Event-triggered load frequency control of smart grids under deception attacks

Xinghua Liu1 | Dandan Bai1 | Yi-De Wu2 | Ming-Feng Ge2 | Alessandro N. Vargas3

1 School of Electrical Engineering, Xi’an University of Technology, Xi’an, China
2 School of Mechanical Engineering and Electronic Information, China University of Geosciences, Wuhan, China
3 Universidade Tecnológica Federal do Paraná, UTFPR, Av. Alberto Carazzai 1640, Cornélia, Procópio, Paraná, Brazil

Correspondence
Xinghua Liu, Department of Electrical Engineering, School of Automation and Information Engineering, Xi’an University of Technology, Xi’an 710054, China.
Email: liuxh@xaut.edu.cn

Abstract
This paper shows a result for the load frequency control with event-triggering mechanism under deception attacks. Specifically, the event-triggering mechanism and deception attacks are considered in the dynamic model of power systems. The event-triggering is used to reduce the frequency of controller update and communication between nodes. The $H_{\infty}$ controller is designed and the stability of the system is guaranteed by utilising the Lyapunov–Krasovskii functional method and truncated Bessel–Legendre inequality. Finally, a three-area interconnected networked power system is given and the simulated results are presented to show the effectiveness of the developed theoretical results.

1 INTRODUCTION

Driven by green energy conservation awareness, smart grid has become a key area of competing development in the world, which has the advantages of high controllability, high energy efficiency, and self-healing [1–3]. However, at the same time, privacy and security problems in the smart grid are gradually exposed and become an important factor restricting its further development [4–6]. With the development of the smart power grid, a mass of smart terminals are introduced into the smart power grid. In the aspect of network attacks, Denial-of-Service (DoS) attacks [7–9] and deception attacks [10, 11] are the most concerned at present. Deception attacks are a kind of attack commonly adopted by attackers. The attacker will inject wrong data information into the target system, making the data transmitted in the sensor produce errors, and then make biased decisions [12]. Compared with DoS attacks, the attacker can keep deception attacks hidden and not easy to be detected, and deception attacks have randomness. Therefore, to ensure the safe and stable operation of the smart grid, it is of great significance to study the secure communication and protection technology of the smart grid.

Load frequency control plays an indispensable role in the smart grid [13]. It should be noted that frequency fluctuation can cause power system vibrations, operation instability and various faults, and may affect the safety. Therefore, load frequency problem has attracted many scholars’ attention since it came into being. In the past few decades, there have been many LFC schemes. When it comes to the control approaches of LFC, proportional–integral–differential (PID) control [14–16] is the most widely used in practical power systems, since PID control strategy is simple to apply, and can well adjust the steady error of the systems to zero. PI control [17–19] is then designed to overcome the complexity of PID algorithm. In [20], a graphical method to compute the stabilizing values of PI controller parameters is presented for a single-area LFC system with time delay. In [21], a new PI control method is proposed to solve the stability problem of delayed LFC scheme with fixed and time-varying delay, where the further improved integral inequality in the form of infinite series is used to prove the stability of the power grids.

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2021 The Authors. IET Control Theory & Applications published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology
During the past few years, event-triggered control, also called event-based control or event-driven control has been proposed to reduce the date transmission, minimize the network pressure and save the network bandwidth in the network system. Wen et al. [22] considered the load frequency control for power systems with communication delays via an event-triggering mechanism to reduce the communication burdens and lower the control updating frequency. In this trend, an LFC architecture based on auxiliary adaptive dynamic planning is proposed in [23], and event-triggered management will play an important role in reducing communication and computing costs. Considering the influence of network induced delay, signal quantization, and data loss in the communication link between the device and the controller, a design framework of an event-triggered network control system based on passivity is introduced in [24]. For a multi-area closed-loop power system, a scheme of flexible event-triggered communication is introduced in [24].

For a multi-area closed-loop power system, a scheme of flexible event-triggered communication is designed in [7]; this scheme allows DoS attacks to cause a system, a scheme of flexible event-triggered communication is designed in [7]; this scheme allows DoS attacks to cause a certain degree of packet loss advantage of improving transaction efficiency. However, LFC of smart grid subject to random deception attacks has not been paid enough attention especially when the event-triggered control protocol is simultaneously considered. In response to the above discussion, we endeavour to investigate the event-triggered LFC of smart grids under deception attacks in this paper, since deception attacks will randomly reduce the integrity of transmission packets and affect the performance of smart grid. By employing the stochastic analysis techniques and matrix inequalities, sufficient conditions are established to guarantee the $H_{\infty}$ performance and the desired controller gain is given in terms of some linear matrix inequalities. The main contributions of this paper are highlighted as follows:

1. A closed-loop time-delay LFC dynamic model is established within which load frequency control problem can be conveniently handled in the presence of event-triggering mechanism and random deception attacks.

2. In the process of proving the stability criterion, we utilize the truncated Bessel–Legendre integral inequality, which is less conservative than Jensen inequality and Wirtinger inequality. Simultaneously, we construct appropriate multiple Lyapunov functions, which is less conservative than the single Lyapunov functional method.

3. Based on the stochastic analysis techniques, Lyapunov–Krasovskii (L–K) theory and matrix inequalities, sufficient conditions are derived in terms of LMIs to achieve asymptotical stability and $H_{\infty}$ performance for the smart grid under deception attacks.

The rest of this paper is organized as follows. In Section 2, we propose our time-delay LFC dynamic model with an event-triggering mechanism under deception attacks. In Section 3, we analyse the stability of the system and design the controller. A numerical example and simulated studies are conducted to verify the proposed results in Section 4. Finally, Section 5 concludes this paper.

Notation. The following notations are used throughout this paper. $\mathbb{E}\{\cdot\}$ represent mathematical expectation. We use $\mathbb{R}^n$ to denote the $n$-dimensional Euclidean space and $\mathbb{R}^{m \times n}$ the set of all $m \times n$ matrices. diag(·) represent diagonal matrix. Let $\|x\|$ and $\|A\|$ be the Euclidean norm of a vector $x$ and a matrix $A$, respectively. For a symmetric block matrix, we use $\star$ to denote the terms introduced by symmetry.

2 | PROBLEM FORMULATION

2.1 | Multi-area LFC model in smart grid

The power system is a complex dynamical system with nonlinear and time-varying terms. Inspired by [10], the framework of network-based LFC of the $i$th area power system is given in Figure 1.

From Figure 1, the following relation can be obtained

$$\begin{align*}
\Delta \dot{f}_i &= -\frac{D_i}{M_i} \Delta f_i - \frac{1}{M_i} \Delta P_{\text{tie}-i} + \frac{1}{M_i} \Delta P_{\text{m}i} - \frac{1}{M_i} \Delta P_{\text{di}} \\
\Delta \dot{P}_{\text{m}i} &= -\frac{1}{T_{\text{ch}i}} \Delta P_{\text{m}i} + \frac{1}{T_{\text{ch}i}} \Delta P_{\text{di}} \\
ACE_i &= \beta_i \Delta f_i + \Delta P_{\text{tie}-i} \\
\Delta \dot{P}_{\text{v}i} &= -\frac{1}{R_i T_{\text{g}i}} \Delta f_i - \frac{1}{T_{\text{g}i}} \Delta P_{\text{v}i} + \frac{1}{T_{\text{g}i}} u(t) \\
\Delta \dot{P}_{\text{tie}-i} &= 2\pi \sum_{j=1,j \neq i} T_{ij}(\Delta f_i - \Delta f_j).
\end{align*}$$

(1)

where $\dot{s}$ is the Laplace variable. $\Delta f_i$ is the system deviation value of the $i$th area, $\Delta P_{\text{m}i}$ represents the mechanical power deviation value, $\Delta P_{\text{v}i}$ represents the position quantity of regulating valve, and $\Delta P_{\text{di}}$ represents the load of the $i$th area. $R_i$ is the speed drop coefficient, $M_i$ is the moment of inertia of the generator, $D_i$ is the damping coefficient of the generator, $T_{\text{ch}i}$ and $T_{\text{g}i}$ are the steam capacity time constant and the governor time constant respectively, $\beta_i$ represents the conversion coefficient of system power and frequency. $ACE_i(t)$ is the area control error signal of the $i$th area. $\Delta P_{\text{tie}-i}$ is the power deviation value of the sub-area tie-line in the $i$th area, $T_{ij}$ is the synchronization power coefficient of the tie-line between the $i$th and $j$th control areas [10].

According to equation (1), the LFC dynamic model of the multi-area power system can be described as follows

$$\begin{align*}
\dot{x}(t) &= Ax(t) + Bu(t) + Fw(t) \\
y(t) &= Cx(t),
\end{align*}$$

(2)
FIGURE 1  The framework of network-based LFC of \(i\)th area power system

where

\[
\begin{align*}
\mathbf{x}(t) &= \begin{bmatrix} x_1^T(t) & x_2^T(t) & \cdots & x_N^T(t) \end{bmatrix}^T, \\
\mathbf{y}(t) &= \begin{bmatrix} y_1^T(t) & y_2^T(t) & \cdots & y_N^T(t) \end{bmatrix}^T, \\
\mathbf{u}(t) &= \begin{bmatrix} u_1^T(t) & u_2^T(t) & \cdots & u_N^T(t) \end{bmatrix}^T, \\
\mathbf{\omega}(t) &= \begin{bmatrix} \omega_1(t) & \omega_2(t) & \cdots & \omega_N(t) \end{bmatrix}^T, \\
\mathbf{\chi}(t) &= \begin{bmatrix} \triangle f_i & \triangle P_{m_i} & \triangle P_{v_i} & \int_0^t A C E_i(s) ds & \triangle P_{tie-j} \end{bmatrix}^T, \\
\mathbf{\phi}(t) &= \begin{bmatrix} A \mathbf{1}_1 & A \mathbf{1}_2 & \cdots & A \mathbf{1}_N \\ A \mathbf{2}_1 & A \mathbf{2}_2 & \cdots & A \mathbf{2}_N \\ \vdots & \vdots & \ddots & \vdots \\ A \mathbf{N}_1 & A \mathbf{N}_2 & \cdots & A \mathbf{N}_N \end{bmatrix}, \\
\mathbf{C}_i &= \begin{bmatrix} \beta_i & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \\
B &= \text{diag}\{B_1, \ldots, B_N\}, \quad C = \text{diag}\{C_1, \ldots, C_N\}, \\
F &= \text{diag}\{F_1, \ldots, F_N\}, \\
B_i &= \begin{bmatrix} 0 & 0 & \frac{1}{T_{gi}} & 0 & 0 \end{bmatrix}^T,
\end{align*}
\]

Using ACE as the input of the controller, the PI load frequency controller is designed as follows

\[
u(t) = -K P A C E(t) - K I \int_0^t A C E(s) ds = -K P_i(t) = -K C \chi(t),
\]

where \(K = \text{diag}\{K_1, \ldots, K_N\}\), \(K_i = [K_{P_i} \ K_{I_i}]\), \(K_{P_i}\) and \(K_{I_i}\) are the proportional and integral gains, respectively.

We assume the controller works under an open network communication. It means that the transmission is vulnerable to
network attacks. Therefore, an attacker sends false system information to the controller or sensor, including inaccurate measurements, faulty controller output, or wrong timestamps. In this scenario, corrupted information gives rise to deception, which disrupts data transmission. In order to account attacks in our formulation, we write the control rule as

\[ u(t) = \alpha(t) \zeta(t) - (1 - \alpha(t)) K C x(t), \]  

where \( \zeta(t) \) is an energy-bounded signal belonging to \( L_2[0, +\infty) \). \( \alpha(t) \in \{0, 1\} \) is a stochastic variable that defines the occurrence of attacks and obeys Bernoulli distribution. More specifically, if \( \alpha(t) = 1 \), the controller \( u(t) = \zeta(t) \), which means that the deception attacks occurred in transmission. If \( \alpha(t) = 0 \), the controller becomes \( u(t) = -BK C x(t) \), indicating that the sampling measurement has been transmitted successfully. We assume in addition that \( \mathbb{E}\{\alpha(t)\} = \alpha_0 \).

Define \( G(\alpha(t)) = - (1 - \alpha(t)) BK C \), \( J(\alpha(t)) = \alpha(t) B^T \zeta(t) \), then the state equation can be rewritten as

\[
\begin{align*}
\dot{x}(t) &= Ax(t) + G(\alpha(t)) x(t) + J(\alpha(t)) + F \omega(t) \\
y(t) &= Cx(t).
\end{align*}
\]

(5)

### 2.2 Event-triggered control

Motivated by [7], we introduce the event-triggering mechanism as follows:

\[
t_{k+1} = t_k + \min_{l \in \mathbb{N}} \{ \| b \| e^T(i_j, b) C T C \rho C x(i_j, b) > \sigma y^T(t_k) x(t_k) \},
\]

(6)

where \( e(i_j, b) = x(i_j, b) - x(t_k, b) \), \( t_k = t_k + l \| b \| \) \( l = 0, 1, ..., t_{k+1} - t_k - 1 \). \( t_k \) \( k = 0, 1, 2, ... \) are some integers such that \( \{ l_0, l_1, l_2, ... \} \subset \{ 0, 1, 2, ... \} \). \( t_k, b \) and \( t_{k+1}, b \) are the sampling times of two adjacent signals transmitted to the controller before and after satisfying the triggering conditions, respectively. The event-triggering parameter \( \sigma \) is a preset constant. The trigger matrix \( \rho \) is a positive definite matrix to be solved, and \( b \) is the sampling period of LFC.

**Remark 1.** The sampling period \( b \) can significantly affect the frequency stability of the power systems. In [28], the transmission delay margin of the control schemes under different sampling period is studied. The results show that the proposed control schemes can provide good robustness under small sampling period \( (b = 0.1) \), and the designed controllers can tolerate large parameter uncertainties. If the sampling period of the power systems is too large, the control signal packet will be lost when the communication or physical fault occurs. In such a large sampling period (e.g. \( b = 11.6 \) s given in [28]), the stable operation of the systems cannot be guaranteed if multiple packets are continuously lost within tens of seconds. Therefore, we had better choose a smaller sampling period to reduce the burden of the communication network and ensure the stable operation of the systems in the case of communication failure.

By substituting the output \( y(t) \) of (5) into the threshold condition (6), the triggering condition of the event-triggering mechanism can be obtained as follows:

\[
t_{k+1} = t_k + \min_{l \in \mathbb{N}} \{ \| b \| e^T(i_j, b) \Phi e(i_j, b) > \sigma y^T(t_k) x(t_k) \},
\]

(7)

where \( \Phi = C^T \rho C \).

Based on the communication scheme (6), it is known that the sampled-data are not transmitted over the communication networks unless the threshold condition is satisfied. For introducing the proposed event-triggered communication scheme (6) at each sampling instant to determine whether the currently sampled data should be transmitted through the communication networks, the holding interval \( \Omega = \{ t_k + \tau_k, t_{k+1} + \tau_{k+1} \} \) of the ZOH is also divided into the following subsets \( \Omega_i \),

\[
\Omega = \bigcup \Omega_i, \Omega_i = \{ i_j, i_j + b + \tau_i \},
\]

where

\[
\tau_i = \begin{cases} 
\tau_i, l = 0, 1, 2, ..., t_{k+1} - t_k - 2, \\
\tau_i + 1, l = t_{k+1} - t_k - 1.
\end{cases}
\]

**Remark 2.** It should be mentioned that \( \tau_i \) represents the time delay existing when all released signals \( x(i_j, b) \) arrive at the actuator. \( \tau_k \) represents the time delay generated from time 0 to time \( t_{k+1} - t_k - 2 \), and \( \tau_{k+1} \) represents the time delay generated from time \( t_{k+1} - t_k - 1 \).

Define \( \tau(t) = t - i_j, t \in \Omega_i \), output feedback \( u(t) \) can be rewritten as

\[
u(t) = -(1 - \alpha(t)) K C x(t - \tau(t)) + \alpha(t) \zeta(t) + K C x(i_j, b),
\]

(8)

where \( \tau(t) = 1, 0 \leq \tau(t) \leq \bar{\tau} + \tau_M \), \( \bar{\tau} = b + \tau_M \), \( \tau_M \) is the upper bound of the maximum allowable delay. Substituting (8) into (2) we have that the initial state model (2) of the multi-area power system with LFC can be rewritten as the following \( ACE \)-dependent time-delay model

\[
\begin{align*}
\dot{x}(t) &= Ax(t) + G(\alpha(t)) x(t - \tau(t)) \\
&+ J(\alpha(t)) + BK C e(i_j, b) + F \omega(t) \\
y(t) &= Cx(t), t \in \Omega_i.
\end{align*}
\]

(9)

For sake of simplicity, we split (9) into two parts, i.e.

\[
\dot{x}(t) = \phi(t) + (\alpha_0 - \alpha(t)) \psi(t),
\]

(10)
where

\[
\begin{aligned}
\begin{cases}
\dot{\phi}(t) = A\phi(t) + G(x_i)x(t - \tau(t)) \\
+ f(x_i) + BKCx_i(t) + F\omega(t) \\
\psi(t) = -BKCx(t - \tau(t)) - B\xi(t).
\end{cases}
\end{aligned}
\]

**Definition 1.** If the following conditions are satisfied, the closed-loop system (9) is asymptotically stable in the security sense, and the disturbance rejection level of $H_{\infty}$ is $\gamma$.

1. When $\omega(t) = 0$ and $\xi(t) = 0$, the system (9) is asymptotically stable, that is, in the neighbourhood of equilibrium state, there is a continuous first-order partial derivative of $V(x(t))$ and $V'(x(t))$ is positive definite and $E[V'(x(t))]$ is negative definite, then the system is asymptotically stable in equilibrium;
2. Under the zero initial condition, i.e. $x(t) = 0, t \in [-\tau, 0]$, for any non-zero $\omega(t) \in L_2[0, \infty]$ and $\xi(t) \in L_2[0, \infty]$, for a given $\gamma$, the following inequality hold:

\[
E[\|y(t)\|_2] \leq \gamma E[\|\omega(t)\|_2 + \|\xi(t)\|_2].
\]

**Remark 3.** Asymptotically stable in the security sense means that the closed-loop system (9) can be achieved asymptotically stability performance even if the measurement and control signals transmission fails under deception attacks.

**Lemma 1.** [26] For a given positive definite symmetric real matrix $R > 0$, any differentiable function $x$ in $[a, b] \rightarrow \mathbb{R}^n$,

\[
\int_a^b x^T(u)Rx(u)du \geq \frac{1}{b - a} \Theta^T \text{diag}(R, 3R, 5R) \Theta
\]

holds, where

\[
\Theta = \begin{bmatrix}
    x(b) - x(a) \\
    x(b) + x(a) - \frac{2}{b - a} \int_a^b x(u)du \\
    x(b) - x(a) - \frac{6}{b - a} \int_a^b \lambda_{x,u}(u)x(u)du
\end{bmatrix},
\]

\[
\lambda_{x,u}(u) = \frac{2u - a}{b - a} - 1.
\]

**Lemma 2.** [25] (Convex property) For any symmetric positive integer $n, \alpha$ and scalar $\alpha \in (0, 1)$, given the $n \times n$-dimensional matrix $R > 0$, two matrices $W_1 \in \mathbb{R}^{\alpha \times n}$ and $W_2 \in \mathbb{R}^{\alpha \times n}$, all vectors $\xi \in \mathbb{R}^n$ are defined, and the function $\Theta(\alpha, R)$ is defined as

\[
\Theta(\alpha, R) = \frac{1}{\alpha} \xi^T W_1 RW_1^T \xi + \frac{1}{1 - \alpha} \xi^T W_2 RW_2^T \xi.
\]

If there is a matrix $X \in \mathbb{R}^{n \times n}$ that satisfies $X^T R X > 0$, then the following inequality holds

\[
\min_{\alpha \in [0,1]} \Theta(\alpha, R) \geq \begin{bmatrix} W_1^T \xi \\ W_2^T \xi \end{bmatrix}^T \begin{bmatrix} R & X \\ X^T & R \end{bmatrix} \begin{bmatrix} W_1^T \xi \\ W_2^T \xi \end{bmatrix}.
\]

### 3 | MAIN RESULTS

In this section, we first analyse the asymptotical stability and $H_{\infty}$ performance of the LFC dynamic model of the power system (9), which takes into account the event-triggered mechanism and deception attacks. Then a PI controller design method based on event-triggered is presented and the controller gain is derived.

**Theorem 1.** For given disturbance rejection level $\gamma > 0$, $\alpha_0 \geq 0$, $\tau_M > 0, \sigma > 0, \tau = b + \tau_M$, the LFC system (9) is asymptotically stable, if there exist real symmetric matrices $P > 0, Q_1 > 0, Q_2 > 0, R > 0, W > 0, \Phi > 0$ with appropriate dimensions and an arbitrary matrix $N$ satisfying the following LMI

\[
\begin{bmatrix}
    \Gamma_{11} & \Gamma_{12}^T \\
    \Gamma_{21} & \Gamma_{22}
\end{bmatrix} < 0,
\]

\[
\Xi = \begin{bmatrix}
    \text{diag}(R, 3R, 5R) \\
    N^T \\
    \text{diag}(R, 3R, 5R)
\end{bmatrix} > 0,
\]

where

\[
\Gamma_{11} = \Gamma_{111} - \Gamma_{112},
\]

\[
\Gamma_{111} = \begin{bmatrix}
    \Sigma_1^{3 \times 3} & * & * \\
    0^{3 \times 3} & \Sigma_2^{3 \times 3} & * \\
    0^{3 \times 3} & 0^{3 \times 3} & \Sigma_3^{3 \times 3}
\end{bmatrix},
\]

\[
\Sigma_1 = \begin{bmatrix}
    B^T P + C^T C + Q_1 - \frac{\pi^2}{4} W & * & * \\
    -(1 - \alpha_0)C^T K^T B^T P + \frac{\pi^2}{4} & -\frac{\pi^2}{4} & W + \sigma \Phi & * \\
    0 & 0 & -Q_2
\end{bmatrix},
\]

\[
\Sigma_2 = \begin{bmatrix}
    C^T K^T B^T P & -\sigma \Phi & 0 \\
    F^T P & 0 & 0 \\
    \alpha_0 B^T P & 0 & 0
\end{bmatrix},
\]

\[
\Sigma_3 = \text{diag}(\sigma - 1) \Phi, -\gamma^2 I, -\gamma^2 I),
\]
Let
\[
\xi(t) = \text{col} \begin{bmatrix}
\xi(t), \xi(t-\tau(t)), \xi(t-\bar{\tau}), \frac{1}{\tau(t)} \\
\int_{t-\tau(t)}^{t} \xi(p) dp, \frac{1}{\tau(t)} \int_{t-\tau(t)}^{t} \lambda_{t-\tau(t)}(p) \xi(p) dp, \frac{1}{\bar{\tau} - \tau(t)} \\
\int_{t-\bar{\tau}}^{t-\tau(t)} \xi(p) dp, \frac{1}{\bar{\tau} - \tau(t)} \int_{t-\bar{\tau}}^{t-\tau(t)} \lambda_{t-\tau(t)}(p) \xi(p) dp, \frac{1}{\tau(t)} \\
\end{bmatrix}
\]

By Lemma 1 we can obtain that
\[
-\tau \int_{t-\tau(t)}^{t} \dot{\xi}(p) R \dot{\xi}(p) dp \leq -\frac{1}{\bar{\tau} - \tau(t)} \left[ \begin{array}{c}
\xi(t) - \xi(t-\tau(t)) \\
\int_{t-\tau(t)}^{t} \xi(p) dp - \frac{2}{\tau(t)} \int_{t-\tau(t)}^{t} \xi(p) dp \\
\int_{t-\bar{\tau}}^{t-\tau(t)} \xi(p) dp - \frac{6}{\tau(t)} \int_{t-\bar{\tau}}^{t-\tau(t)} \lambda_{t-\tau(t)}(p) \xi(p) dp \\
\end{array} \right]^T.
\]

Take the expectation for both sides of derivative $\mathcal{L} V' (x(t))$, and then we have that
\[
E[\mathcal{L} V' (x(t)) ] = E[\mathcal{L} V'_1 (x(t)) ] + E[\mathcal{L} V'_2 (x(t)) ] + E[\mathcal{L} V'_3 (x(t)) ].
\]

Remark 4. It should be mentioned that we explicitly construct multiple Lyapunov functionals (13) to deal with smart grids under deception attacks, which is less conservative than the single Lyapunov functional method used in many existing papers.
Define $\frac{1}{\eta} = \frac{\tau}{t(\tau)}$, i.e. $\frac{1}{1-\eta} = \frac{\tau}{\tau-\tau(t)}$. By using Lemma 2 (Convex theorem), we have

$$-\frac{1}{\eta} \xi^T(t)(e_1 - e_2) R(e_1 - e_2) + 3(e_1 + e_2 - 2e_h) R(e_1 + e_2 - 2e_h)$$

$$+ 5(e_1 - e_2 - 6e_h) R(e_1 - e_2 - 6e_h)] \xi(t)$$

$$- \frac{1}{\eta} \xi^T(t)(e_3 - e_3) R(e_2 - e_3)$$

$$+ 3(e_2 + e_3 - 2e_h) R(e_2 + e_3 - 2e_h)$$

$$+ 5(e_2 - e_3 - 6e_h) R(e_2 - e_3 - 6e_h)] \xi(t)$$

$$\leq \xi^T(t) H_1^T \Xi H_1 \xi(t).$$

(16)

By (15) and (16), we can obtain that

$$E\{L^* (x(t))\} \leq 2x^T(t) P \Phi(t) + \xi^T(t)$$

$$Q_1 x(t) - x^T(t) \Phi(t) Q_2 x(t - \tau) + \Phi^T(t) \Xi(t) R \Phi(t)$$

$$+ \alpha_0 (1 - \alpha_0) \psi^T(t) \Xi(t) R \psi(t) - \xi^T(t) H_1^T \Xi H_1 \xi(t)$$

$$- \pi^2 \tau \frac{1}{\pi} [x(t) - x(i_k h)]^T W [x(t) - x(i_k h)]$$

$$+ \epsilon^T(i_k h) \Phi (x(i_k h)) - \epsilon^T(i_k h) \Phi (x(i_k h)).$$

(17)

Event-triggered communication strategy can ensure

$$\epsilon^T(i_k h) \Phi (x(i_k h)) < \sigma (\tau - \tau(t))$$

$$- \epsilon(i_k h)^T \Phi (\tau - \tau(t)) - \epsilon(i_k h).$$

(18)

Substituting (18) into (17), we have

$$E\{L^* (x(t))\} \leq E\{L^* (x(t))\}$$

$$+ \gamma^2 E\{\omega^T(t) \omega(t) + \xi^T(t) \xi(t)\}.$$

(19)

From the Schur theorem, the following holds

$$E\{L^* (x(t))\} \leq E\{L^* (x(t))\}$$

$$+ \gamma^2 E\{\omega^T(t) \omega(t) + \xi^T(t) \xi(t)\}.$$

(20)

Integrating both sides of (20), we have

$$E\{L^* (x(t))\} \leq E\{L^* (0)\}$$

$$\leq \gamma\|L^*\|_2 + E\{L^* (x(t))\}. (21)$$

At zero initial condition, then there are

$$E\{L^* (x(t))\} \leq \gamma\|L^*\|_2 + E\{L^* (x(t))\}. (22)$$

when $\omega(t) = 0$, $\xi(t) = 0$, we have

$$E\{L^* (x(t))\} \leq -E\{L^* (x(t))\} < 0. (23)$$

Then, there exists a positive scalar $\epsilon > 0$ that makes the following inequality hold

$$E\{L^* (x(t))\} \leq -\epsilon E\{L^* (x(t))\}. (24)$$

By above, when $\omega(t) = 0$ and $\xi(t) = 0$, we have $E\{L^* (x(t))\} \leq -\epsilon E\{L^* (x(t))\}$, the closed-loop system (9) is asymptotically stable in the security sense. When $\omega(t) \neq 0$ and $\xi(t) \neq 0$, we proved that under the zero initial condition, the closed-loop system (9) has $H_\infty$ disturbance suppression performance and the disturbance rejection level is $\gamma$. This completes the proof.  

Remark 6. By employing the truncated Bessel–Legendre inequality, which is more compact than Wirtinger inequality, to estimate the expectation of L–K function, we propose a new delay-dependent stability criterion for LFC smart grids under deception attacks. Besides, the convex lemma is used in the
closed-loop stability analysis. Hence, the method of combining the truncated Bessel–Legendre inequality and the convex lemma can be regarded as unique feature of our study.

Since the controller gain cannot be calculated directly from Theorem 1 due to the coupling terms, we give the following theorem to obtain the controller gains.

**Theorem 2.** For a given disturbance rejection level \( \gamma > 0 \), given scalars \( \alpha_0 \geq 0 \), upper and lower bounds of time delay \( \tau_M > 0 \), \( \sigma > 0 \) and positive scalar \( \varepsilon \to 0 \), the LFC system (9) is asymptotically stable, if there exist real symmetric matrices \( X > 0 \), \( P > 0 \), \( Q > 0 \), \( \Phi > 0 \), full rank matrix \( U \) with appropriate dimensions, and arbitrary matrices \( \bar{N}, V \) satisfying the following LMI

\[
\begin{bmatrix}
\Gamma_{11} & * & * \\
\Gamma_{21} & \Gamma_{22} & * \\
\Gamma_{31} & 0 & -I
\end{bmatrix} < 0,
\]

where

\[
\Gamma_{11} = \Gamma_{111} - \Gamma_{112},
\]

\[
\Gamma_{111} = \begin{bmatrix}
\Sigma_1 & * & * \\
0 & \Sigma_2 & * \\
0 & 0 & \Sigma_3
\end{bmatrix},
\]

\[
\Sigma_1 = \begin{bmatrix}
AX + XA^T + \tilde{Q}_1 - \frac{\pi^2}{4} \tilde{E}^2 & * & * \\
-(1 - \alpha_0)C^T V^T B^T + \frac{\pi^2}{4} \tilde{E}^2 & * & * \\
0 & 0 & -\tilde{Q}_2
\end{bmatrix},
\]

\[
\Sigma_2 = \begin{bmatrix}
C^T V^T B^T & -\sigma \Phi & 0 \\
F^T & 0 & 0 \\
\alpha_0 B^T & 0 & 0
\end{bmatrix},
\]

\[
\Sigma_3 = \text{diag}(\delta - 1)\Phi, -\gamma^2 I, -\gamma^2 I,
\]

\[
\Gamma_{112} = H_2^T \bar{H}_2, \quad \Gamma_{31} = [C^T \quad 0^{\frac{2}{3}}]
\]

\[
\Gamma_{21} = [FR \tilde{G}, T \sqrt{A_0(1 - A_0)R \tilde{G}}]^T, \quad \Gamma_{22} = \text{diag}(R - 2X, R - 2X),
\]

\[
H_1 = [e_1 - e_2, e_1 + e_2 - 2e_4, e_1 - e_2 - 6e_5, e_2 - e_1 + e_2
\]

\[
+ e_1 - 2e_4 + e_2 - 6e_5]^{T},
\]

\[
\Lambda_0 = \{A^X - (1 - \alpha_0)BWC, 0^{4 \times 5} \quad BWC \quad F \quad \alpha_0 B\},
\]

\[
\Lambda_0 = \{0 \quad -BWC \quad 0^{\frac{2}{3}} \quad -B\}.
\]

**Proof.** Define

\[
\begin{aligned}
X &= P^{-1}, \quad \bar{Q}_1 = XQ_1 X, \quad \bar{Q}_2 = XQ_2 X, \\
\bar{R} &= XRX, \quad \bar{\Phi} = X\Phi X,
\end{aligned}
\]

\[
\bar{N} = \text{diag}(X, X, X) N \text{diag}(X, X, X),
\]

then pre- and post-multiplying inequality \( \Xi \) with \( \text{diag}(X, X, X, X, X) \), and pre- and post-multiplying inequality (11) with \( \text{diag}(X, \cdots, X, I, I, R^{-1}, R^{-1}) \), and using the Schur complement, we can get inequalities (25) and (27).

According to the above definition, there are nonlinear terms \(-X \bar{R}^{-1} X\). We need to linearize the nonlinear terms, then the nonlinear term \(-X \bar{R}^{-1} X\) is linearized by inequality \(-X \bar{R}^{-1} X \leq R - 2X\), and \(-X \bar{R}^{-1} X\) in the theorem is replaced by \(R - 2X\).

Since the matrix \( C \) is not invertible, in order to solve the controller gain, we define it as follows

\[
UC = KCX, \quad UC = CX,
\]

where \( U, V \) are matrices of appropriate dimensions. And then we can get

\[
(UC - CX)^T (UC - CX) = 0.
\]

**Remark 7.** In order to solve the stability condition described in Theorem 1 and obtain a feasible LMI solution, inspired by [30], we can transform (29) into a minimization problem. In such a way, by utilizing Schur complement we can get inequality (26) and \( \varepsilon \) can be solved as a minimum positive scalar. However, this paper does not give a specific value range for \( \varepsilon \) but restrict \( \varepsilon \to 0 \), since we can easily find a sufficiently small \( \varepsilon \) when (26) is satisfied.

According to Equation (28), the controller gain matrix \( K \) may be described as \( K = VU^{-1} \). This completes the proof.

### 4 NUMERICAL EXAMPLE

This section analyses a three-area interconnected power system to verify the effectiveness of the proposed load frequency control method. Table 1 shows the parameters of the three-area interconnected power system [22]. Figure 2 shows a schematic
TABLE 1  Three-area power system parameters

| Parameter | $D_i$ | $M_i$ | $\bar{R}_i$ | $T_{ch}$ | $T_{gi}$ | $\beta_i$ |
|-----------|-------|-------|-------------|--------|--------|---------|
| Area 1    | 1     | 10    | 0.05        | 0.30 s | 0.37 s | $\frac{2}{\bar{R}_1} + D_1$ |
| Area 2    | 1.5   | 12    | 0.05        | 0.17 s | 0.4 s  | $\frac{2}{\bar{R}_2} + D_2$ |
| Area 3    | 1.8   | 12    | 0.05        | 0.20 s | 0.35 s | $\frac{2}{\bar{R}_3} + D_3$ |

FIGURE 2  Schematic diagram of the relationship between the three-area interconnected power systems

diagram of the relationship between the three-area interconnected power systems.

Based on the results of Theorem 2, we set the sampling period $h = 0.01$, PI-based controller gains $K_p = 0.1$, $K_i = 0.1$, and $T_{12} = 0.2$ (pu/rad), $T_{13} = 0.12$ (pu/rad), $T_{23} = 0.25$ (pu/rad). From Table 1 and the modelling part mentioned earlier in this article, we can get the parameter matrices of each region as shown in [27].

The evolutions of random variable $\alpha(t)$ and random attack signals $\alpha(t)\xi(t)$ are shown in Figures 3 and 4, respectively. It can be seen the control input in Figure 5 and state trajectories

in Figure 7 that the frequency deviation of the controlled interconnected power system can be stabilized at about 15 s, which shows the effectiveness of the proposed method. The trigger frequency under the event-triggered mechanism is shown in Figure 6. Not only a lot of unnecessary continuous information interaction is avoided, but also certain attacks can be resisted, which effectively saves the limited network communication bandwidth.

5 | CONCLUSION

This paper mainly solved the problem of LFC under the combination of event-triggered communication and random attack signals. By using the convex property, we have derived the asymptotical stability and $H_{\infty}$ performance criteria. The
effectiveness of the controller has been verified by simulation. It has been proved that in the environment with random attack signals, the event-triggering mechanism is still effective and the control of the system can still achieve the expected effect, that is, the entire control process does not produce unnecessary frequency fluctuation. In future, our work will focus on anti-GDB (anti-GRC) schemes for load frequency control of power systems and renewable energy systems.

ACKNOWLEDGEMENTS
This work is partially supported by the National Natural Science Foundation of China (under Grant 61903296, U2003110), Innovative Talents Promotion Program-Young Science and Technology Nova Project (2020KJXX-094), Key Laboratory Project of Shaanxi Educational Committee under Grant 20JSl10, High Level Talents Plan of Shaanxi Province for Young Professionals, and Brazilian Agency CNPq Grant 421486/2016-3

ORCID
Xinghua Liu https://orcid.org/0000-0001-5665-3535

REFERENCES
1. Xing, H., et al.: Distributed algorithm for dynamic economic power dispatch with energy storage in smart grids. IET Control Theory & Applications 11(11), 1813–1821 (2017)
2. Zafar, U., Bayhan, S., Sanfilippo, A.: Home energy management system concepts, configurations, and technologies for the smart grid. IEEE Access 8, 119271–119286 (2020)
3. Chen, B., et al.: Networked microgrids for grid resilience, robustness, and efficiency: A review. IEEE Transactions on Smart Grid 12(1), 18–32 (2021)
4. Khurana, H., et al.: Smart-grid security issues. IEEE Security & Privacy 8(1), 81–85 (2010)
5. Shames, I., Farokhi, F., Summers, T.H.: Security analysis of cyber-physical systems using $H_2$ norm. IET Control Theory & Applications 11(11), 1749–1755 (2017)
6. Gope, P., Sikdar, B.: Privacy-aware authenticated key agreement scheme for secure smart grid communication. IEEE Transactions on Smart Grid 10(4), 3953–3962 (2019)
7. Peng, C., Li, J., Fei, M.: Resilient event-triggering $H_\infty$ load frequency control for multi-area power systems with energy-limited DoS attacks. IEEE Trans. Power Syst. 32(5), 4110–4118 (2017)
8. Sun, H.T., et al.: Output-based resilient event-triggered control for networked control systems under denial of service attacks. IET Control Theory & Applications 13(16), 2521–2528 (2019)
9. Qu, H., Zhao, J.: Stabilisation of switched linear systems under denial of service. IET Control Theory & Applications 14(11), 1438–1444 (2020)
10. Zhao, F., et al.: Secure load frequency control of smart grids under deception attack: a piecewise delay approach. Energies 12(12), 2266 (2019)
11. Tian, E., Peng, C.: Memory-based event-triggering $H_\infty$ load frequency control for power systems under deception attacks. IEEE Transactions on Cybernetics 50(11), 4610–4618 (2020)
12. Bu, X., et al: Event-triggered distributed filtering over sensor networks with deception attacks and partial measurements. Int. J. Gen. Syst. 47(5), 395–407 (2018)
13. Shayeghi, H., Shayanfar, H., Jalili, A.: Load frequency control strategies: A state-of-the-art survey for the researcher. Energy Convers Manage 50(2), 344–353 (2009)
14. Khodabakhshian, A., Hooshmand, R.: A new PID controller design for automatic generation control of hydro power systems. Electrical Power and Energy Systems 32(5), 375–382 (2010)
15. Tan, W.: Tuning of PID load frequency controller for power systems. Energy Conversion Management 50(6), 1465–1472 (2009)
16. Tan, W.: Unified tuning of PID load frequency controller for power systems via IMC. IEEE Trans. Power Syst. 25(1), 341–350 (2010)
17. Jiang, C.-F., Lu, C.-F.: Load-frequency control by hybrid evolutionary fuzzy PI controller. IEEE Proceedings-Generation, Transmission and Distribution 153(2), 196–204 (2006)
18. Li, P.-K., Zhu, H.-J., Li, Y.-Y.: Genetic algorithm optimization for AGC of multi-area power systems. Proceedings of IEEE TENCON 2(3), 1818–1821 (2002)
19. Daneshfar, F., Bevrani, H.: Multi-objective design of load frequency control using genetic algorithms. Electrical Power and Energy Systems 42(1), 257–263 (2012)
20. Sonmez, S., Ayasun, S.: Stability region in the parameter space of PI controller for a single-area load frequency control system with time delay. IEEE Trans. Power Syst. 31(1), 829–830 (2016)
21. Yang, F., He, J., Wang, D.: New stability criteria of delayed load frequency control systems via infinite-series-based inequality. IEEE Transactions on Industrial Informatics 14(1), 231–240 (2018)
22. Wen, S., et al.: Event-triggering load frequency control for multiarea power systems with communication delays. IEEE Trans. Ind. Electron. 63(2), 1308–1317 (2016)
23. Dong, L., et al.: An event-triggered approach for load frequency control with supplementary ADP. IEEE Trans. Power Syst. 32(1), 581–589 (2017)
24. Rahnama, A., Xia, M., Antsaklis, P.-J.: Passivity-based design for event-triggered networked control systems. IEEE Trans. Autom. Control 63(9), 2755–2770 (2018)
25. Peng, C., Yue, D., Han, Q.-L., Communication and Control for Networked Complex Systems. Springer, Heidelberg (2015)
26. Liu, K., Seuret, A., Xia, Y.: Stability analysis of systems with timevarying delays via the second-order Bessel-Legendre inequality. Automatica 76, 138–142 (2017)
27. Liu, X., et al.: Stability analysis for networked power systems with LFC and event-triggered communication. In: The 39th Chinese Control Conference, pp. 4424–4429. IEEE, Piscataway, NJ (2020)
28. Shangguan, X., et al.: Robust load frequency control for power system considering transmission delay and sampling period. IEEE Transactions on Industrial Informatics, https://doi.org/10.1109/TII.2020.3026336 (2020)
29. Peng, C., Zhang, J., Yan, H.: Adaptive event-triggering $H_\infty$ load frequency control for network-based power systems. IEEE Trans. Ind. Electron. 65(2), 1685–1694 (2018)
30. Yang, Y., Niu, Y., Zhang, Z.: Dynamic event-triggered sliding mode control for interval Type-2 fuzzy systems with fading channels. ISA Trans., https://doi.org/10.1016/j.isatra.2020.10.035 (2020)

How to cite this article: Liu X, Bai D, Wu Y-D, Ge M-F, Vargas AN. Event-triggered load frequency control of smart grids under deception attacks. IET Control Theory Appl. 2021;15:1335–1345. https://doi.org/10.1049/cth2.12124