(y_{i,k} - z_{i,k}\right)\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{M}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}} \tag{47}$$

$$\sigma_l^{2,(\eta+1)} = \frac{\sum_{i=1}^{M}\sum_{k=1}^{K}\left(y_{i,k} - z_{i,k} - \mu_l^{(\eta+1)}\right)^2\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{M}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}} \tag{48}$$

Given the detailed estimation, we introduced the workflow of the proposed JMAP-ML in algorithm 1. Then, to better understand, a flow chart of detecting FDIAs which is shown in Figure 2 is also introduced.

Algorithm 1 JMAP-ML Algorithm for Estimating Parameters of GMM

Input: Y and Z. For each dataset with $i = 1, 2, \ldots, N$, $k = 1, 2, \ldots, K$.

Step1 Initialize:

Chose a convergence tolerance Δ and the maximum number of iterations $N_{itr}^{\max}$; Set the iteration index $\eta = 0$; Chose an initial guess $\boldsymbol{\theta}^{(0)} = \left[\alpha_1, \alpha_2, \mu_1, \mu_2, \sigma_1^2, \sigma_2^2\right]^T$.

Step2 JMAP-ML algorithm loop:

In the $(\eta+1)$th iteration $(\eta > 0)$,

1: Compute $h_{i,k}^{(\eta)}$ according to Equation (34).

2: Compute $\omega_{i,k,l}^{(\eta)}$ according to Equation (39).

3: Find close form $\boldsymbol{\theta}^{(0)}$ in attempts to maximize Equation (40).

Step3 Convergence Check:

If the increment of the log-likelihood value is less than Δ or $N_{itr}^{\max}$ has been reached, then terminate this algorithm; otherwise set $\eta \to \eta + 1$ and return to Step2.

Output: $\left\{E, \boldsymbol{h}^{(\eta+1)}\right\}$ and $\boldsymbol{\theta}^{(\eta+1)}$.

VI. ALGORITHM ANALYSIS

A. CONVERGENCE ANALYSIS

As it is shown in Algorithm V-B, the JMAP-ML algorithm is an iterative algorithm. Hence, it is necessary to ensure the algorithm converges which means the JMAP-ML algorithm converges monotonically to some stationary point $\mathcal{L}_C{}^*$ of the complete data log-likelihood function at the end. To verify this question, we conducted a correlation analysis.

In the first step of the JMAP-ML algorithm, we maximize $\mathcal{L}_C(\boldsymbol{\theta}; \boldsymbol{E}, \boldsymbol{h})$ with respect to $\boldsymbol{h}$ for a given a priori parameter estimate $\boldsymbol{\theta}^{(\eta)}$. Since $\boldsymbol{h}^{(\eta+1)}$ is the global optimal solution, it is

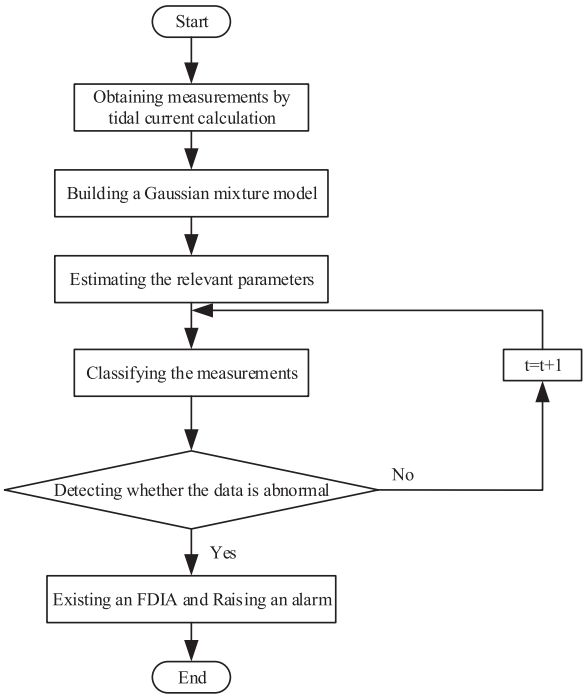

FIGURE 2. The flow chart of detecting FDIAs.

guaranteed that

$$\mathcal{L}_{\mathcal{C}}\left(\boldsymbol{\theta}^{(\eta)};\boldsymbol{h}^{(\eta+1)},\boldsymbol{E}\right)\geq\mathcal{L}_{\mathcal{C}}\left(\boldsymbol{\theta}^{(\eta)};\boldsymbol{h}^{(\eta)},\boldsymbol{E}\right)\tag{49}$$

holds for any $\boldsymbol{h}^{(\eta)}$ in its parameter space.

In the second step, we maximine $\mathcal{L}_{\mathcal{C}}\left(\boldsymbol{\theta};\boldsymbol{h}^{(\eta+1)},\boldsymbol{E}\right)$ with respect to $\boldsymbol{\theta}$. Similar to the EM algorithm, here we need to consider the Q function:

$$Q\left(\boldsymbol{\theta},\boldsymbol{\theta}^{(\eta)}\right)=\sum_{h}\ln\left[p\left(h,E;\boldsymbol{\theta}\right)\right]p\left(h\,|E\,;\boldsymbol{\theta}^{(\eta)}\right)\tag{50}$$

then, we need to prove that $Q\left(\boldsymbol{\theta}^{(\eta+1)},\boldsymbol{\theta}^{(\eta)}\right)\geq Q\left(\boldsymbol{\theta}^{(\eta)},\boldsymbol{\theta}^{(\eta)}\right)$ holds for any $\boldsymbol{\theta}^{(\eta)}$ in its parameters space. In EM algorithm, the E-step is $\boldsymbol{\theta}^{(\eta+1)}=\arg\max_{\theta}Q(\boldsymbol{\theta},\boldsymbol{\theta}^{(\eta)})$, so the above relationship can be proven. For Gaussian distribution, [31] and [32] show that the update parameters $\alpha_1^{(\eta+1)}$, $\alpha_2^{(\eta+1)}$, $\mu_1^{(\eta+1)}$, $\mu_2^{(\eta+1)}$, $\sigma_1^{2,(\eta+1)}$, $\sigma_2^{2,(\eta+1)}$ are global optimal solutions to the corresponding maximization problems. Based on it, we can easily prove that

$$\mathcal{L}_{\mathcal{C}}\left(\boldsymbol{\theta}^{(\eta+1)};\boldsymbol{h}^{(\eta+1)},\boldsymbol{E}\right)\geq\mathcal{L}_{\mathcal{C}}\left(\boldsymbol{\theta}^{(\eta)};\boldsymbol{h}^{(\eta+1)},\boldsymbol{E}\right)\tag{51}$$

which means that the value of $\mathcal{L}_{\mathcal{C}}\left(\boldsymbol{\theta};h,E\right)$ increases monotonically over iterations. Since $\mathcal{L}_{\mathcal{C}}\left(\boldsymbol{\theta};h,E\right)$ is bounded from above, the convergence to some stationary point $\mathcal{L}^*$ is ensured.

B. COMPLEXITY ANALYSIS

In the complexity analysis, we pay more attention to the iterative process of the JMAP-ML algorithm, as it consumes the most computational power. The complexity is evaluated in terms of floating-point operations (FLOPs). We define the FLOPs required for some elementary operations as follows:

(1) ε_{add}: FLOPs for addition.
(2) ε_{sub}: FLOPs for subtraction.
(3) ε_{mul}: FLOPs for multiplication.
(4) ε_{div}: FLOPs for division.
(5) ε_{exp}: FLOPs for exponential.
(6) ε_{pow}: FLOPs for raising to real power.
(7) ε_{com}: FLOPs for comparison.

Note that the actual FLOPs required for the above operations may vary with processors.

Since the JMAP-ML algorithm is iterative in nature, we spotlight the analysis in one JMAP-ML iteration, for instance, the $(\eta+1)$th. The estimation step starts with the evaluations of $\omega_{i,k,l}^{(\eta)}=\delta\left(l-h_{i,k}^{(\eta)}\right)$ for $i=1,2,\cdots,M$, $k=1,2,\cdots,K$ and $l=1,2$, given the prior parameter estimate $\boldsymbol{\theta}^{(\eta)}$. This requires us to compute

$$e_{i,k}=y_{i,k}-z_{i,k}\tag{52}$$

for $i=1,2,\cdots,M,k=1,2,\cdots,K$.

$$\Gamma_{i,k,l}=\frac{\alpha_l^{(\eta)}}{\sqrt{2\pi\sigma_l^{2,(\eta)}}}.\exp\left[\frac{\left(e_{i,k}-\mu_l^{(\eta)}\right)}{-2\sigma_l^{2,(\eta)}}\right]\tag{53}$$

for $i=1,2,\cdots,M,k=1,2,\cdots,K,l=1,2$.

It is clear that the equation (52) requires $MK\varepsilon_{sub}$ FLOPs, the equation (53) requires $2((MK+3)\varepsilon_{mul}+(MK+1)\varepsilon_{pow}+MK\varepsilon_{sub}+MK\varepsilon_{div}+MK\varepsilon_{exp})$ FLOPs. To get $h_{i,k}$, we also need $MK\varepsilon_{com}$ FLOPs.

Having $\delta\left(l-h_{i,k}^{(\eta)}\right)$'s, we then compute

$$\alpha_l^{(\eta+1)}=\frac{1}{MK}\sum_{i=1}^{M}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}\tag{54}$$

$$\mu_l^{(\eta+1)}=\frac{\sum_{i=1}^{M}\sum_{k=1}^{K}\left(y_{i,k}-z_{i,k}\right)\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{M}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}}\tag{55}$$

$$\sigma_l^{2,(\eta+1)}=\frac{\sum_{i=1}^{M}\sum_{k=1}^{K}\left(y_{i,k}-z_{i,k}-\mu_l^{(\eta+1)}\right)^2\omega_{i,k,l}^{(\eta)}}{\sum_{i=1}^{M}\sum_{k=1}^{K}\omega_{i,k,l}^{(\eta)}}\tag{56}$$

for $i=1,2,\cdots,M,k=1,2,\cdots,K,l=1,2$.

It is easy to verify that Equation (54) requires $(MK-1)\,\varepsilon_{add}+1\varepsilon_{div}+1\varepsilon_{sub}$ FLOPs. Equation (55) requires $2\left(MK\varepsilon_{mul}+(MK-1)\,\varepsilon_{add}+\varepsilon_{div}\right)$ FLOPs, and Equation (56) requires $2(MK\varepsilon_{mul}+(MK+1)\varepsilon_{pow}+\varepsilon_{sub}+\varepsilon_{div}+(MK-1)\,\varepsilon_{add})$ FLOPs. Let us define $FL\,(\boldsymbol{\theta})$ to be the total number of FLOPs consumed for an estimate of $\boldsymbol{\theta}$ in one JMAP-ML iteration. It is straightforward that $FL\,(\boldsymbol{\theta})$ is equal to the total FLOPs.

$$\begin{aligned}FL\,(\boldsymbol{\theta})=&\,(5MK-5)\,\varepsilon_{add}+(3MK+3)\varepsilon_{sub}\\&+(6NK+6)\,\varepsilon_{mul}+(2MK+5)\,\varepsilon_{div}\end{aligned}$$

$$+ 2MK\varepsilon_{exp} + (4MK + 4)\,\varepsilon_{pow} + MK\varepsilon_{com} \quad (57)$$

Finally, let $N_{iter}^{JMAP-ML}$ be the number of iterations used to reach the convergence of the JMAP-ML algorithm. The total FLOPs used to compute an ultimate JMAP-ML estimate is

$$FL_{JMAP-ML} \approx N_{iter}^{JMAP-ML} FL(\boldsymbol{\theta}) \quad (58)$$

VII. SIMULATIONS

In this section, we verify the feasibility of the proposed algorithm via the IEEE-14-bus and IEEE-30-bus power systems. We conduct the simulation in MATLAB R2020b software and use the MATPOWER 7.1 power simulation package to calculate the routine power flow of the related data. Based on it, the optimal tidal current is solved, and we can obtain the true measurements. Then, the Gaussian white noise is superimposed as the sensor measurements.

A. IEEE-14-BUS POWER SYSTEM

First, the power standard IEEE-14-bus system which is shown in Figure 3 is used for simulation analysis. A Gaussian mixture model is utilized to fit the bus measurement sequences for the grid system buses. The JMAP-ML algorithm is used to estimate the parameter values of the model to which the normal and attacked measurements belong, respectively. Based on the obtained mixing model, the test data are fed into the model for binary categorization of the measurements. Thus, normal measurements are categorized with false measurements.

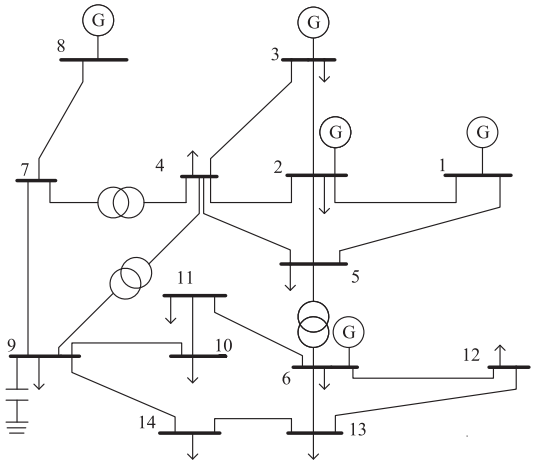

FIGURE 3. IEEE-14-bus power system.

A summary of the simulation parameters used throughout the process is provided in Table 1. The relevant parameters in the table are explained as follows: M stands for the dimension of the measurements; K represents the number of groups of measurements; $\alpha_1 and \alpha_2$ is component ratio; μ_1 and μ_2 is the mean of the Gaussian distribution, respectively; σ_1 and σ_2 represent the variance of the Gaussian distribution; Δ is convergence tolerance; $N_{itr}^{\max}$ is the maximum number of iterations.

We represent the errors of the 1640 normal measurements as bar graphs, and the distribution characteristics of the

TABLE 1. Simulation parameters.

Parameters	Value
M	41
K	40
α_1	0.8
α_2	0.2
μ_1	0
μ_2	0.03
σ_1	0.1
σ_2	0.05
Δ	10^{-6}
$N_{itr}^{\max}$	50

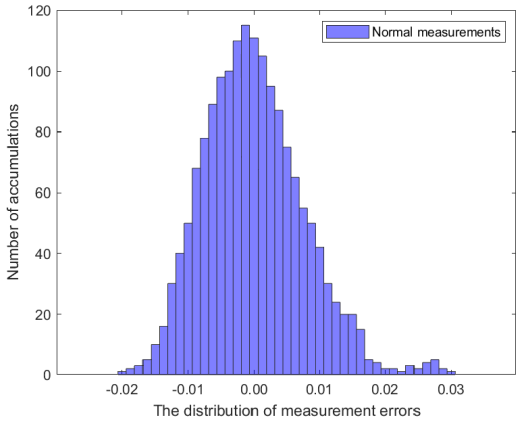

FIGURE 4. The normal distribution of measurement errors.

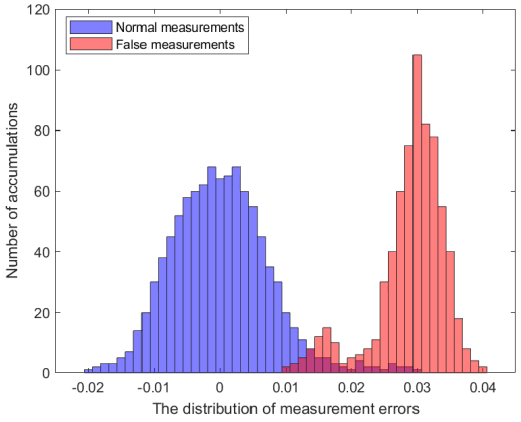

FIGURE 5. The actual distribution of measurement errors under FDIAs.

normal measurement errors are shown in Figure 4. After the power system is subjected to the FDIAs, the measurements z will change, the error in some of the measurements changes from e to $a + e$. Figure 5 shows the actual distribution characteristics of the mixed measurement errors. Then, to verify the proposed algorithm, we use the JMAP-ML algorithm to classify the measurement errors, and also fit the error distribution, the final result is shown in Figure 6.

Next, it is necessary to verify the convergence of the proposed algorithm. Utilizing the IEEE-14-bus power system, we assume $N = 8$ and use the Monte Carlo method to produce the measurements and perform 1200 independent experiments. Meanwhile, we need to record the values of incomplete data and complete data and parameter estimates versus the number of iterations for the JMAP-ML algorithm.

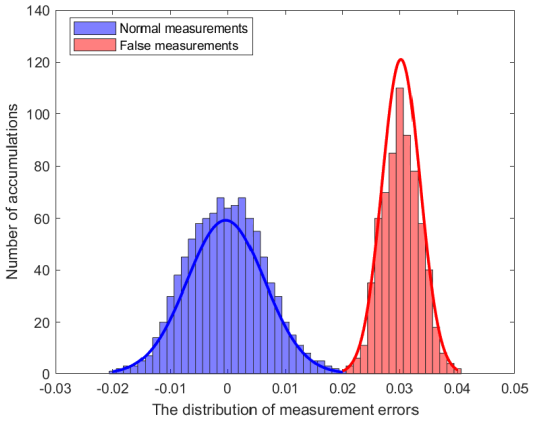

FIGURE 6. The distribution of measurement errors with JMAP-ML.

Then we compute the mean of the incomplete data, complete data and parameter estimates. Figure 7 shows the relationship between incomplete data and complete data and the number of iterations. In Figure 8, Figure 9 and Figure 10, it can be easily seen the relationship between the parameters α_1, μ_2, σ_1^2 and the number of iterations. For better understanding, we give their real values.

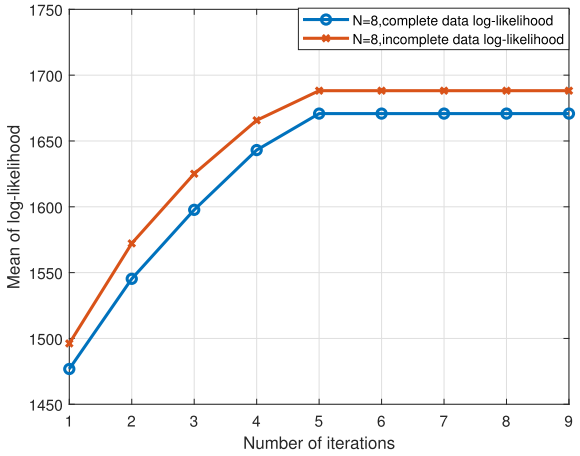

FIGURE 7. The change in the mean of the log-likelihood function value under the JMAP-ML algorithm.

We explain some of the important conclusions in the above figures as follows:

- From Figure 7, we can observe that the incomplete data and complete data log-likelihoods increase monotonically iterations until the convergence condition has been fulfilled, which coincides with our theoretical proofs.
- From Figure 8, Figure 9 and Figure 10, we can conclude that the JMAP-ML algorithm generates a biased estimator, it can estimate the relevant parameters with high accuracy.
- The JMAP-ML algorithm is converged after 5 iterations.

In addition, we simulate different attack scenarios and estimate the relevant parameters using the proposed algorithm. Below, we explore the relationship between the accuracy of the parameter estimates and the number of attacked buses. Because of the limited space, we only give the parameter α_2,

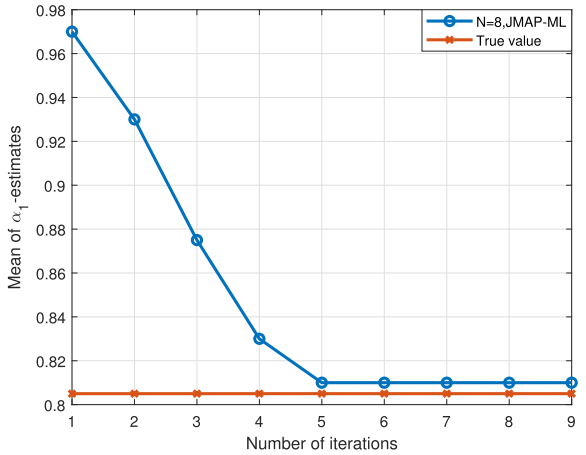

FIGURE 8. Mean of α_1 estimates as the number of iterations increases.

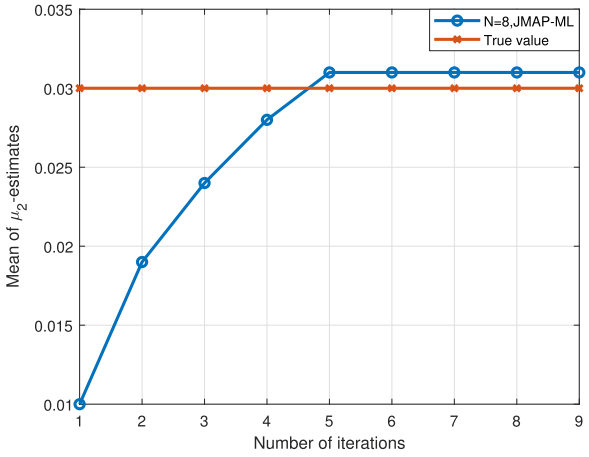

FIGURE 9. Mean of μ_2 estimates as the number of iterations increases.

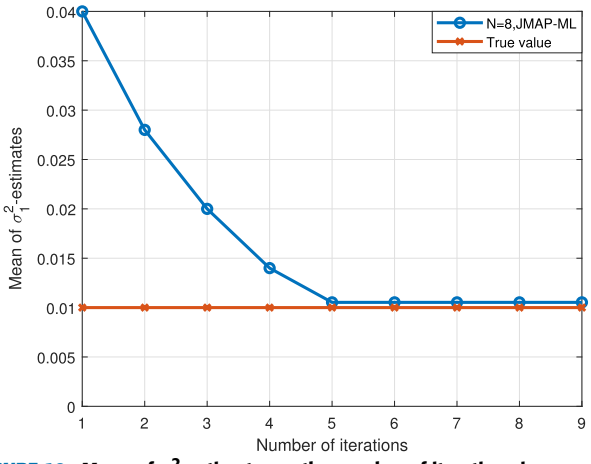

FIGURE 10. Mean of σ_1^2 estimates as the number of iterations increases.

μ_2, σ_2^2. From Figure 11, Figure 12 and Figure 13, we can obviously see that as the attacked buses increase, the accuracy of the parameters becomes higher and higher.

The receiver operating characteristic (ROC) curve is adopted for analysis. The ROC curve is shown with true positive rate (TPR) as the vertical coordinate and false positive rate (FPR) as the horizontal coordinate. Here, the true

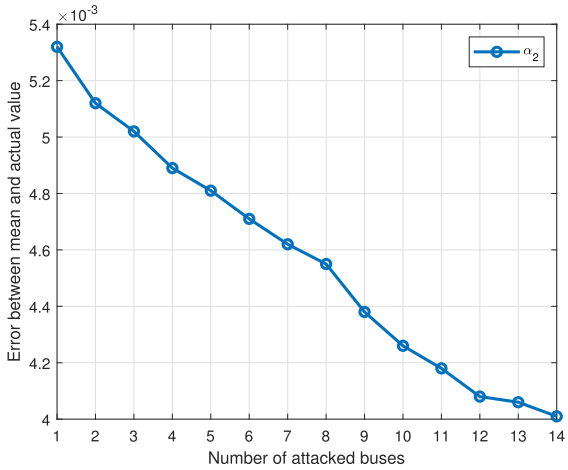

FIGURE 11. The error variation of the parameter α_2 as the number of attacked buses varies.

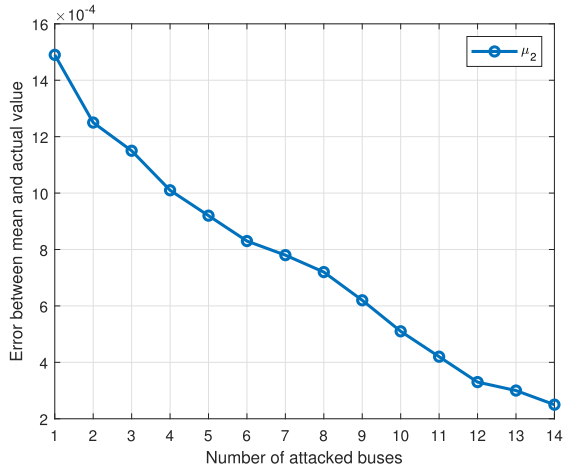

FIGURE 12. The error variation of the parameter μ_2 as the number of attacked buses varies.

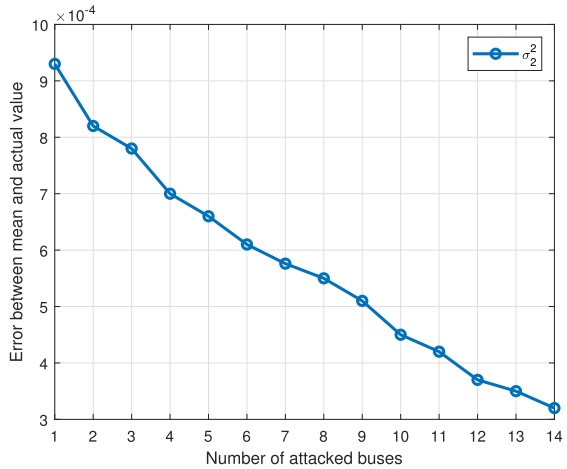

FIGURE 13. The error variation of the parameter σ_2^2 as the number of attacked buses varies.

positive rate is also called detection probability, and the false positive rate is also called the false alarm rate. The specific formulas for both are as follows:

$$TPR = \frac{TP}{TP + FN} \tag{59}$$

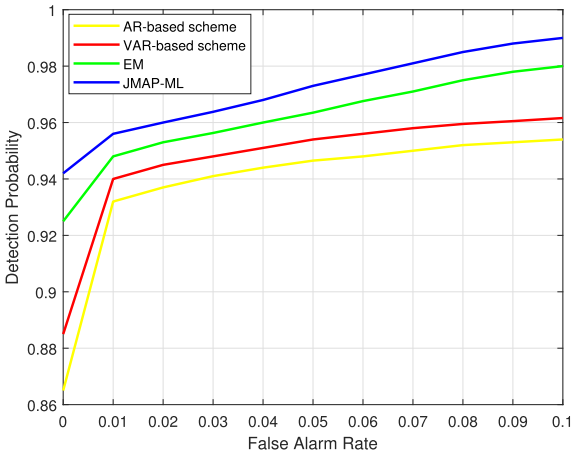

FIGURE 14. The relationship between detection probability and false alarm rate.

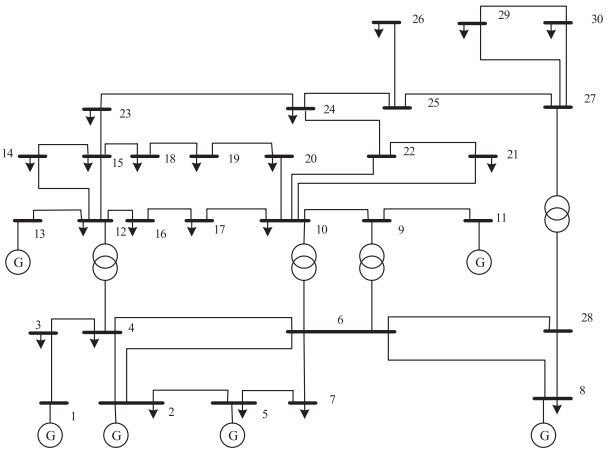

FIGURE 15. IEEE-30-bus power system.

$$FPR = \frac{FP}{FP + TN} \tag{60}$$

where TP is the number of true positives, which stands for the number of successful detection of false measurements; FN is the number of false negatives, which stands for the number of missed detection of false measurements; FP is the number of false positives, which stands for the number of wrong detection of false measurements; TN is the number of true negatives, which stands for the number of correct detection of normal measurements.

The ROC curves characterize the tradeoff between the detection probability and the false alarm rate. We compare the performance of the proposed JMAP-ML algorithm with the previously proposed AR scheme, VAR scheme [21] and EM algorithm [33]. In the presence of FDIAs, the ROC curves of all four methods are shown in Figure 14. Note that the detection probability of the proposed JMAP-ML algorithm is the highest among the four methods. Specifically, when the false alarm rate is 5%, the detection probability is over 97%, implying a low false alarm rate and a high detection probability.

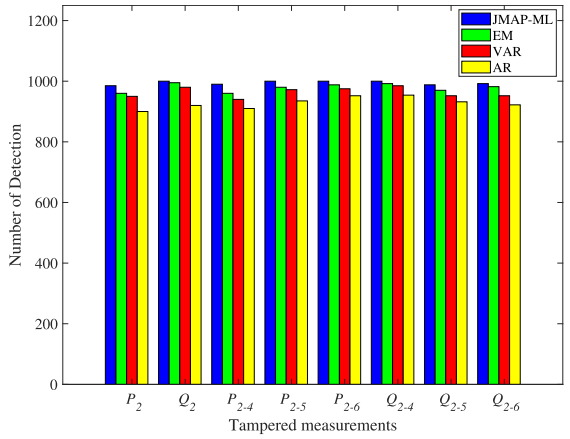

FIGURE 16. Detection of the false measurements.

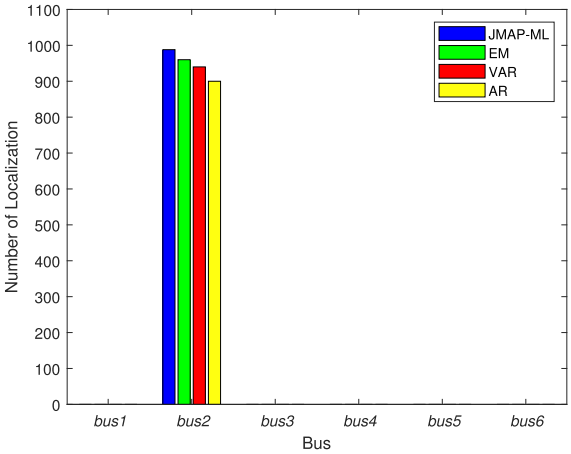

FIGURE 17. Localization of the attacked bus.

B. IEEE-30-BUS POWER SYSTEM

For smart grid false data detection is done in terms of grid buses. Based on the identified anomalies that are neighboring and related to each other, the attacked bus will be detected and localized. The detection performance of the algorithm is further analyzed below using the IEEE-30-bus system as an example. The IEEE-30-bus is shown in Figure 15, which consists of 30 buses, 6 generation zones and 41 branch circuits.

It is assumed that the attacker achieved the FDIA without being detected by the BDD mechanism. Because of the limited space, we only show the detection and localization effect of Bus 2. It is supposed that there are some attacked measurements which include P_2, Q_2, P_{2-4}, P_{2-5}, P_{2-6}, Q_{2-4}, Q_{2-5}, Q_{2-6}. We conduct 1000 independent experiments and use bar charts to count the performance of the four methods in detecting tampered measurements. The relevant result is shown in Figure 16. Compared with the other three methods, the proposed algorithm has a better performance. When the bus is attacked, all measurements associated with it are tampered with. According to the detection result, we can localize the attacked bus. The localization effect of bus 2 is shown in Figure 17.

VIII. CONCLUSION

Given that false data injection attacks can largely affect the normal operation of smart grid, we proposed a JMAP-ML algorithm for detecting and localizing false data injection attacks in power systems. In the algorithm design, we use a Gaussian mixture model to model the measurement errors, in the process of solving the model parameters, the idea of iteration is essentially utilized. Meanwhile, with the help of the latent variable, we can differentiate between normal measurements and tampered measurements. When the bus is attacked, all measurements associated with it are tampered with. Using this knowledge, based on the detection of the tampered measurements, we can localize the attacked bus. Through a large number of simulations on the IEEE-14-bus and IEEE-30-bus power systems, the performance of the JMAP-ML algorithm on convergence and estimation accuracy is researched in this paper. The experimental results show that the JMAP-ML algorithm has a better performance in detecting and localizing FDIAs than the other algorithms.

In the future, integrating multiple models becomes a promising direction, and we will combine Gaussian mixture model (GMM) and deep learning models to form a more comprehensive detection system. Meanwhile, we will work on deploying false data injection attack detection models into real-time systems to build real-time notification and response mechanisms.

REFERENCES

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

[2] O. P. Mahela, M. Khosravy, N. Gupta, B. Khan, H. H. Alhelou, R. Mahla, N. Patel, and P. Siano, "Comprehensive overview of multi-agent systems for controlling smart grids," *CSEE J. Power Energy Syst.*, vol. 8, no. 1, pp. 115–131, Jan. 2022.

[3] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[4] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[5] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[6] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.

[7] F. R. Robertson and W. T. Boston, "The utility operational response to the 14 August 2003 blackout: Analysis and case studies," *IEEE Power Energy Mag.*, vol. 21, no. 3, pp. 43–50, May 2023.

[8] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[9] K.-D. Lu and Z.-G. Wu, "Multi-objective false data injection attacks of cyber–physical power systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 9, pp. 3924–3928, Sep. 2022.

[10] W. Yu, X. Bu, and Z. Hou, "Security data-driven control for nonlinear systems subject to deception and false data injection attacks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2910–2921, Jul. 2022.

[11] K. Huang, Z. Xiang, W. Deng, C. Yang, and Z. Wang, "False data injection attacks detection in smart grid: A structural sparse matrix separation method," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2545–2558, Jul. 2021.
[12] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*., Chicago, IL, USA, Nov. 2009, pp. 1–33.
[13] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.
[14] D. Mukherjee, "Data-driven false data injection attack: A low-rank approach," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2479–2482, May 2022.
[15] Y. Wang, Z. Zhang, J. Ma, and Q. Jin, "KFRNN: An effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6893–6904, May 2022.
[16] 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.
[17] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.
[18] M. N. Kurt, Y. Yilmaz, and X. Wang, "Secure distributed dynamic state estimation in wide-area smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 800–815, 2020.
[19] C. H. Ho, H. C. Wu, S. C. Chan, and Y. Hou, "A robust statistical approach to distributed power system state estimation with bad data," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 517–527, Jan. 2020.
[20] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.
[21] W. Shi, Y. Wang, Q. Jin, and J. Ma, "PDL: An efficient prediction-based false data injection attack detection and location in smart grid," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2. Tokyo, Japan, Jul. 2018, pp. 676–681.
[22] M. Jorjani, H. Seifi, and A. Y. Varjani, "A graph theory-based approach to detect false data injection attacks in power system AC state estimation," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2465–2475, Apr. 2021.
[23] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3271–3280, Jul. 2018.
[24] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.
[25] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8462–8471, Sep. 2020.
[26] B. Li, R. Lu, W. Wang, and K.-K.-R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *J. Parallel Distrib. Comput.*, vol. 103, pp. 32–41, May 2017.
[27] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.
[28] 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.
[29] P. Hu, W. Gao, Y. Li, F. Hua, L. Qiao, and G. Zhang, "Detection of false data injection attacks in smart grid based on joint dynamic and static state estimation," *IEEE Access*, vol. 11, pp. 45028–45038, 2023.
[30] H. Karimipour and V. Dinavahi, "Robust massively parallel dynamic state estimation of power systems against cyber-attack," *IEEE Access*, vol. 6, pp. 2984–2995, 2018.
[31] M. R. Gupta, "Theory and use of the EM algorithm," *Found. Trends® Signal Process.*, vol. 4, no. 3, pp. 223–296, 2010.
[32] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.
[33] P. Hu, W. Gao, Y. Li, M. Wu, F. Hua, and L. Qiao, "Detection of false data injection attacks in smart grids based on expectation maximization," *Sensors*, vol. 23, no. 3, p. 1683, Feb. 2023.

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.

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 papers in international conferences. His research interests include microgrid 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.

WENXIN HU is currently pursuing the bachelor's degree with the School of Electrical Engineering, Anhui Polytechnic University, China. Her research interests include cyber security and power system state estimation.

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.

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 grid, and optimal placement of PMUs.