

ORIGINAL RESEARCH

Robust networked power system load frequency control against hybrid cyber attack

Xinxin Lv¹  | Yonghui Sun² | Venkata Dinavahi³  | Xinlong Zhao¹ | Feng Qiao¹

¹School of Information Science and Engineering, Zhejiang Sci-tech University, Hangzhou, China

²College of Energy and Electrical Engineering, Hohai University, Nanjing, China

³Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta, Canada

Correspondence

Xinxin Lv.

Email: xinxinlv@zstu.edu.cn

Funding information

National Natural Science Foundation of China, Grant/Award Number: 61673161; General Projects of Zhejiang Provincial Department of Education, Grant/Award Number: 22220109-F; Natural Science and Engineering Research Council of Canada; Science Foundation of Zhejiang Sci-Tech University, Grant/Award Number: 21022311-Y

Abstract

Modern network and communication technologies are essential for the implementation and operation of load frequency control (LFC) systems. The measurements of crucial LFC system parameters will be compromised by attackers, rendering data received by the defence inaccurate and causing frequency fluctuations or even system collapse. To detect the potential attack on measured data and keep the LFC performance, an adaptive event-triggered scheme with fractional order global sliding mode control scheme is proposed in this paper. Furthermore, Markov theory is employed for the modelling process with energy storage to present a multi-area LFC power system considering renewable energy and hybrid cyber attacks. Stability and stabilisation criteria are built by employing improved Lyapunov stability theory and second-order Bessel-Legendre inequality. Finally, a two-area LFC system under hybrid cyber attacks and a modified IEEE 39-bus New England test power system with 3 wind farms are simulated to explore the efficacy of the proposed method.

KEYWORDS

linear matrix inequalities, load frequency control, Lyapunov methods, power system stability, robust control

1 | INTRODUCTION

Load frequency control (LFC) is significant for multi-area power systems since it is accountable for ensuring nominal frequency and the power exchange between areas is stable [1–3]. Depending on the area control errors (ACE) gathered from the distributed sensors, LFC may create the adjustment commands and send it to the generator set to control the power output [4–6]. Load frequency control is one of the essential applications of automatic generation control. However, the structure of the power system is becoming increasingly complex with new energy grid connections and the requirements for security and reliability of power systems are increasing [7–9]. Meanwhile, due to its reliance on modern network and communication technology, LFC is exposed to cyber attacks, like denial-of-service (DoS) attacks and deception attack, which will interfere with the control centre's directives for

adjustment and could result in severe grid mishaps [10–12]. Therefore, it is necessary to investigate the LFC power system under hybrid cyber attack.

To avoid fluctuation and keep the system operating normally when it is subject to hybrid cyber attacks, specific actions must be taken quickly. DoS attack will block the communication medium, while the communication data are neither sent nor received, thereby the communication information is lost; while the deception attack will steal and disguise the transmitted packets [13–15]. Hybrid cyber attacks will lead to serious communicated information leakage and undermine the security of infrastructure [16, 17]. For a deception attack, the stochastic variable which obeys the Bernoulli distribution is employed to model it [18–20]. To investigate the deception attack, a networked power system model with deception attacks and memory-based event-triggered schemes has been built [21]. The distributed model-free adaptive control method

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2023 The Authors. *IET Smart Grid* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

was applied for MIMO non-linear multiagent systems under deception attacks with consensus control and containment control [22]. Moreover, by assuming the period of attack and lower bound on attack sleeping periods are known, a state error-dependent switched system model was built to study the LFC power system subject to DoS attacks [23]. With the event-triggered scheme extensively applied in power systems, event-triggered LFC subject to DoS attack was investigated, such as event-triggered H_∞ LFC with DoS [24] and resilient dynamic event-triggered LFC power system under DoS attack [25]. In addition, some defence methods were designed against DoS attacks, for example, hierarchical attention-based defence methods were applied in LFC power systems to offset DoS attacks [26]. Inspired by this, considering that the deception attack and DoS attack will interrupt the measurement data, the event-trigger scheme can be applied to supplement the missing information. Therefore, when the system is under hybrid cyber-attacks, the design of performance event-triggered schemes and control strategies to offset the impact of hybrid cyber attacks on the LFC power system is a motivation for this investigation.

Motivated by the challenges of hybrid cyber-attacks integrated into power systems, the robust LFC with adaptive event-triggered (AET) scheme, fractional-order global sliding mode control (FOGSMC) strategy is investigated in this article. Considering the impact of hybrid cyber-attacks, further quantity data packets are needed to offset the missing and false information than the traditional event-triggered schemes. Thus, an AET scheme with an adaptively adjusted threshold is adopted in this paper. Meanwhile, to improve the system stability of multi-area LFC power systems subject to hybrid cyber-attacks, a novel FOGSMC strategy is designed in this study. In addition, Markov theory is utilised to model the multi-area LFC power system considering transmission time delays. Then, the improved Lyapunov stability theory and second-order Bessel-Legendre (B-L) inequality are applied to build stability and stabilisation criteria. Consequently, the following improvements are proposed:

- (1) To mitigate the congested communication traffic and keep the security of the power system, an AET scheme is deployed in this LFC power system under deception and DoS attacks condition. Considering the hybrid cyber attacks will interrupt control information and the AET scheme can be employed to eliminate the impact of attacks. Moreover, the transmission of redundant data can be reduced and network communication efficiency can be significantly increased by applying the AET scheme with an adaptively adjustable threshold.
- (2) The FOGSMC scheme is designed to resolve the challenge of LFC power system robustness subject to hybrid cyber-attacks. Global sliding mode control (GSMC) scheme has superior performance to keep system stability during the entire control process than traditional sliding mode control (SMC) scheme. At the same time, the fractional term supplies more adjustable parameters to advance the control performance. Therefore, the designed FOGSMC

scheme will provide outstanding robustness of the multi-area LFC power system.

- (3) To take the challenge of stability and stabilisation for the LFC power system, Markov theory, improved Lyapunov function and second-order B-L inequality are employed in this article. First, Markov theory is developed to describe the model of LFC with deception and DoS attacks, transmission time delays, wind energy and energy storage units. Then, the improved Lyapunov function with triple integral term considering maximum transmission time delay is adopted to produce system stability criteria with less conservatism. Moreover, second-order B-L inequality is also deployed to lessen the conservatism of the resulting linear matrix inequality (LMI).

The remaining sections of this document are structured as follows: Section 2 builds the model of LFC power system with deception and DoS attacks, transmission time delays, wind energy and energy storage units. In Section 3, the stability and stabilisation of the designed multi-area LFC power system based on LMI are discussed. Section 4 presents the simulation results and comparative analysis. The conclusion of this work is shown in Section 5.

2 | PROBLEM STATEMENT

The linearised model can be applied to model the system as load deviation is relatively small when the system is operating at a nominal point. The investigated multi-area LFC taking into account wind power and energy storage is shown in Figure 1. Parameters of the i th control area are listed in Table 1.

2.1 | Load frequency control model with wind power and energy storage

The following is a description of the investigated multi-area LFC power system's dynamic model.

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + F\omega(t) \\ y(t) = Cx(t) \end{cases} \quad (1)$$

$$\text{where } x_i(t) = \begin{bmatrix} \Delta f_i & \Delta P_{mi} & \Delta P_{vi} & \Delta P_{windi} \\ \Delta P_{Bi} & \int ACE_i & \Delta P_{tie-i} \end{bmatrix}^T$$

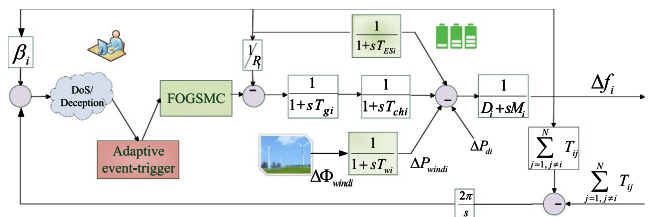


FIGURE 1 Transfer function model of multi-area power system.

TABLE 1 Notations for parameters of i th control area.

Symbol	Quantity
ΔP_{di}	Load deviation
ΔP_{mi}	Generator mechanical output deviation
ΔP_{vi}	Valve position deviation
ΔP_{windi}	Output power fluctuation of the wind turbine generator
ΔP_{Bi}	Output power fluctuation of the battery
Δf_i	Frequency deviation
$\Delta \Phi_{windi}$	Wind power deviation
M_i	Moment of inertia
D_i	Generator damping coefficient
T_{gi}	Time constant of the governor
T_{chi}	Time constant of the turbine
T_{wi}	Time constant of the wind turbine
T_{ESi}	Time constant of the battery
R_i	Speed drop
β_i	Frequency bias factor
T_{ij}	Tie-line synchronizing coefficient
ACE_i	Area control error

$$x(t) = [x_1^T(t) \quad x_2^T(t) \quad x_3^T(t) \quad \dots \quad x_n^T(t)]^T$$

$$u(t) = [u_1^T(t) \quad u_2^T(t) \quad u_3^T(t) \quad \dots \quad u_n^T(t)]^T$$

$$\omega_i(t) = [\Delta P_{di} \quad \Delta \Phi_{windi}]^T, A_{ij} = [(7, 1) = -2\pi T_{ij}]$$

$$y_i(t) = [ACE_i \quad \int ACE_i]^T, B = \text{diag}\{B_1, \dots, B_n\}$$

$$\omega(t) = [\omega_1^T(t) \quad \omega_2^T(t) \quad \omega_3^T(t) \quad \dots \quad \omega_n^T(t)]^T$$

$$y(t) = [y_1^T(t) \quad y_2^T(t) \quad y_3^T(t) \quad \dots \quad y_n^T(t)]^T$$

$$A_{ii} = \begin{bmatrix} (1, 1) = \frac{-D}{M_i}, (1, 2) = \frac{1}{M_i}, (1, 4) = \frac{1}{M_i}, \\ (1, 5) = \frac{1}{M_i}, (1, 7) = \frac{-1}{M_i}, (2, 2) = \frac{-1}{T_{chi}}, \\ (2, 3) = \frac{1}{T_{chi}}, (3, 1) = \frac{-1}{RT_{gi}}, (3, 3) = \frac{-1}{T_{gi}}, \\ (4, 4) = \frac{-1}{T_{wi}}, (5, 1) = \frac{1}{T_{ESi}}, \\ (5, 5) = -\frac{1}{T_{ESi}}, (6, 1) = \beta_i, \\ (6, 6) = 1, (7, 1) = 2\pi \sum_{j=1, j \neq i}^n T_{ij} \end{bmatrix}$$

$$A = \begin{bmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \dots & A_{nn} \end{bmatrix}$$

$$B_i = \begin{bmatrix} 0 & 0 & \left(\frac{1}{T_{gi}}\right)^T & 0 & 0 & 0 & 0 \end{bmatrix}^T$$

$$C_i = \begin{bmatrix} \beta_i & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$F_i = \begin{bmatrix} \frac{-1}{M_i^T} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{T_{wi}} & 0 & 0 & 0 \end{bmatrix}^T$$

$$C = \text{diag}\{C_1, \dots, C_n\}, F = \text{diag}\{F_1, \dots, F_n\}$$

The ACE signal can be written as

$$ACE_i = \beta_i \Delta f_i + \Delta P_{tie-i} \quad (2)$$

2.2 | Hybrid cyber attacks with adaptive event-triggered scheme

DoS attacks and deception attacks are the two main types of cyber attacks. In this section, two types of cyber attacks with an AEt scheme for LFC power systems are considered. In this work, the DoS attack is assumed as a pulse-width modulated signal. It can be represented as

$$\Gamma_{DoS}(t) = \begin{cases} 0 & t \in [(n-1)T_{DoS}, (n-1)T_{DoS} + T_{off}) \\ 1 & t \in [(n-1)T_{DoS} + T_{off}, nT_{DoS}) \end{cases} \quad (3)$$

where $T_{DoS} \in R > 0$ means jammer period; T_{off} represents the sleeping time of jammer; $T_{off_{min}} \leq T_{off} < T_{DoS}$. In every period, $[0, T_{off})$ is sleeping interval of jamming signal; $[T_{off}, T_{DoS})$ denotes the active interval of jamming signal.

Remark 1. To describe the DoS attack, a pulse-width modulated signal is applied in this study. If $\Gamma_{DoS}(t) = 1$, it means the proposed LFC power system is under DoS attack, while real frequency deviation and tie-line power flow can not be transmitted. If $\Gamma_{DoS}(t) = 0$, it means the proposed LFC power system is in a sleeping state, while the real frequency deviation and tie-line power flow can be transmitted.

For the AEt scheme, signal packets can be delivered if the designed trigger threshold can be satisfied. Otherwise, the

latest transmitted signal will be transmitted again. In addition, this scheme can reduce the transmission frequency of superfluous information to enhance network communication utilization.

The AEt criterion is designed as

$$\begin{aligned} & [x(t_k h + jh) - x(t_k h)]^T \Phi_r [x(t_k h + jh) - x(t_k h)] \\ & \leq \lambda(t_k h) x(t_k h)^T \Phi_r x(t_k h) \end{aligned} \quad (4)$$

where Φ_r is an unknown positive matrix; $\lambda(t_k h)$ denotes the triggering threshold which can be adaptively adjusted.

$$\lambda(t_k h) = \max(\lambda_m, \eta \lambda(t_{k-1} h)) \quad (5)$$

where $\lambda_m > 0$ and

$$\eta = \begin{cases} 0, & \text{if } \|x(t_k h)\| \geq \|x(t_{k-1} h)\| \\ 1 - \frac{2\alpha_2}{\pi} \arctan\left(\frac{\|x(t_k h)\| - \|x(t_{k-1} h)\|}{\|x(t_k h)\|}\right), & \text{otherwise} \end{cases}$$

Taking DoS attack into consideration, the next transmitted signal time is

$$\begin{aligned} t_{k,n} h &= \{t_k h + jh \mid e^T(t_k h) \Phi_r e(t_k h) \leq \lambda(t_k h) \\ & \quad x^T(t_k h + kh) \Phi_r x(t_k h + kh), \quad (6) \\ t_k h + jh &\in [(n-1)T_{DoS}, (n-1)T_{DoS} + T_{off}]\} \end{aligned}$$

Define:

$$\tau_{k,n}(t) = \begin{cases} t - t_k h, & t \in \Omega_{k,n}^1 \\ t - t_k h - mh, & t \in \Omega_{k,n}^2 \\ t - t_k h - Kh, & t \in \Omega_{k,n}^3 \end{cases} \quad (7)$$

where $\Omega_{k,n}^1 = [t_k h + \tau_k, (t_k + 1)h + \tau_k] \cap [(n-1)T_{DoS}, (n-1)T_{DoS} + T_{off}]$, $\Omega_{k,n}^2 = \cup_{m=1}^{K-1} [t_k h + mh + \tau_k, t_k h + (m-1)h + \tau_k] \cap [(n-1)T_{DoS}, (n-1)T_{DoS} + T_{off}]$, $\Omega_{k,n}^3 = [t_k h + Kh + \tau_k, t_{k+1} h + \tau_{k+1}] \cap [(n-1)T_{DoS}, (n-1)T_{DoS} + T_{off}]$

The controller input can be described as

$$y(t_{k,n} h) = C e_{k,n}(t) + C x(t - \tau_{k,n}(t)) \quad (8)$$

where

$$e(t) = \begin{cases} 0, & k \in \Omega_{k,n}^1 \\ x(t_{k,n} h) - x(t_{k,n} h + mh), & k \in \Omega_{k,n}^2 \\ x(t_{k,n} h) - x(t_{k,n} h + jh), & k \in \Omega_{k,n}^3 \end{cases}$$

and $j = \sup\{m \in N \mid t_k h + mh < t_{k+1} h, m = 1, 2, \dots\}$, $\tau_M = \max(\tau_{k,n}(t))$.

A deception attack that can steal and disguise the transmitted information is considered in this work. How to model deception attacks is an important factor to study the impact on the power system. When the power system is under deception attack, the transmitted information will be stolen and disguised. Hence, the nonlinear function $g(y(t))$ is applied to describe malicious information. The $g(y(t))$ will satisfy the following inequality:

$$\|g(y)\|^2 \leq \|Gy\|^2 \quad (9)$$

Consecutive and random are two types of launching modes of deception attack. In the following, Bernoulli random variable $\beta(t)$ with $E[\beta(t)] = \bar{\beta}$ and $E[(\beta(t) - \bar{\beta})] = \delta^2$ is applied to describe the probability of a deception attack occurring. Therefore, the following inequality can be obtained:

$$\bar{\beta} y^T(t_{k,n} h) G^T G y(t_{k,n} h) - \bar{\beta} g^T(y(t_{k,n} h)) G^T G g(y(t_{k,n} h)) \geq 0 \quad (10)$$

Then, the real transmitted signal can be modelled as

$$y_{real}(t) = \beta(t) g(y(t_{k,n} h)) + (1 - \beta(t)) y(t_{k,n} h) \quad (11)$$

Therefore, the studied LFC power system model can be revised as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \beta(t) BK_r C e_{k,n}(t) + \beta(t) BK_r C x(t - \tau_{k,n}(t)) \\ & \quad + (1 - \beta(t)) g(y(t_{k,n} h)) + F\omega(t) \end{aligned} \quad (12)$$

Time delays introduced by network environments present a new challenge for the stability of the closed-loop LFC scheme. Hence, the transmission time delay $\tau_{k,n}(t)$ is considered, where $\tau_{k,n}(t) \in [0, \tau_M)$, $\tau_M = \max(\tau_{k,n}(t))$, $\dot{\tau} = \tau_{k,n}^{\cdot}(t) = \lim_{\Delta t_k \rightarrow 0} \frac{\tau_{k,n}(t + \Delta t_k) - \tau_{k,n}(t)}{\Delta t_k}$. To describe the studied LFC model with transmission time delay, the Markov theory is exploited. To enhance the stability of the LFC power system, different controller gains are designed for different time delays.

The description of the finite-state Markov process is as follows:

$$\begin{aligned} P[r_s(t + \Delta t) = j \mid r_s(t) = i] &= p_{ij} \\ 0 \leq i, j \leq L, 0 \leq \pi_{ij} \leq 1, \sum_{j=0}^L \pi_{ij} &= 1 \end{aligned} \quad (13)$$

Hence, the studied LFC model with Markov theory can be modelled as

$$\begin{aligned} \dot{x}(t) = & Ax(t) + \beta(t)BK_r C e_{k,n}(t) + \beta(t)BK_r C x(t - \tau_{k,n}(t)) \\ & + (1 - \beta(t))g(y(t_{k,n}h)) + F\omega(t) \end{aligned} \quad (14)$$

3 | STABILITY AND STABILISATION ANALYSIS OF DESIGNED LOAD FREQUENCY CONTROL

To develop the stability and stabilisation criteria for designed multi-area LFC model, improved Lyapunov function and second-order B-L inequality are employed in the following.

3.1 | Improved Lyapunov function and second-order Bessel-Legendre inequality in stability analysis

Theorem 1. For given constant $\lambda_m, \tau_M, \dot{\tau}$, if there exists positive definite matrices $P_r, Q_{1r}, Q_{2r}, R_{1r}, R_2, S_1, S_2, \Phi_r$ appropriate dimensions $T_{11}, T_{12}, T_{13}, T_{21}, T_{22}, T_{23}, T_{31}, T_{32}, T_{33}$, and the following LMIs hold for all $r = 0, \dots, L$, the studied LFC model Equation (14) with $\omega(k) = 0$ is asymptotically stable.

$$\Pi_{2r} = \Pi_1 + \Pi_{3r} + \Pi_{4r} < 0 \quad (15)$$

$$v_{4r} = S_3 - \tau_M \sum_{j=1}^L \pi_{rj} R_{1j} > 0 \quad (16)$$

$$v_{5r} = R_2 - \tau_M \sum_{j=1}^L \pi_{rj} (Q_{1j} + Q_{2j}) > 0 \quad (17)$$

$$\tilde{\varphi}_2 = \begin{bmatrix} \varphi_{1r} + \tilde{S}_1 & * \\ T_1 & \varphi_{1r} + \tilde{S}_2 \end{bmatrix} > 0 \quad (18)$$

where $\Pi_{3r} = \hat{H}_2 \tilde{\varphi}_1 \hat{H}_2^T + \varphi_{3r} + \varphi_4 + 2P_r \chi_1$, $\Pi_{4r} = \chi_1 v_2 \chi_1^T + \delta^2 \chi_2 v_2 \chi_2^T$, $\Pi_1 = e_1 v_1 r e_1^T - e_2 \Phi_r e_2^T - \bar{\beta} e_3 e_3^T - e_4 Q_{2r} e_4^T - e_5 v_3 r e_5^T$, $v_{1r} = \sum_{j=0}^1 \pi_{rj} P_j + Q_{1r} + Q_{2r} + \tau_M R_2 + \bar{\beta} G^T C^T C G$, $v_{2r} = \tau_M^2 R_{1r} + \frac{\tau_M^2}{2} S_1 + \frac{\tau_M^2}{2} S_2$, $v_{3r} = (1 - \dot{\tau}(t)) Q_{2r} - \lambda_m \Phi_r$, $v_{4r} = S_3 - \tau_M \sum_{j=1}^L \pi_{rj} R_{1j}$, $v_{5r} = R_2 - \tau_M \sum_{j=1}^L \pi_{rj} (Q_{1j} + Q_{2j})$, $v_{6r} = R_2 - \tau_M \sum_{j=1}^L \pi_{rj} Q_{1j}$,

$$H_1 = [e_1 - e_5 \quad e_1 + e_5 - 2e_6 \quad e_1 - e_5 - 6e_7],$$

$$H_2 = [e_5 - e_4 \quad e_5 + e_4 - 2e_8 \quad e_5 - e_4 - 6e_9],$$

$$\hat{H}_2 = [H_1 \quad H_2], \varphi_{1r} = \text{diag}\{R_{1r}, 3R_{1r}, 5R_{1r}\},$$

$$H_3 = [e_1 - e_6 \quad e_1 - e_6 - 3e_7 \quad e_5 - e_8 \quad e_5 - e_8 - 3e_9],$$

$$H_4 = [e_6 - e_5 \quad e_5 - e_6 + 3e_7 \quad e_8 - e_4 \quad e_4 - e_8 + 3e_9],$$

$$\varphi_{3r} = \text{diag}\{-2v_{4r}, -4v_{4r}, -2v_{4r}, -4v_{4r}\},$$

$$\varphi_4 = \text{diag}\{2S_2, 4S_2, 2S_2, 4S_2\},$$

$$\tilde{S}_1 = \text{diag}\{S_1, 3S_1, 5S_1\}, \tilde{S}_2 = \text{diag}\{S_2, 3S_2, 5S_2\},$$

$$e_j = [\underbrace{0 \dots 0}_{j-1}, 1, \underbrace{0 \dots 0}_{11-j}], (j = 1, \dots, 11),$$

$$\tilde{\varphi}_{1r} = \begin{bmatrix} \varphi_{1r} & * \\ T_1 & \varphi_{1r} \end{bmatrix}, T_1 = \begin{bmatrix} T_{11} & T_{12} & T_{13} \\ T_{21} & T_{22} & T_{23} \\ T_{31} & T_{32} & T_{33} \end{bmatrix}$$

Proof. Build Lyapunov function as follows:

$$\begin{aligned} V(t) = & x^T(t) P_r x(t) + \int_{t-\tau_M}^t x^T(s) Q_{1r} x(s) ds \\ & + \int_{t-\tau(t)}^t x^T(s) Q_{2r} x(s) ds \\ & + \tau_M \int_{-\tau_M}^0 \int_{t+\alpha}^t \dot{x}^T(s) R_{1r} \dot{x}(s) ds d\alpha \\ & + \int_{-\tau_M}^0 \int_{t+\alpha}^t x^T(s) R_2 x(s) ds d\alpha \\ & + \int_{-\tau_M}^0 \int_{\beta}^0 \int_{t+\alpha}^t \dot{x}^T(s) S_1 \dot{x}(s) ds d\alpha d\beta \\ & + \int_{-\tau_M}^0 \int_{-\tau_M}^{\beta} \int_{t+\alpha}^t \dot{x}^T(s) S_2 \dot{x}(s) ds d\alpha d\beta \end{aligned}$$

Calculating the derivative of $V(t)$ along the trajectory of Equation (14) with $\omega(t) = 0$ yields

$$\begin{aligned}
\Delta V(t) &= x^T(t) \sum_{j=0}^1 \pi_{rj} P_j x(t) + 2\dot{x}^T(t) P_r x(t) + x^T(t) \\
&\quad Q_{1r} x(t) - x^T(t - \tau_M) Q_{1r} x(t - \tau_M) + x^T(t) \\
&\quad Q_{2r} x(t) - (1 - \dot{\tau}(t)) x^T(t - \tau(t)) Q_{1r} x(t - \tau(t)) \\
&\quad + \dot{x}^T(t) \tau_M^2 R_{1r} \dot{x}(t) + x^T(t) \tau_M R_{2r} x(t) \\
&\quad + \frac{\tau_M^2}{2} \dot{x}^T(t) S_1 \dot{x}(t) + \frac{\tau_M^2}{2} \dot{x}^T(t) S_2 \dot{x}(t) \\
&\quad + \int_{t-\tau_M}^t x^T(\alpha) \sum_{j=0}^1 \pi_{rj} Q_{1j} x(\alpha) d\alpha \\
&\quad + \int_{t-\tau(t)}^t x^T(\alpha) \sum_{j=0}^1 \pi_{rj} Q_{2j} x(\alpha) d\alpha \\
&\quad - \tau_M \int_{t-\tau_M}^t \dot{x}^T(\alpha) R_{1r} \dot{x}(\alpha) d\alpha - (\tau_M - \tau(t)) \\
&\quad \int_{t-\tau(t)}^t \dot{x}^T(\alpha) S_1 \dot{x}(\alpha) d\alpha - \int_{t-\tau(t)}^t x^T(\alpha) R_{2r} x(\alpha) d\alpha \\
&\quad + \tau_M \int_{-\tau_M}^0 \int_{t+\alpha}^t \dot{x}^T(s) \sum_{j=0}^1 \pi_{rj} R_{1r} \dot{x}(s) ds \\
&\quad - \int_{t-\tau_M}^{t-\tau(t)} x^T(\alpha) R_{2r} x(\alpha) d\alpha \\
&\quad - \int_{-\tau(t)}^0 \int_{t+\alpha}^t \dot{x}^T(s) S_1 \dot{x}(s) ds d\alpha \\
&\quad - \int_{-\tau_M}^{t-\tau(t)} \int_{t+\alpha}^{t-\tau(t)} \dot{x}^T(s) S_1 \dot{x}(s) ds d\alpha \\
&\quad - \int_{-\tau_M}^{t-\tau(t)} \int_{t-\tau_M}^{t+\alpha} \dot{x}^T(s) S_2 \dot{x}(s) ds d\alpha \\
&\quad - \int_{-\tau(t)}^0 \int_{t-\tau(t)}^{t+\alpha} \dot{x}^T(s) S_2 \dot{x}(s) ds d\alpha
\end{aligned}$$

Recalling Equation (4) and Equation (10), the following inequality can be derived as

$$\begin{aligned}
\Delta V(t) &\leq \Delta V(t) + \bar{\beta} y^T(t_{k,n} b) G^T G y(t_{k,n} b) \\
&\quad + \sigma_m x^T(t - \tau(t)) \Phi_r x(t - \tau(t)) - e^T(t) \Phi_r e(t) \\
&\quad - \bar{\beta} g^T(y(t_{k,n} b)) G^T G g(y(t_{k,n} b)) \quad (19)
\end{aligned}$$

Set the augmented vector as follows:

$$\begin{aligned}
\xi(t) &= \left[x(t) \ e(t) \ g(y(t_{k,n} b)) \ x(t - \tau_M) \ x(t - \tau(t)) \ \frac{1}{\tau(t)} \right. \\
&\quad \left. \int_{-\tau(t)}^0 x(t + \alpha) d\alpha \ \frac{1}{\tau(t)} \int_{-\tau(t)}^0 \lambda_{-\tau(t)}(\alpha) x(t + \alpha) d\alpha \ \frac{1}{\tau_M - \tau(t)} \int_{-\tau(t)}^0 \right. \\
&\quad \left. x(t + \alpha) d\alpha \ \frac{1}{\tau_M - \tau(t)} \int_{-\tau_M}^{t-\tau(t)} \lambda_{-\tau(t)}(\alpha) x(t + \alpha) d\alpha \right]
\end{aligned}$$

Then, the following inequality can be obtained as

$$\Delta V(t) \leq \xi(t) \Pi_1 \xi^T(t) + 2\dot{x}(t) P_r x^T(t) + \dot{x}(t) v_2 \dot{x}^T(t) + \Delta \tilde{V}(t)$$

where

$$\begin{aligned}
\Delta \tilde{V}(t) &= -\tau_M \int_{t-\tau_M}^t x(s) R_{1r} x^T(s) ds - (\tau_M - \dot{\tau}) \\
&\quad \int_{t-\tau_{k,n}(t)}^t x(s) S_1 x^T(s) ds - \dot{\tau} \int_{t-\tau_M}^{t-\tau_{k,n}(t)} x(s) S_2 x^T(s) ds \\
&\quad - \int_{-\tau_{k,n}(t)}^0 \int_{t+\alpha}^t \dot{x}(s) v_{4r} \dot{x}^T(s) ds d\alpha \\
&\quad - \int_{-\tau_M}^{t-\tau_{k,n}(t)} \int_{t+\alpha}^{t-\tau_{k,n}(t)} \dot{x}(s) v_{4r} \dot{x}^T(s) ds d\alpha \\
&\quad - \int_{-\tau_{k,n}(t)}^0 \int_{t-\tau_{k,n}(t)}^{t+\alpha} \dot{x}(s) S_2 \dot{x}^T(s) ds d\alpha \\
&\quad - \int_{-\tau_M}^{t-\tau_{k,n}(t)} \int_{t-\tau_M}^{t+\alpha} \dot{x}^T(s) S_2 \dot{x}(s) ds d\alpha \\
&\quad - \int_{t-\tau_{k,n}(t)}^t x(s) v_{5r} x^T(s) ds \\
&\quad - \int_{t-\tau_M}^{t-\tau_{k,n}(t)} x(s) v_{6r} x^T(s) ds
\end{aligned}$$

Define:

$$\begin{aligned}
\chi_1 &= A e_1 + (1 - \bar{\beta}) B K_r C e_2 + \bar{\beta} B K_r C e_3 + (1 - \bar{\beta}) B K_r C e_5 \\
\chi_2 &= B K_r C e_2 + B K_r C e_3 + B K_r C e_5
\end{aligned}$$

Recalling $E\{\beta(t) - \bar{\beta}\} = 0$ and $E\{(\beta(t) - \bar{\beta})^2\} = \delta^2$, the studied LFC model with $\omega(k) = 0$ can be derived as

$$\dot{x}(t) = [\chi_1 + [\beta(t) - \bar{\beta}] \chi_2] \xi(t) \quad (20)$$

Then, it yields

$$\begin{aligned}
E\{2\dot{x}(t) P_r x^T(t)\} &= 2x^T(t) P_r \chi_1 \xi(t) \\
E\{\dot{x}(t) v_2 \dot{x}^T(t)\} &= \xi(t) \chi_1 v_2 \chi_1^T \xi^T(t) + \delta^2 \xi(t) \chi_2 v_2 \chi_2^T \xi^T(t)
\end{aligned}$$

In the following, the second-order B-L inequality in [27] can be applied for $\Delta \tilde{V}(t)$. Define $\frac{1}{l} = \frac{\tau_{k,n}(t)}{\tau_M}$ and $\frac{1}{\kappa} = \frac{\tau_M - \tau_{k,n}(t)}{\tau_M}$, the following inequality can be derived:

$$\begin{aligned}
& -\tau_M \int_{t-\tau_M}^t x(s)R_{1r}x^T(s)ds \\
& -(\tau_M - \hat{\tau}(t)) \int_{t-\hat{\tau}(t)}^t x(s)S_1x^T(s)ds \\
& \leq -\frac{1}{l}\xi(t)H_1(\varphi_{1r} + \tilde{S}_1)H_1^T\xi^T(t) \\
& -\frac{1}{\kappa}\xi(t)H_2(\varphi_{1r} + \tilde{S}_2)H_2^T\xi^T(t) \\
& +\xi(t)H_1\tilde{S}_1H_1^T\xi^T(t) + \xi(t)H_2\tilde{S}_2H_2^T\xi^T(t) \\
& \leq -\xi(t)\hat{H}_2\tilde{\varphi}_1\hat{H}_2^T\xi^T(t)
\end{aligned} \tag{21}$$

and $\tilde{\varphi}_2 > 0$. Then, double integral inequality in [28] can be utilised, the following inequalities can be obtained:

$$\begin{aligned}
& -\int_{-\tau_{k,n}(t)}^0 \int_{t+\alpha}^t \dot{x}(s)v_{4r}\dot{x}^T(s)dsd\alpha \\
& -\int_{-\tau_M}^{-\tau_{k,n}(t)} \int_{t+\alpha}^{t-\tau_{k,n}(t)} \dot{x}(s)v_{4r}\dot{x}^T(s)dsd\alpha \\
& \leq H_3\varphi_{3r}H_3^T \\
& -\int_{-\tau_{k,n}(t)}^0 \int_{t-\tau_{k,n}(t)}^{t+\alpha} \dot{x}(s)S_2\dot{x}^T(s)dsd\alpha \\
& -\int_{-\tau_M}^{-\tau_{k,n}(t)} \int_{t-\tau_M}^{t+\alpha} \dot{x}^T(s)S_2\dot{x}(s)dsd\alpha \\
& \leq -H_4\varphi_4H_4^T
\end{aligned} \tag{22}$$

Therefore, if $\tilde{\varphi}_2 > 0$, $v_{5r} > 0$ and $v_{6r} > 0$ can be satisfied, the following inequality can be yielded:

$$\begin{aligned}
\Delta V(t) & \leq \xi(t)\Pi_1\xi^T(t) + 2\dot{x}(t)P_r x^T(t) + \dot{x}(t)v_2\dot{x}^T(t) \\
& +\Delta\tilde{V}_1(t) + \Delta\tilde{V}_2(t) + \Delta\tilde{V}_3(t) + \Delta\tilde{V}_4(t) \\
& \leq \xi(t)\Pi_{2r}\xi^T(t)
\end{aligned} \tag{24}$$

Thus, by utilising Lemma 1 in [28], condition Equation (15) can be derived. With a condition that $\omega(k) = 0$, if Equations (15–18) are satisfied, there exists a sufficiently small scalar $c \in (0, 1)$, such that $\Delta V(k) < -c\|\xi_1(t)\|^2 < 0$ can be procured. As a result, the system Equation (14) with $\omega(k) = 0$ is asymptotically stable.

Remark 2. The improved Lyapunov function with a triple integral term in $V(t)$ is applied in this section. Then, the maximum time delay τ_M and $\hat{\tau}$ are considered in this theorem. Besides, second-order B-L inequality is applied in $\Delta\tilde{V}(t)$ due to which tighter upper bounds can be provided than those acquired by [28]. Moreover, augmented vector $\xi(t)$, $\frac{1}{l} = \frac{\tau_{k,n}(t)}{\tau_M}$ and

$\frac{1}{\kappa} = \frac{\tau_M - \tau_{k,n}(t)}{\tau_M}$ are designed in this theorem to improve the performance further.

Following that, H_∞ stability criterion of multi-area LFC model Equation (14) will be developed.

Theorem 2. For given constant λ_m , τ_M , $\hat{\tau}$, if there exists positive definite matrices P_r , Q_{1r} , Q_{2r} , R_{1r} , R_{2r} , S_1 , S_2 , Φ_r , appropriate dimensions T_{11} , T_{12} , T_{13} , T_{21} , T_{22} , T_{23} , T_{31} , T_{32} , T_{33} , and the following LMIs hold for all $r = 0, \dots, L$, the multi-area LFC model Equation (14) is asymptotically stable with an H_∞ norm bound γ .

$$\begin{aligned}
\Pi'_{2r} & = \Pi_1 + \Pi'_{3r} + \Pi'_{4r} < 0 \\
v_{4r} & > 0, v_{5r} > 0, \tilde{\varphi}_2 > 0
\end{aligned} \tag{25}$$

where $\Pi'_{3r} = \hat{H}_2\tilde{\varphi}_1\hat{H}_2^T + \varphi_{3r} + \varphi_4 - \gamma^2 e_{10}^T e_{10} + e_1^T C^T C e_1 + 2P_r\chi'_1$, $\Pi'_{4r} = \chi'_1 v_2 \chi'^T_1 + \delta^2 \chi'_2 v_2 \chi'^T_2$, $\chi'_1 = Ae_1 + (1 - \bar{\beta})BK_r Ce_2 + \bar{\beta}BK_r Ce_3 + (1 - \bar{\beta})BK_r Ce_5 + Fe_{12}$, $\chi'_2 = BK_r Ce_2 + BK_r Ce_3 + BK_r Ce_5 + Fe_{12}$, $e_j = \underbrace{[0 \dots 0]_{j-1}}_{j-1}, \underbrace{[1, 0 \dots 0]}_{10-j}$, ($j = 1, \dots, 10$)

For prescribed attenuation level $\gamma > 0$, taking the disturbance $\omega(t)$ into account, the cost function J is considered as

$$J = \int_0^\infty y^T(t)y(t) - \gamma^2 \omega^T(t)\omega(t)dt \tag{26}$$

Setting the augmented vector as

$$\xi'(t) = [\xi(t) \quad \omega(t)]$$

Remembering condition Equation (15), and utilising the same method in Theorem 1, condition Equation (25) can be obtained. Therefore, model Equation (14) is asymptotically stable with an H_∞ norm bound γ . In this theorem, the stability criteria guarantee the closed-loop stability under the initially triggered threshold λ_m . An algorithm is designed to keep the LFC system stable with triggered threshold $\lambda(t_k b)$ in [Appendices](#).

The sufficient stability condition of the multi-area LFC model Equation (14) is provided in Theorem 1 and Theorem 2. To study the stabilisation of the system Equation (14), the next theorem is built.

3.2 | Stabilisation analysis

This section will derive the system's stabilisation criterion. Moreover, minimum H_∞ performance index γ is derived to keep a better stabilisation performance.

Theorem 3. For given constant λ_m , τ_M , $\hat{\tau}$, if there exists positive definite matrices P_r , Q_{1r} , Q_{2r} , R_{1r} , R_{2r} , S_1 , S_2 , Φ_r

appropriate dimensions $T_{11}, T_{12}, T_{13}, T_{21}, T_{22}, T_{23}, T_{31}, T_{32}, T_{33}$, and the following LMIs hold for all $r = 0, \dots, L$, the power system Equation (14) is asymptotically stable with an H_∞ norm bound γ , and the feedback controller gain can be obtained as \tilde{K}_r .

min κ

$$s.t. \begin{cases} \Pi''_{2r} < 0, v_{4r} > 0, \\ v_{5r} > 0, \tilde{\varphi}_2 > 0 \end{cases} \quad (27)$$

$$\text{where } \kappa = \gamma^2, \Pi''_{2r} = \begin{bmatrix} \Pi'_{3r} & * & * \\ \Pi'_{4r} & \Pi'_{5r} & * \\ \Pi'_{6r} & * & \delta\Pi'_{5r} \end{bmatrix}$$

$$\chi''_1 = P_r A e_1 + (1 - \bar{\beta}) \tilde{K}_r C e_2 + \bar{\beta} \tilde{K}_r C e_3 + (1 - \bar{\beta}) \tilde{K}_r C e_5 + P_r F e_{12}, \chi''_2 = \tilde{K}_r C e_2 + \tilde{K}_r C e_3 + \tilde{K}_r C e_5 + P_r F e_{12},$$

$$\Pi'_{4r} = [\tau \chi''_1 \tau_M / \sqrt{2} \chi''_1 \chi''_1]^T, \Pi'_{6r} = [\tau \chi''_2 \tau_M / \sqrt{2} \chi''_2 \chi''_2]^T$$

$$\Pi'_{5r} = \text{diag}(R_{1r} - 2P_r, S_1 - 2P_r, S_2 - 2P_r)$$

Recalling Equation (25) and applying Lemma 1 in [28], it yields

$$\begin{bmatrix} \Pi'_{3r} & * & * \\ \Pi'_{4r} & \Pi'_{5r} & * \\ \Pi'_{6r} & * & \delta\Pi'_{5r} \end{bmatrix} < 0 \quad (28)$$

$$\text{where } \Pi_{4r} = [\tau \chi''_1 \tau_M / \sqrt{2} \chi''_1 \chi''_1]^T, \Pi_{6r} = [\tau \chi''_2 \tau_M / \sqrt{2} \chi''_2 \chi''_2]^T,$$

$$\Pi_{5r} = \text{diag}(-R_{1r}^{-1}, -S_1^{-1}, -S_2^{-1})$$

Pre-multiplying and post-multiplying both sides of Equation (28) with $\text{diag}\{I, \underbrace{\dots}_{10}, I, P_r, P_r, P_r\}$ and utilising the fact

that $Z < 0$ and $Y^T = Y$; then $Y^T Z Y \leq -2Y - Z^{-1}$ can be procured and $\Pi''_{2r} < 0$ can be further converted. Therefore, the theorem is proved and controller gain is $\tilde{K}_r = P_r K_r$.

To improve the studied LFC power system transient performance, FOGSMC scheme is applied in this research. The controller is designed as follows.

The FOGSMC sliding surface is defined as

$$s(t) = Gx(t) - \int_0^t G(A - BKC)x(\tau) d\tau - f(t) + \mu D^{\alpha_1 - 1} x(t) \quad (29)$$

where $D^{\alpha_1 - 1}$ is the fractional order operator, $f(t)$ is a function designed specially to achieve global sliding mode, K is the controller gain to be designed, and μ denotes the coefficient of fractional order term.

The ideal sliding surface should satisfy $s(t) = 0$ and $\dot{s}(t) = 0$. Thus, the equivalent SMC law is expressed as follows:

$$u_{eq}(t) = -KCx(t) - (GB)^{-1}GF\omega(t) + (GB)^{-1}\dot{f}(t) - \mu(GB)^{-1}D^{\alpha_1}x(t) \quad (30)$$

Then, the controller is designed as the following theorem.

Theorem 4. A decentralised switching control law can be designed as the following to guarantee the reaching condition $s(t)\dot{s}(t) < 0$.

$$u(t) = -K_r Cx(t) + (GB)^{-1}\dot{f}(t) - \mu(GB)^{-1}D^{\alpha_1}x(t) + k(\text{sgn}(s(t)) + s(t)) \quad (31)$$

The proof of this theorem is identical to that given in ref. [28]. To improve the robustness of the studied multi-area LFC model, the FOGSMC with fraction order and GSMC are adopted in this paper. On the other hand, the fraction order provides new degrees of freedom for controller gain. Moreover, GSMC has better robustness performance in the whole control process. As a result, it can significantly improve the system's robustness.

4 | CASE STUDY AND DISCUSSION

Effectiveness and superiority of the proposed approach in designing LFC scheme subjected to hybrid cyber attacks are discussed in this section. In Case 1, a two-area LFC power system under hybrid cyber attacks is built with Matlab/Simulink. Moreover, to verify the efficacy of the proposed LFC scheme in a realistic power system condition, the IEEE 39-bus system with hybrid cyber attacks is implemented in Case 2.

4.1 | Case 1: two-area load frequency control power system under hybrid cyber attacks

In this case, a two-area LFC power system with wind farms and energy storage units is implemented as shown in Figure 2. The detailed parameters are in Table 2. To analyse LFC performance with hybrid cyber-attacks, the two-area LFC power systems with $E[\beta(t)] = 0.2$ and $E[\beta(t)] = 0.4$, $T_{off} = 0.8$ and $T_{off} = 0.9$ are explored, respectively. In addition, the wind turbine induction generator with 9 m/s wind speed and 0.2 trip coefficient are carried out.

For transmission time delays, the transition probability matrix is given as follows:

$$P = \begin{bmatrix} 0.5088 & 0.4912 \\ 0.4286 & 0.5714 \end{bmatrix}$$

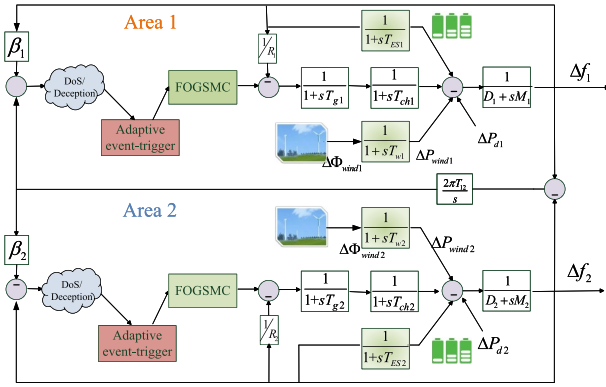


FIGURE 2 Transfer function model of two-area power system with wind farm and energy storage unit.

TABLE 2 Parameters of two-area load frequency control (LFC) scheme

Area	R	M	D	T_g	T_{ch}	T_{12}
1	0.05	10.0	1.0	0.1	0.3	0.1986
2	0.05	12.0	1.5	0.17	0.4	0.1986

In light of Theorem 3 with $\lambda_m = 0.1$, $\gamma = 2.8422$, $\dot{d} = 0.1$, $\tau_M = 0.01$ can be obtained and FOGSMC scheme can be designed as the following:

$$u(t) = -K_{ij}Cx(t) + 1.0\dot{f}(t) - 0.001(s(t) + \text{sgn}(s(t))) - 0.08D^{0.92}x(t)$$

where Area 1:

$$K_{11} = [0.0195, 0.5805], K_{12} = [0.1275, 0.5092].$$

Area 2:

$$K_{21} = [0.0176, 0.1466], K_{22} = [0.0401, 0.2588].$$

To demonstrate the designed AEt performance, release time instants and intervals with $T_{off} = 0.8$ and $T_{off} = 0.9$ are depicted in Figure 3. It can be observed that less information is transmitted in the second situation with $T_{off} = 0.9$, when compared with the first situation with $T_{off} = 0.8$. The proposed AEt strategy can eliminate unnecessarily information exchange and relieve transmission burden for LFC power system. Moreover, it helps reduce the impact of hybrid cyber attacks for the LFC power system.

To scrutinise the developed LFC scheme performance with FOGSMC, it is compared with two representative controllers of PI control and fractional order PID (FOPID) control [29] under hybrid cyber-attacks $E[\beta(t)] = 0.2$ and $T_{off} = 0.8$, as shown in Figure 4. When a hybrid cyber-attack occurs, for the LFC power system with the FOGSMC situation, the designed power frequency deviation changes and ACE changes can back to preset value quickly. Therefore, the designed LFC with FOGSMC can adjust the frequency to near stable conditions effectively than the designed LFC with PI control and FOPID control.

To further verify the effective performance of the designed LFC with the FOGSMC scheme, the situation with $E[\beta(t)] = 0.4$

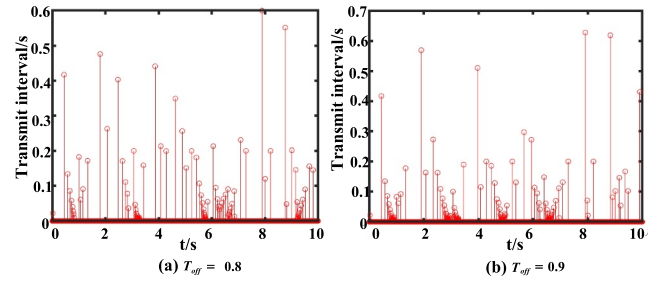


FIGURE 3 Results of adaptive event-triggered (AEt) Scheme: (a) release time instants and intervals with $T_{off} = 0.8$, (b) release time instants and intervals with $T_{off} = 0.9$.

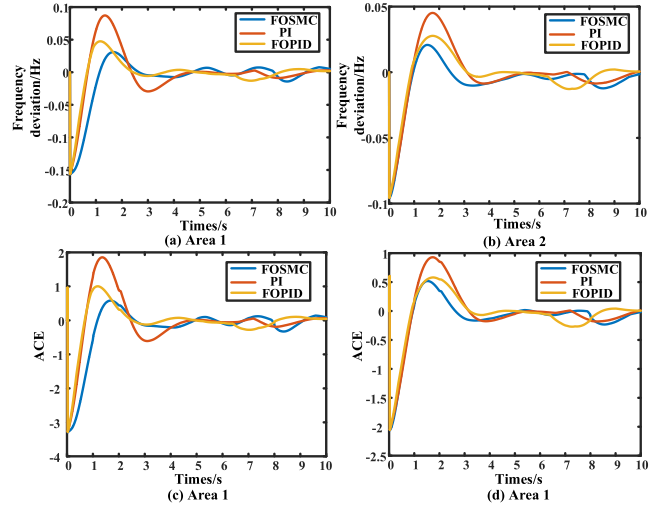


FIGURE 4 Results of $T_{off} = 0.8$ and $E[\beta(t)] = 0.2$: (a) Frequency deviations of Area 1, (b) Frequency deviations of Area 2, (c) area control errors (ACE) of Area 1, (d) ACE of Area 2.

and $T_{off} = 0.8$ is discussed. In this contrast experiment, other parameters remain the same as before. As presented in Figure 5, the frequency with FOGSMC exhibits lower overshoot and faster response compared with that of other methods. When hybrid cyber attacks are launched, the LFC with FOGSMC scheme received the measurement values, adjusting the frequency to match the preset range effectively. There the power system recovered to a stable operating state. To summarise, the designed LFC with FOGSMC can regulate frequency effectively to restore system stability consequently, when the power system is under external load disturbances and hybrid cyber-attacks.

4.2 | Case 2: modified IEEE 39-bus New England test system

To scrutinise the performance of the proposed LFC under hybrid cyber attacks within a more realistic power system condition, the IEEE 39-bus power system with 3 wind farms is detailed as indicated in Figure 6. As presented in Figure 6, this system includes 10 generators, 19 loads, 34 transmission lines, 12 transformers, and 3 wind farms, splitting into three control

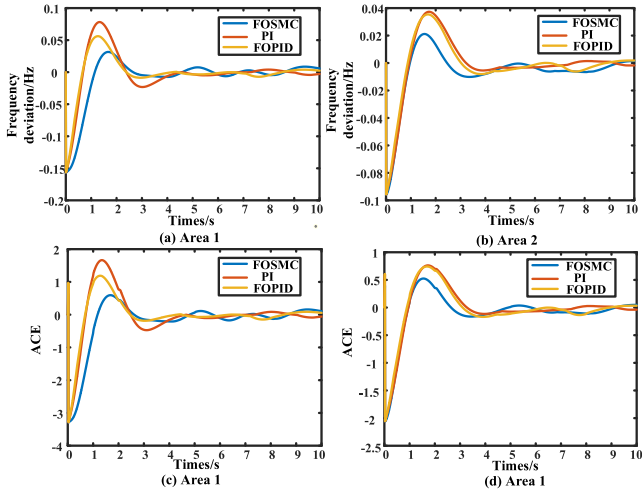


FIGURE 5 Results of $T_{off} = 0.8$ and $E[\beta(t)] = 0.4$: (a) Frequency deviations of Area 1, (b) Frequency deviations of Area 2, (c) area control errors (ACE) of Area 1, (d) ACE of Area 2.

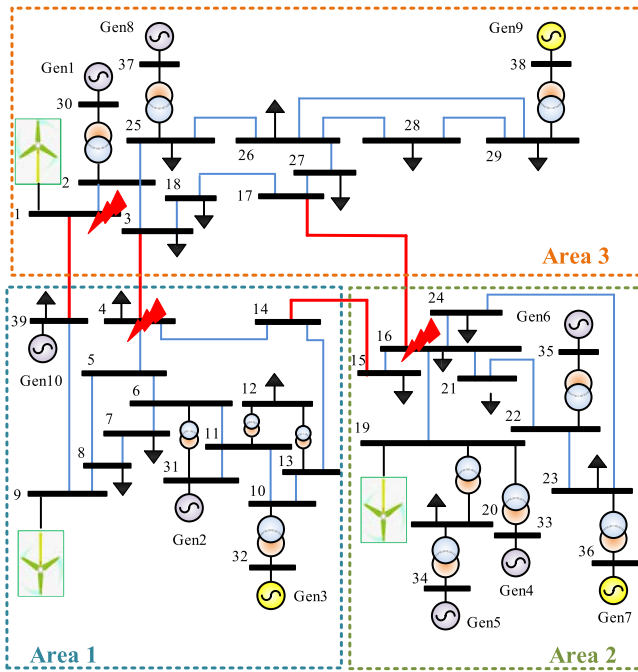


FIGURE 6 Modified IEEE-39 bus test system.

areas. In this test system, G_3 in Area 1, G_7 in Area 2, and G_9 in Area 3 are accountable for the performance of LFC in each control area, respectively.

The explanation for the FOGSMC scheme is as follows:

$$u(t) = -0.9x(t) + 0.7 \int_0^t x(s)ds + 0.1\dot{f}(t) + 21s(t) - 0.01\text{sgn}(s(t)) - 14D^{0.92}x(t)$$

where $s(t) = x(t) + 4 \int_0^t x(s)ds + 0.1653f(t) + 14D^{0.08}x(t)$

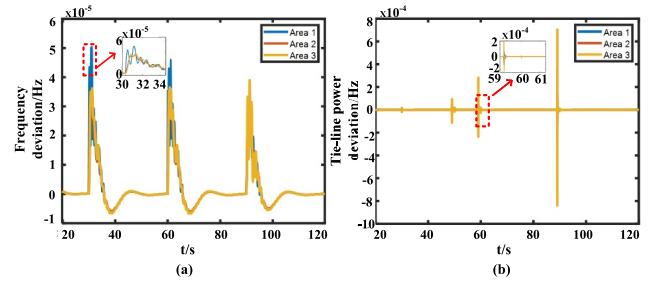


FIGURE 7 Results: (a) Frequency deviations of Modified IEEE 39-bus test system, (b) Tie line power deviations of Modified IEEE-39 bus test system.

To study the effectiveness of the designed method under hybrid cyber attacks in a realistic power system, step load disturbances $0.038p.u.MW$ on Bus 8 at $t = 30s$ in Area 1, $0.064p.u.MW$ on Bus 16 at $t = 60s$ in Area 2, and $0.038p.u.MW$ on Bus 3 at $t = 90s$ in Area 3 are setting, and implementing the hybrid cyber attacks on bus 3, 8, and 16.

It is observed from Figure 7a,b that, after hybrid cyber attacks and external load disturbances are launched, three area frequency and tie-line power deviations are greatly influenced. Then, by employing the designed LFC scheme with FOGSMC, frequency and tie-line power deviation can restore to zero in a short time with barely perceptible overshoots and acceptable transient performance. Thereby, the LFC scheme developed with FOGSMC can maintain system stability, it is effective for hybrid cyber attacks and external load disturbances. In a future study, the application of the designed method for searching engineering issues will be focussed on.

5 | CONCLUSION

Considering hybrid cyber attacks and external load disturbances, the stability and stabilisation of the LFC power system with wind power and energy storage have been investigated. First, the Markov jump linear theory is proposed to model the delay-dependent multi-area LFC under DoS and deception attacks. Meanwhile, an AEt scheme with an adjustable triggering threshold has been utilised in this study, which can effectively save more network resources, by considering the impacts of DoS and deception attacks. Moreover, the proposed FOGSMC approach combined the merits of robust stability and a new degree of freedom, providing an outstanding disturbance rejection performance, which can be rigorously proven by the comparison simulation results. Then, in the simulation example, the designed approach exhibits faster performance to restore frequency to preset value than other approaches. Finally, in the IEEE 39-bus test system, the effectiveness of the proposed approach under hybrid cyber-attacks is verified.

AUTHOR CONTRIBUTIONS

Xinxin Lv: Conceptualisation; Methodology; Software; Writing - Original Draft. **Yonghui Sun:** Writing - Review & Editing; Data Curation, Validation. **Venkata Dinavahi:**

Supervision; Writing - Review & Editing. **Xinlong Zhao**: Validation; Investigation. **Feng Qiao**: Software; Methodology

ACKNOWLEDGEMENTS

This work was supported in part by the Science Foundation of Zhejiang Sci-Tech University under Grant 21022311-Y, General Projects of Zhejiang Provincial Department of Education under Grant 22220109-F, National Natural Science Foundation of China under Grant 61673161, in part by the Natural Science and Engineering Research Council (NSERC) of Canada.

CONFLICT OF INTEREST STATEMENT


We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Xinxin Lv  <https://orcid.org/0000-0001-5007-2123>

Venkata Dinavahi  <https://orcid.org/0000-0001-7438-9547>

REFERENCES

- Chen, X., et al.: Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks. *IEEE Trans. Smart Grid* 13(3), 2357–2368 (2022)
- Shangguan, X., et al.: Control performance standards-oriented event-triggered load frequency control for power systems under limited communication bandwidth. *IEEE Trans. Control Syst. Technol.* 30(2), 860–868 (2022). <https://doi.org/10.1109/tcst.2021.3070861>
- Hu, S., et al.: Resilient load frequency control of islanded AC microgrids under concurrent false data injection and denial-of-service attacks. *IEEE Trans. Smart Grid* 14(1), 690–700 (2022). <https://doi.org/10.1109/TSG.2022.3190680>
- Hasnat, M., Rahnamay-Naeini, M.: Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states. *IET Smart Grid* 4(3), 307–320 (2021). <https://doi.org/10.1049/stg2.12030>
- Su, Y., Cai, H., Huang, J.: The cooperative output regulation by the distributed observer approach. *Int. J. Dyn. Control*, 20–35 (2022). <https://doi.org/10.53941/ijndi0101003>
- Oladipo, S., Sun, Y., Wang, Z.: An enhanced flower pollinated algorithm with a modified fluctuation rate for global optimisation and load frequency control system. *IET Renew. Power Gener.* 16(6), 1220–1245 (2022). <https://doi.org/10.1049/rpg2.12435>
- Jia, K., et al.: Analytical calculation of transient current from an inverter-interfaced renewable energy. *IEEE Trans. Power Syst.* 37(2), 1554–1563 (2021). <https://doi.org/10.1109/tpwrs.2021.3107580>
- Guo, Z., et al.: Optimisation methods for dispatch and control of energy storage with renewable integration. *IET Smart Grid* 5(3), 137–160 (2022). <https://doi.org/10.1049/stg2.12063>
- Wang, Y., Liang, H., Dinavahi, V.: Decentralized stochastic programming for optimal vehicle-to-grid operation in smart grid with renewable generation. *IET Smart Grid* 15(4), 746–757 (2021). <https://doi.org/10.1049/rpg2.12064>
- Kim, Y., Hakak, S., Ghorbani, A.: Smart grid security: attacks and defence techniques. *IET Smart Grid* (2022). <https://doi.org/10.1049/stg2.12090>
- Wang, Y., et al.: Detection of false data injection attacks in smart grid: a secure federated deep learning approach. *IEEE Trans. Smart Grid* 13(6), 4862–4872 (2022). <https://doi.org/10.1109/tsg.2022.3204796>
- Zhang, Q., Zhou, Y.: Recent advances in non-Gaussian stochastic systems control theory and its applications. *Int. J. Dyn. Control*, 111–119 (2022). <https://doi.org/10.53941/ijndi0101010>
- Liu, X., et al.: Event-triggered load frequency control of smart grids under deception attacks. *IET Control. Theory A* 15(15), 1335–1345 (2021). <https://doi.org/10.1049/cth2.12124>
- Yang, J., et al.: Dynamic-memory event-triggered H_∞ load frequency control for reconstructed switched model of power systems under hybrid attacks. *IEEE Trans. Cybern.*, 1–13 (2021). <https://doi.org/10.1109/TCYB.2022.3170560>
- Liu, M., et al.: Converter-based moving target defense against deception attacks in DC microgrids. *IEEE Trans. Smart Grid* 13(5), 3984–3996 (2022). <https://doi.org/10.1109/tsg.2021.3129195>
- Zhu, S., et al.: An adaptive torus-event-based controller design for networked T-S fuzzy systems under deception attacks. *Int. J. Robust Nonlinear Control* 32(6), 3425–3441 (2022). <https://doi.org/10.1002/rnc.5957>
- Liu, J., et al.: Event-based security tracking control for networked control systems against stochastic cyber-attacks. *Inf. Sci.* 612, 306–321 (2022). <https://doi.org/10.1016/j.ins.2022.08.085>
- Chen, P., et al.: Dynamic event-triggered output feedback control for load frequency control in power systems with multiple cyber attacks. *IEEE Trans. Syst., Man, Cybern., Syst.* 52(10), 6246–6258 (2022). <https://doi.org/10.1109/tsmc.2022.3143903>
- Yao, W., et al.: Resilient wide-area damping control for inter-area oscillations to tolerate deception attacks. *IEEE Trans. Smart Grid* 12(5), 4238–4249 (2021). <https://doi.org/10.1109/TSG.2021.3068390>
- Zha, L., et al.: Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks. *IEEE Trans. Cybern.* 52(12), 13800–13808 (2022). <https://doi.org/10.1109/tcyb.2021.3125851>
- Tian, E., Peng, C.: Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks. *IEEE Trans. Cybern.* 50(11), 4610–4618 (2020). <https://doi.org/10.1109/tcyb.2020.2972384>
- Li, F., Hou, Z.: Distributed model-free adaptive control for MIMO nonlinear multiagent systems under deception attacks. *IEEE Trans. Syst., Man, Cybern., Syst.*, 1–11 (2022). <https://doi.org/10.1109/TSMC.2022.3211871>
- Hu, S., et al.: Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. *IEEE Trans. Cybern.* 49(12), 4271–4281 (2018). <https://doi.org/10.1109/tcyb.2018.2861834>
- Liu, J., et al.: Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks. *IEEE Trans. Syst., Man, Cybern., Syst.* 49(8), 1665–1678 (2019). <https://doi.org/10.1109/tsmc.2019.2895060>
- Cheng, Z., et al.: Resilient dynamic event-triggered control for multi-area power systems with renewable energy penetration under DoS attacks. *IET Control. Theory A* 14(16), 2267–2279 (2020). <https://doi.org/10.1049/iet-cta.2019.1478>
- Li, Y., Huang, R., Ma, L.: Hierarchical-attention-based defense method for load frequency control system against DoS attack. *IEEE Internet Things J.* 20(8), 15522–15530 (2021). <https://doi.org/10.1109/jiot.2021.3073060>
- Liu, K., Seuret, A., Xia, Y.: Stability analysis of systems with time-varying delays via the second-order Bessel-Legendre inequality. *Automatica* 76, 138–142 (2017). <https://doi.org/10.1016/j.automatica.2016.11.001>
- Lv, X., et al.: Robust load frequency control for networked power system with renewable energy via fractional-order global sliding mode control. *IET Renew. Power Gener.* 15(5), 1046–1057 (2021). <https://doi.org/10.1049/rpg2.12088>
- Abazari, A., Monsef, H., Wu, B.: Load frequency control by de-loaded wind farm using the optimal fuzzy-based PID droop controller. *IET Renew. Power Gener.* 13(1), 180–190 (2019). <https://doi.org/10.1049/iet-rpg.2018.5392>

How to cite this article: LV, X., et al.: Robust networked power system load frequency control against hybrid cyber attack. IET Smart Grid. 1–12 (2023). <https://doi.org/10.1049/stg2.12107>

APPENDICES

For a given control performance parameter γ , an algorithm to find the allowable communication parameters $\lambda_{\min} = \min(\lambda(t_k b))$ and $\lambda_{\max} = \max(\lambda(t_k b))$ can be described as follows:

step 1: For given γ , setting $\lambda_m = \lambda_m + \iota$, where ι is the step increment of λ_m .

step 2: For a given λ_m , if there exists a feasible solution satisfying matrix inequalities Equations (15–18), go to the next step; otherwise, go to Step 1.

step 3: Using the MATLAB/LMI Toolbox, the Φ_r with matrix inequalities Equations (15–18) can be obtained.

step 4: Store λ_m, Φ_r and go to Step 1 until $\lambda_m \geq 1$ when the search is terminated.

In this theorem, the stability criteria can guarantee the closed-loop stability under the initial triggered threshold in Theorem 2.