Adaptive Two-stage Unscented Kalman Filter for Dynamic State Estimation of Synchronous Generator Under Cyber Attacks Against Measurements

Dongchen Hou, *Student Member*, *IEEE*, Yonghui Sun, *Member*, *IEEE*, Venkata Dinavahi, *Fellow*, *IEEE*, and Yi Wang, *Member*, *IEEE*

***Abstract*—This paper develops an adaptive two-stage unscented Kalman filter (ATSUKF) to accurately track operation states of the synchronous generator (SG) under cyber attacks. To achieve high fidelity, considering the excitation system of SGs, a detailed 9th-order SG model for dynamic state estimation is established. Then, for several common cyber attacks against measurements, a two-stage unscented Kalman filter is proposed to estimate the model state and the bias in parallel. Subsequently, to solve the deterioration problem of state estimation performance caused by the mismatch between noise statistical characteristics and model assumptions, a multi-dimensional adaptive factor matrix is derived to modify the noise covariance matrix. Finally, a large number of simulation experiments are carried out on the IEEE 39-bus system, which shows that the proposed filter can accurately track the SG state under different abnormal test conditions.**

***Index Terms*—Cyber attack, dynamic state estimation, Kalman filtering, synchronous generator (SG), unscented transformation.**

I. Introduction

DUE to the development of monitoring, sensing, and communication technologies, a great quantity of intelligent devices are applied to modern power systems, making the information exchange between power systems and cyber systems increasingly frequent. Because of such features, the power system relies on critical cyber infrastructure, making it vulnerable to cyber attacks [1]-[5]. As one of the core functions of the energy management system (EMS), the dynamic state estimation (DSE) can help operators perceive the system state and its results can be used as the basis for other advanced functions of power grid [6]. However, the results of state estimation are often limited by the quality of measurements and the understanding of system parameters. This allows attackers to compromise the information and transmission of the measurement by exploiting the security vulnerabilities in communication, authentication, and data collection of the device [7]. Once the attack succeeds, the operator's awareness of the power system state will be diminished, resulting in system failures or outages and huge financial losses. Therefore, cyber attacks are gradually becoming one of the important factors threatening the security and stability of modern power systems.

At present, a great quantity of phasor measurement units (PMUs) have been installed in the wide-area measurement system (WAMS), which provides significant measurement data for DSE. The operators can dynamically track operation states of the system [8]. In this situation, Kalman filtering and its extension methods have attracted wide attention [9]-[13]. In [14], considering the parameter changes of the state-space model caused by cyber attacks, a robust forecasting-aided state estimation method based on extended Kalman filter (EKF) was proposed to estimate the distribution system state. In [15], based on EKF, the batch-mode regression and S-estimator were used to identify and suppress the impact of outliers to ensure the accuracy of state estimation results under cyber attacks. In [16], a fast detection strategy of network attack based on EKF was proposed by using generalized likelihood ratio. In [17], an optimal two-stage Kalman filter (OTSKF) method was developed to estimate system state vectors and attack vectors in automatic generation control (AGC) system. Estimating attack vectors can help operators understand cyber attacks more deeply, which can pro-

Manuscript received: May 25, 2023; revised: August 23, 2023; accepted: December 25, 2023. Date of CrossCheck: December 25, 2023. Date of online publication: February 2, 2024.

This work was supported by the National Natural Science Foundation of China (No. 62073121), the National Natural Science Foundation of China-State Grid Joint Fund for Smart Grid (No. U1966202), the Six Talent Peaks High Level Project of Jiangsu Province (No. 2017-XNY-004), and the Natural Sciences and Engineering Research Council (NSERC) of Canada.

D. Hou and Y. Sun (corresponding author) are with the School of Electrical and Power Engineering, Hohai University, Nanjing 210098, China, and D. Hou is also with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 2V4, Canada (e-mail: houdc15966868@163.com; sunyonghui168@gmail.com).

V. Dinavahi is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 2V4, Canada (e-mail: dinavahi@ualberta.ca).

Y. Wang is with the School of Electrical and Information Engineering, Zhengzhou University, Zhengzhou 450001, China, and he is also with the Henan Engineering Research Center of Power Electronics and Energy Systems, Zhengzhou 450001, China (e-mail: wangyi1414599008@163.com).

DOI: 10.35833/MPCE.2023.000352

vide effective information for tracing network attack sources and formulating defense strategies.

Moreover, to avoid the error caused by EKF, a derivative-free unscented Kalman filter (UKF) was proposed in [18]-[20]. In [21], based on the robust control theory, an adaptive UKF was proposed to suppress the estimation error of synchronous generator (SG) caused by cyber attacks or unpredictable changes of model parameters. In [22], a new decentralized DSE method was proposed to estimate unknown inputs by using statistical linearization method. A method was presented to improve the numerical stability of UKF in [23]. Based on the separation deviation theory, a two-stage unscented Kalman filter (TSUKF) was presented in [24]. To reduce the computation burden, an improved TSUKF based on non-augmented UKF is proposed in [25]. Nevertheless, in a Kalman filter, noise statistical parameters will directly affect the performance of DSE. Due to the interference of uncertain factors in actual systems, it is difficult to obtain the noise statistical parameters accurately, which leads to the decrease in estimation accuracy or deviation from the true value [26], [27].

In an effort to address these problems, an adaptive two-stage unscented Kalman filter (ATSUKF) is developed based on the adaptive noise correction method, which is suitable for the DSE of SGs. The contributions of this work are as follows.

1) To effectively reflect the operation states of SGs, the DSE model is extended based on the consideration of *d*-axis windings and *q*-axis damping windings. Considering the excitation system of SGs, a novel 9th-order SG model is proposed for DSE.

2) A TSUKF for DSE of SGs is proposed to separate the bias caused by cyber attacks or noise signals, which can estimate the state and the bias in parallel.

3) Considering the influence of unknown noise statistical characteristics caused by uncertainties on the performance of state estimation, an adaptive noise correction method is proposed and the multi-dimensional adaptive factor matrix is derived.

The remainder of this paper is organized as follows. A novel 9th-order SG model including an excitation system is introduced in Section II. In Section III, an ATSUKF is presented to estimate the state and bias of SGs in parallel. In Section IV, by using the constructed 9th-order SG model, a large number of simulation and numerical results are used to prove the advantages of the proposed filter. Finally, the conclusions are given in Section V.

II. Novel 9th-order SG Model

The detailed SG model can reflect operation states of the generator more comprehensively [28], [29]. Therefore, a detailed 9th-order SG model is utilized for DSE, which will help operators accurately predict operation states of the generator. Two mechanical equations, four electrical equations, and an excitation system model are included in the model.

The two mechanical equations can be expressed as:

$$\dot{\delta} = \omega_R \Delta\omega \tag{1}$$

$$\dot{\omega} = \frac{\omega_R}{2H}\left(T_m - T_e - D\Delta\omega\right) \tag{2}$$

where δ is the rotor position; ω is the rotor speed in per unit; ω_R is the synchronous speed; $\Delta\omega$ is the rotor speed deviation in per unit and $\Delta\omega = \left(\omega - \omega_R\right)/\omega_R$; T_e is the electrical torque; T_m is the mechanical torque; H is the inertia constant; and D is the damping coefficient.

The four electrical equations of the field winding and damper winding fluxes are expressed as [30]:

$$\dot{\psi}_{fd} = \omega_R\left(e_{fd} + \frac{\psi_{ad} - \psi_{fd}}{L_{fd}} R_{fd}\right) \tag{3}$$

$$\dot{\psi}_{1d} = \omega_R\left(e_{1d} + \frac{\psi_{ad} - \psi_{1d}}{L_{1d}} R_{1d}\right) \tag{4}$$

$$\dot{\psi}_{1q} = \omega_R\left(e_{1q} + \frac{\psi_{aq} - \psi_{1q}}{L_{1q}} R_{1q}\right) \tag{5}$$

$$\dot{\psi}_{2q} = \omega_R\left(e_{2q} + \frac{\psi_{aq} - \psi_{2q}}{L_{2q}} R_{2q}\right) \tag{6}$$

where e is the voltage; ψ is the flux; L is the leakage reactance; R is the resistance; the subscripts fd, $1d$, and iq represent the field winding, d-axis damper winding, and q-axis damper winding i $(i = 1, 2)$, respectively; and the fluxes ψ_{ad} and ψ_{aq} can be calculated by:

$$\psi_{ad} = L''_{ad}\left(-i_d + \frac{\psi_{fd}}{L_{fd}} + \frac{\psi_{1d}}{L_{1d}}\right) \tag{7}$$

$$\psi_{aq} = L''_{aq}\left(-i_q + \frac{\psi_{1q}}{L_{1q}} + \frac{\psi_{2q}}{L_{2q}}\right) \tag{8}$$

$$L''_{ad} = \frac{1}{L_{ad}^{-1} + L_{fd}^{-1} + L_{1d}^{-1}} \tag{9}$$

$$L''_{aq} = \frac{1}{L_{aq}^{-1} + L_{1q}^{-1} + L_{2q}^{-1}} \tag{10}$$

where i_d and i_q are the d- and q-axis currents, respectively; and L_{ad} and L_{aq} are the saturated values of the d- and q-axis mutual inductances, respectively [31].

Then, the electric torque T_e can be expressed as:

$$T_e = \psi_{ad} i_q - \psi_{aq} i_d \tag{11}$$

In addition, the currents can be written in terms of fluxes as:

$$i_{fd} = \frac{\psi_{fd} - \psi_{ad}}{L_{fd}} \tag{12}$$

$$i_{1d} = \frac{\psi_{1d} - \psi_{ad}}{L_{1d}} \tag{13}$$

$$i_{1q} = \frac{\psi_{1q} - \psi_{aq}}{L_{1q}} \tag{14}$$

$$i_{2q} = \frac{\psi_{2q} - \psi_{aq}}{L_{2q}} \tag{15}$$

The excitation system model including the power system stabilizer (PSS) and automatic voltage regulator (AVR) is

shown in Fig. 1. The equations of the excitation system model are expressed as:

$$\dot{v}_1 = \frac{1}{T_R}\left(v_t - v_1\right) \tag{16}$$

$$\dot{v}_2 = K_{STAB}\Delta\dot{\omega} - \frac{1}{T_w}v_2 \tag{17}$$

$$\dot{v}_3 = \frac{1}{T_2}\left(T_1\dot{v}_2 + v_2 - v_3\right) \tag{18}$$

where v_1-v_3 are the excitation system state variables; K_{STAB} is the stabilizer gain; T_w is washout time constant; T_1 is the time constant of lead compensator; T_R is the time constant of terminal voltage transducer; T_2 is the time constant of lag compensator; and v_t is the generator terminal voltage.

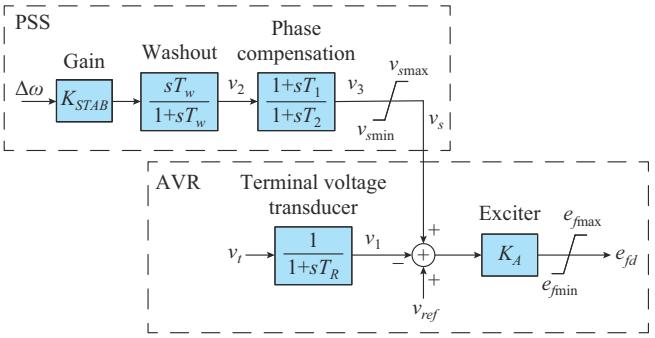

Fig. 1. Excitation system model of SGs.

For convenience, the above equations can be written in the following form:

$$\begin{cases} \dot{\boldsymbol{x}} = \boldsymbol{f}\left(\boldsymbol{x}, \boldsymbol{u}\right) + \boldsymbol{w} \\ \boldsymbol{y} = \boldsymbol{h}\left(\boldsymbol{x}, \boldsymbol{u}\right) + \boldsymbol{v} \end{cases} \tag{19}$$

where $\boldsymbol{f}(\cdot)$ is the system function; $\boldsymbol{h}(\cdot)$ is the measurement function; $\boldsymbol{x}$ is the state vector; $\boldsymbol{u}$ is the input vector; $\boldsymbol{y}$ is the measurement vector; and $\boldsymbol{w}$ and $\boldsymbol{v}$ represent the process and measurement noises, respectively.

$$\boldsymbol{x} = \left[\delta, \omega, \psi_{fd}, \psi_{1d}, \psi_{1q}, \psi_{2q}, v_1, v_2, v_3\right]^{\mathrm{T}} \tag{20}$$

$$\boldsymbol{u} = \left[e_{fd}, e_{1d}, e_{1q}, e_{2q}, T_m, i_d, i_q, v_t\right]^{\mathrm{T}} \tag{21}$$

$$\boldsymbol{y} = \left[\delta, \omega, i_{fd}, i_{1d}, i_{1q}, i_{2q}, v_1, v_2, v_3\right]^{\mathrm{T}} \tag{22}$$

Considering the discrete nature of the measured data, (19) can be rewritten in the discrete-time form as:

$$\begin{cases} \boldsymbol{x}_{k+1} = \boldsymbol{f}\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + \boldsymbol{w}_k \\ \boldsymbol{y}_k = \boldsymbol{h}\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + \boldsymbol{v}_k \end{cases} \tag{23}$$

where k is a discrete time factor.

III. Proposed ATSUKF

A. Measurement Data Attack Model

To successfully gain access, the attacker needs to know the complete knowledge about the target before attacking [32]. However, it is difficult for attackers to obtain the system parameters because there are a large number of measures to protect information in actual power systems, such as identity authentication, intrusion detection, and firewalls [33]. The measurement equipment relies on the network to transmit the measurement data, and has frequent communication with the outside world, so its defense is relatively vulnerable. Therefore, accessing the measurement data becomes one of the most common methods to attack systems. The measurement vector $\boldsymbol{y}_k = \left[y_{1,k}, y_{2,k}, \ldots, y_{N,k}\right]^{\mathrm{T}}$ can be written as:

$$\boldsymbol{y}_k = \boldsymbol{h}\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + \boldsymbol{G}\boldsymbol{b}_k + \boldsymbol{v}_k \quad k \geq \tau \tag{24}$$

where $\boldsymbol{b}_k = \left[b_{1,k}, b_{2,k}, \ldots, b_{N,k}\right]^{\mathrm{T}}$ is the attack/bias vector at time k; τ is the moment when the attacker successfully accesses the measurement data; $\boldsymbol{G}$ is the attack distribution matrix of measurement variables; and $\boldsymbol{v}_k = \left[v_{1,k}, v_{2,k}, \ldots, v_{N,k}\right]^{\mathrm{T}}$ is the measurement noise vector at time k.

$$y_{n,k} = \begin{cases} h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + v_{n,k} & n \notin S_k^f, k \geq \tau \\ h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + b_{n,k} + v_{n,k} & n \in S_k^f, k \geq \tau \end{cases} \tag{25}$$

where $h_n(\cdot)$ is the measurement function of the n^{th} measurement variable; $S_k^f \subset \{1, 2, \ldots, N\}$ is the set of the measurement variable affected by cyber attacks; and $n \in \{1, 2, \ldots, N\}$.

Several common cyber attacks against measurement data can be expressed in the following forms.

1) False Data Injection (FDI)

FDI, as the most common type of cyber attack, injects false data $b_{n,k}^{FDI}$ into real data to affect the operator's awareness of the system:

$$y_{n,k} = \begin{cases} h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + v_{n,k} & n \notin S_k^f, k \geq \tau \\ h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + b_{n,k}^{FDI} + v_{n,k} & n \in S_k^f, k \geq \tau \end{cases} \tag{26}$$

2) Scaling Attack

The attacker can scale down/up the measurement through scaling factors λ_a:

$$y_{n,k} = \begin{cases} h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + v_{n,k} & n \notin S_k^f, k \geq \tau \\ \lambda_a h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + v_{n,k} & n \in S_k^f, k \geq \tau \end{cases} \tag{27}$$

3) Data Replay Attack

The attacker can inject previous data $y_{n,k-t}$ in place of real measurements:

$$y_{n,k} = \begin{cases} h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + v_{n,k} & n \notin S_k^f, k \geq \tau \\ y_{n,k-t} + v_{n,k} & n \in S_k^f, k \geq \tau \end{cases} \tag{28}$$

4) Ramp Attack

By utilizing the growth factor r_b, the injected data $b_{n,k}^{RA} = r_b(k - \tau)$ will change over time.

$$y_{n,k} = \begin{cases} h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + v_{n,k} & n \notin S_k^f, k \geq \tau \\ h_n\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + b_{n,k}^{RA} + v_{n,k} & n \in S_k^f, k \geq \tau \end{cases} \tag{29}$$

B. TSUKF

Consider the nonlinear discrete system with attack/bias, and then (23) can be written as:

$$\begin{cases} \boldsymbol{x}_{k+1} = \boldsymbol{f}\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + \boldsymbol{F}\boldsymbol{b}_k + \boldsymbol{w}_k \\ \boldsymbol{y}_k = \boldsymbol{h}\left(\boldsymbol{x}_k, \boldsymbol{u}_k\right) + \boldsymbol{G}\boldsymbol{b}_k + \boldsymbol{v}_k \end{cases} \tag{30}$$

where $\boldsymbol{F}$ is the attack distribution matrix of state variables.

TSUKF is an extension of UKF. The attack-/bias-free estimation and attack/bias estimation processes of TSUKF are as follows:

$$\hat{\boldsymbol{x}}_{k+1|k+1}=\tilde{\boldsymbol{x}}_{k+1|k+1}+\boldsymbol{\beta}_{k+1|k+1}\hat{\boldsymbol{b}}_{k+1|k+1} \tag{31}$$

$$\boldsymbol{P}^{\boldsymbol{x}}_{k+1|k+1}=\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k+1}+\boldsymbol{\beta}_{k+1|k+1}\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k+1}\boldsymbol{\beta}^{\mathrm{T}}_{k+1|k+1} \tag{32}$$

where $\boldsymbol{\beta}_{k+1|k+1}$ is the coupling matrix; $\tilde{\boldsymbol{x}}_{k+1|k+1}$ is the state vector of attack-/bias-free estimation; $\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k+1}$ is the variance matrix of attack-/bias-free estimation; and $\hat{\boldsymbol{b}}_{k+1|k+1}$ and $\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k+1}$ are the state vector and its variance matrix of attack/bias estimation, respectively.

In the attack-/bias-free estimation, the expected value of the estimator is equal to the true value. There is a deviation between the expected value and the true value of the estimator in the attack/bias estimation. When the measurement is attacked, the results of attack-/bias-free estimation will deviate from the true value. Therefore, it is necessary to estimate the bias caused by cyber attacks through attack/bias estimation to suppress the impact of false measurements.

1) Attack-/bias-free Estimation

Similar to UKF, by utilising the unscented transform, the sigma points can be selected as:

$$\boldsymbol{\chi}^{0}_{k}=\hat{\boldsymbol{x}}_{k|k} \tag{33}$$

$$\boldsymbol{\chi}^{j}_{k}=\hat{\boldsymbol{x}}_{k|k}\pm\sqrt{(n+\lambda)\boldsymbol{P}^{\boldsymbol{x}}_{k|k}}\,\boldsymbol{e}_{i}\quad j=1,2,\ldots,n \tag{34}$$

where λ is the scaling parameter; and $\boldsymbol{e}_i$ is the column vector where the i^{th} element is 1 and the other elements are 0.

Using the state transfer function to propagate sigma points, the predicted state vector $\boldsymbol{m}_k$ and its corresponding error covariance matrix $\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k}$ can be obtained by:

$$\boldsymbol{m}_{k}=\sum_{j=0}^{2n}W^{s}_{j}\boldsymbol{f}\left(\boldsymbol{\chi}^{j}_{k}\right) \tag{35}$$

$$\hat{\boldsymbol{x}}_{k+1|k}=\boldsymbol{m}_{k}+\boldsymbol{F}\hat{\boldsymbol{b}}_{k|k} \tag{36}$$

$$\begin{aligned}\boldsymbol{P}^{\boldsymbol{x}}_{k+1|k}=&\sum_{j=0}^{2n}W^{c}_{j}\left(\boldsymbol{f}\left(\boldsymbol{\chi}^{j}_{k}\right)-\boldsymbol{m}_{k}\right)\left(\boldsymbol{f}\left(\boldsymbol{\chi}^{j}_{k}\right)-\boldsymbol{m}_{k}\right)^{\mathrm{T}}-\\&\boldsymbol{M}_{k}\boldsymbol{\beta}_{k|k}\boldsymbol{P}^{\boldsymbol{b}}_{k|k}\boldsymbol{\beta}^{\mathrm{T}}_{k|k}\boldsymbol{M}^{\mathrm{T}}_{k}+\boldsymbol{R}_{k}\boldsymbol{P}^{\boldsymbol{b}}_{k|k}\boldsymbol{R}^{\mathrm{T}}_{k}+\boldsymbol{W}_{\boldsymbol{x}}\end{aligned} \tag{37}$$

$$\tilde{\boldsymbol{x}}_{k+1|k}=\hat{\boldsymbol{x}}_{k+1|k}-\boldsymbol{\beta}_{k+1|k}\hat{\boldsymbol{b}}_{k+1|k} \tag{38}$$

$$\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k}=\boldsymbol{P}^{\boldsymbol{x}}_{k+1|k}-\boldsymbol{\beta}_{k+1|k}\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k}\boldsymbol{\beta}^{\mathrm{T}}_{k+1|k} \tag{39}$$

where $\boldsymbol{M}_k$ and $\boldsymbol{R}_k$ are the coupling matrices that can be obtained through the calculation of the coupling equations; $\boldsymbol{W}_{\boldsymbol{x}}$ is the process noise variance matrix; and the weights W^{s}_{j} and W^{c}_{j} are defined as:

$$\begin{cases}W^{s}_{0}=\dfrac{\lambda}{n+\lambda}\\[2mm] W^{c}_{0}=\dfrac{\lambda}{n+\lambda}+1-\alpha^{2}_{c}+\beta_{c}\end{cases} \tag{40}$$

$$W^{s}_{j}=W^{c}_{j}=\frac{1}{2(n+\lambda)}\quad j=1,2,\ldots,2n \tag{41}$$

where α_c is the scaling factor that can control the range of sigma point sets; and β_c is a constant used to reflect the high-order information characteristics of state information.

After that, using the measurement function to instantiate sigma points, the measurement vector $\boldsymbol{n}_{k+1}$ and its corresponding error covariance matrix $\tilde{\boldsymbol{P}}^{\boldsymbol{yy}}_{k+1|k}$ can be obtained by:

$$\boldsymbol{n}_{k+1}=\sum_{j=0}^{2n}W^{s}_{j}\boldsymbol{h}\left(\boldsymbol{\chi}^{j}_{k+1}\right) \tag{42}$$

$$\tilde{\boldsymbol{y}}_{k+1|k}=\boldsymbol{n}_{k+1}-\boldsymbol{N}_{k+1}\boldsymbol{\beta}_{k+1|k}\hat{\boldsymbol{b}}_{k+1|k} \tag{43}$$

$$\begin{aligned}\tilde{\boldsymbol{P}}^{\boldsymbol{yy}}_{k+1|k}=&\sum_{j=0}^{2n}W^{c}_{j}\left(\boldsymbol{h}\left(\boldsymbol{\chi}^{j}_{k+1}\right)-\boldsymbol{n}_{k+1}\right)\left(\boldsymbol{h}\left(\boldsymbol{\chi}^{j}_{k+1}\right)-\boldsymbol{n}_{k+1}\right)^{\mathrm{T}}-\\&\boldsymbol{N}_{k+1}\boldsymbol{\beta}_{k+1|k}\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k}\boldsymbol{\beta}^{\mathrm{T}}_{k+1|k}\boldsymbol{N}^{\mathrm{T}}_{k+1}+\boldsymbol{V}_{\boldsymbol{x}}\end{aligned} \tag{44}$$

where $\tilde{\boldsymbol{y}}_{k+1|k}$ is the predicted measurement vector; $\boldsymbol{N}_{k+1}$ is a coupling matrix; and $\boldsymbol{V}_{\boldsymbol{x}}$ is the measurement noise variance matrix.

The gain matrix $\boldsymbol{K}^{\boldsymbol{x}}_{k+1}$ and filtered states $\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k+1}$ and $\tilde{\boldsymbol{x}}_{k+1|k+1}$ can be calculated by:

$$\boldsymbol{K}^{\boldsymbol{x}}_{k+1}=\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k}\boldsymbol{N}^{\mathrm{T}}_{k+1}\left(\tilde{\boldsymbol{P}}^{\boldsymbol{yy}}_{k+1|k}\right)^{-1} \tag{45}$$

$$\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k+1}=\tilde{\boldsymbol{P}}^{\boldsymbol{x}}_{k+1|k}-\boldsymbol{K}^{\boldsymbol{x}}_{k+1}\tilde{\boldsymbol{P}}^{\boldsymbol{yy}}_{k+1|k}\left(\boldsymbol{K}^{\boldsymbol{x}}_{k+1}\right)^{\mathrm{T}} \tag{46}$$

$$\tilde{\boldsymbol{x}}_{k+1|k+1}=\tilde{\boldsymbol{x}}_{k+1|k}+\boldsymbol{K}^{\boldsymbol{x}}_{k+1}\left(\boldsymbol{y}_{k+1}-\tilde{\boldsymbol{y}}_{k+1|k}\right) \tag{47}$$

2) Attack/bias Estimation

Notably, the attack-/bias-free estimation and the attack/bias estimation run in parallel.

$$\hat{\boldsymbol{b}}_{k+1|k}=\hat{\boldsymbol{b}}_{k|k} \tag{48}$$

$$\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k}=\boldsymbol{P}^{\boldsymbol{b}}_{k|k}+\boldsymbol{W}_{\boldsymbol{b}} \tag{49}$$

$$\hat{\boldsymbol{y}}_{k+1|k}=\boldsymbol{n}_{k+1}+\boldsymbol{G}\hat{\boldsymbol{b}}_{k+1|k} \tag{50}$$

$$\boldsymbol{P}^{\boldsymbol{by}}_{k+1|k}=\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k}\boldsymbol{H}^{\mathrm{T}}_{k+1|k} \tag{51}$$

$$\boldsymbol{P}^{\boldsymbol{yy}}_{k+1|k}=\tilde{\boldsymbol{P}}^{\boldsymbol{yy}}_{k+1|k}+\boldsymbol{H}_{k+1|k}\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k}\boldsymbol{H}^{\mathrm{T}}_{k+1|k} \tag{52}$$

$$\boldsymbol{K}^{\boldsymbol{b}}_{k+1}=\boldsymbol{P}^{\boldsymbol{by}}_{k+1|k}\left(\boldsymbol{P}^{\boldsymbol{yy}}_{k+1|k}\right)^{-1} \tag{53}$$

$$\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k+1}=\boldsymbol{P}^{\boldsymbol{b}}_{k+1|k}-\boldsymbol{K}^{\boldsymbol{b}}_{k+1}\boldsymbol{P}^{\boldsymbol{yy}}_{k+1|k}\left(\boldsymbol{K}^{\boldsymbol{b}}_{k+1}\right)^{\mathrm{T}} \tag{54}$$

$$\hat{\boldsymbol{b}}_{k+1|k+1}=\hat{\boldsymbol{b}}_{k+1|k}+\boldsymbol{K}^{\boldsymbol{b}}_{k+1}\left(\boldsymbol{y}_{k+1}-\hat{\boldsymbol{y}}_{k+1|k}\right) \tag{55}$$

where $\hat{\boldsymbol{y}}_{k+1|k}$ is the predicted measurement vector of attack/bias estimation; $\boldsymbol{P}^{\boldsymbol{yy}}_{k+1|k}$ is the predicted measurement covariance matrix; $\boldsymbol{H}_{k+1|k}$ is the coupling matrix in the prediction process of bias estimation; $\boldsymbol{K}^{\boldsymbol{b}}_{k+1}$ is the gain matrix of attack/bias estimation; and $\boldsymbol{W}_{\boldsymbol{b}}$ and $\boldsymbol{P}^{\boldsymbol{by}}_{k+1|k}$ are the process noise variance matrix and cross-covariance matrix in attack-/bias-free estimation, respectively.

3) Coupling Equations

$$\boldsymbol{R}_{k}=\boldsymbol{M}_{k}\boldsymbol{\beta}_{k|k}+\boldsymbol{F} \tag{56}$$

$$\boldsymbol{\beta}_{k+1|k}=\boldsymbol{R}_{k}\boldsymbol{P}^{\boldsymbol{b}}_{k|k}\left(\boldsymbol{P}^{\boldsymbol{b}}_{k|k}+\boldsymbol{W}_{\boldsymbol{b}}\right)^{-1} \tag{57}$$

$$\boldsymbol{H}_{k+1|k}=\boldsymbol{N}_{k+1}\boldsymbol{\beta}_{k+1|k}+\boldsymbol{G} \tag{58}$$

$$\boldsymbol{\beta}_{k+1|k+1}=\boldsymbol{\beta}_{k+1|k}-\boldsymbol{K}_{k+1}^{\boldsymbol{x}}\boldsymbol{H}_{k+1|k} \tag{59}$$

$$\boldsymbol{M}_k=\frac{1}{2\sqrt{n+\lambda}}\left[\sum_{j=1}^{n}\left(\boldsymbol{f}\left(\boldsymbol{\chi}_k^j\right)-\boldsymbol{f}\left(\boldsymbol{\chi}_k^{j+n}\right)\right)\boldsymbol{e}_i^{\mathrm{T}}\right]\left(\sqrt{\boldsymbol{P}_{k|k}^{\boldsymbol{x}}}\right)^{-1} \tag{60}$$

$$\boldsymbol{N}_{k+1}=\frac{1}{2\sqrt{n+\lambda}}\left[\sum_{j=1}^{n}\left(\boldsymbol{h}\left(\boldsymbol{\chi}_{k+1}^j\right)-\boldsymbol{h}\left(\boldsymbol{\chi}_{k+1}^{j+n}\right)\right)\boldsymbol{e}_i^{\mathrm{T}}\right]\left(\sqrt{\boldsymbol{P}_{k+1|k}^{\boldsymbol{x}}}\right)^{-1} \tag{61}$$

C. Noise Modification

Similar to the Kalman filter, TSUKF has good estimation effects only when accurate knowledge about DSE model can be obtained [34]. However, in the actual system, due to unknown factors such as cyber attacks, equipment aging, and environmental changes, the statistical parameters of the DSE model may change and cannot be accurately obtained [35]-[37]. Under these circumstances, the performance of TSUKF is significantly degraded and it is difficult to track the dynamic changes of the model state. This limits the use of TSUKF method in DSE. Considering the error caused by the uncertainty of noise prior statistics, a multi-dimensional adaptive factor matrix is introduced to modify the noise statistics, so that TSUKF can adapt to the statistical characteristics of noise. The scaling matrix $\boldsymbol{S}_{k+1}$ is used to realize the adaptive modification of measurement noise covariance, and the measurement variance can be expressed as:

$$\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}=\boldsymbol{C}^{\boldsymbol{y}}+\boldsymbol{S}_{k+1}\boldsymbol{V}_{\boldsymbol{x}} \tag{62}$$

$$\boldsymbol{C}^{\boldsymbol{y}}=\sum_{j=0}^{2n}W_j^c\left(\boldsymbol{h}\left(\boldsymbol{\chi}_{k+1}^j\right)-\boldsymbol{n}_{k+1}\right)\left(\boldsymbol{h}\left(\boldsymbol{\chi}_{k+1}^j\right)-\boldsymbol{n}_{k+1}\right)^{\mathrm{T}}-\boldsymbol{N}_{k+1}\boldsymbol{\beta}_{k+1|k}\boldsymbol{P}_{k+1|k}^{\boldsymbol{b}}\boldsymbol{\beta}_{k+1|k}^{\mathrm{T}}\boldsymbol{N}_{k+1}^{\mathrm{T}} \tag{63}$$

According to the actual measurement, the covariance matrix can be obtained as:

$$\bar{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}=\frac{1}{l-1}\sum_{j=k-l+2}^{k+1}\tilde{\boldsymbol{\varepsilon}}_j\tilde{\boldsymbol{\varepsilon}}_j^{\mathrm{T}} \tag{64}$$

where l is the size of the window; and $\tilde{\boldsymbol{\varepsilon}}_j$ is the residual vector of attack-free estimation at time j, and $\tilde{\boldsymbol{\varepsilon}}_j=\boldsymbol{y}_j-\boldsymbol{N}_j\tilde{\boldsymbol{x}}_{j|j-1}$.

Therefore, the equation relationship is as follows:

$$\frac{1}{l-1}\sum_{j=k-l+2}^{k+1}\tilde{\boldsymbol{\varepsilon}}_j\tilde{\boldsymbol{\varepsilon}}_j^{\mathrm{T}}=\boldsymbol{C}^{\boldsymbol{y}}+\boldsymbol{S}_{k+1}\boldsymbol{V}_{\boldsymbol{x}} \tag{65}$$

The scaling matrix $\boldsymbol{S}_{k+1}$ can be written as:

$$\boldsymbol{S}_{k+1}=\left(\bar{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}-\boldsymbol{C}^{\boldsymbol{y}}\right)\boldsymbol{V}_{\boldsymbol{x}}^{-1} \tag{66}$$

If the noise variance matches the system model, the scaling matrix is the unit matrix. However, the scaling matrix $\boldsymbol{S}_{k+1}$ obtained by (66) may not be a diagonal matrix, and the diagonal elements may be less than or equal to 0. To avoid this, the scaling matrix needs to be modified as:

$$\boldsymbol{S}_{k+1}=\mathrm{diag}\left(s_1,s_2,\ldots,s_i\right)\quad i=1,2,\ldots,n \tag{67}$$

where $s_i=\max\left\{1,S_{k+1,ii}\right\}$ is the diagonal element of the modified scaling matrix, and $S_{k+1,ii}$ is the diagonal element of matrix $\boldsymbol{S}_{k+1}$ before modification. By using the scaling matrix in (67), the covariance matrix $\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}$ and filter gain matrix $\boldsymbol{K}_{k+1}^{\boldsymbol{x}}$ can be recalculated.

In addition, the adaptive scaling matrix of the system and the noise variance matrix $\boldsymbol{W}_{\boldsymbol{x}}$ and $\boldsymbol{W}_{\boldsymbol{b}}$ can be obtained in the same way. By using (65), the scaling matrix $\boldsymbol{S}_{k+1}^{\boldsymbol{x}}$ can be expressed as:

$$\frac{1}{l-1}\sum_{j=k-l+2}^{k+1}\tilde{\boldsymbol{\varepsilon}}_j\tilde{\boldsymbol{\varepsilon}}_j^{\mathrm{T}}=\boldsymbol{N}_{k+1}\left(\boldsymbol{C}^{\boldsymbol{x}}+\boldsymbol{S}_{k+1}^{\boldsymbol{x}}\boldsymbol{W}_{\boldsymbol{x}}\right)\boldsymbol{N}_{k+1}^{\mathrm{T}}+\boldsymbol{V}_{\boldsymbol{x}} \tag{68}$$

$$\boldsymbol{C}^{\boldsymbol{x}}=\sum_{j=0}^{2n}W_j^c\left(\boldsymbol{f}\left(\boldsymbol{\chi}_k^j\right)-\boldsymbol{m}_k\right)\left(\boldsymbol{f}\left(\boldsymbol{\chi}_k^j\right)-\boldsymbol{m}_k\right)^{\mathrm{T}}+\boldsymbol{R}_k\boldsymbol{P}_{k|k}^{\boldsymbol{b}}\boldsymbol{R}_k^{\mathrm{T}}-\boldsymbol{M}_k\boldsymbol{\beta}_{k|k}\boldsymbol{P}_{k|k}^{\boldsymbol{b}}\boldsymbol{\beta}_{k|k}^{\mathrm{T}}\boldsymbol{M}_k^{\mathrm{T}}-\boldsymbol{\beta}_{k+1|k}\boldsymbol{P}_{k+1|k}^{\boldsymbol{b}}\boldsymbol{\beta}_{k+1|k}^{\mathrm{T}} \tag{69}$$

By using matrix operations, (68) can be simplified as:

$$\boldsymbol{S}_{k+1}^{\boldsymbol{x}}=\boldsymbol{N}_{k+1}^{-1}\left(\bar{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}-\boldsymbol{N}_{k+1}\boldsymbol{C}^{\boldsymbol{x}}\boldsymbol{N}_{k+1}^{\mathrm{T}}-\boldsymbol{V}_{\boldsymbol{x}}\right)\left(\boldsymbol{W}_{\boldsymbol{x}}\boldsymbol{N}_{k+1}^{\mathrm{T}}\right)^{-1} \tag{70}$$

The scaling matrix $\boldsymbol{S}_{k+1}^{\boldsymbol{x}}$ can be defined as:

$$\boldsymbol{S}_{k+1}^{\boldsymbol{x}}=\mathrm{diag}\left(s_1^{\boldsymbol{x}},s_2^{\boldsymbol{x}},\ldots,s_i^{\boldsymbol{x}}\right)\quad i=1,2,\ldots,n \tag{71}$$

where $s_i^{\boldsymbol{x}}=\max\left\{1,S_{k+1,ii}^{\boldsymbol{x}}\right\}$ is the diagonal element of the modified scaling matrix, and $S_{k+1,ii}^{\boldsymbol{x}}$ is the diagonal element of matrix $\boldsymbol{S}_{k+1}^{\boldsymbol{x}}$ before modification.

The covariance matrix $\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{x}}$ can be recalculated as:

$$\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{x}}=\boldsymbol{C}^{\boldsymbol{x}}+\boldsymbol{S}_{k+1}^{\boldsymbol{x}}\boldsymbol{W}_{\boldsymbol{x}} \tag{72}$$

For the scaling matrix $\boldsymbol{S}_{k+1}^{\boldsymbol{b}}$, the residual vector $\tilde{\boldsymbol{\varepsilon}}_j^{\boldsymbol{b}}$ and covariance matrix $\hat{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}$ are defined as:

$$\tilde{\boldsymbol{\varepsilon}}_j^{\boldsymbol{b}}=\boldsymbol{y}_j-\boldsymbol{N}_j\tilde{\boldsymbol{x}}_{j|j-1}-\boldsymbol{H}_{j|j-1}\boldsymbol{b}_{j|j-1} \tag{73}$$

$$\hat{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}=\frac{1}{l-1}\sum_{j=k-l+2}^{k+1}\tilde{\boldsymbol{\varepsilon}}_j^{\boldsymbol{b}}\left(\tilde{\boldsymbol{\varepsilon}}_j^{\boldsymbol{b}}\right)^{\mathrm{T}} \tag{74}$$

$$\frac{1}{l-1}\sum_{j=k-l+2}^{k+1}\tilde{\boldsymbol{\varepsilon}}_j^{\boldsymbol{b}}\left(\tilde{\boldsymbol{\varepsilon}}_j^{\boldsymbol{b}}\right)^{\mathrm{T}}=\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}+\boldsymbol{H}_{k+1|k}\left(\boldsymbol{P}_{k|k}^{\boldsymbol{b}}+\boldsymbol{S}_{k+1}^{\boldsymbol{b}}\boldsymbol{W}_{\boldsymbol{b}}\right)\boldsymbol{H}_{k+1|k}^{\mathrm{T}} \tag{75}$$

The adaptive scaling matrix can be obtained by:

$$\boldsymbol{S}_{k+1}^{\boldsymbol{b}}=\boldsymbol{H}_{k+1|k}^{-1}\left(\hat{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}-\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}-\boldsymbol{H}_{k+1|k}\boldsymbol{P}_{k|k}^{\boldsymbol{b}}\boldsymbol{H}_{k+1|k}^{\mathrm{T}}\right)\left(\boldsymbol{W}_{\boldsymbol{b}}\boldsymbol{H}_{k+1|k}^{\mathrm{T}}\right)^{-1} \tag{76}$$

$$\boldsymbol{S}_{k+1}^{\boldsymbol{b}}=\mathrm{diag}\left(s_1^{\boldsymbol{b}},s_2^{\boldsymbol{b}},\ldots,s_i^{\boldsymbol{b}}\right)\quad i=1,2,\ldots,n \tag{77}$$

where $s_i^{\boldsymbol{b}}=\max\left\{1,S_{k+1,ii}^{\boldsymbol{b}}\right\}$ is the diagonal element of the modified scaling matrix, and $S_{k+1,ii}^{\boldsymbol{b}}$ is the diagonal element of matrix $\boldsymbol{S}_{k+1}^{\boldsymbol{b}}$ before modification.

The covariance matrix $\boldsymbol{P}_{k+1|k}^{\boldsymbol{b}}$ can be recalculated as:

$$\boldsymbol{P}_{k+1|k}^{\boldsymbol{b}}=\boldsymbol{P}_{k|k}^{\boldsymbol{b}}+\boldsymbol{S}_{k+1}^{\boldsymbol{b}}\boldsymbol{W}_{\boldsymbol{b}} \tag{78}$$

For convenience, the proposed ATSUKF based on adaptive noise correction method can be presented as Algorithm 1.

Remark 1: in order to track the operation states of SGs, the 4th-order model of generators is usually used for DSE [21], [26]. However, the detailed SG model can reflect the operation states of SGs more comprehensively. Thereby, the DSE model was extended based on the consideration of d-axis damping windings and q-axis damping windings, and a 9th-order SG model including an excitation system is proposed for DSE.

Remark 2: generally, in the DSE algorithm based on Kalman filter [21]-[23], the estimation accuracy under cyber attacks is guaranteed by enhancing the robustness of the algo-

rithm. Considering the nonlinear characteristics of the model equation, a TSUKF is proposed to separate the bias caused by cyber attacks. To deal with the deterioration of the state estimation performance caused by mismatches between the statistical characteristics of the measurement noise and model assumptions, a multi-dimensional adaptive factor matrix is derived to modify the measurement noise covariance matrix. On this basis, considering the impact of system fault on noise, the application of adaptive scaling matrix is extended to adaptively modify process noise of attack-free estimation and attack estimation. Compared with the method in [24] and [25], a multi-dimensional adaptive factor matrix is introduced in the proposed ATSUKF to modify the noise statistics, which effectively decreases the error caused by the uncertainty of noise prior statistics.

Algorithm 1: proposed ATSUKF based on adaptive noise correction method

Initialization: parameter initialization

Input: $\boldsymbol{u}_k$, $\boldsymbol{y}_k$, and the number of iterations N_t

While $k=0$ to N_t

Step 1: generate the predicted state of attack-/bias-free estimation by (33)-(39)

Step 2: calculate the scaling matrix $\boldsymbol{S}_{k+1}^{\boldsymbol{x}}$ by (68)-(72) and recalculate the covariance matrix $\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{x}}$

Step 3: obtain the predicted measurement of attack-/bias-free estimation by (42)-(45)

Step 4: obtain the scaling matrix $\boldsymbol{S}_{k+1}$ by (62)-(67) and recalculate the covariance matrix $\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}$

Step 5: complete the attack-/bias-free estimation

$$\tilde{\boldsymbol{x}}_{k+1|k+1}=\tilde{\boldsymbol{x}}_{k+1|k}+\boldsymbol{K}_{k+1}^{\boldsymbol{x}}\left(\boldsymbol{y}_{k+1}-\tilde{\boldsymbol{y}}_{k+1|k}\right)$$

$$\tilde{\boldsymbol{P}}_{k+1|k+1}^{\boldsymbol{x}}=\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{x}}-\boldsymbol{K}_{k+1}^{\boldsymbol{x}}\tilde{\boldsymbol{P}}_{k+1|k}^{\boldsymbol{yy}}\left(\boldsymbol{K}_{k+1}^{\boldsymbol{x}}\right)^{\mathrm{T}}$$

Step 6: generate the predicted state of attack/bias estimation by (48)-(53)

Step 7: obtain the scaling matrix $\boldsymbol{S}_{k+1}^{\boldsymbol{b}}$ by (73)-(78) and recalculate the covariance matrix $\boldsymbol{P}_{k+1|k}^{\boldsymbol{b}}$

Step 8: complete the attack/bias estimation

$$\hat{\boldsymbol{b}}_{k+1|k+1}=\hat{\boldsymbol{b}}_{k+1|k}+\boldsymbol{K}_{k+1}^{\boldsymbol{b}}\left(\boldsymbol{y}_{k+1|k}-\hat{\boldsymbol{y}}_{k+1|k}\right)$$

$$\boldsymbol{P}_{k+1|k+1}^{\boldsymbol{b}}=\boldsymbol{P}_{k+1|k}^{\boldsymbol{b}}-\boldsymbol{K}_{k+1}^{\boldsymbol{b}}\boldsymbol{P}_{k+1|k}^{\boldsymbol{yy}}\left(\boldsymbol{K}_{k+1}^{\boldsymbol{b}}\right)^{\mathrm{T}}$$

Step 9: complete the estimation by utilizing the results of attack/bias estimation and attack-/bias-free estimation

$$\hat{\boldsymbol{x}}_{k+1|k+1}=\tilde{\boldsymbol{x}}_{k+1|k+1}+\boldsymbol{\beta}_{k+1|k+1}\hat{\boldsymbol{b}}_{k+1|k+1}$$

$$\boldsymbol{P}_{k+1|k+1}^{\boldsymbol{x}}=\tilde{\boldsymbol{P}}_{k+1|k+1}^{\boldsymbol{x}}+\boldsymbol{\beta}_{k+1|k+1}\boldsymbol{P}_{k+1|k+1}^{\boldsymbol{b}}\boldsymbol{\beta}_{k+1|k+1}^{\mathrm{T}}$$

Step 10: output $\hat{\boldsymbol{x}}_{k+1|k+1}$ and $\boldsymbol{P}_{k+1|k+1}^{\boldsymbol{x}}$ and update time instant

End while

IV. Numerical Results

To access the performance of the proposed ATSUKF under unknown noise statistics and cyber attack interference, extensive simulations are carried out in the IEEE 39-bus system by using the detailed 9th-order SG model developed in Section II. The topology of IEEE 39-bus system is shown in Fig. 2, and its parameters can be obtained from [38]. PSCAD/EMTDC® is used to simulate the dynamic change process of power system to obtain the real states and measurements. To simulate the system operation, it is assumed that a three-phase grounding fault occurs at Bus 16 when $t=0.5$ s, and the fault is cleared when $t=0.7$ s. Due to space limitation, only the DSE results of Generator 8 (G8) are shown in this section.

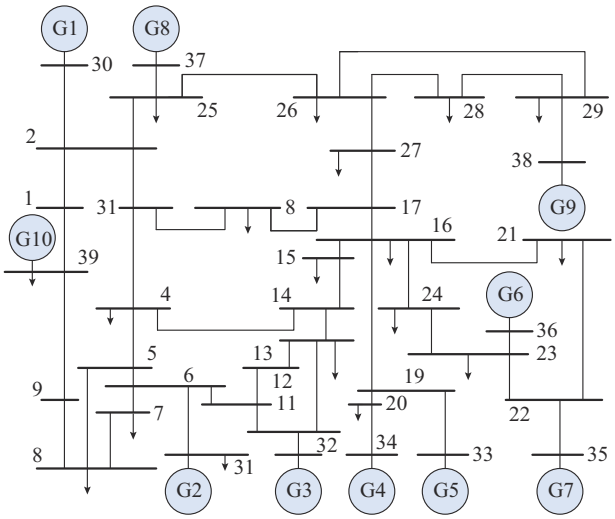

Fig. 2. Topology of IEEE 39-bus system.

Because of the interference of uncertain factors and the change of system operation state, it is difficult for operators to obtain accurate prior knowledge of noise. Furthermore, malicious cyber attacks against power systems will also lead to the deterioration of DSE performance. Consequently, considering the interference of uncertain factors in the actual power system, simulation scenarios are set up as follows.

Scenario 1: the UKF, TSUKF, and proposed ATSUKF are compared and discussed under normal operation conditions.

Scenario 2: the above-mentioned filters are analyzed and compared in the test system with unknown noise statistics.

Scenario 3: the robustness of above-mentioned filters is discussed under the malicious network attack against the measurement data.

In addition, set the number of Monte Carlo simulations N_m as 200. The average state estimation error index E is utilized to appraise the performance of the discussed filters:

$$E=\frac{1}{N_m}\sum_{j=1}^{N_m}\sqrt{\frac{1}{N_t}\sum_{k=1}^{N_t}\left(\hat{x}_{i,k}-x_{i,k}\right)^2} \tag{79}$$

where $x_{i,k}$ is the true value; and $\hat{x}_{i,k}$ is the estimation value.

A. Scenario 1

Without loss of generality, we assume that operators can master the knowledge of system model and accurate prior noise statistics. Assuming that the process noise and measurement noise are zero-mean Gaussian noise, the standard deviations of the process noise and measurement noise are both 10^{-4}. At this time, the actual noise variance matches the system model, and the multi-dimensional adaptive factor matrices are all unity matrices.

The estimation results of rotor speed and rotor angle of G8 are shown in Fig. 3. The estimation results of field winding and damper winding fluxes of G8 are shown in Figs. 4 and 5. By using UKF, TSUKF, and the proposed ATSUKF

to track the states of G8 in Scenario 1, the estimation results of SG excitation system state variables of G8 can be observed in Fig. 6. Additionally, the average estimation error results in Scenario 1 are given in Table I. From the results of numerical simulation, it can be observed that the proposed ATSUKF and TSUKF inherit the advantages of UKF and can accurately track the changes of generator operation states. Notably, because of the bias estimation, the proposed ATSUKF and TSUKF have small deviations from the results of UKF in tracking the state change of the excitation system, which can be ignored. When the actual noise variance matches the system model, the proposed ATSUKF and TSUKF have the same estimation performance.

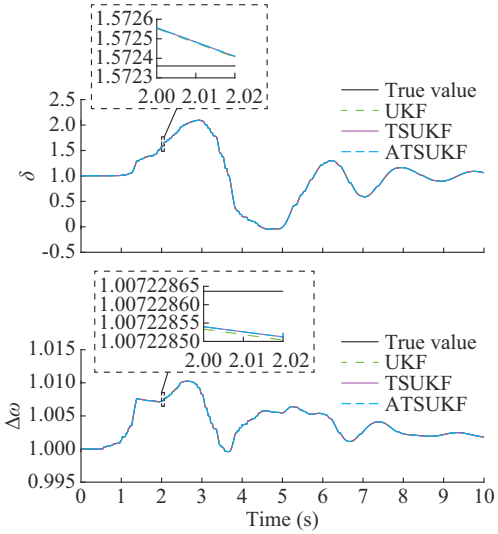

Fig. 3. Estimation results of rotor speed and rotor angle of G8 in Scenario 1.

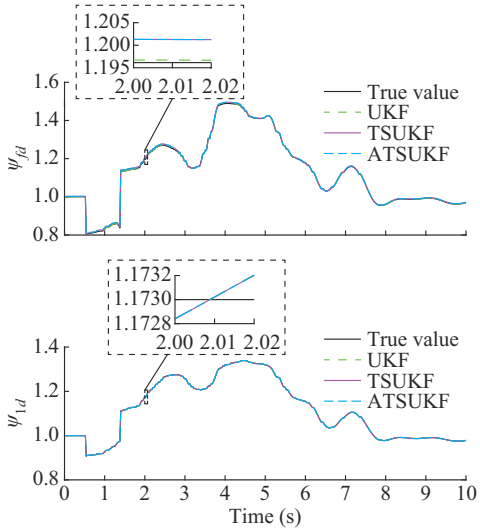

Fig. 4. Estimation results of field winding and *d*-axis damper winding fluxes of G8 in Scenario 1.

B. Scenario 2

In the actual power system, the statistical characteristics of noise are easily disturbed by many factors.

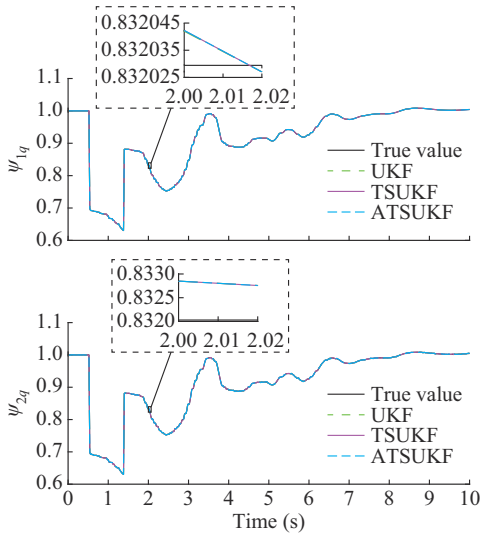

Fig. 5. Estimation results of *q*-axis damper winding fluxes of G8 in Scenario 1.

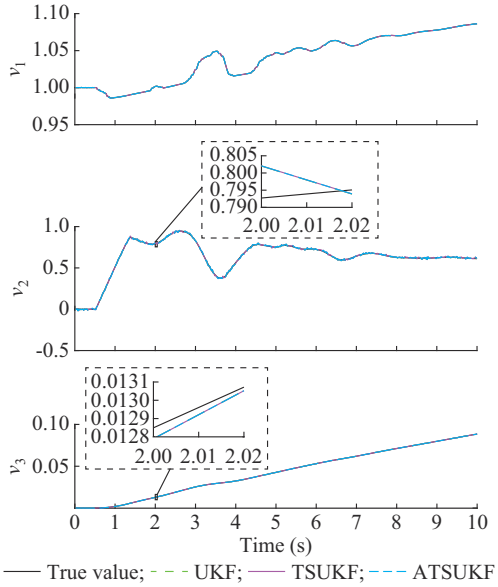

Fig. 6. Estimation results of SG excitation system state variables of G8 in Scenario 1.

TABLE I
AVERAGE ESTIMATION ERROR RESULTS IN SCENARIO 1

Variable	Average estimation error		
	UKF	TSUKF	ATSUKF
δ	0.000097	0.000097	0.000097
ω	0.000096	0.000096	0.000096
ψ_{fd}	0.000368	0.000404	0.000404
ψ_{1d}	0.000168	0.000168	0.000169
ψ_{1q}	0.000021	0.000021	0.000021
ψ_{2q}	0.000713	0.000713	0.000713
v_1	0.000099	0.000099	0.000099
v_2	0.007440	0.007444	0.007445
v_3	0.000102	0.000102	0.000102

Under the interference of uncertain factors such as network attacks, equipment aging, and environmental changes, the prior statistical information of noise cannot be accurately known by the operator, resulting in the mismatch between noise statistics and model assumptions. In order to simulate the influence of this situation on the performance of estimation, it is assumed that the statistical characteristics of noise do not match the model assumptions. The standard deviations of the process noise and measurement noise are set to be 10^{-2} and 10^{-3}, respectively, which deviate from the true values 10^{-4} and 10^{-4}.

The estimation results of field winding fluxes and *d*-axis damper winding fluxes in Scenario 2 are shown in Fig. 7. The estimation results of SG excitation system state variables in Scenario 2 are shown in Fig. 8. It is worth mentioning that UKF and TSUKF perform well in the estimation of δ, ω, ψ_{1q}, and ψ_{2q}. As can be observed in Fig. 7 and Fig. 8, when ψ_{fd} and v_2 are estimated by UKF, the result seriously deviates from the true value and can only track the approximate trend of the change of the state variable. Additionally, the average estimation error results in Scenario 2 are given in Table II. Due to unknown prior noise statistics, TSUKF has errors in the process of no-attack estimation, resulting in inaccurate attack estimation. This problem degrades the estimation performance of TSUKF significantly. Compared with other filters, the proposed ATSUKF can accurately track the dynamic changes of state variables by using multi-dimensional adaptive factor matrices to correct the estimation error covariance.

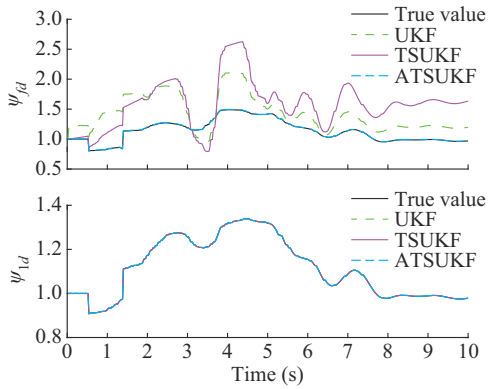

Fig. 7. Estimation results of field winding and *d*-axis damper winding fluxes of G8 in Scenario 2.

C. Scenario 3

Accessing the measurement data has become one of the most common ways to attack power systems. Attackers can compromise the authenticity of data by injecting attack data into the data collected by the measuring device. Once the real measurement is altered, the state estimation results will deviate from the actual state, which will cause the operator to make a wrong decision. The common measurement cyber attack methods include false data injection, scaling attack, data replay attack, and ramp attack. To analyze the effectiveness of state estimation algorithms under cyber attacks, it is assumed that the measurement data v_3 are accessed by multiple types of malicious network attacks.

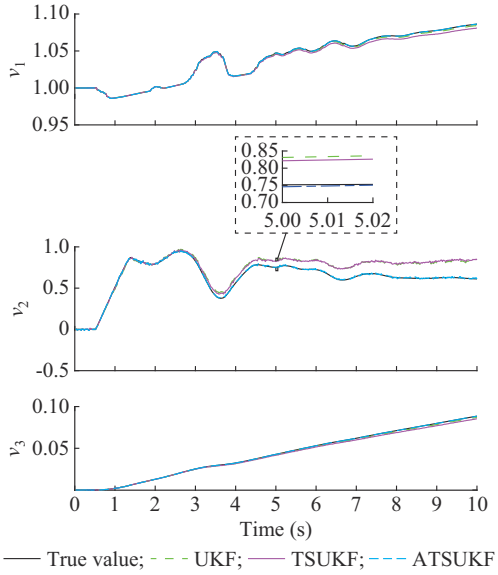

Fig. 8. Estimation results of SG excitation system state variables of G8 in Scenario 2.

TABLE II
AVERAGE ESTIMATION ERROR RESULTS IN SCENARIO 2

Variable	Average estimation error		
	UKF	TSUKF	ATSUKF
δ	0.000255	0.001265	0.000101
ω	0.001021	0.000111	0.000099
ψ_{fd}	0.364208	0.544942	0.003684
ψ_{1d}	0.000174	0.000173	0.000173
ψ_{1q}	0.000176	0.000091	0.000072
ψ_{2q}	0.000708	0.000698	0.000765
v_1	0.001088	0.002760	0.000101
v_2	0.115421	0.117418	0.008041
v_3	0.000813	0.001639	0.000116

The following four attack conditions are considered.

1) Condition 1: the measurement is successfully accessed by FDI at $t=2$ s and the attack stops at $t=8$ s. Once the attack succeeds, false data injection attacks will inject false data $b_k^{FDI}=0.02$ into the measurement.

2) Condition 2: when the measurement device is manipulated by the data replay attack at $t=5$ s, the device will repeatedly transmit the same measurement data.

3) Condition 3: the attacker uses scaling attacks to scale up the measurement after $t=4$ s, and the scaling factor λ_a is set to be 1.5.

4) Condition 4: the attacker uses ramp attacks to inject data into the measurement data after $t=6$ s. The data injected through ramp attacks will grow over time and $r_b=3\times10^{-4}$.

The estimation results of v_3 under FDI attacks are shown in Fig. 9. When the data replay attack occurs, the measurement device will continuously transmit the measurement data from $t=5$ s to replace real measurements. The estimation results of v_3 under data replay attack are shown in Fig. 10.

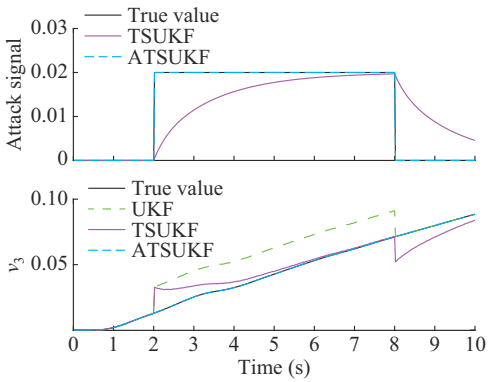

Fig. 9. Estimation results of v_3 under FDI attack.

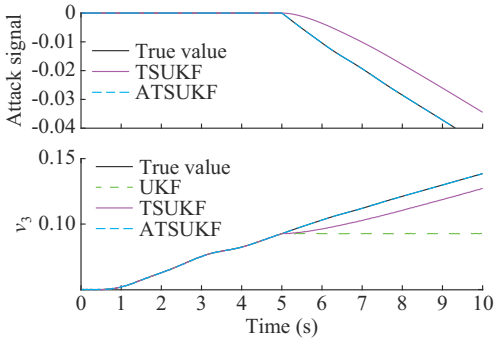

Fig. 10. Estimation results of v_3 under data replay attack.

For the scaling attacks, suppose that the attacker scales up the measurement by using scaling factor $\lambda_a = 1.5$ after $t = 4$ s, and the result comparison is given in Fig. 11. When the ramp attack occurs at $t = 6$ s, the estimation results of v_3 are shown in Fig. 12. Additionally, the average estimation error results of v_3 under four common cyber attacks are given in Table III. As can be observed from the above results, the estimation effect of the proposed ATSUKF is significantly superior to other filters. Since there is no way to separate the deviations caused by cyber attacks during state estimation, UKF is vulnerable to cyber attacks. As expected, due to the inability to update the error covariance matrix, TSUKF cannot quickly and accurately track the attack signal. In contrast, the proposed ATSUKF can adaptively update the covariance matrix during the process of attack/bias estimation to obtain better results.

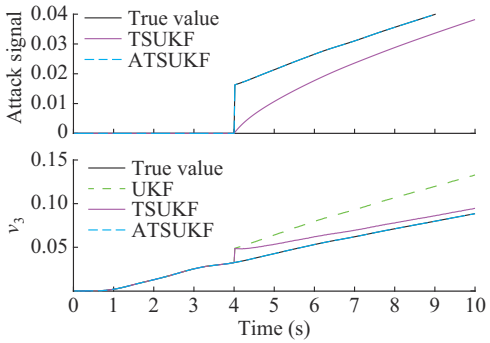

Fig. 11. Estimation results of v_3 under scaling attack.

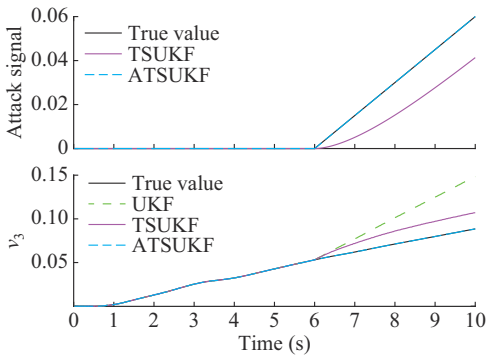

Fig. 12. Estimation results of v_3 under ramp attack.

TABLE III
AVERAGE ESTIMATION ERROR RESULTS IN SCENARIO 3

Attack mode	Average estimation error		
	UKF	TSUKF	ATSUKF
FDI attack	0.015490	0.006696	0.000112
Data replay attack	0.019197	0.006615	0.000132
Scaling attack	0.024678	0.006707	0.000103
Ramp attack	0.021983	0.008893	0.000143

In order to compare the computational efficiency of different filters discussed under different conditions, simulations are implemented on a system with an Intel i7-7700 CPU and 16 GB of RAM in the MATLAB environment. The execution time of different filters under different conditions is shown in Table IV. The results in Table IV are achieved without complete optimization and the computational time can be further reduced by using C code. Since the state and the bias can be estimated in parallel, the proposed ATSUKF and TSUKF exhibit similar computational efficiency to UKF under all designed conditions. A multi-dimensional adaptive factor matrix is introduced in the proposed ATSUKF to modify the noise statistics, which effectively decreases the error caused by the uncertainty of noise prior statistics. Therefore, the computational efficiency of the proposed ATSUKF will be lower than that of TSUKF. It is worth mentioning that when the attacker accesses multiple measurement data simultaneously, the computational burden of attack/bias estimation will further increase and the computational efficiency of the filter will decrease.

TABLE IV
EXECUTION TIME OF DIFFERENT FILTERS UNDER DIFFERENT CONDITIONS

Condition	Execution time (ms)		
	UKF	TSUKF	ATSUKF
Normal operation condition	7565	7617	7693
Unknown noise statistics condition	7670	7651	7728
Condition 1	7850	7961	8014
Condition 2	7849	7919	8187
Condition 3	7992	7988	8210
Condition 4	7940	7957	8203

V. Conclusion

In this study, an adaptive DSE algorithm is proposed against cyber attacks. Considering the nonlinear characteristics of the model equation, a filter is proposed based on the unscented transform technology and two-stage Kalman filtering theory, which can suppress the impact of cyber attacks on the estimation results. On this basis, the adaptive scaling matrix is utilized to modify the error covariance matrix in the estimation process of the TSUKF, which can effectively deal with the problem when the statistical parameters of noise do not match the model assumptions. Compared with other filters, the effectiveness of the proposed ATSUKF is illustrated under cyber attacks.

As it turns out, the proposed ATSUKF can effectively estimate the system state vector and attack vector in parallel. When the statistical parameters of generator model noise are unknown, the proposed ATSUKF is still effective. In the future, we will build more types of cyber attack models and extend the proposed ATSUKF to bound the uncertainty caused by cyber attacks to provide effective information for tracing the source of cyber attacks and formulating defense strategies. In addition, we will design an effective attack detection strategy to distinguish between noise signals and cyber attacks, thereby reducing unnecessary calculations and improving the computational efficiency of the proposed ASUKF.

References

[1] H. Long, Z. Wu, C. Fang *et al*., "Cyber-attack detection strategy based on distribution system state estimation," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 669-678, Jul. 2020.

[2] T. Duan and V. Dinavahi, "Starlink space network-enhanced cyber-physical power system," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3673-3675, Jul. 2021.

[3] C. Chen, K. Zhang, M. Ni *et al*., "Cyber-attack-tolerant frequency control of power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 2, pp. 307-315, Mar. 2021.

[4] M. Ni, M. Li, J. Li *et al*., "Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 3, pp. 477-484, May 2021.

[5] D. Hou, Y. Sun, J. Wang *et al*., "Dynamic state estimation of power systems with uncertainties based on robust adaptive unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 4, pp. 1065-1074, Jul. 2023.

[6] Y. Chen, Y. Yao, Y. Lin *et al*., "Dynamic state estimation for integrated electricity-gas systems based on Kalman filter," *CSEE Journal of Power and Energy Systems*, vol. 8, no. 1, pp. 293-303, Jan. 2022.

[7] H. Karimipour and V. Dinavahi, "Extended Kalman filter-based parallel dynamic state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1539-1549, May 2015.

[8] T. Ahmad and N. Senroy, "An information theoretic approach to power-substation level dynamic state estimation with non-Gaussian noise," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1642-1645, Mar. 2020.

[9] S. Wang, W. Gao, and A. P. S. Meliopoulos, "An alternative method for power system dynamic state estimation based on unscented transform," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 942-950, May 2012.

[10] P. Risbud, N. Gatsis, and A. Taha, "Multi-period power system state estimation with PMUs under GPS spoofing attacks," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 597-606, Jul. 2020.

[11] B. Tan, J. Zhao, and M. Netto, "A general decentralized dynamic state estimation with synchronous generator magnetic saturation," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 960-963, Jan. 2023.

[12] E. Ghahremani and I. Kamwa, "Dynamic state estimation in power system by applying the extended Kalman filter with unknown inputs to phasor measurements," *IEEE Transactions on Power Systems*, vol. 26, no. 4, pp. 2556-2566, Nov. 2011.

[13] Y. Wang, Y. Wang, Y. Sun *et al*., "Resilient dynamic state estimation for multi-machine power system with partial missing measurements," *IEEE Transactions on Power Systems*. doi: 10.1109/TPWRS. 2023. 3287151

[14] Y. Wang, Y. Sun, and V. Dinavahi, "Robust forecasting-aided state estimation for power system against uncertainties," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 691-702, Jan. 2020.

[15] Y. Chakhchoukh, H. Lei, and B. K. Johnson, "Diagnosis of outliers and cyber attacks in dynamic PMU-based power state estimation," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1188-1197, Mar. 2020.

[16] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2725-2735, Nov. 2015.

[17] A. S. L. V. Tummala and R. K. Inapakurthi, "A two-stage Kalman filter for cyber-attack detection in automatic generation control system," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 1, pp. 50-59, Jan. 2022.

[18] H. Liu, F. Hu, J. Su *et al*., "Comparisons on Kalman-filter-based dynamic state estimation algorithms of power systems," *IEEE Access*, vol. 8, pp. 51035-51043, Mar. 2020.

[19] H. Zhao and B. Tian, "Robust power system forecasting-aided state estimation with generalized maximum mixture correntropy unscented Kalman filter," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1-10, Mar. 2022.

[20] W. Ma, J. Qiu, X. Liu *et al*., "Unscented Kalman filter with generalized correntropy loss for robust power system forecasting-aided state estimation," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 11, pp. 6091-6100, Nov. 2019.

[21] Y. Wang, Y. Sun, V. Dinavahi *et al*., "Robust dynamic state estimation of power systems with model uncertainties based on adaptive unscented filter," *IET Generation*, *Transmission & Distribution*, vol. 13, no. 12, pp. 2455-2463, Jun. 2019.

[22] G. Anagnostou and B. C. Pal, "Derivative-free Kalman filtering based approaches to dynamic state estimation for power systems with unknown inputs," *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 116-130, Jan. 2018.

[23] J. Qi, K. Sun, J. Wang *et al*., "Dynamic state estimation for multi-machine power system by unscented Kalman filter with enhanced numerical stability," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1184-1196, Mar. 2018.

[24] J. Xu, Y. Jing, G. M. Dimirovski *et al*., "Two-stage unscented Kalman filter for nonlinear systems in the presence of unknown random bias," in *Proceedings of 2008 American Control Conference*, Seattle, USA, Jun. 2008, pp. 3530-3535.

[25] X. Chen, R. Sun, F. Wang *et al*., "Two-stage unscented Kalman filter algorithm for fault estimation in spacecraft attitude control system," *IET Control Theory & Applications*, vol. 12, no. 13, pp. 1781-1791, Sept. 2018.

[26] Y. Wang, Y. Sun, V. Dinavahi *et al*., "Adaptive robust cubature Kalman filter for power system dynamic state estimation against outliers," *IEEE Access*, vol. 7, pp. 105872-105881, Jul. 2019.

[27] Y. Wang, Z. Yang, Y. Wang *et al*., "Robust dynamic state estimation for power system based on adaptive cubature Kalman filter with generalized correntropy loss," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1-11, May 2022.

[28] S. Cao, N. Lin, and V. Dinavahi, "Faster-than-real-time hardware emulation of extensive contingencies for dynamic security analysis of large-scale integrated AC/DC grid," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 861-871, Jan. 2023.

[29] S. Cao, N. Lin, and V. Dinavahi, "Damping of subsynchronous control interactions in large-scale PV installations through faster-than-real-time dynamic emulation," *IEEE Access*, vol. 9, pp. 128481-128493, Sept. 2021.

[30] G. Valverde, E. Kyriakides, G. T. Heydt *et al*., "Nonlinear estimation of synchronous machine parameters using operating data," *IEEE Transactions on Energy Conversion*, vol. 26, no. 3, pp. 831-839, Sept. 2011.

[31] P. Kundur, N. Balu, and M. Lauby, *Power System Stability and Control*. New York: McGraw-Hill, 1994.

[32] K. Lu and Z. Wu, "Constrained-differential-evolution-based stealthy sparse cyber-attack and countermeasure in an AC smart grid," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5275-5285, Aug. 2022.

[33] K. Lu and Z. Wu, "Genetic algorithm-based cumulative sum method for jamming attack detection of cyber-physical power systems," *IEEE Transactions on Instrumentation Measurement*, vol. 71, p. 3186360, Jan. 2022.
[34] L. Dang, B. Chen, S. Wang *et al*., "Robust power system state estimation with minimum error entropy unscented Kalman filter," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 11, pp. 8797-8808, Nov. 2020.
[35] J. Zhao, J. Qi, Z. Huang *et al*., "Power system dynamic state estimation: motivations, definitions, methodologies, and future work," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3188-3198, Jul. 2019.
[36] S. Wang, W. Zhang, Y. Sun *et al*., "Wind power forecasting in the presence of data scarcity: a very short-term conditional probabilistic modeling framework," *Energy*. doi: 10.1016/j.energy.2024.130305
[37] C. Hajiyev and H. E. Soken, "Robust adaptive Kalman filter for estimation of UAV dynamics in the presence of sensor/actuator faults," *Aerospace Science and Technology*, vol. 28, no. 1, pp. 376-383, Jul. 2013.
[38] C. Canizares, T. Fernandes, E. Geraldi *et al*., "Benchmark models for the analysis and control of small-signal oscillatory dynamics in power systems," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 715-722, Jan. 2017.

Dongchen Hou received the B.S. degree in electrical engineering and automation from North China University of Water Resources and Electric Power, Zhengzhou, China, in 2017. He is currently studying as a Ph.D. in the School of Electrical and Power Engineering, Hohai University, Nanjing, China. His research interests include theoretical and algorithmic studies in power system estimation.

Yonghui Sun received the Ph.D. degree from the City University of Hong Kong, Hong Kong, China, in 2010. He is currently a Professor with the School of Electrical and Power Engineering, Hohai University, Nanjing, China. His research interests include stability analysis and control of power systems, optimal planning and operation of integrated energy system, optimization algorithms, and data analysis.

Venkata Dinavahi received the B. Eng. degree in electrical engineering from Visvesvaraya National Institute of Technology (VNIT), Nagpur, India, in 1993, the M.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT) Kanpur, Kanpur, India, in 1996, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Ontario, Canada, in 2000. He is currently a Professor with the Department of Electrical and Computer Engineering, University of Alberta, Alberta, Canada. He is a Fellow of the Engineering Institute of Canada (EIC) and a Fellow of the Asia-Pacific Artificial Intelligence Association (AAIA). His research interests include real-time simulation of power systems and power electronic systems, electromagnetic transients, device-level modeling, artificial intelligence machine learning, large-scale systems, and parallel and distributed computing.

Yi Wang received the B.S. degree from Luoyang Institute of Science and Technology, Luoyang, China, in 2014, and the Ph.D. degree from Hohai University, Nanjing, China, in 2020. He was a Visiting Scholar at the University of Alberta, Alberta, Canada, between 2018 and 2019. He is currently a Lecturer at Zhengzhou University, Zhengzhou, China. His current research interests include theoretical and algorithmic studies in power system estimation, parameter identification, power system dynamics, signal processing, and cyber security.