Load frequency control under false data inject attacks based on multi-agent system method in multi-area power systems

Tengfei Weng¹, Yan Xie¹, Guorong Chen¹, Qi Han¹, Yuan Tian¹, Liping Feng² and Yangjun Pei¹

Abstract
This article considers the load frequency control of multi-area power system-based multi-agent system method under false data injection attacks. The research can provide better solutions for multi-area power system load frequency control under false data injection attacks. First, an event-triggered mechanism is introduced to decide which data should be transmitted in the controller to save the limited network bandwidth. Besides, a model of cyberattacks is built using the Bernoulli random variables. Then, conditions are given for maintaining the system asymptotic stability under attack. Finally, simulations are performed to demonstrate the validity of the theory proposed in this article.

Keywords
Load frequency control, multi-area power system, false data injection attacks, event-triggered

Date received: 17 November 2021; accepted: 3 March 2022

Handling Editor: Yanjiao Chen

Introduction
Load frequency control (LFC) is the key to maintain the frequency stability of power systems. More recently, a large number of researchers published papers on LFC because of the security and stability of power systems.¹⁻⁵ The multi-area power system is connected by the power systems of multiple regions. Besides, distributed cooperative control method based on multi-agent system (MAS) has been widely used in multi-area power system.⁶⁻⁹ MAS refers to a network system associated with a group of agents with functions of perception, communication, computation, and execution.¹⁰ Singh et al.⁸ presented an intelligent controller for LFC in “smart grid” environment which has been changed in communication topology via MAS technology. A two-level coordinated control frame based on MAS was proposed in Yang et al.⁹ to improve the frequency control performance of the power system.

The control center and measurement center of LFC system are typical networked control system (NCS), and the communication between them adopts open communication network or special communication network. Actually, open communication networks rely on open communication channels to share large amounts of data. The communication channels may be attacked by an attacker to inject false data into the network to create false frequency signals. Therefore, it is necessary to design a fault-tolerant control algorithm to prevent false data injection attacks.
of data, while special communication networks only allow specified data to be shared through channels. Compared with the latter, open communication network has the characteristics of more flexibility and practicality. However, open networks are vulnerable to malicious network attacks, which lead to security accidents in power systems. Therefore, it is necessary to study the LFC under malicious network attacks. From the target of attack, data integrity and availability are the main targets of attack. From the type of attack, attack can be divided into denial-of-service (DoS), deception attack, false data injection attack (FDIAs), random attack, \(^1\) and so on. ShangGuan et al. \(^2\) proposed a switched system model based on the LFC of multi-area power systems to reduce the adverse effects of DoS. In Wang et al., \(^3\) an \(H_x\) load frequency controller was designed for power systems which was subject to deception attack based on event-triggered secure control strategy. A credibility-based secure distributed LFC strategy was proposed in Hu et al. \(^4\) to sustain the stability operation of the power systems under FDIAs. Xiahou et al. \(^5\) investigated a perturbation estimation-based robust LFC scheme for power systems which was subject to random time-delay attack. In Chen et al., \(^6\) a hidden layer-based attack-resilient distributed cooperative control algorithm was introduced to solve the problem of the secondary control of islanded microgrids under FDIAs.

In order to avoid system failure caused by network congestion, event-triggered transmission scheme was often applied to NCS. \(^7\)–\(^9\) The LFC for power systems with communication delays was studied in Wen et al. \(^10\) where an event-triggered control method was used to reduce the amount of communications required. In Liu et al., \(^11\) the LFC for multi-area power systems under DoS attacks and deception attacks was solved by introducing an event-triggered mechanism and a switched system model. An adaptive condition for event-triggered scheme was given in Zhang et al. \(^12\) for the multi-area uncertain power systems. The robust stability and stabilization of adaptive event-triggered LFC of multi-area power systems were investigated under a networked environment via sliding mode control in Lv et al. \(^13\) Li et al. \(^14\) investigated dynamic event-triggered \(H_x\) LFC for multi-area power systems with communication delays. Hu et al. \(^15\) proposed intermittent communication consensus control based on dynamic event triggering mechanism for leaderless directed MAS networks. In other side, the false measurements’ data may not be transmitted when an attack occurs because the state values are updated only when the given conditions are destroyed in the event-triggered mechanism. Therefore, event-triggered transmission scheme can also improve the security of information transmission. However, it was rare to apply event-triggered transmission scheme to the LFC of multi-area power systems in the existing literature when an attack occurs on the network. Therefore, this article considers the LFC of multi-area power systems under FDIAs based on MAS.

The main contributions of this article are summarized as follows:

1. The important goal of LFC is to ensure the stability of frequency in the area, which is similar to the consensus based on MAS. Therefore, the consensus control based on MAS is used for the theoretical analysis of the LFC.
2. The event-triggered mechanism is introduced to lighten the load of network bandwidth, which not only reduced the update frequency of the controller, but also improved the security of information transmission. Furthermore, we proved that the proposed event-triggered mechanism does not have the Zeno phenomenon by deducing the lower bound of the time interval of any adjacent triggering moment.
3. In addition, most of the literatures \(^20\)–\(^24\) mentioned above rarely take FDIAs into account. Therefore, the conditions for maintaining the system asymptotic stability under FDIAs are given to guarantee the safe and stability operation of the system.

The rest of this article is organized as follows. The models of the multi-area power systems, FDIAs, and event-triggered mechanism are introduced in section “Problem formulation.” In section “Main results,” the sufficient conditions of tolerable attack parameters are proposed and are further analyzed, which guarantees the asymptotic stability of the multi-area power systems. In section “Simulation example,” a simulation example is given to illustrate the effectiveness of the theory under the FDIAs.

**Notions**

In this article, \(n\) denote the sets of real and natural numbers, respectively. \(\mathbb{R}^n\) and \(\mathbb{R}^{n\times n}\) denote the \(n\)-dimensional vector space and \(n \times n\) matrix space, respectively. \(C^T\) is the transpose of matrix \(C\). For a vector \(u\), \(\|u\|\) represents the Euclidean norm.

**Problem formulation**

This section gives the background of the problem which includes multi-area LFC power systems description, FDIAs model, and event-triggered transmission mechanism.
Multi-area LFC power system description

The multi-area LFC power systems of the $i$th area are shown in Figure 1 and the parameters are listed in Table 1.\textsuperscript{24} Area control error (ACE) is used to measure the tie-line switching power between control areas. $ACE_i$ signal is a linear combination of frequency deviation and tie-line power deviation of $i$th area, which can be defined as

$$ACE_i = \beta_i \Delta f_i + \sum_{j=1,j\neq i}^{n} \Delta P_{tie-i}$$

(1)

Therefore, it can be induced to equation (2) based on Figure 1

$$\Delta f_i(s) = \frac{1}{D_i + sM_i} (\Delta P_{mi}(s) - \Delta P_{di}(s) - \Delta P_{tie-i}(s))$$

$$\Delta P_{tie-i}(s) = \frac{2\pi}{s} \sum_{j=1,j\neq i}^{n} T_{ij} (\Delta f_i(s) - \Delta f_j(s))$$

$$\Delta P_{mi}(s) = \frac{1}{1 + sT_{chi}} \Delta P_{vi}(s)$$

$$\Delta P_{vi}(s) = \frac{1}{1 + sT_{gi}} \left( u(s) - \frac{1}{R} \Delta f_i(s) \right)$$

(2)

The dynamic behavior of the power systems is achieved using the inverse Laplace transform with equation (2) based on\textsuperscript{26}

---

**Table 1.** Parameters in $i$th LFC power systems.

| Parameter | Definition |
|-----------|------------|
| $\beta_i$ | Frequency bias factor |
| $M_i$     | Moment of inertia of the generator |
| $D_i$     | Damping coefficient of the generator |
| $R_i$     | Speed droop |
| $T_{fi}$  | Tie-line synchronizing coefficient between the $i$th and $j$th control area |
| $T_{ch}$  | Time constant of the turbine |
| $T_{g}$   | Time constant of the governor |
| $\Delta P_{tie-i}$ | Tie-line active power deviation |
| $\Delta P_{mi}$ | Generator mechanical output deviation |
| $\Delta P_{di}$ | Load disturbance |
| $\Delta f_i$ | Frequency deviation |

**Governor**
An automatic regulating device that enables the diesel engine to operate at a stable speed.

**Turbine**
An engine that generates power using fluid to impact the impeller rotation.

**Generator**
A mechanical device that converts other forms of energy into electrical energy.

---

**Figure 1.** Dynamic model of the $i$th LFC power systems under FDIA's.

---

\textsuperscript{3} Weng et al.
\[ \Delta f_i(t) = \frac{1}{M_i} (\Delta P_{mi}(t) - \Delta P_{di}(t) - \Delta P_{tie-}(t) - D_f(t)) \]
\[ \Delta P_{tie-}(t) = 2\pi \sum_{j=1, j \neq i}^n T_{ij} (\Delta f_i(t) - \Delta f_j(t)) \]
\[ \Delta P_{mi}(t) = \frac{1}{T_{chi}} (\Delta P_{v1}(t) - \Delta P_{m}(t)) \]
\[ \Delta P_{v1}(t) = \frac{1}{T_{gi}} \left( (u(t) - \Delta P_{v1}(t) - \frac{1}{R} \Delta f_i(t)) \right) \]

The ith-area of LFC power systems dynamic model is given as follows
\[ \begin{cases} x_i(k + 1) = A_i x_i(k) + B_i u_i(k) + C_i \phi_i(k) + A_i y_i(k) \\ y_i(k) = D_i x_i(k) \end{cases} \]

where
\[ x_i(k) = \left[ \begin{array}{c} \Delta P_{tie-}(k) \\ \Delta f_i(k) \\ \Delta P_{mi}(k) \\ \Delta P_{v1}(k) \end{array} \right] \]
\[ y_i(k) = \left[ \begin{array}{c} -2\pi \sum_{j=1, j \neq i}^n T_{ij} 0 0 0 0 \\ 0 0 0 0 0 \\ 0 0 0 0 0 \\ 0 0 0 0 0 \end{array} \right] \]
\[ B_i = \left[ \begin{array}{c} 0 0 0 \frac{1}{v_p} 0 \end{array} \right] \]
\[ C_i = \left[ \begin{array}{c} 0 \frac{1}{M_i} 0 0 0 \end{array} \right] \]
\[ D_i = \left[ \begin{array}{c} 1 \beta_i 0 0 0 \\ 0 0 0 0 1 \end{array} \right] \]

The purpose of this article is to design the proportional–integral (PI) controller applied in the LFC power systems, which can be expressed as
\[ u_i(k) = -K_p A_i C_i - K_i \int_0^k A_i C_i(s) ds \]

where \( K_p \) and \( K_i \) denote the controller gains.

The control input of the multi-area LFC power systems can be rewritten as
\[ u(k) = -K y(k) \]
where \( u(k) \) is the control input of area, \( y(k) \) is the measurement output of area, \( K = \text{diag}[k_1, \ldots, k_n] \), and \( k_i = [K_{pi} \ K_{ki}] \).

**False data inject attacks**

For FDIAs, it destroys system stability by injecting false data into the system. As shown in Figure 2, the data are damaged by malicious FDIAs in the process of network transmission. The measurement output \( y(k) \) send by sensor is tampered with \( \tilde{y}(k) \). The controller obtained bad data and make the wrong command.

Besides, we assume that the false signals \( z(k) \) injected by the adversary for the FDIAs are described as follows. Under FDIAs, the measurements’ output \( y(k) \) received by the controllers is tampered as
\[ \tilde{y}(k) = y(k) + z(k) \]
where \( z(k) \) is a bounded attack energy function.

In this article, we assumed that the FDIAs occur randomly. Therefore, we use a Bernoulli random variable \( Y(k) \in \{0, 1\} \) to describe the probability of FDIAs. \( Y(k) \) obeys the Bernoulli distribution with the following probability distribution
\[ \mathbb{P}\{Y(k) = 1\} = \bar{Y}(k), \mathbb{P}\{Y(k) = 0\} = 1 - \bar{Y}(k) \]
where \( 0 \leq \bar{Y}(k) \leq 1 \).

Thus, the real measurements’ output \( y(k) \) of controller is as follows \( \bar{y}(k) \), \( \tilde{y}(k) \) the measurement output tampered by attackers
\[ \bar{y}(k) = Y(k) y(k) + (1 - Y(k)) \tilde{y}(k) \]

Combining equations (6) and (8), the control protocol under false data inject attack can be rewritten as
\[ u(k) = -K(Y(k) \bar{y}(k) + (1 - Y(k)) \tilde{y}(k)) \]
Assumption 1. To restrain the FDIAs, suppose that the following condition of attack energy function $z(k)$ holds\textsuperscript{26,27}

\[ ||z(k)||^2 \leq ||Sy(k)||^2 \]

where $S$ is a constant matrix, and represents the upper bound of the attack capability.

Remark 1. Inspired by Pang et al.\textsuperscript{28} and Sakthivel et al.,\textsuperscript{29} malicious attacks by attackers cannot inject false information unboundedly. It is reasonable to assume that the energy of attack signal is constrained. In addition, motivated by the works in Liu et al.,\textsuperscript{21} a probability-dependent false data inject model is adopted during the design of the reliable controller for the multi-area power systems.

Event-triggered mechanism

In this section, an event-triggered mechanism under LFC controller for multi-area power systems is given as

\[ \hat{\vartheta}^T(k)\Lambda \hat{\vartheta}(k) \leq \delta x^T(k^*) \Lambda x(k^*) \] (10)

where $\vartheta(k) = x(k^*) - x(k)$, $x(k^*)$, $k^* \in [k^*_s, k^*_s + 1)$, and $x(k)$ indicate the current sampled data and the latest transmitted data, respectively. Therefore, $\vartheta(k)$ is the error between the current sampled data and the latest transmitted data. $\delta \in [0, 1]$ is a constant and $\Lambda > 0$ is a matrix with appropriate dimensions. The principle of the event-triggered transmission mechanism is that the value of controller will update if the condition (10) is destroyed; otherwise, the newly sampled data will be discarded.

Remark 2. The non-periodic intermittent information transmission mode of event-triggered control can not only improve the security of information transmission to a certain extent, but also reduce the use of communication and computing resources, which can effectively improve the economy and practicability of LFC in multi-area power system.

Main results

This part will analyzes the security consensus of the multi-area power system (4) under FDIAs and proves that the proposed event triggering condition (10) does not result in Zeno behavior.

By applying the Kronecker product, the multi-area power systems (4) can be transformed as following based on equation (9)

\[
\begin{align*}
\{x(k + 1) &= (I_N \otimes (A - BKD))x(k) \\
-(L \otimes BK)Y(k)z(k) + (I_N \otimes C)\varphi(k) \}
\end{align*}
\] (11)

where $x(k) = [x^T(k) \cdot \cdot \cdot x^T(k)]^T$, $u(k) = [u^T(k) \cdot \cdot \cdot u^T(k)]^T$, $\varphi(k) = [\varphi^T(k) \cdot \cdot \cdot \varphi^T(k)]^T$, and $y(k) = [y^T(k) \cdot \cdot \cdot y^T(k)]^T$, and $z(k)$ represents the attack energy function.

Stability of the multi-area power systems

Definition 1. The multi-area power system (11) is asymptotically stable,\textsuperscript{14,21} and $H_s$ performance constraint is satisfied, if the following requirements are satisfied:

1. The multi-area power system (11) with $\varphi(k) = 0$ is asymptotically stable.
2. Under zero initial conditions, the inequality $\|y_i(k)\|^2 < \gamma^2 \|\varphi_i(k)\|^2$ holds for all nonzero $\varphi_i(k) \in [0, \infty)$ and prescribed scalar $\gamma > 0$.

Lemma 1. Suppose that there exist constant matrices $X$, $Y$, and $Z$ satisfying\textsuperscript{30}

\[ X - Y^TZ^{-1}Y < 0 \]

if and only if

\[ \begin{pmatrix} X & * \\ Z & Y \end{pmatrix} < 0 \]

Theorem 1. Under the FDIAs, the multi-area power systems (11) are asymptotically stable with the $H_s$ performance standard $\gamma > 0$, if there exist a positive matrix $Q$, controller gain $K$, and such that the following linear matrix inequality (LMI) holds

\[
\begin{bmatrix}
\bar{A}^TQ\bar{A} - Q + \delta \Lambda & \bar{A}^TQC + \bar{A}^TQBY(k) \\
* & C^TQC - \Lambda - C^TQBY(k) \\
\end{bmatrix} < 0
\]

(12)

and

\[
\begin{bmatrix}
\bar{A}^TQC + C^TQA - Q + \delta \Lambda & 0 & QA \\
* & -\Lambda & QC \\
* & * & -Q \\
\end{bmatrix} < 0
\]

where $\bar{A} = A - BKD$.

Proof. Choose a Lyapunov function candidate for multi-area power systems (11) as follows

\[ V(k) = x^T(k)Qx(k) \] (13)

When $\varphi^T(k) = 0$, define $\eta_i(k) = [x^T(k) \cdot \cdot \cdot x^T(k)]^T$. Then, calculate the difference of $V(k)$. We have
\[ VV(k) = V(k + 1) - V(k) \]
\[ = x^T(k + 1)Qx(k + 1) - x^T(k)Qx(k) \]
\[ - \theta^T(k)\Lambda\theta(k) + \delta x^T(k)\Lambda x(k) \]
\[ = [(A - BKD)x(k) - BKY(k)z(k)]^T \]
\[ Q[(A - BKD)x(k) - BKY(k)z(k)] - x^T(k)Qx(k) \]
\[ - \theta^T(k)\Lambda\theta(k) + \delta x^T(k)\Lambda x(k) \]
\[ = \eta_1^T(k) \]
\[ \begin{bmatrix} \hat{A}^T Q\hat{A} - Q + \delta\Lambda & -\hat{A}^T QBK(k) \\ * & Y^T(k)K^TB^TQKY(k) - \Lambda \end{bmatrix} \eta_1(k) \]

(14)

It is clearly that

\[ \begin{bmatrix} \hat{A}^T QC - Q + \delta\Lambda & -\hat{A}^T QBK(k) \\ * & Y^T(k)K^TB^TQKY(k) - \Lambda \end{bmatrix} \]
\[ = \begin{bmatrix} \hat{A}^T QC + C^T QC - \delta\Lambda & 0 \\ 0 & -\Lambda \end{bmatrix} \]
\[ + \begin{bmatrix} \hat{A}^T Q \\ C^T QC \end{bmatrix} Q^{-1} \begin{bmatrix} QC \\ Q \end{bmatrix} \]

(15)

By employing Lemma 1 to equation (15), it can be concluded that \( VV(k) < 0 \), if the following LMI holds

\[ \begin{bmatrix} \hat{A}^T QC + C^T QC - Q + \delta\Lambda & 0 \\ * & -\Lambda \end{bmatrix} < 0 \]

When \( \varphi^T(k) \neq 0 \), define \( \eta_2(k) = [x^T(k) \quad \varphi^T(k) \quad \varphi^T(k) \quad \varphi^T(k)]^T \).

Then, calculate the difference of \( V(k) \). We have

\[ \Delta V(k) = V(k + 1) - V(k) \]
\[ = x^T(k + 1)Qx(k + 1) - x^T(k)Qx(k) \]
\[ - \theta^T(k)\Lambda\theta(k) + \delta x^T(k)\Lambda x(k) \]
\[ = [(A - BKD)x(k) - BKY(k)z(k) + C\varphi(k)]^T \]
\[ Q[(A - BKD)x(k) - BKY(k)z(k) + C\varphi(k)] \]
\[ - x^T(k)Qx(k) - e^T(k)\Lambda e(k) + \delta x^T(k)\Lambda x(k) \]
\[ = \eta^T_2(k) \]
\[ \begin{bmatrix} \hat{A}^T Q\hat{A} - Q + \delta\Lambda & \hat{A}^T QC & -\hat{A}^T QBK(k) \\ * & C^T QC - \Lambda & -C^T QBK(k) \\ * & * & Y^T(k)K^TB^TQKY(k) \end{bmatrix} \eta_2(k) \]

(16)

Moreover, we need to guarantee that system (11) is asymptotically stability. According to equation (17), it follows that

\[ VV(k) < y^T(k)y(k) - \gamma^2\varphi^T(k)\varphi(k) \]

(17)
Summing up both sides of equation (19) with \( k = 0, 1, \ldots, \infty \), we can get the following inequality
\[
\|y_i(k)\|^2 < \gamma^2 \|\phi_r(k)\|^2
\]
so the asymptotic stability of system (11) is guaranteed. The proof of Theorem 1 is completed.

**Zeno phenomenon**

Another problem that cannot be ignored for the event-triggered control algorithm is to prove that the algorithm will not appear Zeno phenomenon. Next, we will prove that the proposed event-triggered algorithm does not have the Zeno phenomenon by deducing the lower bound of the time interval of any adjacent triggering moment.

**Definition 2.** The Zeno phenomenon is presented if it takes an infinite number of triggers countless times in a finite amount of time. In other words, the time interval is more than zero for any two adjacent events.

**Theorem 2.** For the event-triggered condition (10), there is a positive lower bound on the interval between two adjacent triggering event points.

**Proof.** According to the definition of \( \vartheta(k) \), we can obtain the differential of \( \vartheta(k) \) as follows
\[
\frac{d\vartheta(k)}{dk} = (I_N \otimes A)\vartheta(k) + (I_N \otimes B)\bar{u}(k) + (I_N \otimes C)\bar{\phi}(k)
\]
where \( \bar{u}(k) = u(k^*) - u(k) \) and \( \bar{\phi}(k) = \varphi(k^*) - \varphi(k) \).

Integration from \( k^* \) to \( k \), we have
\[
\vartheta_i(k) = e^{(I_N \otimes A)(k-k^*)}\vartheta_i(k^*) + e^{(I_N \otimes B)(k-k^*)}z_i(k^*)
\]
\[
+ e^{(I_N \otimes C)(k-k^*)}\phi_i(k^*)
\]
(21)

Define \( k^*_{i+1} \) as the next triggered time, it can be obtained from event-triggered condition (10)
\[
e^{(I_N \otimes A)(k^*_{i+1}-k^*)}\vartheta_i(k^*_i) + e^{(I_N \otimes B)(k^*_{i+1}-k^*)}z_i(k^*_i)
\]
\[
+ e^{(I_N \otimes C)(k^*_{i+1}-k^*)}\phi_i(k^*_i) - \delta x_i^T(t)A_i x_i(t) > 0
\]
(22)

Define \( K^* = k^*_{i+1} - k^*_i \), equation (22) can be rewritten as
\[
e^{(I_N \otimes A)K^*}\vartheta_i(k^*_i) + e^{(I_N \otimes B)K^*}z_i(k^*_i) + e^{(I_N \otimes C)K^*}\phi_i(k^*_i)
\]
\[
> \delta x_i^T(t)A_i x_i(t)
\]
(23)

Therefore, we can obtain
\[
K^* = k^*_{i+1} - k^*_i > 0
\]
(24)

The proof of Theorem 2 is completed.

**Simulation example**

In this section, a three-area power system is employed to identify the effectiveness of our proposed event-triggered secure control strategy for LFC under FDIAs. The system parameters setting of the three-area power system (12) is shown in Table 2. The communication topology of the interconnected three-area power system is given in Figure 3 and each area adopts wired connection.

In this simulation, we suppose that \( \delta = 0.63 \). Moreover, the probabilities of FDIAs are \( P\{Y(k) = 1\} = 0.37 \). The Bernoulli variable \( Y(k) \) indicating the occurrence of FDIAs is characterized in Figure 4 with \( Y(k) = 0.21 \). The exogenous disturbance is chosen as \( \Delta P_{di}(k) = 0.8 \sin(k) \). \( T_{12} = T_{21} = 0.2609 \).
The false signals injected by adversary is defined as $z(k) = 0.2e^k \sin y(k)$. The initial values are $x_1(0) = [0.1980 \ 0.0572 \ 0.7700 \ 0.5 \ 0.5]^T$, $x_2(0) = [-0.0037 \ 0.0193 \ 0.4300 \ 0.6 \ 0.6]^T$, and $x_3(0) = [-0.0028 \ 0.0186 \ 0.2200 \ 0.3 \ 0.7]^T$, respectively.

The simulation results are shown in Figure 5, which gives the frequency response of the conventional LFC in and our method. It can be seen from Figure 5(a) that the traditional LFC takes a long time to restore the stability of the system when multi-area power system is attacked by FDIA. However, it is unacceptable for power systems. Figure 5(b) perceives that the proposed method has improved the iteration speed, which meets the conditions of safe and stability operation of the power system.

Figures 6 and 7 delineate the tie-line active power deviation and generator mechanical output deviation change of the three-area power system. It should be pointed out that system (11) maintaining recovery and synchronization of communication links under FDIA.

It is worth noting that the method proposed in this article does not consider the influence of time-delay on the system, but time-delay is inevitable for any engineering system. Therefore, we will continue to study the LFC with time-delay in multi-area power system under FDIA in subsequent studies.
Conclusion
In summary, this article studies the LFC of multi-area power system based on MAS distributed control technology under FDIAs. The Bernoulli random variables are used to model the multi-regional power system affected by FDIAs. Then, an event-triggered mechanism is proposed to reduce the bandwidth of the network, and the asymptotic stability condition of multi-area power system is given. In addition, by deducing the lower bound of the time interval of any adjacent moment, it is proved that the event triggering mechanism proposed in this article does not have the Zeno phenomenon. According to this theorem, the simulation of specific cases is completed using LMI toolbox. The simulation results show that the proposed control algorithm can realize LFC security control of multi-area power system. Compared with other literature, the proposed algorithm has the advantages of faster and stronger robustness.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this
article: This work was supported in part by the West Light Foundation of the Chinese Academy of Science, in part by the Scientific and Technological Research Program of Chongqing Municipal Education Commission (KJZD-K201901504 and KJQN201901537), in part by the Humanities and Social Sciences Research of Ministry of Education (19YJCZH047), in part by the Research Foundation of The Natural Foundation of Chongqing City (cstc2021jcyj-msxmX0146), and in part by the National Innovation and Entrepreneurship Training Platform for College Students (202111551002).

ORCID iDs

Yan Xie https://orcid.org/0000-0001-5373-7899
Liping Feng https://orcid.org/0000-0003-1072-5438

References

1. Tian E and Peng C. Memory-based event-triggering $H_\infty$ load frequency control for power systems under deception attacks. IEEE Trans Cybernet 2020; 50(11): 4610–4618.

2. Bi W, Zhang K and Chen C. Cyber attack detection scheme for a load frequency control system based on dual-source data of compromised variables. Appl Sci 2021; 11(4): 1584.

3. Zhao X, Zou S and Ma Z. Decentralized resilient $H_\infty$ load frequency control for cyber-physical power systems under DoS attacks. IEEE/CAA J Autom Sinica 2021; 8(11): 1737–1751.

4. Thenmalar K. Fuzzy logic based load frequency control of power system. Mater Today 2021; 45: 8170–8175.

5. Li J, Yu T and Zhang X. Coordinated load frequency control of multi-area integrated energy system using multi-agent deep reinforcement learning. Appl Energy 2022; 306: 117900.

6. Logenthiran T, Srinivasan D and Khambadkone AM. Multi-agent system for energy resource scheduling of integrated microgrids in a distributed system. Electric Power Syst Res 2011; 81(1): 138–148.

7. Logenthiran T and Srinivasan D. Multi-agent system for the operation of an integrated microgrid. J Renew Sustain Energ 2012; 4(1): 013116.

8. Singh VP, Kishor N and Samuel P. Distributed multi-agent system-based load frequency control for multi-area power system in smart grid. IEEE Trans Ind Electron 2017; 64(6): 5151–5160.

9. Yang S, Huang C, Yu Y, et al. Load frequency control of interconnected power system via multi-agent system method. Electr Power Component Syst 2017; 45(8): 839–851.

10. Li Z, Xie Y, Han Q, et al. Group consensus of second-order multi-agent systems via intermittent sampled control. In: 2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Chengdu, China, 18–20 June 2021, pp. 185–189. New York: IEEE.

11. Ding D, Han QL, Xiang Y, et al. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing 2018; 275: 1674–1683.

12. Shang Guan XC, He Y, Zhang CK, et al. Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks. Control Eng Pract 2021; 107: 104678.

13. Wang D, Chen F, Meng B, et al. Event-based secure $H_\infty$ load frequency control for delayed power systems subject to deception attacks. Appl Math Comput 2021; 394: 125788.

14. Hu Z, Liu S, Luo W, et al. Credibility-based secure distributed load frequency control for power systems under false data injection attacks. IET General Trans Distrib 2020; 14(17): 3498–3507.

15. Xiahou KS, Liu Y and Wu QH. Robust load frequency control of power systems against random time-delay attacks. IEEE Trans Smart Grid 2020; 12(1): 909–911.

16. Chen Y, Qi D, Dong H, et al. A FDI attack-resilient distributed secondary control strategy for islanded microgrids. IEEE Trans Smart Grid 2020; 12(3): 1929–1938.

17. Zhang TY and Ye D. Distributed event-triggered control for multi-agent systems under intermittently random denial-of-service attacks. Inform Sci 2021; 542: 380–390.

18. Li XM, Zhou Q, Li P, et al. Event-triggered consensus control for multi-agent systems against false data injection attacks. IEEE Trans Cybernet 2019; 50(5): 1856–1866.

19. Hu S, Yue D, Xie X, et al. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans Cybernet 2018; 49(12): 4271–4281.

20. Wen S, Yu X, Zeng Z, et al. Event-triggering load frequency control for multiarea power systems with communication delays. IEEE Trans Ind Electron 2015; 62(3): 1308–1317.

21. Liu J, Gu Y, Zha L, et al. Event-triggered $H_\infty$ load frequency control for multiarea power systems under hybrid cyber attacks. IEEE Trans Syst Man Cybernet 2019; 49(8): 1665–1678.

22. Zhang H, Su S, Zhao YY, et al. Networked load frequency control of multi-area uncertain power systems via adaptive event-triggered communication scheme. J Franklin Inst 2019; 356(16): 9600–9626.

23. Lv X, Sun Y, Wang Y, et al. Adaptive event-triggered load frequency control of multi-area power systems under networked environment via sliding mode control. IEEE Access 2020; 8: 86585–86594.

24. Li C, Wang ZS and Tian YF. Dynamic event-triggered $H_\infty$ load frequency control for multi-area power systems with communication delays. Int J Robust Nonlin Control 2021; 31(9): 4100–4117.

25. Hu W, Yang C, Huang T, et al. A distributed dynamic event-triggered control approach to consensus of linear multiagent systems with directed networks. IEEE Trans Cybernet 2018; 50(2): 869–874.
26. Cao J, Ding D, Liu J, et al. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. *Inform Sci* 2021; 548: 69–84.

27. Liu J, Wei L, Xie X, et al. Quantized stabilization for T–S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks. *IEEE Trans Fuzzy Syst* 2018; 26(6): 3820–3834.

28. Pang ZH, Liu GP, Zhou D, et al. Two-channel false data injection attacks against output tracking control of networked systems. *IEEE Trans Ind Electron* 2016; 63(5): 3242–3251.

29. Sakthivel R, Kaviarasan B, Ahn CK, et al. Observer and stochastic faulty actuator-based reliable consensus protocol for multiagent system. *IEEE Trans Syst Man Cybernet* 2017; 48(12): 2383–2393.

30. Li R and Cao J. Stability analysis of reaction-diffusion uncertain memristive neural networks with time-varying delays and leakage term. *Appl Math Comput* 2016; 278: 54–69.