Cyber-attack Detection Strategy Based on Distribution System State Estimation

Huan Long, *Member*, *IEEE*, Zhi Wu, *Member*, *IEEE*, Chen Fang, Wei Gu, *Senior Member*, *IEEE*, Xinchi Wei, and Huiyu Zhan

***Abstract*—Cyber-attacks that tamper with measurement information threaten the security of state estimation for the current distribution system. This paper proposes a cyber-attack detection strategy based on distribution system state estimation (DSSE). The uncertainty of the distribution network is represented by the interval of each state variable. A three-phase interval DSSE model is proposed to construct the interval of each state variable. An improved iterative algorithm (IIA) is developed to solve the interval DSSE model and to obtain the lower and upper bounds of the interval. A cyber-attack is detected when the value of the state variable estimated by the traditional DSSE is out of the corresponding interval determined by the interval DSSE. To validate the proposed cyber-attack detection strategy, the basic principle of the cyber-attack is studied, and its general model is formulated. The proposed cyber-attack model and detection strategy are conducted on the IEEE 33-bus and 123-bus systems. Comparative experiments of the proposed IIA, Monte Carlo simulation algorithm, and interval Gauss elimination algorithm prove the validation of the proposed method.**

***Index Terms*—Cyber-attack detection, distribution network, interval state estimation, distribution system state estimation, cyber-attack model.**

I. Introduction

SMART grid technology is widely developing by combining traditional power systems with measurement and information technology. With the bidirectional flow and efficient utilization of data and information in power systems, severe security incidents caused by cyber-attack occur frequently. In 2015, many regional power grids in Ukraine suffered large-scale blackouts due to cyber-attacks [1]. In 2016, Israel Electric Power Company forced a large number of computers running offline due to a cyber-attack [2]. In 2019, Venezuela's power system suffered a series of cyber-attacks, and more than two-thirds of its territory suffered blackouts. All these incidents indicate that cyber-attacks threaten the security of power system operation.

Based on an analysis of the current cyber-attacks on power systems, cyber-attacks can be divided into three types: physical, communication, and information attacks. Physical attacks use viruses to attack physical devices, such as computers and measurement devices. Communication attacks take the communication protocols as the attack objective. Information attacks tamper with control system commands via false data-injection attacks (FDIAs).

Based on the characteristics of different cyber-attack types, the corresponding cyber-attack defense strategies are proposed: ① physical security: applying appropriate protection for measurement devices or replacing them with more accurate phase measurement units [3]; ② communication security: using various cryptography technologies to prevent cyber-attacks [4]; ③ information security: utilizing state estimation to track the actual power system under various malicious cyber-attacks [5], [6]. This paper focuses on the information cyber-attack defense strategy based on state estimation.

Under an information attack, bad data are injected into the supervisory control and data-acquisition (SCADA) system, which affects the regular operation of the power system. The traditional bad data detection and identification (BDDI) algorithm can effectively detect simple FIDAs. If the attacker obtains the power system topology, an FIDA based on the state estimation can elude the BDDI and increase the successful attack rate [6]-[10]. In [8], a cyber-attack was implemented to falsify the voltage measurement in the distribution system connected with photovoltaic systems. In [9], an FIDA model with incomplete information of the system network was proposed. In [7]-[9], an FIDA model against state estimation of a linear power system was proposed. Considering the nonlinearity of the distribution network, the nonlinear state estimation equations were relaxed and a single-phase FIDA model assuming a small variation in the voltage phase angle was established [10]. However, the typical characteristic of the distribution network is the three-phase unbalancing and coupling caused by the asymmetrical loads and line parameters. To improve the successful attack rate, the nonlinearity and three-phase unbalancing of distribution network limits should be considered in FIDA modeling.

Manuscript received: February 8, 2020; accepted: May 9, 2020. Date of CrossCheck: May 9, 2020. Date of online publication: June 29, 2020.

This work was supported in part by the National Key Research and Development Program of China (No. 2017YFB0902900) and the State Grid Corporation of China.

H. Long, Z. Wu (corresponding author), and W. Gu are with the School of Electrical Engineering, Southeast University, Nanjing, China (e-mail: hlong@seu.edu.cn; zwu@seu.edu.cn; wgu@seu.edu.cn).

C. Fang and X. Wei are with State Grid Shanghai Electric Power Company, Electric Power Research Institute, Shanghai, China (e-mail: chenfang_shh@163.com; newlate@126.com).

H. Zhan is with China Electric Power Research Institute, Beijing, China (e-mail: zhanhy@epri.sgcc.com.cn).

DOI: 10.35833/MPCE.2019.000216

The current research on FIDA-based detection strategies is divided into state-estimation-based, trace-prediction-based, and artificial-intelligence-based strategies. ① The state-estimation-based detection strategy improves the traditional state estimation algorithm to identify false data, including residual detection [11], mutation detection [12], and correlation detection [13]. ② The trace-prediction-based detection strategy [14], [15] detects false data by comparing the predicted and actual measurements. In [15], a statistics-based measurement consistency test method to determine the consistency between the predicted and actual measurements was proposed. ③ The artificial-intelligence-based detection strategy utilizes artificial intelligence algorithms such as deep learning [16] and clustering algorithms [17] to detect false data directly. However, the trace-prediction-based and artificial-intelligence-based strategies require large historical data and high computation costs, which are not suitable for complex distribution networks.

As the distribution network shows stochastic uncertainty, the cyber-attack detection performance is affected based on the traditional state estimation algorithm. To deal with the uncertainty of the distribution network, the current derivative of the main uncertain distribution system state estimation (DSSE) algorithm includes Monte Carlo (MC) simulation [18], stochastic state estimation [19], [20], fuzzy state estimation [21], [22], and interval estimation [23]. The MC simulation and stochastic state estimation use distributions to describe the uncertainty. The fuzzy state estimation method utilizes fuzzy numbers to represent the uncertainty, and the interval estimation uses the interval to qualify the uncertainty. The MC simulation obtains the probability distribution of uncertain variables through a large number of repeated random sampling experiments [18]. In [20], a probabilistic model was used to deal with random information. In [22], a distribution network state estimation model with fuzzy numbers was established, which handled uncertain information with fuzzy membership functions. In [23], the upper and lower bounds were used to represent the uncertain information to calculate the possible range of system state.

However, except for interval estimation, the other three uncertain DSSE algorithms require the assumption of the distribution or fuzzy function. Thus, the interval estimation is utilized in this paper for combination with DSSE. Compared with traditional state estimation, the calculation of the uncertain state estimation based on interval DSSE is usually complex, which affects its convergence and rapidity. It is important to accurately formulate a reasonable interval DSSE mathematical model and propose a fast solving algorithm. Therefore, a cyber-attack detection strategy based on the interval DSSE method is proposed to deal with the above-mentioned challenges. The main contributions of this paper can be summarized as follows:

1) Aiming at the three-phase unbalancing and uncertainty problems in the distribution network, a three-phase interval state estimation model based on equivalent current measurements is proposed.

2) An improved iterative algorithm (IIA) based on the Krawczyk operator is proposed to solve the interval, DSSE model effectively and to obtain the interval of each state variable.

3) A general FDIA model is formulated based on the three-phase DSSE model.

4) A cyber-attack detection strategy based on interval DSSE is proposed and applied to realize real-time monitoring and warning of cyber-attacks in the distribution network.

The remainder of the paper is organized as follows. Section II introduces the interval DSSE model and the corresponding solution algorithm. Section III introduces the general cyber-attack model. Section IV shows the details of cyber-attack strategy based on interval DSSE. Section V presents the numerical experiments tested on the IEEE 33-bus and 123-bus systems. Section VI draws the conclusions and provides the direction for future work.

II. Interval DSSE Model

In this section, the traditional three-phase linear DSSE model is firstly introduced. Then, the proposed interval DSSE model combining the interval estimation with three-phase linear DSSE is displayed. Finally, the interval DSSE model solved by the IIA is presented.

A. Traditional Three-phase Linear DSSE Model

Currently, the three-phase measurement data of distribution network mainly include [24]: ① the current complex phasor $I_{ij,mea}$ of branch *i*-*j*; ② the power complex phasor $S_{ij,mea}$ of branch *i*-*j*; ③ the injected power complex phasor $S_{i,mea}$ of bus *i*; ④ the voltage complex phasor $V_{i,mea}$; ⑤ the voltage amplitude $|V_{i,mea}|$ of bus *i*.

$|V_{i,mea}|$ can be converted to the equivalent voltage complex phasor $V_{i,equ}$ according to the phase-angle measurement of the adjacent bus. $S_{ij,mea}$ and $S_{i,mea}$ can be converted to the equivalent current complex phasors $I_{ij,equ}$ and $I_{i,equ}$ according to (1) and (2), respectively.

$$I_{ij,equ}=\left(\frac{S_{ij,mea}}{V_{i,mea}}\right)^{*} \tag{1}$$

$$I_{i,equ}=\left(\frac{S_{i,mea}}{V_{i,mea}}\right)^{*} \tag{2}$$

The measurement equations of $I_{ij,mea}$, $I_{ij,equ}$, and $I_{i,equ}$ are expressed as (3) and (4) in [25], [26].

$$\begin{bmatrix} I_{ij,re} \\ I_{ij,im} \end{bmatrix}=\boldsymbol{Y}_{ij}\begin{bmatrix} V_{i,re}-V_{j,re} \\ V_{i,im}-V_{j,im} \end{bmatrix} \tag{3}$$

$$\begin{bmatrix} I_{i,re} \\ I_{i,im} \end{bmatrix}=\boldsymbol{Y}_{i}\begin{bmatrix} V_{i1} \\ V_{i2} \\ \vdots \\ V_{iN} \end{bmatrix} \tag{4}$$

where $I_{ij}=I_{ij,re}+\mathrm{j}I_{ij,im}$ is the three-phase current complex phasor of branch *i*-*j*; $I_i=I_{i,re}+\mathrm{j}I_{i,im}$ is the three-phase current complex phasor of bus *i*; $V_i=V_{i,re}+\mathrm{j}V_{i,im}$ is the three-phase voltage complex phasor of branch *i*-*j*; $\boldsymbol{Y}_{ij}$ and $\boldsymbol{Y}_i$ are the matrices of the branch mutual admittance and bus self-admittance, respectively, which are the constant measurement function matrices; and $[V_{i1}, V_{i2}, \ldots, V_{iN}]^{\mathrm{T}}$ is the voltage drop of *N*

branches connected to bus *i*.

The three-phase measurements of $\boldsymbol{V}_{i,mea}$ and $\boldsymbol{V}_{i,equ}$ are expressed as (5), where $\boldsymbol{U}$ is the identity matrix.

$$\begin{cases} \begin{bmatrix} V_{i,equ}^{a} \\ V_{i,equ}^{b} \\ V_{i,equ}^{c} \end{bmatrix} = \boldsymbol{U} \begin{bmatrix} V_{i}^{a} \\ V_{i}^{b} \\ V_{i}^{c} \end{bmatrix} \\ \begin{bmatrix} V_{i,mea}^{a} \\ V_{i,mea}^{b} \\ V_{i,mea}^{c} \end{bmatrix} = \boldsymbol{U} \begin{bmatrix} V_{i}^{a} \\ V_{i}^{b} \\ V_{i}^{c} \end{bmatrix} \end{cases} \tag{5}$$

Thus, the three-phase linear DSSE model is expressed as (6), where $\boldsymbol{x}$ is the vector set of state variables which represents the complex bus voltage. The three-phase linear DSSE can be further simplified as (7).

$$\begin{bmatrix} \boldsymbol{V}_{i,equ} \\ \boldsymbol{V}_{i,mea} \\ \boldsymbol{I}_{i,equ} \\ \boldsymbol{I}_{ij,mea} \\ \boldsymbol{I}_{ij,equ} \end{bmatrix} = \begin{bmatrix} \boldsymbol{U} \\ \boldsymbol{U} \\ \boldsymbol{Y}_{i} \\ \boldsymbol{Y}_{ij} \\ \boldsymbol{Y}_{ij} \end{bmatrix} \boldsymbol{x} + \boldsymbol{v} \tag{6}$$

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{v} \tag{7}$$

where $\boldsymbol{z}$ and $\boldsymbol{H}$ are the measurement vector and the measurement coefficient matrix, respectively; and $\boldsymbol{v}$ is the vector of measurement error set, which follows normal distribution.

B. Three-phase Interval DSSE Model

In the interval model, the uncertainty of parameters and measurements is described as the upper and lower limits [27], as shown in (8).

$$[x]=[\underline{x},\bar{x}]=\{x \in \mathbf{R} | \underline{x} \le x \le \bar{x}\} \tag{8}$$

where $\underline{x}$ and $\bar{x}$ are the lower and upper bounds of interval $[x]$, respectively.

Considering the uncertainty of the parameters and measurement data of distribution network, all variables are expressed in the interval form. Each part of the linear DSSE model is transformed into the interval form expressed by (9)-(11).

$$[\boldsymbol{z}]=\begin{bmatrix} [\boldsymbol{V}_{i,equ}] \\ [\boldsymbol{V}_{i,mea}] \\ [\boldsymbol{I}_{i,equ}] \\ [\boldsymbol{I}_{ij,mea}] \\ [\boldsymbol{I}_{ij,equ}] \end{bmatrix} = \begin{bmatrix} [z_1] \\ [z_2] \\ \vdots \\ [z_N] \end{bmatrix} = \{z \in \mathbf{R}^{N\times 1} : \underline{z}_n \le z_n \le \bar{z}_n, n=1,2,...,N\} \tag{9}$$

$$[\boldsymbol{H}]=\begin{bmatrix} [\boldsymbol{U}] \\ [\boldsymbol{U}] \\ [\boldsymbol{Y}_i] \\ [\boldsymbol{Y}_{ij}] \\ [\boldsymbol{Y}_{ij}] \end{bmatrix} = \begin{bmatrix} [\boldsymbol{H}_{1,1}] & [\boldsymbol{H}_{1,2}] & \cdots & [\boldsymbol{H}_{1,M}] \\ [\boldsymbol{H}_{2,1}] & [\boldsymbol{H}_{2,2}] & \cdots & [\boldsymbol{H}_{2,M}] \\ \vdots & \vdots & & \vdots \\ [\boldsymbol{H}_{N,1}] & [\boldsymbol{H}_{N,2}] & \cdots & [\boldsymbol{H}_{N,M}] \end{bmatrix} = \{\boldsymbol{H} \in \mathbf{R}^{N\times M}:$$

$$\underline{\boldsymbol{H}}_{n,m} \le \boldsymbol{H}_{n,m} \le \overline{\boldsymbol{H}}_{n,m}, n=1,2,...,N, m=1,2,...,M\} \tag{10}$$

$$[\boldsymbol{x}]=\{\boldsymbol{x} \in \mathbf{R}^{M\times 1} : \boldsymbol{H}\boldsymbol{x} \in [\boldsymbol{z}]\} \tag{11}$$

where $[\boldsymbol{x}]$, $[\boldsymbol{z}]$, and $[\boldsymbol{H}]$ are the state vector, measurement vector, and measurement coefficient matrix in interval form, respectively; and $\boldsymbol{H}_{n,m}$ is each element of the measurement coefficient matrix $[\boldsymbol{H}]$.

Equation (9) is the expression of the measurement vector in the interval DSSE model, including the node voltage and branch current. Equation (10) is the expression of the measurement coefficient matrix related to network parameters. Equation (11) represents the real and imaginary parts of the node voltage, which are taken as the state variables in the interval model.

The whole interval DSSE model can be defined as:

$$[\boldsymbol{H}][\boldsymbol{x}]=[\boldsymbol{z}] \tag{12}$$

Since the dimension of the measurements is larger than that of the system state variables, the proposed model (12) is the problem of an interval over-determined equation. It is difficult to establish a unified analytical expression and standard analysis method. To solve model (12), the over-determined equation is converted into a linear one as:

$$\begin{bmatrix} [\boldsymbol{H}] & -\boldsymbol{1} \\ \boldsymbol{0} & [\boldsymbol{H}]^{\mathrm{T}}\boldsymbol{W}^{-1} \end{bmatrix} \begin{bmatrix} [\boldsymbol{x}] \\ \boldsymbol{0} \end{bmatrix} = \begin{bmatrix} [\boldsymbol{z}] \\ \boldsymbol{0} \end{bmatrix} \tag{13}$$

Equation (13) is further simplified to (14) which is a linear equation with an interval element:

$$[\boldsymbol{A}][\boldsymbol{x}]=[\boldsymbol{b}] \tag{14}$$

where $[\boldsymbol{A}]$ is a square matrix of size $(N+2M-1)\times(N+2M-1)$; and $[\boldsymbol{x}]$ and $[\boldsymbol{b}]$ are both vectors with $(N+2M-1)$ dimensions.

C. Improved Interval Iterative Algorithm

The width of the interval obtained through the interval DSSE directly affects the detection of cyber-attacks. If the interval is too narrow, a false alarm may occur due to the uncertainty of the distribution network. Otherwise, the cyber-attack may not be detected. To achieve a suitable interval quickly, an improved interval iterative algorithm based on the Krawczyk operator is proposed in this paper. Based on (14), the detailed process of solving the interval DSSE can be summarized as follows:

1) Select any $\boldsymbol{A} \in [\boldsymbol{A}]$ and $\boldsymbol{b} \in [\boldsymbol{b}]$, where $\boldsymbol{A}^{-1}\boldsymbol{b} \in [\boldsymbol{x}]$ according to (14).

2) A specific $\boldsymbol{C} \in \mathbf{R}^{(N+2M-1)\times(N+2M-1)}$ can be found in (15) and (16), which is the inverse of the midpoint matrix of $[\boldsymbol{A}]$, so that $\boldsymbol{A}^{-1}\boldsymbol{b}$ can be further expanded into (17).

$$\boldsymbol{C}=(Mid([\boldsymbol{A}]))^{-1} \tag{15}$$

$$Mid([\boldsymbol{A}])= \begin{bmatrix} Mid([a_{1,1}]) & Mid([a_{1,2}]) & \cdots & Mid([a_{1,N+2M-1}]) \\ Mid([a_{2,1}]) & Mid([a_{2,2}]) & \cdots & Mid([a_{2,N+2M-1}]) \\ \vdots & \vdots & & \vdots \\ Mid([a_{N+2M-1,1}]) & Mid([a_{N+2M-1,2}]) & \cdots & Mid([a_{N+2M-1,N+2M-1}]) \end{bmatrix} \tag{16}$$

$$\boldsymbol{A}^{-1}\boldsymbol{b}=\boldsymbol{C}\boldsymbol{b}-(\boldsymbol{C}\boldsymbol{A}-\boldsymbol{I})\boldsymbol{A}^{-1}\boldsymbol{b} \tag{17}$$

where $Mid(\cdot)$ is the median function of interval numbers; and $\boldsymbol{I}$ is an $(N+2M-1)\times(N+2M-1)$ unit matrix.

3) When (17) satisfies $\boldsymbol{A}^{-1}\boldsymbol{b}=\boldsymbol{C}\boldsymbol{b}-(\boldsymbol{C}\boldsymbol{A}-\boldsymbol{I})\boldsymbol{A}^{-1}\boldsymbol{b} \in \boldsymbol{C}[\boldsymbol{b}]-$

$(\boldsymbol{C}[\boldsymbol{A}]-\boldsymbol{I})[\boldsymbol{x}]$, the Krawczyk operator $\boldsymbol{K}_{operator}$ can be used to obtain the approximate solution set as (18).

$$\begin{cases}\boldsymbol{K}_{operator}=\boldsymbol{C}[\boldsymbol{b}]-(\boldsymbol{C}[\boldsymbol{A}]-\boldsymbol{I})[\boldsymbol{x}^k] \\ [\boldsymbol{x}^{k+1}]=\boldsymbol{K}_{operator}\cap[\boldsymbol{x}^k]\end{cases} \tag{18}$$

where $[\boldsymbol{x}^k]$ is the solution of the k^{th} iteration.

Substituting (13) into (18), the iterative equation (18) can be expressed as:

$$[\boldsymbol{x}^{k+1}]=\left(\boldsymbol{C}\begin{bmatrix}[\boldsymbol{z}]\\ \boldsymbol{0}\end{bmatrix}-\left(\boldsymbol{C}\begin{bmatrix}[\boldsymbol{H}] & -\boldsymbol{1}\\ \boldsymbol{0} & [\boldsymbol{H}]^{\mathrm{T}}\boldsymbol{W}^{-1}\end{bmatrix}-\boldsymbol{I}\right)[\boldsymbol{x}^k]\right)\cap[\boldsymbol{x}^k] \tag{19}$$

According to [28], $\boldsymbol{K}_{operator}$ at the k^{th} iteration is a set containing all feasible solutions, and the interval width is always less than that of $[\boldsymbol{x}^{k-1}]$. Therefore, with the iteration of (19), the interval width of the solution set $[\boldsymbol{x}]$ decreases and gradually approaches the solution set.

4) When the amplitude of the infinite norm of the interval solution vector $[\boldsymbol{x}^k]$ decreases to the convergence criterion, the iteration is stopped when (20) is satisfied.

$$\sum_{i=1}^{n}||Wid([\boldsymbol{x}^k])||-\sum_{i=1}^{n}||Wid([\boldsymbol{x}^{k+1}])||<\varepsilon \tag{20}$$

where $||Wid([\boldsymbol{x}^k])||$ is the interval width of $[\boldsymbol{x}^k]$; and ε is a given small positive number which is usually taken as 10^{-6}.

III. General Cyber-attack Model

In this section, the basic principle of FDIA is introduced. Then, the general FDIA model is formulated based on the three-phase linear DSSE model.

A. Basic Principle of False Data-injection Attack

For a given network connection, branch parameters, and measurement data, denote $\boldsymbol{z}_{mea}$ as the vector of all the measurements. The relationship between $\boldsymbol{z}_{mea}$ and $\boldsymbol{x}$ is expressed by a vector of nonlinear measurement functions $\boldsymbol{h}(\boldsymbol{x})$ in (21), which is called a nonlinear DSSE model.

$$\boldsymbol{z}_{mea}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{v} \tag{21}$$

To inject false data into the system, it is reasonable to make the following assumptions:

1) The attacker knows the complete system information.

2) Any form of nonlinear DSSE model can be transformed into the linear DSSE model proposed in Section II.

3) All the original measurement data $\boldsymbol{z}_{mea}$ can be transformed into the equivalent measurement data $\boldsymbol{z}_{equ}$ in the linear DSSE model by the attacker.

In the linear three-phase DSSE model, a closed-form solution of model (7) is derived in (22).

$$\hat{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{z}_{mea} \tag{22}$$

where $\hat{\boldsymbol{x}}$ is the state computed by traditional linear DSSE; and $\boldsymbol{R}$ is the variance matrix of measurement error with the size of $N\times N$. Based on the equivalent data, model (7) can be expressed as:

$$\boldsymbol{z}_{equ}=\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{v} \tag{23}$$

By introducing a false data-injection attack vector $\boldsymbol{a}$, the linear three-phase DSSE model after the cyber-attack can be expressed as:

$$\boldsymbol{z}_{equ}+\boldsymbol{a}=\boldsymbol{H}\hat{\boldsymbol{x}}_a+\boldsymbol{v} \tag{24}$$

where $\hat{\boldsymbol{x}}_a$ is the estimated state by the linear DSSE model after the cyber-attack.

It is noteworthy that the measurement coefficient matrix $\boldsymbol{H}$ in the linear DSSE model is different from the measurement function $\boldsymbol{h}(\cdot)$ in the original nonlinear DSSE. Therefore, after the false data-injection attack, the relationship between measurements and estimated states is unequal, expressed by (25).

$$\boldsymbol{z}_{mea}+\boldsymbol{a}\neq\boldsymbol{h}(\hat{\boldsymbol{x}}_a)+\boldsymbol{v} \tag{25}$$

To guarantee the solution $\hat{\boldsymbol{x}}_a$ is the same as the solution of the original nonlinear DSSE model, it is necessary to find a constant vector $\Delta\boldsymbol{z}$ to satisfy (26), and the original measurement data are tampered with $\boldsymbol{z}_{mea}+\Delta\boldsymbol{z}$.

$$\boldsymbol{z}_{mea}+\Delta\boldsymbol{z}=\boldsymbol{h}(\hat{\boldsymbol{x}}_a)+\boldsymbol{v} \tag{26}$$

Currently, bad data detection is generally based on the maximum normalized residual (MNR). Thus, if $\boldsymbol{a}$ can successfully pass through the detection of the MNR, $\Delta\boldsymbol{z}$ is the general form of the vector of FDIA of the original distribution network. In this way, the cyber-attack can be implied to different distribution network state estimation algorithms.

B. General FDIA Model Based on Linear DSSE Model

In linear DSSE model, the residual in (24) is given as (27) after $\boldsymbol{a}$ is injected.

$$\begin{aligned}\boldsymbol{v}_a=\boldsymbol{z}_a-\boldsymbol{H}\hat{\boldsymbol{x}}_a=\boldsymbol{z}_{equ}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{a})= \\ \boldsymbol{z}_{equ}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{a}-\boldsymbol{H}(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{a}\end{aligned} \tag{27}$$

Let $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{d}$, where $\boldsymbol{d}$ is any arbitrary constant vector. The residual can be rewritten as:

$$\begin{aligned}\boldsymbol{v}_a=\boldsymbol{z}_{equ}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{H}\boldsymbol{d}-\boldsymbol{H}(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{H})\boldsymbol{d}= \\ \boldsymbol{z}_{equ}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{H}\boldsymbol{d}-\boldsymbol{H}\boldsymbol{d}=\boldsymbol{z}_{equ}-\boldsymbol{H}\hat{\boldsymbol{x}}=\boldsymbol{v}\end{aligned} \tag{28}$$

It can be seen that the residual after the cyber-attack is the same as that before the attack. Therefore, if the residual $\boldsymbol{v}$ before the attack can pass the MNR test, the residual $\boldsymbol{v}_a$ after the attack can also successfully pass the MNR test.

IV. Cyber-attack Detection Strategy Based on Interval DSSE Model

A. Cyber-attack Vector in Linear Three-phase DSSE Model

In the linear three-phase DSSE model (6), the increments of the original voltage measurement $V_{i,mea}$ and the current measurement $I_{ij,mea}$ after the cyber-attack are $\Delta V_{i,mea}$ and $\Delta I_{ij,mea}$, respectively, as expressed by (29) and (30).

$$\Delta V_{i,mea}=a_{V_{i,equ}} \tag{29}$$

$$\Delta I_{ij,mea}=a_{I_{ij,equ}} \tag{30}$$

where $a_{V_{i,mea}}$ and $a_{I_{ij,mea}}$ are the false data injected in the equivalent voltage and current measurements, respectively.

The increments of the original power measurements $S_{ij,mea}$ and $S_{i,mea}$ under the cyber-attack are ΔP and ΔQ satisfying:

$$\left(\frac{P+\mathrm{j}Q+\Delta P+\mathrm{j}\Delta Q}{V_{a,re}+\mathrm{j}V_{a,im}}\right)^{*}=(I_{equ,re}+\mathrm{j}I_{equ,im})+(a_{I_{equ,re}}+\mathrm{j}a_{I_{equ,im}})\Rightarrow$$
$$\frac{[(P+\Delta P)V_{a,re}+(Q+\Delta Q)V_{a,im}]+\mathrm{j}[(P+\Delta P)V_{a,im}-(Q+\Delta Q)V_{a,re}]}{V_{a,re}^2+V_{a,im}^2}=$$
$$(I_{equ,re}+a_{I_{equ,re}})+\mathrm{j}(I_{equ,im}+a_{I_{equ,im}}) \tag{31}$$

where $V_{a,re}$ and $V_{a,im}$ are the real and imaginary parts of the bus voltage state after the attack, respectively; $I_{equ,re}$ and $I_{equ,im}$ are the real and imaginary parts of the equivalent current measurement before the attack, respectively; and $a_{I_{equ,re}}$ and $a_{I_{equ,im}}$ are the real and imaginary parts of the false data injected in the equivalent current measurement, respectively.

Considering that the amplitude of bus voltage in the distribution network is close to 1 p. u., the real and imaginary parts of (31) can be simplified as:

$$(P+\Delta P)V_{a,re}+(Q+\Delta Q)V_{a,im}\approx I_{equ,re}+a_{I_{equ,re}} \tag{32}$$

$$(P+\Delta P)V_{a,im}-(Q+\Delta Q)V_{a,re}\approx I_{equ,im}+a_{I_{equ,im}} \tag{33}$$

The increment of the real and imaginary parts of the bus voltage state after the cyber-attack are denoted as ΔV_{im} and ΔV_{re}, respectively. Thus, $V_{a,re}=V_{re}+\Delta V_{re}$ and $V_{a,im}=V_{im}+\Delta V_{im}$. Considering $PV_{re}+QV_{im}\approx I_{equ,re}$ and $PV_{im}-QV_{re}\approx I_{equ,im}$, (32) and (33) are further simplified as:

$$\begin{cases}P\Delta V_{re}+\Delta PV_{re}+\Delta P\Delta V_{re}+Q\Delta V_{im}+\Delta QV_{im}+\Delta Q\Delta V_{im}\approx a_{I_{equ,re}}\\ P\Delta V_{im}+\Delta PV_{im}+\Delta P\Delta V_{im}-Q\Delta V_{re}-\Delta QV_{re}+\Delta Q\Delta V_{re}\approx a_{I_{equ,im}}\end{cases} \tag{34}$$

By solving (34), ΔP and ΔQ can be obtained as:

$$\begin{cases}\Delta P=\dfrac{e(V_{re}+\Delta V_{re})+f(V_{im}+\Delta V_{im})}{(V_{re}+\Delta V_{re})^2+(V_{im}+\Delta V_{im})^2}\\ \Delta Q=\dfrac{e(V_{im}+\Delta V_{im})-f(V_{re}+\Delta V_{re})}{(V_{re}+\Delta V_{re})^2+(V_{im}+\Delta V_{im})^2}\end{cases} \tag{35}$$

where $e=a_{I_{equ,re}}-(P\Delta V_{re}+Q\Delta V_{im})$; and $f=a_{I_{equ,im}}-(P\Delta V_{im}+Q\Delta V_{re})$.

It is obvious that the attacker can successfully attack the distribution network only by obtaining the information of V_{re}, V_{im}, P and Q at the corresponding buses.

B. Detection Strategy Based on Interval DSSE

According to the principle that the system state of the distribution network cannot change abruptly, the bus state estimated by DSSE fluctuates up and down slightly. Once the attacker successfully initiates a cyber-attack by injecting malicious false measurement data, the estimated value of the estimated bus state changes greatly. Thus, a cyber-attack detection strategy is proposed based on interval DSSE.

Interval DSSE estimates the lower and upper boundaries of the bus state, which is regarded as the predetermined threshold. When the bus state calculated by traditional DSSE does not fall into the interval, an alarm should be issued to warn the system.

Based on the above analysis, the cyber-attack detection model is formulated based on the indicator function as (36).

$$\begin{cases}\gamma=\sum_{m=1}^{M}1_{\left[\underline{x}_m,\bar{x}_m\right]}\hat{x}_m\\ \text{s.t. } \boldsymbol{z}=\boldsymbol{H}\hat{\boldsymbol{x}}\\ \quad [\boldsymbol{z}]=[\boldsymbol{H}][\boldsymbol{x}]\\ \quad [\underline{\boldsymbol{x}},\bar{\boldsymbol{x}}]=[\boldsymbol{x}]\end{cases} \tag{36}$$

where $\hat{x}_m$ is the m^{th} state estimated by the linear DSSE model; $[\underline{x},\bar{x}]$ is the corresponding predetermined boundary computed by interval DSSE; and $1_{\left[\underline{x}_m,\bar{x}_m\right]}$ is the indictor function, which equals to 1 when $\hat{x}_m\in[\underline{x}_m,\bar{x}_m]$, otherwise 0.

If $\gamma=0$, the distribution network has never been attacked. If $\gamma\neq 0$, the distribution network has been attacked and the state obtained by the traditional DSSE algorithm is inaccurate. In addition, the larger γ is, the more serious the cyber-attack suffered by the distribution network is.

It is clear that any calculated $\hat{\boldsymbol{x}}$ beyond the boundaries of interval DSSE will trigger the cyber-attack alarm. Furthermore, the value of γ implies the severity of cyber-attack, which eventually promotes the transformation of the distribution network from passive defense to active defense.

Obviously, the advantages of the detection strategy proposed in this paper are as follows:

1) The proposed detection strategy can be integrated into the traditional bad-data detection module without additional redundancy measurements or protection strategies [23], which is a small investment and is highly economic.

2) The proposed detection strategy makes no assumptions on the nature of the cyber-attack or the topological structure of the distribution network. In theory, it is suitable for most cyber-attack scenarios.

3) Compared with those in previous studies, the proposed detection strategy requires only a few predetermined parameters [29]. It can be applied on any time scale to meet the requirement of real-time cyber-attack detection.

V. Case Studies

The width and computation time of the estimated interval based on the interval DSSE directly affects the detection performance. If the estimated interval is too wide, the cyber-attack may be missed. If the computation time is too long, it is not suitable for real-time cyber-attack detection. Thus, the comparison experiments of the interval state estimation algorithms based on the interval DSSE are firstly conducted. Then, the detection performance is displayed under single- and multiple-bus cyber-attacks. To evaluate the performance of the proposed detection strategy based on interval DSSE, the test and analysis are carried out on the IEEE 33-bus and 123-bus systems shown in Fig. 1 and Fig. 2, respectively.

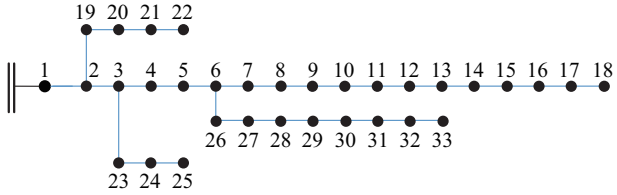

Fig. 1. Topology of IEEE 33-bus system.

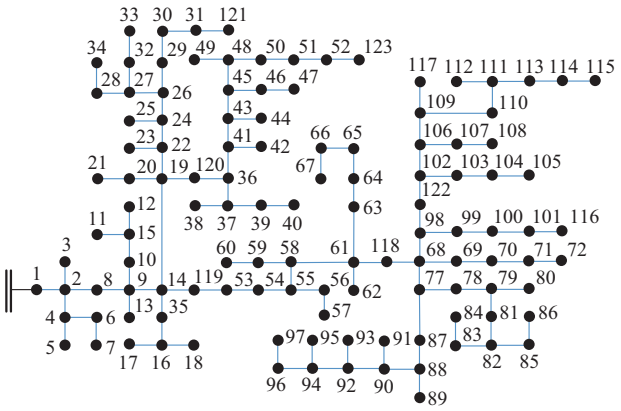

Fig. 2. Topology of IEEE 123-bus system.

A. Performance of Interval State Estimation Algorithm

In this paper, the MC algorithm is employed to evaluate the precision of the algorithm [18]. The interval obtained by the MC algorithm based on the interval DSSE model is considered as the true maximum boundary of the estimated states. The results of interval state estimation based on the proposed IIA are compared with those of deterministic state estimation, MC algorithm, and interval Gauss elimination (IGE) algorithm. The IGE algorithm [30], [31] is the conventional interval analysis algorithm based on the traditional Gaussian method, and uses the interval numbers to replace the point value. The coefficient matrix can be formed and converted to the upper triangular matrix in the interval form.

An indicator is used to evaluate the precision of estimation results based on the interval DSSE model, which is given by:

$$W = \frac{1}{M}\sum_{m=1}^{M}(\bar{x}_m - \underline{x}_m) \tag{37}$$

where W is the average value of the interval width. The smaller W is, the more accurate the interval algorithm will be.

Taking the IEEE 33-bus system as an example, the results of voltage amplitude and phase angle obtained by different interval state estimation algorithms are presented in Fig. 3 and Fig. 4, respectively.

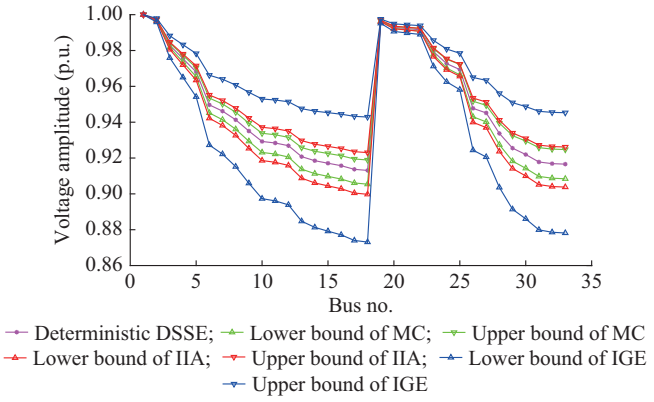

Fig. 3. Voltage amplitude with different interval state estimation algorithms.

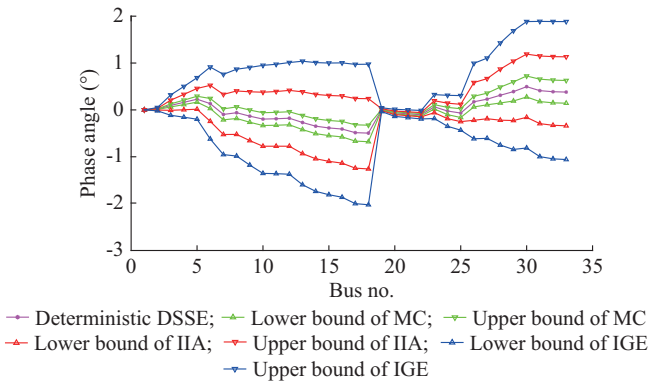

Fig. 4. Phase angle with different interval state estimation algorithms.

It is evident that all the states estimated by the deterministic DSSE are covered by the estimated interval based on the interval DSSE model. This implies that interval DSSE provides a reasonable boundary description of the system state. Furthermore, the interval estimated by the IIA is much narrower than the IGE on the voltage amplitude and phase angle, which benefits the cyber-attack detection. In Fig. 3, the result of IIA is close to the true maximum boundary of the estimated states and is thus suitable as the judging condition of the cyber-attack detection.

To further analyze the precision of the state interval estimation of IIA, the results of the MC algorithm and IIA with different measurement uncertainty levels are shown in Table I, where $[-\delta, \delta]$ is the original measurement uncertainty level.

TABLE I
RESULT OF MC AND IIA BASED ON INTERVAL DSSE MODEL WITH DIFFERENT MEASUREMENT UNCERTAINTY LEVELS

System	Method	Measurement uncertainty	W (p.u.)	Iteration	Time (ms)
IEEE 33-bus system	MC	$[-2\delta, +2\delta]$	0.0174		
		$[-4\delta, +4\delta]$	0.0323		
		$[-6\delta, +6\delta]$	0.0552		
		$[-8\delta, +8\delta]$	0.1204		
	IIA	$[-2\delta, +2\delta]$	0.0298	4	237.68
		$[-4\delta, +4\delta]$	0.0516	7	250.56
		$[-6\delta, +6\delta]$	0.0972	10	281.04
		$[-8\delta, +8\delta]$	0.1658	13	321.23
IEEE 123-bus system	MC	$[-2\delta, +2\delta]$	0.0298		
		$[-4\delta, +4\delta]$	0.0516		
		$[-6\delta, +6\delta]$	0.0972		
		$[-8\delta, +8\delta]$	0.1658		
	IIA	$[-2\delta, +2\delta]$	0.0367	7	1821.89
		$[-4\delta, +4\delta]$	0.0689	10	2121.88
		$[-6\delta, +6\delta]$	0.1063	12	2591.23
		$[-8\delta, +8\delta]$	0.1942	16	3014.46

It is apparent that the interval width becomes large with increasing measurement uncertainty. The result of interval DSSE is close to the true interval obtained by the MC algorithm in different scenarios. Comparing the results on IEEE 33-bus and 123-bus systems, the difference between the MC

algorithm and IIA with different measurement is similar. It means that the performance of IIA can remain stable with increasing complexity of the system. Moreover, the computation time of IIA based on the interval DSSE is fast and acceptable for real-time detection. Thus, the interval of the system state estimated by IIA based on the interval DSSE model is suitable as the predetermined boundary of the cyber-attack detection.

B. Detection Performance Under Attack on Single Bus State

The bus voltage amplitude of a-phase is taken as an example and an attack is constructed by modifying the state of the single bus, bus 61, which is selected randomly. Figure 5 presents the voltage amplitude of the a-phase based on traditional linear DSSE before and after the cyber-attack.

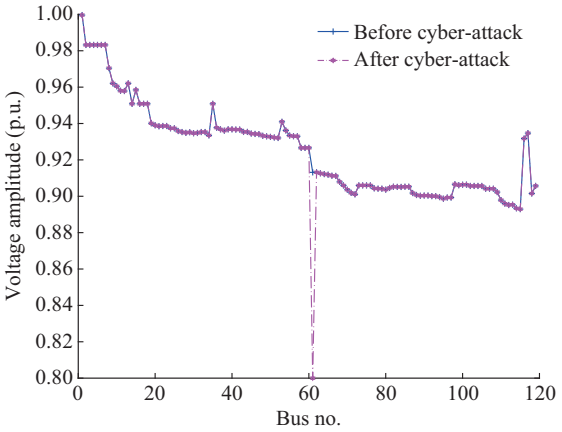

Fig. 5. Traditional linear DSSE results before and after cyber-attack on a single bus.

In Fig. 5, the voltage of bus 61 changes from 0.913 p.u. to 0.8 p.u. after the false-data attack, which indicates that the attacker successfully implements a cyber-attack on the distribution network.

Figure 6 shows the result of the MNR test before and after cyber-attack on bus 61 in 100 MC experiments.

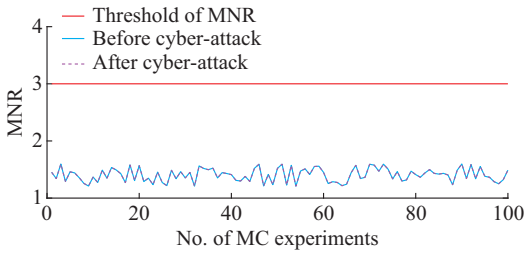

Fig. 6. Result of MNR test before and after cyber-attack on a single bus in 100 MC experiments.

In Fig. 6, the result of the MNR test after the attack is basically consistent with that before the attack, which is also lower than the set residual threshold 3. This illustrates that the proposed cyber-attack model can successfully evade the traditional residual test without being judged as bad data while injecting the false data.

The detection result based on the proposed interval DSSE detection strategy under $[-\delta, \delta]$ is displayed in Fig. 7. The cyber-attack on the single bus can be easily detected. However, with the increase of distribution network uncertainties, the width of the state interval estimated by the interval DSSE also increases. Figure 8 shows the results of the interval DSSE detection strategy when the uncertainties of the distribution network are the standard width δ and 2, 4, 6, and 8 times the width δ, respectively [18].

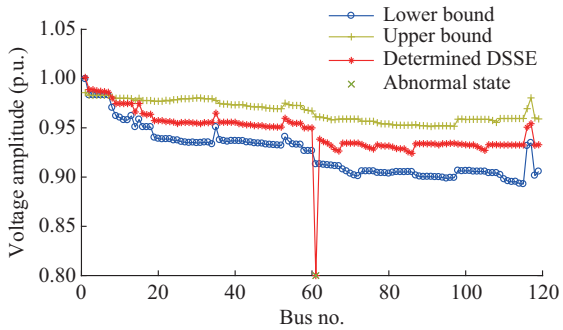

Fig. 7. Detection result of detection strategy based on interval DSSE after cyber-attack on a single bus.

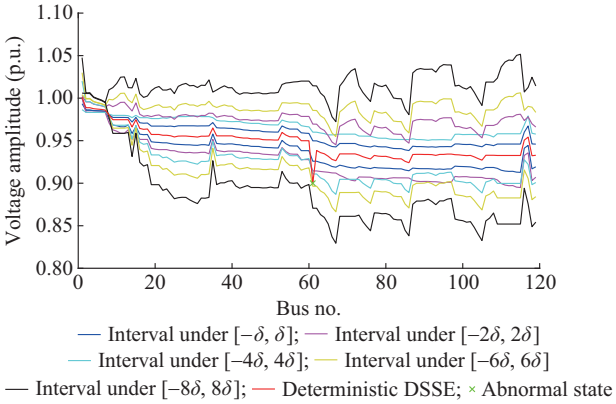

Fig. 8. Results of interval DSSE detection strategy after cyber-attack on a single bus state under various uncertainties of distribution network.

When the uncertainty of the distribution network is $[-8\delta, 8\delta]$, the detection strategy based on interval DSSE is invalid. It is implied that the effectiveness of the detection strategy is affected by the uncertainty of the distribution network. When the uncertainty is too significant, it is highly likely that the distribution network itself operates in an abnormal state. Consequently, it is difficult to judge whether the distribution network is being attacked based on the interval DSSE detection strategy.

C. Detection Performance Under Attack on Multiple Bus States

The detection performance under an FIDA on multiple buses is conducted and analyzed. The uncoupled buses 32, 78, and 101 (Case I) and coupled buses 68, 69, and 118 (Case II) are selected randomly. The test result of MNR test before and after cyber-attack on multiple buses in 100 MC experiments is shown in Fig. 9. It is clear that the MNR after the cyber-attack remains the same as that before the attack, but lower than the threshold 3. Thus, the injected false data on the multiple buses cannot be detected by the MNR

test. The validity of the proposed attack model is further verified.

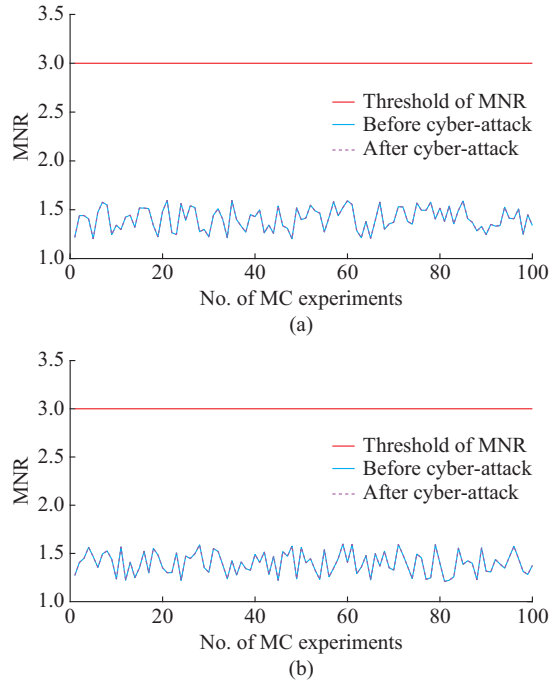

Fig. 9. Result of MNR test before and after cyber-attack on multiple buses in 100 MC experiments. (a) Case I. (b) Case II.

The detection result of the proposed detection strategy is shown in Fig. 10.

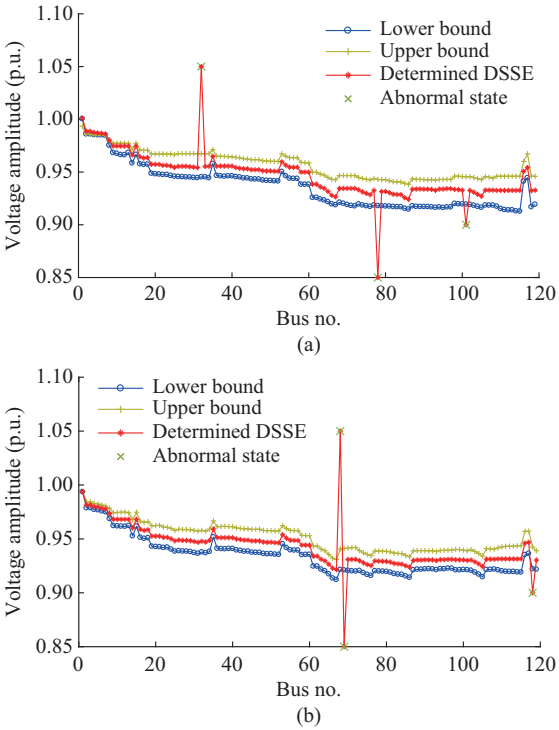

Fig. 10. Detection result of detection strategy based on interval DSSE after cyber-attack on multiple buses. (a) Case I. (b) Case II.

All the abnormal bus states can be detected by the proposed detection strategy. Between the results of Fig. 10(a) and (b), the voltage amplitude of coupled buses is larger than that of the uncoupled ones. It is implied that attacking coupled buses may enhance the attack performance, but also makes the cyber-attack easier to detect.

Figure 11 displays the result of the interval DSSE detection strategy after the cyber-attack when the uncertainty is the standard set $[-\delta, \delta]$ and 2, 4, 6, and 8 times the width δ. When the attacker attacks multiple buses, all the anomalies may not be detected under the large system uncertainty. The detection strategy can warn of a cyber-attack successfully through some detected abnormal states. However, if the uncertainty continues to increase, it may still lead to failure of the detection strategy.

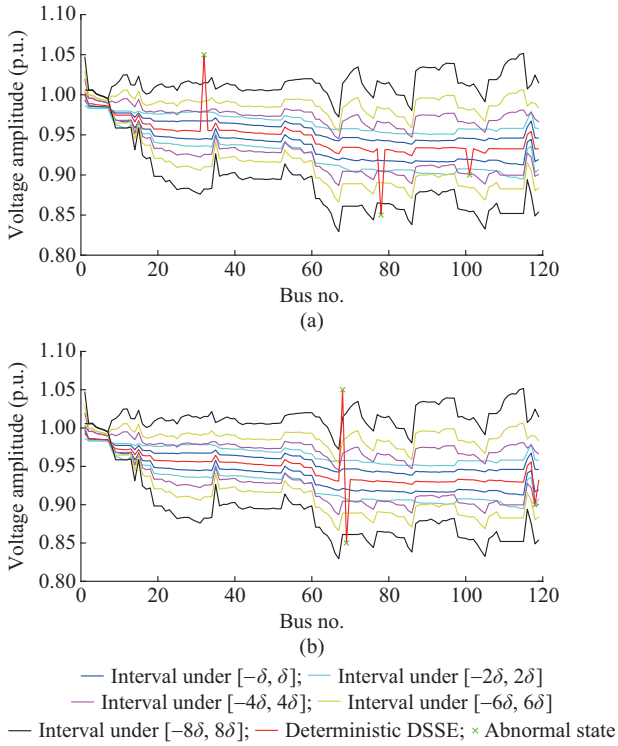

Fig. 11. Results of interval DSSE detection strategy after cyber-attack on multiple buses under various distribution network uncertainties. (a) Case I. (b) Case II.

The attack cost is discussed further. The number of attacked state variables under the coupled and uncoupled conditions is set from 2 to 10. The attacked state variables are selected randomly. The results of the corresponding number of measurements under the cyber-attack are shown in Fig. 12. It can be seen that the relationship between the numbers of attacked measurements and state variables is almost linear. The number of measurements required under cyber-attacks on coupled buses is always less than that required under cyber-attacks on uncoupled buses. In the uncoupled condition, the linear slope increases with the increasing number of attacked buses. The difference between the number of attacked measurements under the coupled and uncoupled conditions gradually becomes large. It is also implied that it is more economical for the attacker to attack coupled buses than uncoupled ones.

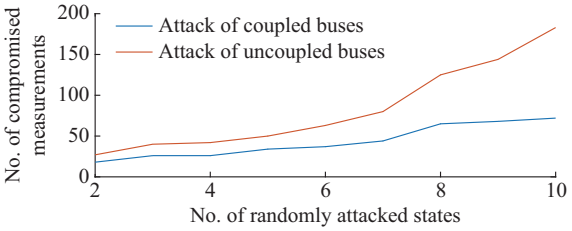

Fig. 12. Required number of compromised measurements.

VI. Conclusion

In this work, a cyber-attack detection strategy based on interval DSSE is developed against FIDA. The interval of each system state variable is constructed based on the interval DSSE to represent the range of its normal value. The cyber-attack is detected when the value of the state variable estimated by the traditional DSSE is outside of the corresponding interval determined by the interval DSSE model. An IIA is developed to solve the interval DSSE model and obtain the lower and upper bounds of the interval. To validate the proposed the cyber-attack detection strategy, the basic principle of the cyber-attack is studied, and its general model is formulated based on the three-phase DSSE model. The proposed cyber-attack model and detection strategy are conducted on IEEE 33-bus and 123-bus systems. Comprehensive comparative experiments of the proposed IIA, MC algorithm, and IGE algorithm validate the state interval estimation based on the interval DSSE model and demonstrate the superiority of IIA.

Based on the numerical results, it is concluded that the proposed detection strategy is nearly 100% effective in warning of the anomalous states caused by the proposed attack model. The proposed detection strategy is still valid when the uncertainty of the distribution network increases within the allowable range. The detection strategy requires not only a small investment and no assumptions regarding the system topology or attack type, but also exhibits high detection accuracy. In addition, the attack on coupled buses is more economical than that on uncoupled ones. However, it also increases the detection probability.

Our potential future works will focus on two aspects. One is to develop the optimal algorithms to narrow the estimated state interval. The other is to exhibit the improved three-phase DSSE model to enhance the accuracy of the state estimation.

References

[1] K. Zetter. (2016, Mar.). Inside the cunning, unprecedented hack of Ukraine's power grid. [Online]. Available: https://wired.com

[2] Russ Read. (2016, Jan.). Israeli power grid suffers one of the largest cyber attack in its history. [Online]. Available: https://dailycaller.com

[3] S. Pal, B. Sikdar, and J. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp.5057-5066, Sept. 2018.

[4] A. Barenghi, L. Breveglieri, I. Koren *et al.*, "Fault injection attacks on cryptographic devices: theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056-3076, Nov. 2012.

[5] R. Deng, G. Xiao, R. Lu *et al.*, "False data injection on state estimation in power systems-attacks, impacts, and defense: a survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, Apr. 2017.

[6] N. Zivkovic and A. T. Saric, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, Sept. 2018.

[7] A. Anwar, A. N. Mahmood, and M. Ahmed, "False data injection attack targeting the LTC transformers to disrupt smart grid operation," in *Proceedings of International Conference on Security and Privacy in Communication Systems*, Beijing, China, Sept. 2014, pp. 252-266.

[8] Y. Isozaki, S. Yoshizawa, Y. Fujimoto *et al.*, "Detection of cyber-attack against voltage control in distribution power grids with PVs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824-1835, Jul. 2016.

[9] X. Liu, Z. Bao, D. Lu *et al.*, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp.1686-1696, Jul. 2015.

[10] A. Teixeira, G. Dán, H.Sandberg *et al.*, "Security of smart distribution grids: data integrity attack on integrated volt/var control and countermeasures," in *Proceedings of 2014 American Control Conference*, Portland, USA, Jun. 2014, pp. 4372-4378.

[11] Z. Hu, Y. Wang, X. Tian *et al.*, "False data injection attacks identification for smart grids," in *Proceedings of the 3rd International Conference on Technological Advances in Electrical, Electronics and Computer Engineering*, Beirut, Lebanon, Apr. 2015, pp. 139-143.

[12] R. B. Bobba, K. M. Rogers, Q. Y. Wang *et al.*, "Detecting false data injection attacks on DC state estimation," in *Proceedings of the 1st Workshop on Secure Control Systems*, Urbana-Champaign, USA, Apr. 2010, pp. 1-9.

[13] Y. Chakhchoukh and H. Ishii, "Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations," *IEEE Transactions on Power Systems*, vol. 31,no. 6, pp. 4395-4405, Nov. 2016.

[14] J. Zhao, G. Zhang, M. L. Scala *et al.*, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580-1590, Jul. 2017.

[15] H. M. Khalid and J. C. H. Peng, "Immunity toward data-injection attacks using multi-sensor track fusion-based model prediction," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 697-707, Jul. 2017.

[16] Y. B. 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 Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505-2516, Mar. 2017.

[17] M. Ozay, I. Esnaola, F. Tunay *et al.*, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773-1786, Aug. 2016.

[18] C. P. Robert and G. Casella, *MC Statistical Methods*. New York: Springer-Verlag, 1999.

[19] J. Dopazo, O. Klitin, and A. Sasson, "Stochastic load flows," *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 2, pp. 299-309, Mar. 1975.

[20] J. Liang, Z. Wang, and X. Liu, "State estimation for coupled uncertain stochastic networks with missing measurements and time-varying delays: the discrete-time case," *IEEE Transactions on Neural Networks*, vol. 20, no. 5, pp. 781-793, May 2009.

[21] A. K. AL-Othman, "A fuzzy state estimator based on uncertain measurements," *Measurement*, vol. 42, no. 4, pp. 628-637, May 2009.

[22] J. Pereira, J. T. Saraiva, and V. Miranda, "An integrated load allocation/state estimation approach for distribution networks," in *Proceedings of 2004 International Conference on Probabilistic Methods Applied to Power Systems*, Ames, USA, Sept. 2004, pp. 180-185.

[23] Z. Wu, H. Zhan, W. Gu *et al.*, "Interval state estimation of distribution network with power flow constraint," *IEEE Access*, vol. 6, pp. 40826-40835, Jul. 2018.

[24] M. Bazrafshan and N. Gatsis, "Comprehensive modeling of three-phase distribution systems via the bus admittance matrix," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 2015-2029, Mar. 2018.

[25] M. Abdel-Akher, K. M. Nor, and A. H. Abdul-Rashid, "Development of unbalanced three-phase distribution power flow analysis using sequence and phase components," in *Proceedings of 12th International Middle-East Power System Conference*, Aswan, Egypt, Mar. 2008, pp. 406-411.

[26] H. Ahmadi, J. R. Marti, and A. von Meier, "A linear power flow formulation for three-phase distribution systems," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 5012-5021, Nov. 2016.

[27] R. E. Moore, *Methods and Applications of Interval Analysis*. Philadelphia: SIAM, 1979.

[28] R. Krawczyk, "Newton-algorithms for evaluation of roots with error bounds," *Computing*, vol. 4, no. 3, pp. 187-201, Jan. 1969.

[29] M. S. Rahman, M. A. Mahmud, A. M. T. Oo *et al*., "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 436-447, Apr. 2017.
[30] C. Rakpenthai, S. Uatrongjit, and S. Premrudeepreechacharn, "State estimation of power system considering network parameter uncertainty based on parametric interval linear systems," *IEEE Transactions on Power Systems*, vol. 27, no. 1, pp.305-313, Feb. 2012.
[31] J. Rohn, "On over-estimations produced by the interval Gaussian algorithm," *Reliable Computing*, vol. 3, no. 4, pp. 363-368, Nov. 1997.

Huan Long received her B.Eng. degree from the Department of Automation, Huazhong University of Science & Technology, Wuhan, China, in 2013, and the Ph.D. degree in systems engineering and engineering management from the City University of Hong Kong, Hong Kong, China, in 2017. Currently, she is an Assistant Professor in School of Electrical Engineering, Southeast University, Nanjing, China. Her research interests include data mining applied in modeling, optimizing, monitoring the renewable energy systems and power systems.

Zhi Wu received the B.Eng. degree in mathematics from Southeast University, Nanjing, China, in 2009, the M. Sc. degree in electrical engineering from the School of Electrical Engineering, Southeast University, in 2012, and the Ph.D. degree from the University of Birmingham, Birmingham, U.K., in 2016. He is currently an Associated Professor with Southeast University. His research interests include renewable energy and planning and optimization techniques.

Chen Fang is currently with State Grid Shanghai Electric Power Company, Electric Power Research Institute, Shanghai, China. His research interest is optimization and planning of power systems.

Wei Gu received his B.S. and Ph.D. degrees in electrical engineering from Southeast University, Nanjing, China, in 2001 and 2006, respectively. From 2009 to 2010, he was a Visiting Scholar in the Department of Electrical Engineering, Arizona State University, Tempe, USA. He is now a Professor in the School of Electrical Engineering, Southeast University. He is the director of the Institute of Distributed Generations and Active Distribution Networks. His research interests include distributed generations and microgrids, and integrated energy systems.

Xinchi Wei received the Ph.D. degree in electrical engineering from Southeast University, Nanjing, China, in 2018. From June 2016 to June 2017, she was a joint Ph.D. student funded by China Scholarship Council with the School of Electrical, Mechanical and Mechatronic Systems, University of Technology, Sydney, Australia. Since 2018, she has been with State Grid Shanghai Electrical Power Company, Electric Power Research Institute, Shanghai, China. Her research interests include the areas of smart grids, renewable power generation, and grid synchronization.

Huiyu Zhan received her B.S. and M.S. degrees in electrical engineering from Southeast University, Nanjing, China, in 2016 and 2019, respectively. From September 2016 to September 2017, she was a joint student funded by China Scholarship Council and received the M.S. degree from the University of Birmingham, Birmingham, U.K.. She is currently an engineer with China Electric Power Research Institute, Beijing, China. Her research interest is state analysis of power systems.