Detection and Estimation of False Data Injection Attacks for Load Frequency Control Systems

Jun Ye and Xiang Yu

Abstract—**False data injection attacks (FDIAs) against the load frequency control (LFC) system can lead to unstable operation of power systems. In this paper, the problems of detecting and estimating the FDIAs for the LFC system in the presence of external disturbances are investigated. First, the LFC system model with FDIAs against frequency and tie-line power measurements is established. Then, a design procedure for the unknown input observer (UIO) is presented and the residual signal is generated to detect the FDIAs. The UIO is designed to decouple the effect of the unknown external disturbance on the residual signal. After that, an attack estimation method based on a robust adaptive observer (RAO) is proposed to estimate the state and the FDIAs simultaneously. In order to improve the performance of attack estimation, the H_∞ technique is employed to minimize the effect of external disturbance on estimation errors, and the uniform boundedness of the state and attack estimation errors is proven using Lyapunov stability theory. Finally, a two-area interconnected power system is simulated to demonstrate the effectiveness of the proposed attack detection and estimation algorithms.**

Index Terms—**External disturbance, false data injection attacks, load frequency control, robust adaptive observer, unknown input observer.**

I. Introduction

MAINTAINING the balance between the electricity supply and demand is one of the most important issues in power systems. The power imbalance will lead to the deviation of the grid frequency from its nominal value, which might affect the power system stability and security [1]. Load frequency control (LFC) system is a networked control system which keeps the frequency and power interchanges with neighborhood areas at desired values by adjusting the power outputs of generators [2], [3]. In the LFC system, the input control signal called area control error (ACE) is composed of local-area frequency and tie-line power measurements. By tracking the ACE signal, the power outputs of generators are modified to balance random load fluctuation and then the frequency is maintained within an acceptable range around the nominal value [4], [5].

However, due to the heavy reliance on communication networks, the power system is vulnerable to cyber attacks [6], [7]. Cyber attacks on the LFC system will affect the frequency stability of the system, and even trigger remedial actions such as disconnecting generators or customer loads. Such unexpected actions may cause equipment damage and cascading failures leading to massive blackouts [8]. For instance, in December 2015, Ukrainian power grid suffered a cyber attack, causing a blackout and affecting approximately 225000 customers for several hours [9].

False data injection attack (FDIA) is one of most severe types of cyber attacks on smart grids. A malicious attacker can compromise the communication networks and inject false data into the LFC system, which may cause huge damage to the power system [10]. Therefore, it is of great significance to detect and estimate the FDIAs that may occur in the LFC system.

There have been several detection techniques for FDIAs on LFC systems. For instance, in [11], a new full-order state observer is designed for attack detection. In [12], a distributed interval observer is proposed to detect bias injection attacks. Furthermore, a robust adaptive observer-based algorithm is proposed in [13] to detect the bias load injection attacks. In [14], the FDIAs are detected by checking the consistency between the observed and predicted frequency deviations. In [15], a multi-layer perception classifier based method is introduced to extract the features of ACE signals, thus distinguishing compromised signals from normal ones. In [16], a support vector domain description based method is proposed to extract the features of normal LFC signals and then detect the FDIAs. In [17], the forecasted ACE data are utilized for the detection of FDIAs. In [18], global positioning system (GPS) spoofing attacks on the LFC system are studied. An attack detection technique consisting of a Luenberger observer and an artificial neural network observer is proposed to detect this type of FDIA.

After the attack is detected, the next step is attack estimation. The estimation of the attack vector is very worthwhile to discover the attackers' strategies and helps the decision maker take further actions. In recent years, various types of estimation methods have been proposed. In [19], a dynamic state estimator is proposed to estimate the state and un-

Manuscript received: December 30, 2020; revised: February 22, 2021; accepted: April 22, 2021. Date of CrossCheck: April 22, 2021. Date of online publication: July 14, 2021.

This work was supported by the National Natural Science Foundation of China (No. 61833013) and Key Research and Development Project of Zhejiang Province (No. 2021C03158).

J. Ye is with the Hangzhou Innovation Institute, Beihang University, Hangzhou, China (e-mail: yejunz@126.com).

X. Yu (corresponding author) is with the School of Automation Science and Electrical Engineering, Beihang University, Beijing, China (e-mail: xiangyu_buaa@buaa.edu.cn).

DOI: 10.35833/MPCE.2020.000928

known inputs considering the attacks on phasor measurement units of the power grid. In [20], an adaptive sliding mode observer with online parameter estimators is designed to estimate the state and attack of power systems. An unknown input functional observer is proposed to estimate the dynamic states of the LFC system in [21]. In [22], the attack signal is dealt with an unknown input and estimated using a three-step recursive filter. In [23], a co-estimation of the power system states and attack vector based on unknown input observer and Kalman filter is investigated. In [24], model-free defense strategies are proposed to handle the load altering attack with the aid of reinforcement learning and deep neural network techniques. In addition, the attack estimation is somewhat similar to fault reconstructions. Certain relevant techniques such as adaptive observer [25], [26], disturbance observer [27]-[29], and learning observer [30], [31] can be used.

Although some achievements have been made on the detection and estimation of FDIAs in power systems, some issues still remain to be addressed. ① To detect and estimate the attacks, the system model under FDIAs must be obtained. Thus, how to establish the model of the LFC system with the attacks of frequency and tie-line power measurement needs an explicit investigation. ② Both the abrupt load fluctuation and FDIAs will lead to the abnormal operation of power systems. The above-mentioned methods cannot distinguish the FDIAs from the load variation. The wrong distinction may lead to wrong decisions. ③ The accurate estimation of the FDIAs when the attacks and the load disturbance are mixed together is challenging and has rarely been addressed.

To resolve these shortcomings, this paper focuses on the problems of the detection and estimation of FDIAs for the LFC system. An unknown input observer (UIO) is then developed to detect the FDIAs for the LFC system. Furthermore, inspired by the composite hierarchical anti-disturbance control theory [27], a robust adaptive observer (RAO) is developed to investigate the problem of simultaneously estimating the state and attacks in the presence of the load disturbance.

The main contributions of this paper are listed and discussed as follows.

1) A new model for describing the attacked LFC system is proposed. This model can be used for analyzing the system during the attacks of frequency and tie-line power measurements. Different from the existing research works [15], [22], the attacks of frequency and tie-line power measurements are modeled as a lumped attack in order to attain better detection and estimation performance due to the existence of both disturbances and multiple attacks. Furthermore, three types of FDIAs are modeled and analyzed considering the impact of the attacks on the LFC system.

2) A UIO-based attack detection method against FDIAs is designed for the LFC system. The load fluctuation is modeled as an unknown input and can be completely decoupled from the residual signal. Thus, the residual signal is sensitive to the attacks and robust to the disturbance. FDIAs are then detected by comparing the residual signal and the prescribed threshold.

3) An RAO is developed to estimate the state and the attack signal simultaneously for the LFC system. In order to improve the accuracy of attack estimation, the H_∞ technique is applied and the disturbance attenuation level is minimized by employing the linear matrix inequality (LMI) based optimization approach. The stability of the proposed RAO is proven by using Lyapunov stability theory. Compared with the traditional adaptive observer [32], the proposed RAO can attenuate the influence of the external disturbance on the attack estimation error.

Throughout the paper, the vector norm is defined as $\|\boldsymbol{x}\|=\sqrt{\boldsymbol{x}^{\mathrm{T}}\boldsymbol{x}}$ and the matrix norm is defined as $\|\boldsymbol{A}\|=\sigma_{\max}(\boldsymbol{A})=\sqrt{\lambda_{\max}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})}\,\sigma_{\max}(\boldsymbol{A})$, where $\lambda_{\max}(\boldsymbol{A})$ is the maximum singular value; $\|\boldsymbol{x}\|_2$ is the L_2-norm defined as $\|\boldsymbol{x}\|_2=\sqrt{\int_0^{\infty}\|\boldsymbol{x}\|^2\mathrm{d}t}$; and $\boldsymbol{I}$ is an identity matrix of appropriate dimension. For a matrix $\boldsymbol{Y}$, $sym(\boldsymbol{Y})=\boldsymbol{Y}+\boldsymbol{Y}^{\mathrm{T}}$.

The rest of this paper is organized as follows. Section II presents the modeling and analysis of LFC system subject to FDIAs. Section III presents the UIO-based attack detection. Section IV presents the RAO-based attack estimation. In Section V, simulation results of a two-area power system are presented to illustrate the effectiveness of the proposed UIO-based attack detection and RAO-based attack estimation method. Finally, Section VI concludes this paper.

II. Modeling and Analysis of LFC System Subject to FDIAs

A. LFC System Model

Large power systems usually consist of several power areas connected together by tie-lines. The LFC system is a large-scale networked control system which regulates the power flow between different power areas while keeping the desired frequency and power interchanges at the desired level. The mathematical model of the i^{th} LFC system under FDIAs can be represented by an equivalent linear model [33] shown in Fig. 1.

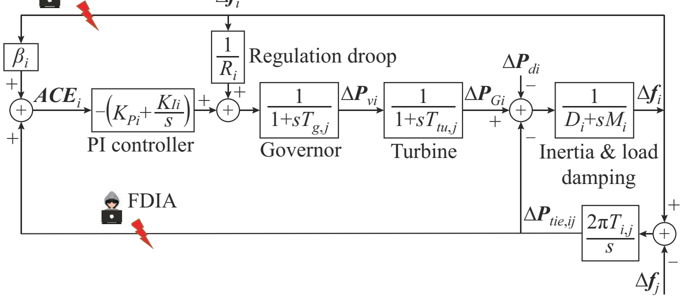

FDIA
$\Delta \boldsymbol{f}_i$
β_i
$\frac{1}{R_i}$
Regulation droop
$\Delta \boldsymbol{P}_{di}$
+
$\boldsymbol{ACE}_i$
$-\left(K_{Pi}+\frac{K_{Ii}}{s}\right)$
+
+
$\frac{1}{1+sT_{g,j}}$
$\Delta \boldsymbol{P}_{vi}$
$\frac{1}{1+sT_{tu,j}}$
$\Delta \boldsymbol{P}_{Gi}$
−
+
$\frac{1}{D_i+sM_i}$
$\Delta \boldsymbol{f}_i$
+
PI controller
Governor
Turbine
−
Inertia & load damping
FDIA
$\Delta \boldsymbol{P}_{tie,ij}$
$\frac{2\pi T_{i,j}}{s}$
+
−
$\Delta \boldsymbol{f}_j$

Fig. 1. Mathematical model of i^{th} LFC system under FDIAs.

According the transfer function given in Fig. 1, it can be obtained that:

$$\begin{cases} \Delta\dot{\boldsymbol{f}}_i = \dfrac{1}{M_i}(\Delta\boldsymbol{P}_{Gi} - D_i\Delta\boldsymbol{f}_i - \Delta\boldsymbol{P}_{di} - \Delta\boldsymbol{P}_{tie,i}) \\ \Delta\dot{\boldsymbol{P}}_{Gi} = \dfrac{1}{T_{tu,i}}(\Delta\boldsymbol{P}_{vi} - \Delta\boldsymbol{P}_{Gi}) \\ \Delta\dot{\boldsymbol{P}}_{vi} = \dfrac{1}{T_{g,i}}\left(\boldsymbol{u}_i - \Delta\boldsymbol{P}_{vi} - \dfrac{1}{R_i}\Delta\boldsymbol{f}_i\right) \\ \Delta\dot{\boldsymbol{P}}_{tie,i} = 2\pi\displaystyle\sum_{j=1,j\neq i}^{n} T_{i,j}\Delta\boldsymbol{f}_i \end{cases} \tag{1}$$

where i is the area number; $\Delta\boldsymbol{P}_{Gi}$, $\Delta\boldsymbol{f}_i$, $\Delta\boldsymbol{P}_{vi}$, $\Delta\boldsymbol{P}_{di}$, and $\Delta\boldsymbol{P}_{tie,i}$ are the generator power deviation, frequency deviation, turbine valve position, load deviation, and tie-line power deviation, respectively; M_i, D_i, R_i ,$T_{g,i}$, and $T_{tu,i}$ are the moment of inertia of generator, speed-drop coefficient, damping coefficient, time constant of the governor, and time constant of the turbine for the i^{th} power area, respectively; $\boldsymbol{u}_i$ is the control input; and $T_{i,j}$ is the stiffness constant between the i^{th} and j^{th} power areas.

Furthermore, the LFC center receives the ACE signal, which is a linear combination of the frequency deviation and tie-line power deviation. Then, the LFC center sends the LFC command to the plants, which can mitigate the power imbalance in power areas, thus achieving the stability of frequency and tie-line power. The ACE signal under attack-free conditions can be defined as:

$$\boldsymbol{ACE}_i = \beta_i\Delta\boldsymbol{f}_i + \Delta\boldsymbol{P}_{tie,i} \tag{2}$$

where β_i is the frequency bias factor. Using the ACE signal as a corresponding control input of load frequency controller, a proportional-integral (PI) controller is designed as:

$$\boldsymbol{u}_i = -K_{Pi}\cdot\boldsymbol{ACE}_i - K_{Ii}\int\boldsymbol{ACE}_i\,\mathrm{d}t \tag{3}$$

where K_{Pi} and K_{Ii} are the proportional and integral gains, respectively.

Combining the above analyses, the state-space equation of the i^{th} LFC power area under attack-free conditions can be described as:

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{Ax}(t) + \boldsymbol{Bu}(t) + \boldsymbol{Ed}(t) \\ \boldsymbol{y}(t) = \boldsymbol{Cx}(t) \end{cases} \tag{4}$$

where $\boldsymbol{x}(t)\in\mathbf{R}^n$, $\boldsymbol{u}(t)\in\mathbf{R}^m$, $\boldsymbol{d}(t)\in\mathbf{R}^d$, and $\boldsymbol{y}(t)\in\mathbf{R}^p$ are the state variable vector, input vector, disturbance vector, and output vector, respectively; $\boldsymbol{x}(t) = \left[\Delta\boldsymbol{f}_i, \Delta\boldsymbol{P}_{Gi}, \Delta\boldsymbol{P}_{vi}, \Delta\boldsymbol{P}_{tie,i}\int\boldsymbol{ACE}_i dt\right]^{\mathrm{T}}$ and $\boldsymbol{y}(t) = \left[\boldsymbol{ACE}_i\,, \int\boldsymbol{ACE}_i dt\right]^{\mathrm{T}}$ are the state variable matrix and output matrix, respectively; and $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, and $\boldsymbol{E}$ are the state, input, output, and disturbance matrices, respectively. These matrices can be determined as:

$$\boldsymbol{A} = \begin{bmatrix} -\dfrac{D_i}{M_i} & \dfrac{1}{M_i} & 0 & -\dfrac{1}{M_i} & 0 \\ 0 & -\dfrac{1}{T_{tu,i}} & \dfrac{1}{T_{tu,i}} & 0 & 0 \\ -\dfrac{1}{R_iT_{g,i}} & 0 & -\dfrac{1}{T_{g,i}} & 0 & 0 \\ 2\pi\displaystyle\sum_{j=1,j\neq i}^{N} T_{i,j} & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 1 & 0 \end{bmatrix} \tag{5}$$

$$\boldsymbol{B} = \begin{bmatrix} 0 & 0 & \dfrac{1}{T_{g,i}} & 0 & 0 \end{bmatrix}^{\mathrm{T}} \tag{6}$$

$$\boldsymbol{C} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ \beta_i & 0 & 0 & 1 & 0 \end{bmatrix} \tag{7}$$

$$\boldsymbol{E} = \begin{bmatrix} -\dfrac{1}{M_i} & 0 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}} \tag{8}$$

The power areas are connected to the centralized LFC system. The LFC system sends control signals to the plants and receives signals through sensor measurements. As depicted in Fig. 1, two main measurements of the LFC system are considered as potential attack targets. The false data can be injected to the tie-line and frequency measurements by intruding the susceptible communication channels. When the measurements of the i^{th} area are attacked by the FDIAs, the ACE signal is modified to:

$$\begin{aligned} \boldsymbol{ACE}_{FDIA,i}(t) = \Delta\boldsymbol{P}_{tie,i}(t) + \boldsymbol{f}_{FDIA,tie}(t) + \beta_i(\Delta\boldsymbol{f}_i(t) + \boldsymbol{f}_{FDIA,fr}(t)) = \\ \boldsymbol{ACE}_{true,i}(t) + \boldsymbol{f}_{FDIA,tie}(t) + \beta_i\boldsymbol{f}_{FDIA,fr}(t) \end{aligned} \tag{9}$$

where $\boldsymbol{ACE}_{FDIA,i}(t)$ and $\boldsymbol{ACE}_{true,i}(t)$ are the compromised and true ACE signals, respectively; and $\boldsymbol{f}_{FDIA,tie}(t)$ and $\boldsymbol{f}_{FDIA,fr}(t)$ are the false signals added to the frequency and tie-line power measurements, respectively.

According to the above analyses, the state-space equation of the i^{th} power area during attacks can be modified as:

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{Ax}(t) + \boldsymbol{Bu}(t) + \boldsymbol{Ed}(t) + \boldsymbol{Ff}_{FDIA}(t) \\ \boldsymbol{y}(t) = \boldsymbol{Cx}(t) \end{cases} \tag{10}$$

where $\boldsymbol{F}$ is the attack matrix; and $\boldsymbol{f}_{FDIA}(t)\in\mathbf{R}^r$ denotes the FDIAs, which can be expressed as:

$$\boldsymbol{F} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{\mathrm{T}} \tag{11}$$

$$\boldsymbol{f}_{FDIA}(t) = \boldsymbol{f}_{FDIA,tie}(t) + \beta_i\boldsymbol{f}_{FDIA,fr}(t) \tag{12}$$

Remark 1: since the ACE signal is the control input of the LFC system and it is a linear combination of the frequency deviation and tie-line power deviation. Either the attack on the frequency measurement or on the tie-line power measurement will be reflected in the ACE signal. Therefore, a lumped attack term is adopted to represent the combined effect of the attacks of frequency and tie-line power measurements.

B. Modeling and Analysis of FDIAs

In this paper, three types of attack modes are considered and listed as follows.

1) Attack mode 1: bias attack on the tie-line power measurement.

In this mode, attackers add certain bias vector on tie-line power measurement. Then, the compromised ACE signal $\boldsymbol{ACE}_{FDIA,i}(t)$, which is used to generate frequency control commands in LFC center of area i, can be expressed as a linear combination of the true measurement $\boldsymbol{ACE}_{true,i}(t)$ and an attack term $\boldsymbol{f}_{bias}(t)$:

$$\boldsymbol{ACE}_{FDIA,i}(t) = \Delta\boldsymbol{P}_{tie,i}(t) + \boldsymbol{f}_{bias}(t) + \beta_i\Delta\boldsymbol{f}_i(t) = \boldsymbol{ACE}_{true,i}(t) + \boldsymbol{f}_{bias}(t) \tag{13}$$

The attack model can be described as:

$$\boldsymbol{f}_{FDIA}(t)=\boldsymbol{f}_{FDIA,tie}(t)=\boldsymbol{f}_{bias}(t) \tag{14}$$

2) Attack mode 2: harmonic attack on the frequency measurement.

In this mode, attackers add harmonic vector on the frequency measurement. The harmonic attack can be expressed as:

$$\boldsymbol{f}_{FDIA,fr}(t)=A_h\sin(w_h t+\varphi) \tag{15}$$

where A_h, w_h, and φ are the amplitude, frequency, and phase of the harmonic attack, respectively.

The attack model can be expressed as:

$$\boldsymbol{f}_{FDIA}(t)=\beta_i\boldsymbol{f}_{FDIA,fr}(t)=\beta_i A_h\sin(w_h t+\varphi) \tag{16}$$

Since the system frequency of the power system usually fluctuates periodically due to load fluctuation, the harmonic attack on the frequency measurement is difficult to detect by the system operator.

3) Attack mode 3: simultaneous attacks on the frequency measurement and tie-line power measurement.

In this mode, attackers inject the bias attack on tie-line power measurement and the harmonic attack on frequency measurement simultaneously. The attack model can be expressed as:

$$\boldsymbol{f}_{FDIA}(t)=\boldsymbol{f}_{FDIA,tie}(t)+\beta_i\boldsymbol{f}_{FDIA,fr}(t)=\boldsymbol{f}_{bias}(t)+\beta_i A_h\sin(w_h t+\varphi) \tag{17}$$

The impacts of FDIAs on power systems are shown in Table I. From this table, it can be observed that the FDIAs will have direct impacts on the power system and may lead to load shedding or generator tripping, which would cause severe damages to the power system. Therefore, detection and estimation of the FDIAs are urgent, which can be achieved by the proposed methods.

TABLE I
IMPACTS OF FDIAS ON POWER SYSTEMS

Attack mode	Direct impact	Indirect impact	Severe impact
Bias attack ($\boldsymbol{f}_{bias}(t)>\boldsymbol{0}$)	Frequency drops below nominal value	Generation deficit and load shedding	Massive blackout
Bias attack ($\boldsymbol{f}_{bias}(t)<\boldsymbol{0}$)	Frequency exceeds nominal value	Generation redundancy and generator tripping	Cascading failures
Harmonic attack	Frequency fluctuation	Load shedding or generator tripping	Massive blackout
Composite attack	Frequency fluctuation	Load shedding or generator tripping	Massive blackout

Remark 2: there exist other types of FDIAs such as scaling attack and ramp attack. In this paper, we only focus on the bias attack and harmonic attack. The modeling and analysis of the FDIAs can lay a good foundation for the attack detection and estimation.

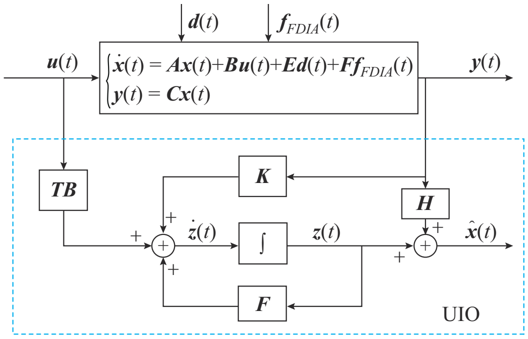
III. UIO-BASED ATTACK DETECTION

A. Design Procedure of UIO

A UIO-based attack detection method is proposed to decouple the external disturbance and detect the FDIAs. The dynamic model of the UIO for the system in (10) can be represented as:

$$\begin{cases}\dot{\boldsymbol{z}}(t)=\boldsymbol{F}\boldsymbol{z}(t)+\boldsymbol{T}\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{K}\boldsymbol{y}(t)\\ \hat{\boldsymbol{x}}(t)=\boldsymbol{z}(t)+\boldsymbol{H}\boldsymbol{y}(t)\end{cases} \tag{18}$$

where $\boldsymbol{z}(t)$ is the state vector of the UIO system; $\hat{\boldsymbol{x}}(t)$ is the estimated state vector of $\boldsymbol{x}(t)$; and $\boldsymbol{F}$, $\boldsymbol{T}$, $\boldsymbol{H}$, and $\boldsymbol{K}$ are the gain matrices, which should be designed to achieve unknown input decoupling. Figure 2 depicts the block diagram of UIO in (18), which has the capability of decoupling the estimation error of the dynamic states from the disturbance in the original system.



$\boldsymbol{d}(t)$
$\boldsymbol{f}_{FDIA}(t)$
$\boldsymbol{u}(t)$
$\begin{cases}\dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{E}\boldsymbol{d}(t)+\boldsymbol{F}\boldsymbol{f}_{FDIA}(t)\\ \boldsymbol{y}(t)=\boldsymbol{C}\boldsymbol{x}(t)\end{cases}$
$\boldsymbol{y}(t)$
$\boldsymbol{TB}$
$\boldsymbol{K}$
$\boldsymbol{H}$
+
+
+
$\dot{\boldsymbol{z}}(t)$
∫
$\boldsymbol{z}(t)$
+
+
$\hat{\boldsymbol{x}}(t)$
$\boldsymbol{F}$
UIO

Fig. 2. Block diagram of UIO for LFC system under FDIAs.

In order to select proper gain matrices for designing the UIO, the state estimation error dynamics can be expanded as:

$$\begin{aligned}\dot{\boldsymbol{e}}(t)=\ &\dot{\boldsymbol{x}}(t)-\dot{\hat{\boldsymbol{x}}}(t)=\\ &(\boldsymbol{A}-\boldsymbol{HCA}-\boldsymbol{K}_1\boldsymbol{C})\boldsymbol{e}(t)+[\boldsymbol{F}-(\boldsymbol{A}-\boldsymbol{HCA}-\boldsymbol{K}_1\boldsymbol{C})]\boldsymbol{z}(t)-\\ &[\boldsymbol{K}_2-(\boldsymbol{A}-\boldsymbol{HCA}-\boldsymbol{K}_1\boldsymbol{C})\boldsymbol{H}]\boldsymbol{y}(t)-[\boldsymbol{T}-(\boldsymbol{I}-\boldsymbol{HC})]\boldsymbol{B}\boldsymbol{u}(t)+\\ &(\boldsymbol{I}-\boldsymbol{HC})\boldsymbol{E}\boldsymbol{d}(t)+(\boldsymbol{I}-\boldsymbol{HC})\boldsymbol{F}\boldsymbol{f}_{FDIA}(t)\end{aligned} \tag{19}$$

where $\boldsymbol{K}=\boldsymbol{K}_1+\boldsymbol{K}_2$. The parametric matrices of the UIO can be obtained by solving:

$$\begin{cases}\boldsymbol{F}=\boldsymbol{A}-\boldsymbol{HCA}-\boldsymbol{K}_1\boldsymbol{C}\\ \boldsymbol{K}_2=(\boldsymbol{A}-\boldsymbol{HCA}-\boldsymbol{K}_1\boldsymbol{C})\boldsymbol{H}\\ \boldsymbol{T}=\boldsymbol{I}-\boldsymbol{HC}\\ (\boldsymbol{I}-\boldsymbol{HC})\boldsymbol{E}=\boldsymbol{0}\end{cases} \tag{20}$$

If the above conditions are satisfied, then the state estimation error dynamics will be:

$$\dot{\boldsymbol{e}}(t)=\boldsymbol{F}\boldsymbol{e}(t)+(\boldsymbol{I}-\boldsymbol{HC})\boldsymbol{F}\boldsymbol{f}_{FDIA}(t) \tag{21}$$

It is clear from (21) that the estimation error is decoupled from the unknown input $\boldsymbol{d}(t)$. If the matrix $\boldsymbol{F}$ is Hurwitz and the system is attack-free, the estimation error of the designed UIO will approach zero asymptotically.

It is proven in [34] that the necessary and sufficient conditions for the existence of the UIO are: ① $rank(\boldsymbol{CE})=rank(\boldsymbol{E})$; ② the pair $(\boldsymbol{C}, \boldsymbol{A}_1)$ is a detectable pair as:

$$\boldsymbol{A}_1=\boldsymbol{A}-\boldsymbol{E}[(\boldsymbol{CE})^{\mathrm{T}}\boldsymbol{CE}]^{-1}(\boldsymbol{CE})^{\mathrm{T}}\boldsymbol{CA} \tag{22}$$

A flow chart that describes the design procedure of the UIO is depicted in Fig. 3. The first step is to check the existence of the UIO by checking whether $rank(\boldsymbol{CE})=rank(\boldsymbol{E})$. If this condition is not met, the UIO does not exist. To solve this problem, the matrix $\boldsymbol{C}$ can be changed by defining new virtual outputs to satisfy the rank condition. If the rank condition is met, the matrices $\boldsymbol{H}$, $\boldsymbol{T}$, and $\boldsymbol{A}_1$ can be calculated. The next step is to check the observability of the pair ($\boldsymbol{C}$, $\boldsymbol{A}_1$). If this condition is satisfied, the matrix $\boldsymbol{K}_1$ can be easily computed by using the pole placement method. Otherwise, a transformation matrix $\boldsymbol{P}_1$ should be constructed by performing the observable canonical decomposition method on the pair ($\boldsymbol{C}$, $\boldsymbol{A}_1$), as demonstrated in (23) and (24).

$$\boldsymbol{P}_1\boldsymbol{A}_1\boldsymbol{P}_1^{-1}=\begin{bmatrix}\boldsymbol{A}_{11} & \boldsymbol{0}\\ \boldsymbol{A}_{12} & \boldsymbol{A}_{22}\end{bmatrix}\quad \boldsymbol{A}_{11}\in\mathbf{R}^{n_1\times n_1} \tag{23}$$

$$\boldsymbol{C}\boldsymbol{P}_1^{-1}=\begin{bmatrix}\boldsymbol{C}^* & \boldsymbol{0}\end{bmatrix}\quad \boldsymbol{C}^*\in\mathbf{R}^{m\times n_1} \tag{24}$$

where n_1 is the rank of the observability matrix for the pair ($\boldsymbol{C}$, $\boldsymbol{A}_1$) in which the pair ($\boldsymbol{C}^*$, $\boldsymbol{A}_{11}$) is observable. The unobservable modes are combined in the eigenvalues of $\boldsymbol{A}_{22}$. More details about the observable canonical decomposition method can be found in [35].

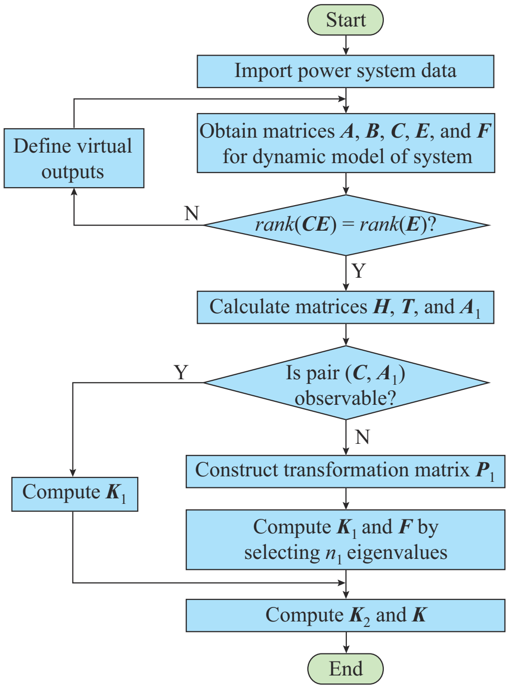

Start
Import power system data
Obtain matrices A, B, C, E, and F for dynamic model of system
Define virtual outputs
N
rank(CE) = rank(E)?
Y
Calculate matrices H, T, and A1
Y
Is pair (C, A1) observable?
N
Construct transformation matrix P1
Compute K1
Compute K1 and F by selecting n1 eigenvalues
Compute K2 and K
End

Fig. 3. Flow chart of design procedure of UIO.

B. Residual Generation

In order to use the UIO for attack detection purposes, a residual signal is needed. In this paper, the difference between the measured output and estimated output is considered as a residual signal.

$$\boldsymbol{r}(t)=\boldsymbol{y}(t)-\hat{\boldsymbol{y}}(t)=\boldsymbol{C}(\boldsymbol{x}(t)-\hat{\boldsymbol{x}}(t))=\boldsymbol{C}\boldsymbol{e}_x(t) \tag{25}$$

where $\boldsymbol{r}(t)$ and $\hat{\boldsymbol{y}}(t)$ are the residual and estimated output vectors, respectively. It can be seen from (21) and (25) that the residual signal will converge to zero with the state estimation error $\boldsymbol{e}_x(t)$ approaching zero in the absence of FDIAs. When FDIAs occur, the residual signal will deviate from zero if the gain matrix $\boldsymbol{H}$ is designed such that $(\boldsymbol{I}-\boldsymbol{HC})\boldsymbol{F}\neq 0$. Then, the detection logic under FDIAs can be expressed as:

$$A_{larm}=\begin{cases}1 & |\boldsymbol{r}(t)|>\alpha\\ 0 & |\boldsymbol{r}(t)|\le\alpha\end{cases} \tag{26}$$

where $A_{larm}=1$ means the FDIAs have been injected into the LFC system and $A_{larm}=0$ otherwise; and α is the detection threshold, which set to be zero under ideal conditions. However, due to the existence of estimation errors and measurement noises, the threshold should be set to a small value to avoid false positive alarms.

Remark 3: the threshold selection is very important since a high threshold would result in high false negative rates and a low threshold would result in high false positive rates (FPR). The detection threshold can be set either by minimizing false attack detection rate under attack-free conditions, or by using hypothesis testing methods such as χ^2-test [36]. In this paper, an empirical method [37] is applied to obtain the threshold value of the proposed attack detection algorithm as follows.

Step 1: define a maximum acceptable FPR.

Step 2: generate measurement noises based on the noise distribution.

Step 3: increase the detection threshold from zero until the FPR meets the desired FPR, e.g., 1%. This step is done to fine tune the detection thresholds for a low FPR.

Step 4: perform the above process (*Steps 2* and *3*) for a large number of trials due to the random nature of measurements noises.

Step 5: obtain the mean values of the detection thresholds for the trials.

Step 6: select the mean value of the detection thresholds as the final detection threshold.

Note that the system model could contain uncertainties, e.g., the parameter uncertainty. The uncertainties would influence the detection accuracy of the UIO. One method to deal with the uncertainties is to obtain a priori knowledge of the upper and lower bounds of the uncertainties. Then, the detection threshold can be adaptively adjusted according to the upper and lower bounds. For example, the adaptive threshold can be obtained by using the L_2-norm method [11]. FDIAs can be detected by comparing the residual signal with the adaptive threshold.

IV. RAO-BASED ATTACK ESTIMATION

A. Observer Design

For system (10), a robust adaptive attack observer can be designed as:

$$\begin{cases}\dot{\hat{\boldsymbol{x}}}(t)=\boldsymbol{A}\hat{\boldsymbol{x}}(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{F}\hat{\boldsymbol{f}}_{FDIA}(t)+\boldsymbol{L}(\boldsymbol{y}(t)-\hat{\boldsymbol{y}}(t))\\ \hat{\boldsymbol{y}}(t)=\boldsymbol{C}\hat{\boldsymbol{x}}(t)\\ \hat{\boldsymbol{f}}_{FDIA}(t)=\varGamma\boldsymbol{Q}(\dot{\boldsymbol{e}}_y(t)+\sigma\boldsymbol{e}_y(t))\end{cases} \tag{27}$$

where $\hat{\boldsymbol{f}}_{FDIA}(t)$ is the attack estimate vector; $\boldsymbol{e}_y(t)=\boldsymbol{y}(t)-\hat{\boldsymbol{y}}(t)$ is the output error vector; $\varGamma>0$ is a positive learning ratio; $\boldsymbol{L}\in\mathbf{R}^{n\times p}$ is the observer gain matrix; $\boldsymbol{Q}\in\mathbf{R}^{r\times p}$ is the matrix to be determined; and σ is the positive scalar.

The state estimate error $\boldsymbol{e}_x(t)$, output estimate error $\boldsymbol{e}_y(t)$, and attack estimate error $\boldsymbol{e}_f(t)$ can be defined as:

$$\begin{cases} \boldsymbol{e}_x(t)=\boldsymbol{x}(t)-\hat{\boldsymbol{x}}(t) \\ \boldsymbol{e}_y(t)=\boldsymbol{y}(t)-\hat{\boldsymbol{y}}(t) \\ \boldsymbol{e}_f(t)=\boldsymbol{f}_{FDIA}(t)-\hat{\boldsymbol{f}}_{FDIA}(t) \end{cases} \tag{28}$$

Then, the error dynamics is described by:

$$\begin{cases} \dot{\boldsymbol{e}}_x(t)=(\boldsymbol{A}-\boldsymbol{LC})\boldsymbol{e}_x(t)+\boldsymbol{Ed}(t)+\boldsymbol{Fe}_f(t) \\ \dot{\boldsymbol{e}}_y(t)=\boldsymbol{Ce}_x(t) \end{cases} \tag{29}$$

B. Stability Analysis

Before the main results are presented, three assumptions and a lemma are given.

Assumption 1: pair $(\boldsymbol{A}, \boldsymbol{C})$ is observable and $rank(\boldsymbol{CF})=rank(\boldsymbol{F})=r$.

Assumption 2: the load disturbance $\boldsymbol{d}(t)\in \boldsymbol{L}_2[0,\infty)$ is bounded, i.e., $\|\boldsymbol{d}(t)\|_2\le d_1$, where d_1 is an unknown constant.

Assumption 3: the derivative of $\boldsymbol{f}_{FDIA}(t)$ with respect to time is norm bounded, i.e.,

$$\left\|\dot{\boldsymbol{f}}_{FDIA}(t)\right\|\le f_1 \tag{30}$$

where $f_1>0$ is an unknown constant. It is evident that the aforementioned three types of FDIAs satisfy this assumption.

Lemma 1 [32]: given a scalar $\mu>0$ and a symmetric positive definite matrix $\boldsymbol{G}$, the inequality (31) holds.

$$2\boldsymbol{x}^{\mathrm{T}}\boldsymbol{y}\le \frac{1}{\mu}\boldsymbol{x}^{\mathrm{T}}\boldsymbol{Gx}+\mu\boldsymbol{y}^{\mathrm{T}}\boldsymbol{G}^{-1}\boldsymbol{y} \quad \boldsymbol{x},\boldsymbol{y}\in \mathbf{R}^n \tag{31}$$

Theorem 1: consider system (10). Under Assumptions 1-3 and given scalars $\sigma,\mu,\gamma>0$, if there exist positive definite symmetric matrices $\boldsymbol{P}\in\mathbf{R}^{n\times n}$, $\boldsymbol{G}\in\mathbf{R}^{r\times r}$, and other matrices $\boldsymbol{Y}\in\mathbf{R}^{n\times p}$ and $\boldsymbol{Q}\in\mathbf{R}^{r\times p}$, such that the following conditions hold:

$$\begin{bmatrix} sym(\boldsymbol{PA}-\boldsymbol{YC})+\boldsymbol{C}^{\mathrm{T}}\boldsymbol{C} & -\dfrac{1}{\sigma}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{PF}-\boldsymbol{C}^{\mathrm{T}}\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{F}) & \boldsymbol{PE} \\ * & -\dfrac{2}{\sigma}\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PF}+\dfrac{1}{\sigma\mu}\boldsymbol{G} & \dfrac{1}{\sigma}\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PE} \\ * & * & -\gamma^2\boldsymbol{I} \end{bmatrix}<\boldsymbol{0} \tag{32}$$

$$\boldsymbol{F}^{\mathrm{T}}\boldsymbol{P}=\boldsymbol{QC} \tag{33}$$

where $*$ represents the symmetric elements in a symmetric matrix, then the proposed robust adaptive observer (27) with $\boldsymbol{Y}=\boldsymbol{PL}$ can ensure that the state estimate error $\boldsymbol{e}_x(t)$ and the attack estimate error $\boldsymbol{e}_f(t)$ are uniformly bounded and output estimate error for the external disturbance satisfies the H_∞ performance $\|\boldsymbol{e}_y(t)\|_2\le\gamma\|\boldsymbol{d}(t)\|_2$.

Proof: consider the following Lyapunov function as:

$$\boldsymbol{V}(t)=\boldsymbol{e}_x^{\mathrm{T}}(t)\boldsymbol{Pe}_x(t)+\frac{1}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\mathit{\Gamma}^{-1}\boldsymbol{e}_f(t) \tag{34}$$

The derivative of the Lyapunov candidate with respect to time can be derived as:

$$\begin{aligned} \dot{\boldsymbol{V}}(t)=&\dot{\boldsymbol{e}}_x^{\mathrm{T}}(t)\boldsymbol{Pe}_x(t)+\boldsymbol{e}_x^{\mathrm{T}}(t)\boldsymbol{P}\dot{\boldsymbol{e}}_x(t)+\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\mathit{\Gamma}^{-1}\dot{\boldsymbol{e}}_f(t)= \\ &\boldsymbol{e}_x[(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}(\boldsymbol{A}-\boldsymbol{LC})]\boldsymbol{e}_x(t)+2\boldsymbol{e}_x^{\mathrm{T}}\boldsymbol{PFe}_f(t)+ \\ &2\boldsymbol{e}_x^{\mathrm{T}}\boldsymbol{PEd}(t)-\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}\boldsymbol{Q}(\dot{\boldsymbol{e}}_y(t)+\sigma\boldsymbol{e}_y(t))+\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\mathit{\Gamma}^{-1}\dot{\boldsymbol{f}}_{FDIA}(t) \end{aligned} \tag{35}$$

According to (33), we can obtain:

$$-\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{Q}(\dot{\boldsymbol{e}}_y(t)+\sigma\boldsymbol{e}_y(t))=-\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}\boldsymbol{F}^{\mathrm{T}}\boldsymbol{P}(\dot{\boldsymbol{e}}_x(t)+\sigma\boldsymbol{e}_x(t)) \tag{36}$$

Substituting (36) into (35) yields:

$$\begin{aligned} \dot{\boldsymbol{V}}(t)=&\dot{\boldsymbol{e}}_x^{\mathrm{T}}(t)\boldsymbol{Pe}_x(t)+\boldsymbol{e}_x^{\mathrm{T}}(t)\boldsymbol{P}\dot{\boldsymbol{e}}_x(t)+\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\mathit{\Gamma}^{-1}\dot{\boldsymbol{e}}_f(t)= \\ &\boldsymbol{e}_x(t)[(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}(\boldsymbol{A}-\boldsymbol{LC})]\boldsymbol{e}_x(t)+2\boldsymbol{e}_x^{\mathrm{T}}\boldsymbol{PEd}(t)- \\ &\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{PFe}_x(t)-\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PFe}_f^{\mathrm{T}}(t)- \\ &\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PEd}(t)+\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\mathit{\Gamma}^{-1}\dot{\boldsymbol{f}}_{FDIA}(t) \end{aligned} \tag{37}$$

From Lemma 1 and Assumption 3, we can obtain:

$$\begin{aligned} &\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\mathit{\Gamma}^{-1}\dot{\boldsymbol{f}}_{FDIA}(t)\le\frac{1}{\sigma\mu}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{Ge}_f(t)+\frac{\mu}{\sigma}\dot{\boldsymbol{f}}_{FDIA}^{\mathrm{T}}(t)\mathit{\Gamma}^{-1}\boldsymbol{G}\mathit{\Gamma}^{-1}\dot{\boldsymbol{f}}_{FDIA}(t)\le \\ &\quad\frac{1}{\sigma\mu}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{Ge}_f(t)+\frac{\mu}{\sigma}f_1^2\lambda_{\max}(\mathit{\Gamma}^{-1}\boldsymbol{G}\mathit{\Gamma}^{-1}) \end{aligned} \tag{38}$$

Substituting (38) into (37), we can further obtain:

$$\begin{aligned} \dot{\boldsymbol{V}}(t)\le&\boldsymbol{e}_x(t)[(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}(\boldsymbol{A}-\boldsymbol{LC})]\boldsymbol{e}_x(t)+2\boldsymbol{e}_x^{\mathrm{T}}\boldsymbol{PEd}(t)- \\ &\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{PFe}_x(t)-\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PFe}_f^{\mathrm{T}}(t)- \\ &\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PEd}(t)+\frac{1}{\sigma\mu}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{Ge}_f(t)+\frac{\mu}{\sigma}f_1^2\lambda_{\max}(\mathit{\Gamma}^{-1}\boldsymbol{G}\mathit{\Gamma}^{-1}) \end{aligned} \tag{39}$$

To guarantee that the proposed adaptive observer is robust to the external unknown disturbance $\boldsymbol{d}(t)$, an H_∞ performance index function is introduced as:

$$\boldsymbol{J}=\int_0^\infty[\boldsymbol{e}_y^{\mathrm{T}}(t)\boldsymbol{e}_y(t)-\gamma^2\boldsymbol{d}^{\mathrm{T}}(t)\boldsymbol{d}(t)]\,\mathrm{d}t \tag{40}$$

Under the zero initial conditions, we have $\boldsymbol{V}(0)=\boldsymbol{0}$ and $\boldsymbol{V}(\infty)\ge\boldsymbol{0}$, which leads to:

$$\begin{aligned} \boldsymbol{J}=&\int_0^\infty[\boldsymbol{e}_y^{\mathrm{T}}(t)\boldsymbol{e}_y(t)-\gamma^2\boldsymbol{d}^{\mathrm{T}}(t)\boldsymbol{d}(t)+\dot{\boldsymbol{V}}(t)]\,\mathrm{d}t-\boldsymbol{V}(\infty)+ \\ &\boldsymbol{V}(0)\le\int_0^\infty[\boldsymbol{e}_y^{\mathrm{T}}(t)\boldsymbol{e}_y(t)-\gamma^2\boldsymbol{d}^{\mathrm{T}}(t)\boldsymbol{d}(t)+\dot{\boldsymbol{V}}(t)]\,\mathrm{d}t \end{aligned} \tag{41}$$

It follows from (41) that:

$$\begin{cases} \begin{aligned} &\boldsymbol{e}_y^{\mathrm{T}}(t)\boldsymbol{e}_y(t)-\gamma^2\boldsymbol{d}^{\mathrm{T}}(t)\boldsymbol{d}(t)+\dot{\boldsymbol{V}}(t)\le \\ &\quad\boldsymbol{e}_x(t)[(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}(\boldsymbol{A}-\boldsymbol{LC})+\boldsymbol{C}^{\mathrm{T}}\boldsymbol{C}]\boldsymbol{e}_x(t)+ \\ &\quad 2\boldsymbol{e}_x^{\mathrm{T}}\boldsymbol{PEd}(t)-\gamma^2\boldsymbol{d}^{\mathrm{T}}(t)\boldsymbol{d}(t)-\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{PFe}_x(t)- \\ &\quad\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PFe}_f^{\mathrm{T}}(t)-\frac{2}{\sigma}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PEd}(t)+ \\ &\quad\frac{1}{\sigma\mu}\boldsymbol{e}_f^{\mathrm{T}}(t)\boldsymbol{Ge}_f(t)+\frac{\mu}{\sigma}f_1^2\lambda_{\max}(\mathit{\Gamma}^{-1}\boldsymbol{G}\mathit{\Gamma}^{-1})= \\ &\quad\boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\Xi}\boldsymbol{\xi}+\frac{\mu}{\sigma}f_1^2\lambda_{\max}(\mathit{\Gamma}^{-1}\boldsymbol{G}\mathit{\Gamma}^{-1}) \end{aligned} \\ \boldsymbol{\Xi}=\begin{bmatrix} sym(\boldsymbol{P}(\boldsymbol{A}-\boldsymbol{LC}))+\boldsymbol{C}^{\mathrm{T}}\boldsymbol{C} & -\dfrac{1}{\sigma}(\boldsymbol{A}-\boldsymbol{LC})^{\mathrm{T}}\boldsymbol{PF} & \boldsymbol{PE} \\ * & -\dfrac{2}{\sigma}\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PF}+\dfrac{1}{\sigma\mu}\boldsymbol{G} & -\dfrac{1}{\sigma}\boldsymbol{F}^{\mathrm{T}}\boldsymbol{PE} \\ * & * & -\gamma^2\boldsymbol{I} \end{bmatrix} \\ \boldsymbol{\xi}=[\boldsymbol{e}_x(t) \quad \boldsymbol{e}_f(t) \quad \boldsymbol{d}(t)]^{\mathrm{T}} \end{cases} \tag{42}$$

If conditions (32) and (33) hold, we can obtain:

$$J=\int_0^{\infty}[\boldsymbol{e}_y^{\mathrm{T}}(t)\boldsymbol{e}_y(t)-\gamma^2\boldsymbol{d}^{\mathrm{T}}(t)\boldsymbol{d}(t)]\,\mathrm{d}t< \int_0^{\infty}\left[-\varepsilon\|\boldsymbol{\xi}\|^2+\frac{\mu}{\sigma}f_1^2\lambda_{\max}(\Gamma^{-1}\boldsymbol{G}\Gamma^{-1})\right]\mathrm{d}t \tag{43}$$

where $\varepsilon=\lambda_{\min}(-\boldsymbol{\Xi})$. Then $J<0$, which indicates $\left\|\boldsymbol{e}_y(t)\right\|_2\leq\gamma\|\boldsymbol{d}(t)\|_2$ for :

$$\varepsilon\|\boldsymbol{\xi}\|^2>\frac{\mu}{\sigma}f_1^2\lambda_{\max}(\Gamma^{-1}\boldsymbol{G}\Gamma^{-1}) \tag{44}$$

Note that Theorem 1 is deduced from the three assumptions and Lemma 1. Specially, Assumption 1 provides a sufficient condition for the existence of the robust adaptive observer. Assumption 2 is used to illustrate the existence of the H_∞ performance index in Theorem 1. Assumption 3 and Lemma 1 are used to deduce (38).

Therefore, both the state estimate error $\boldsymbol{e}_x(t)$ and the attack estimate error $\boldsymbol{e}_f(t)$ converge to a small set while the output estimate error $\boldsymbol{e}_y(t)$ for the external disturbance $\boldsymbol{d}(t)$ satisfies the H_∞ performance $\left\|\boldsymbol{e}_y(t)\right\|_2\leq\gamma\|\boldsymbol{d}(t)\|_2$. This completes the proof.

Remark 4: as illustrated in Theorem 1, compared with the traditional adaptive observer [32], the RAO can suppress the impact of the external disturbance on the attack estimation error. In addition, different from the disturbance observer-based methods [29], the attacks of frequency and tie-line power measurements are modeled as a lumped attack and can be estimated under the condition that the derivative of the attack is bounded.

Remark 5: the effect of the disturbance $\boldsymbol{d}(t)$ on the output estimate error $\boldsymbol{e}_y(t)$ is bounded by the value of γ. The accuracy of state and attack estimations increases with a decrease in the value of γ. Therefore, the robustness of the proposed adaptive observer can be enhanced by minimizing γ. The minimum γ can be obtained by solving the following optimization problem:

$$\begin{cases}\min\gamma^2\\ \text{s.t. (32) and (33)}\end{cases} \tag{45}$$

Remark 6: in Theorem 1, the condition (32) can be solved by using standard LMI toolbox. However, it is difficult to solve (32) and (33) simultaneously. To solve this problem, we can transform (33) into the following LMI-based convex optimization problem:

$$\begin{cases}\min\eta\\ \text{s.t.}\ \begin{bmatrix}\eta\boldsymbol{I} & \boldsymbol{F}^{\mathrm{T}}\boldsymbol{P}-\boldsymbol{QC}\\ * & \eta\boldsymbol{I}\end{bmatrix}>\boldsymbol{0}\end{cases} \tag{46}$$

With this method, a sufficiently small positive scalar η can be selected such that matrices $\boldsymbol{P}$ and $\boldsymbol{Q}$ can be computed to make $\boldsymbol{F}^{\mathrm{T}}\boldsymbol{P}$ approximately equal to $\boldsymbol{QC}$ with satisfactory accuracy.

Using (46), we can transform (45) into the following optimization problem:

$$\begin{cases}\min(\gamma^2+\rho\eta)\\ \text{s.t. (32)}\\ \quad\begin{bmatrix}\eta\boldsymbol{I} & \boldsymbol{F}^{\mathrm{T}}\boldsymbol{P}-\boldsymbol{QC}\\ * & \eta\boldsymbol{I}\end{bmatrix}>\boldsymbol{0}\end{cases} \tag{47}$$

where ρ is a constant that is large enough to guarantee that the optimal value of η is a sufficiently small positive scalar. This optimization problem seeks two objectives. The first one is to find proper matrices $\boldsymbol{P}$, $\boldsymbol{G}$, $\boldsymbol{Y}$, and $\boldsymbol{Q}$ such that the proposed adaptive observer can ensure that the state estimate error $\boldsymbol{e}_x(t)$ and the attack estimate error $\boldsymbol{e}_f(t)$ are uniformly bounded. The other objective is to boost the robustness of the observer against the external disturbance $\boldsymbol{d}(t)$ by minimizing the disturbance attenuation level γ while satisfying the relevant constraints.

V. Simulation Results

In this section, the effectiveness of the proposed detection and estimation methods is illustrated with a two-area interconnected power system. The classical LFC model in Fig. 1 is used. The stiffness constant between the two areas is $T_{1,2}=0.2$. The parameters of two-area interconnected power system are listed in Table II. Attackers compromise the measurements in area 1, while the measurements in area 2 are intact. The load fluctuation is considered as:

$$d(t)=\begin{cases}0 & 0\leq t\leq 5\\ 0.02 & 5<t\leq 20\\ 0.03 & 20<t\leq 40\\ 0 & 40<t\leq 60\end{cases} \tag{48}$$

TABLE II
Parameters of Two-area Interconnected Power System

Area i	M_i	D_i	R_i	$T_{g,i}$	$T_{tu,i}$	β_i
1	10	1.0	0.05	0.10	0.3	21.0
2	12	1.5	0.05	0.17	0.4	21.5

Several simulation scenarios have been carried out for the three aforementioned attack modes. The bias attack on the tie-line power measurement is considered as:

$$f_{bias}(t)=\begin{cases}0 & 0\leq t\leq 10\\ 0.05 & 10<t\leq 30\\ 0 & 30<t\leq 60\end{cases} \tag{49}$$

The harmonic attack on the frequency measurement is considered as:

$$f_{har}(t)=\begin{cases}0 & 0\leq t\leq 20\\ 0.002\sin(3t-10) & 20<t\leq 40\\ 0 & 40<t\leq 60\end{cases} \tag{50}$$

A. Simulation Results of Attack Detection

In this subsection, the performance of the proposed UIO-based attack detection scheme is investigated. Firstly, the existence of the UIO has been checked by validating the rank condition, $rank(\boldsymbol{CE})=rank(\boldsymbol{E})=1$. Then, the residual used for designing the attack detector in the LFC system is chosen as the error between the measured ACE signal and the estimated ones. The simulation results for the three attack modes are shown in Fig. 4.

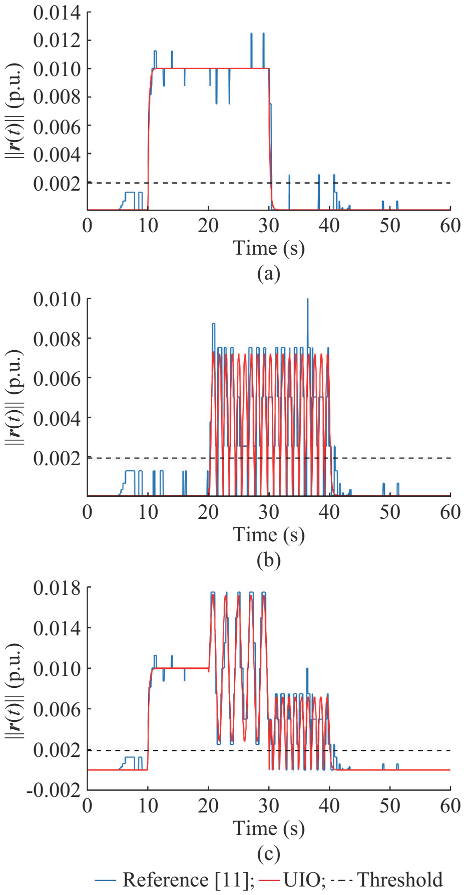


Fig. 4. Simulation results for three attack modes. (a) Bias attack. (b) Harmonic attack. (c) Composite attack.

The threshold is chosen to be higher than the maximum value of these residuals in case of no attacks. As shown in Fig. 4, the attack signals can be immediately detected by comparing the norm of the residuals with the predefined threshold. To demonstrate the superiority of the proposed attack detection method, a comparison between the proposed UIO-based detection method and the detection method designed in [11] is conducted. The comparison results shown in Fig. 4 reveal that the accuracy of attack detection of the UIO is much higher than the observer designed in [11]. The reason lies in that the observer designed in [11] cannot decouple the residual signal from the disturbance and the residual exceeds the threshold at certain times under attack-free conditions.

In order to assess the robustness of the proposed approach against the measurement noises, a Gaussian white noise with zero mean and covariance matrix $\boldsymbol{Q}=0.002\boldsymbol{I}$ is added to the measurement vector. The maximum acceptable FPR is set to be 0.5%. By using the proposed threshold selection method, the threshold is set to be 0.19×10^{-2} p.u.. The detection results for the three types of FDIAs are shown in Fig. 5. As can be seen, before the attacks occur, the residuals are always below the threshold and thus, no detection alarm is issued. However, when the attacks are launched, the residual signals exceed the threshold. Therefore, it can be concluded that the designed attack detection scheme can effectively detect the occurrence of FDIAs in the presence of measurement noises.

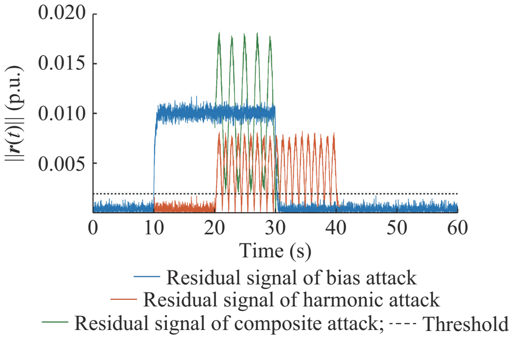


Fig. 5. Detection results for three types of FDIA.

B. Simulation Results of Attack Estimation

In this subsection, the accuracy of the proposed RAO-based attack estimation scheme is studied. For the RAO (27), the parameters are chosen such that $\sigma=1$, $\mu=1$, $\varGamma=0.01$. Using Theorem 1 and solving (47), we can obtain:

$$\left\{\begin{aligned}
&\eta=6.0320\times10^{-11}\\
&\gamma=1.0448\times10^{-3}\\
&\boldsymbol{P}=10^{6}\times\begin{bmatrix}0.0320 & 0.0000 & 0.0000 & 0.0000 & 0.0000\\ 0.0000 & 3.4244 & -0.0050 & 0.0000 & 0.0000\\ 0.0000 & -0.0050 & 3.4393 & 0.0000 & -0.0012\\ 0.0000 & 0.0000 & 0.0000 & 3.4217 & 0.0059\\ 0.0000 & 0.0000 & -0.0012 & 0.0059 & 3.6604\end{bmatrix}\\
&\boldsymbol{L}=\begin{bmatrix}75.4214 & 0.0859 & -13.8640 & 70.8911 & 0.0146\\ 0.0003 & -2.8280 & 1.6609 & -0.0000 & -0.0000\\ -0.1149 & 1.6634 & -9.5052 & 0.0002 & 0.0001\\ 0.5920 & 0.0000 & -0.0002 & 0.5000 & -0.0007\\ 41.0013 & 0.0005 & 0.0005 & 0.9988 & 0.3722\end{bmatrix}
\end{aligned}\right. \tag{51}$$

The simulation results shown in Figs. 6-8 indicate that the proposed RAO leads to an accurate estimation for the bias, harmonic and composite attacks with the load disturbance. However, as shown in Figs. 6-8, the estimation accuracy of the traditional adaptive observer (AO) [32] or the adaptive sliding mode observer (ASMO) [38] is much lower than that of the RAO with the same disturbance. By combining the above simulation results, we can see that the proposed RAO is not disturbance-sensitive. The reason lies in that the proposed RAO can attenuate the influence of the external disturbance on the attack estimation error, and therefore it can be concluded that the proposed observer is robust to the external disturbance.

Furthermore, to demonstrate the effectiveness of the proposed method more quantitatively, the root mean squared error (RMSE) is utilized as a measure to evaluate the accuracy of the observers. The RMSE for the attack signals is calculated using the following formula:

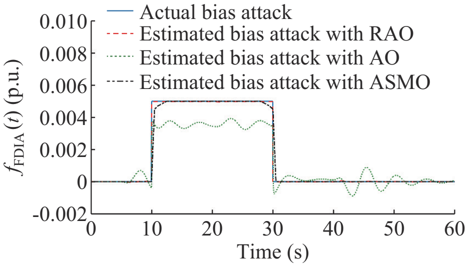


Fig. 6. Bias attack and its estimate with RAO, traditional AO, and ASMO.

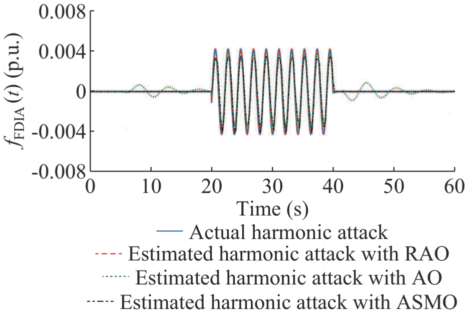


Fig. 7. Harmonic attack and its estimate with RAO, traditional AO, and ASMO.

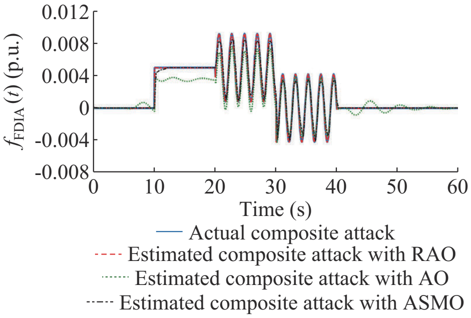


Fig. 8. Composite attack and its estimate with RAO, traditional AO, and ASMO

$$RMSE=\sqrt{\frac{\sum_{t=1}^{m}\left(f_{FDIA}(t)-\hat{f}_{FDIA}(t)\right)^2}{m}} \tag{52}$$

where m is the total number of sample points. A Gaussian white noise with zero mean and covariance matrix $\boldsymbol{Q}=0.002\boldsymbol{I}$ is also added to the measurement vector. The RMSEs for the three types of estimated attack signals using the RAO and traditional adaptive observer are shown in Table III. It is observed that the proposed method is superior for its higher accuracy in the estimation of the attack signals in the presence of measurement noises.

TABLE III
COMPARISON BETWEEN PROPOSED RAO AND TRADITIONAL AO

Attack mode	RMSE with traditional AO	RMSE with proposed RAO	Improvement rate (%)
Bias attack	0.009699	0.004175	56.95
Harmonic attack	0.005879	0.003884	33.93
Composite attack	0.010121	0.004166	58.83

VI. CONCLUSION

In this paper, the problem of cyber attacks on the LFC system is studied. Firstly, the dynamic model of the LFC system subject to external disturbance and FDIAs is established and three attack modes are modeled and analyzed considering the FDIAs on frequency measurements and tie-line power measurements. Then, an attack detection and an attack estimation algorithm are proposed for the LFC system in the presence of FDIAs. Based on the UIO, a design procedure for the residual generation to detect the attack is presented. By designing the parameters in the observer, the unknown external disturbance is decoupled from the residual signal. An RAO-based attack estimation method is proposed to estimate the state and the attack signal simultaneously. In order to improve the robustness against the external disturbance, the H_∞ technique is introduced by minimizing the disturbance attenuation level. Finally, three attack modes are simulated with a two-area power system. The simulation results show that the proposed detection method is able to effectively detect the attacks and the estimation method can accurately estimate the attacks for the LFC system in the presence of the external unknown disturbance. How to mitigate the impact of FDIAs on the LFC system will become our next consideration.

REFERENCES

[1] K. Liao and Y. Xu, “A robust load frequency control scheme for power systems based on second-order sliding mode and extended disturbance observer,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3076-3086, Jul. 2018.

[2] K. Lu, G. Zeng, X. Luo *et al.*, “An adaptive resilient load frequency controller for smart grids with DoS attacks,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 4689-4699, May 2020.

[3] T. N. Pham, H. Trinh, and L. V. Hien, “Load frequency control of power systems with electric vehicles and diverse transmission links using distributed functional observers,” *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 238-252, Jun. 2016.

[4] S. Wen, X. Yu, Z. Zeng *et al.*, “Event-triggering load frequency control for multiarea power systems with communication delays,” *IEEE Transactions on Industrial Electronics*, vol. 63, no. 2, pp. 1308-1317, Feb. 2016.

[5] R. Patel, L. Meegahapola, L. Wang *et al.*, “Automatic generation control of multi-area power system with network constraints and communication delays,” *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 3, pp. 454-463, May 2020.

[6] C. Zhou, B. Hu, Y. Shi *et al.*, “A unified architectural approach for cyberattack-resilient industrial control systems,” *Proceedings of the IEEE*, vol. 109, no. 4, pp. 1-25, Nov. 2020.

[7] E. Kontouras, A. Tzes, and L. Dritsas, “Set-theoretic detection of data corruption attacks on cyber physical power systems,” *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 872-886, Sept. 2018.

[8] G. Liang, S. R. Weller, J. Zhao *et al.*, “The 2015 Ukraine blackout: implications for false data injection attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, Jul. 2017.

[9] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580-591, Mar. 2014.

[10] C. Peng, J. Li, and M. Fei, “Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 4110-4118, Sept. 2017.

[11] X. Luo, Q. Yao, X. Wang *et al.*, “Observer-based cyber attack detection and isolation in smart grids,” *International Journal of Electrical Power & Energy Systems*, vol. 101, pp. 127-138, Oct. 2018.

[12] X. Luo, X. Wang, M. Zhang *et al.*, “Distributed detection and isolation of bias injection attack in smart energy grid via interval observer,” *Applied Energy*, vol. 256, p. 113703, Dec. 2019.

[13] X. Wang, X. Luo, X. Pan *et al.*, "Detection and location of bias load injection attack in smart grid via robust adaptive observer," *IEEE Systems Journal*, vol. 14, no. 3, pp. 4454-4465, Sept. 2020.

[14] R. Tan, H. H. Nguyen, Y. S. Foo *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609-1624, Jul. 2017.

[15] C. Chen, K. Zhang, K. Yuan *et al.*, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932-1941, May 2018.

[16] W. Bi, K. Zhang, Y. Li *et al.*, "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2859-2868, Sept. 2019.

[17] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2023-2031, Jun. 2020.

[18] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad *et al.*, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951-7962, Sept. 2020.

[19] A. F. Taha, J. Qi, J. Wang *et al.*, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 886-899, Mar. 2018.

[20] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory & Applications*, vol. 10, no. 12, pp. 1458-1468, Aug. 2016.

[21] H. H. Alhelou, M. E. H. Golshan, and N. D. Hatziargyriou, "A decentralized functional observer based optimal LFC considering unknown inputs, uncertainties, and cyber-attacks," *IEEE Transactions on Power Systems*, vol. 34, no. 6, pp. 4408-4417, Nov. 2019.

[22] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4985-4995, Sept. 2019.

[23] Z. Kazemi, A. A. Safavi, F. Naseri *et al.*, "A secure hybrid dynamic-state estimation approach for power systems under false data injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7275-7286, Dec. 2020.

[24] C. Chen, M. Cui, X. Fang *et al.*, "Load altering attack-tolerant defense strategy for load frequency control system," *Applied Energy*, vol. 280, p. 116015, Oct. 2020.

[25] B. Jiang, J. Wang, and Y. C. Soh, "An adaptive technique for robust diagnosis of faults with independent effects on system outputs," *International Journal of Control*, vol. 75, no. 11, pp. 792-802, Oct. 2002.

[26] J. Zhang, A. K. Swain, and S. K. Nguang, "Robust H_∞ adaptive descriptor observer design for fault estimation of uncertain nonlinear systems," *Journal of the Franklin Institute*, vol. 351, no. 11, pp. 5162-5181, Sept. 2014.

[27] L. Guo and W. Chen, "Disturbance attenuation and rejection for systems with nonlinearity via DOBC approach," *International Journal of Robust and Nonlinear Control*, vol. 15, no. 3, pp. 109-125, Dec. 2005.

[28] L. Guo and S. Cao, "Anti-disturbance control theory for systems with multiple disturbances: a survey," *ISA Transactions*, vol. 53, no. 4, pp. 846-849, Jan. 2014.

[29] W. Chen, J. Yang, L. Guo *et al.*, "Disturbance-observer-based control and related methods – an overview," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 2, pp. 1083-1095, Sept. 2016.

[30] Q. Jia, W. Chen, Y. Zhang *et al.*, "Robust fault reconstruction via learning observers in linear parameter-varying systems subject to loss of actuator effectiveness," *IET Control Theory & Applications*, vol. 8, no. 1, pp. 42-50, Sept. 2014.

[31] Q. Jia, W. Chen, Y. Zhang *et al.*, "Fault reconstruction and accommodation in linear parameter-varying systems via learning unknown-input observers," *Journal of Dynamic Systems, Measurement, and Control*, vol. 137, no. 6, pp. 1-9, Jan. 2015.

[32] Z. Ke, B. Jiang, and C. Vincent, "Adaptive observer-based fast fault estimation," *International Journal of Control, Automation, and Systems*, vol. 6, no. 3, pp. 320-326, Jun. 2008.

[33] J. Liu, Y. Gu, L. Zha *et al.*, "Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1665-1678, Aug. 2019.

[34] J. Chen and R. J. Patton, *Robust Model-based Fault Diagnosis for Dynamic Systems*. New York: Springer Science & Business Media, 1999.

[35] H. H. Alhelou, M. E. H. Golshan, and J. Askari-Marnani, "Robust sensor fault detection and isolation scheme for interconnected smart power systems in presence of RER and EVs using unknown input observer," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 682-694, Jul. 2018.

[36] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396-1407, Jul. 2014.

[37] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636-1646, Jul. 2016.

[38] A. Taherkhani and F. Bayat, "Wind turbines robust fault reconstruction using adaptive sliding mode observer," *IET Generation, Transmission & Distribution*, vol. 13, no. 14, pp. 3096-3104, Jul. 2019.

Jun Ye received his B.Sc., M.Sc., and Ph.D degrees in electrical engineering from Wuhan University, Wuhan, China, in 2010, 2012, and 2018, respectively. He is now a Postdoctoral Research Fellow with Hangzhou Innovation Institute, Beihang University, Hangzhou, China. His research interests include modeling and stability analysis of power systems.

Xiang Yu received his B.Sc., M.Sc., and Ph.D. degrees in automation science and engineering from Northwestern Polytechnical University, Xi'an, China, in 2003, 2004, and 2008, respectively. He is currently a Professor with the School of Automation Science and Electrical Engineering, Beihang University, Beijing, China. He was a Postdoctoral Research Fellow with the Department of Electrical and Computer Engineering, Western University, London, Canada, and a Research Associate with the Department of Mechanical, Industrial and Aerospace Engineering, Concordia University, Montreal, Canada. He was a recipient of the Recruitment Program for Young Professionals, the Best Paper and Best Paper Finalist at international conferences. He has also served as the Associate Editor of Asian Journal of Control, Associate Editor of Chinese Journal of Aeronautics, Program Co-chair, Invitation Chair, and IPC Member of several academic conferences. His current research interests include safety control of aerospace engineering systems and control of unmanned aerial vehicles and power systems.