A Highly Discriminative Detector against False Data Injection Attacks in AC State Estimation

Gang Cheng, *Student Member*, *IEEE*, Yuzhang Lin, *Member*, *IEEE*, Junbo Zhao, *Senior Member*, *IEEE*, and Jun Yan, *Member*, *IEEE*

***Abstract*—False data injection attacks (FDIAs) can bypass conventional bad data detection methods. Recently developed FDIA detection methods based on statistical consistency of measurement values may not work effectively when false data do not significantly deviate from historical trends. They may also mistakenly treat actual power grid events as FDIAs. In this paper, a highly discriminative FDIA detector named the *k*-smallest residual similarity (*k*SRS) test is proposed. The method is based on the rationale that perfect FDIAs can hardly be achieved in AC state estimation, and real-world imperfect FDIAs always lead to subtle changes in the probability distributions of measurement residuals. Therefore, the statistical consistency of measurement residuals can be carefully portrayed to detect practical FDIAs in AC state estimation. Herein, the Jensen-Shannon distance (JSD) is used to precisely quantify the similarity of measurement residual distributions. Simulations on the IEEE 30-bus system demonstrate that the proposed method can achieve high detection rates and low false alarm rates under a variety of conditions where existing methods do not yield satisfactory results.**

***Index Terms*—Cyber attacks, state estimation, false data injection attacks, hypothesis testing, measurement residuals**

I. Introduction

STATE estimation (SE) is an essential function for power system monitoring, which provides grid operators with real-time snapshots of system operating conditions [1]. SE is supported by the supervisory control and data acquisition (SCADA) system, which gathers the measurement data and network topology information from remote terminal units deployed in substations. As conventional power systems are being transformed toward smart grids with pervasive information and communications technologies (ICT) [2], the cyber network for sensing, communication, storage, and data analysis becomes a major vulnerability for system operation [3]-[6]. Cyber adversaries may stealthily access the computer networks in power plants, substations, or even control centers to disrupt service, manipulate data, or even disable the entire monitoring and control system. Hence, it is of great significance to investigate cyber security issues in power system operations.

As a major type of potential cyber threat against power system operations, false data injection attacks (FDIAs) against SE were first proposed by Liu *et al.* in [7]. It is found that adversaries may have the capability to introduce desirable errors to certain state variables by injecting well-designed false measurements. As a result, the decision-making process may be interfered, leading to risky operating conditions such as biased locational marginal prices (LMPs) in real-time electricity markets, inefficient dispatch of generation and load, or even the loss of stability and system collapse [9]-[11]. Notably, FDIAs are capable of escaping conventional bad data detection schemes, such as the largest normalized residual (LNR) test and the Chi-square test [7], [8].

Aiming to reliably detect FDIAs, a number of approaches have been proposed in the literature. Earlier approaches are typically based on the DC power flow model [12]-[18]. In [12]-[14], FDIA detection is enabled by deploying or securing a set of sensors such as phasor measurement units (PMUs). In [15], [16], the FDIA detection problem is formulated as a matrix separation problem based on the low dimensionality of the measurement matrix and the sparsity of the attack matrix. In [17], [18], forecasting-aided methods are proposed to detect FDIAs by checking the statistical consistency between forecasted and gathered measurements. All these methods are formulated based on a linear DC power flow model. In practice, however, nonlinear state estimators with a complete AC power flow model are adopted by the power industry [19]. There is no guarantee that the DC model-based FDIA detection methods have equivalent performance under the nonlinear AC SE [20], [26].

To overcome the limitations of DC model-based methods, a few categories of FDIA detection approaches based on the AC power flow model are developed recently [21]-[28]. In [21]-[23], the Kullback-Leibler distance (KLD) is used to evaluate the similarity between two probability distributions derived from measurement variations. In [24], [25], the statistical consistency between received measurements and the expected measurements derived from a limited number of secure PMUs is explored to detect FDIAs. In [26]-[28], several FDIA detection methods are proposed based on deep learning approaches.

Among all existing works mentioned above [12]-[28], the core underlying logics of FDIA detection are either checking

This work was supported by the National Science Foundation Award No. 1947617.

Gang Cheng and Yuzhang Lin are with the Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, MA 01854 (e-mails: gang_cheng@student.uml.edu; yuzhang_lin@uml.edu).

Junbo Zhao is with is with the Department of Electrical and Computer Engineering at University of Connecticut, Storrs, CT, 06269, USA (e-mail: junbo@uconn.edu).

Jun Yan is with the Concordia Institute for Information Systems Engineering, Concordia University, Montréal, QC H3G 1M8, Canada (e-mail: jun.yan@concordia.ca).

statistical consistency of measurements (or states) against the information from secure PMUs [12]-[14], [24], [25], or checking statistical consistency of measurements (or states) against the information derived from historical data [15]-[23], [26]-[28]. In practice, several limitations are present for these existing concepts. For methods relying on secure PMUs, the underlying assumption that a specific set of PMUs is fully invincible may not hold all the time. Besides, the deployment of additional PMUs and/or cyber secure hardware/software inevitably results in additional costs. For methods relying on historical measurements, the performance may not be satisfactory if the false data do not significantly deviate from historical trends [21]-[23]. Furthermore, such methods can hardly differentiate between an actual grid event (such as generation or load switching) and an FDIA, as both may appear as anomalies concerning the probability distribution of historical data. As a result, actual events occurring in physical power systems may be mistakenly detected as FDIAs, leading to severely faulty decision-making in system operation.

Instead of checking the statistical consistency of *measurement values*, this paper takes a fundamentally different approach for FDIA detection: checking the statistical consistency of *measurement residuals* in AC SE. It will be reasoned that cyber attackers can hardly achieve perfect FDIAs against AC SE, and imperfect FDIAs inevitably result in subtle changes of measurement residual statistics. Remarkably, the probability distribution of *measurement values* changes with both system operating conditions and FDIAs, while the probability distribution of *measurement residuals* only changes with FDIAs [29], [30]. Hence, statistical tests based on *measurement residuals* can effectively discriminate between FDIAs and system operating point variations, yielding very high detection capability. Compared with existing methods, the unique features and original contributions of the proposed method based on measurement residual statistics are summarized as follows.

1) Independent of secure sensors. The proposed method is generally applicable to all measurements, and no deployment of PMUs or cyber secure hardware/software is needed.

2) Highly discriminative between actual operating condition changes and FDIAs. Unlike most existing methods, the proposed method can easily discriminate FDIAs from actual operating condition changes including unexpected grid events.

3) Highly discriminative against sophisticated ramping FDIAs. While some existing methods relying on abrupt measurement changes cannot detect gradually ramping false data, the proposed method remains highly sensitive in such cases.

4) Implementation-friendly. The proposed method only requires measurement residuals produced by SE, which is directly available in energy management systems without the need to deploy additional sensors or data collectors.

The rest of the paper is organized as follows. Section II provides the context by reviewing the formulations of SE, bad data detection, FDIA, and FDIA detection. Section III details the concept and implementation of the proposed *k*-smallest residual similarity (*k*SRS) test for FDIA detection. Section IV presents comparative simulation results between the proposed method and the conventional methods. Section V concludes the paper.

II. Preliminaries

This section briefly reviews the background problem and typical existing solutions. The presented bad data detection and FDIA detection methods will be used as baselines for demonstrating the effectiveness of the proposed method in Section IV.

A. AC Power System State Estimation

Consider a power system with *m* measurements and *n* state variables. The non-linear relationship between measurements and state variables are shown as follows:

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

where $\boldsymbol{z} \in \mathbb{R}$ is the measurement vector; $\boldsymbol{x} \in \mathbb{R}$ is the state vector; $\boldsymbol{e} \in \mathbb{R}$ is the measurement error vector, which is assumed to follow a Gaussian distribution with zero mean; $\boldsymbol{h}(\cdot)$ represents the non-linear function between the state vector $\boldsymbol{x}$ and the measurement vector $\boldsymbol{z}$.

The solutions to state estimates can be obtained via the weighted least squares (WLS) criterion as follows:

$$\hat{\boldsymbol{x}} = \arg\min \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right]^T \boldsymbol{R}^{-1} \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right] \tag{2}$$

where $\boldsymbol{R} = diag\left(\sigma_1^2, \cdots \right.$ $\mathbb{R}$ is the covariance of the measurement error vector; $\hat{\boldsymbol{x}} \in \mathbb{R}$ is the state estimate vector; σ_i^2 is the variance of the measurement error of the *i*th channel.

The solution to (2) can be obtained by performing the Gauss-Newton iterative algorithm [19]:

$$\boldsymbol{x}^{l+1} = \boldsymbol{x}^l + \left[\boldsymbol{G}\left(\boldsymbol{x}^l\right)\right]^{-1} \left\{\boldsymbol{H}^T\left(\boldsymbol{x}^l\right) \boldsymbol{R}^{-1} \left[\boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}^l\right)\right]\right\} \tag{3}$$

$$\boldsymbol{G}\left(\boldsymbol{x}^l\right) = \boldsymbol{H}^T\left(\boldsymbol{x}^l\right) \boldsymbol{R}^{-1} \boldsymbol{H}\left(\boldsymbol{x}^l\right) \tag{4}$$

where *l* is the iteration index; $\boldsymbol{x}^l$ is the solution vector at iteration *l*; $\boldsymbol{H} \in \mathbb{R}$ is the Jacobian matrix. The WLS SE is the mostly widely used method in power system, while there are some limitations. For example, the WLS SE is not robust against natural bad data, which will result in large-biased state estimates. In practice, therefore, the bad data detection procedure will be implemented following the WLS SE.

B. Bad Data Detection

Conventional bad data detection methods such as the LNR test and the Chi-square test are performed based on the outcomes of WLS SE.

The Chi-square test detects bad data by checking the value of the SE objective function as follows:

$$J(\hat{\boldsymbol{x}}) = \left[\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})\right]^T \boldsymbol{R}^{-1} \left[\boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}})\right] \tag{5}$$

In the Chi-square test, the null hypothesis H_0 represents the case where there is no bad data. The detection criterion can be expressed as follows:

$$\begin{cases} J(\hat{\boldsymbol{x}}) \geq \chi^2_{(m-n),p}, & \textit{Reject } H_0 \\ J(\hat{\boldsymbol{x}}) < \chi^2_{(m-n),p}, & \textit{Accept } H_0 \end{cases} \tag{6}$$

where $J(\hat{\boldsymbol{x}})$ is the objective function value of WLS SE evaluated at the solution points $\hat{\boldsymbol{x}}$, and $\chi^2_{(m-n),p}$ is the threshold with confidence level *p* and (*m*-*n*) degrees of freedom.

The LNR test is another widely used bad data detection method. The core is to normalize the measurement residuals:

$$r_i^N = \frac{|z_i - h_i(\hat{\boldsymbol{x}})|}{\sqrt{\Omega_{ii}}} \tag{7}$$

$$\boldsymbol{\Omega} = \left[\boldsymbol{I} - \boldsymbol{H}\left(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\right]\boldsymbol{R} \tag{8}$$

where z_i represents the *i*th measurement; $h_i(\cdot)$ is the nonlinear function relating the state vector to the *i*th measurement; r_i^N is the *i*th normalized residual; Ω_{ii} is the *i*th diagonal entry of $\boldsymbol{\Omega}$; $\boldsymbol{I} \in \mathbb{R}$ is the identity matrix. If the largest normalized residual is greater than a threshold *ε*, then the corresponding measurement will be suspected as a bad data.

The Chi-square test and the LNR test are generally effective for detecting natural bad data which typically induces large measurement residual perturbation. However, for maliciously designed false data which only induces small residual perturbation, these methods tend to be ineffective.

C. AC-based False Data Injection Attacks

On the condition that the attacker has the capability to obtain accurate information about real-time state estimates, network topology and parameters, a perfect FDIA can be launched, where the attack vector $\boldsymbol{a}$ is designed as follows:

$$\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) \tag{9}$$

where $\hat{\boldsymbol{x}}$ represents the state estimate vector without FDIAs; $\boldsymbol{c}$ represents a bias vector injected into the state estimates.

It has been readily shown that under such perfect information availability, the attack vector $\boldsymbol{a}$ constructed as (9) will result in the same measurement residual vector as the attack-free condition. As such, the false data can bypass the Chi-square test and the LNR test [24]. In reality, the perfect attack vectors can hardly be achieved. Even so, the attackers may create attack vectors that are close enough to (9) such that the perturbation of the residual vector remains small. As the conventional bad data detection methods are not designed for such malicious conditions, and they have very limited sensitivity under small residual perturbation. As a result, there is still a considerable chance that the imperfect FDIA will bypass these tests [24], [25].

D. FDIA Detection based on Statistical Consistency of Measurements

Due to the ineffectiveness of conventional bad data detectors against FDIAs, a new category of detection methods based on statistical consistency of measurements are proposed. In [21]-[23], the KLD is used to compute the similarity between probability distributions of measurement variations between the current time step and historical time steps. If an FDIA is present in power systems, the distance metric will abnormally increase. Let $\boldsymbol{V}^{cur} \in \mathbb{R}$ represent the measurement variation vector of the current time step *t*, i.e., $\boldsymbol{V}^{cur} = \boldsymbol{z}(t) - \boldsymbol{z}(t-1)$. Let $\boldsymbol{V}^{his} \in \mathbb{R}$ represent the measurement variation vector from historical data as follows:

$$\boldsymbol{V}^{his} = \left[\left(\boldsymbol{v}^{his}_{t-N^{his}}\right)^T, \left(\boldsymbol{v}^{his}_{t-N^{his}+1}\right)^T, \cdots \boldsymbol{v} \quad \cdots \boldsymbol{v}\right]^T \tag{10}$$

$$\boldsymbol{v}^{his}_f = \boldsymbol{z}(f) - \boldsymbol{z}(f-1), f = t - N^{his}, t - N^{his} + 1, \cdots \tag{11}$$

where $\boldsymbol{v}^{his}_f \in \mathbb{R}$ represents the measurement variation vector of the historical time step *f*; N^{his} represents the number of measurement variation vectors from historical time steps.

To obtain the probability density functions (PDFs) of $\boldsymbol{V}^{cur}$ and $\boldsymbol{V}^{his}$, the histogram consisting of $\boldsymbol{V}^{cur}$ and $\boldsymbol{V}^{his}$ is divided into S_{KLD} bins. The approximate PDFs can be obtained as:

$$p_s^{cur} = \frac{count\left(\boldsymbol{V}_s^{cur}\right)}{m}, s = 1, 2, \cdots \tag{12}$$

$$p_s^{his} = \frac{count\left(\boldsymbol{V}_s^{his}\right)}{N^{his} \times m}, s = 1, 2, \cdots \tag{13}$$

where S_{KLD} is the number of bins of the histogram; $\boldsymbol{V}_s^{cur}$ and $\boldsymbol{V}_s^{his}$ contain the current and historical measurement variation samples located in the *s*th bin, respectively; $count(\cdot)$ is a function that counts the entry of a vector; p_s^{cur} and p_s^{his} are the probabilities of the current and historical samples located in the *s*th bin, respectively.

In order to compare the similarity between two different PDFs, the KLD is defined as follows:

$$d_{KL} = \sum_{s=1}^{S_{KLD}} p_s^{cur} \ln \frac{p_s^{cur}}{p_s^{his}} \tag{14}$$

where d_{KL} represents the KLD from the PDF of $\boldsymbol{V}^{cur}$ to the PDF of $\boldsymbol{V}^{his}$, respectively.

If an FDIA is launched, the distance d_{KL} will be abnormally large. To detect potential FDIAs, a distance threshold ς is set given a confidence level based on historical distance metric values without FDIAs.

In this FDIA detection method, the null hypothesis H_0 represents the case where there is no FDIA. The detection criterion can be expressed as follows:

$$\begin{cases} d_{KL} \geq \varsigma, & Reject\ H_0 \\ d_{KL} < \varsigma, & Accept\ H_0 \end{cases} \tag{15}$$

The FDIA detection method described above has some limitations. For example, if an FDIA follows the historical measurement distributions or is gradually ramped up, instead of abruptly launched, this method tends to be ineffective. Moreover, this method may mistakenly detect physical grid events as FDIAs, since the change of system operating conditions can also lead to large measurement variations.

III. Proposed FDIA Detection Method

To overcome the limitations of FDIA detection method based on statistical consistency of *measurement values*, a novel FDIA detection method based on the statistical consistency of *measurement residuals* is proposed in this section.

A. Imperfect AC-based False Data Injection Attacks

The proposed method is based on the assumption that a perfect AC-based FDIA can hardly be achieved in the real world.

In particular, it is highly unlikely that attackers can obtain both accurate real-time state estimates and accurate model parameters at the same time, especially the real-time state estimates.

1) The network parameters and state estimates are stored in the database of the control center, which are relatively well protected. For attackers, due to the communication or technique constraints, it is more difficult to hank into the control center than the substation-level network [1], [2], [5].

2) Even if accurate network parameters are obtained by breaching into the control center [31]-[34], it is still difficult to obtain accurate state estimates. Power flows are time-varying because of the fluctuations of loads in real time. Consequently, *up-to-date* state estimates are necessary for launching perfect AC-based FDIAs. However, once the FDIAs are launched, the state estimates in the control center will be biased. Hence, attackers are faced with the dilemma that they cannot obtain *accurate up-to-date* state estimates from the control center anymore once the FDIAs are launched.

3) The only possible avenue to launch perfect AC-based FDIAs is that attackers can obtain accurate network parameters from the control center and accurate measurements from substations, then perform their own state estimation function in real time to derive the *up-to-date* state estimates. Furthermore, the attackers' state estimation function should be executed in the same time resolution at SCADA measurements (every 2-3 seconds) in order to determine how to manipulate the measurements perfectly. However, this is almost an impossible task for attackers, because it is dependent on the full availability of real-time measurements as well as powerful computing capabilities, which are not available for attackers. Please note that it does not require accurate *up-to-date* state estimates to launch a perfect DC-based FDIA. However, almost all existing state estimators in control centers are AC-based, and it does require accurate *up-to-date* state estimates to launch an AC-based FDIA.

For insider attacks, i.e., attacks launched or assisted by insiders, model parameters are easier to attain. However, attaining *up-to-date* state estimates during the whole span of the attack may still be difficult due to the aforementioned reasons, and thus the FDIAs are still likely to be imperfect.

As it is almost impossible to satisfy both conditions above, it is reasonable to assume that AC-based FDIAs are imperfect.

Consider an imperfect AC-based FDIA as follows [25]:

$$\tilde{\boldsymbol{a}} = \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}+\boldsymbol{c}) - \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}) \tag{16}$$

where $\tilde{\boldsymbol{a}}$ is an imperfect attack vector; $\tilde{\boldsymbol{h}}(\cdot)$ represents the non-linear function with inaccurate model parameters; $\boldsymbol{\xi}$ represents the error of state estimate vector guessed by attackers.

The measurement residual vector resulting from the imperfect AC-based FDIA is derived as follows:

$$\begin{aligned}\boldsymbol{r}_{\tilde{a}} &= \boldsymbol{z} + \tilde{\boldsymbol{a}} - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\tilde{a}}) \\ &= \boldsymbol{z} + \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}+\boldsymbol{c}) - \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\tilde{a}}) \\ &= \boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}}) + \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}+\boldsymbol{c}) - \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}) + \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\tilde{a}}) \\ &= \boldsymbol{r} + \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}+\boldsymbol{c}) - \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}) + \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\tilde{a}})\end{aligned} \tag{17}$$

where $\hat{\boldsymbol{x}}_{\tilde{a}}$ and $\boldsymbol{r}_{\tilde{a}}$ are state estimate vectors and measurement residual vectors in the presence of the FDIA, respectively.

The estimated state vector is given by:

$$\hat{\boldsymbol{x}}_{\tilde{a}} = \hat{\boldsymbol{x}} + \boldsymbol{\eta} + \boldsymbol{c} \tag{18}$$

where $\boldsymbol{\eta}$ represents the state estimate bias vectors for system operators. Note that $\boldsymbol{\eta}$ and $\boldsymbol{\xi}$ are different since the model parameters obtained by attackers are inaccurate.

Let Δ represent the bias vector of measurement residuals induced by the imperfect AC-based FDIA, then:

$$\boldsymbol{r}_{\tilde{a}} = \boldsymbol{r} + \Delta \tag{19}$$

where

$$\Delta = \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}+\boldsymbol{c}) - \tilde{\boldsymbol{h}}(\boldsymbol{x}+\boldsymbol{\xi}) + \boldsymbol{h}(\hat{\boldsymbol{x}}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_{\tilde{a}}) \tag{20}$$

In this case, the PDFs of measurement residuals with imperfect FDIAs are different from those without FDIAs:

$$f_{r_{\tilde{a},i}}(r_{\tilde{a},i}) = \int f_{joint}(r_i, r_{\tilde{a},i})\, dr_i \tag{21}$$

where $r_{\tilde{a},i}$ and r_i represent the measurement residuals of the *i*th measurement channel with and without imperfect FIDAs, respectively; $f_{r_{\tilde{a},i}}(r_{\tilde{a},i})$ represents the PDF of measurement residuals $r_{\tilde{a},i}$; $f_{joint}(r_i, r_{\tilde{a},i})$ represents the joint PDF of measurement residuals r_i and $r_{\tilde{a},i}$.

If $\Delta_i = r_{\tilde{a},i} - r_i$ is non-zero (imperfect AC-based FDIA), $f_{r_{\tilde{a},i}}(r_{\tilde{a},i})$ and $f_{r_i}(r_i)$ will be different. Such a nuance may not trigger the conventional LNR or Chi-square tests, but it is possible to design more dedicated and refined tests to pick it up.

B. WLAV SE based on AC Power Flow Model

To develop a statistical test based on measurement residuals, an SE should be selected first to produce the residuals. Here, the weighted least absolute value (WLAV) SE is adopted for the following two reasons. First, WLAV SE is robust against natural gross errors. Bad data will be automatically filtered out before FDIA detection. Second, due to its undifferentiable objective function, the distribution of measurement residuals usually has a larger change from the original distribution in the presence of an FDIA compared with WLS SE.

The WLAV estimator aims to minimize the sum of weighted absolute residual errors, stated as follows:

$$\begin{aligned}\min \quad & \sum_{i=1}^{m} w_i |r_i| \\ \text{s.t.} \quad & r_i = z_i - h_i(\boldsymbol{x})\end{aligned} \tag{22}$$

where w_i and r_i are the weight and residual of the *i*th measurement, respectively.

The WLAV problem given by (22) can be transformed into a successive set of linear programming (LP) problems [19]. The LP problem to be solved at iteration *l* is given by:

$$\begin{aligned}\min \quad & \sum_{i=1}^{m} w_i \left(u_i^l + v_i^l\right) \\ \text{s.t.} \quad & \boldsymbol{H}(\boldsymbol{x}^l)\Delta\boldsymbol{x}_u^l - \boldsymbol{H}(\boldsymbol{x}^l)\Delta\boldsymbol{x}_v^l + \boldsymbol{u}^l - \boldsymbol{v}^l = \Delta\boldsymbol{z}^l \\ & \Delta x_{u,i}^l, \Delta x_{v,i}^l, u_i^l, v_i^l \ge 0\end{aligned} \tag{23}$$

where $\boldsymbol{u}^l - \boldsymbol{v}^l = \boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}^l) - \boldsymbol{H}(\boldsymbol{x}^l)\Delta\boldsymbol{x}^l = \Delta\boldsymbol{z}^l - \boldsymbol{H}(\boldsymbol{x}^l)\Delta\boldsymbol{x}^l$ is the measurement residual vector at the *l*th SE iteration, and $\Delta\boldsymbol{x}^l = \Delta\boldsymbol{x}_u^l - \Delta\boldsymbol{x}_v^l$.

C. Similarity Metric for Measurement Residual Distributions

As discussed in section III-A, the measurement residual distribution based on WLAV SE will be reshaped when an im-

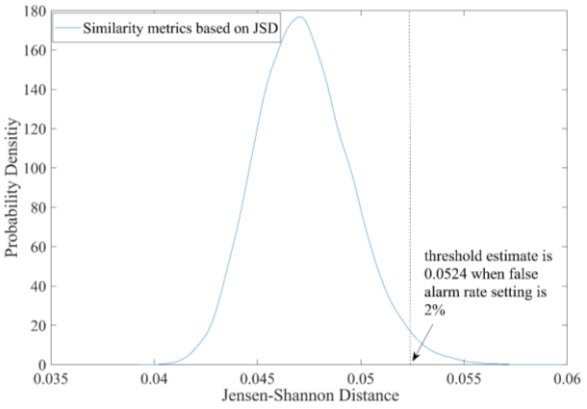

Fig. 1. Threshold estimate for a certain false alarm rate setting.

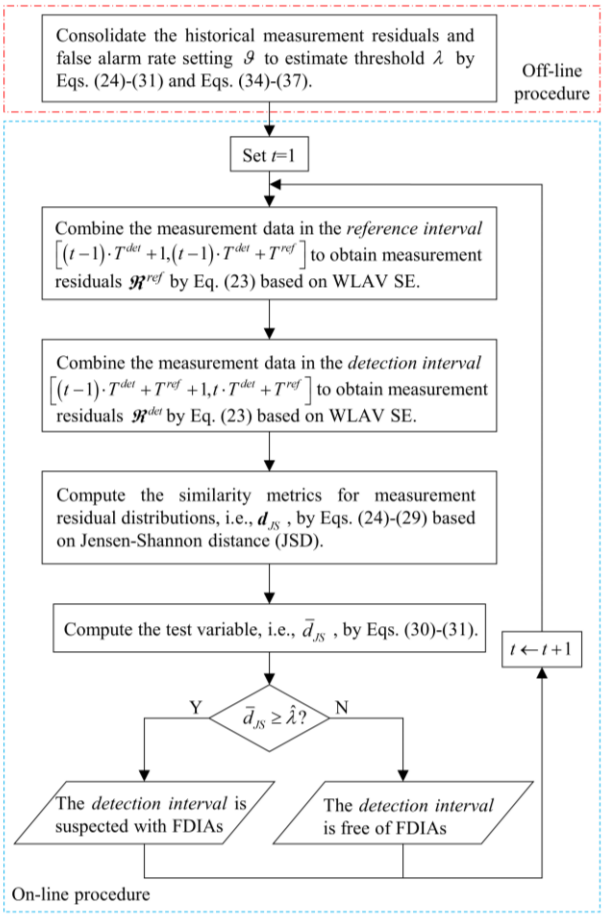

Fig. 2. Flow chart of the *k*SRS test.

perfect AC-based FDIA is launched. In this subsection, a novel AC-based FDIA detection approach will be proposed, which checks the statistical consistency of measurement residual distributions between two consecutive time intervals. The time interval containing measurement data that is assumed to be free of FDIAs is defined as the *reference interval*. The time interval containing the latest gathered measurement scans which needs to be examined is defined as the *detection interval*. The lengths of the *reference interval* and the *detection interval* are denoted as T^{ref} and T^{det}, respectively. To determine the statistical consistency of measurement residuals in the two intervals, the similarity between the residual probability distributions of the *reference interval* and the *detection interval* should be evaluated for each measurement channels.

In this paper, the Jensen-Shannon distance (JSD) [35]-[37] is introduced to evaluate the similarity of measurement residual distributions. JSD has advantages over KLD used in [21]-[23] in two aspects. First, JSD is a symmetric distance, i.e., the order of two distributions does not affect the results. On the contrary, KLD is asymmetric due the result based on Eq. (14) is changed when the positions of two distributions are swapped. Second, JSD can process discontinuous data. In reality, the computed probability using actual sample data may be equal to zero for certain ranges. In such a case, KLD cannot be evaluated, but JSD is still feasible. Therefore, JSD is chosen as a similarity metric in this paper.

Define the residual matrices of the *reference interval* and the *detection interval* as follows:

$$\mathfrak{R}^{ref}=\left[\boldsymbol{r}_1^{ref},\boldsymbol{r}_2^{ref},\cdots \boldsymbol{r} \quad \cdots \boldsymbol{r} \quad \cdots\right] \tag{24}$$

$$\mathfrak{R}^{det}=\left[\boldsymbol{r}_1^{det},\boldsymbol{r}_2^{det},\cdots \boldsymbol{r} \quad \cdots \boldsymbol{r} \quad \cdots\right] \tag{25}$$

where $\boldsymbol{r}_j^{ref}\in\mathbb{R}$ represents the residual vector of the *j*th measurement scan in the *reference interval*; $\boldsymbol{r}_j^{det}\in\mathbb{R}$ represents the residual vector of the *j*th measurement scan in the *detection interval*; $\mathfrak{R}^{ref}\in\mathbb{R}$ and $\mathfrak{R}^{det}\in\mathbb{R}$ represent the measurement residual matrices in the *reference interval* and the *detection interval*, respectively; N^{ref} and N^{det} represent the numbers of measurement scans in the *reference interval* and the *detection interval*, respectively.

Let $\mathfrak{R}_i^{ref}$ and $\mathfrak{R}_i^{det}$ represent the measurement residual vectors of the *i*th measurement channel in the *reference interval* and the *detection interval*, respectively. To obtain the PDFs of $\mathfrak{R}_i^{ref}$ and $\mathfrak{R}_i^{det}$, the histograms consisting of $\mathfrak{R}_i^{ref}$ and $\mathfrak{R}_i^{det}$ are divided into S_{JSD} bins. The approximate PDFs for the corresponding histograms are obtained as follows [35]:

$$p_{i,s}^{ref}=\frac{count\left(\mathfrak{R}_{i,s}^{ref}\right)}{N^{ref}},i=1,2,\cdots \quad \cdots \tag{26}$$

$$p_{i,s}^{det}=\frac{count\left(\mathfrak{R}_{i,s}^{det}\right)}{N^{det}},i=1,2,\cdots \quad \cdots \tag{27}$$

where $\mathfrak{R}_{i,s}^{ref}$ and $\mathfrak{R}_{i,s}^{det}$ represent the measurement residual vectors of the *i*th channel located in the *s*th bin within the *reference interval* and the *detection interval*, respectively; $count(\cdot)$ is a function that counts the entry of a vector; $p_{i,s}^{ref}$ and $p_{i,s}^{det}$ represent the probabilities corresponding to $\mathfrak{R}_{i,s}^{ref}$ and $\mathfrak{R}_{i,s}^{det}$ located in the *s*th bin, respectively.

The similarity metric JSD, denoted as $d_{JS,i}$, is computed as:

$$d_{JS,i}=\frac{1}{2}\left[\sum_{s=1}^{S_{JSD}}p_{i,s}^{ref}\ln\left(\frac{2p_{i,s}^{ref}}{p_{i,s}^{ref}+p_{i,s}^{det}}\right)+\sum_{s=1}^{S_{JSD}}p_{i,s}^{det}\ln\left(\frac{2p_{i,s}^{det}}{p_{i,s}^{ref}+p_{i,s}^{det}}\right)\right] \tag{28}$$

$$\boldsymbol{d}_{JS}=\left[d_{JS,1},d_{JS,2},\cdots \quad \cdots\right] \tag{29}$$

where S_{JSD} represents the number of bins in the histogram consisting of $\mathfrak{R}_i^{ref}$ and $\mathfrak{R}_i^{det}$; $d_{JS,i}$ is the JSD, i.e., the similarity metric, of measurement residual distributions of the *i*th chan-

nel; $\boldsymbol{d}_{JS}$ represents the JSD vector for all measurement channels.

D. k-smallest Residual Similarity Test

Based on the components developed in the previous subsections, the proposed FDIA detection method will be constructed in this subsection.

To construct a test variable, it should first be determined how many measurement channels should be reflected in the test variable. On the one hand, creating a test variable using the residual of only one measurement channel, like the LNR test which takes the largest residual as the test variable, can make the test non-robust against disturbances and result in false alarm. On the other hand, creating a test variable based on the residuals of all measurement channels, like the Chi-square test which takes the weighted sum of squares of all residuals as the test variable, can make the test insensitive, especially for large-scale systems where numerous normal measurements may suppress the effects of a few anomalies. To achieve a reasonable trade-off between sensitivity and robustness, the *k*SRS test is proposed, wherein the *k* measurement channels with the smallest similarities (i.e., largest JSDs) are selected to construct the test variable shown as follows:

$$\vec{\boldsymbol{d}}_{JS} = rank\left(\boldsymbol{d}_{JS}\right) \tag{30}$$

$$\bar{d}_{JS} = \frac{1}{k}\sum_{q=1}^{k}\vec{u}_{JS,q}, q = 1,2,\cdots \tag{31}$$

where $rank(\cdot)$ is a function that reorders the entries of a vector in descending order; $\vec{\boldsymbol{d}}_{JS}$ represents the reordered vector from $\boldsymbol{d}_{JS}$; $\vec{u}_{JS,q}$ represents the qth entry of vector $\vec{\boldsymbol{d}}_{JS}$; $\bar{d}_{JS}$ is the average of the k chosen JSDs, and it is used as the test variable to check the statistical consistency of measurement residuals between the *reference interval* and the *detection interval*.

In the proposed *k*SRS test, the null hypothesis H_0 represents the case where there is no FDIA. The relationship between the false alarm rate setting and the detection threshold is formulated as follows:

$$\begin{aligned}\vartheta &= P\left(\bar{d}_{JS} \ge \lambda \middle| H_0\right)\\ &= \int_{\lambda}^{\infty} f(\tau)d\tau\\ &= F(\infty) - F(\lambda)\\ &= 1 - F(\lambda)\end{aligned} \tag{32}$$

$$\lambda = F^{-1}(1-\vartheta) \tag{33}$$

where ϑ represents the false alarm rate setting; λ represents the detection threshold; $f(\cdot)$ is the PDF of $\bar{d}_{JS}$; $F(\cdot)$ is the cumulative density function (CDF) of $\bar{d}_{JS}$.

In reality, however, λ is difficult to derive from Eqs. (32)-(33) because $f(\cdot)$ is unavailable. Hence, one way to estimate the threshold is to obtain the frequency distribution of $\bar{d}_{JS}$ under H_0 using historical measurements. Select the *reference interval* and the *detection interval* randomly from historical measurements, calculate $\bar{d}_{JS}$, and collect the results as:

$$\bar{\boldsymbol{d}}_{JS}^{his} = \left[\bar{d}_{JS,1}^{his}, \bar{d}_{JS,2}^{his}, \cdots\right]^{T} \tag{34}$$

where $\bar{\boldsymbol{d}}_{JS}^{his}$ represents the vector of the averages of *k*-smallest similarities taken from historical measurement residuals; M is the number of samples used to estimate the threshold λ [38].

To estimate the threshold λ, the entries of vector $\bar{\boldsymbol{d}}_{JS}^{his}$ are reordered as follows:

$$\begin{aligned}\vec{\boldsymbol{d}}_{JS} &= rank\left(\bar{\boldsymbol{d}}_{JS}^{his}\right)\\ &= \left[\vec{a}_{\overline{JS},1}, \vec{a}_{\overline{JS},2}, \cdots\right]\end{aligned} \tag{35}$$

where $\vec{\boldsymbol{d}}_{JS}$ represents the reordered vector of $\bar{\boldsymbol{d}}_{JS}^{his}$ in descending order based on the values of all entries.

From this frequency distribution, the threshold λ corresponding to a given false alarm rate setting can be estimated as follows:

$$o = \vartheta \cdot M \tag{36}$$

$$\hat{\lambda} = \vec{a}_{\overline{JS},o} \tag{37}$$

where $\vec{a}_{\overline{JS},o}$ represents the oth entry of vector $\vec{\boldsymbol{d}}_{\overline{JS}}$, and $\hat{\lambda}$ is the estimated threshold. As an illustrative example, Fig. 1 shows the frequency distribution of $\bar{d}_{JS}$ from a set of historical measurements on the IEEE 30-bus test system, where the detection threshold is estimated as $\hat{\lambda} = 0.0524$ based on a false alarm rate setting of 2%.

With the estimated threshold $\hat{\lambda}$, the criterion of FDIA detection can be set as:

$$\begin{cases}\bar{d}_{JS} \ge \hat{\lambda}, & Reject\ H_0\\ \bar{d}_{JS} < \hat{\lambda}, & Accept\ H_0\end{cases} \tag{38}$$

The flow chart of the proposed *k*SRS test is shown in Fig. 2, which consists of two sub-procedures, i.e., the off-line procedure and the on-line procedure. In the off-line procedure, the detection threshold corresponding to a specified false alarm rate setting is estimated using the historical data. It should be noted that the threshold estimate does not need to be updated frequently. With the detection threshold set up, in the on-line procedure, the *k*SRS test is executed to detect potential FDIAs within the *detection interval* by means of comparing the residual similarity between the *detection interval* and the *reference interval*. The *reference interval* can be the interval that immediately precedes the *detection interval*. The detection frequency is dependent on the length of the *detection interval*, i.e., T^{det}.

E. Discussions on the Advantages of Using Measurement Residuals Over Measurement Values (Variations) in FDIA Detection

There are several advantages to detect FDIA based on the probability distribution of *measurement residuals* instead of based on the probability distribution of *measurement values* (or *variations*). The rationale is discussed in two aspects below.

1) The proposed *measurement residual*-based *k*SRS test produces less false-positive results than the *measurement variation*-based MS test under actual operating condition changes.

Define two consecutive measurement scans as follows:

$$\boldsymbol{z}^{(t)} = \boldsymbol{h}\left(\boldsymbol{x}^{(t)}\right) + \boldsymbol{e}^{(t)}, \tag{39}$$

$$\boldsymbol{z}^{(t+1)} = \boldsymbol{h}\left(\boldsymbol{x}^{(t+1)}\right) + \boldsymbol{e}^{(t+1)}, \tag{40}$$

where $\boldsymbol{z}^{(t)}$ and $\boldsymbol{z}^{(t+1)}$ represent the measurement vectors at instant t and t+1, respectively; $\boldsymbol{x}^{(t)}$ and $\boldsymbol{x}^{(t+1)}$ represent the state variable vectors in instant t and t+1, respectively; $\boldsymbol{h}(\cdot)$ represents the non-linear function between the state variable $\boldsymbol{x}$ and the measurement $\boldsymbol{z}$; $\boldsymbol{e}^{(t)}$ and $\boldsymbol{e}^{(t+1)}$ represent the measurement error vectors in instant t and t+1, respectively. The *variations of measurement values* between two consecutive measurement scans are as follows:

$$\begin{aligned}\Delta\boldsymbol{z} &= \boldsymbol{z}^{(t+1)} - \boldsymbol{z}^{(t)} \\ &= \boldsymbol{h}\left(\boldsymbol{x}^{(t+1)}\right) - \boldsymbol{h}\left(\boldsymbol{x}^{(t)}\right) + \Delta\boldsymbol{e}.\end{aligned} \tag{41}$$

Measurement residuals of two consecutive measurement scans can be defined as follows:

$$\boldsymbol{r}^{(t)} = \boldsymbol{z}^{(t)} - \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t)}\right), \tag{42}$$

$$\boldsymbol{r}^{(t+1)} = \boldsymbol{z}^{(t+1)} - \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t+1)}\right), \tag{43}$$

where $\boldsymbol{r}^{(t)}$ and $\boldsymbol{r}^{(t+1)}$ represent the measurement residual vectors at instant t and t+1, respectively; $\hat{\boldsymbol{x}}^{(t)}$ and $\hat{\boldsymbol{x}}^{(t+1)}$ represent the state estimate vectors in instant t and t+1, respectively. The *variations of measurement residuals* between two consecutive measurement scans are as follows:

$$\begin{aligned}\Delta\boldsymbol{r} &= \boldsymbol{r}^{(t+1)} - \boldsymbol{r}^{(t)} \\ &= \boldsymbol{z}^{(t+1)} - \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t+1)}\right) - \boldsymbol{z}^{(t)} + \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t)}\right) \\ &= \Delta\boldsymbol{z} - \left[\boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t+1)}\right) - \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t)}\right)\right].\end{aligned} \tag{44}$$

When the power system is under steady-state operations, the power flow is steady, i.e., $\boldsymbol{x}^{(t+1)} = \boldsymbol{x}^{(t)}$. Under this situation, $\hat{\boldsymbol{x}}^{(t+1)} \approx \hat{\boldsymbol{x}}^{(t)}$, thus, $\Delta\boldsymbol{r} \approx \Delta\boldsymbol{z}$. In this case, the MS test will have a similar *false alarm rate* to the *k*SRS test (Please refer to the simulation results in Fig. 3 and Table III).

However, when the power system is under physical switching events, the power flow will suddenly change. For example, suppose that the power flows have fluctuations such that $\boldsymbol{h}\left(\boldsymbol{x}^{(t+1)}\right) - \boldsymbol{h}\left(\boldsymbol{x}^{(t)}\right) > \boldsymbol{0}$. In this case, it is straightforward to have $\boldsymbol{h}\left(\boldsymbol{x}^{(t+1)}\right) - \boldsymbol{h}\left(\boldsymbol{x}^{(t)}\right) \approx \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t+1)}\right) - \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t)}\right)$ when the magnitude of measurement noise is negligible compared with the operating point change. Thus, $\boldsymbol{0} \approx \left[\boldsymbol{h}\left(\boldsymbol{x}^{(t+1)}\right) - \boldsymbol{h}\left(\boldsymbol{x}^{(t)}\right)\right] - \left[\boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t+1)}\right) - \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t)}\right)\right] \ll \boldsymbol{h}\ \boldsymbol{x}\ \ \ \right) - \boldsymbol{h}\left(\boldsymbol{x}^{(t)}\right)$ and $\boldsymbol{0} \approx \Delta\boldsymbol{r} = \Delta\boldsymbol{z} - \left[\boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t+1)}\right) - \boldsymbol{h}\left(\hat{\boldsymbol{x}}^{(t)}\right)\right] \ll \ \ \boldsymbol{z}$. In other words, variations of *measurement residuals* will be much smaller than that of *measurements* under physical switching events. This conclusion has been discussed in the published papers [29], [30]. Therefore, the MS test will have a significant larger *false alarm rate* than the *k*SRS test, i.e., the MS test can easily misidentify an actual switching event in the power grid as an FDIA, while the proposed *k*SRS test can distinguish the two very well.

2) The proposed *measurement residual*-based *k*SRS test is more *sensitive* than the *measurement variation*-based MS test under ramping FDIAs.

The ramping attack vector $\tilde{\boldsymbol{a}}$ is given as follows:

$$\tilde{\boldsymbol{a}} \quad \begin{cases} \quad \boldsymbol{a} & \le \hat{} \\ \quad \tilde{\boldsymbol{a}} & \end{cases} \tag{45}$$

where $\hat{}$ represents the time required for increasing the attack vector to its full extent $\tilde{\boldsymbol{a}}$; T^{det} represents the length of the *detection interval*.

When the FDIA is ramping-type, the *measurement variations* between two consecutive measurement scans will be smaller than the full extent $\tilde{\boldsymbol{a}}$, since $\tilde{\boldsymbol{a}}$ $\tilde{\boldsymbol{a}}$. The longer the $\hat{}$, the smaller the *measurement variations*. In the case of a very long ramp (i.e., $\hat{}$), the *measurement variations* will be too small to trigger the MS test (i.e., $\tilde{\boldsymbol{a}}$). In other words, the signature used by the MS test to detect FDIA will vanish as the ramp of the FDIA becomes sufficiently long. By contrast, the *k*SRS test is dependent on the *measurement residuals* within two different time intervals. As long as the FDIA is not perfect (please see the explanation regarding the practicality of imperfect AC-based FDIA at the beginning of Section III-A), it will change the probability distributions of *measurement residuals* sufficiently when it ramps to the full scale and the *k*SRS test will be triggered. In other words, the performance of the MS test is strongly dependent on the *process* of the FDIA, but the performance of the *k*SRS test is only dependent on the final *outcome* of the FDIA and is effective against any sophisticated processes of launching FDIAs. Therefore, the *k*SRS test is more *sensitive* than the MS test when discriminating against sophisticated ramping FDIAs.

IV. Simulation Results

In this section, the effectiveness of the proposed FDIA detection method is verified using the IEEE 30-bus standard test system. In order to emulate the realistic operation in power systems, the variation trend of the loads for the IEEE 30-bus system is derived from the actual real-time electricity usage of the ISO New England in Dec. 2020 [39]. It is assumed that the test system is measured by SCADA measurements including 10 voltage magnitude measurements, 25 pairs of (active and reactive) bus injection measurements, and 40 pairs of (active and reactive) branch flow measurements. The performances of the proposed method and baseline methods will be evaluated in two aspects: *robustness* and *sensitivity*.

1) *Robustness* implies that the test should not produce a false positive result when there are other disturbances in the system instead of an FDIA. High *robustness* of a test translates into a low *false alarm rate* when there is no FDIA. This aspect of the performances will be examined in Section IV-A.

2) *Sensitivity* implies that the test should not produce a false negative result when there is an FDIA. High *sensitivity* of a test translates into a high *detection rate*. This aspect of the performances will be examined in Section IV-B.

In both Sections IV-A and IV-B, the LNR test, the Chi-square test, and the measurement similarity (MS) test will be simulated as baselines for comparison. In Section IV-C, besides the above three tests, two existing machine learning-based algorithms [40]-[44], i.e., the support vector machines (SVM) and the *k*-nearest neighbors (KNN), will be applied for further comparisons. The LNR test and the Chi-square test

are both well-known bad data detection tests [19], [45], [46]. The MS test refers to the recently developed FDIA detection test based on the statistical consistency of *measurement variations* [21]-[23]. The SVM and KNN are the most widely used classification algorithms in the machine learning area. They can train the model using labeled samples and perform the classification for the latest received measurements based on the trained model. In comparison, the proposed *k*SRS test is based on the statistical consistency of *measurement residuals*.

A Gaussian distribution with zero mean and variance of 1×10^{-4} p.u. is used to synthesize the measurement errors in Cases 1, 3, and 4. Moreover, to evaluate the FDIA detection methods under complex measurement error distribution [47], a Gaussian Mixture Model (GMM) with 3 Gaussian components is explored to synthesize the measurement errors in Cases 2 and 5. The standard deviations of the three components are 0.01 p.u., 0.004 p.u., and 0.005 p.u., respectively. The means of the three components are -0.025 p.u., 0, and 0.0167 p.u., respectively. The proportions of the three components are 0.2, 0.5, and 0.3, respectively. Considering trade-off between the accuracy of the similarity test and the reporting frequency, the length of the *reference interval* (i.e., T^{ref}) is set to 20 minutes, and the length of the *detection interval* (i.e., T^{det}) is set to 3 minutes based on empirical evidences. As the sampling rate of SCADA is assumed to be one measurement scan per second, there are 1200 measurement scans and 180 measurement scans in the *reference interval* and the *detection interval*, respectively. The parameter k is selected as 5. Each simulation is repeated 3,000 times with the average result reported.

A. Absence of False Data Injection Attacks

In this subsection, the power system is assumed to be free of FDIAs. By definition, false positives (FP) and true negatives (TN) are the cases where the detection method falsely detects an FDIA and correctly detects no FDIA when there is actually no FDIA, respectively. The *false alarm rate* is defined as the ratio of FP to the total negatives, i.e., *false alarm rate* = *FP*/(*FP*+*TN*). The FP, the TN, and the *false alarm rate* are standard metrics that are commonly used in existing works [13], [17], [18], [21], [22], [24], [25], [27]. In the following two cases, the *false alarm rate* is evaluated to verify the *robustness* of the proposed *k*SRS test.

Case 1) Steady-State Operation: In this case, it is assumed that the power system is under normal operating conditions, and no major event takes place. The actual *false alarm rates* of different FDIA detection methods under a range of *false alarm rate settings* are shown in Fig. 3. Noticeably, the actual *false alarm rate* of the LNR test is the highest among the four methods, and it does not match its own *false alarm rate setting*. The reason is related to an inherent limitation of the LNR test: only the largest residual is chosen as the test variable, while the threshold setting is based on the residuals of all measurement channels. Due to this inconsistency, the *false alarm rate* is considerably underestimated. In contrast, the Chi-square test, the MS test, and the proposed *k*SRS test all have relatively low actual *false alarm rates*, and they are consistent with the corresponding *false alarm rate settings*. Therefore, the simulation results of Case 1 verify that the proposed *k*SRS test, the Chi-square test, and the MS test all have satisfactory *robustness* when the power system operates under steady-state conditions.

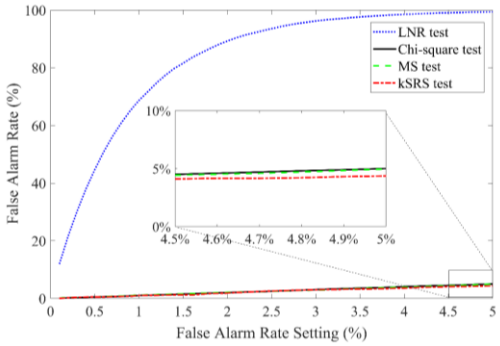

Fig. 3. False alarm rates under steady-state operation (Case 1).

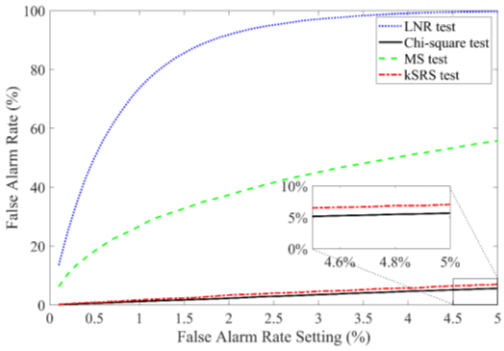

Fig. 4. False alarm rates under an actual grid switching event (Case 2).

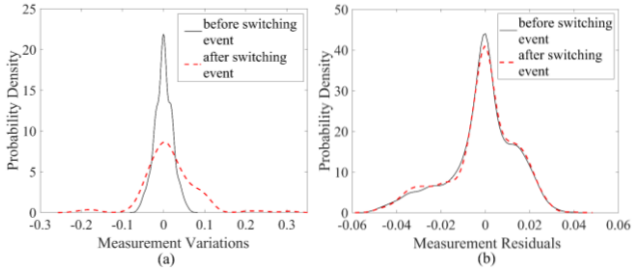

Fig. 5. PDFs of a) measurement variations before and after an actual grid switching event; b) measurement residuals before and after an actual grid switching event.

Case 2) Physical Grid Switching Event: In this case, while no FDIA is present, an actual load switching event takes place in the physical power grid. Specifically, a major load is suddenly connected to bus 24, changing the active power from 0.087 p.u. to 0.1305 p.u., and the reactive power from 0.067 p.u. to 0.1005 p.u. This actual event abruptly changes the power flow profile as well as the corresponding measurements, but the measurements remain authentic.

Fig. 4 shows the actual *false alarm rates* of all four detection methods. Compared with Case 1, the most noticeable change is that the MS test now has very high *false alarm rates*. Clearly, the MS test mistakenly detects an actual switching event in the physical grid as an FDIA. This is a highly risky error, since it may lead to the mistaken correction of authentic measurements, covering up an actual operating condition change from system operators. By contrast, the proposed kSRS test still maintains fairly low *false alarm rates*. The essential reason for the drastically different performances of the two methods can be revealed by plotting the PDFs of measurement variations and measurement residuals of a channel, as in Figs. 5-a and 5-b, respectively. It can be observed that the

TABLE I
ATTACKED STATE VARIABLES IN CASE 3 AND CASE 4

i	7	12	15	18
c_i	-0.2636 deg.	1.0485 deg.	0.0413 deg.	2.8820 deg.
i	21	49	54	55
c_i	-1.3063 deg.	-0.0040 p.u.	-0.0178 p.u.	0.0292 p.u.

TABLE II
ATTACKED STATE VARIABLES IN CASE 5

i	17	30	33	36	40
c_i	1.0256 deg.	2.8075 deg.	-0.0061 p.u.	0.0026 p.u.	-0.0129 p.u.
i	44	53	54	55	56
c_i	0.0243 p.u.	-0.0161 p.u.	-0.0239 p.u.	0.0087 p.u.	0.0288 p.u.

distribution of measurement variations, which the MS test relies on for detecting FDIAs, exhibits a major change before and after the switching event. This is easily understandable, since the power flow profile changes significantly during the event. In contrast, the distributions of measurement residuals remain almost unchanged, because the measurement residuals are strongly related to measurement errors. They do not change significantly in the presence of an accrual event in the grid, since the measurements are still authentic after the event. This feature ensures the agile discrimination between an FDIA and a physical grid event, and defuses a major risk of false alarm suffered by the existing method.

B. Presence of False Data Injection Attacks

In this subsection, the power system is assumed to be compromised by FDIAs. By definition, false negatives (FN) and true positives (TP) are the cases where the detection method falsely detects no FDIA and correctly detects an FDIA when there is actually an FDIA, respectively. The *detection rate* is defined as the ratio of TP to the total positives, i.e., *detection rate* = $TP/(FN+TP)$. The FN, the TP, and the *detection rate* are standard metrics that are commonly used in existing works [13], [17], [18], [21], [22], [24], [25], [27]. In the following three cases, the *detection rate* is evaluated to verify the *sensitivity* of the proposed *k*SRS test.

Case 3) Attacks with Inaccurate Model Parameters: In this case, it is assumed that attackers cannot attain accurate power system model parameters, and their estimates have -10%~10% random biases. In addition, 8 state variables randomly chosen are attacked with random biases following uniform distributions. The values of bias vector injected into state estimates are shown in Table I, where c_i represents the ith entry of bias vector $\boldsymbol{c}$. The attack vector (i.e., $\tilde{\boldsymbol{a}}$) is computed by Eq. (16). In this Case 3, the number of manipulated measurements is 72. In the presence of an FDIA, the *detection rates* of all four methods are shown in Fig. 6. Note that the *detection rates* of the proposed *k*SRS test are the highest among the four methods. Especially, when the false alarm rate setting is 0.1%, the *k*SRS test reaches a *detection rate* of 98.2%, implying that a low *false alarm rate* and a high *detection rate* can be achieved at the same time. At the same level of false alarm rate setting, the MS test only achieves a 79.3% *detection rate*, implying a considerable risk of missing an FDIA. The LNR test and the Chi-square test are even less *sensitive* against FDIAs. Noticeably, the Chi-square test performs very poorly, partially because it takes the residuals of all measurement channels to construct the test variable, and the subtle evidence of the FDIA can be overwhelmed by numerous good measurements.

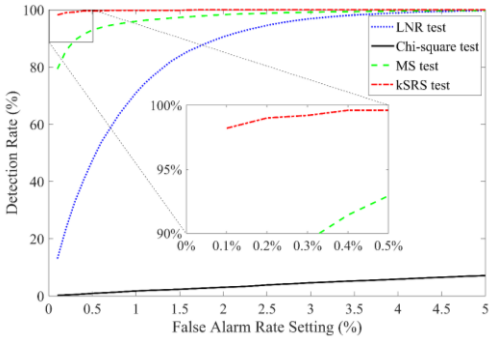

Fig. 6. Detection rates under inaccurate model parameters (Case 3).

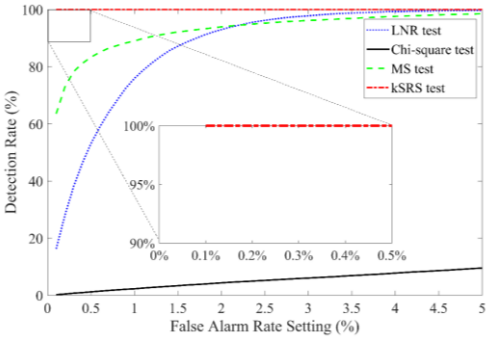

Fig. 7. Detection rates under inaccurate state estimates (Case 4).

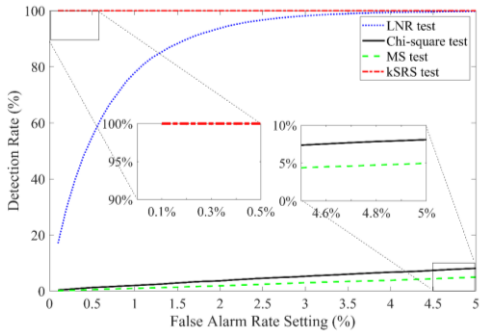

Fig. 8. Detection rates under a ramping FDIA (Case 5).

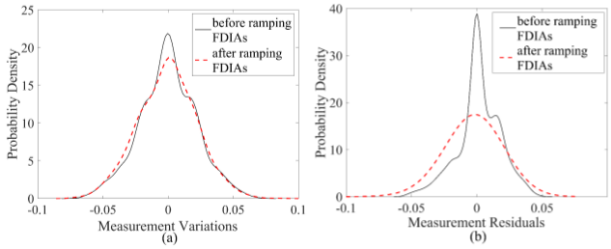

Fig. 9. PDFs of a) measurement variations before and after the start of a ramping FDIA; b) measurement residuals before and after the start of a ramping FDIA.

Case 4) Attacks with Inaccurate State Estimates: In this case, it is assumed that attackers cannot attain accurate real-time state estimates, and their estimates have -7%~7% random biases. The bias vector $\boldsymbol{c}$ in Case 4 is the same as that in Case 3. The FDIA *detection rates* of all four methods are shown in Fig. 7. Compared with Case 3 (Fig. 6), the superiority of the proposed *k*SRS test is even more significant. When the false alarm rate setting is 0.1%, the *k*SRS test reaches a *detection*

rate of 100%, while the MS test has a *detection rate* of 63.5%. Again, the results show superior sensitivity of the developed *k*SRS test compared with other existing methods.

Case 5) Ramping FDIAs: This case considers a more realistic situation where the attackers attain neither accurate model parameters nor accurate state estimates. The biases of model parameters and state estimates are the same as those in Cases 3 and 4, respectively. In addition, 10 state variables randomly chosen are attacked with random biases following uniform distributions. The values of bias vector injected into state estimates are shown in Table II, where c_i represents the ith entry of bias vector $\boldsymbol{c}$. In this Case 5, the number of manipulated measurements is 91. Meanwhile, instead of an abrupt start, the attackers aim to inject gradually increasing errors to avoid detection. The ramping attack vector $\tilde{\boldsymbol{a}}$ is given by Eq. (45) in Section III-E. In this case, τ is set to 20s.

The *detection rates* of all four methods are shown in Fig. 8. Compared with Cases 3 and 4, the MS test performs poorly under in this case. The reason is that there is no significant change of measurement values between any two consecutive time instants, thus the MS test cannot capture evidence of the FDIA. In contrast, the proposed *k*SRS test keeps the highest *detection rates* among all four methods. The reason can be revealed by plotting the PDFs of measurement variations and measurement residuals before and after launching the ramping FDIA, as shown in Fig. 9-a and Fig. 9-b, respectively. The distribution of measurement variations does not change much due to the lack of abrupt changes, while the distribution of measurement residuals changes significantly.

Theoretically, the performance of the *k*SRS test is satisfactory as long as the ramp of the attack is not significantly longer than the *detection interval*. This holds true for most FDIAs with limited resources, as false data should be derived from the *up-to-date* system state. During a long ramp, the operating state of the system can vary significantly, the attackers need to keep track of these changes and carefully recompute the attack vector in order to make the ramp smooth and consistent with the system model and state. Thus, making the ramp longer introduces higher risks of "imperfection" in the FDIA, and attackers may not opt to implement it unless they have strong capability of data processing and control over measurement streams.

C. Comparisons with Machine Learning-based Methods

In Section IV-A and IV-B, the performances of the proposed *k*SRS test have been compared with the LNR test, the Chi-square test, and the MS test for different cases. In this subsection, the SVM and KNN algorithms along with the aforementioned three tests are compared with the proposed *k*SRS test.

To emulate realistic operation conditions, the variation trend of the loads for the IEEE 30-bus system follows the actual load data of the ISO New England in Dec. 2020 [39]. For the training data, 1000 samples are manipulated by FDIAs and labeled with "-1", and the other 1000 samples are free of FDIAs and labeled with "+1". Note that the training samples are generated by system operators, while the testing samples represent actual FDIA conditions. As system operators do not really have the knowledge of FDIA distributions, the training samples and testing samples will inevitably be inconsistent.

TABLE III
PERFORMANCES OF ALL SIX DETECTION METHODS WITH 0.5% FALSE ALARM RATE SETTING

Methods	*False alarm rate* (%) (the smaller the better)		*Detection rate* (%) (the larger the better)		
	Case 1	Case 2	Case 3	Case 4	Case 5
LNR test	44.65	50.15	69.58	75.14	56.38
Chi-2 test	0.4889	0.6500	7.428	15.15	1.915
MS test	0.5112	18.34	100	100	15.22
*k*SRS test	0.5020	0.8333	100	100	100
SVM	7.600	9.300	80.30	82.20	46.23
KNN	5.500	8.200	78.40	78.50	44.46

Herein, this is assumed that system operators have a correct guess on the sign of the bias vectors, but an incorrect guess on the magnitude of the bias vectors. The bias vector $\boldsymbol{c}$ for training samples and testing samples follows the uniform distributions in the range of $[0.8\cdot\boldsymbol{c}_{base},\ 1.3\cdot\boldsymbol{c}_{base}]$ and $[0.4\cdot\boldsymbol{c}_{base},\ 0.7\cdot\boldsymbol{c}_{base}]$, respectively. $\boldsymbol{c}_{base}$ is the maximum variation range of the power flows in one day, and $\boldsymbol{c}_{base}=\boldsymbol{x}_{max}-\boldsymbol{x}_{min}$, where $\boldsymbol{x}_{max}$ and $\boldsymbol{x}_{min}$ are the state variables when the loads are heaviest and lightest, respectively.

Cases 1 and 2 designed in Section IV-A and Cases 3, 4, and 5 designed in Section IV-B still will be used in this subsection. It should be noted that the FDIAs used in Section IV-C are different from that in Section IV-B in two senses.

1) In Section IV-B, only one attack vector $\boldsymbol{a}$ is utilized for each case. In Section IV-C, however, 1000 FDIA vectors (i.e., 1000 attack vectors $\boldsymbol{a}$) are utilized for evaluating the performances of different methods.

2) In Section IV-B, the values of the bias vector $\boldsymbol{c}$ are deterministic, i.e., Tables I and II. In Section IV-C, however, the bias vector $\boldsymbol{c}$ follows the uniform distribution in the range of $[0.4\cdot\boldsymbol{c}_{base},\ 0.7\cdot\boldsymbol{c}_{base}]$.

The performances of all six detection methods for different cases are summarized in Table III. The 0.5% false alarm rate setting is used to estimate detection thresholds for the first four detection methods. For the machine learning-based methods, they do not need to set thresholds. Noticeably, the LNR test and the Chi-square test are neither *robust* nor *sensitive* for different cases. By contrast, the proposed *k*SRS test manifests both *robustness* and *sensitivity* as it has low *false alarm rates* in Cases 1 and 2 and high *detection rates* in Cases 3, 4, and 5, respectively. Similar to the results in Section IV-B, the MS test has a higher *false alarm rate* and a lower *detection rate* compared with the *k*SRS test in Case 2 and Case 5, respectively. For the SVM and the KNN methods, they have higher *false alarm rates* in Cases 1 and 2 and lower *detection rates* in Cases 3, 4, and 5 compared with the *k*SRS test. In other words, the *k*SRS test has advantages over the SVM and the KNN methods for all cases. This owes to the fact that the machine-learning-based methods are, in essence, check the *measurement value* distributions, not the *measurement residual* distributions. Therefore, they still bear the limitations of the *measurement-value-based* methods. In particular, when these methods do not have knowledge on the degree of mismatch between the power flow model and the measurement data. When the measurement value distribution changes, they are

unable to correctly determine whether the change is due to an FDIA or an actual operating condition change.

There is no method to have the best of both worlds. The comparison between model-based methods and machine-learning-based methods can be viewed from a higher perspective. Model-based methods do not need training samples and processes, but require system model and parameters along with detection threshold settings. Machine learning-based methods are independent of the system model and parameters, and allow FDIA detection even prior to power system state estimation. However, the need of abundant and representative training samples to characterize the true FDIA conditions in power system applications may be quite challenging. Machine-learning methods usually perform well when training samples have similar distributions as testing samples. As FDIAs are rare in power systems, system operators do not really have the knowledge of FDIA distributions, and the training samples they generate will inevitably be inconsistent with testing samples. Under such circumstances, the performances of machine-learning methods cannot be guaranteed. On the other hand, accurate model and parameters of power systems, which are required by model-based methods, are relatively more attainable to system operators. The simulation cases presented in this subsection exactly reflect the consequences of such realistic situations.

D. Computational Efficiency

The simulations are executed using a PC with Intel Core i7-9700K CPU, 32GB RAM, and Windows 10 64-bit operating system. The proposed *k*SRS test procedure is implemented using MATLAB version R2020b. The average computational cost for SE based on the WLAV estimator is 0.0578 seconds, and the average total computational cost for the *k*SRS test including SE and similarity calculation is 0.0589 seconds. Note that the SCADA reporting rate is assumed to be 1 Hz in this paper, and the average total computational cost (i.e., 0.0589 seconds) is far less than 1 second. Therefore, the on-line procedure of the proposed *k*SRS test is feasible.

V. Conclusion

Based on the reasonable assumption that real-world AC-based FDIAs can hardly be perfect, a highly discriminative detector, i.e., the *k*SRS test, is developed by checking the statistical consistency of *measurement residuals* to detect the *imperfect* AC-based FDIAs. Compared with the bulk of the existing FDIA detection methods based on *measurement values*, the *k*SRS test achieves better *robustness* and *sensitivity* in a variety of situations. Specifically, it does not produce a high *false alarm rate* under normal operating conditions or physical grid events, while achieves high *detection rate* in the presence of FDIAs, including sophisticated ramping attacks. The proposed *k*SRS test is easy to implement since it only requires measurement residuals from SEs as inputs, and therefore is highly applicable in energy management systems today. The validations of the proposed method based on real-world systems and data deserve more investigations in the future.

References

[1] S. W. Blume, "System control centers and telecommunications," *Electric power system basics for the nonelectrical professional*, Hoboken, NJ, USA: Wiley, 2007, pp. 203-219.

[2] V. C. Gungor *et al*., "Smart grid technologies: communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529-539, Nov. 2011.

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

[4] Y. Mo *et al*., "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

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

[6] A. R. Metke and R. L. Ekl, "Smart grid security technology," *Proc. Innov. Smart Grid Technol.*, Gaithersburg, MD, USA, 2010, pp. 1-7.

[7] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," *Proc. ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, 2009, pp. 21-32.

[8] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," *Prof. IEEE Global Commun. Conf.*, Anaheim, CA, USA, 2012, pp. 3153-3158.

[9] 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.

[10] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630-1638, Jul. 2017.

[11] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864-3872, Sep. 2016.

[12] J. Kim and L. Tong, "On phasor measurement unit placement against state and topology attacks," *Proc. IEEE Int. Conf. Smart Grid Commun.*, Vancouver, BC, Canada, 2013, pp. 396-401.

[13] J. Zhao *et al.*, "Robust detection of cyber attacks on state estimators using phasor measurements," *IEEE Trans. Power Syst.*, vol. 32, no. 3, pp. 2468-2470, May 2017.

[14] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, 2010.

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

[16] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, "Detecting false data injection attacks against power system state estimation with fast Go-decomposition approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2892-2904, May 2019.

[17] J. Zhao, G. Zhang, M. La Scala, Z. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580-1590, Jul. 2017.

[18] 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.

[19] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*, New York, NY: Marcel Dekker, 2004.

[20] M. Jin, J. Lavaei, and K. Johansson, "Power grid AC-based state estimation: vulnerability analysis against cyber attacks," *IEEE Trans. Autom. Control*, vol. 64, no. 5, pp. 1784-1799, May 2019.

[21] 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.

[22] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 1, pp. 89-97, Jan. 2018.

[23] 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," *Prof. IEEE Power Energy Soc. Gen. Meeting*, Chicago, IL, USA, 2017, pp. 1-5.

[24] Z. Wang, H. He, Z. Wan, and Y. Sun, "Detection of false data injection attacks in AC state estimation using phasor measurements," *IEEE Trans. Smart Grid*. DOI: 10.1109/TSG.2020.2972781. (early access)
[25] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868-4877, Sep. 2018.
[26] J. Yu, Y. Hou, and V. 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.
[27] 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.
[28] Y. He, G. J. Mendis and J. Wei, "Real-Time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505-2516, Sep. 2017.
[29] M. B. Do Coutto Filho and J. C. Stacchini de Souza, "Forecasting-aided state estimation—part I: panorama," *IEEE Trans. Power Syst.*, vol. 24, no. 4, pp. 1667-1677, Nov. 2009.
[30] M. B. Do Coutto Filho, J. C. Stacchini de Souza, and R. S. Freund, "Forecasting-aided state estimation—part II: implementation," *IEEE Trans. Power Syst.*, vol. 24, no. 4, pp. 1678-1685, Nov. 2009.
[31] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346-1355, May 2016.
[32] M. Yue, T. Hong, and J. Wang, "Descriptive analytics-based anomaly detection for cybersecure load forecasting," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 5964-5974, Nov. 2019.
[33] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3438-3446, July 2020.
[34] Y. Lin, A. Abur, and H. Xu, "Identifying security vulnerabilities in electricity market operations induced by weakly detectable network parameter errors," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 627-636, Jan. 2021.
[35] S.-H. Cha, "Comprehensive survey on distance/similarity measures between probability density functions," *Int. J. Math. Models Methods Appl. Sci.*, vol. 4, no. 1, pp. 300-307, 2007.
[36] D. M. Endres and J. E. Schindelin, "A new metric for probability distributions," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1858-1860, Jul. 2003.
[37] M. Huang *et al*., "Detecting false data injection attacks on modern power systems based on Jensen-Shannon distance," *Proc. IEEE 8th Annual Int. Conf. CYBER Technol. Autom., Control, and Intell. Syst.*, Tianjin, China, 2018, pp. 1154-1159.
[38] P. Mathews, *Sample size calculations*: *practical methods for engineers and scientists*. Fairport Harbor, OH, USA: Mathews Malnar and Bailey Inc., 2010.
[39] "System load graphs," *ISO New England-Real-Time Maps and Charts*. [Online]. Available: https://www.iso-ne.com/isoexpress/web/charts.
[40] A. Kumar, N. Saxena, and B. J. Choi, "Machine learning algorithm for detection of false data injection attack in power system," *Proc. 2021 International Conference on Information Networking (ICOIN)*, Jeju island, Korea (South), 2021, pp. 385-390.
[41] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005-1016, June 2016.
[42] 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.
[43] M. Mohammadpourfard, A Sami, and A. R. Seifi, "A statistical unsupervised method against false data injection attacks: A visualization-based approach," *Expert Syst. With Appl.*, vol. 84, pp. 242-261, 2017.
[44] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *J. Inf. Secur. Appl.*, vol. 46, pp. 42-52, 2019.
[45] Y. Lin and A. Abur, "A highly efficient bad data identification approach for very large scale power systems," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 5979-5989, Nov. 2018.
[46] 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.
[47] G. Cheng, Y. Lin, Y. Chen, and T. Bi, "Adaptive state estimation for power systems measured by PMUs with unknown and time-varying error statistics," *IEEE Trans. Power Syst.*, vol. 36, no. 5, pp. 4482-4491, Sep. 2021.

Gang Cheng (Student Member, IEEE) received his B.S. degree in Electrical Engineering and Automation from Henan Polytechnic University, Jiaozuo, China, in 2016. He received his M.S. degree in Control Theory and Control Engineering from Guangxi University, Nanning, China, in 2019. He has been a Ph.D. student in the Department of Electrical and Computer Engineering at the University of Massachusetts, Lowell, MA, USA, since 2020. His current research interests include situational awareness, cyber security, and data analysis of power systems.

Yuzhang Lin (Member, IEEE) is currently an assistant professor in the Department of Electrical and Computer Engineering at the University of Massachusetts, Lowell, MA, USA. He obtained his Bachelor and Master's degrees from Tsinghua University, Beijing, China, and Ph.D. degree from Northeastern University, Boston, MA, USA. His research interests include modeling, situational awareness, data analytics, and cyber-physical resilience of smart grids.

Junbo Zhao (Senior Member, IEEE) is an assistant professor of the Department of Electrical and Computer Engineering at the University of Connecticut. He was an assistant professor and research assistant professor at Mississippi State University and Virginia Tech from 2019-2021 and 2018-2019, respectively. He received the Ph.D. degree from Bradley Department of Electrical and Computer Engineering Virginia Tech, in 2018. He was a Research Assistant Professor at Virginia Tech from May 2018 to August 2019. He did the summer internship at Pacific Northwest National Laboratory from May to August 2017. He is currently the chair of the IEEE Task Force on Power System Dynamic State and Parameter Estimation, the IEEE Task Force on Cyber-Physical Interdependency for Power System Operation and Control, co-chair of the IEEE Working Group on Power System Static and Dynamic State Estimation, the Secretary of the IEEE PES Bulk Power System Operation Subcommittee and officer of the IEEE PES Renewable Systems Integration Coordinating Committee.

He has published three book chapters and more than 140 peer-reviewed journal and conference papers, where more than 70 appear in IEEE Transactions. His research interests are cyber-physical power system modeling, estimation, security, dynamics and stability, uncertainty quantification, renewable energy integration and control, robust statistical signal processing and machine learning. He serves as the editor of IEEE Transactions on Power Systems, IEEE Transactions on Smart Grid and IEEE Power and Engineering Letters, the Associate Editor of International Journal of Electrical Power & Energy Systems, and the subject editor of IET Generation, Transmission & Distribution. He is the receipt of the best paper awards of 2020 and 2021 IEEE PES General Meeting (3 papers) and 2019 IEEE PES ISGT Asia. He received the 2020 Top 3 Associate Editor Award from IEEE Transactions on Smart Grid, the 2020 IEEE PES Outstanding Engineer Award, and the 2021 IEEE PES Outstanding Volunteer Award. He has been listed as the 2020 and 2021 World's Top 2% Scientists released by Stanford University in both Single-Year and Career tracks.

Jun Yan (Member, IEEE) received the B.Eng. degree in Information and Communication Engineering from Zhejiang University, China, in 2011, and the M.S. and Ph.D. (with Excellence in Doctoral Research) degrees in Electrical Engineering from the University of Rhode Island, USA, in 2013 and 2017, respectively. He is currently an Assistant Professor at the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada. His research focuses on computational intelligence and cyber-physical security, with applications in smart grids, smart cities, and other smart critical infrastructures. His research has been funded by NSERC, FRQNT, FRQSC, CFI, and Mitacs. He was also the recipient of several best paper awards at IEEE ICC, IEEE WCCI, among others.