IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 31, 2019, accepted April 26, 2019, date of publication May 2, 2019, date of current version May 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914492

Resilient Event-Triggered Output Feedback Control for Load Frequency Control Systems Subject to Cyber Attacks

XIAOHONG ZHOU[1], ZHOU GU[1,2], AND FAN YANG[1]
[1]College of Mechanical and Electronic Engineering, Nanjing Forestry University, Nanjing 210037, China
[2]College of Automation Electronic Engineering, Qingdao University of Science and Technology, Qingdao 260061, China

Corresponding author: Zhou Gu (gzh1808@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 61473156.

ABSTRACT This paper considers the problem of load frequency control (LFC) design for multi-area power systems. Owing to the multi-area power system with a feature of spatial distribution, it becomes necessary to use the network as a signal transmission medium. The following two problems need to be addressed: 1) the transmission signals transmitted over the communication network are vulnerable to be attacked by adversaries. How to ensure the security of the control system and 2) multi-area power systems have a large amount of data need to be exchanged via the network, how to guarantee the network quality of service and the control performance under the limited network bandwidth. To address these problems, in this paper, a resilient output feedback control strategy in secure means is proposed for LFC systems based on the security criteria. Moreover, a new event triggered mechanism (ETM) is developed, under which the average data releasing rate is much lower than the one using the conventional data transmission mechanism, while it becomes high when the system encounters some external disturbances. To validate the effectiveness of the proposed approach, simulations are performed on a 3-area power system. The results show that the proposed control strategy can maintain the LFC system with a satisfactory control performance in the presence of stochastic cyber-attacks, and the average data releasing rate is of a lower level to save communication and computation resources.

INDEX TERMS Event-triggered mechanism, load frequency control, stochastic cyber-attack.

I. INTRODUCTION

It has been critical to ensure the frequency stability and power balance of interconnected power grids. In the past decades, a large number of distributed renewable generations (DRGs), such as wind power and solar photo voltaic, are taped to the grid. Due to the intermittency of output power of DRGs and some other disturbances, the frequency stability of the power systems is difficult to maintain. Load area control (LFC) which is an important part of the automatic generation control (AGC) has been shown the effectiveness to ensure the frequency close to its nominal value and tie-line power to its scheduling value. The conventional ways to bring back the frequency and tie-power to their respective scheduled values are proportional-integral (PI) or proportional-integral-derivative (PID) control strategy for the system [1]. The authors in [2] dealed with a PI control design for a four-area interconnected power system with generation rate constraints by using a method of fuzzy gain scheduling. Based on PI control strategy, a sector-bounded H_∞ control approach for modeling the constraints of the generation rate and valve position of the governor is used for LFC systems in [3]. Although the PI controller can improve the quality of the frequency for LFC systems using local control information, global information, such as the area control error (ACE) from other areas, is hard to acquire as a control input to improve the control performance by using the existing PI/PID control strategy.

For multi-area power systems, large-scale information exchanging, wide geographical distribution and along with their large computation cost pose a great difficulty to the implementation of the control scheme. Thanks to the wide area measurement system (WAMS), communication infrastructure of smart grids, the signal transmission from remote terminal unit (RTU) to control center, such as ACE signal, is communicated through a dedicated power network and

The associate editor coordinating the review of this manuscript and approving it for publication was Md Jahangir Hossain.

open communication infrastructure. The networked transmission, especially for the remote transmission via an open communication network, has a merit of low cost, high efficiency, strong flexibility and great scalability. Meanwhile, it inevitably brings some technical and theoretical challenges, such as the limited network-bandwidth, the security of the shared information against various malicious attacks.

Notice that a large amount of data accessing a limited bandwidth network will result in a poor network quality of service (QoS). Under the traditional time triggered mechanism (TTM), numerous ''unnecessary'' data are transmitted over the network. These redundant data occupies a large amount of communication and computing resource. In this context, ETM is studied as an alternative of data transmission. Considerable efforts have been devoted to ETMs in recent years [4], [5]. For example, in [6], the authors developed an event-triggered control for networked control systems (NCSs) based on the assumptions that the communication network is ideal (no delay and no packet dropouts) and the controller is known in *prior*. However, a Zeno behavior may be generated under this ETM. To avoid the Zeno behavior, an improved ETM was proposed based on the discrete sampled data, in [7], [8], to decide whether the current sampling data is needed for a networked control system. Under this ETM, the average data releasing rate (DRR) is much lower than that of the traditional TTM, moreover, the controller gains can be co-designed together with the parameters of ETM. In [9], the authors studied a dynamic event triggered scheme under which the event of data release is generated in the light of sampling states adaptively. It should be pointed that a better control performance can be achieved for the system with ETM if the DRR increases relatively when the system has some external disturbances. For this goal, in this paper, an improved ETM will be investigated.

Information security is critical for LFC systems if the remote ACE signals from the other area are transmitted via the network which is vulnerable to be attacked by adversaries, especially when it is transmitted over the shared communication network. If the control strategy of LFC systems has no any defense, the frequency will deviate from the nominal operation when the control signals are compromised by malicious attackers. The safe operation of the entire grid will be affected. In recent years, considerable efforts, such as cyber attack detection, secure control, etc. have been devoted to the control design against cyber attacks. The authors in [10] investigated the detectability of cyber attacks against cyber-physical systems. The attack detection method was put forward in [11] with the help of the intersection of two ellipsoidal sets. The methods of cyber attack detection, such as Bayesian detection [12], weighted least square [13] and $\mathcal{X}^2$-detector [14] are generally used. For maintaining a normal operation of the control system subject to cyber attacks, much research work has been conducted according to different attack types, for example, denial-of-service (DoS) attacks [15], the replay attacks [16], [17], and the deception attacks [18]–[20]. In [15], [21], a resilient control strategy was designed for the system compromised by DoS attacks imposed by partially identified power-constrained pulse width-modulated jammers.

This paper focuses on designing a novel resilient LFC scheme for multi-area power systems subject to deception cyber-attacks. The main contributions of this paper are as follows: 1) A new ETM has been developed. Under the proposed, when the system has external interference, the DRR is significantly higher than other periods. Additionally, the DRR is relatively low when the system tends to be stable; and 2) new security criteria are developed for LFC systems against the malicious attacks launched by adversaries.

The remainder of the paper is organized as follows. The dynamic model of multi-area power system with LFC scheme, ETM scheme, controller scheme and cyber-attacks model are presented in Section II. Section III investigates the ETM and the controller co-design method for frequency secure control of multi-area power systems subject to stochastic cyber-attacks. Case studies using 3-areas power systems are given to demonstrate the effectiveness of the proposed method in Section IV. Section V concludes the paper.

Notation: $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, $\mathbb{R}^{n\times m}$ is the set of real $n \times m$ matrices. $\|\cdot\|$ stands for the Euclidean vector norm or spectral norm as appropriate. The notation $X > 0$ (respectively, $X < 0$), for $X \in \mathbb{R}^{n\times n}$ means that the matrix X is a real symmetric positive definite (respectively, negative definite). X^T represents the transpose of X. $\mathbb{E}\{x\}$ stands for the expectation of stochastic variable x. The shorthand $diag_N\{X_i\}$ and $col_N\{x_i\}$ denotes a block diagonal matrix with diagonal blocks being the matrices $X_1, \cdots, X_n$ and a vector of $[x_1^T, \cdots, x_N^T]^T$, respectively. The asterisk $*$ in a matrix is used to denote term that is induced by symmetry, Matrices, if they are not explicitly stated, are assumed to have compatible dimensions.

II. SYSTEM MODELING AND PROBLEM FORMULATION

Frequency regulations are critical to the generator output in response to the load changes, since the power grid requires to keep a close balance between generation and load. In the future smart grid, the phaser measurement units (PMUs) are expected to be widely installed across the grid. The signal of frequency and tie-line power can be obtained by PMU and transmitted to control center via the communication network. It is assume that all the PMUs are time-synchronized with GPS satellites. LFC aims to enhance the stability level of multi-machine power systems by regulating the steam vale according to ACEs which are composed by the deviations of frequency and tie line exchange power, such that the power generation output and load power of the whole system are rebalanced. As is shown in Figure 1, the controller receives the ACE signals via communication network such that the frequency meets the control quality requirements.

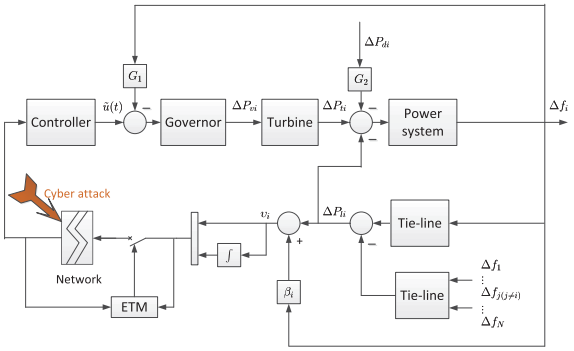

FIGURE 1. Multi-area LFC scheme of the i-th control area.

A. DYNAMIC MODELS OF LFC

The i-*th* governor dynamics is given by

$$\Delta\dot{P}_{vi}(t) = -\frac{1}{R_i T_{gi}}\Delta f_i(t) - \frac{1}{T_{gi}}\Delta P_{vi}(t) - \frac{1}{T_{gi}}\Delta E_i(t) \quad (1)$$

where $P_{vi}, f_i(t)$ and $E_i(t)$ are the i-th steam valve opening, frequency and the load generation balance point, respectively; $i \in \{0, 1, \cdots, N\} \triangleq \mathcal{N}$; "$\Delta$" denotes the deviation, for example, ΔP_{vi} means that the deviation of the i-th steam valve opening; R_i and T_{gi} are the speed droop coefficient and the governor time constant of each area, respectively.

The turbine dynamics is governed by

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

where T_{ti} is the turbine constant of each area, and P_{ti} is the mechanical power for i-*th* turbine.

The frequency deviation is given by

$$\Delta\dot{f}_i(t) = -\frac{1}{T_{pi}}\Delta f_i(t) + \frac{k_{pi}}{T_{pi}}\Delta P_{ti}(t) - \frac{k_{pi}}{T_{pi}}\Delta P_{tie-i}(t) \quad (3)$$

where P_{tie-i} denotes tie-line power. Let $D_i = \frac{1}{k_{pi}}$ and $I_i = \frac{T_{pi}}{k_{pi}}$. D_i and I_i are called as the damping coefficient and equivalent inertia of each area, respectively.

The net tie-line deviation between two areas is govern by

$$\Delta\dot{P}_{tie-i}(t) = \sum_{j=1, j\neq i}^{N} 2\pi T_{ij}(\Delta f_i(t) - \Delta f_j(t)) \quad (4)$$

where T_{ij} is the synchronization coefficient.

For convenience to analyses, we define the state vector $x_i(t) = [\Delta P_{vi}(t)\ \Delta P_{ti}(t)\ \Delta f_i(t)\ \Delta P_{tie-i}(t)]^T$. Then the dynamic model of LFC can be represented as

$$\dot{x}_i(t) = A_{ii}x_i(t) + \sum_{j=1, j\neq i}^{N} A_{ij}x_j(t) + B_i u_i(t) + B_{\omega i}\omega(t) \quad (5)$$

from (1) to (4), where

$$A_{ii} = \begin{bmatrix} -\frac{1}{T_{gi}} & 0 & -\frac{1}{R_i T_{gi}} & 0 \\ \frac{1}{T_{ti}} & -\frac{1}{T_{ti}} & 0 & 0 \\ 0 & \frac{k_{pi}}{T_{pi}} & -\frac{1}{T_{pi}} & -\frac{k_{pi}}{T_{pi}} \\ 0 & 0 & \sum_{j=1, j\neq i}^{N} 2\pi T_{ij} & 0 \end{bmatrix},$$

$$A_{ij} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -2\pi T_{ij} & 0 \end{bmatrix},$$

$$B_i = \begin{bmatrix} -\frac{1}{T_{gi}} & 0 & 0 & 0 \end{bmatrix}^T,$$

$$B_{\omega i} = \begin{bmatrix} \frac{k_{pi}}{T_{pi}} & 0 & 0 & 0 \end{bmatrix}^T$$

From Figure 1, one can see that the ACE (denoted by υ) and its integration are selected to transmit over the network. The ACE signal is depended on both the tie-line power exchange between areas and the local frequency, which is defined by

$$\upsilon_i(t) = \Delta P_{tie-i}(t) + \beta_i \Delta f_i(t) \quad (6)$$

where β_i is the frequency bias factor. Define $H_i = [0\ 0\ \beta_i\ 1]$, the i-th ACE signal can be denoted by

$$\upsilon_i(t) = H_i x_i(t) \quad (7)$$

For convenience of description, we denote: $A = [A_{ij}]_{n\times n}$, $B = diag_N\{B_i\}$, $H = diag_N\{H_i\}$, $B_\omega = diag_N\{B_{\omega i}\}$, and $x(t) = col_N\{x_i(t)\}$, $u(t) = col_N\{u_i(t)\}$, $\upsilon(t) = col_N\{\upsilon_i(t)\}$, $\omega(t) = col_N\{\omega_i(t)\}$. Then the overall power system can be described by

$$\dot{x}(t) = Ax(t) + Bu(t) + B_\omega\omega(t) \quad (8)$$

B. THE CONTROL SCHEME

In this study, a proportional plus integral control scheme is consider as follows

$$u(t) = K_p\upsilon(t) + K_I\int_0^t \upsilon(s)ds \quad (9)$$

where K_p and K_I are the parameters to be designed.

Define $y_i(t) = [\upsilon_i^T(t)\ \int_0^t \upsilon_i^T(s)ds]^T$ which is selected as a transmission signal via network (see Figure 1). The control input is held by the current value till a new data updates. Therefore, the networked control scheme for LFC systems is then developed as

$$u(t) = Ky(t_k h) \quad t \in [t_k h + \tau_{t_k}, t_{k+1}h + \tau_{t_{k+1}}) \triangleq \mathcal{U}_k \quad (10)$$

from (9), where $K = diag_N\{[K_P\ K_I]\}$, $y(t) = col_N\{y_i(t)\}$, t_k is a monotonically increasing sequence, h is a sampling instant, then $t_k h$ denotes the releasing instant, and τ_{t_k} is the network-induced delay that satisfies $\underline{\tau} \leq \tau_{t_k} \leq \bar{\tau}$.

Define $\bar{x}(t) = [x^T(t) \ \int_0^t \upsilon^T(s)ds]^T$, we can get the following augmented system

$$\begin{cases} \dot{\bar{x}}(t) = \bar{A}\bar{x}(t) + \bar{B}u(t) + \bar{B}_\omega\omega(t) \\ y(t) = \bar{H}\bar{x}(t) \\ u(t) = Ky(t) \qquad t \in \mathscr{U}_k \end{cases} \tag{11}$$

where

$$\bar{A} = \begin{bmatrix} A & 0 \\ H & 0 \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \bar{B}_\omega = \begin{bmatrix} B_\omega \\ 0 \end{bmatrix} \quad \bar{H} = \begin{bmatrix} H & 0 \\ 0 & 1 \end{bmatrix}$$

C. THE MODEL OF CYBER ATTACK

We first give the following secure definition for LFC systems before designing the control system.

Definition 1: The LFC system subject to stochastic attacks is said to be secure in mean square, if the frequency deviation margin satisfies

$$\|\Delta f(t)\| \leq \bar{f} \tag{12}$$

where $\bar{f}$ is a given constant.

From the adversaries point of view, the following issues need to be considered: 1) the attack can impact the system; and 2) the attack cannot be detected. To achieve the first objective, the adversaries inject the false data into the healthy data. To implement the second objective, the adversaries take the following two measures as a) let the malicious attacks injected into the healthy data be intermittent; and b) let the amplitude of the attacks is not big enough. Suppose the false data that injects into the healthy data is $\lambda(t)$. Based on the above analysis, we have following reasonable assumption

Assumption 1: The signal to be transmitted though the communication network is subject to be compromised by the adversary. The attack signal $\lambda(t) = col_N\{\lambda_i(t)\}$ is assumed to satisfy

$$\|\lambda(t)\| \leq \varsigma^2 \tag{13}$$

where ς is a positive constant.

Under the above analysis, the transmission signal being attacked is then modeled as

$$\bar{y}(t) = y(t_k h) + \theta(t)(\lambda(t_k h) - y(t_k h)) \qquad t \in \mathscr{U}_k \tag{14}$$

where $\theta(t)$ is a rand variable which satisfies that $\theta(t) \in \{1, 0\}$ with $\mathbb{E}\{\theta(t) = 1\} = \bar{\theta}$ and $\mathbb{E}\{\theta(t) = 0\} = 1 - \bar{\theta}$.

Remark 1: Besides the reasons analyzed above for the attack model with an intermittent form as in (14), it still has following reasons: 1) some attack signals are failed to be transmitted over the network; and 2) some malicious attack signals are blocked by the monitoring system, such as the hardware detecting device or software defense system.

D. THE DATA TRANSMISSION SCHEME

In the conventional time-triggered mechanism, the sampling data are transmitted over the network periodically. Under this mechanism, a large amount of sampling data that have little contribution for improving the frequency quality of LFC system due to the adjacent sampling data with litter variation waste the resource of network-bandwidth and computation. In this subsection, we are in position to develop a novel event-triggered mechanism for the LFC system, by which the burden of the limited network-bandwidth will be alleviated. For this purpose, we propose the following event-triggering condition

$$\begin{aligned} \varepsilon_i^T(t)\Xi_i\varepsilon_i(t) \leq \ & \sigma y_i^T(t_k h)\Xi_i y_i(t_k h) \\ & + \kappa\sigma\left[y_i^T(t_k h)\Xi_i\varepsilon_i(t) + \varepsilon_i^T(t)\Xi_i y_i(t_k h)\right] \end{aligned} \tag{15}$$

where $\varepsilon_i(t) = y_i(t_k h) - y_i(t_k h + lh)$, κ and σ are given positive scalars, $l = 0, 1, 2, \cdots$, and Ξ is a positive weighting matrix.

Remark 2: Under the above event-triggering condition, the amount of releasing data can be largely reduced than that using TTM within a certain period. On the other hand, the releasing rate can be increased as well to get more information from the controlled plant when the system is attacked or disturbed.

When the event-triggering condition in (15) is violated over time, the event of data-releasing will be generated. Therefore, the next releasing instant is

$$t_{k+1}h = t_k h + h + l_M h \tag{16}$$

where $l_M = \max_{l \in \mathbb{N}^+, s.t.(15)} l$. Therefore, the releasing period is not a constant period h, but a varying period $l_M h$ which is depend on the condition (15).

E. THE OVERALL MODEL OF LFC SYSTEM

Combining (11) and (14), we can get the following closed-loop LFC system that is subjected to cyber-attacks

$$\begin{aligned} \dot{\bar{x}}(t) = \ & \bar{A}\bar{x}(t) + (1 - \bar{\theta})\bar{B}K\bar{y}(t_k h) \\ & + \bar{\theta}\bar{B}K\lambda(t_k h) + \bar{B}_\omega\omega(t) \\ & + (\theta(t) - \bar{\theta})[-\bar{B}K\bar{y}(t_k h) + \bar{B}K\lambda(t_k h)] \end{aligned} \tag{17}$$

Define $\mathscr{U}_k^l \triangleq [t_k h + lh + \tau_{t_k}^l, t_k h + lh + h + \tau_{t_{k+1}}^{l+1})$ with $l = 0, 1, \cdots, l_M$. Obviously, $\mathscr{U}_k = \cup_{l=0}^{l_M} \mathscr{U}_k^l$ if we set $\tau_{t_k}^0 = \tau_{t_k}$ and $\tau_{t_{k+1}}^{l_M+1} = \tau_{t_{k+1}}$.

For $t \in \mathscr{U}_k^l$, defining $\mu(t) = t - t_k h - lh$ yields that

$$\mu_1 = \underline{\tau} < \mu(t) \leq h + \bar{\tau} = \mu_2 \tag{18}$$

Recalling the definition of $\varepsilon_i(t)$ in (15), we can easily know that $y(t_k h) = \varepsilon(t) + \bar{H}\bar{x}(t - \mu(t))$ with $\varepsilon(t) = col_N\{\varepsilon_i(t)\}$. Then, for $t \in \mathscr{U}_k^l$, we can transfer the dynamic (17) into

$$\dot{\bar{x}}(t) = \Gamma_1\zeta(t) + (\theta(t) - \bar{\theta})\Gamma_2\zeta(t) \tag{19}$$

by defining $\zeta(t) = [\bar{x}^T(t) \ \bar{x}^T(t - \mu_1) \ \bar{x}^T(t - \mu(t)) \ \bar{x}^T(t - \mu_2) \ \varepsilon^T(t) \ \lambda^T(t_k h) \ \omega^T(t)]^T$, where $\Gamma_1 = [\bar{A} \ 0 \ (1 - \bar{\theta})\bar{B}K\bar{H} \ 0 \ (1 - \bar{\theta})\bar{B}K\bar{H} \ \bar{\theta}\bar{B}K \ \bar{B}_\omega]$, $\Gamma_2 = [0 \ 0 \ -\bar{B}K\bar{H} \ 0 \ -\bar{B}K \ \bar{B}K \ 0]$.

The main objective of paper is to design the networked PI control and ascertain the parameter of ETM in (15) for LFC systems subject to injection attacks, such that the system is secure in mean square.

III. CO-DESIGN OF NETWORKED PI CONTROL AND ETM FOR LFC SYSTEMS

In this section, we will derive the criteria of the stability and stabilization in secure means for LFC systems subject to stochastic injection attacks.

The following Lemma is needed in deriving our results.

Lemma 1: [22] Suppose $\mu(t) \in [\mu_1, \mu_2]$, $\bar{x}(t) \in \mathbb{R}_2^{\bar{n}}$ and there exist matrices $R \in \mathbb{R}^{\bar{n}\times\bar{n}}$, $W \in \mathbb{R}^{\bar{n}\times\bar{n}}$. Then the following inequalities hold:

$$-(\mu_2-\mu_1)\int_{t-\mu_2}^{t-\mu_1}\dot{\bar{x}}^T(s)R_2\dot{\bar{x}}(s)ds \le \zeta^T(t)M_2\zeta(t) \quad (20)$$

where

$$M_2 = \begin{bmatrix}\mathcal{I}_2\\ \mathcal{I}_3\\ \mathcal{I}_4\end{bmatrix}^T \mathcal{W}\begin{bmatrix}\mathcal{I}_2\\ \mathcal{I}_3\\ \mathcal{I}_4\end{bmatrix}$$

$$\mathcal{W} = \begin{bmatrix}-R_2 & * & *\\ R_2-W & -2R_2+W+W^T & *\\ W & R_2-W & -R_2\end{bmatrix}$$

and $\mathcal{I}_i$ $(i = 1, \cdots, 7)$ is compatible row-block matrix with i th block of identify matrix, for example, $\mathcal{I}_3 = [0\ 0\ I\ 0\ 0\ 0\ 0]$.

Theorem 1: For some given positive constants $\mu_i, \kappa, \sigma, \bar{f}$, $\bar{\theta}, \gamma$, the LFC system (8) subject to stochastic injection attacks is secure in mean square by using the PI controller in (9) and the data transmission scheme in subsection II-D, if there exist matrices $P > 0, \Xi > 0, Q_i > 0, R_i > 0$ $(i = 1, 2)$ and matrices W with appropriate dimensions such that

$$\Upsilon := \Upsilon_{11} + \Gamma_1^T\mathcal{R}\Gamma_1 + \bar{\theta}(1-\bar{\theta})\Gamma_2^T\mathcal{R}\Gamma_2 < 0 \quad (21)$$

where M_2 is defined in Lemma 1, and

$$\begin{aligned}\Upsilon_{11} &= \mathcal{I}_1^TP\Gamma_1 + \Gamma_1^TP\mathcal{I}_1 + \mathcal{I}_1(Q_1+Q_2)\mathcal{I}_1 - \mathcal{I}_2^TQ_1\mathcal{I}_2\\ &\quad -\mathcal{I}_4^TQ_2\mathcal{I}_4 + M_1 + M_2 - \varsigma\mathcal{I}_6^T\mathcal{I}_6 - \gamma^2\mathcal{I}_7^T\mathcal{I}_7\\ &\quad +[\bar{H}\mathcal{I}_3 + (1+\kappa)\mathcal{I}_5]^T\sigma\Xi[\bar{H}\mathcal{I}_3 + (1+\kappa)\mathcal{I}_5]\\ &\quad -(1+\kappa^2\sigma)\mathcal{I}_5^T\Xi\mathcal{I}_5 + \mathcal{I}_1(\varsigma\bar{F}^T\bar{F} + \bar{H}^T\bar{H})\mathcal{I}_1,\\ \bar{F} &= [F\ 0], F = diag_N\{F_i\}, F = [0\ 0\ 1\ 0],\\ \mathcal{R} &= \mu_1^2R_1 + (\mu_2-\mu_1)^2R_2,\\ M_1 &= \begin{bmatrix}\mathcal{I}_1\\ \mathcal{I}_2\end{bmatrix}^T\begin{bmatrix}-R_1 & *\\ R_1 & -R_1\end{bmatrix}\begin{bmatrix}\mathcal{I}_1\\ \mathcal{I}_2\end{bmatrix}\end{aligned}$$

Proof: Choose a Lyapunov-Krasovskii functional candidate for system (19) as

$$\begin{aligned}V(t) &= \bar{x}^T(t)P\bar{x}(t) + \sum_{i=1}^{2}\int_{t-\mu_i}^{t}\bar{x}^T(s)Q_i\bar{x}(s)ds\\ &\quad +\mu_1\int_{t-\mu_1}^{t}\int_{s}^{t}\dot{\bar{x}}^T(v)R_1\dot{\bar{x}}(v)dvds\\ &\quad +(\mu_2-\mu_1)\int_{t-\mu_2}^{t-\mu_1}\int_{s}^{t}\dot{\bar{x}}^T(v)R_2\dot{\bar{x}}(v)dvds\end{aligned}$$

Taking derivation and expectation on $V(t)$ for $t \in \mathscr{U}_k^l$ yields

$$\begin{aligned}\mathbb{E}\{\dot{V}(t)\} &= \mathbb{E}\left\{2\bar{x}^T(t)P\Gamma_1\zeta(t) + \bar{x}^T(t)(Q_1+Q_2)\bar{x}(t)\right\}\\ &\quad -\mathbb{E}\left\{\sum_{i=1}^{2}\bar{x}^T(t-\mu_i)Q_i\bar{x}(t-\mu_i)\right\}\\ &\quad +\mathbb{E}\left\{\mu_1^2\dot{\bar{x}}^T(t)R_1\dot{\bar{x}}(t) + (\mu_2-\mu_1)^2\dot{\bar{x}}^T(t)R_2\dot{\bar{x}}(t)\right\}\\ &\quad -\mathbb{E}\left\{\mu_1\int_{t-\mu_1}^{t}\dot{\bar{x}}^T(s)R_1\dot{\bar{x}}(s)ds\right\}\\ &\quad -\mathbb{E}\left\{(\mu_2-\mu_1)\int_{t-\mu_2}^{t-\mu_1}\dot{\bar{x}}^T(s)R_2\dot{\bar{x}}(s)ds\right\} \quad (22)\end{aligned}$$

It is noted that $\mathbb{E}\{\theta(t)-\bar{\theta}\} = 0$ and $\mathbb{E}\{(\theta(t)-\bar{\theta})^2\} = \bar{\theta}(1-\bar{\theta})$. Then it follows that

$$\begin{aligned}\mathbb{E}\left\{\dot{\bar{x}}^T(t)R_i\dot{\bar{x}}(t)\right\} &= \mathbb{E}\left\{\zeta^T(t)\Gamma_1^TR_i\Gamma_1\zeta(t)\right.\\ &\quad \left.+\mathbb{E}\left\{\bar{\theta}(1-\bar{\theta})\zeta^T(t)\Gamma_2^TR_i\Gamma_2\zeta(t)\right\}\right. \quad (23)\end{aligned}$$

The event-triggering condition in (15) can is equivalent to

$$\begin{aligned}\zeta^T(t)\left([\bar{H}\ \mathcal{I}_3 + (1+\kappa)\mathcal{I}_5]^T\sigma\Xi[\bar{H}\mathcal{I}_3 + (1+\kappa)\mathcal{I}_5]\right.\\ \left.-(1+\kappa^2\sigma)\mathcal{I}_5^T\Xi\mathcal{I}_5\right)\zeta(t) > 0 \quad (24)\end{aligned}$$

From the Definition 1, one knows that $\|\Delta f(t)\| \le \bar{f}$ is secure. Otherwise, if $\|\Delta f(t)\| > \bar{f}$, under the Assumption (1), it yields

$$\bar{x}^T(t)\varsigma\bar{F}^T\bar{F}\bar{x}(t) > \varsigma\bar{f} > \varsigma^3 > \varsigma\lambda^T(t)\lambda(t) \quad (25)$$

Recalling Lemma 1 and combing (23) and (24) follows that

$$\begin{aligned}&\mathbb{E}\{\dot{V}(t) + y^T(t)\,y(t) - \gamma^2\omega^T(t)\omega(t)\}\\ &\le \mathbb{E}\left\{2\bar{x}^T(t)P\Gamma_1\zeta(t) + \bar{x}^T(t)(Q_1+Q_2)\bar{x}(t)\right\}\\ &\quad -\mathbb{E}\left\{\sum_{i=1}^{2}\bar{x}^T(t-\mu_i)Q_i\bar{x}(t-\mu_i)\right\}\\ &\quad +\mathbb{E}\left\{\zeta^T(t)(M_1+M_2+\Gamma_1^T\mathcal{R}\Gamma_1\right\}\\ &\quad +\mathbb{E}\left\{\bar{\theta}(1-\bar{\theta})\Gamma_2^T\mathcal{R}\Gamma_2)\zeta(t)\right\}\\ &\quad +\mathbb{E}\left\{\bar{x}^T(t)\varsigma\bar{F}^T\bar{F}\bar{x}(t) - \varsigma\lambda^T(t)\lambda(t)\right\}\\ &\quad +\mathbb{E}\left\{y^T(t)y(t) - \gamma^2\omega^T(t)\omega(t)\right\}\end{aligned}$$

One can see that if (21) holds, then

$$\mathbb{E}\{\dot{V}(t)\} \le \mathbb{E}\left\{-y^T(t)y(t) + \gamma^2\omega^T(t)\omega(t)\right\} \quad (26)$$

which implies that the LFC system is asymptotically stable in mean square sense since $\mathbb{E}\{\dot{V}(t)\} < 0$ for $\omega(t) = 0$.

Taking integration both side of (26) from $0 \to +\infty$ yields

$$\begin{aligned}&\mathbb{E}\{V(+\infty) - V(0)\}\\ &\le \mathbb{E}\left\{\int_0^{+\infty}\left[-y^T(t)y(t) + \gamma^2\omega^T(t)\omega(t)\right]dt\right\}\end{aligned}$$

Under the zero initial condition, we have

$$\mathbb{E}\left\{\int_0^{+\infty} y^T(t)y(t)dt\right\} \leq \mathbb{E}\left\{\int_0^{+\infty} \gamma^2\omega^T(t)\omega(t)dt\right\} \quad (27)$$

From above analyses, we can conclude that when the transmission signal of LFC systems is attacked by the adversary in the form of (14), the system can return to be secure. That is to say that the condition (21) is a sufficient condition to ensure the security of the LFC system in mean square. ■

Theorem 1 gives a sufficient condition to ensure the LFC system is secure in mean square with H_∞ performance γ. However, it is hard to achieve the parameters of the networked PI controller gains. Next, we are in a position to design the parameters of the PI controller gains for LFC systems in (9), together with the parameter of the ETM in (15). First we introduce the following Lemma.

Lemma 2: Suppose the matrix $\bar{B} \in \mathbb{R}^{m\times n}$ has a singular decomposition $\bar{B} = U\bar{B}_0V$, where $\bar{B}_0$ is a rectangular diagonal matrix with positive real numbers on the diagonal in decreasing order of magnitude, U and V are orthogonal matrices, and $\bar{B}$ is full column rank. Then there exist a symmetric matrix P and a matrix X such that $P\bar{B} = \bar{B}X$ if and only if P is of the form of $P = U\bar{P}U^T$ with $\bar{P} = diag\{P_1, P_2\}$, where $P_1 \in \mathbb{R}^{m\times m}$ and $P_2 \in \mathbb{R}^{(n-m)\times(n-m)}$.

Theorem 2: For some given positive constants $\mu_i, \kappa, \sigma, \bar{f}$, $\bar{\theta}, \gamma$ and ρ_i, the LFC system (8) subject to stochastic injection attacks is secure in mean square by using the networked PI controller in (9) and the data transmission scheme in II-D, if there exist matrices $P_i > 0, \Xi > 0, Q_i > 0, R_i > 0$ $(i = 1, 2)$ and matrices W and M with appropriate dimensions such that

$$\begin{bmatrix} \bar{\Upsilon}_{11} & * \\ \bar{\Upsilon}_{21} & \bar{\Upsilon}_{22} \end{bmatrix} < 0 \quad (28)$$

where

$$\begin{aligned}
\bar{\Upsilon}_{11} &= \mathcal{I}_1^T\bar{\Gamma}_1 + \bar{\Gamma}_1^T\mathcal{I}_1 + \mathcal{I}_1(Q_1+Q_2)\mathcal{I}_1 - \mathcal{I}_2^TQ_1\mathcal{I}_2 \\
&\quad -\mathcal{I}_4^TQ_2\mathcal{I}_4 + M_1 + M_2 - \varsigma\mathcal{I}_6^T\mathcal{I}_6 - \gamma^2\mathcal{I}_7^T\mathcal{I}_7 \\
&\quad +[\bar{H}\mathcal{I}_3 + (1+\kappa)\mathcal{I}_5]^T\sigma\Xi[\bar{H}\mathcal{I}_3 + (1+\kappa)\mathcal{I}_5] \\
&\quad -(1+\kappa^2\sigma)\mathcal{I}_5^T\Xi\mathcal{I}_5 + \mathcal{I}_1(\varsigma\bar{F}^T\bar{F} + \bar{H}^T\bar{H})\mathcal{I}_1, \\
\bar{\Gamma}_1 &= [P\bar{A}\ 0\ (1-\bar{\theta})\bar{B}M\bar{H}\ 0\ (1-\bar{\theta})\bar{B}M\bar{H}\ \bar{\theta}\bar{B}M\ P\bar{B}_\omega], \\
\bar{\Gamma}_2 &= [0\ 0\ -\bar{B}M\bar{H}\ 0\ -\bar{B}M\ \bar{B}M\ 0], \\
\bar{\Upsilon}_{21} &= \begin{bmatrix} \bar{\Gamma}_1 \\ \sqrt{\bar{\theta}(1-\bar{\theta})}\bar{\Gamma}_2 \end{bmatrix}, P = U\begin{bmatrix} P_1 & 0 \\ 0 & P_2 \end{bmatrix}U^T, \\
\bar{\Upsilon}_{22} &= diag\{-2\rho_1 P + \rho_1^2\mathcal{R}, -2\rho_2 P + \rho_2^2\mathcal{R}\}
\end{aligned}$$

matrix U is defined in Lemma 2, and the other symbols are defined in Theorem 1. Furthermore, the controller gains are given by

$$K = (\bar{B}^TP\bar{B})^{-1}\bar{B}^T\bar{B}M \quad (29)$$

Proof: Using Schur complement, one has

$$\begin{bmatrix} \Upsilon_{11} & * \\ \Upsilon_{21} & \Upsilon_{22} \end{bmatrix} < 0 \quad (30)$$

from (21), where Υ_{11} is defined in Theorem 1, and

$$\Upsilon_{21} = \begin{bmatrix} P\Gamma_1 \\ \sqrt{\bar{\theta}(1-\bar{\theta})}P\Gamma_2 \end{bmatrix}, \Upsilon_{22} = -diag\{P\mathcal{R}^{-1}P, P\mathcal{R}^{-1}P\}$$

For a positive scalar ρ_i, it is true that

$$(\mathcal{R} - \rho_i^{-1}P)\mathcal{R}^{-1}(\mathcal{R} - \rho_i^{-1}P) > 0 \quad (31)$$

It follows that

$$-P\mathcal{R}^{-1}P \leq -2\rho_iP + \rho_i^2\mathcal{R} \quad (32)$$

Then, one can know that

$$\begin{bmatrix} \Upsilon_{11} & * \\ \Upsilon_{21} & \bar{\Upsilon}_{22} \end{bmatrix} < 0 \quad (33)$$

is a sufficient condition to guarantee (30) holds.

Notice that $\bar{B}$ is full column rank, and it has singular decomposition $\bar{B} = U\bar{B}_0V$. From Lemma 2, one knows that there exist a matrix X such that $P\bar{B} = \bar{B}X$. Defining $M = XK$ yields that $P\bar{B}K = \bar{B}XK = \bar{B}M$. Therefore, (28) can be obtained by substituting P and $P\bar{B}K$ with $U\bar{P}U^T$ and $\bar{B}M$, respectively.

It is easy to obtain (29) from the equation that $K = (\bar{B}^TP\bar{B})^{-1}(\bar{B}^TP\bar{B})K$ with $P\bar{B}K = \bar{B}M$. ■

To summarize, the design of event-triggered LFC systems subject to stochastic attacks can be described as follows

Step 1: Initialize the parameters of ETM (κ, σ) in (15), network $(\mu_1, \mu_2, \bar{\theta})$ and control performance $(\gamma, \bar{f})$;

Step 2: Initialize ρ_1 and ρ_2, use Matlab LMI Toolbox to find feasible results of Ξ in (15) and K_P and K_I in (9) according to Theorem 2, go to step 3; otherwise, repeat step 1;

Step 3: Based on the current releasing instant, find the next releasing instant according to (16), repeat Step 3.

IV. CASE STUDIES

In this section, a 3-area power system with networked LFC scheme is studied to show the effectiveness of the proposed method. The synchronization coefficient between the areas are: $T_{12} = 0.2\ p.u./rad, T_{13} = 0.25p.u./rad$ and $T_{23} = 0.12\ p.u./rad$.The other nominal parameters are listed in Table 1.

TABLE 1. Nominal parameters of 3-area LFC systems.

	T_p	T_g	T_t	k_p	R	β
Area 1	10	0.1	0.3	1.0	0.05	21.0
Area 2	8	0.17	0.4	0.67	0.05	21.5
Area 3	6.67	0.2	0.35	0.56	0.05	21.8

Suppose the sampling period $h = 0.02$ s, and the network-induced delay satisfies 5ms $\leq \tau_{t_k} \leq$ 20 ms. The bound of cyber-attack is $\varsigma = 0.05$. Set $\kappa = 0.35, \sigma = 0.4, \bar{f} = 0.02$

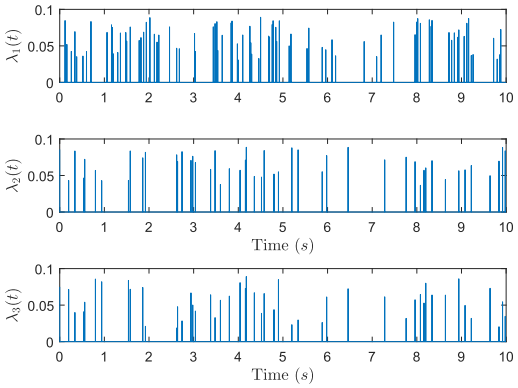

FIGURE 2. The attacks launched by adversaries.

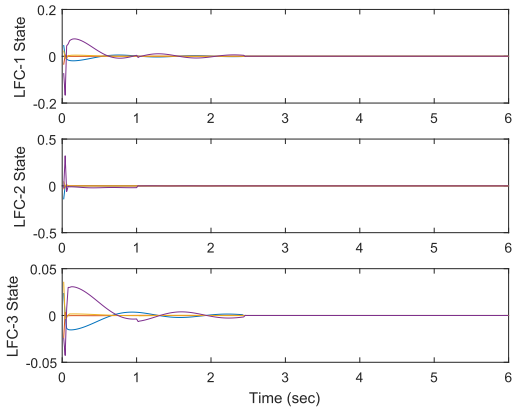

FIGURE 3. State responses of LFC systems under attacks.

and $\gamma = 15$. From Theorem 2, one can get the controller gains as

$$K_1 = \begin{bmatrix} -0.0470 & -0.0102 \end{bmatrix},$$
$$K_2 = \begin{bmatrix} -0.0504 & -0.0089 \end{bmatrix},$$
$$K_3 = \begin{bmatrix} -0.0530 & -0.0089 \end{bmatrix}$$

and the weight of ETM as

$$\Xi_1 = \begin{bmatrix} 9.2602 & 3.8756 \\ 3.8756 & 803.0429 \end{bmatrix},$$
$$\Xi_2 = \begin{bmatrix} 8.7566 & 2.7590 \\ 2.7590 & 796.2120 \end{bmatrix},$$
$$\Xi_3 = \begin{bmatrix} 8.4733 & 2.2480 \\ 2.2480 & 792.0907 \end{bmatrix}$$

Suppose the initial state $x_1(t) = [0.048, -0.036, 0.024, -0.072]$, $x_2(t) = [-0.144, -0.036, 0.048, -0.024]$, $x_3(t) = [0.024, -0.024, 0.036, -0.024]$, and the stochastic false data injection attacks are depicted in Figure 2. Figure 3 shows the state responses of the LFC system under the attack. It can be seen that the LFC system can operate normally under the attacks. The data releasing instants and releasing period are depicted in Figure 4, from which one can see that the releasing rate when the system has disturbance is higher than the one in other periods thanks to the proposed ETM. Accordingly, the controller can get more sampling data to meet the requirement of control performance. However, the average releasing period is much higher than the sampling period.

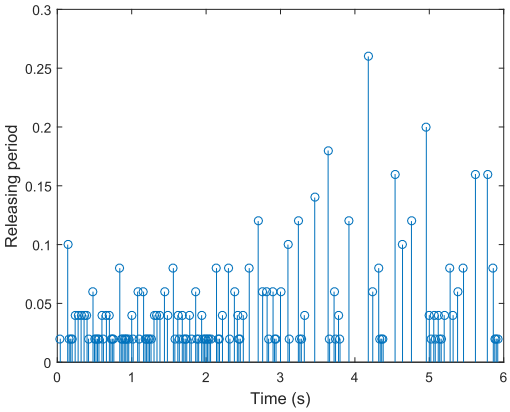

FIGURE 4. Data releasing period.

V. CONCLUSION

The problem of secure load frequency control for multi-area power systems has been formulated. A resilient output feedback control strategy was developed for the LFC system subject to stochastic cyber-attacks. New secure criteria are proposed to guarantee the frequency within a secure range. To relieve the burden of network bandwidth, a novel ETM was proposed. Under which the average data releasing rate is far below than the one using the time triggered mechanism. However the controller can receive much more sampling data transmitted from the network than the conventional ETM when the system has some external disturbances under the proposed ETM. A 3-area power system was studied to manifest the effectiveness of the proposed method.

REFERENCES

[1] A. Pappachen and A. P. Fathima, "Critical research areas on load frequency control issues in a deregulated power system: A state-of-the-art-of-review," *Renew. Sustain. Energy Rev.*, vol. 72, pp. 163–177, May 2017.

[2] C. Chang and W. Fu, "Area load frequency control using fuzzy gain scheduling of pi controllers," *Electr. Power Syst. Res.*, vol. 42, no. 2, pp. 145–152, 1997.

[3] N. Chuang, "Robust H_∞ load-frequency control in interconnected power systems," *IET Control Theory Appl.*, vol. 10, no. 1, pp. 67–75, 2016.

[4] C. Peng, D. Yue, and M. R. Fei, "A higher energy-efficient sampling scheme for networked control systems over IEEE 802.15.4 wireless networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1766–1774, Oct. 2016.

[5] D. Ye, M.-M. Chen, and H.-J. Yang, "Distributed adaptive event-triggered fault-tolerant consensus of multiagent systems with general linear dynamics," *IEEE Trans. Cybern.*, to be published.

[6] M. C. F. Donkers and W. P. M. H. Heemels, "Output-based event-triggered control with guaranteed L_∞-gain and improved and decentralized event-triggering," *IEEE Trans. Autom. Control*, vol. 57, no. 6, pp. 1362–1376, Jun. 2012.

[7] D. Yue, E. Tian, and Q.-L. Han, "A delay system method for designing event-triggered controllers of networked control systems," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 475–481, Feb. 2013.

[8] E. Tian, Z. Wang, L. Zou, and D. Yue, "Probabilistic-constrained filtering for a class of nonlinear systems with improved static event-triggered communication," *Int. J. Robust Nonlinear Control*, vol. 29, no. 5, pp. 1484–1498, 2019.

[9] Z. Gu, P. Shi, D. Yue, and Z. Ding, "Decentralized adaptive event-triggered H_∞ filtering for a class of networked nonlinear interconnected systems," *IEEE Trans. Cybern.*, vol. 49, no. 5, pp. 1570–1579, May 2019.
[10] Y. Chen, S. Kar, and J. M. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4618–4624, Sep. 2017.
[11] E. Mousavinejad, F. Yang, Q. L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/TCYB.2018.2843358.
[12] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Distributed Bayesian detection in the presence of Byzantine data," *IEEE Trans. Signal Process.*, vol. 63, no. 19, pp. 5250–5263, Oct. 2015.
[13] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.
[14] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Syst.*, vol. 35, no. 1, pp. 93–109, Feb. 2015.
[15] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/TCYB.2018.2861834.
[16] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.
[17] D. Ye, T.-Y. Zhang, and G. Guo, "Stochastic coding detection scheme in cyber-physical systems against replay attack," *Inf. Sci.*, vol. 481, pp. 432–444, May 2019.
[18] Z. Gu, X. Zhou, T. Zhang, F. Yang, and M. Shen, "Event-triggered filter design for nonlinear cyber-physical systems subject to deception attacks," *ISA Trans.*, to be published. doi: 10.1016/j.isatra.2019.02.036.
[19] J. Liu, L. Wei, X. Xie, and D. Yue, "Distributed event-triggered state estimators design for sensor networked systems with deception attacks," *IET Control Theory Appl.*, to be published. doi: 10.1049/iet-cta.2018.5868.
[20] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.
[21] J. Liu, T. Yin, M. Shen, X. Xie, and J. Cao, "State estimation for cyber–physical systems with limited communication resources, sensor saturation and denial-of-service attacks," *ISA Trans.*, to be published. [Online]. Available: https://doi.org/10.1016/j.isatra.2018.12.032.
[22] Z. Gu, T. Zhang, F. Yang, H. Zhao, and M. Shen, "A novel event-triggered mechanism for networked cascade control system with stochastic nonlinearities and actuator failures," *J. Franklin Inst.*, vol. 356, no. 4, pp. 1974–1995, 2019.

XIAOHONG ZHOU was born in Hunan, China, in 1992. She received the B.S. degree from Nanjing Forestry University, Nanjing, China, in 2013, where she is currently pursuing the Ph.D. degree. Her research interests include networked control systems, time-delay systems, and their applications.

ZHOU GU received the B.S. degree from North China Electric Power University, Beijing, China, in 1997, and the M.S. and Ph.D. degrees in control science and engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2007 and 2010, respectively. From 1996 to 2013, he was with the School of Power engineering, Nanjing Normal University, as an Associate Professor. He was a Visiting Scholar with Central Queensland University, Rockhampton, QLD, Australia, and The University of Manchester, Manchester, U.K. He is currently a Professor with Nanjing Forestry University, Nanjing. His current research interests include networked control systems, time-delay systems, reliable control, and their applications.

FAN YANG received the B.S. and Ph.D. degrees from Southeast University, Nanjing, China, in 2010 and 2016, respectively. He is currently a Lecturer with Nanjing Forestry University, Nanjing. His research interests include networked control systems, time-delay systems, reliable control, and their applications.