Hybrid Dynamic Event-Triggered Load Frequency Control for Power Systems With Unreliable Transmission Networks

Guopin Liu, Ju H. Park, *Senior Member, IEEE*, Changchun Hua, *Senior Member, IEEE*, and Yafeng Li

***Abstract*—In this article, we consider the load frequency control problem for a class of power systems based on the dynamic event-triggered control (ETC) approach. The transmission networks are unreliable in the sense that malicious denial-of-service (DoS) attacks may arise in the power system. First, a model-based feedback controller is designed, which utilizes estimated states, and thus can compensate the error between plant states and the feedback data. Then, a dynamic event-triggered mechanism (DETM) is proposed by introducing an internal dynamic variable and a timer variable with jump dynamics. The proposed (DETM) can exclude Zeno behavior by regularizing a prescribed strictly positive triggering interval. Incorporated in the ETC scheme, a novel hybrid model is established to describe the flow and jump dynamics of the power system in the presence of DoS attacks. Based on the hybrid dynamic ETC scheme, the power system stability can be preserved if the attacks frequency and duration sustain within an explicit range. In addition, the explicit range is further maximized based on the measurement trigger-resetting property. Finally, a numerical example is presented to show the effectiveness of our results.**

***Index Terms*—Denial-of-service (DoS) attacks, dynamic event-triggered mechanism (DETM), hybrid system approach, load frequency control, power systems.**

I. Introduction

IN PRACTICE, the power system frequency is a crucial performance index, which should tightly maintain around an expected nominal value (50 or 60 Hz). The system frequency is essentially connected with real power balance, hence in the past decades, a traditional solution is to control real power output in the generator side, for instance, the automatic generation control (AGC) system approach. Nowadays, power systems are faced with new challenges, such as increasing stress in the transmission system and high penetration of renewable energies. Renewable power outputs with intermittent and large instantaneous variations limit the generation controllability [1], [2]. In addition, the increasing stress in the transmission system may limit the effective power transfer from generation to load [3]. Thus, researchers in recent years are revisiting the frequency control problem under this new paradigm [3], [4].

Compared with the frequency regulation methods that focus on power generation, direct load side control attracts an increasing interests as an alternative solution for frequency regulation due to its distinct merits, such as instantaneous response and distributed availability via the grid [2]. Many works on the implementation of load frequency control have been reported in the literature, see for instance [5]–[8]. In [9], based on the decentralized sliding-mode control technique, a load frequency control scheme is presented for multiarea power systems with uncertainties. By modeling the disturbance and parameter uncertainties into the power system, an adaptive dynamic programming-based load frequency control approach is proposed in [10] for the single area and multiarea power systems. In particular, numerous load frequency control results have been reported for power systems with the incorporation of electric vehicles (EVs), which can be adopted to suppress the fluctuations caused by load disturbances [11]–[16].

As a matter of fact, the power systems can be conceptualized as a class of networked control systems (NCSs), where distributed resources and assets of power systems are connected through wide-area transmission networks. This conceptualization can enhance the control and operation abilities. While, on the other hand, it triggers numerous theoretical and practical challenges to frequency regulation of power system, such as transmission delay [17] and faults of sensor [18]. In particular, the power systems transmit regulation control signals through public networks, which makes the networked power systems safety critical to malicious cyber attacks [19]. The safety sensitivity has promoted considerable attention to the cyber-security problems that arisen in the network power systems.

Manuscript received 12 April 2021; revised 7 September 2021 and 24 January 2022; accepted 25 March 2022. Date of publication 12 April 2022; date of current version 13 January 2023. This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1308300; in part by the National Natural Science Foundation of China under Grant 62103355, Grant U20A20187, and Grant 618255304; in part by the Science Fund for Creative Research Groups of Hebei Province under Grant F2020203013; in part by the Science and Technology Development Grant of Hebei Province under Grant 20311803D and Grant 19011824Z; and in part by the National Defence Fundamental Project under Grant 2020A130. This work of Ju H. Park was supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea Government (MSIT) under Grant 2020R1A2B5B02002002. This article was recommended by Associate Editor Y. Shi. *(Corresponding author: Ju H. Park.)*

Guopin Liu and Changchun Hua are with the School of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China (e-mail: guopinliu@outlook.com; cch@ysu.edu.cn).

Ju H. Park is with the Department of Electrical Engineering, Yeungnam University, Gyeongsan 38541, South Korea (e-mail: jessie@ynu.ac.kr).

Yafeng Li is with the Institute for Automatic Control and Complex Systems, University of Duisburg–Essen, 47057 Duisburg, Germany (e-mail: y.f.li@foxmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCYB.2022.3163271.

Digital Object Identifier 10.1109/TCYB.2022.3163271

For NCSs, one of the most common attacks is denial-of-service (DoS) attack, which primarily aims at compromising the availability of data and thus causing packet losses. The research on NCSs with DoS attacks has been widely investigated for the past decades [20]–[25]. For instance, Persis and Tesi [20] proposed a general DoS attack model based on its frequency and duration, then the input-to-state stability is analyzed for a class of NCSs subject to DoS attacks. Under switching communication network, Wang *et al.* [24] proposed a novel cooperative output-feedback control strategy for a class of cyber–physical systems with intermittent DoS attacks. However, due to the new challenges as mentioned above for power systems, there are still many open problems for the load frequency control of power systems in the presence of DoS attacks.

Traditional load frequency control approaches are implemented by the sample-data scheme, which usually utilizes time-triggered sampling approach. In this framework, networked congestion problems may arise due to the excessive transmission data or node energy. Therefore, it is of significant importance to design a load frequency control scheme such that the power system frequency can be well regulated, and the network resources consumption can be reduced as well. Over the past years, event-triggered control (ETC), which updates the control input only when the designed triggering rules are satisfied, has been verified as an effective strategy in saving transmission data. The research on ETC has been well investigated for NCSs [26]–[28]. For instance, Dimarogonas *et al.* [26] proposed an ETC scheme with integrator dynamics, based on which, the control input updates in accordance to the state measurement error ratio. A novel dynamic triggering mechanism is proposed for ETC in [29]. Zhao *et al.* [30], [31] then extended the dynamic triggering mechanism to multiagent systems in a hybrid system framework. The research of [32] inspires our article from a theoretical perspective, which presents a hybrid dynamic event-trigger mechanism for a class of nonlinear NCSs in the presence of DoS attacks. For LFC of power systems, Peng [33] proposed an adaptive ETC scheme by dynamically regulating the triggering threshold. The event-triggered strategies also have been incorporated for NCSs in the presence of cyber-attacks [34]–[38]. Liu *et al.* [36] investigated event-triggered LFC control for multiarea power systems in the presence of hybrid cyber-attacks. Observer-based ETC methods are proposed in [37] and [38] for NCSs subject to DoS attacks. While that the event-triggered approach has been extensively investigated, few of them focus on dynamic ETC of power systems in the presence of DoS attacks.

Motivated by the above observation, this article is concerned with the dynamic event-triggered LFC problem for a class of power systems with DoS attacks via a hybrid system approach. The main contributions are summarized as follows.

1) A hybrid dynamic ETM is proposed for load frequency control of power systems, which introduces an internal dynamic variable and a timer variable with jump dynamics. To the best of our knowledge, it is the first attempt to develop a hybrid dynamic ETM for power systems, which extends the application field of theoretical dynamic ETM results [29], [31], [32].
2) With the proposed dynamic ETM, a novel hybrid model is established for the closed-loop LFC power system, which can describe the flow and jump dynamics of the power system in the presence of DoS attacks.
3) A sufficient stability condition is provided, which explicitly characterizes the restriction on DoS attacks by its frequency and duration. Besides, compared with existing results [32], [39], the stability threshold is maximized based on the trigger-resetting property of estimated states, which significantly improve the power system robustness in the presence of DoS attacks.

TABLE I
PARAMETERS AND VARIABLES OF THE LFC POWER SYSTEM

Notations	Nomenclatures
D, M	load damping coefficient and inertia constant.
R_g	governor droop characteristic.
T_g, T_t	speed governor and turbine time constants.
ρ_e	EVs droop characteristic.
α_e, α_g	EVs participation factors and thermal turbine.
$\bar{K}$, T_e	EVs gain and time constants.
b	frequency bias constant.
$f(t)$	frequency deviation.
X_g	governor value position.
P_g	turbine output powers.
P_e	the incremental changes in EVs.
$\Delta(t)$	integration of the area control error.

The remainder of this article is organized as follows. Section II provides system description and preliminaries. In Section III, the hybrid dynamic ETM is presented and a hybrid model is established for the closed-loop power system with DoS attacks. Section IV presents the main results, which provides sufficient conditions and stability analysis for the LFC of a power system. In Section V, a numerical example is provided to verify the validity of the proposed approach. The final conclusion is given in Section VI.

Notation: Let $\mathbb{R}$ represent the set of reals. Given any $\alpha \in \mathbb{R}$, we denote the set of reals greater than (respectively, no less than) α by $\mathbb{R}_{>\alpha}$ (respectively, $\mathbb{R}_{\geq\alpha}$). Denote $\mathbb{R}^n$ to be a set of all n dimensional real column vectors. For any matrix Q, Q^{T} and $\|Q\|$ represent its transpose and spectral norm, respectively. The smallest and largest eigenvalues of Q are represented by $\lambda_{\min}(Q)$ and $\lambda_{\max}(Q)$, respectively. Given a measurable time function $g(t)$ mapping $\mathbb{R}_{\geq 0}$ to $\mathbb{R}^n$, denote the $\mathcal{L}_\infty$ norm of $g(\cdot)$ on time interval $[0, t)$ by $\|g_t\|_\infty := \sup_{s\in[0,t)} \|g(s)\|$. For any sets A and B, let $B\backslash A$ represent the relative complement of A in B, that is, the set of all elements that belong to B, but not to A.

II. PROBLEM FORMULATION

A. Systems Description

We consider the dynamic event-triggered LFC for a class of power systems, whose block diagram is shown as Fig. 1. The explanations for corresponding parameters and variables are listed in Table I [12], [39].

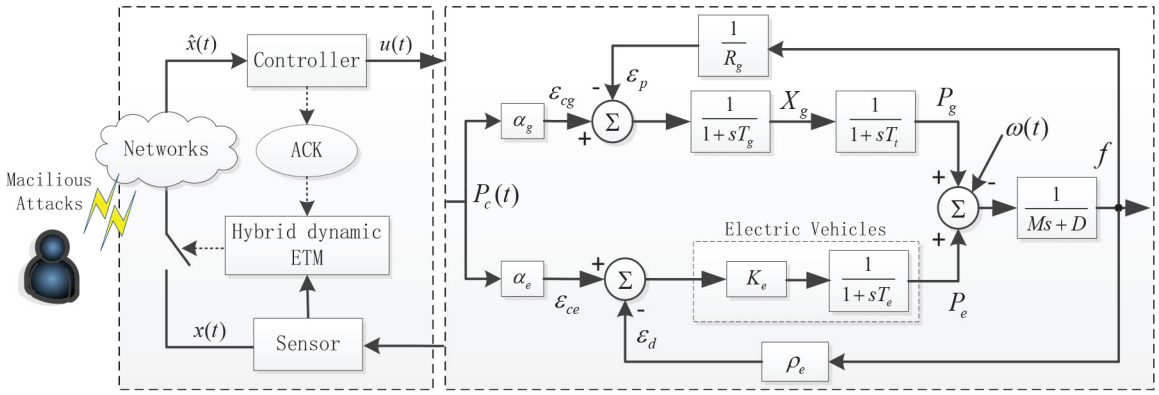


Fig. 1. Block diagram of the hybrid dynamic event-triggered power system with network attacks.

The dynamics of the power system can be derived as

$$\begin{aligned}\dot{x}(t) &= Ax(t) - B_u u(t) + B_w \omega(t)\\ y(t) &= Cx(t)\end{aligned} \tag{1}$$

where $x^{\mathrm{T}}(t) = [f(t) \;\; X_g(t) \;\; P_g(t) \;\; P_e(t) \;\; \Delta(t)]$ is the system states, $u(t) \in \mathbb{R}$, $y(t) \in \mathbb{R}^2$, and $\omega(t) \in \mathbb{R}$ represent the control input, system output, and external disturbance, respectively. A, B_u, B_w, and C are matrices in the following form:

$$A = \begin{bmatrix} -\frac{D}{M} & 0 & \frac{1}{M} & \frac{1}{M} & 0 \\ -\frac{1}{R_g T_g} & -\frac{1}{T_g} & 0 & 0 & 0 \\ 0 & \frac{1}{T_t} & -\frac{1}{T_t} & 0 & 0 \\ -\frac{\rho_e \bar{K}_e}{T_e} & 0 & 0 & -\frac{1}{T_e} & 0 \\ b & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$B_u^{\mathrm{T}} = \begin{bmatrix} 0 & \frac{\alpha_g}{T_g} & 0 & \frac{\alpha_e \bar{K}_e}{T_e} & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_w^{\mathrm{T}} = \begin{bmatrix} -\frac{1}{M} & 0 & 0 & 0 & 0 \end{bmatrix}.$$

In this article, the control action is finalized through a sensor-actuator network. We assume that (A, B_u) is stabilizable, and the control input applied to the power system is designed by

$$u(t) = K\hat{x}(t) \tag{2}$$

where feedback matrix $K = \alpha B_u^{\mathrm{T}} P$, α is a positive constant. $P > 0$ is the solution to the algebraic Riccati equation

$$PA + A^{\mathrm{T}}P - \alpha P B_u B_u^{\mathrm{T}} P + Q = 0 \tag{3}$$

where $Q > 0$. $\hat{x}(t)$ is the estimator states, which is specified by

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t), \; t \in (t_k, t_{k+1}] \\ \hat{x}^+(t) = x(t), \; t = t_k \end{cases} \tag{4}$$

in which $\{t_k\}_{k\in\mathbb{N}}$ represents the instant sequence of trigger.

Define $e(t)$ as the state estimated error in the form

$$e(t) = \hat{x}(t) - x(t) \tag{5}$$

and denote the performance output of the power system by $z(t) = C_z x(t)$, where C_z is constant matrix with appropriate size.

According to (1), (2), and (5), one can obtain the following results:

$$\begin{aligned}\dot{x}(t) &= Ax(t) - B_u K\hat{x}(t) + B_w\omega(t)\\ &= A_{11}^c x(t) + A_{12}^c e(t) + B_w\omega(t)\\ \dot{e}(t) &= Ae(t) + B_u K(e(t) + x(t)) - B_w\omega(t)\\ &= A_{21}^c x(t) + A_{22}^c e(t) - B_w\omega(t)\end{aligned} \tag{6}$$

where $A_{11}^c = A - B_u K$, $A_{12}^c = -B_u K$, $A_{21}^c = B_u K$, and $A_{22}^c = A + B_u K$.

Remark 1: In our article, an estimator (4) is established, which compared with the zero-order-hold strategy, can improve the control performance by eliminating the possible large error between plant state and the kept feedback data at the controller side. The variable $\hat{x}(t)$ is thus introduced and will be utilized as an estimation of $x(t)$. In fact, the design idea behind (2) and (4) is the well known model-based approach in NCSs, which have been studied in [40]–[43], just to name a few. In addition, the estimator with resetting property plays another crucial way in maximizing the stability condition characterized by the frequency and duration of DoS attacks. This property will be revisited in Section IV.

Remark 2: As illustrated in Fig. 1, the control action is implemented through a sensor-to-actuator network, which consequently indicates the malicious attacks can degrade the measurement (sensor-to-controller) channel. While, it should be pointed out that the proposed hybrid dynamic ETC scheme framework also can be extended to other practical configurations, such as decentralized control [44].

B. Denial-of-Service Attacks

The DoS in our article is referred as the phenomenon that communication is blocked by a malicious attacker and consequently prevent the control input (2) from being executed at a desired time. Specifically, the mth DoS attack period is denoted as $H_m = \{h_m\} \cup [h_m, h_m + \tau_m)$, where $h_m \in \mathbb{R}_{\geq 0}$ represents the instant when the mth DoS period starts and $\tau_m \in \mathbb{R}_{\geq 0}$ is the length of the period. As illustrated in Fig. 1, this article only consider the influence of DoS attacks on measurement (sensor-to-controller) channel.

For $T_1, T_2 \in \mathbb{R}_{\geq 0}$ with $T_1 < T_2$, define $\Xi(T_1, T_2) := [T_1, T_2] \cap \mathcal{I}_{\mathrm{DoS}}$, where $\mathcal{I}_{\mathrm{DoS}} = \bigcup_{m\in\mathbb{N}_0} H_m$, as the sets of time

instants where communication is denied for interval $[T_1, T_2]$. Then, for the interval $[T_1, T_2]$, the sets of time instants over which communication is free from the attacks can be obtained as $\Theta(T_1, T_2) := [T_1, T_2]\backslash\Xi(T_1, T_2)$. The length of time interval $\Xi(T_1, T_2)$ and $\Theta(T_1, T_2)$ are denoted as $|\Xi(T_1, T_2)|$ and $|\Theta(T_1, T_2)|$, respectively. Denote $n(T_1, T_2)$ as the attack numbers that the power system suffered during time interval $[T_1, T_2]$. Let $\underline{\Delta} \in \mathbb{R}_{>0}$ represent the minimum sample interval, namely, $\underline{\Delta} \leq t_{k+1} - t_k$ for all $k \in \mathbb{N}_0$. We propose the following assumptions to characterize the DoS attack sequence.

Assumption 1 (DoS Frequency [20]): Given any $T_1, T_2 \in \mathbb{R}_{\geq 0}$ with $T_1 \leq T_2$, one can find constants $\kappa_f \in \mathbb{R}_{\geq 0}$, $\tau_f \in \mathbb{R}_{\geq \underline{\Delta}}$ such that

$$n(T_1, T_2) \leq \kappa_f + \frac{T_2 - T_1}{\tau_f}. \tag{7}$$

Assumption 2 (DoS Duration [20]): Given any $T_1, T_2 \in \mathbb{R}_{\geq 0}$ with $T_1 \leq T_2$, one can find constants $\kappa_d \in \mathbb{R}_{\geq 0}$, $\tau_d \in \mathbb{R}_{>1}$ such that

$$|\Xi(T_1, T_2)| \leq \kappa_d + \frac{T_2 - T_1}{\tau_d}. \tag{8}$$

Remark 3: Assumptions 1 and 2, proposed by [20], characterize a class of time-constrained DoS attacks model, which is quite general since it constrains nothing but the frequency and duration properties of attacks. Therefore, these assumptions are widely utilized in existing works on DoS attacks, such as [21]–[23], and [32]. In this article, we use these assumptions to determine the amount of attacks that the power system can tolerate, see (21) in Theorem 1 and (45) in Lemma 3.

C. Problem Statement

The control objective of this article is as follows.

Design the control input as (2) and the hybrid dynamic event-triggered mechanism (DETM) described by (10) such that under DoS attacks which satisfy Assumption 1 and 2, the power system (1) is globally uniformly exponentially stable (GUES) if $\omega(t) = 0$. While if $\omega(t) \neq 0$, the power system is $\mathcal{L}_\infty$ stable from $\omega(t)$ to $z(t)$. In addition, maximize the amount of DoS attacks that characterized by its frequency and duration without destroying the stability of LFC for the power system.

III. Hybrid Power System Model Subject to DoS Attacks

A. Hybrid Dynamic ETM

In this part, a hybrid dynamic ETM is presented. Before that, a new time variable $\tau(t) \in \mathbb{R}_{\geq 0}$ is introduced to represent the elapsed time after the latest trigger attempt. The hybrid dynamics of $\tau(t)$ is set as

$$\begin{cases} \dot{\tau}(t) = 1, & \tau(t) \in \mathbb{C} \\ \tau^+(t) = 0, & \tau(t) \in \mathbb{D} \end{cases} \tag{9}$$

where $\mathbb{C}$ represents the flow set and $\mathbb{D}$ denotes the jump set, which both will be specified later.

With that, the hybrid dynamic ETM is designed as

$$t_{k+1} = \inf\left\{t \geq t_k + \tau_{\text{miet}}^{m(t)} | \eta(t) \leq 0, k \in \mathbb{N}_0\right\} \tag{10}$$

where $m(t) \in \{0, 1\}$ is an symbol variable, which is used to show the allowed or denied status of latest transmission attempt at time t. Without loss of generality, let $m(t) = 0$ denote that the latest transmission attempt is allowed and let $m(t) = 1$ represent the attempt is denied. $\tau_{\text{miet}}^{m(t)} > 0$ is a predetermined minimum event-triggering interval satisfying $0 < \tau_{\text{miet}}^1 < \tau_{\text{miet}}^0$ and $\tau_{\text{miet}}^0 \leq \underline{\Delta}$, where $\underline{\Delta}$ is as in Assumption 1. $\eta(t)$ is a crucial dynamical variable for the event-triggered scheme, which satisfies the following hybrid dynamics:

$$\begin{aligned} \dot{\eta}(t) &= \Psi(m(t), \eta(t), \varsigma(t)), \quad t \in (t_k, t_{k+1}) \\ \eta^+(t_k) &= \begin{cases} \bar{\eta}(t_k), & t_k \notin \mathcal{I}_{\text{DoS}} \\ \eta(t_k), & t_k \in \mathcal{I}_{\text{DoS}} \end{cases} \end{aligned} \tag{11}$$

where $\varsigma(t) = (e(t), \tau(t), \phi(t)) \in \mathbb{R}^5 \times \mathbb{R}_{\geq 0} \times [\lambda, \lambda^{-1}]$. $\phi \in [\lambda, \lambda^{-1}]$ is an auxiliary variable for the hybrid event-triggered scheme and λ is a tuning parameter satisfying $0 < \lambda < 1$. $\Psi(\cdot)$ is a function that depends on local variables.

Now, we present the specification of $\phi(t)$, $\tau_{\text{miet}}^{m(t)}$, $\Psi(\cdot)$, and $\bar{\eta}(t_k)$.

First, the follow dynamics of $\phi(t)$ is set as:

$$\dot{\phi}(t) = f_\phi(t)$$

where

$$f_\phi(t) = \begin{cases} (m(t) - 1)(2L\phi(t) + \gamma(\phi^2(t) + 1)), & \tau(t) \leq \tau_{\text{miet}}^{m(t)} \\ 0, & \tau(t) \geq \tau_{\text{miet}}^{m(t)} \end{cases} \tag{12}$$

with that $L = \|A + B_u K\|$, γ is a positive constant that satisfies the conditions specified in Theorem 1.

The time constant $\tau_{\text{miet}}^{m(t)}$ in this article is selected no larger than τ_M, which is denoted as the allowable bound for transmission interval. Specifically, τ_M is given in the following form [45]:

$$\tau_M = \begin{cases} \frac{1}{Lr} \arctan\left(\frac{r(1-\lambda)}{\Upsilon}\right), & \gamma > L \\ \frac{1}{L} \frac{1-\lambda}{1+\lambda}, & \gamma = L \\ \frac{1}{Lr} \text{arctanh}\left(\frac{r(1-\lambda)}{\Upsilon}\right), & \gamma < L \end{cases} \tag{13}$$

where $r = \sqrt{|(\gamma/L)^2 - 1|}$, $\Upsilon = (2\lambda/1 + \lambda)([\gamma/L] - 1) + 1 + \lambda$.

Consider τ_M given in (13). The following result holds.

Lemma 1 [45]: Let $\tilde{\phi}(0) = \lambda^{-1}$, where $\tilde{\phi}(t)$ is the solution to

$$\dot{\tilde{\phi}}(t) = -2L\tilde{\phi}(t) - \gamma\left(\tilde{\phi}^2(t) + 1\right). \tag{14}$$

If τ_M is determined by (13), then one has $\tilde{\phi}(t) \in [\lambda, \lambda^{-1}]$ for all $t \in [0, \tau_M]$, and $\tilde{\phi}(\tau_M) = \lambda$.

Lemma 1 indicates that the solution $\tilde{\phi}(t)$ to (14) will always be positive for $t \in [0, \tau_M]$, which is a crucial property for stability analysis. With the selection $\tau_{\text{miet}}^1 \leq \tau_{\text{miet}}^0 \leq \tau_M$, define $\phi_{\text{miet}} = \tilde{\phi}(\tau_{\text{miet}}^0)$, then the triggering function $\Psi(\cdot)$ is designed as

$$\Psi(\cdot) = \begin{cases} -\beta\eta(t), & \tau(t) \leq \tau_{\text{miet}}^0 \\ -\beta\eta(t) - \bar{\gamma}\|e(t)\|^2, & \tau(t) > \tau_{\text{miet}}^0 \\ 0, & m = 1, \tau(t) \in \mathbb{R}_{\geq 0} \end{cases} \tag{15}$$

where $\bar{\gamma} = \gamma(2\phi_{\text{miet}}L + \gamma(1 + \phi_{\text{miet}}^2))$.

In addition, for variable $\eta(t)$, the reset initial value $\bar{\eta}(t)$ in (11) and (18) is defined as $\bar{\eta}(t) = \gamma\phi_{\text{miet}}\|e(t)\|^2$.

The following lemma gives some properties on function $\phi(t)$, $\eta(t)$, and constant ϕ_{miet}.

Lemma 2 [32]: Denote $\mathcal{R}(\mathbb{X}_0)$ as the reachable states of the hybrid system $\mathcal{H}_{\text{DoS}}$ (16)–(18) with $\xi(0,0) \in \mathbb{X}_0$, then for any $\xi \in \mathcal{R}(\mathbb{X}_0)$, the following results hold:

1) $\tau(t) \geq \tau^0_{\text{miet}} \Leftrightarrow \phi(t) = \phi_{\text{miet}}$;
2) $\phi_{\text{miet}} \leq \phi(t) \leq \lambda^{-1}$;
3) $\eta(t) \geq 0$.

Remark 4: According to the hybrid ETM (10), a transmission attempt will occur after the elapsed time $\tau^{m(t)}_{\text{miet}}$ provided that $\eta(t) \leq 0$. In fact, after the triggered condition is satisfied at the instant when $\eta(t) = 0$, it will be reset to a positive value according to (11). Therefore, as indicated by Lemma 2, we have $\eta(t) \geq 0$ for all $t \geq 0$. On the other hand, the status of the measurement channel determines whether the transmission attempt is denied ($m(t) = 1$) or allowed ($m(t) = 0$). If a DoS sequence is affecting the channel, transmission attempts should be triggered frequently compared with when $m(t) = 0$ to figure out the end of attack. Hence, we can set $0 \leq \tau^1_{\text{miet}} \leq \tau^0_{\text{miet}}$, which indicates the triggering interval can be adjusted according to the DoS attack status. While to finalize the forementioned schedule, it assumes that the hybrid dynamic ETM can obtain the reception information of packages at the controller side.

Remark 5: A hybrid system exhibits both continuous and discrete dynamic behavior, which has benefit in modeling systems with ETC mechanism. In control literature, hybrid dynamic ETC strategies have also been investigated in some existing works for NCSs, such as [30] and [31]. Compared with above works, the specific event-triggered mechanism is different in our article. Besides, we also concerns the malicious attacks in the transmission network, which complicates the design procedure and stability analysis. In addition, to our best knowledge, this is the first attempt that concerns hybrid dynamic ETC for LFC of power systems in the presence of DoS attacks.

B. Hybrid Model of Power Systems

In this part, a hybrid model is proposed to describe the power system with both flow and jump dynamics.

Define $\xi(t) := [x^{\mathrm{T}}(t), e^{\mathrm{T}}(t), \eta^{\mathrm{T}}(t), \tau^{\mathrm{T}}(t), \phi^{\mathrm{T}}(t)]^{\mathrm{T}}$. Then, we can rewrite the power system with DoS attacks by the hybrid model as follows:

$$\mathcal{H}_{\text{DoS}}: \begin{cases} \dot{\xi}(t) = F(\xi(t), \omega(t)), & \xi(t) \in \mathbb{C} \\ \xi^+(t) \in G(\xi(t)), & \xi(t) \in \mathbb{D} \end{cases} \tag{16}$$

where $F(\xi(t), \omega(t))$ represents the flow dynamics and $G(\xi(t))$ represents the jump dynamics. $\mathbb{C}$ and $\mathbb{D}$ are as in (9).

According to (6), (9), and (11), the flow dynamics for the power system is derived in the following form:

$$\dot{\xi}(t) = F(\xi(t), \omega(t)), \quad \xi \in \mathbb{C} \tag{17}$$

where

$$F(\xi, \omega) = \begin{bmatrix} \dot{x}(t) \\ \dot{e}(t) \\ \dot{\eta}(t) \\ \dot{\tau}(t) \\ \dot{\phi}(t) \end{bmatrix} = \begin{bmatrix} A^c_{11}x(t) + A^c_{12}e(t) + B_w\omega(t) \\ A^c_{21}x(t) + A^c_{22}e(t) - B_w\omega(t) \\ \Psi(\cdot) \\ 1 \\ f_\phi(t) \end{bmatrix}.$$

The flow set is defined as

$$\mathbb{C} := \left\{\xi(t) \in \mathbb{X} | \tau(t) \leq \tau^{m(t)}_{\text{miet}} \text{ or } \eta(t) > 0\right\}$$

where $\mathbb{X} = \mathbb{R}^5 \times \mathbb{R}^5 \times \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \times [\lambda, \lambda^{-1}]$.

Recall (6), (9), and (11), and one can obtain the jump dynamics for the power system as

$$\xi^+(t) \in \begin{cases} G_0(\xi(t)), \ \xi \in \mathbb{D} \text{ and } t \notin \mathcal{I}_{\text{DoS}} \\ G_1(\xi(t)), \ \xi \in \mathbb{D} \text{ and } t \in \mathcal{I}_{\text{DoS}} \end{cases} \tag{18}$$

where

$$G_0(\xi(t)) = \begin{bmatrix} x(t) \\ 0 \\ \bar{\eta}(t) \\ 0 \\ \lambda^{-1} \end{bmatrix}, \ G_1(\xi(t)) = \begin{bmatrix} x(t) \\ e(t) \\ \eta(t) \\ 0 \\ \phi(t) \end{bmatrix}.$$

The dynamic set is defined as

$$\mathbb{D} := \{\xi(t) \in \mathbb{X} | \tau(t) > \tau^{m(t)}_{\text{miet}} \text{ and } \eta(t) \leq 0\}.$$

From (18), some variables in $\xi(t)$ do not show discrete dynamic behavior if the trigger instance is affected by a DoS sequence. Based on suitable restrictions on DoS frequency and duration, this problem is compensated by the convergence property in a normal working period. For the closed-loop hybrid power system model (16)–(18). The following definitions on its stability and performance are provided.

Definition 1: For the power system described by hybrid model (16)–(18), the set $\bar{\mathcal{A}} = \{\xi(t) \in \mathbb{X} | x(t) = 0, e(t) = 0\}$ is said to be GUES if there exist constants $C > 0, a > 0$ such that

$$|\xi(t)|_{\bar{\mathcal{A}}} \leq C|\xi(0)|_{\bar{\mathcal{A}}} \exp(-at) \tag{19}$$

holds for any initial condition $\xi(0) \in \mathbb{X}_0$, where $\mathbb{X}_0 = \{\xi(t) \in \mathbb{X} | \tau(t) \geq \tau^0_{\text{miet}}, \eta(t) = 0, \phi(t) = \phi_{\text{miet}}\}$, ϕ_{miet} is a constant specified in Section IV.

Definition 2: For the power system described by hybrid model (16)–(18), if there exist $\mathcal{K}_\infty$ function β and positive constant γ^* such that

$$\|z(t)\|_{\mathcal{L}_\infty} \leq \beta(|\xi(0)|_{\bar{\mathcal{A}}}) + \gamma^*\|\omega(t)\|_{\mathcal{L}_\infty}$$

holds for any initial condition $\xi(0) \in \mathbb{X}_0$ and exogenous disturbance $\omega \in \mathcal{L}_\infty$, then the closed set $\bar{\mathcal{A}}$ as given in Definition 1 is said to be $\mathcal{L}_\infty$ stable from $\omega(t)$ to $z(t)$ with an $\mathcal{L}_\infty$-gain no larger than γ^*.

IV. Main Results

In this section, we present sufficient conditions for the LFC of power systems, under which the closed-loop stability can be preserved in the presence of DoS attacks.

A. Stability Performance Under DoS Attacks

First, we present the main result of this section.

Theorem 1: Consider the power system with hybrid model (16)–(18). If there exist constants $c \geq \|\alpha P B_u B_u^{\mathrm{T}} P\|$, $\epsilon > 0$, $\gamma > \epsilon + c$, $0 < \rho < 1$, and $\gamma_\omega > 0$ such that

$$\begin{bmatrix} \Pi_{11} & 0 & \Pi_{13} \\ * & \Pi_{22} & 0 \\ * & * & \Pi_{33} \end{bmatrix} \leq 0 \tag{20}$$

where $\Pi_{11} = -(1-\rho)Q + (B_u K)^{\mathrm{T}} B_u K$, $\Pi_{13} = -(B_u K)^{\mathrm{T}} B_w + PB_w$, $\Pi_{22} = -\gamma^2 + c + \epsilon$, and $\Pi_{33} = B_w^{\mathrm{T}} B_w - \gamma_\omega^2 I$. Then, for any DoS attacks characterized by (7) and (8) with parameters τ_d and τ_f satisfying

$$\frac{\tau_{\mathrm{miet}}^1}{\tau_f} + \frac{1}{\tau_d} < \frac{\lambda_s}{\lambda_s + \lambda_u} \tag{21}$$

the designed controller (2) with (4) and hybrid dynamic ETM (10) can ensure the closed set $\bar{\mathcal{A}} = \{\xi(t) \in \mathbb{X} | x(t) = 0, e(t) = 0\}$ is GUES in case of $\omega(t) = 0$, and the power system is $\mathcal{L}_\infty$-stable in case of $\omega(t) \neq 0$ with a finite $\mathcal{L}_\infty$-gain less than $\gamma_\omega \sqrt{(\alpha_z \kappa^*)/\lambda^*}$, where $\alpha_z \geq \|c_z^{\mathrm{T}} c_z / P\|$, $\lambda_s = \min\{[\lambda_{\min}(Q)\rho/\lambda_{\max}(P)], (\lambda/\gamma)\epsilon, \beta\}$, $\lambda_u = ([\bar{\gamma} - \epsilon]/\gamma\phi_{\mathrm{miet}})$, $\kappa^* = (\lambda_s + \lambda_u)\kappa_{\mathrm{dos}}$, and $\lambda^* = \lambda_s - (\lambda_s + \lambda_u)/\tau_{\mathrm{dos}}$.

Proof: In order to construct a proper Lyapunov function, which decreases at the triggering instant, consider the locally Lipschitz function $V_e(e(t)) = \|e(t)\| : \mathbb{R}^5 \to \mathbb{R}_{\geq 0}$. Recall (4) and (5), one has $e^+(t) = 0$ due to that $\hat{x}(t)$ resets to $x(t)$ at triggering instant. Hence, we can find constants $0 < \underline{\alpha}_e \leq \bar{\alpha}_e$, and $0 < \lambda_e < 1$ such that $\underline{\alpha}_e \|e(t)\| \leq V_e(e(t)) \leq \bar{\alpha}_e \|e(t)\|$ and $V_e^+(e(t)) \leq \lambda_e V_e(e(t))$ for all $e(t) \in \mathbb{R}^5$. In the remainder of this article, we adopt the notation $\|e(t)\|$ instead of $V_e(e(t))$. According to (6), one has that the upper bound of the derivative of $\|e(t)\|$ satisfies

$$\left\langle \frac{\partial \|e(t)\|}{\partial e(t)}, \dot{e}(t) \right\rangle \leq L\|e(t)\| + \|B_u K x(t) - B_\omega \omega(t)\| \tag{22}$$

where $L = \|A + B_u K\|$, which is as defined in (12).

Then, the candidate Lyapunov function is constructed as

$$V(\xi(t)) = x^{\mathrm{T}}(t) P x(t) + \gamma \phi(t) \|e(t)\|^2 + \eta(t). \tag{23}$$

From Lemma 2, we know that $\phi(t) \geq \phi_{\mathrm{miet}}(t) > 0$ and $\eta(t) \geq 0$. Thus, the radial unboundedness of $V(\xi(t))$ can be verified according to that $x^{\mathrm{T}}(t)Px(t)$ and $\|e(t)\|$ are radially unbounded. Therefore, we can find positive constant $\underline{\alpha}_V \in \mathbb{R}_{\geq 0}$ such that $\underline{\alpha}_V |\xi|_{\bar{\mathcal{A}}}^2 \leq V(\xi)$ for all $\xi \in \bar{\mathcal{A}}(\mathbb{X}_0)$, where $\bar{\mathcal{A}}$ is as defined in Definitions 1 and 2. Therefore, we have that $V(\xi)$ is an appropriate candidate Lyapunov function.

Now, we analyze the closed-loop hybrid power system with jump dynamics and flow dynamics subject to DoS attacks.

Jumps: We first prove that the Lyapunov function does not increase at the triggering instants, that is, $t = t_k, k \in \mathbb{N}$.

For the case $t_k \notin \mathcal{I}_{\mathrm{DoS}}$, the transmission channel is free from the DoS attacks. According to the trigger condition (10), we have $\eta(t_k) = 0$. From (18), one has

$$V(\xi^+(t)) - V(\xi(t)) = \bar{\eta}(t) - \gamma \phi(\tau(t)) \|e(t)\|^2. \tag{24}$$

Since $\tau \geq \tau_{\mathrm{miet}}^0$ at the triggering instant, one has $\phi(t) = \phi_{\mathrm{miet}}$, which yields

$$V\big(\xi^+(t)\big) - V(\xi(t)) = 0. \tag{25}$$

For the case $t_k \in \mathcal{I}_{\mathrm{DoS}}$, from (18), one has $e^+(t) = e(t)$, $\phi^+(t) = \phi(t)$, $\eta^+(t) = \eta(t)$, which indicates that (25) still hold. Thus, we claim that the at the triggering instants, the constructed Lyapunov function does not increase no matter the transmission channel is under attacks or not.

Flows: Now, we analyze the stability of the closed-loop hybrid power system during the flow.

First of all, consider the case that the latest transmission attempt is successful, that is, $m(t) = 0$. For almost all $\xi(t) \in \mathcal{R}(\mathbb{X}_0)$, one has

$$\begin{aligned} &\langle \nabla V(\xi(t)), F(\xi(t), \omega(t)) \rangle \\ &= x^{\mathrm{T}}(t)(PA_{11}^c + A_{11}^{cT} P) + 2x^{\mathrm{T}}(t) P A_{12}^c e(t) \\ &\quad + 2x^{\mathrm{T}}(t) P B_w \omega(t) + \gamma \|e(t)\|^2 \dot{\phi}(t) \\ &\quad + 2\gamma \phi(\tau) \|e(t)\| \dot{e}(t) + \dot{\eta}(t) \\ &= x^{\mathrm{T}}(t)\big[P(A - B_u K) + (A - B_u K)^{\mathrm{T}} P\big] x(t) \\ &\quad + 2x^{\mathrm{T}} P(-B_u K) e(t) + 2x^{\mathrm{T}}(t) P B_w \omega(t) \\ &\quad + \gamma \|e(t)\|^2 \dot{\phi}(t) + 2\gamma \phi(\tau) \|e(t)\| \dot{e}(t) + \dot{\eta}(t) \end{aligned} \tag{26}$$

where the second equality is obtained according to $A_{11}^c = A - B_u K$ and $A_{12}^c = -B_u K$. Substituting $K = \alpha B_u^{\mathrm{T}} P$ into (26), one has

$$\begin{aligned} &\langle \nabla V(\xi(t)), F(\xi(t), \omega(t)) \rangle \\ &\leq x^{\mathrm{T}}(t)\big[PA + A^{\mathrm{T}} P - (2\alpha - \alpha) P B_u B_u^{\mathrm{T}} P\big] x(t) \\ &\quad + \alpha e^{\mathrm{T}}(t) \|P B_u B_u^{\mathrm{T}} P\| e(t) + 2x^{\mathrm{T}}(t) P B_w \omega(t) \\ &\quad + \gamma \|e(t)\|^2 \dot{\phi}(t) + 2\gamma \phi(\tau) \|e(t)\| \dot{e}(t) + \dot{\eta}(t) \\ &\leq -x^{\mathrm{T}}(t) Q x(t) + \alpha e^{\mathrm{T}}(t) \|P B_u B_u^{\mathrm{T}} P\| e(t) \\ &\quad + 2x^{\mathrm{T}}(t) P B_w \omega(t) + \gamma \|e(t)\|^2 \dot{\phi}(t) \\ &\quad + 2\gamma \phi(\tau) \|e(t)\| \dot{e}(t) + \dot{\eta}(t). \end{aligned} \tag{27}$$

If (20) can be satisfied, the following results can be obtained by letting the matrix in (20) left multiplied by $[x^{\mathrm{T}}(t)\ e^{\mathrm{T}}(t)\ \omega^{\mathrm{T}}(t)]$ and right multiplied by $[x^{\mathrm{T}}(t)\ e^{\mathrm{T}}(t)\ \omega^{\mathrm{T}}(t)]^{\mathrm{T}}$

$$\begin{aligned} &-x^{\mathrm{T}}(t) Q x(t) + 2x^{\mathrm{T}}(t) P B_w \omega(t) \\ &\leq -\rho x^{\mathrm{T}}(t) Q x(t) + (\gamma^2 - c - \epsilon) \|e(t)\|^2 \\ &\quad + \gamma_w^2 \|\omega(t)\|^2 - \|B_u K x(t) - B_w \omega(t)\|^2. \end{aligned} \tag{28}$$

From (27) and (28), when $\tau(t) \leq \tau_{\mathrm{miet}}^0$, one has

$$\begin{aligned} &\langle \nabla V(\xi(t)), F(\xi(t), \omega(t)) \rangle \\ &\leq -\rho x^{\mathrm{T}}(t) Q x(t) + (\gamma^2 - c - \epsilon) \|e(t)\|^2 \\ &\quad + \gamma_w^2 \|\omega(t)\|^2 - \|B_u K x(t) - B_w \omega(t)\|^2 \\ &\quad + \gamma \|e(t)\|^2 \Big(-2L\phi(\tau) - \gamma(\phi(\tau)^2 + 1)\Big) \\ &\quad + \alpha e^{\mathrm{T}}(t) P B_u B_u^{\mathrm{T}} P e(t) - \beta \eta(t) \\ &\quad + 2\gamma \phi(\tau) \|e(t)\| (L\|e(t)\| + \|B_u K x(t) - B_w \omega(t)\|). \end{aligned} \tag{29}$$

Select parameter c such that $c \geq \|\alpha P B_u B_u^{\mathrm{T}} P\|$, then we can obtain

$$\langle \nabla V(\xi(t)), F(\xi(t), \omega(t)) \rangle$$

$$\begin{aligned}&\le -\rho x^{\mathrm{T}}(t)Qx(t)-\epsilon\|e(t)\|^2-\beta\eta(t)+\gamma_w^2\|\omega(t)\|^2\\&\quad-(\|B_uKx(t)-B_w\omega(t)\|-\gamma\phi(\tau)\|e(t)\|)^2\\&\le -\lambda_s V(\xi(t))+\gamma_w^2\|\omega(t)\|^2\end{aligned}\tag{30}$$

where $\lambda_s=\min\{[\lambda_{\min}(Q)\rho/\lambda_{\max}(P)],(\lambda/\gamma)\epsilon,\beta\}$.

When $\tau(t)\ge\tau^0_{\mathrm{miet}}$, according to (12), (15), (27), and (28), we have

$$\begin{aligned}&\langle\nabla V(\xi(t)),F(\xi(t),\omega(t))\rangle\\&\le -\rho x^{\mathrm{T}}(t)Qx(t)+(\gamma^2-c-\epsilon)\|e(t)\|^2\\&\quad+\gamma_w^2\|\omega(t)\|^2-\|B_uKx(t)-B_w\omega(t)\|^2\\&\quad+\alpha e^{\mathrm{T}}(t)PB_uB_u^{\mathrm{T}}Pe(t)-\beta\eta(t)-\bar\gamma\|e(t)\|^2\\&\quad+2\gamma\phi(\tau)\|e(t)\|(L\|e(t)\|+\|B_uKx(t)-B_w\omega(t)\|).\end{aligned}\tag{31}$$

According to Lemma 2, $\tau(t)\ge\tau^0_{\mathrm{miet}}$ implies $\phi=\phi_{\mathrm{miet}}$. Substituting $\bar\gamma$ into (31), we can obtain that (30) still hold.

Now, we consider the case $m(t)=1$, namely, the latest transmission attempt fails due to the effects caused by DoS attacks. From (12) and (15) for this case, one has $\dot\phi(\tau)=0$, $\dot\eta(t)=0$. Continued from (27) and (28), we have

$$\begin{aligned}&\langle\nabla V(\xi(t)),F(\xi(t),\omega(t))\rangle\\&\le -\rho x^{\mathrm{T}}(t)Qx(t)+(\gamma^2-\epsilon)\|e(t)\|^2\\&\quad+\gamma_w^2\|\omega(t)\|^2-\|B_uKx(t)-B_w\omega(t)\|^2\\&\quad+2\gamma\phi(\tau)\|e(t)\|(L\|e(t)\|+\|B_uKx(t)-B_w\omega(t)\|).\end{aligned}\tag{32}$$

Since $2\gamma\phi\|e(t)\|\|B_uKx(t)-B_w\omega(t)\|\le\gamma^2\phi^2\|e(t)\|^2+\|B_uKx(t)-B_w\omega(t)\|^2$, one has

$$\begin{aligned}&\langle\nabla V(\xi(t)),F(\xi(t),\omega(t))\rangle\\&\le -\rho x^{\mathrm{T}}(t)Qx(t)+\gamma_w^2\|\omega(t)\|^2\\&\quad+\left(\gamma^2+2L\gamma\phi(\tau)+\gamma^2\phi^2-\epsilon\right)\|e(t)\|^2\\&\le(\bar\gamma-\epsilon)\|e(t)\|^2+\gamma_w^2\|\omega(t)\|^2.\end{aligned}\tag{33}$$

We can conclude that when $m(t)=1$, one has

$$\langle\nabla V(\xi(t)),F(\xi(t),\omega(t))\rangle\le\lambda_u V(\xi(t))+\gamma_w^2\|\omega(t)\|^2\tag{34}$$

where $\lambda_u=([\bar\gamma-\epsilon]/\gamma\phi_{\mathrm{miet}})$.

From previous analysis, we can find the Lyapunov function has different behaviors depending on the cases of $m(t)=0$ or $m(t)=1$. The proof idea is to decompose the time axis and determine the collection of time intervals where the DoS attack is either *on* ($m(t)=1$) or *off* ($m(t)=0$). However, the DoS attacks will cause *attack-induced actuation delay*, which arises due to the lower bound of the intertriggering interval τ^1_{miet}, that is to say, the states cannot updated immediately when a DoS signal is over until after a time interval with length τ^1_{miet}.

To address this problem, we consider the *effective* time intervals, over which either (30) or (34) hold. Given any $0\le T_1\le T_2$, consider the component $\xi(t)$ in hybrid system (16)–(18) and define $\bar\Theta(T_1,T_2)=\{s\in(T_1,T_2)|m(s)=0\}$ and $\bar\Xi(T_1,T_2)=[T_1,T_2]\backslash\bar\Theta(T_1,T_2)$. Then the interval $[T_1,T_2]$ is the disjoint union of $\bar\Theta(T_1,T_2)$ and $\bar\Xi(T_1,T_2)$, where $\bar\Theta(T_1,T_2)$ [respectively, $\bar\Xi(T_1,T_2)$] is the union of subintervals of $[T_1,T_2]$ over which the transmission is reliable (respectively, blocked), see example (Lemma 2, [20]) for details.

It is easy to find that the mth effective time interval over which condition (34) hold consist of H_m^i and the corresponding attack-induced actuation delay. Thus, one can obtain the upper bound of $|\bar\Xi(T_1,T_2)|$ by

$$|\bar\Xi(T_1,T_2)|\le|\Xi(T_1,T_2)|+n(T_1,T_2)\tau^1_{\mathrm{miet}}.\tag{35}$$

Substitute (7) and (8) into (35), it holds that

$$|\bar\Xi(T_1,T_2)|\le\kappa_{\mathrm{dos}}+\frac{T_2-T_1}{\tau_{\mathrm{dos}}}\tag{36}$$

where $\kappa_{\mathrm{dos}}=\kappa_d+\kappa_f\tau^1_{\mathrm{miet}}$, $\tau_{\mathrm{dos}}=\tau_d\tau_f/(\tau_d\tau^1_{\mathrm{miet}}+\tau_f)$.

In order to analyze the bounds of the constructed Lyapunov function, we represent $\bar\Xi(T_1,T_2)$ and $\bar\Theta(T_1,T_2)$ by the following disjoint unions:

$$\bar\Xi(T_1,T_2):=\bigcup_{k\in\mathbb{N}}Z_k\cap[T_1,T_2]\tag{37}$$

$$\bar\Theta(T_1,T_2):=\bigcup_{k\in\mathbb{N}}W_{k-1}\cap[T_1,T_2]\tag{38}$$

where

$$Z_k:=\begin{cases}[\zeta_k,\zeta_k+v_k], & \text{if } v_k>0\\ \{\zeta_k\}, & \text{if } v_k=0\end{cases}$$

$$W_k:=\begin{cases}[\zeta_k+v_k,\zeta_{k+1}], & \text{if } v_k>0\\ (\zeta_k,\zeta_{k+1}), & \text{if } v_k=0\end{cases}$$

where $\{\zeta_k\}_{k\in\mathbb{N}}$ is an auxiliary sequence representing the time instants at which the effective attacks begin ($\zeta_0:=h_0$). v_k represents the time elapsed from ζ_k to the next allowed transmission attempt.

The intervals Z_k and W_k actually represent the power system's stable and unstable mode subject to DoS attacks. Consider the intervals $W_k,k\in\mathbb{N}$. According to (30), one has

$$\begin{aligned}V(\xi(t))\le{}&e^{-\lambda_s(t-\zeta_k-v_k)}V(\xi(\zeta_k+v_k))\\&+\gamma_w^2\int_{\zeta_k+v_k}^t e^{-\lambda_s(t-s)}|\omega(s)|^2ds.\end{aligned}\tag{39}$$

Next, consider the intervals $Z_k,k\in\mathbb{N}$. Recall (34), and we obtain

$$\begin{aligned}V(\xi(t))\le{}&e^{\lambda_u(t-\zeta_k)}V(\xi(\zeta_k))\\&+\gamma_w^2\int_{\zeta_k}^t e^{\lambda_u(t-s)}|\omega(s)|^2ds.\end{aligned}\tag{40}$$

With (39) and (40), and according to (25), one can obtain the following upper bound [20]:

$$\begin{aligned}V(\xi(t))\le{}&e^{-\lambda_s|\bar\Theta(0,t)|}e^{\lambda_u|\bar\Xi(0,t)|}V(\xi(0))\\&+\gamma_\omega^2\int_0^t e^{-\lambda_s|\bar\Theta(s,t)|}e^{\lambda_u|\bar\Xi(s,t)|}|\omega(s)|^2ds.\end{aligned}\tag{41}$$

According to (35) and (36) and the relationship that $|\bar\Theta(T_1,T_2)|=T_2-T_1-\bar\Xi(T_1,T_2)$, (41) can be rewritten as

$$\begin{aligned}V(\xi(t))\le{}&\kappa^*e^{-\lambda^*t}V(\xi(0))\\&+\kappa^*\gamma_\omega^2\|\omega\|^2_{\mathcal{L}_\infty}\int_0^t e^{-\lambda^*(t-s)}ds\end{aligned}\tag{42}$$

where $\kappa^*=(\lambda_s+\lambda_u)\kappa_{\mathrm{dos}}$ and $\lambda^*=\lambda_s-(\lambda_s+\lambda_u)/\tau_{\mathrm{dos}}$.

With (42) and the properties that $\underline{\alpha}_V|\xi|^2_{\bar{\mathcal{A}}}\le V(\xi)$, $\underline{\alpha}_e\|e\|\le\|V_e(e(t))\|\le\bar\alpha_e\|e(t)\|$ and $\eta(0)=0$, the following results hold.

1) In the case $\omega(t) = 0$

$$|\xi(t)|_{\bar{\mathcal{A}}} \leq \sqrt{\frac{\kappa^* \max\{\bar{\alpha}_x, \tilde{\alpha}_e\}}{\underline{\alpha}_V}} e^{-\frac{\lambda^*}{2}t} |\xi(0)|_{\bar{\mathcal{A}}} \tag{43}$$

where $\bar{\alpha}_x = \lambda_{\max}(P)$ and $\tilde{\alpha}_e = \gamma\phi_{\text{miet}}\bar{\alpha}_e^2$. Under the condition (21), we obtain $\lambda^* > 0$. Thus, we can claim that the closed set $\bar{\mathcal{A}}$ is GUES.

2) In the case $\omega(t) \neq 0$, from (42), one has

$$V(\xi(t)) \leq \kappa^* V(\xi(0)) + \kappa^* \gamma_\omega^2 \|\omega\|_{\mathcal{L}_\infty}^2 \int_0^t e^{-\lambda^*(t-s)} ds.$$

For any constant α_z such that $\alpha_z \geq \|c_z^{\mathrm{T}} c_z / P\|$, it holds that $|z(t)|^2 \leq \alpha_z V(\xi(t))$. In addition, since $V(\xi(0)) \leq \max\{\bar{\alpha}_x, \tilde{\alpha}_e\}|\xi(0)|_{\bar{\mathcal{A}}}^2$, one has that

$$\|z\|_{\mathcal{L}_\infty} \leq \beta(|\xi(0)|_{\bar{\mathcal{A}}}) + \gamma^* \|\omega\|_{\mathcal{L}_\infty} \tag{44}$$

where $\beta(|\xi(0)|_{\bar{\mathcal{A}}}) = \sqrt{\alpha_z \kappa^* \max\{\bar{\alpha}_x, \tilde{\alpha}_e\}}|\xi(0)|_{\bar{\mathcal{A}}}$ and $\gamma^* = \gamma_\omega \sqrt{(\alpha_z \kappa^*)/\lambda^*}$. According to Definition 2, we finally conclude that the power system is $\mathcal{L}_\infty$ stable. This completes the proof. ■

The condition (21) in Theorem 1 illustrates tradeoff between attack intensity and closed-loop stability. To be specific, increasing the DoS intensity can be implemented by decreasing τ_d and τ_f, which definitely increase the left-hand side of (21). Consequently, this stability criterion may be destroyed. In order to compensated the influence from DoS attacks, one may increase the convergence rate in the attack-free period, that is, the value of λ_s, to make condition (21) hold.

Remark 6: In order to make the proposed results technically clear, we summarize the design procedure as follows.

1) Initialize the parameters of the LFC power system as given in Table I.
2) Select proper parameter $\alpha > 0$ and matrix $Q > 0$ for the Riccati equation (3).
3) Obtain control gain K by solving (3) and $K = \alpha B_u^{\mathrm{T}} P$.
4) Select proper c such that $c \geq \|\alpha P B_u B_u^{\mathrm{T}} P\|$, and obtain parameter L by $L = \|A + B_u K\|$.
5) Select proper $\epsilon > 0$ and γ such that $\gamma > \epsilon + c$.
6) Select positive parameters β for (15), and $\lambda \in (0, 1)$ for initialization of $\tilde{\phi}(t)$ of (14) by $\tilde{\phi}(0) = \lambda^{-1}$.
7) Obtain τ_M according to (13), and obtain ϕ_{miet} from (14) by $\phi_{\text{miet}} = \tilde{\phi}(\tau_{\text{miet}}^0)$.
8) Derive $\bar{\gamma}$ for (15) by $\bar{\gamma} = \gamma(2\phi_{\text{miet}} L + \gamma(1 + \phi_{\text{miet}}^2))$.
9) Specify trigger intervals τ_{miet}^0 and τ_{miet}^1. With $\bar{\eta} = \gamma\phi_{\text{miet}}\|e(t)\|^2$, the HDETS (10) can be finalized according to (11) and (15).
10) Select proper $0 < \rho < 1$, and specify λ_s, λ_u. Allowable DoS sequence can be obtained by (21) in Theorem 1.

From Remark 6, one may notice the various parameters in our ETC mechanism. Following a rough guidance, one can increase the control gain K by enlarging the parameter α and matrix Q for the Riccati equation (3) to obtain a rapid convergence rate of $x(t)$ and $e(t)$. As for the triggering mechanism, the selection of parameter λ can influence the solution of $\tilde{\phi}(t)$ in (14). A smaller value of β can result in a slow convergence of η, which according to (10) can reduce the triggering number. Although this is also suit for parameter $\bar{\gamma}$, it is not easy to directly adjust this parameter since $\bar{\gamma}$ depends on many other parameters, such as α, ϵ, and λ.

B. DoS-Tolerance Maximization

According to (4) and (5), the estimation error $e(t)$ will reset to zero if the measured data is transmitted successfully through the measurement channel. If the resetting of $e(t)$, could be guaranteed, we know the attacks amount is tolerable intuitively. Bearing that in mind, in this part, we investigate the maximal amount of DoS attacks described by Assumptions 1 and 2 that the LFC power system can tolerant.

Define $\{z_m\}_{m\in\mathbb{N}}$ as the time instant sequence of successful transmission. The following lemma is crucial for this part.

Lemma 3: Consider the transmission network for the power system with the sampling interval larger than τ_{miet}^1. If the DoS sequence characterized by Assumptions 1 and 2 satisfies

$$\frac{1}{\tau_d} + \frac{\tau_{\text{miet}}^1}{\tau_f} < 1 \tag{45}$$

then

$$\begin{cases} z_0 \leq \Delta_{\text{dos}} \\ z_{m+1} - z_m \leq \Delta_{\text{dos}} + \tau_{\text{miet}}^1 \end{cases} \tag{46}$$

where $\Delta_{\text{dos}} = (\kappa_d + \kappa_f \tau_{\text{miet}}^1)(1 - [1/\tau_d] - [\tau_{\text{miet}}^1/\tau_f])^{-1}$.

Proof: Since $|\bar{\Theta}(h_m, t)| = t - h_m - \bar{\Xi}(h_m, t)$, from (36), one has

$$|\bar{\Theta}(h_m, t)| \geq (t - h_m)\left(1 - \frac{1}{\tau_d} - \frac{\tau_{\text{miet}}^1}{\tau_f}\right) - \kappa_d - \kappa_f \tau_{\text{miet}}^1. \tag{47}$$

If $|\bar{\Theta}(h_m, t)| > 0$, one has that at least one successful transmission occurs within the interval $[h_m, t]$, which shows that the $[h_m, t]$ includes a interval without DoS attacks larger than τ_{miet}^1. Suppose no successful transmission attempt occurs during $[h_m, h_m + \Delta_{\text{dos}}]$, then there exists a time $t_h \geq h_m + \Delta_{\text{dos}}$ such that $|\bar{\Theta}(h_m, t_h)| = 0$. However, recall (47), and one has $|\bar{\Theta}(h_m, t)| > 0$ for all $t > h_m + \Delta_{\text{dos}}$, which contradicts the above hypothesis. Therefore, one has that a successful transmission always occur within $[h_m, h_m + \Delta_{\text{dos}}]$.

Bearing that in mind, we now prove (46). First of all, consider the first inequality. If $h_0 > 0$, then $z_0 = t_0 = 0 \leq \Delta_{\text{dos}}$. While if $h_0 = 0$, based on above arguments, one successful transmission will occur within $[h_0, h_0 + \Delta_{\text{dos}}]$. Therefore, $z_0 \leq \Delta_{\text{dos}}$ still holds. Next, consider the second inequality. If the transmission at instant $z_m + \tau_{\text{miet}}^1$ is successful, one immediately has $z_{m+1} - z_m \leq \Delta_{\text{dos}} + \tau_{\text{miet}}^1$. While if the transmission at $z_m + \tau_{\text{miet}}^1$ is failed, it indicates one DoS attack must occur within $[z_m, z_m + \tau_{\text{miet}}^1]$. Namely, there exists $k \in \mathbb{N}_0$ such that $h_k \in [z_m, z_m + \tau_{\text{miet}}^1]$. In a similar analysis framework, we know one successful transmission will occur within $[z_m + \tau_{\text{miet}}^1, h_k + \Delta_{\text{dos}}]$, therefore, $z_{m+1} - z_m \leq \Delta_{\text{dos}} + \tau_{\text{miet}}^1$. ■

Remark 7: Lemma 3 shows that the estimation error $e(t)$ can always reset to zero in a finite-time provided that the DoS sequence characterized by Assumptions 1 and 2 satisfies (45). Therefore, condition (45) in fact provides a kind of stability

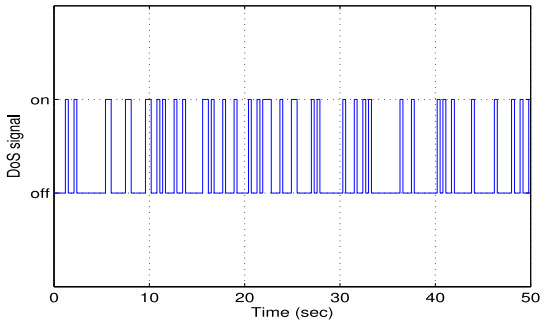


Fig. 2. Trajectory of DoS attack signal.

threshold under which the power system can preserve its stability under DoS attacks specified by Assumptions 1 and 2. Considering that $\tau_d > 1$ and $\tau_f > \tau^1_{\text{miet}}$, condition (45) illustrates the maximum amount boundary of DoS attacks with respect to τ_d and τ_f that the power system can tolerate.

The following proposition delivers the main idea of this section.

Proposition 1: Consider the power systems with DoS attacks that described by the hybrid model (16)–(18). Let the parameters and variables are as in Theorem 1. If the matrix condition (20) can be satisfied, then under the designed controller (2) with (4), and the hybrid dynamic ETM, the closed set $\bar{\mathcal{A}} = \{\xi(t) \in \mathbb{X} | x(t) = 0, e(t) = 0\}$ is stable provided that the DoS attacks described by Assumptions 1 and 2 satisfy (45).

Proof: With the boundedness of $e(t)$ under condition (45), the stability can be obtained immediately, and the detailed proof is thus omitted. ■

With Proposition 1, the restriction on DoS attacks can be significantly relaxed compared with (21) in Theorem 1. Therefore, the family of satisfactory DoS sequence is obviously increased.

V. Example

This section provides a numerical example to verify the proposed result of this article. Consider the LFC power system with incorporation of EVs, which has also been investigated in [12] and [39]. The power system parameters are given as

$$\begin{aligned} &D = 0.0083 \quad M = 0.1667 \quad R_g = 2.4 \quad T_g = 0.08 \\ &T_t = 0.3 \quad \rho_e = 0.4167 \quad K_e = 1 \quad T_e = 1 \\ &b = 0.425 \quad \alpha_g = 0.8 \quad \alpha_e = 0.2. \end{aligned}$$

Select parameters as $\alpha = 0.08$, $Q = I$, $\epsilon = 0.1$, $\lambda = 0.21$, and $\beta = 1$. Solving the Riccati equation (3), we can obtain the control gain

$$K = [0.0863 \quad 0.0936 \quad 0.0651 \quad 0.2812 \quad 0.2828]. \tag{48}$$

In addition, one obtains $L = \|A + B_u K\| = 20.6216$, $c = 2.2442$, $\gamma = 2.3542$, $\tau_M = 0.0650$, $\phi_{\text{miet}} = 0.2100$, and $\bar{\gamma} = 26.1760$.

With the results proposed in Section IV-B, the restriction on DoS attacks frequency and duration is significantly relaxed. One DoS attack signal example is illustrated in Fig. 2.

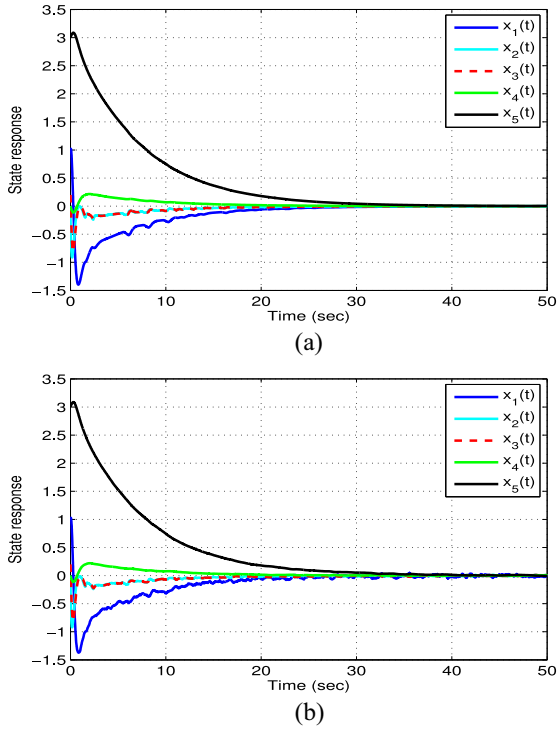


Fig. 3. Trajectories of states $x(t)$ in the presence of DoS attacks. (a) State response with $\omega(t) = 0$. (b) State response with $\omega(t) \neq 0$.

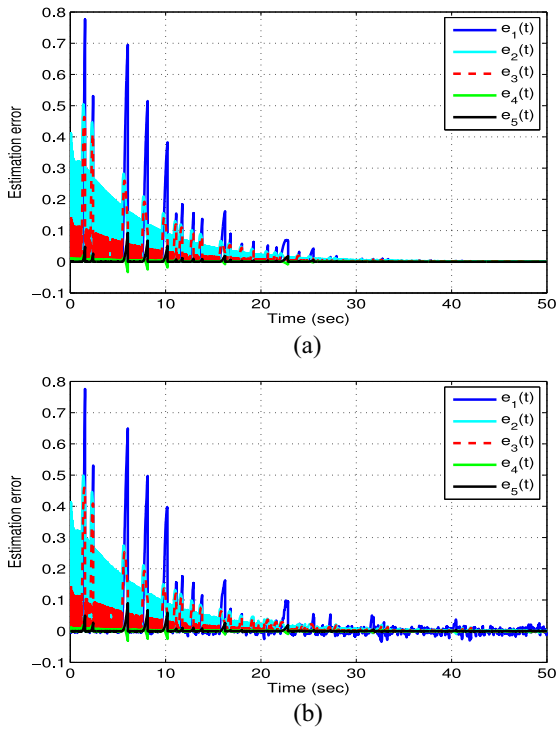


Fig. 4. Trajectories of estimate error $e(t)$. (a) Trajectories of $e(t)$ with $\omega(t) = 0$. (b) Trajectories of $e(t)$ with $\omega(t) \neq 0$.

Under the proposed hybrid dynamic event-triggered LFC scheme, the simulation results are shown in Figs. 3–6, respectively. The state responses are illustrated in Fig. 3, where both Fig. 3(a) and (b) clearly verified the convergence of power system states in the presence of DoS attacks. The estimation

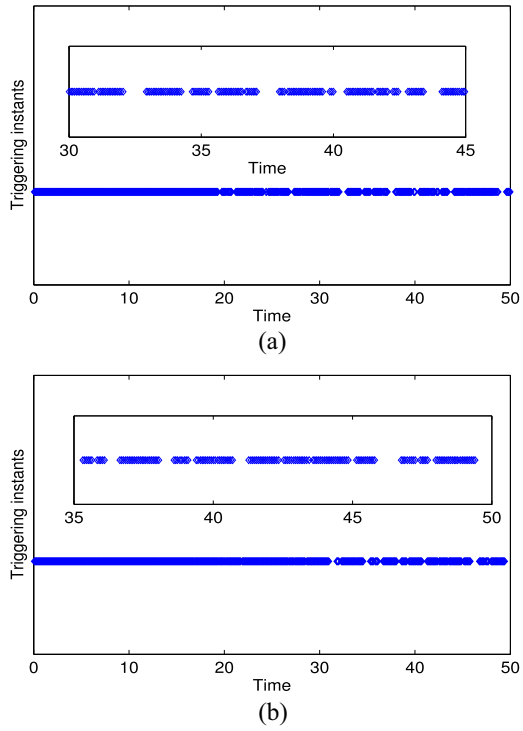


Fig. 5. Triggering instants for the power system. (a) Triggering instants for the power system with $\omega(t) = 0$. (b) Triggering instants for the power system with $\omega(t) \neq 0$.

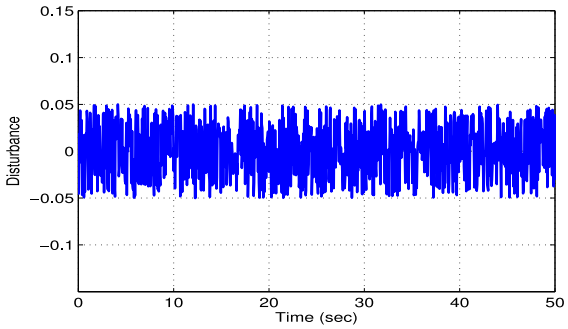


Fig. 6. Random external disturbances.

errors $e(t)$ are displayed in Fig. 4(a) [respectively, (b)] with the external disturbance $\omega(t) \neq 0$ [respectively, $\omega(t) = 0$]. The corresponding triggering instants are shown in Fig. 5, and the external disturbance applied to the simulation is illustrated in Fig. 6.

In order to illustrate the impact of design parameters on the control performance, we reset $\alpha = 0.4$, $\beta = 0.45$, and keep the other parameters as in previous setup. Solving the Riccati equation (3), we obtain another control gain as

$$K = [0.3202 \quad 0.3522 \quad 0.2446 \quad 0.7981 \quad 0.6325].$$

One also can obtain other parameters according to the design procedure demonstrated by Remark 6.

As mentioned in the context, this adjustment can increase the convergence rate of $x(t)$ and $e(t)$. The triggering number can be decreased as well. The simulation results are provided in Figs. 7–9.

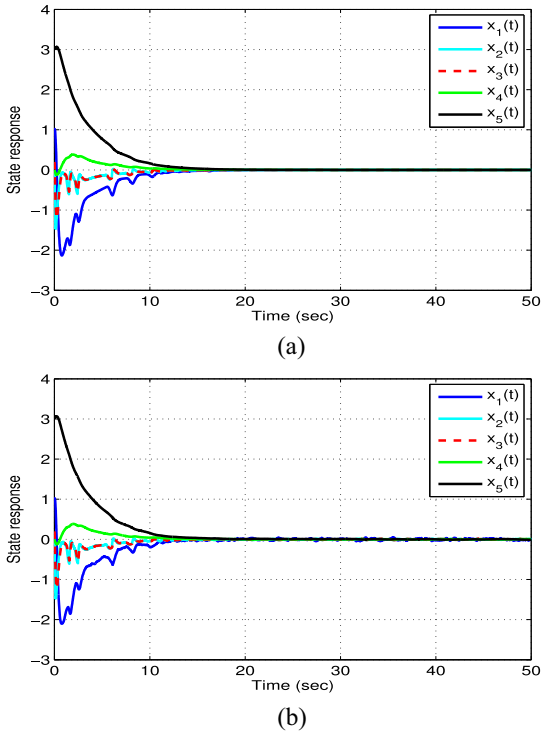


Fig. 7. Closed-loop state response in the presence of DoS attacks. (a) State response with $\omega(t) = 0$. (b) State response with $\omega(t) \neq 0$.

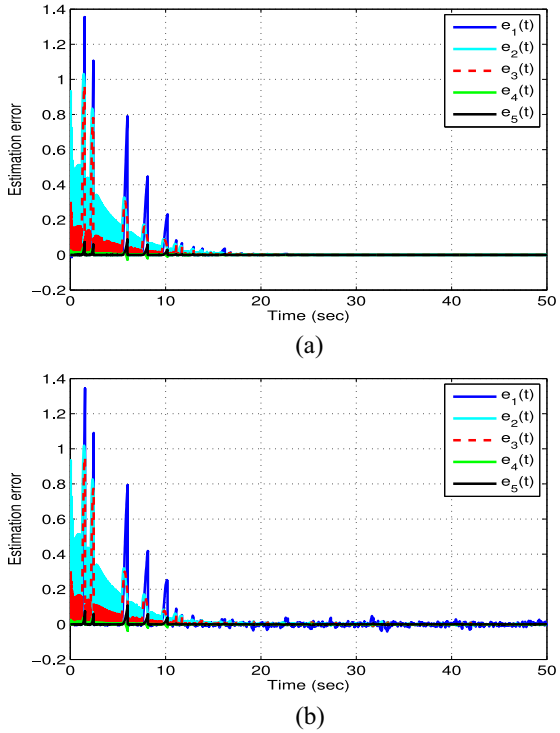


Fig. 8. Trajectories of estimate error $e(t)$. (a) Trajectories of $e(t)$ with $\omega(t) = 0$. (b) Trajectories of $e(t)$ with $\omega(t) \neq 0$.

VI. Conclusion

This article investigates the LFC problem for a class of power systems with unreliable measurement channel. A model-based controller is designed by equipping a state

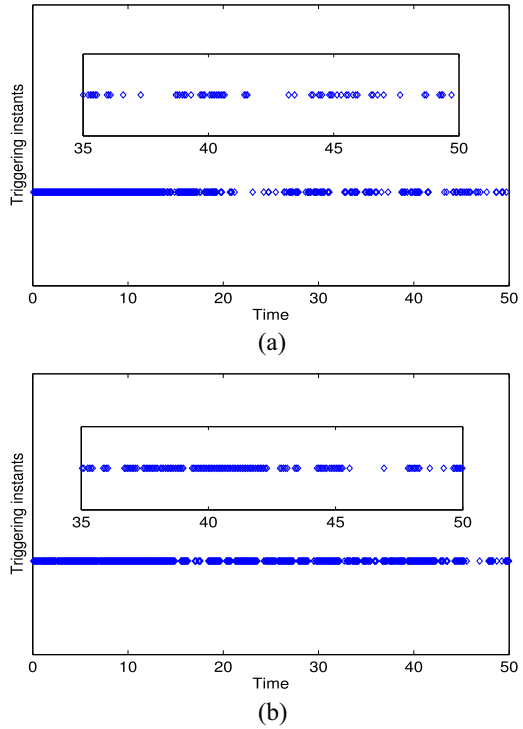


Fig. 9. Triggering instants for the power system. (a) Triggering instants for the power system with $\omega(t) = 0$. (b) Triggering instants for the power system with $\omega(t) \neq 0$.

estimator for the power system. Then a hybrid dynamic ETM is proposed, which regularizes a strictly positive triggering interval by a timer variable and thus exclude the Zeno behavior. In the presence of DoS attacks, a novel hybrid system model is established to describe the closed-loop power system with flow dynamics and jump dynamics. Based on a hybrid system approach, a sufficient stability condition is proposed for the LFC of power system, which explicitly illustrate the allowable DoS-range that the power system can tolerant. Besides, the allowable range is maximized using the resetting property of estimated states. Finally, an illustrative example is given to verify the proposed results. Future work may concern decentralized LFC for multiarea power systems.

REFERENCES

[1] L. Xie *et al.*, "Wind integration in power systems: Operational challenges and possible solutions," *Proc. IEEE*, vol. 99, no. 1, pp. 214–232, Jan. 2011.

[2] T. Liu, D. J. Hill, and C. Zhang, "Non-disruptive load-side control for frequency regulation in power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2142–2153, Jul. 2016.

[3] H. Huang and F. Li, "Sensitivity analysis of load-damping characteristic in power system frequency regulation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1324–1335, May 2013.

[4] S. Mukherjee, S. Teleke, and V. Bandaru, "Frequency response and dynamic power balancing in wind and solar generation," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2011, pp. 1–5.

[5] P. M. Anderson and M. Mirheydar, "An adaptive method for setting underfrequency load shedding relays," *IEEE Trans. Power Syst.*, vol. 7, no. 2, pp. 647–655, May 1992.

[6] A. Ulbig, T. S. Borsche, and G. Andersson, "Impact of low rotational inertia on power system stability and operation," in *Proc. IFAC World Congr.*, 2014, pp. 7290–7297.

[7] H. Chen, R. Ye, X. Wang, and R. Lu, "Cooperative control of power system load and frequency by using differential games," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 3, pp. 882–897, May 2015.

[8] C. Hua and Y. Wang, "Delay-dependent stability for load frequency control system via linear operator inequality," *IEEE Trans. Cybern.*, early access, Dec. 14, 2020, doi: 10.1109/TCYB.2020.3037113.

[9] Y. Mi, Y. Fu, C. Wang, and P. Wang, "Decentralized sliding mode load frequency control for multi-area power systems," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4301–4309, Nov. 2013.

[10] C. Mu, Y. Tang, and H. He, "Improved sliding mode design for load frequency control of power system integrated an adaptive learning strategy," *IEEE Trans. Ind. Electron.*, vol. 64, no. 8, pp. 6742–6751, Aug. 2017.

[11] M. Yilmaz and P. T. Krein, "Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces," *IEEE Trans. Power Electron.*, vol. 28, no. 12, pp. 5673–5689, Dec. 2013.

[12] T. N. Pham, S. Nahavandi, L. V. Hien, H. Trinh, and K. P. Wong, "Static output feedback frequency stabilization of time-delay power systems with coordinated electric vehicles state of charge control," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3862–3874, Sep. 2017.

[13] Y. Ota, H. Taniguchi, T. Nakajima, K. M. Liyanage, J. Baba, and A. Yokoyama, "Autonomous distributed V2G (vehicle-to-grid) satisfying scheduled charging," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 559–564, Mar. 2012.

[14] S. Izadkhast, P. Garcia-Gonzalez, and P. Frias, "An aggregate model of plug-in electric vehicles for primary frequency control," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1475–1482, May 2015.

[15] H. Liu, Z. Hu, Y. Song, J. Wang, and X. Xie, "Vehicle-to-grid control for supplementary frequency regulation considering charging demands," *IEEE Trans. Power Syst.*, vol. 30, no. 6, pp. 3110–3119, Nov. 2015.

[16] T. N. Pham, H. Trinh, and L. V. Hien, "Load frequency control of power systems with electric vehicles and diverse transmission links using distributed functional observers," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 238–252, Jan. 2016.

[17] Z. Zhang, Y. Mishra, D. Yue, C. Dou, B. Zhang, and Y.-C. Tian, "Delay-tolerant predictive power compensation control for photovoltaic voltage regulation," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4545–4554, Jul. 2021.

[18] J.-W. Zhu, C.-Y. Gu, S. X. Ding, W.-A. Zhang, X. Wang, and L. Yu, "A new observer-based cooperative fault-tolerant tracking control method with application to networked multiaxis motion control system," *IEEE Trans. Ind. Electron.*, vol. 68, no. 8, pp. 7422–7432, Aug. 2021.

[19] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019.

[20] C. D. Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[21] S. Feng and P. Tesi, "Networked control systems under denial-of-service: Co-located vs. remote architectures," *Syst. Control Lett.*, vol. 108, pp. 40–47, Oct. 2017.

[22] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, May 2017.

[23] A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channeds under denial of service," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1813–1820, Jun. 2018.

[24] X. Wang, J. H. Park, H. Liu, and X. Zhang, "Cooperative output-feedback secure control of distributed linear cyber-physical systems resist intermittent dos attacks," *IEEE Trans. Cybern.*, vol. 51, no. 10, pp. 4924–4933, Oct. 2021, doi: 10.1109/TCYB.2020.3034374.

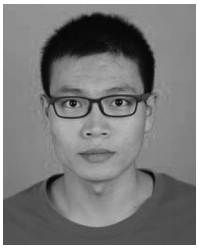
[25] G. Liu, C. Hua, P. X. Liu, H. Xu, and X. Guan, "Stabilization and data-rate condition for stability of networked control systems with denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 52, no. 1, pp. 700–711, Jan. 2022.

[26] D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson, "Distributed event-triggered control for multi-agent systems," *IEEE Trans. Autom. Control*, vol. 57, no. 5, pp. 1291–1297, May 2012.

[27] Y. Li, L. Liu, C. Hua, and G. Feng, "Event-triggered/self-triggered leader-following control of stochastic nonlinear multiagent systems using high-gain method," *IEEE Trans. Cybern.*, vol. 51, no. 6, pp. 2969–2978, Jun. 2021, doi: 10.1109/TCYB.2019.2936413.

[28] B. Zhang, C. Dou, D. Yue, Z. Zhang, and T. Zhang, "A packet loss-dependent event-triggered cyber-physical cooperative control strategy for islanded microgrid," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 267–282, Jan. 2021.

[29] A. Girard, "Dynamic triggering mechanisms for event-triggered control," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1992–1997, Jul. 2015.
[30] G. Zhao, C. Hua, and X. Guan, "Reset observer-based zeno-free dynamic event-triggered control approach to consensus of multiagent systems with disturbances," *IEEE Trans. Cybern.*, early access, Jul. 13, 2020, doi: 10.1109/TCYB.2020.3003330.
[31] G. Zhao and C. Hua, "A hybrid dynamic event-triggered approach to consensus of multi-agent systems with external disturbances," *IEEE Trans. Autom. Control*, vol. 66, no. 7, pp. 3213–3220, Jul. 2021, doi: 10.1109/TAC.2020.3018437.
[32] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 93–105, Mar. 2017.
[33] C. Peng, J. Zhang, and H. Yan, "Adaptive event-triggering load frequency H_∞ control for network-based power systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 2, pp. 1685–1694, Feb. 2018.
[34] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 1936–1947, Aug. 2017.
[35] 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.*, vol. 49, no. 12, pp. 4271–4282, Dec. 2019.
[36] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1665–1678, Aug. 2019.
[37] S. Hu, D. Yue, Q.-L. Han, X. Xie, X. Chen, and C. Dou, "Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1952–1964, May 2020.
[38] A.-Y. Lu and G.-H. Yang, "Observer-based control for cyber-physical systems under denial-of-service with a decentralized event-triggered scheme," *IEEE Trans. Cybern.*, vol. 50, no. 12, pp. 4886–4895, Dec. 2020.
[39] E. Tian and C. Peng, "Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4610–4618, Nov. 2020.
[40] C. Brosilow and B. Joseph, *Techniques of Model-Based Control*. Upper Saddle River, NJ, USA: Prentice Hall Prof., 2002.
[41] L. A. Montestruque and P. J. Antsaklis, "On the model-based control of networked systems," *Automatica*, vol. 39, no. 10, pp. 1837–1843, 2003.
[42] E. Garcia and P. J. Antsaklis, "Model-based event-triggered control for systems with quantization and time-varying network delays," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 422–434, Feb. 2013.
[43] K.-Z. Liu, A. R. Teel, X.-M. Sun, and X.-F. Wang, "Model-based dynamic event-triggered control for systems with uncertainty: A hybrid system approach," *IEEE Trans. Autom. Control*, vol. 66, no. 1, pp. 444–451, Jan. 2021.
[44] V. S. Dolk, D. P. Borgers, and W. P. M. H. Heemels, "Output-based and decentralized dynamic event-triggered control with guaranteed $\mathcal{L}_p$-gain performance and zeno-freeness," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 34–49, Jan. 2017.
[45] D. Carnevale, A. R. Teel, and D. Nesic, "A Lyapunov proof of an improved maximum allowable transfer interval for networked control systems," *IEEE Trans. Autom. Control*, vol. 52, no. 5, pp. 892–897, May 2007.



Guopin Liu received the B.Sc. and Ph.D. degrees from Yanshan University, Qinhuangdao, China, in June 2014 and January 2020, respectively.

From 2018 to 2019, he was a Visiting Researcher with the Faculty of Science and Engineering, University of Groningen, Groningen, The Netherlands. From 2020 to 2021, he worked as a Postdoctoral Fellow with Yeungnam University, Gyeongsan, South Korea. He is currently a Lecturer with Yanshan University. His research interests include nonlinear switched systems and networked control systems.

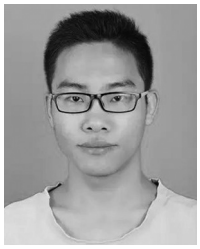
Ju H. Park (Senior Member, IEEE) received the Ph.D. degree in electronics and electrical engineering from the Pohang University of Science and Technology (POSTECH), Pohang, Republic of Korea, in 1997.

From May 1997 to February 2000, he was a Research Associate with the Engineering Research Center-Automation Research Center, POSTECH. He joined Yeungnam University, Gyeongsan, Republic of Korea, in March 2000, where he is currently the Chuma Chair Professor. He is a coauthor of the monographs *Recent Advances in Control and Filtering of Dynamic Systems With Constrained Signals* (New York, NY, USA: Springer-Nature, 2018) and *Dynamic Systems With Time Delays: Stability and Control* (New York, NY, USA: Springer-Nature, 2019) and is an Editor of an edited volume *Recent Advances in Control Problems of Dynamical Systems and Networks* (New York, NY, USA: Springer-Nature, 2020). His research interests include robust control and filtering, neural/complex networks, fuzzy systems, multiagent systems, and chaotic systems. He has published a number of articles in these areas.

Prof. Park has been a recipient of the Highly Cited Researchers Award by Clarivate Analytics (formerly, Thomson Reuters) since 2015 and listed in three fields, Engineering, Computer Sciences, and Mathematics, in 2019, 2020, and 2021. He also serves as an Editor for the *International Journal of Control, Automation and Systems*. He is also a Subject Editor/Advisory Editor/Associate Editor/Editorial Board Member of several international journals, including *IET Control Theory & Applications*, *Applied Mathematics and Computation*, *Journal of The Franklin Institute*, *Nonlinear Dynamics*, *Engineering Reports*, *Cogent Engineering*, the IEEE TRANSACTION ON FUZZY SYSTEMS, the IEEE TRANSACTION ON NEURAL NETWORKS AND LEARNING SYSTEMS, and the IEEE TRANSACTION ON CYBERNETICS. He is a Fellow of the Korean Academy of Science and Technology.

Changchun Hua (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Yanshan University, Qinhuangdao, China, in 2005.

He was a Research Fellow with the National University of Singapore, Singapore, from 2006 to 2007. From 2007 to 2009, he was with Carleton University, Ottawa, ON, Canada, funded by the Province of Ontario Ministry of Research and Innovation Program. From 2009 to 2010, he was with the University of Duisburg–Essen, Essen, Germany, funded by the Alexander von Humboldt Foundation. He is currently a Full Professor with Yanshan University. He has authored or coauthored over 80 papers in mathematical, technical journals, and conferences. He has been involved in over ten projects supported by the National Natural Science Foundation of China, the National Education Committee Foundation of China, and other important foundations. His current research interests include nonlinear control systems, control systems design over network, teleoperation systems, and intelligent control.



Yafeng Li received the B.S. degree from the Hebei University of Science and Technology, Shijiazhuang, China, in June 2013, and the Ph.D. degree from Yanshan University, Qinhuangdao, China, in January 2019.

He worked as a Research Associate with the City University of Hong Kong, Hong Kong, in 2018 and as a Postdoctoral Fellow with Yeungnam University, Gyeongsan, South Korea, from March 2019 to February 2020. He is currently a Humboldt Fellow with the University of Duisburg–Essen, Duisburg, Germany. His current research interests include nonlinear system control, multiagent systems, adaptive control, and fault-tolerant control.