Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks

James J. Q. Yu, *Member, IEEE*, Yunhe Hou, *Senior Member, IEEE*, and Victor O. K. Li, *Fellow, IEEE*

***Abstract*—State estimation is critical to the operation and control of modern power systems. However, many cyber-attacks, such as false data injection attacks, can circumvent conventional detection methods and interfere the normal operation of grids. While there exists research focusing on detecting such attacks in dc state estimation, attack detection in ac systems is also critical, since ac state estimation is more widely employed in power utilities. In this paper, we propose a new false data injection attack detection mechanism for ac state estimation. When malicious data are injected in the state vectors, their spatial and temporal data correlations may deviate from those in normal operating conditions. The proposed mechanism can effectively capture such inconsistency by analyzing temporally consecutive estimated system states using wavelet transform and deep neural network techniques. We assess the performance of the proposed mechanism with comprehensive case studies on IEEE 118- and 300-bus power systems. The results indicate that the mechanism can achieve a satisfactory attack detection accuracy. Furthermore, we conduct a preliminary sensitivity test on the control parameters of the proposed mechanism.**

***Index Terms*—AC state estimation, cyber-attack detection, deep neural network (DNN), discrete wavelet transform (DWT), false data injection attack (FDIA).**

I. Introduction

With the incorporation of information and communication technologies, power systems are gradually transforming into smart grids [1]. However, power system applications, such as state estimation [2], are facing great challenges due to their dependence on telecommunications. One significant concern is their vulnerability to cyber-attacks [3]–[5]. Adversaries of power grids can access and manipulate system variable measurements by either attacking the measurement devices or compromising the communication infrastructures [6]. As a result, compromised system states may interfere the operation of the grid, leading to either physical or economical impacts on the power system. Liang *et al.* [7] and Deng *et al.* [8] presented comprehensive surveys on the impacts of such cyber-attacks.

Among common attacks in cyber-physical systems, false data injection attack (FDIA) is considered one of the most challenging threats for the state estimation [7], [9]. Different from other attacks such as distributed denial of service and jamming, successful FDIA can circumvent the conventional residual-based bad data detection mechanism [10]. Without advanced detection mechanism, FDIA can be stealthily launched multiple times, rendering a significant threat to the grid [8].

Much research effort has been devoted to investigating possible ways of constructing FDIA [8]. Most of the existing work on constructing FDIA focuses on attacks in power systems with dc state estimation under different scenarios, due to simple analytical models of the system [7]. For instance, a commonly recognized attack scenario is that the adversary has partial configuration information of the power network, and can manipulate a partial set of system variable measurements [9], [11], [12]. In the presented methods, FDIA can successfully bypass conventional detection methods and inject malicious data into the system. In the meantime, FDIA targeting ac state estimation is gradually gaining attention in recent years, and analytical studies have been conducted to construct such attacks. In [13]–[15], viable methods were presented to perform FDIA in ac state estimation with complete or incomplete system knowledge. To conclude, both dc and ac state estimations are prone to FDIA.

At the same time, many results have been reported to defend against FDIA in dc state estimations.[1] Various techniques have been employed to detect dc FDIA, such as statistical methods [16], [17], Kalman filter [18], sparse optimization [19], state forecasting [20], [21], network theory [22], time-series simulation [23], and machine learning [24]–[28]. They all demonstrate satisfactory detection performance and false-alarm rates against dc FDIA. See [7] for a survey on the detection methods of FDIA.

However, there is still a research gap in the current FDIA detection paradigm. All previously referenced publications investigate attacks targeting dc state estimations, which use different system models from the ac ones employed in most real-world utilities [15]. As will be demonstrated in Section IV, conventional dc FDIA detection methods cannot detect ac FDIA with

Manuscript received January 21, 2018; revised January 31, 2018, March 4, 2018, and April 2, 2018; accepted April 3, 2018. Date of publication April 10, 2018; date of current version July 2, 2018. This work was supported by the Theme-based Research Scheme of the Research Grants Council of Hong Kong under Grant T23-701/14-N. Paper no. TII-18-0176. *(Corresponding author: James J. Q. Yu.)*

The authors are with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong (e-mail: jqyu@eee.hku.hk; yhhou@eee.hku.hk; vli@eee.hku.hk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2018.2825243

[1]FDIAs aiming to compromise system states in ac/dc power systems are called ac/dc FDIA in the sequel.

satisfactory performance. Little work has been done on detecting ac FDIA in the literature, especially defending against recent attack patterns, e.g., [14] and [15]. In [29], Chaojun *et al.* propose an FDIA detection mechanism for ac state estimation based on the Kullback–Leibler distance of the probability distributions of nominal operating conditions and compromised system states. However, its robustness considering normal power system events, such as load distribution changes, is unknown. As the manipulated system states of new attack methods obey Kirchhoff's circuit laws [15], it is possible that these attacks can pretend to be normal operating condition changes to avoid being detected. In [30], Liu *et al.* developed an information-network-based state estimation technique to defend against ac FDIA. In [31], Tian *et al.* actively changed the transmission line parameters to detect ac FDIA. Both studies aim at ac FDIA constructed with full power network information, and their performance on the latest proposed attacks based on partial network information, e.g., [15], is unknown.

To bridge the research gap, in this paper, a new ac FDIA detection mechanism is proposed, which considers recent ac FDIA patterns. Different from the previous work for detecting FDIA, which only adopts the spatial data characteristics in the system state of one time instance to identify attacks, the proposed mechanism also learns from the temporal data correlation presented in consecutive system states. To achieve this, we adopt the discrete wavelet transform (DWT) algorithm and recent advances of deep neural networks (DNN) techniques and construct an intelligent system for ac FDIA detection. In the system, DWT aims to extract the system state features in a given time period, and DNN further learns from the temporal–spatial characteristics of the features in a sequence of time periods to distinguish ac FDIA from normal power system operation events. The main contributions of this paper are listed as follows.

1) This paper is among the pioneer studies of using DNN in FDIA detection research. In addition, the proposed mechanism extracts not only spatial (as did in [24] and [26]) but also temporal power system dynamic features for attack detection, which is novel and effective.
2) The proposed mechanism aims to detect FDIA in ac state estimation, especially recent attack patterns with incomplete power network information [15].
3) We assess the proposed mechanism with recently proposed FDIA patterns on two power system test cases. The simulation results demonstrate satisfactory attack detection accuracy and false-alarm rate.
4) Parameter sensitivity test is carried out to evaluate the performance and characteristics of the proposed mechanism.

The remainder of this paper is organized as follows. In Section II, we briefly introduce the current state estimation methods and its vulnerability against FDIA. Section III elaborates the proposed FDIA detection mechanism with detailed explanation on the architecture and implementation issues. Section IV demonstrates the numerical results on the tested power systems with parameter sensitivity studies. Finally, we conclude this work in Section V.

II. State Estimation and FDIA

In this section, we first briefly introduce the state estimation method employed by the utilities and the incorporated bad data detection mechanism. Then, we give a general pattern of successful FDIA targeting ac state estimation.

A. State Estimation and Bad Data Detection

The basic principle of state estimation is to estimate the operating condition of the power system using system variable samples from the measurement units [32]. Typical measurements include voltage and complex power injections at buses, and complex power flows on branches. Based on the ac power flow model, we can construct the relationship between measurements $\mathbf{z}$ and system states $\mathbf{x}$ as follows:

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

where $h(\cdot)$ is the nonlinear dependency between measurements and system states, and $\mathbf{e}$ is the additive noise with a covariance $\mathbf{R}$. The equations defined by $h(\cdot)$ are determined by the grid topology and transmission line parameters. State estimation tries to find an estimated system state $\hat{\mathbf{x}}$ that fits the measurements $\mathbf{z}$ best, according to the dependency $h(\cdot)$ considering sampling noise. Subsequently, given $\mathbf{z}$, $h(\cdot)$, and $\mathbf{R}$, system states can be estimated by minimizing the weighted least square [32], [33]

$$\hat{\mathbf{x}} = \underset{\mathbf{x}}{\operatorname{argmin}} [\mathbf{z} - h(\mathbf{x})]^{\mathsf{T}} \mathbf{W} [\mathbf{z} - h(\mathbf{x})] \tag{2}$$

where $\mathbf{W} \equiv \operatorname{diag}\{\mathbf{R}^{-1}\}$. In practice, (2) can be solved using iterative approximation methods, e.g., Newton–Raphson method.

However, due to the nonlinearity of $h(\cdot)$ and the iterative manner of the approximation solutions, solving (2) can be computationally expensive [2]. Furthermore, the convergence is not guaranteed [33]. As an alternative, power system engineers sometimes employ a linearized dc power flow model to approximate the ac model. A dc model simplifies the system by making three assumptions:

1) line resistance is negligible;
2) bus voltage profile is flat; and
3) voltage angle deviation over transmission lines is small.

As a result, the relationship in (1) can be simplified to

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{3}$$

where $\mathbf{H}$ is the measurement Jacobian matrix [33]. Accordingly, (2) is transformed into

$$\begin{aligned} \hat{\mathbf{x}} &= \underset{\mathbf{x}}{\operatorname{argmin}} [\mathbf{z} - \mathbf{H}\mathbf{x}]^{\mathsf{T}} \mathbf{W} [\mathbf{z} - \mathbf{H}\mathbf{x}] \\ &= (\mathbf{H}^{\mathsf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{\mathsf{T}}\mathbf{W}\mathbf{z} \equiv \mathbf{E}\mathbf{z} \end{aligned} \tag{4}$$

where $\mathbf{E} \equiv (\mathbf{H}^{\mathsf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{\mathsf{T}}\mathbf{W}$. This closed-form solution can provide fast estimated states, but also introduce approximation error due to the dc power flow model assumptions [33].

Considering the sampling error of measurement units and potential malicious attacks, current power systems employ a residual-based bad data detection mechanism to protect state estimations [33]. The measurement residual is calculated

using the difference between observed measurements $\mathbf{z}$ and measurements inferred by the estimated system state, denoted by $\hat{\mathbf{z}} = h(\hat{\mathbf{x}})$ (ac model) or $\hat{\mathbf{z}} = \mathbf{H}\hat{\mathbf{x}}$ (dc model). Bad data detection mechanism compares the Euclidean norm of the residual $\mathbf{r} = \mathbf{z} - \hat{\mathbf{z}}$ with threshold τ. If $||\mathbf{r}||_2 > \tau$, the estimated state is considered compromised by bad data; otherwise $\hat{\mathbf{x}}$ is trustworthy. The value of τ is typically determined by a hypothesis test $\Pr\{||\mathbf{r}||_2^2 \geq \tau^2\} = \alpha$, where α is the confidence level [33].

B. FDIA With Complete Network Information

The objective of adversaries to perform FDIA is to mislead the system operator to consider a compromised $\hat{\mathbf{x}}_a = \hat{\mathbf{x}} + \mathbf{c}$ as the estimated system state, where $\mathbf{c}$ is the deviation of power system state. To achieve this, an adversary can change the received measurements at the control center to $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$, where $\mathbf{a}$ is the injected attack vector. To circumvent bad data detection mechanism,[2] the attack vector should be constructed as

$$\mathbf{a} = h(\hat{\mathbf{x}} + \mathbf{c}) - h(\hat{\mathbf{x}}). \tag{5}$$

In such cases, the Euclidean norm of the residual is unchanged

$$\begin{aligned} ||\mathbf{r}_a||_2 &= ||\mathbf{z}_a - h(\hat{\mathbf{x}}_a)||_2 = ||\mathbf{z} + \mathbf{a} - h(\hat{\mathbf{x}} + \mathbf{c})||_2 \\ &= ||\mathbf{z} - \hat{\mathbf{z}}||_2 = ||\mathbf{r}||_2 \end{aligned} \tag{6}$$

and the attack can bypass the residual-based detection. The detailed attack vector construction process is elaborated in [13] and [34]. However, there is one drawback in this FDIA pattern. According to (5), the adversary requires complete knowledge of the grid, including the topology ($h(\cdot)$) and estimated states ($\hat{\mathbf{x}}$). In the meantime, FDIA can only utilize less-than-perfect system information in practice [7]. To consider this limitation, recent work proposed new FDIA patterns using partial system knowledge [14], [15]. For instance, a recently published result in [15] successfully constructs injected attack vectors using voltage angle differences of selected transmission lines, which will be introduced in the following.

C. FDIA With Partial Network Information

In [15], the rule of thumb of using partial network information to construct FDIA injection vector is to satisfy Kirchhoff's circuit laws, given only selected voltage angle differences. Specifically, the voltage angle differences of lines connecting a compromised bus and another noncompromised one are used to calculate feasible power flows of respective lines, and thus, the power injections of the compromised buses are obtained. Those for the other buses can consequently be calculated by the algebraic sum of all connecting buses. Utilizing the above-mentioned idea, an attack vector can be constructed as follows [15].

1) Initialize the system state vector $[\boldsymbol{V\theta}]^\mathsf{T} = [\boldsymbol{V}_0\boldsymbol{\theta}_0]^\mathsf{T}$, where $\boldsymbol{V}_0$ is the initial attack voltage profile.
2) Compute the attack vector $[\boldsymbol{PQpq}]^\mathsf{T}$(bus real/reactive power injection and line flow) using the current $[\boldsymbol{V\theta}]^\mathsf{T}$.
3) Check the constructed attack vector against the upper and lower bounds of real power bus injections and real/reactive power line flows [15]

$$\underline{\boldsymbol{P}} \leq \boldsymbol{P} \leq \overline{\boldsymbol{P}}, -\overline{\boldsymbol{p}} \leq \boldsymbol{p} \leq \overline{\boldsymbol{p}}, -\overline{\boldsymbol{q}} \leq \boldsymbol{q} \leq \overline{\boldsymbol{q}} \tag{7}$$

where the overlined and underlined variables are the upper and lower bounds, respectively. If all bounds are satisfied, $[\boldsymbol{V\theta}]^\mathsf{T}$ is used as the attack vector. Otherwise continue.
4) Calculate the incremental state vector $[\Delta\boldsymbol{V}\Delta\boldsymbol{\theta}]^\mathsf{T}$ by solving an optimization problem

$$\text{minimize} \quad \sum_{i=1}^{10} \mathbf{1}^\mathsf{T}\boldsymbol{S}_i \tag{8a}$$

$$\text{subject to} \quad \begin{bmatrix} \Delta\boldsymbol{P} \\ \Delta\boldsymbol{Q} \\ \Delta\boldsymbol{p} \\ \Delta\boldsymbol{q} \\ \Delta\boldsymbol{V} \end{bmatrix} = \begin{bmatrix} \partial\boldsymbol{P}/\partial\boldsymbol{V} & \partial\boldsymbol{P}/\partial\boldsymbol{\theta} \\ \partial\boldsymbol{Q}/\partial\boldsymbol{V} & \partial\boldsymbol{Q}/\partial\boldsymbol{\theta} \\ \partial\boldsymbol{p}/\partial\boldsymbol{V} & \partial\boldsymbol{p}/\partial\boldsymbol{\theta} \\ \partial\boldsymbol{q}/\partial\boldsymbol{V} & \partial\boldsymbol{q}/\partial\boldsymbol{\theta} \\ \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} \Delta\boldsymbol{V} \\ \Delta\boldsymbol{\theta} \end{bmatrix} \tag{8b}$$

$$\underline{\boldsymbol{P}} \leq \boldsymbol{P} + \Delta\boldsymbol{P} + \boldsymbol{S}_1 - \boldsymbol{S}_2 \leq \overline{\boldsymbol{P}} \tag{8c}$$

$$-\overline{\boldsymbol{p}} \leq \boldsymbol{p} + \Delta\boldsymbol{p} + \boldsymbol{S}_3 - \boldsymbol{S}_4 \leq \overline{\boldsymbol{p}} \tag{8d}$$

$$-\overline{\boldsymbol{q}} \leq \boldsymbol{q} + \Delta\boldsymbol{q} + \boldsymbol{S}_5 - \boldsymbol{S}_6 \leq \overline{\boldsymbol{q}} \tag{8e}$$

$$\underline{\boldsymbol{V}} \leq \boldsymbol{V} + \Delta\boldsymbol{V} + \boldsymbol{S}_7 - \boldsymbol{S}_8 \leq \overline{\boldsymbol{V}} \tag{8f}$$

$$\underline{\boldsymbol{\theta}} \leq \boldsymbol{G}(\boldsymbol{\theta} + \Delta\boldsymbol{\theta}) + \boldsymbol{S}_9 - \boldsymbol{S}_{10} \leq \overline{\boldsymbol{\theta}} \tag{8g}$$

where $\boldsymbol{G}$ is the coefficient matrix that transforms bus voltage angles into line angle differences. Variables $\boldsymbol{S}_i$ are slack control variables that determine the incremental state and attack vector [15].
5) Update attack vector $[\boldsymbol{V\theta}]^\mathsf{T} \leftarrow [\boldsymbol{V\theta}]^\mathsf{T} + [\Delta\boldsymbol{V}\Delta\boldsymbol{\theta}]^\mathsf{T}$ and go to Step 2.

By repeating this process, the adversary can construct an attack vector against ac state estimations without being detected by the residual-based bad data detection method [15]. In addition, as will be illustrated in Section IV, the constructed attack vectors can also bypass the detection of many existing dc FDIA detection methods. Therefore, it is essential to develop a new mechanism that focuses on detecting ac FDIA.

III. Online FDIA Detection Mechanism

As analyzed in Section II, well-constructed FDIA can effectively bypass bad data detection mechanism in ac state estimation. This is because the injected false data satisfy Kirchhoff's circuit laws [15], rendering all residual-based attack detection methods invalid. Thus, it is not possible for the system operator to distinguish FDIA from normal power system events, given measurements from the same sampling time period. However, this does not make FDIA undetectable. Synchrophasor data of a power system over a period of time can be considered as a temporal–spatial matrix/tensor. It is widely accepted that the data have spatial correlation, which is represented by

[2]In the sequel, we consider ac power flow model unless mentioned.

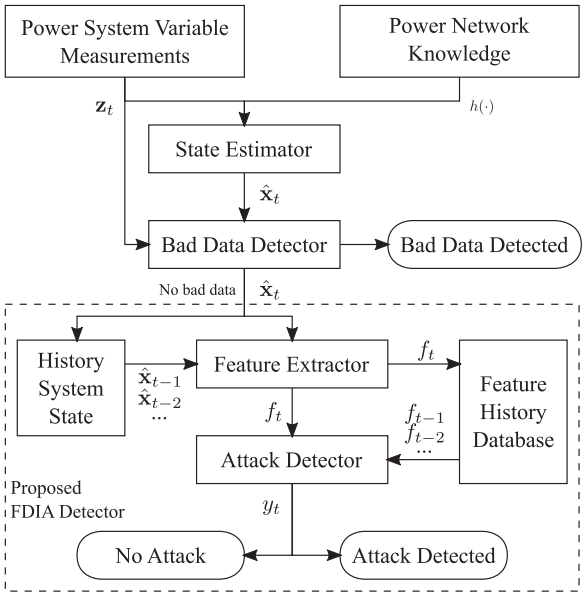


Fig. 1. Proposed online FDIA detection mechanism with a DNN-based attack detector.

Kirchhoff's Laws. At the same time, the temporal correlation also exists in power systems among consecutive time slots, which is especially strong in transient and dynamic operations due to the inertia and momentum in the whole system. In current FDIA constructions, adversaries focus on constructing attack vectors satisfying the spatial dependencies of system variables, i.e., (5), and ac power flow equations [14], [15]. The temporal dependency between consecutive system states, or power system dynamics, is ignored. This correlation in system states can provide more information for the system operator to detect FDIA while reducing false alarms on normal grid events.

Utilizing this principle, in this section, we propose an online FDIA detection mechanism using recent advances in deep learning techniques. We first elaborate the structure and data flow of the proposed mechanism. Then, we present the detailed implementation of the mechanism with brief introductions to the techniques employed. Finally, we discuss the offline training and online detection processes of the proposed mechanism.

A. Proposed Detection Mechanism

The proposed FDIA detection mechanism is depicted in Fig. 1. This mechanism considers the system states and measurements from consecutive discrete sampling time instances, i.e., the time instances when the conventional state estimation takes place. These sampling time instances may have an interval Δ ranging from milliseconds (PMU-based measurement systems) to a few seconds (conventional supervisory control and data acquisition (SCADA) system). At an arbitrary sampling time instance t, the mechanism takes real-time measurements $\mathbf{z}_t$ and the utility's knowledge of the power network $h(\cdot)$ as inputs, and develop FDIA attack detection results as the output. The input data first go through an ac state estimator, which estimates the current system state as $\hat{\mathbf{x}}_t$ [2], [32], [33]. The estimated state is then tested with the bad data detector to prune any measurements with bad data. In this step, bad data caused by sampling and communication errors can be effectively detected, since they generally do not satisfy the circuit laws, rendering high residual values [8], [33].

After these conventional state estimation processes, the proposed FDIA detection mechanism introduces a new FDIA detector to further analyze the estimated system states. The detector, as shown in the dashed box in Fig. 1, comprises two data processing schemes. It takes the estimated system states $\hat{\mathbf{x}}_t$ from the previous state estimator as input. The system state is first stored in a system state history database. Then, a feature extractor identifies the spatial data correlations (features) of the immediately past 60 system states, and the resulting information, denoted by $\mathbf{f}_t$, is stored in a feature history database. Subsequently, the features of the current and previous $w-1$ sampling time instances are input to an attack detector, which learns the temporal data correlation and detects FDIA. In this process, w is a user-defined control variable. A large w can lead to more features in the time domain, rendering a thorough system dynamics. However, the computational efficiency may be compromised. We will study the sensitivity of w in Section IV.

In this FDIA detector design, it is evident that the detection performance is dominated by the feature extractor and attack detector. These two blocks need to derive the distinguishing spatial–temporal characteristics of the system state dynamics, and make accurate classifications on attack events against others. In this paper, we employ DWT algorithm to extract the attack features due to its outstanding feature extraction capability [35], [36]. In addition, existing neural network units are adopted to construct a DNN to further identify attack patterns from the extracted features. Contributed by recent advances of deep learning technologies, DNN is widely recognized as a superior methodology for classification tasks [37]. Variants of DNN have been employed recently in solving many power system operation problems; see [24] and [38] for examples.

B. DWT-Based Feature Extractor

DWT is a digital signal processing technique aiming to extract the hidden time–frequency domain characteristics of any input signals. The technique convolves the input data sequence with wavelets, which are zero-mean functions derived from predefined mother wavelets. Typically, a wavelet $\psi_{a,b}(t)$ can be developed from its mother wavelet $\psi(t)$ as follows:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}}\psi\left(\frac{t-b}{a}\right) \tag{9}$$

where a and b are scaling and shifting parameters, respectively. DWT is performed based on discrete form of (9) by discretizing $a = 2^j$ and $b = 2^j \times k$, $j, k \in \mathbb{Z}$. Then, this wavelet can be employed to transform a sequence of input signal $s(t)$ using the following equation:

$$d_{j,k}(s(t), \psi(t)) = \int_{-\infty}^{+\infty} s(t)\psi^*_{j,k}(t)dt \tag{10}$$

where $\psi^*_{j,k}(t)$ is the complex conjugate of discrete wavelet $\psi_{j,k}(t) = \psi(t/2^j - k)/\sqrt{2^j}$.

TABLE I
FEATURE EXTRACTION WAVELETS AND DECOMPOSITION LEVELS

Wavelet	Filter Length	M	Wavelet	Filter Length	M
db2	4	4	sym2	4	4
db8	16	2	sym8	16	2

However, the analytical solutions to (10) is not always obtainable [35], [39], [40]. To address this problem, a widely adopted method proposed in [35] is employed in this paper. The basic concept of the method is to utilize the multiresolution decomposition of $s(t)$ at level M, which is defined by

$$\begin{aligned} s(t) &= \sum_k a_{M,k}\varphi\left(\frac{1}{2^M}-k\right)/\sqrt{2^M} \\ &\quad + \sum_j^M \sum_k d_{j,k}\psi\left(\frac{1}{2^j}-k\right)/\sqrt{2^j} \\ &\triangleq A_M(t) + \sum_j D_j(t) \end{aligned} \tag{11}$$

where $a_{M,k}$ and $\varphi(t)$ are the approximation coefficient at level M and the companion scaling function, respectively [35]. Using this relation, $s(t)$ can be decomposed into an approximation coefficient $A_M(t)$ and M detailed coefficients $D_j(t)$. Mallat [35] gives the detailed algorithm for this decomposition.

From (10) and (11), it can be observed that different wavelets and decomposition levels M can lead to different decomposed signal coefficients. These coefficients will further influence the feature extraction capability of the DWT-based feature extractor. While there should be an optimal setting of wavelets and M values for optimal performance, it is impractical to test all wavelets. As an alternative, they are typically selected strategically according to the data properties [40], [41]. Specifically, when the data contain sufficient sample of signals, `db` and `sym` families of wavelets are generally preferred due to their robustness regardless of special data properties [40]. Other wavelets, e.g., `bior` and `coif` families, suffer from their longer filter lengths, which can lead to low level of decomposition and bad feature extraction capability [40]. Therefore, in this paper, four wavelets from `db` and `sym` families are employed to decompose the input signal, i.e., bus voltage magnitudes and phase angles. The wavelets and their respective M values are recorded in Table I.

According to (11), in total 16 signal coefficients can be calculated from one input signal. However, the decomposed data sequences are generally too long to be employed in subsequent calculations [36]. In addition, it has been shown that the statistical features of these data sequences can also represent critical features of the input signal [36]. Hence, we adopt the mean and standard deviation values of all coefficients to represent the features of the input signal in the proposed feature extractor. These statistical features have demonstrated their efficacy in the literature for classification tasks; see [36], [40] and [41] for examples. Consequently, 16(coefficients) $\times$ 2(mean and standard deviation) $\times\, 2N$(bus voltage magnitudes and angles) $= 64N$ features are calculated for each system state of an N-bus power system. These features are stored as a representative feature vector of the respective time instance in the feature history database, as depicted in Fig. 1.

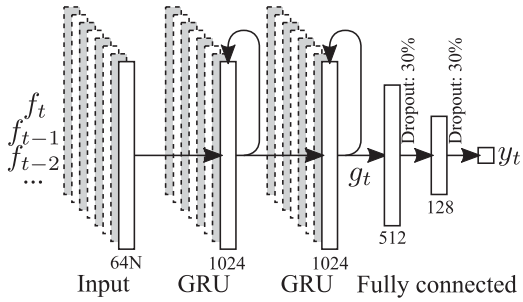


Fig. 2. Proposed DNN-based attack detector.

C. DNN-Based Attack Detector

In the proposed DNN-based attack detector, we adopt existing DNN units to construct a recurrent neural network (RNN) model. This network aims to distinguish attacks from normal power system operating events, by learning from the temporal–spatial system state features extracted by DWT. RNN is a type of neural network that considers both the temporal and spatial dependencies of a sequence of input data. In the constructed network, two types of neuron layers are utilized, namely, gated recurrent unit (GRU) [42] and fully-connected (dense) layers. Each layer can establish a mathematical relationship between the input and output data. When these layers are chained up, the combined mathematical expression is used to simulate nonlinear system models.

In this paper, we carefully tuned the hyperparameters of the network, namely numbers of layers and neurons in each layer, to achieve a satisfactory attack detection accuracy. Fig. 2 presents the schema of the proposed DNN-based attack detector. The constructed RNN model is composed of two GRU layers and two Dense layers. In GRU, given a sequence of input data $\{f_{t-w+1}, \ldots, f_t\}$, GRU calculates a sequence of output $\{g_{t-w+1}, \ldots, g_t\}$ as follows:

$$\begin{aligned} g_t &= z_t \otimes g_{t-1} \\ &\quad + (1-z_t) \otimes \tanh(w_{fg} f_t + w_{gg}(r_t \otimes g_{t-1}) + b_g) \end{aligned} \tag{12a}$$

$$z_t = \mathrm{sigm}(w_{fz} f_t + w_{gz} g_{t-1} + b_z) \tag{12b}$$

$$r_t = \mathrm{sigm}(w_{fr} f_t + w_{gr} g_{t-1} + b_r) \tag{12c}$$

where $\otimes$ is the elementwise multiplication operator, and all w and b matrices are the learning parameters of GRU. The Dense layers map the input–output relationship using the following equation:

$$y = \mathrm{actv}(w_{\mathrm{dense}} * x + b_{\mathrm{dense}}) \tag{13}$$

where x and y are the input and output, respectively. w_{dense} and b_{dense} are the learning parameters of Dense layers, and actv is the activation function [43].

After feature extractor processes the current estimated system state, this attack detector first queries the feature history database for the extracted features in the past w sampling time instances. The $64Nw$ features are input into two layers of GRU, each of which has 1024 neurons, to investigate the temporal dependency of these w time instances. The result is fed into two fully-connected layers with 512 and 128 neurons, respectively. Both layers are activated by a sigmoid function. These two layers aim to interpret the temporal dependency generated by GRU into an index indicating whether an FDIA is detected in the studied time span. Finally, the index is considered as the output of the FDIA detector.

In this DNN design, hundreds of thousands of learning parameters needs fine-tuning in order to achieve a satisfactory FDIA detection accuracy. However, it has been demonstrated to be impractical to simultaneously optimize so many parameters without considerable overfitting problem, which may lead to poor performance on the accuracy with new data [44]. In the implementation, an effective technique, called "dropout," is employed to address this issue [44]. This technique randomly sets the output of neurons to zero with a predefined probability. The dropped-out neurons thus do not contribute to the calculation. This technique reduces the coadaptation relationship among neurons, so more robust features can be extracted in the learning process [45]. In the constructed DNN, dropout is applied to both of the fully-connected layers at a 30% dropout ratio.

D. Offline Training and Online Attack Detection

Before using the proposed FDIA detector to identify FDIAs, the optimal values for the network learning parameters, i.e., the values for the w and b matrices/vectors in (12) and (13), need to be first optimized. This parameter tuning process is called training, which aims to find the optimal learning parameter set that matches the input and output relationship presented in the training data [46]. The training data can include real attack system dynamics in the operating history. However, due to the relative scarcity of such real data, synthetic simulated power system dynamics subject to FDIA and normal events can be employed to enrich the training dataset for better detection performance. As illustrated in [15] and [34], constructing attack vectors for such systems are notably harder than in dc systems. So the adversaries are quite likely to follow existing patterns for attack, e.g., [15]. In such cases, using synthetic training data generated by these patterns can emulate the real-world attack characteristics, since both attack vectors are computed by algorithms instead of being measured. This data enrichment method is also employed in other FDIA research, e.g., [18]–[20], [24]–[27], [29].

To construct a complete training set, the desired output of the FDIA detector, i.e., y_t in Fig. 2, is set according to the following rule:

$$y_t = \begin{cases} 1, & \text{FDIA in the past } w \text{ time instances from } t \\ 0, & \text{otherwise} \end{cases}. \quad (14)$$

Given a collection of D training cases $\{\hat{\mathbf{x}}_{t,(i)}, y_{t,(i)}\}_{i=1}^{D}$, we employ the Adam optimizer [47] to find the optimal values of all learning parameters in the DNN-based attack detector. The binary cross entropy error function is employed as the training objective

$$\text{minimize } -\sum_{i=1}^{D}[y_{t,(i)} \log \hat{y}_{t,(i)} + (1 - y_{t,(i)}) \log(1 - \hat{y}_{t,(i)})] \quad (15)$$

where $\hat{y}_{t,(i)}$ is the actual FDIA detection result of $\hat{\mathbf{x}}_{t,(i)}$ with the proposed mechanism.

For online detection of FDIA, the previously trained learning parameters are utilized to establish the mathematical relationship between power system dynamics and attacks. With estimated power system states, it is trivial to calculate the corresponding $\hat{y}_t \in (0, 1)$ value. FDIA is detected if this value is greater than 0.5, and vice versa. As will be demonstrated in Section IV, the attack detecting process is fast enough to detect FDIA in an online manner.

IV. Case Studies

In this section, we assess the performance of the proposed ac FDIA detection mechanism on IEEE 118-bus and 300-bus power systems. Three sets of analyses are conducted. We first test the general ac FDIA detection accuracy and false-alarm rate of the proposed mechanism, and compare the results with those in the previous work. Next, we summarize the performance of the proposed mechanism on various groups of attacks with different statistical characteristics. Then, we investigate the impact of history window size w and system sampling interval Δ on the performance.

Data volume is critical to the performance of DNN [37]. While too few samples cannot include the characteristics of ac FDIA for learning, too many samples may potentially lead to overfitting problem. In this paper, 200 000 samples are employed to train the proposed DNN. These data are generated by time-domain simulation of power system dynamics, and the attack vectors are developed by the existing attack pattern introduced in Section II-C. In the simulation, we consider both the nominal and randomly selected $N-1$ power network topologies,[3] and the power network parameters are obtained from [48]. The initial load level is set to be a random value between 80% and 110% of the nominal value. As a result, 200 base operating conditions of each test system are recorded. We generate the power dynamics of normal load changing events and FDIAs based on these conditions. For each operating condition, we first generate 500 random load changing events. In each event, randomly selected loads in the system are changed to new values, ranging from 50% to 150% of their nominal loads. Consequently, the time-domain simulation for the power system dynamics of the 100 000 cases are conducted using DIgSILENT PowerFactory [49]. In addition, we follow the approach in [50] and [51] to

[3]Most power systems are designed to maintain at least $N-1$ reliability/stability, and it is quite possible that these systems operate on such topologies, e.g., in maintenance and construction tasks. Therefore, considering $N-1$ cases is appropriate in order to develop a generalized mechanism for ac FDIA detection.

generate random noise for the dynamics

$$\tilde{V}\angle\tilde{\theta} = V\angle\theta + \Delta V\angle\Delta\theta$$

where $V\angle\theta + \Delta$, $\Delta V\angle\Delta\theta$, and $\tilde{V}\angle\tilde{\theta}$ are the simulated voltage phasor, imposed noise phasor, and the resulting voltage phasor in the dataset, respectively. The noise phasor is generated from a truncated complex Gaussian distribution [50]

$$f(\Delta V\angle\Delta\theta|0,(10^{-2})^2) = \begin{cases} \frac{9}{\pi(1-e^{-9})(10^{-2})^2|V\angle\theta|^2}\exp(-\frac{9|\Delta V\angle\Delta\theta|^2}{(10^{-2})^2|V\angle\theta|^2}), \\ \qquad\qquad \text{if } |\Delta V\angle\Delta\theta| \le 10^{-2}|\Delta V\angle\Delta\theta| \\ 0, \qquad\qquad \text{otherwise} \end{cases}.$$

These phasors comply with the phasor measurement system (PMU) accuracy requirement by IEEE Standard for Synchrophasor Data Transfer for Power Systems [52], i.e., the total vector error is no more than 1%.

Besides the above 100 000 normal operational cases, we also construct another set of 100 000 FDIA cases with the 200 base operating conditions. For each operating condition, first, 100 attack cases are constructed with (5) to simulate FDIAs with complete system knowledge. Then, 400 other attack cases are constructed using the heuristic summarized in Section II-C, which was developed in [15]. These attack cases are distinguished by their different maximum allowed bus power injections (−50% to +50%), voltage magnitudes (−20% to +20%), angle difference (−15° to +15°), and line power flows (up to 1.5 times of the nominal value), whose values are randomly generated according to the record in [15]. Interested readers can refer to this literature for a more detailed introduction on the method to develop valid FDIA attack vectors for ac state estimation. Finally, the attack vector is injected into the power dynamics of the corresponding operating condition to construct an FDIA case.

For cross validation, the total 200 000 power dynamics test cases for each test system are randomly divided into a training set and a testing test by 3:1 ratio, which accords with the common practice [38]. The training set is used to train the learning parameters in the DNN, and the testing set is employed to assess the attack detection accuracy. All simulations are conducted on computers with an Intel Core i7-7700 CPU, an nVidia GTX 1080 GPU, and 32-GB RAM. The DNN is constructed using TensorFlow for computational speed boost [53].

A. FDIA Detection Performance

We first study the general FDIA detection performance of the proposed mechanism. In this test, we set the feature history window size $w = 5$, and the sampling interval $\Delta = 33.3$ ms to simulate a typical wide-area measurement system. Both test power systems are assessed, and the simulation results are shown in Table II.

From the simulation results, it can be observed that the proposed mechanism can develop a satisfactory ac FDIA detection accuracy. For both test systems, the detection accuracy is more than 90%, and the mechanism works slightly better on the 118-bus system due to its less complex topology. By comparing the detection results on testing and training cases, it can also be concluded that overfitting is insignificant in the trained DNN.

TABLE II
AC FDIA DETECTION PERFORMANCE OF THE PROPOSED MECHANISM

		118-bus system	300-bus system
Testing cases	Correct	45,901 (91.80%)	45,422 (90.84%)
	False positive	2291 (4.58%)	2531 (5.06%)
	False negative	1808 (3.62%)	2047 (4.09%)
Training cases	Correct	137,943 (91.96%)	136,539 (91.02%)
	False positive	6604 (4.40%)	7569 (5.05%)
	False negative	5360 (3.64%)	5892 (3.93%)
Average Detection Time		3.51 ms	7.17 ms
DNN Training Time		2713.2 s	2856.8 s

TABLE III
COMPARISON OF AC FDIA DETECTION PERFORMANCE WITH EXISTING AC AND DC FDIA DETECTION METHODS

Mechanism	118-bus system	300-bus system	Recorded
Proposed	91.80%	90.84%	-
[29, Table I]	-	-	88.56%
KLD [29]	72.05%	65.34%	-
Kalman Filter [18]	70.35%	68.15%	-
Sparse optimization [19]	81.68%	76.51%	-

In both test systems, the detection accuracy remains to be more than 90% with new unknown data not used in training. This result demonstrates the satisfactory generalization capability of the proposed mechanism. In addition, we also present the average detection and DNN training times for both the test systems. While the former represents the system overhead introduced by the proposed detection method, the latter can describe the complexity of the adopted DNN. From the simulation results, it is clear that the overhead is insignificant compared with either the sampling rate (30 Hz) or the system frequency (60 Hz). While the DNN training time is huge compared with others, this process is typically conducted offline.

For a complete comparison, we also present the simulation results of the other ac FDIA detection mechanism proposed in [29]. We summarize the data presented in [29, Table I], which is the FDIA detection accuracy on a small-scale IEEE 14-bus system. Since it is unfair to directly compare the results with ours on 118- and 300-bus systems, we also implement the Kullback–Leibler detector presented in [29] and test this mechanism on the same systems for reference. The comparison is presented in Table III. From the table, it can be observed that the proposed FDIA detection mechanism can remarkably outperform the previous work. The detection accuracy is improved from around 70% by [29] to more than 90%, and the proposed mechanism provides more robust performance when handling normal system operation events.

Furthermore, we also employ previously proposed dc FDIA detection mechanisms in the literature to protect the ac test systems for demonstration. Specifically, the methods proposed in [18] and [19] are implemented and tested with the same data. The detection accuracy is presented in Table III. It can be observed that dc FDIA detection mechanisms present mediocre fault detection accuracy values at around 70% to 80%. This is due to the fact that ac state estimation is generally more accurate than dc one due to line loss, rendering voltage deviations over transmission lines. This can lead to more difficult FDIA attack construction, but the constructed attack vectors are less perceptible, especially with dc FDIA mechanisms.

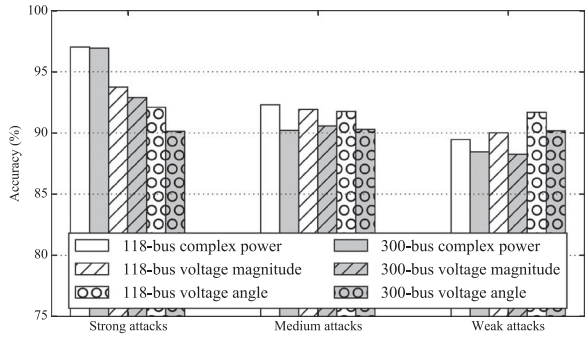


Fig. 3. Detection accuracy on FDIAs with different attack strengths.

B. Attacks With Different Statistical Characteristics

Besides the previous general accuracy analysis, we are also interested in how the proposed mechanism performs subject to FDIAs with different statistical characteristics. In this section, we further summarize the testing performance of the mechanism. We classify all generated FDIAs into three categories, namely strong, medium, and weak attacks according to the following rules.

1) Strong attacks: The average power injection deviation in $\mathbf{c}$ exceeds 30% of the nominal value in $\mathbf{x}$, or average voltage magnitude deviation exceeds 10% of the nominal value, or average voltage angle deviation exceeds 5°.
2) Weak attacks: The average deviation of these three system variables are smaller than 10%, 5%, and 2° of their nominal values, respectively.
3) Medium attacks: All other generated FDIAs.

These classes can represent the "strength" of attacks in terms of system variable deviations.

The detection accuracies of attacks with different statistical characteristics are depicted in Fig. 3. From the figure, we can conclude that generally it is easier to detect "stronger" attacks than those with minor system state deviations. This is because a larger sudden change in consecutive system states, which does not comply with the nature of system dynamics, is a significant indication of FDIA, and the proposed mechanism can successfully capture this feature. Furthermore, it can also be observed that the detection accuracy of the proposed mechanism is greatly influenced by the complex power injection deviation. The influence is not as significant for voltage magnitude deviation, and different angle deviations do not have an obvious impact on the detection performance. This is because normal power system operation events may also introduce frequent complex power injection changes, which increase the false positive detections by the mechanism. Despite the slightly degraded performance on weak attacks, our mechanism can still achieve a satisfactory detection accuracy (greater than 85% in worst case scenarios).

C. Impact of History Window Size and Sampling Interval

In previous simulations, we assume that the power system states are available at 30 Hz. While this configuration emulates the PMU-driven measurement systems, current utilities are still in the process of gradually introducing PMUs on top of the existing SCADA system [54], [55]. Hence, it is important to study the performance of the proposed mechanism when it is applied to power system with slower sampling rate, e.g., [54]. In addition, we set the feature history window size to five, and the window size sensitivity and its impact on the offline time needs further investigation.

In this section, we study the parameter sensitivities of Δ and w by testing the proposed mechanism with different parameter values. The value for w is selected from $\{2, 3, 5, 7\}$, and three scenarios with different sampling rates are tested. Specifically, Δ is selected from $\{33.3, 100, 500\}$ ms, which correspond to 30-Hz, 10-Hz, and 2-Hz system state sampling, respectively. The difference in the sampling rate leads to different numbers of system states in the same period of time, and thus, higher sampling rate can better preserve the system dynamics, or input data temporal correlation. We adopt the training and testing data generated for the 118-bus power system, and simulation results are presented in Table IV.

From the sensitivity result, it can be concluded that in general, five is a good candidate value for parameter w considering the FDIA detection accuracy when the measurements are developed by high-frequency wide-area monitoring system (WAMS). For smaller w values, the training process can be significantly shortened due to less computation required in back-propagating gradient deviations in Adam optimizer [47]. However, the less computationally expensive training also leads to inferior detection accuracies regardless of Δ. This is because reducing the feature history window size undermines the completeness of power system dynamics in the time domain, which is a critical factor of the proposed mechanism. On the other hand, while the attack detection accuracy for $w = 7$ is similar to that of $w = 5$, the drastically increased training time renders $w = 7$ less efficient. However, when the sampling interval increases, the more information brought by $w = 7$ can contribute to detection accuracy improvements and, is therefore, more preferred.

Comparing the performance with different Δ values, we can observe that the proposed mechanism can develop more accurate detection results with a higher system variable sampling frequency. The reason for this result is that the system variables sampled at a higher frequency can better represent the system dynamics, which is especially strong in transient and dynamic operations due to the inertia and momentum in the whole system. However, this correlation decays with time due to the mechanical momentum. Therefore, shorter time intervals show stronger correlation than longer ones, and the sampled system states at low rates are merely quasi-steady-state approximations of the grid. As previously analyzed, successful detection of FDIA of the proposed mechanism largely depends on the characteristics of system dynamics. Hence, it performs better in power systems with high sampling frequencies. Despite this, the proposed mechanism can still provide less than 10% false positive/negative detection with $\Delta = 500$ ms, which is still helpful in identifying FDIAs. Note that with the gradual and steady adoption of PMUs into conventional power grid monitoring systems, it can be expected that system measurements will be provided at a much higher frequency. The proposed mechanism can provide outstanding FDIA detection performance in these systems.

TABLE IV
SENSITIVITY TEST RESULTS OF Δ AND w ON IEEE 118-BUS SYSTEM

Value of Δ		33.3ms (30Hz Sampling)				100ms (10Hz Sampling)				500ms (2Hz Sampling)			
Value of w		2	3	5	7	2	3	5	7	2	3	5	7
Testing cases	Correct (%)	69.50	81.24	91.80	89.63	67.73	77.75	88.74	88.21	63.85	69.45	78.77	82.59
	False positive (%)	15.29	9.11	4.58	5.84	16.21	10.93	6.06	5.83	17.86	14.81	10.97	8.91
	False negative (%)	15.21	9.65	3.62	4.53	16.06	11.32	5.20	5.97	18.29	15.74	10.27	8.50
Training cases	Correct (%)	70.25	81.98	91.96	90.17	68.21	78.91	87.77	88.68	64.76	71.28	79.50	82.54
	False positive (%)	15.21	9.28	4.40	5.87	16.43	10.98	6.06	5.91	18.33	15.47	11.22	9.17
	False negative (%)	14.54	8.73	3.64	3.96	15.36	10.11	6.17	5.41	16.91	13.25	9.28	8.29
DNN Training time (s)		1463.8	1930.6	2713.2	3871.5	1507.3	1916.6	2688.3	3960.6	1485.7	1885.1	2701.0	3905.1

V. CONCLUSION

In this paper, we propose a new FDIA detection mechanism for ac state estimation. While much research has been conducted for attacks and detections in dc state estimation, little work has focused on the ac counterpart, which is widely adopted by power utilities. As FDIAs can construct compromised system states satisfying Kirchhoff's circuit laws, conventional residual-based methods have difficulties detecting such attacks. However, current FDIA methods focus on constructing attack vectors satisfying the spatial dependencies of system variables. The temporal dependency of consecutive system states is commonly ignored, which can actually provide more information for system operators to detect FDIAs. The proposed FDIA detector can learn from the system state dynamics in both the space and time domains. Utilizing the extracted time-series features, the detector is capable of distinguishing FDIAs from normal power system operating condition changes. In the proposed mechanism, we employ DWT to efficiently reveal the spatial data characteristics. Then, the temporal correlations are captured by a DNN, which then develops the FDIA detection result.

To assess the performance of our FDIA detection mechanism, we carry out a series of comprehensive simulations on IEEE 118-bus and 300-bus power systems. In both the systems, the proposed detector can achieve outstanding attack detection performance. In addition, our work can outperform the existing FDIA detectors with notable accuracy improvements. Furthermore, we conduct a parameter sensitivity test on two control parameters. The results reveal a tradeoff between the training time and detection accuracy, and suggest an appropriate set of these parameters for implementation.

Future research of this paper can be divided into two parts. On the one hand, the false positive and negative rates of the proposed mechanism may be reduced by improving the structure of DNN and incorporating more advanced DNN techniques. On the other hand, how to apply the proposed mechanism in detecting a wider range of cyber-security attacks is worth investigating.

REFERENCES

[1] 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.

[2] F. F. Wu, "Power system state estimation: A survey," *Int. J. Elect. Power Energy Syst.*, vol. 12, no. 2, pp. 80–87, Apr. 1990.

[3] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tut.*, vol. 15, no. 1, pp. 5–20, Jan.–Mar. 2013.

[4] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[5] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[6] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[7] 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.

[8] R. Deng *et al.*, "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.

[9] 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.

[10] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[11] Z. H. Yu and W. L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

[12] X. Liu *et al.*, "Modeling of local false data injection attacks with reduced network information," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015.

[13] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

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

[15] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[16] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 161–171, Dec. 2017.

[17] 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.

[18] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[19] 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.

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

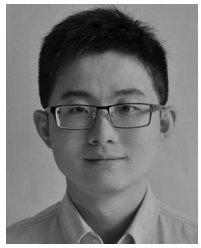
[21] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13787–13798, 2017.

[22] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.

[23] O. Beg, T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[24] 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.

[25] U. Adhikari, T. H. Morris, and S. Pan, "Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection," *IEEE Trans. Smart Grid*, to be published.
[26] 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.
[27] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.
[28] K. Khanna, B. K. Panigrahi, and A. Joshi, "AI-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Gener., Transmiss., Distrib.*, vol. 12, no. 5, pp. 1052–1066, 2018.
[29] 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.
[30] T. Liu *et al.*, "Abnormal traffic-indexed state estimation: A cyber-physical fusion approach for smart grid attack detection," *Future Gener. Comput. Syst.*, vol. 49, pp. 94–103, 2015.
[31] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Trans. Smart Grid*, to be published.
[32] A. G. Phadke, J. S. Thorp, and K. J. Karimi, "State estimation with phasor measurements," *IEEE Trans. Power Syst.*, vol. PWRS-1, no. 1, pp. 233–238, Feb. 1986.
[33] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.
[34] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.
[35] S. G. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11, no. 7, pp. 674–693, Jul. 1989.
[36] D. P. Mishra, S. R. Samantaray, and G. Joos, "A combined wavelet and data-mining based intelligent protection scheme for microgrid," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2295–2304, Sep. 2016.
[37] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.
[38] J. J. Q. Yu, D. J. Hill, A. Y. S. Lam, J. Gu, and V. O. K. Li, "Intelligent time-adaptive transient stability assessment system," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 1049–1058, Jan. 2018.
[39] E. Magosso, M. Ursino, A. Zaniboni, and E. Gardella, "A wavelet-based energetic approach for the analysis of biomedical signals: Application to the electroencephalogram and electro-oculogram," *Appl. Math. Comput.*, vol. 207, no. 1, pp. 42–62, Jan. 2009.
[40] D. Chen, S. Wan, and F. S. Bao, "Epileptic focus localization using discrete wavelet transform based on interictal intracranial EEG," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 25, no. 5, pp. 413–425, May 2017.
[41] J. J. Q. Yu, Y. Hou, A. Y. S. Lam, and V. O. K. Li, "Intelligent fault detection scheme for microgrids with wavelet-based deep neural networks," *IEEE Trans. Smart Grid*, to be published.
[42] K. Cho *et al.*, "Learning phrase representations using RNN encoder–decoder for statistical machine translation," in *Proc. Conf. Empirical Methods Natural Lang. Process.*, Doha, Qatar, Oct. 2014, pp. 1724–1734.
[43] R. Reed and R. J. Marks, II, *Neural Smithing: Supervised Learning in Feedforward Artificial Neural Networks*. Cambridge, MA, USA: MIT Press, Feb. 1999.
[44] G. E. Hinton *et al.*, "Improving neural networks by preventing co-adaptation of feature detectors," arXiv preprint arXiv:1207.0580, Jul. 2012.
[45] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2012, pp. 1097–1105.
[46] R. Lippmann, "An introduction to computing with neural nets," *IEEE ASSP Mag.*, vol. 4, no. 2, pp. 4–22, Apr. 1987.
[47] D. Kingma and J. Ba, "Adam: A method for stochastic optimization," in *Proc. 3rd Int. Conf. Learn. Represent.*, San Diego, Jul. 2015, pp. 1–15.
[48] A. Semerow *et al.*, "Dynamic study model for the interconnected power system of continental Europe in different simulation tools," in *Proc. IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–6.
[49] "PowerFactory—DIgSILENT Germany," 2017. [Online]. Available: http://www.digsilent.de/index.php/products-powerfactory.html
[50] M. He, V. Vittal, and J. Zhang, "Online dynamic security assessment with missing PMU measurements: A data mining approach," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1969–1977, May 2013.
[51] J. J. Q. Yu, A. Y. S. Lam, D. J. Hill, and V. O. K. Li , "Delay aware intelligent transient stability assessment system," *IEEE Access*, vol. 5, pp. 17 230–17 239, 2017.
[52] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*, IEEE Std. C37.118.2-2011, Dec. 2011.
[53] M. Abadi *et al.*, "TensorFlow: Large-scale machine learning on heterogeneous systems," Tech. Rep., 2015. [Online]. Available: tensorflow.org
[54] T. S. Bi, X. H. Qin, and Q. X. Yang, "A novel hybrid state estimator for including synchronized phasor measurements," *Elect. Power Syst. Res.*, vol. 78, no. 8, pp. 1343–1352, Aug. 2008.
[55] M. Göl and A. Abur, "LAV based robust state estimation for systems measured by PMUs," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1808–1814, Jul. 2014.



James J. Q. Yu (S'11–M'15) received the B.Eng. and Ph.D. degrees in electrical and electronic engineering from The University of Hong Kong, Hong Kong, in 2011 and 2015, respectively.

He is currently an honorary Assistant Professor and Postdoctoral Fellow with the Department of Electrical and Electronic Engineering, The University of Hong Kong. His research interests include smart city technologies, deep learning and big data industrial applications, and evolutionary computation.

Yunhe Hou (M'08–SM'15) received the B.E. and Ph.D. degrees in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1999 and 2005, respectively.

From 2005 to 2007, he was a Postdoctoral Research Fellow with Tsinghua University, Beijing, China, and a Postdoctoral Researcher with Iowa State University, Ames, IA, USA, and from 2008 to 2009, the University College Dublin, Dublin, Ireland. He was also a Visiting Scientist with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA, USA, in 2010. Since 2017, he has been a Guest Professor with the Huazhong University of Science and Technology. In 2009, he joined the faculty of The University of Hong Kong, Hong Kong, where he is currently an Associate Professor with the Department of Electrical and Electronic Engineering.

Dr. Hou is an Editor for the IEEE TRANSACTIONS ON SMART GRID and the *Journal of Modern Power Systems and Clean Energy*.

Victor O. K. Li (S'80–M'81–F'92) received the SB, SM, EE, and ScD degrees in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1977, 1979, 1980, and 1981, respectively.

He is currently the Chair Professor in information engineering and the Head of the Department of Electrical and Electronic Engineering, The University of Hong Kong (HKU), Hong Kong. He has also served as the Associate Dean of Engineering and the Managing Director of Versitech, Ltd., the technology transfer and commercial arm of HKU. He served on the Board of China.com, Ltd., and is currently serving on the Board of Sunevision Holdings, Ltd., listed on the Hong Kong Stock Exchange. Previously, he was a Professor in Electrical engineering with the University of Southern California, Los Angeles, CA, USA, and the Director of the USC Communication Sciences Institute. Sought by government, industry, and academic organizations, he has lectured and consulted extensively around the world.

Prof. Li was the recipient of numerous awards, including the PRC Ministry of Education Changjiang Chair Professorship at Tsinghua University, the UK Royal Academy of Engineering Senior Visiting Fellowship in Communications, the Croucher Foundation Senior Research Fellowship, and the Order of the Bronze Bauhinia Star, Government of the Hong Kong. He is a registered Professional Engineer and a Fellow of the IAE and the HKIE.