International Journal of Innovative
Computing, Information and Control
Volume **20**, Number **6**, December **2024**

ICIC International ©2024 ISSN 1349-4198
pp. 1555–1572

OBSERVER-BASED SECURE DISTRIBUTED SLIDING MODE CONTROL FOR A MULTI-AREA INTERCONNECTED POWER SYSTEM UNDER FALSE DATA INJECTION ATTACKS

Zengbo Shen[1], Dezhi Xu[2,*], Tinglong Pan[1], Weilin Yang[1] and Dongnian Jiang[3]

[1]School of Internet of Things Engineering
Jiangnan University
No. 1800, Lihu Avenue, Wuxi 214122, P. R. China
6211920006@stu.jiangnan.edu.cn; {tlpan; wlyang}@jiangnan.edu.cn

[2]School of Electrical Engineering
Southeast University
No. 2, Sipailou, Xuanwu District, Nanjing 210096, P. R. China
*Corresponding author: xudezhi@seu.edu.cn

[3]School of Electrical Engineering and Information Engineering
Lanzhou University of Technology
No. 36, Pengjiaping Road, Qilihe District, Lanzhou 730050, P. R. China
jiangdn@lut.edu.cn

Received January 2024; revised April 2024

Abstract. *In the load frequency control (LFC) strategy, regions compromised by attackers pose a potential threat to the power system. In this paper, distributed sliding mode control based on the robust asymptotic estimation observer (RAEO) and attack compensation under false data injection (FDI) attacks is designed. The system state and FDI attacks can be estimated effectively via the robust observer. Based on the estimation of the FDI attacks, attack compensation is devised to mitigate the influence of FDI attacks on the system frequency. Then, a distributed sliding mode control is formulated to maintain the stable operation of the system when FDI attacks occur. Finally, the effectiveness of the control scheme is validated through an experimental platform. According to the experimental results, it is proved that the control strategy can improve the performance of the power system under FDI attacks.*

Keywords: Multi-area interconnected power system, FDI attacks, Robust asymptotic estimation observer, Distributed integral sliding mode control

1. **Introduction.** In order to maintain the frequency stability of the power system, it is necessary to ensure the balance of active power in the system. With the rapid development of communication and control technologies, modern power systems are gradually evolving into multi-area power systems with multiple areas connected to each other [1]. Any imbalance in power can result in the grid frequency deviating from its designated nominal value, potentially jeopardizing the stability and security of the entire power system [2, 3]. The design and operation of power systems are significantly improved by load frequency control (LFC) strategy. A well-designed infrastructure and effectively managed power system must be capable of withstanding load disturbances while ensuring acceptable and economical power quality [4, 5]. Moreover, load change will induce corresponding deviations in the system frequency, leading to corresponding adjustments in the generated power [6, 7, 8]. Many methods have been used in the power system, e.g., classical PI

DOI: 10.24507/ijicic.20.06.1555

control, robust control, predictive control, and sliding mode control [9, 10, 11, 12]. All methods are used to keep the system frequency at a stable value.

However, the LFC system, as a cyber-physical system, relies on communication technologies for data collection and control output and is therefore subject to cyber attacks [13, 14, 15]. As an example, the extensive power disruption resulting from malevolent cyber-physical attacks resulted in substantial losses in Ukraine in 2015 [16]. The safe and stable operation of the power system is directly related to the development of the country, once the power industry suffers cyber attacks, it may not only lead to information leakage, but also trigger the paralysis of social production, transportation and other aspects of the country, which is a serious threat to the security and stability of the country. Numerous incidents of cyber attacks have been reported in power systems, such as false data injection (FDI) attacks [17, 18] and denial-of-service (DoS) attacks [19, 20]. Hence, it is crucial to explore methods for improving the performance of the power system when cyber attacks occur.

There have been several detection techniques for FDI attacks on LFC systems. For instance, in [21], the detection of FDI attacks is accomplished by employing a Kalman filter in conjunction with an evolutionary game model for attack detection. In [3], a method for detecting FDI attacks using residual signals from unknown input observers is proposed. A sliding mode observer with online parameter estimation is devised to identify the system state and detect unknown attacks in [22]. However, these methods only serve the purpose of attack detection. A three-step recursive filter is utilized for estimating the FDI attacks in [23]. In [24], a robust adaptive observer is designed to estimate the FDI attacks simultaneously. In [25], a method based on intermediate observer is introduced to calculate the FDI attacks. And the intermediate variables can be used to calculate the load deviations. Unfortunately, these methods solely focus on the estimation of FDI attacks, neglecting considerations for compensation.

In addition, studies on cyber attacks targeting systems have primarily concentrated on the detection and compensation of attacks [26, 27, 28]. In [29], a control strategy based on observer-derived output feedback is introduced to estimate and compensate FDI attack signals. In [30], the security model free adaptive controller is proposed to keep the system stability under FDI attacks. To guarantee the secure operation of the system, a secure distributed load frequency control scheme is investigated in [31]. Improving the performance of power systems under FDI attacks poses a significant significance, considering the adverse effects that cyberattacks can have on power systems.

Motivated by these discussions, this paper focuses on FDI attack detection and compensation. Robust asymptotic estimation observer-based attack compensation and distributed integral sliding mode control are proposed for the multi-area load frequency control system, which can stabilize the system frequency. Experimental results in dSPACE MicroLabBox 1202 demonstrate the proposed method has good steady and dynamic performance. The main contributions and innovations are listed as follows.

1) Based on $L_2 - L_\infty$ performance and the pole configuration conditions, robust asymptotic estimation observers are designed in each control region separately, which can estimate the system state and FDI attacks rapidly.

2) As a combination of attack estimates and actual measured output, the compensation outputs are designed to counteract the FDI attacks acting on the sensor channel and provide the basis for the subsequent design of the slide mode surface.

3) Distributed adaptive integral sliding mode control is devised to reduce the impact of load disturbance and improve the performance of the system when FDI attacks occur.

The remainder of this paper is organized as follows. In Section 2, the structure of a multi-area power system under FDI attacks is formulated, and several lemmas and assumptions

are proposed. In Section 3, the robust asymptotic estimation observer and distributed integral sliding mode control are designed. In Section 4, the experimental results show that the proposed robust asymptotic estimation observer can track FDI attacks more quickly than another observer in [25]. Meanwhile, the power system can operate stably under the distributed integral sliding mode control with attack compensation. Conclusions are provided in Section 5.

2. **Problem Description.** A multi-area interconnected power system consists of multiple control areas, and each area exchanges energy through tie-lines. In this paper, the schematic of the three-area interconnected power system is established in Figure 1.

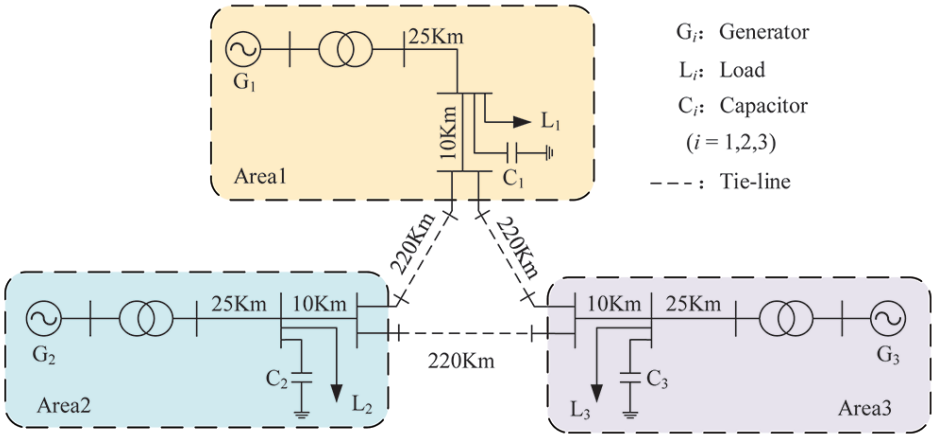


FIGURE 1. Schematic of the three-area interconnected power system

2.1. **Model of LFC system.** The interconnected power system is characterized as a sophisticated nonlinear dynamic system due to its susceptibility to minor load disturbances during routine operational states. The LFC within each area is designed to maintain a consistent local frequency and power interchange with other interconnected areas. By ensuring this constancy, the dynamic characteristics of the power system can be accurately depicted through the utilization of a linearized model that approximates its operational point. In this paper, an equivalent generator is simplified to streamline the representation of generators within each area. The schematic depiction of the model for the ith control area of the power system is shown in Figure 2.

The notations and their actual physical meanings are as follows. Δf_i, ΔP_{ti}, ΔP_{gi}, ΔP_{ci} and $\Delta P_{tie,i}$ are the deviation of frequency, generator output power, governor valve position, unit power command and tie-line power, respectively. ΔP_{di} is the load disturbances. T_{ti}, T_{gi} and T_{ij} are the turbine time constant, governor time constant and interconnection gain between areas i and j, respectively. H_i and D_i are the inertia and damping coefficient of generator. β_i, R_i and K_i are the frequency bias factor, speed control gain and integral coefficient, respectively.

In each area, the dynamic equation of the syatem can be expressed as

$$\Delta \dot{f}_i(t) = -\frac{D_i}{H_i}\Delta f_i(t) + \frac{1}{H_i}\Delta P_{ti}(t) - \frac{1}{H_i}\Delta P_{tie,i}(t) - \frac{1}{H_i}\Delta P_{di}(t) \tag{1}$$

$$\Delta \dot{P}_{ti}(t) = -\frac{1}{T_{ti}}\Delta P_{ti}(t) + \frac{1}{T_{ti}}\Delta P_{gi}(t) \tag{2}$$

$$\Delta \dot{P}_{gi}(t) = -\frac{1}{R_i T_{gi}}\Delta f_i(t) - \frac{1}{T_{gi}}\Delta P_{gi}(t) - \frac{1}{T_{gi}}u_i(t) \tag{3}$$

$$\Delta\dot{P}_{tie,i}(t) = 2\pi \sum_{j\neq i}^{N} T_{ij}\left(\Delta f_i(t) - \Delta f_j(t)\right) \tag{4}$$

$$ACE_i(t) = \beta_i \Delta f_i(t) + \Delta P_{tie,i}(t) \tag{5}$$

$$\Delta\dot{P}_{ci}(t) = -K_i ACE_i(t) \tag{6}$$

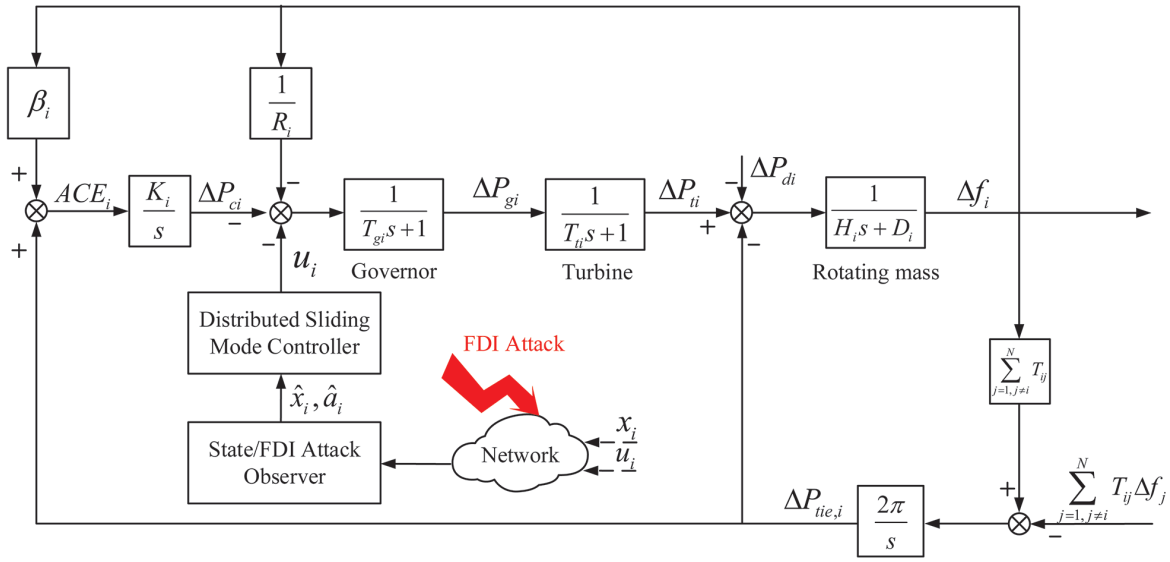


FIGURE 2. The ith control area of the power system

Synthesizing (1)-(6), the system model is written as

$$\begin{cases} \dot{x}_i(t) = A_{ii}x_i(t) + B_i u_i(t) + \sum_{j=1,j\neq i}^{N} A_{ij}x_j(t) + h_i(t) \\ y_i(t) = C_i x_i(t) \end{cases} \tag{7}$$

where $x_i(t) \triangleq \left[\ \Delta f_i(t) \quad \Delta P_{ti}(t) \quad \Delta P_{gi}(t) \quad \Delta P_{ci}(t) \quad \Delta P_{tie,i}(t)\ \right]^T$,

$$A_{ii} \triangleq \begin{bmatrix} -\frac{D_i}{H_i} & \frac{1}{H_i} & 0 & 0 & -\frac{1}{H_i} \\ 0 & -\frac{1}{T_{ti}} & \frac{1}{T_{ti}} & 0 & 0 \\ -\frac{1}{R_i T_{gi}} & 0 & -\frac{1}{T_{gi}} & -\frac{1}{T_{gi}} & 0 \\ K_i\beta_i & 0 & 0 & 0 & K_i \\ 2\pi\sum_{j\neq i}^{N} T_{ij} & 0 & 0 & 0 & 0 \end{bmatrix}, \quad B_i \triangleq \begin{bmatrix} 0 \\ 0 \\ -\frac{1}{T_{gi}} \\ 0 \\ 0 \end{bmatrix}, \quad h_i = \begin{bmatrix} -\frac{\Delta P_{di}}{H_i} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$A_{ij} \triangleq \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{ij} & 0 & 0 & 0 & 0 \end{bmatrix}, \quad C_i \triangleq \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Moreover, $x_i(t) \in \mathbb{R}^n$ and $y_i(t) \in \mathbb{R}^m$ are the system state and the output measurement value, respectively. h_i is the system disturbance.

2.2. **FDI attacks against LFC system.** Data transmitted by sensors over the network is susceptible to malicious tampering through FDI attacks, which will affect the security control performance. When the transmission in area i is attacked, $a_i(t) \in \mathbb{R}^p$ is defined as the FDI attacks, and the system dynamic model can be expressed as

$$\begin{cases} \dot{x}_i(t) = A_{ii}x_i(t) + B_i u_i(t) + \sum\limits_{j=1, j\neq i}^{N} A_{ij}x_j(t) + h_i(t) \\ y_i(t) = C_i x_i(t) + E_i a_i(t) \end{cases} \tag{8}$$

where E_i is the constant matrix of the appropriate dimension.

Construct the following matrices:

$$\bar{x}_i(t) = \begin{bmatrix} x_i(t) \\ a_i(t) \end{bmatrix}, \quad \bar{I}_n = \begin{bmatrix} I_n & 0 \\ 0 & 0 \end{bmatrix}, \quad \bar{A}_{ii} = \begin{bmatrix} A_{ii} & 0 \\ 0 & 0 \end{bmatrix}, \quad \bar{B}_i = \begin{bmatrix} B_i \\ 0 \end{bmatrix},$$
$$\bar{A}_{ij} = \begin{bmatrix} A_{ij} & 0 \\ 0 & 0 \end{bmatrix}, \quad \bar{h}_i = \begin{bmatrix} h_i \\ 0 \end{bmatrix}, \quad \bar{C}_i = \begin{bmatrix} C_i & E_i \end{bmatrix}$$

where I_n is an n-dimensional identity matrix, and (8) can be written as

$$\begin{cases} \bar{I}_n \dot{\bar{x}}_i(t) = \bar{A}_{ii}\bar{x}_i(t) + \bar{B}_i u_i(t) + \sum\limits_{j=1, j\neq i}^{N} \bar{A}_{ij}\bar{x}_j(t) + \bar{h}_i(t) \\ y_i(t) = \bar{C}_i \bar{x}_i(t) \end{cases} \tag{9}$$

2.3. **Some lemmas and assumptions.** For the convenience of proof, the correlation lemmas and assumptions are given.

Lemma 2.1. [32] *The eigenvalues of the matrix $A \in \mathbb{R}^{n\times n}$ are contained within the circular region $\mathcal{D}(\varepsilon, \tau)$ with a center at $\varepsilon + j0$ and a radius of τ if and only if there exists a symmetric positive-definite matrix $P \in \mathbb{R}^{n\times n}$ that satisfies*

$$\begin{bmatrix} -P & PA - \varepsilon P \\ * & -\tau^2 P \end{bmatrix} < 0 \tag{10}$$

Assumption 2.1. *The states of the system are all measurable.*

Assumption 2.2. *The aggregated uncertainties $h_i(t)$ are bounded, which satisfy $\|h_i(t)\| \leq d_i$, where d_i is a positive number.*

Assumption 2.3. *The constraints on the derivatives of FDI attacks are bounded.*

$$\|\dot{a}_i(t)\| \leq \theta_i$$

where $\theta_i \geq 0$ is a positive number.

3. **Main Results.** In this section, an LFC strategy using robust asymptotic estimation observer-based distributed sliding mode control is presented. Robust asymptotic estimation observer is established to estimate the state of the system and FDI attacks. Then the attack estimations are used for attack compensation. Finally, distributed sliding mode controller is designed to maintain system stability.

3.1. **State/FDI attack observer design.** The robust asymptotic estimation observer is designed as follows.

$$\begin{cases} \bar{I}_n\dot{\hat{\bar{x}}}_i(t) = \bar{A}_{ii}\hat{\bar{x}}_i(t) + \bar{B}_i u_i(t) + \sum\limits_{j=1,j\neq i}^{N} \bar{A}_{ij}\hat{\bar{x}}_j(t) - \bar{L}_i\left(\hat{y}_i(t) - y_i(t)\right) \\ \qquad\qquad - \bar{N}_i\left(\dot{\hat{y}}_i(t) - \dot{y}_i(t)\right) \\ \hat{y}_i(t) = \bar{C}_i\hat{\bar{x}}_i(t) \end{cases} \tag{11}$$

where $\hat{\bar{x}}_i(t) \in \mathbb{R}^{n+p}$ and $\hat{y}_i(t) \in \mathbb{R}^m$ are the estimated values of $\bar{x}_i(t)$ and $y_i(t)$, respectively. $\bar{L}_i \in \mathbb{R}^{(n+p)\times m}$ and $\bar{N}_i = \begin{bmatrix} R_i \\ N_i \end{bmatrix} \in \mathbb{R}^{(n+p)\times m}$ with $R_i \in \mathbb{R}^{n\times m}$ and $N_i \in \mathbb{R}^{p\times m}$ are the observer gain matrices.

Remark 3.1. *Due to the fact that the augmented matrix $\bar{I}_n$ lacks full rank, the inclusion of terms $\bar{N}_i\left(\dot{\hat{y}}_i(t) - \dot{y}_i(t)\right)$ is employed to address the singularity of Equation (9). This approach proves to be convenient for the computation of observer gain matrices.*

Then, the estimation error is expressed as

$$\bar{e}_i(t) = \hat{\bar{x}}_i(t) - \bar{x}_i(t) \tag{12}$$

Taking account of Equations (9) and (11), the estimation error is written as

$$\bar{I}_n\dot{\bar{e}}_i(t) = \left(\bar{A}_{ii} - \bar{L}_i\bar{C}_i\right)\bar{e}_i(t) - \bar{h}_i + \sum_{j=1,j\neq i}^{N} \bar{A}_{ij}\bar{e}_j(t) - \bar{N}_i\bar{C}_i\dot{\bar{e}}_i(t) \tag{13}$$

It can be further obtained that

$$\left(\bar{I}_n + \bar{N}_i\bar{C}_i\right)\dot{\bar{e}}_i(t) = \left(\bar{A}_{ii} - \bar{L}_i\bar{C}_i\right)\bar{e}_i(t) - \bar{h}_i + \sum_{j=1,j\neq i}^{N} \bar{A}_{ij}\bar{e}_j(t) \tag{14}$$

Because of the introduction of matrices $\bar{I}_n$ and $\bar{C}_i$, the matrices $\bar{I}_n + \bar{N}_i\bar{C}_i$ are nonsingular, that is

$$\begin{aligned} \bar{I}_n + \bar{N}_i\bar{C}_i &= \begin{bmatrix} I_n & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} R_i \\ N_i \end{bmatrix}\begin{bmatrix} C_i & E_i \end{bmatrix} \\ &= \begin{bmatrix} I_n + R_iC_i & R_iE_i \\ N_iC_i & N_iE_i \end{bmatrix} \end{aligned} \tag{15}$$

Remark 3.2. *We can choose $R_i = 0$ and $N_i = E_i^+$, where E_i^+ is the pseudo inverse of E_i for convenience, so that $\bar{I}_n + \bar{N}_i\bar{C}_i = \begin{bmatrix} I_n & 0 \\ E_i^+C_i & I_r \end{bmatrix}$, which are nonsingular obviously.*

Defining

$$\bar{Q}_i = \bar{I}_n + \bar{N}_i\bar{C}_i \tag{16}$$

then, the error dynamic equation of the system is written as

$$\begin{cases} \dot{\bar{e}}_i(t) = \bar{Q}_i^{-1}\left(\bar{A}_{ii} - \bar{L}_i\bar{C}_i\right)\bar{e}_i(t) + \bar{Q}_i^{-1}\sum\limits_{j=1,j\neq i}^{N} \bar{A}_{ij}\bar{e}_j(t) - \bar{Q}_i^{-1}\bar{h}_i \\ e_{ai}(t) = \bar{I}_r\bar{e}_i(t) \end{cases} \tag{17}$$

where $\bar{I}_r = \begin{bmatrix} 0 & I_r \end{bmatrix}$.

Theorem 3.1. *Given an $L_2 - L_\infty$ performance level γ, if there have matrices $\bar{Y}_i \in \mathbb{R}^{(n+p)\times m}$ and symmetric positive definite matrices $\bar{P}_i \in \mathbb{R}^{(n+p)\times(n+p)}$, that satisfy the conditions (18) and (19),*

$$\begin{bmatrix} \Psi_{11} & \Psi_{12} & \cdots & \Psi_{1N} \\ * & \Psi_{22} & \cdots & \Psi_{2N} \\ * & * & \ddots & \vdots \\ * & * & * & \Psi_{NN} \end{bmatrix} < 0 \tag{18}$$

$$\begin{bmatrix} -\bar{Q}_i^T \bar{P}_i \bar{Q}_i & \bar{I}_r^T \\ * & -\gamma I \end{bmatrix} < 0 \tag{19}$$

where

$$\Psi_{ii} = \begin{bmatrix} \bar{Q}_i^T \bar{P}_i \left(\bar{A}_{ii} - \bar{L}_i \bar{C}_i\right) + \left(\bar{A}_{ii} - \bar{L}_i \bar{C}_i\right)^T \bar{P}_i \bar{Q}_i & -\bar{Q}_i^T \bar{P}_i \\ * & -\gamma I \end{bmatrix},$$

$$\Psi_{ij} = \begin{bmatrix} \bar{Q}_i^T \bar{P}_i \bar{A}_{ij} + \bar{A}_{ji}^T \bar{P}_j \bar{Q}_j & 0 \\ 0 & 0 \end{bmatrix},$$

then the error dynamics Equation (17) satisfies the $L_2 - L_\infty$ *performance* $\|e_{ai}(t)\|_\infty < \gamma \|\bar{h}_i(t)\|_2$.

Proof: A Lyapunov function candidate is defined as

$$V(t) = \sum_{i=1}^{N} \bar{e}_i^T(t) \left(\bar{Q}_i^T \bar{P}_i \bar{Q}_i\right) \bar{e}_i(t) \tag{20}$$

It can be further obtained that

$$\begin{aligned} \dot{V}(t) = & \sum_{i=1}^{N} \bar{e}_i^T(t) \left[\bar{Q}_i^T \bar{P}_i \left(\bar{A}_{ii} - \bar{L}_i \bar{C}_i\right) + \left(\bar{A}_{ii} - \bar{L}_i \bar{C}_i\right)^T \bar{P}_i \bar{Q}_i\right] \bar{e}_i(t) - 2\bar{e}_i^T(t) \bar{Q}_i^T \bar{P}_i \bar{h}_i \\ & + 2\bar{e}_i^T(t) \bar{Q}_i^T \bar{P}_i \sum_{j=1, j\neq i}^{N} \bar{A}_{ij} \bar{e}_j(t) \end{aligned} \tag{21}$$

Construct the performance J_1:

$$\begin{aligned} J_1 &= V(t) - \gamma \int_0^t \left[\bar{h}^T(s) \bar{h}(s)\right] ds \\ &= V(t) - \gamma \int_0^t \sum_{i=1}^{N} \bar{h}_i^T(s) \bar{h}_i(s) ds \\ &\leq \int_0^t \left[\dot{V}(s) - \gamma \sum_{i=1}^{N} \bar{h}_i^T(s) \bar{h}_i(s)\right] ds \end{aligned} \tag{22}$$

Combining (21) and (22), we can obtain

$$\begin{aligned} & \dot{V}(t) - \gamma \sum_{i=1}^{N} \bar{h}_i^T(t) \bar{h}_i(t) \\ = & \sum_{i=1}^{N} \bar{e}_i^T(t) \left[\bar{Q}_i^T \bar{P}_i \left(\bar{A}_{ii} - \bar{L}_i \bar{C}_i\right) + \left(\bar{A}_{ii} - \bar{L}_i \bar{C}_i\right)^T \bar{P}_i \bar{Q}_i\right] \bar{e}_i(t) - 2\bar{e}_i^T(t) \bar{Q}_i^T \bar{P}_i \bar{h}_i \\ & - \gamma \bar{h}_i^T(t) \bar{h}_i(t) + 2\bar{e}_i^T(t) \bar{Q}_i^T \bar{P}_i \sum_{j=1, j\neq i}^{N} \bar{A}_{ij} \bar{e}_j(t) \end{aligned} \tag{23}$$

Subsequently, defining $\xi_i(t) = \begin{bmatrix} \bar{e}_i(t) & \bar{h}_i(t) \end{bmatrix}^T$, it can be further obtained that

$$\dot{V}(t)-\gamma\sum_{i=1}^{N}\bar{h}_i^T(t)\bar{h}_i(t)=\begin{bmatrix}\xi_1(t)\\ \xi_2(t)\\ \vdots\\ \xi_N(t)\end{bmatrix}^T\begin{bmatrix}\Psi_{11}&\Psi_{12}&\cdots&\Psi_{1N}\\ *&\Psi_{22}&\cdots&\Psi_{2N}\\ *&*&\ddots&\vdots\\ *&*&*&\Psi_{NN}\end{bmatrix}\begin{bmatrix}\xi_1(t)\\ \xi_2(t)\\ \vdots\\ \xi_N(t)\end{bmatrix} \tag{24}$$

Therefore, the condition (18) is proved. Then, construct the following performance J_2:

$$J_2=e_a^T(t)e_a(t)-\gamma V(t) \tag{25}$$

It can be further obtained that

$$\begin{aligned}e_a^T(t)e_a(t)-\gamma V(t)&=\sum_{i=1}^{N}e_{ai}^T(t)e_{ai}(t)-\gamma\sum_{i=1}^{N}\bar{e}_i^T(t)\left(\bar{Q}_i^T\bar{P}_i\bar{Q}_i\right)\bar{e}_i(t)\\&=\sum_{i=1}^{N}\bar{e}_i^T(t)\bar{I}_r^T\bar{I}_r\bar{e}_i(t)-\gamma\bar{e}_i^T(t)\left(\bar{Q}_i^T\bar{P}_i\bar{Q}_i\right)\bar{e}_i(t)\\&=\sum_{i=1}^{N}\bar{e}_i^T(t)\left(\bar{I}_r^T\bar{I}_r-\gamma\bar{Q}_i^T\bar{P}_i\bar{Q}_i\right)\bar{e}_i(t)\end{aligned} \tag{26}$$

So if $\bar{I}_r^T\bar{I}_r-\gamma\bar{Q}_i^T\bar{P}_i\bar{Q}_i<0$, according to Schur complement [33], it is written as

$$\begin{bmatrix}-\bar{Q}_i^T\bar{P}_i\bar{Q}_i&\bar{I}_r^T\\ *&-\gamma I\end{bmatrix}<0 \tag{27}$$

The condition (19) is proved.

Remark 3.3. *To enhance the estimation performance of the RAEO, the pole configuration conditions are established. According to Lemma 2.1, when the conditions*

$$\begin{bmatrix}-\bar{P}_i&\bar{P}_i\bar{A}_i-\bar{Y}_i\bar{C}_i-\varepsilon_i\bar{P}_i\bar{Q}_i\\ *&-\tau_i^2\bar{Q}_i^T\bar{P}_i\bar{Q}_i\end{bmatrix}<0 \tag{28}$$

hold, then the eigenvalues of $\left(\bar{A}_{ii}-\bar{L}_i\bar{C}_i\right)$ *within the given disk* $\mathcal{D}(\varepsilon_i,\tau_i)$.

3.2. **FDI attack compensation.** Since the RAEO has been designed to estimate FDI attacks, the FDI attack estimation can be written as

$$\hat{a}_i(t)=\bar{I}_r\hat{\bar{x}}_i(t) \tag{29}$$

Due to the FDI attacks act on sensor channel, traditional controllers are unable to proactively address the impact that the attack signals have on the system. Hence, the output after the compensation $y_{ci}(t)$ is written as

$$\begin{aligned}y_{ci}(t)&=y_i(t)-E_i\hat{a}_i(t)\\&=C_ix_i(t)+E_ia_i(t)-E_i\hat{a}_i(t)\\&=C_ix_i(t)+E_i\left(a_i(t)-\hat{a}_i(t)\right)\\&=C_ix_i(t)+E_ie_{ai}(t)\end{aligned} \tag{30}$$

3.3. **Distributed sliding mode controller design.** To improve the performance of the power system when FDI attacks occur, a novel LFC is devised, utilizing the distributed sliding mode control. The switching surfaces are defined as

$$s_i(t)=G_iy_{ci}(t)-\int_0^t G_i\left(A_{ii}+B_iK_i\right)y_{ci}\left(\tau\right)d\tau \tag{31}$$

where G_i and K_i are constant matrices. It can be further obtained that

$$\dot{s}_i(t)=G_i\left(\dot{x}_i(t)+E_i\dot{e}_{ai}(t)\right)-G_i\left(A_{ii}+B_iK_i\right)\left(x_i(t)+E_ie_{ai}(t)\right)$$

$$
\begin{aligned}
&= G_i \left[\left(A_{ii}x_i(t) + B_i u_i + \sum_{j=1,j\neq i}^{N} A_{ij}x_i(t) + h_i(t) \right) + E_i \dot{e}_{ai}(t) \right] \\
&\quad - G_i \left(A_{ii} + B_i K_i \right) \left(x_i(t) + E_i e_{ai}(t) \right) \\
&= G_i \left[B_i u_i + \sum_{j=1,j\neq i}^{N} A_{ij}x_i(t) + h_i(t) + E_i \dot{e}_{ai}(t) - B_i K_i x_i(t) \right. \\
&\quad \left. - \left(A_{ii} + B_i K_i \right) E_i e_{ai}(t) \right]
\end{aligned} \tag{32}
$$

Theorem 3.2. *Using the load frequency controller (33) along with the adaptive law (34) for FDI attack reconstruction ensures the stability of the LFC system.*

$$
u_i(t) = K_i y_{ci}(t) - (G_i B_i)^{-1} \left[G_i \sum_{j=1,j\neq i}^{N} A_{ij} y_{cj}(t) + (\hat{\sigma}_i + k_i)\, sign(s_i(t)) \right] \tag{33}
$$

where $k_i > 0$,

$$
\sigma_i = \|G_i\| d_i + \|G_i E_i\| \|\dot{e}_{ai}(t)\| + \|G_i A_{ij} E_i\| \|e_{ai}(t)\| + \|G_i\| \sum_{j=1,j\neq i}^{N} \|A_{ij} E_i\| \|e_{aj}(t)\|
$$

is a positive number. We define the adaptive law of $\hat{\sigma}_i$ *as follows:*

$$
\dot{\hat{\sigma}}_i = m_i \|s_i(t)\| \tag{34}
$$

where $m_i > 0$.

Proof: Constructing the Lyapunov function as follows:

$$
V_i(t) = \frac{1}{2} s_i^T(t) s_i(t) + \frac{1}{2m_i} \tilde{\sigma}_i^2 \tag{35}
$$

where $\tilde{\sigma}_i = \sigma_i - \hat{\sigma}_i$.

According to the derivative equation of the sliding mode surface (31), it is achieved that

$$
\begin{aligned}
\dot{V}_i(t) &= s_i^T(t) \dot{s}_i(t) - \tilde{\sigma}_i \dot{\hat{\sigma}}_i \\
&= s_i^T(t) G_i \left[B_i u_i + \sum_{j=1,j\neq i}^{N} A_{ij}x_i(t) + h_i(t) + E_i \dot{e}_{ai}(t) - B_i K_i x_i(t) \right. \\
&\quad \left. - \left(A_{ii} + B_i K_i \right) E_i e_{ai}(t) \right] - \tilde{\sigma}_i \|s_i(t)\|
\end{aligned} \tag{36}
$$

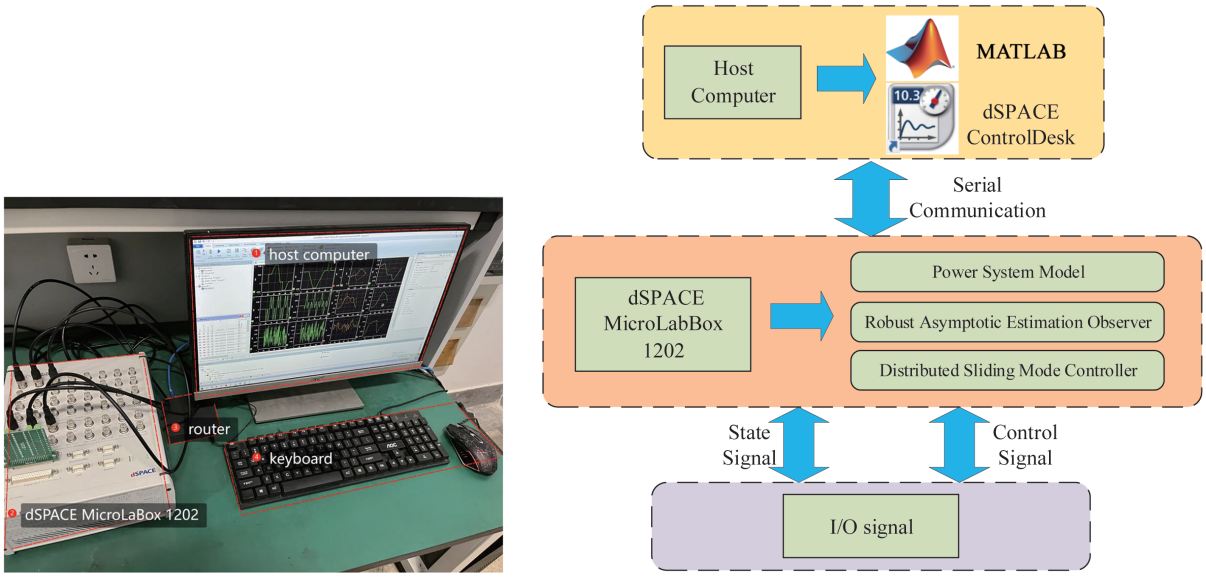
Substituting the control input (33) into (36), it can be obtained that

$$
\begin{aligned}
\dot{V}_i(t) &= s_i^T(t) \left[G_i h_i(t) + G_i E_i \dot{e}_{ai}(t) - G_i \sum_{j=1,j\neq i}^{N} A_{ij} E_j e_{aj}(t) \right. \\
&\quad \left. - G_i A_{ii} E_i e_{ai}(t) - (\hat{\sigma}_i + k_i)\, sign(s_i(t)) \right] - \tilde{\sigma}_i \|s_i(t)\| \\
&\leq \left[\|G_i\| \|h_i(t)\| + \|G_i E_i\| \|\dot{e}_{ai}(t)\| + \|G_i A_{ij} E_i\| \|e_{ai}(t)\| \right.
\end{aligned}
$$

$$
\begin{aligned}
&- \|G_i\| \sum_{j \neq i}^{N} \|A_{ij} E_i\| \|e_{aj}(t)\| \Big] \|s_i(t)\| - (\sigma_i + k_i) \|s_i(t)\| \\
&= -k_i \|s_i(t)\| + \|G_i\| \left[\|h_i(t)\| - d_i \right] \|s_i(t)\| \\
&\leq 0
\end{aligned} \tag{37}
$$

It can be noticed that the proposed controller ensures the reachability of the sliding motion on the power system. Consequently, in the event of FDI attacks on the power system, the attack estimation and compensation are used so that the system can still maintain a stable frequency.

4. **Experimental Results.** To verify the effectiveness of the robust asymptotic estimation observer and the distributed sliding mode control strategy proposed when a single area and multi-area are simultaneously attacked by injecting false data, simulation experiments were conducted in two scenarios. A three-area interconnected power system is constructed on the MATLAB/Simulink platform. Then, the LFC control platform based on dSPACE MicroLabBox 1202 is established to carry out experiments on the control algorithm in Figure 3. The details of the parameters are presented in Table 1. The experiment time and step size are set to 100 s and 0.0001 s, respectively.



(a) Experimental platform (b) Topology of experimental platform

FIGURE 3. Experimental system

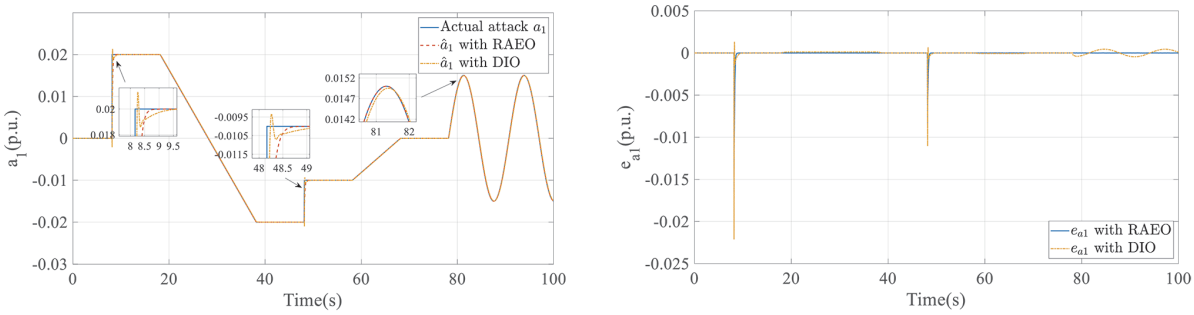
TABLE 1. System parameters

	Area1	Area2	Area3
H_i (p.u.s)	0.3708	0.2708	0.2508
D_i (p.u./Hz)	0.025	0.025	0.022
T_{ti} (s)	0.19	0.23	0.26
T_{gi} (s)	0.05	0.05	0.04
R_i (Hz/p.u.)	2.15	2.45	2.25
k_i	0.6	0.6	0.6
β_i (Hz/p.u.)	0.49	0.43	0.47
T_{ij} (p.u./Hz)	$T_{12} = 0.15$	$T_{13} = 0.12$	$T_{23} = 0.10$

4.1. **Scenario 1.** In this scenario, the hybrid FDI attack occurs on the first power area as follows:

$$a_1(t) = \begin{cases} 0.02 & 10 \text{ s} \leq t < 20 \text{ s} \\ -0.002t + 0.06 & 20 \text{ s} \leq t < 40 \text{ s} \\ -0.02 & 40 \text{ s} \leq t < 50 \text{ s} \\ -0.01 & 50 \text{ s} \leq t < 60 \text{ s} \\ 0.001t - 0.07 & 60 \text{ s} \leq t < 70 \text{ s} \\ 0.015 \sin(t - 80) & 80 \text{ s} \leq t < 100 \text{ s} \\ 0 & \text{else} \end{cases} \tag{38}$$

Meanwhile, by setting the regional pole placement condition as $\mathcal{D}(-30, 30)$, the minimum $L_2 - L_\infty$ performance level is $\gamma = 0.727$ according to Theorem 3.1. In order to highlight the superiority of the observer designed in this paper, the distributed intermediate observer (DIO) is designed in [25] as a comparison. The experimental result of the FDI attack estimation and its error are shown in Figure 4. From Figure 4, we can see that the power system attacked at 8.16 s in advance. This is due to the fact that during the experiment, the actual sampling time of dSPACE MicroLabBox 1202 does not match the sampling time set by the simulation. The distributed intermediate observer has a large estimation error, while the RAEO proposed in this paper has a small estimation error and a fast response time. Therefore, it can be considered the proposed detection technique can more accurately estimate FDI attacks.



(a) (b)

FIGURE 4. Scenario 1: (a) Actual FDI attack a_1 and its estimation; (b) the estimation error of a_1

4.2. **Scenario 2.** In this scenario, we consider different types of FDI attacks to be applied on the each area as follows:

$$a_{11}(t) = \begin{cases} 0.02 & 20 \text{ s} \leq t < 30 \text{ s} \\ 0.002t - 0.04 & 30 \text{ s} \leq t < 40 \text{ s} \\ 0.04 & 40 \text{ s} \leq t < 50 \text{ s} \\ -0.004t + 0.06 & 50 \text{ s} \leq t < 60 \text{ s} \\ -0.02 & 70 \text{ s} \leq t < 80 \text{ s} \\ 0.002t - 0.036 & 80 \text{ s} \leq t < 90 \text{ s} \\ 0 & \text{else} \end{cases},$$

$$a_{12}(t) = \begin{cases} -0.001t + 0.02 & 20 \text{ s} \leq t < 40 \text{ s} \\ -0.02 & 40 \text{ s} \leq t < 50 \text{ s} \\ 0.001t - 0.07 & 50 \text{ s} \leq t < 70 \text{ s} \\ 0.01 & 80 \text{ s} \leq t < 90 \text{ s} \\ 0 & \text{else} \end{cases} \tag{39}$$

$$a_{21}(t) = \begin{cases} 0 & 0\text{ s} \le t < 20\text{ s} \\ -0.1\sin(0.5(t-20))\cos(0.25(t-20)) & 20\text{ s} \le t \le 100\text{ s} \end{cases},$$

$$a_{22}(t) = \begin{cases} 0 & 0\text{ s} \le t < 20\text{ s} \\ -0.1\sin(0.25(t-20))\cos(0.5(t-20)) & 20\text{ s} \le t \le 100\text{ s} \end{cases} \tag{40}$$

$$a_{31}(t) = \begin{cases} 0 & 0\text{ s} \le t < 20\text{ s} \\ -0.03\text{randn}() & 20\text{ s} \le t \le 100\text{ s} \end{cases},$$

$$a_{32}(t) = \begin{cases} 0 & 0\text{ s} \le t < 20\text{ s} \\ -0.03\text{randn}() & 20\text{ s} \le t \le 100\text{ s} \end{cases} \tag{41}$$

Then, setting the regional pole placement condition as $\mathcal{D}(-50, 50)$, the minimum $L_2 - L_\infty$ performance level is $\gamma = 0.5969$ according to Theorem 3.1. By using the RAEO, the estimation results of FDI attacks are shown in Figure 5. The attack estimation is extremely close to its actual value. Figure 6 and Figure 7 show the responses of Δf_i and $\Delta P_{tie,i}$, respectively, when FDI attacks occur.

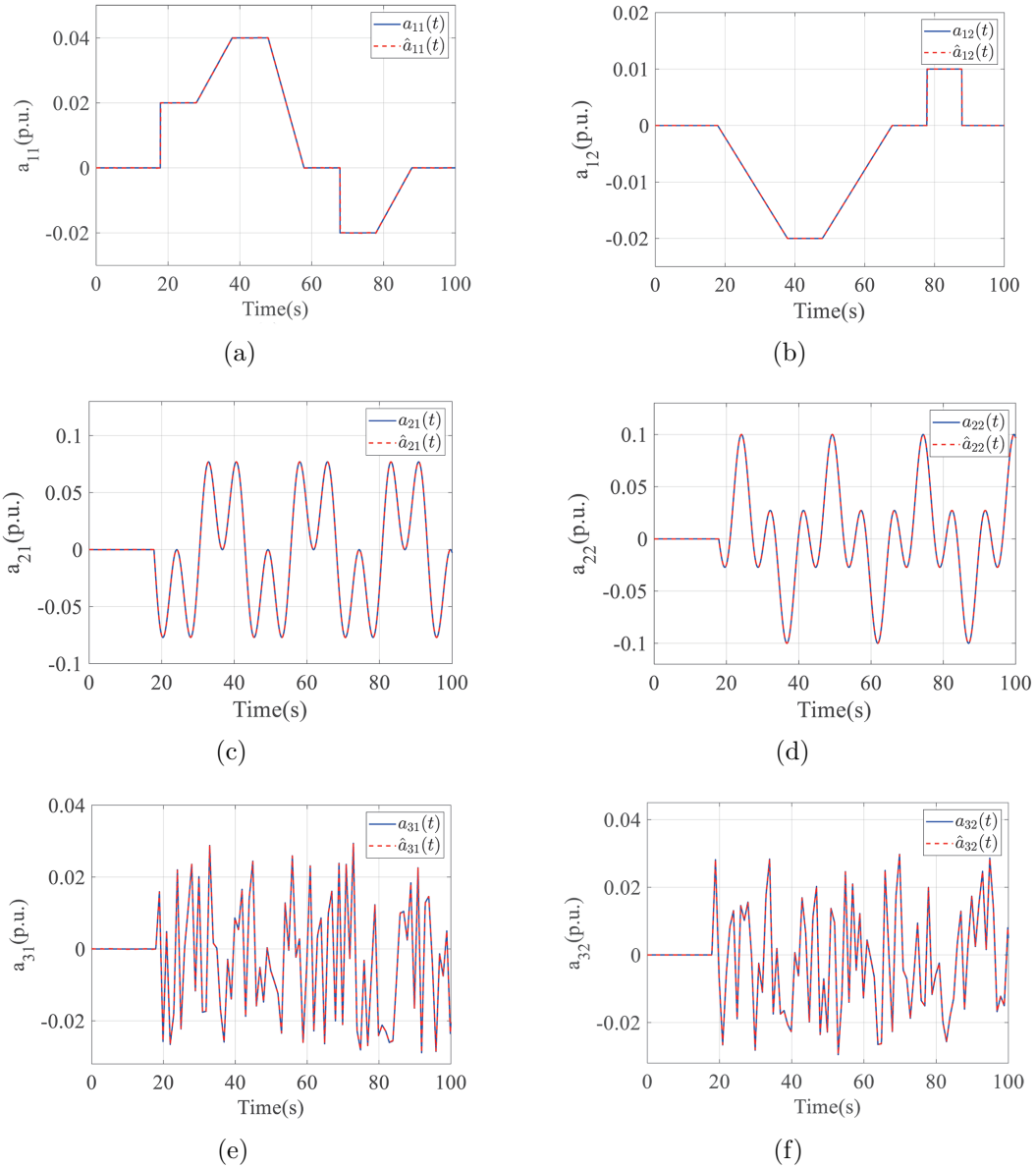


FIGURE 5. Actual FDI attacks and its estimation in Scenario 2

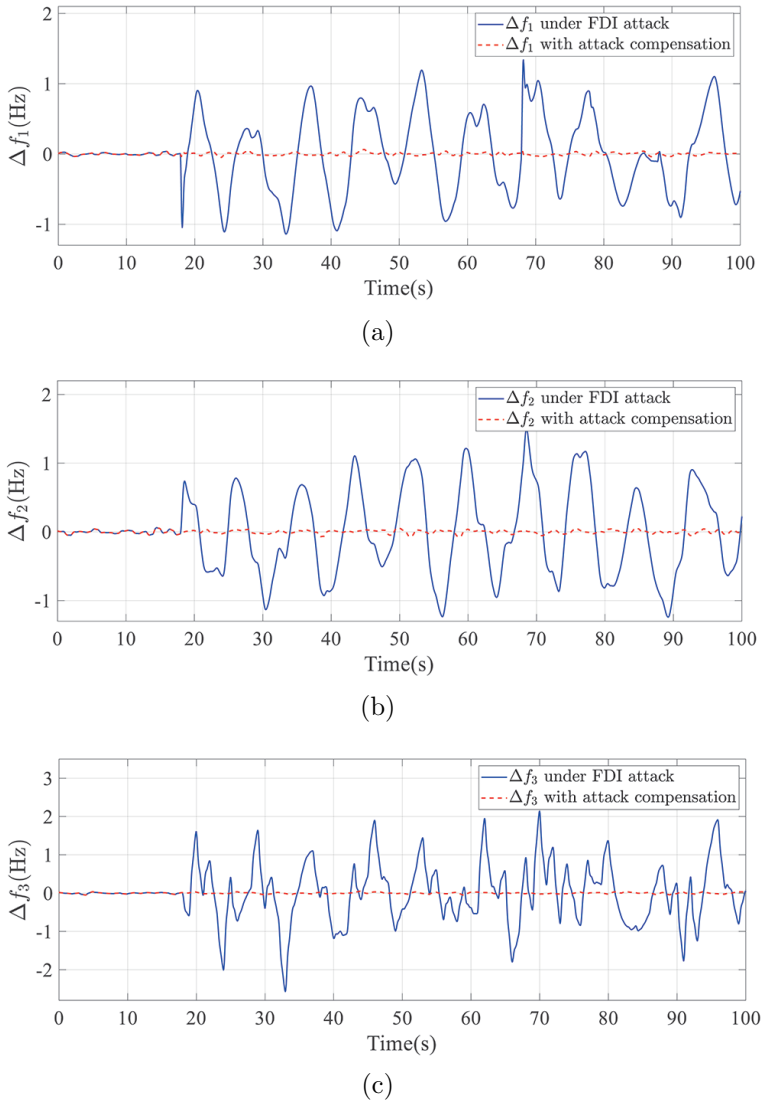


FIGURE 6. The responses of Δf_i in each area

It can be observed from the experiment that, under the same FDI attacks conditions, a controller without considering attack compensation finds it challenging to mitigate the interference caused by FDI attacks. This results in significant deviations in system frequency and tie-line power, posing challenges in upholding grid stability. Meanwhile, a controller based on attack compensation effectively minimizes the effect on the system when FDI attacks occur. This allows the system frequency and tie-line power to remain within a narrow range, thereby maintaining grid stability.

5. **Conclusion.** This paper introduces a robust asymptotic estimation observer-based secure distributed sliding mode controller for a multi-area LFC system when FDI attacks occur. Firstly, the system model under FDI attacks is built. Secondly, FDI attacks are observed by the robust asymptotic estimation observer and compensated as feedforward signals, which can mitigate the influence of FDI attacks on the LFC system. Then, the secure distributed sliding mode controller is proposed on the power system. Finally, experimental results indicate the conclusion that the secure distributed sliding mode control scheme can maintain the power system stability. Since the delayed communication is

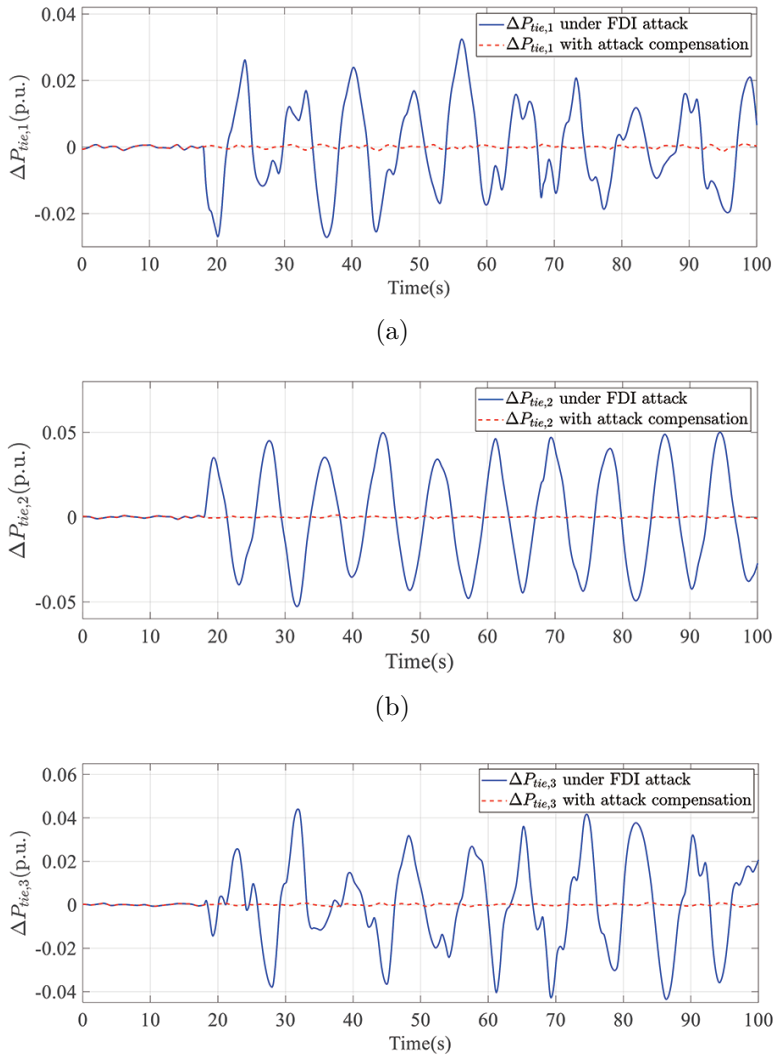


FIGURE 7. The responses of $\Delta P_{tie,i}$ in each area

not considered in the power system, our future work will study in depth the time-delay problem on the power system.

Acknowledgment. This work is partially supported by the National Natural Science Foundation of China (Grant No. 62222307, No. 61973140) and the Natural Science Foundation of Jiangsu Province (Grant No. BK20211235). The authors also appreciatively acknowledge the helpful suggestions and comments of the reviewers, which have enhanced the presentation.

REFERENCES

[1] W. Zhang and K. Fang, Controlling active power of wind farms to participate in load frequency control of power systems, *IET Generation Transmission & Distribution*, vol.11, no.9, pp.2194-2203, 2017.

[2] S. Weckx, R. D'Hulst and J. Driesen, Primary and secondary frequency support by a multi-agent demand control system, *IEEE Transactions on Power Systems*, vol.30, no.3, pp.1394-1404, 2015.

[3] A. Ameli, A. Hooshyar, E. F. El-Saadany and A. M. Youssef, Attack detection and identification for automatic generation control systems, *IEEE Transactions on Power Systems*, vol.33, no.5, pp.4760-4774, 2018.

[4] R. Shankar, S. Pradhan, K. Chatterjee and R. Mandal, A comprehensive state of the art literature survey on LFC mechanism for power system, *Renewable and Sustainable Energy Reviews*, vol.76, pp.1185-1207, 2017.

[5] T. Roth and B. M. McMillin, Physical attestation in the smart grid for distributed state verification, *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, vol.1, pp.626-627, 2017.

[6] S. Yang, C. Huang, Y. Yu, D. Yue and J. Xie, Load frequency control of interconnected power system via multi-agent system method, *Electric Power Components and Systems*, vol.45, no.8, pp.839-851, 2017.

[7] M. Ma, H. Chen, X. Liu and F. Allgöwer, Distributed model predictive load frequency control of multi-area interconnected power system, *International Journal of Electrical Power & Energy Systems*, vol.62, pp.289-298, 2014.

[8] D. Xu, J. Liu, X.-G. Yan and W. Yan, A novel adaptive neural network constrained control for a multi-area interconnected power system with hybrid energy storage, *IEEE Transactions on Industrial Electronics*, vol.65, no.8, pp.6625-6634, 2018.

[9] W. Tan, Tuning of PID load frequency controller for power systems, *Energy Conversion and Management*, vol.50, no.6, pp.1465-1472, 2009.

[10] W. Yan, L. Sheng, D. Xu, W. Yang and Q. Liu, H_∞ robust load frequency control for multi-area interconnected power system with hybrid energy storage system, *Applied Science-Basel*, vol.8, no.10, 2018.

[11] J. Yang, X. Sun and K. Liao, Model predictive control-based load frequency control for power systems with wind-turbine generators, *IET Renewable Power Generation*, vol.13, pp.2871-2879, 2019.

[12] Q. Zhu, J. Wang and Y. Zhu, Adaptive backstepping nonsingular terminal sliding mode control of servo system based on new sliding mode and reaching law, *International Journal of Innovative Computing, Information and Control*, vol.18, no.6, pp.1689-1700, 2022.

[13] C. Chen, K. Zhang, K. Yuan, L. Zhu and M. Qian, Novel detection scheme design considering cyber attacks on load frequency control, *IEEE Transactions on Industrial Informatics*, vol.14, no.5, pp.1932-1941, 2018.

[14] W. Bi, K. Zhang, Y. Li, K. Yuan and Y. Wang, 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, 2019.

[15] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer and H. B. Gooi, 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, 2017.

[16] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, The 2015 Ukraine Blackout: Implications for false data injection attacks, *IEEE Transactions on Power Systems*, vol.32, no.4, pp.3317-3318, 2017.

[17] Z. Cheng, X. Bu, J. Liang and J. Liu, Indirect-direct secure load frequency control against false data injection attacks, *IEEE Transactions on Industrial Informatics*, pp.1-13, 2023.

[18] Y. Li, R. Huang and L. Ma, False data injection attack and defense method on load frequency control, *IEEE Internet of Things Journal*, vol.8, no.4, pp.2910-2919, 2021.

[19] J. Liu, Y. Gu, L. Zha, Y. Liu and J. Cao, 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, 2019.

[20] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei and B. Carbunar, Resilient design of networked control systems under time delay switch attacks, application in smart grid, *IEEE Access*, vol.5, pp.15901-15912, 2017.

[21] Z. Zhang, J. Hu, J. Lu, J. Cao and F. E. Alsaadi, Preventing false data injection attacks in LFC system via the attack-detection evolutionary game model and KF algorithm, *IEEE Transactions on Network Science and Engineering*, vol.9, no.6, pp.4349-4362, 2022.

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

[23] 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, 2019.

[24] J. Ye and X. Yu, Detection and estimation of false data injection attacks for load frequency control systems, *Journal of Modern Power Systems and Clean Energy*, vol.10, no.4, pp.861-870, 2022.
[25] S. Weng, P. Weng, B. Chen, S. Liu and L. Yu, Distributed secure estimation against unknown FDI attacks and load deviation in multi-area power systems, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol.69, no.6, pp.3007-3011, 2022.
[26] M. L. Corradini and A. Cristofaro, Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes, *IET Control Theory and Applications*, vol.11, no.11, pp.1756-1766, 2017.
[27] Y. Gu, X. Yu, K. Guo, J. Qiao and L. Guo, Detection, estimation, and compensation of false data injection attack for UAVs, *Information Sciences*, vol.546, pp.723-741, 2021.
[28] H. Zhao, J. Shan, L. Peng and H. Yu, Distributed event-triggered bipartite consensus for multiagent systems against injection attacks, *IEEE Transactions on Industrial Informatics*, vol.19, no.4, pp.5377-5386, 2023.
[29] X. Chen, S. Hu, Y. Li, D. Yue, C. Dou and L. Ding, Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DOS attacks, *IEEE Transactions on Smart Grid*, vol.13, no.3, pp.2357-2368, 2022.
[30] W. Yu, X. Bu and Z. Hou, Security data-driven control for nonlinear systems subject to deception and false data injection attacks, *IEEE Transactions on Network Science and Engineering*, vol.9, no.4, pp.2910-2921, 2022.
[31] Z. Hu, S. Liu, W. Luo and L. Wu, Credibility-based secure distributed load frequency control for power systems under false data injection attacks, *IET Generation Transmission & Distribution*, vol.14, no.17, pp.3498-3507, 2020.
[32] G. Garcia and J. Bernussou, Pole assignment for uncertain systems in a specified disk by state feedback, *IEEE Transactions on Automatic Control*, vol.40, no.1, pp.184-190, 1995.
[33] P. Gahinet and P. Apkarian, A linear matrix inequality approach to H_∞ control, *International Journal of Robust and Nonlinear Control*, vol.4, no.4, pp.421-448, 1994.

Author Biography

Zengbo Shen received the B.S. degree in Electrical Engineering and Automation from Jiangnan University, Wuxi, China, in 2021. He is currently pursuing the M.S. degree in Electrical Engineering with Jiangnan University, Wuxi, China.

His current research interests include sliding mode control, cyber attack, and multi-area power systems.

Dezhi Xu received the Ph.D. degree in Control Theory and Control Engineering from Nanjing University of Aeronautics and Astronautics, China, in 2013.

He was a Visiting Fellow with the Department of Biomedical Engineering, City University of Hong Kong, China, from 2018 to 2019. He is currently a Professor and Doctoral Supervisor with the Southeast University. His research interests include data-driven control, fault diagnosis and fault-tolerant control, multi-agent systems and cyber-physical systems, technologies of renewable energy, motor control, and smart grid.

Prof. Xu was supported by the National Natural Science Fund for Excellent Young Scientists Fund Program in 2022. He was a recipient of the First Class Prize of Science and Technology Progression from the China General Chamber of Commerce in 2016, and the Best Young Scholar of Jiangnan University in 2022. He was a Guest Editor for the International Journal of Innovative Computing, Information and Control and the Electric Power. He currently serves as an Editorial Board Member for the International Journal of Innovative Computing, Information and Control, the Electric Power, the Electrotechnical Application and the Electrical Engineering. He is a Committee Member of the Association of Energy Internet, and Trusted Control in Chinese Association of Automation (CAA), and the Energy Storage in China Renewable Energy Society (CRES).

Tinglong Pan received his B.Eng. degree in Industrial Automation from China University of Mining and Technology, Xuzhou, China, in 1999, and the Ph.D. degree in Power Electronics and Power Drive from China University of Mining and Technology, Xuzhou, China, in 2004.

He is currently a Professor at Jiangnan University, where his research interests include microgrid control technology, power conversion technology, power drive system and its intelligent control technology.

Weilin Yang received his B.Eng. degree in Machine Design & Manufacture and Their Automation from University of Science and Technology of China, Hefei, China, in 2009, and the Ph.D. degree in Mechanical Engineering from City University of Hong Kong, Hong Kong SAR in 2013.

He was a postdoctoral researcher at Masdar Institute of Science and Technology (now Khalifa University), Abu Dhabi, UAE, 2013-2016. He was a research engineer of General Electric (GE) Global Research, Shanghai, 2016-2017. He joined Jiangnan University in July 2017, where he is currently an Associate Professor. His research interests include modeling and control of energy systems, robust model predictive control, and data-driven control.

Dongnian Jiang received the B.S. degree in Information and Computing Science from Xiamen University, Xiamen, China, in 2006, and the M.S. and Ph.D. degrees in Control Theory and Control Engineering from the Lanzhou University of Technology, Lanzhou, China, in 2010 and 2018, respectively, where he is currently an Associate Professor.

His research interests include fault diagnosis and tolerant control, fault diagnosability evaluation, and design for control systems.