Event-Based Security Control for State-Dependent Uncertain Systems Under Hybrid-Attacks and Its Application to Electronic Circuits

Jinliang Liu, Meng Yang, Engang Tian, Jie Cao, and Shumin Fei

***Abstract*— This paper investigates the problem of event-based security control for state-dependent uncertain systems under hybrid-attacks. An event-triggered scheme is adopted to mitigate the communication burden, where the sampled data are delivered only when the predefined triggering condition is violated. Meanwhile, a new hybrid-attacks model, which contains denial-of-service attacks and replay attacks, is established to describe the randomly occurring cyber-attacks. By taking hybrid-attacks into account, a novel mathematical model for state-dependent uncertain systems with event-triggered scheme is established. Then, through employing Lyapunov–Krasocskii stability theory and linear matrix inequality techniques, sufficient conditions ensuring the state-dependent uncertain systems being exponentially mean-square stable are deduced. Based on the derived sufficient conditions, the desired output feedback controller gain is obtained. Finally, the feasibility of the proposed method is demonstrated by a numerical example, and the applicability of the developed theoretical results is also illustrated by the controller design for electronic circuits.**

***Index Terms*— Electronic circuits, state-dependent uncertain system, event-triggered scheme, hybrid-attacks.**

I. Introduction

STATE-DEPENDENT uncertain systems are often encountered due to the unavoidable environmental changes, component failures, torn-and-worn factors, etc [1]–[4]. During the last decades, state-dependent uncertain systems have exhibited widely industrial applications such as aerospace, automobile, electronic circuit and so on. In order to achieve perfect system performance, the researchers hope to establish system models which closely match real-world dynamics. Among various modeling methods, the polytope-type model is recognized to be feasible in describing the parameter uncertainty [5]. For example, the authors in [6] investigated the uncertain systems with state-dependent uncertainties which are applied in the electronic circuits. In [7], a class of network-based state-dependent uncertain systems are studied with the consideration of event-triggered robust filtering problem. The goal of this note will apply the polytope-type model to investigate the control of state-dependent systems subject to cyber-attacks.

In the past few years, many researchers focus on how to deal with the constraints of limited energy resource and network-bandwidth in networked control systems. Many outstanding results can be available in the literature [8]–[13]. Compared with the time triggered transmission method, event-triggered transmission scheme is more popular with researchers because of its advantages in reducing network communication and guaranteeing the desired system performance. For example, the periodic event-triggered scheme was proposed in [14]. In [15], a novel event-triggered control law was proposed and the problem of synchronization of switched delayed neural network was discussed. The decentralized event-triggered filtering for networked nonlinear interconnected system was studied in [16]. Aperiodic sampled-data control was investigated in [17] for fuzzy systems with event-triggered method. Tremendous attention has been attracted on designing various event-triggered schemes [18]–[21]. However, among the existed publications, little effort has been devoted to the event-triggered control method while the addressed system is subject to cyber-attacks. This is the first motivation of this paper.

Actually, due to the openness of network and the defects of system design, networked control systems are unavoidably influenced by more and more attacks. Thus, it is necessary to analyze the performance of networked control systems when it comes to the security issue [22]–[24]. In general, the most common types of cyber-attacks include denial-of-service (DoS) attacks, deception attacks and replay attacks, etc [25]. In DoS attacks, the attackers aim to block the communication channels from transmitting some significant information. In deception attacks, the attackers intentionally

Manuscript received April 1, 2019; revised July 2, 2019; accepted July 4, 2019. Date of publication August 27, 2019; date of current version December 6, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61973152 and Grant 61903182, in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20171481, in part by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 19KJA510005 and Grant 18KJB120002, in part by the Postgraduate Research Practice Innovation Program of Jiangsu Province of China under Grant KYCX18_1439, and in part by the Qing Lan Project. This article was recommended by Associate Editor G. Russo. *(Corresponding author: Jie Cao.)*

J. Liu is with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China, and also with the College of Automation Electronic Engineering, Qingdao University of Science and Technology, Qingdao 266061, China (e-mail: liujinliang@vip.163.com).

M. Yang and J. Cao are with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: mengyang9505@163.com; caojie690929@163.com).

E. Tian is with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: tianengang@163.com).

S. Fei is with the School of Automation, Southeast University, Nanjing 210096, China (e-mail: smfei@seu.edu.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2019.2930572

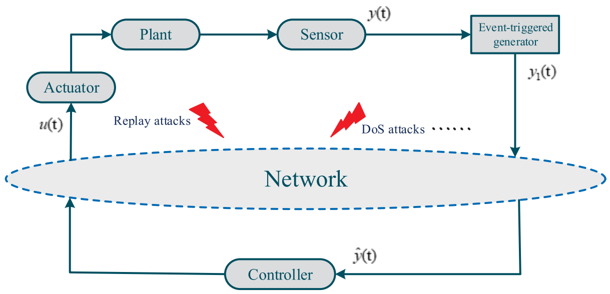

Fig. 1. The structure of event-based security control for networked control system with hybrid-attacks.

send incorrect sensor measurements or control packets to the operator. In a replay attack [26], the attackers record a sequence of transmitted data and the sequence will be repeated afterwards. Recognizing the threatens of the above cyber-attacks, researchers have devoted much attention in proposing secure resilient control methods against malicious cyber-attacks [27]–[30]. For example, in [31], the authors discussed the state estimation for cyber-physical systems with the consideration of sensor saturation and DoS attacks. The authors in [26] investigated the secure Kalman fusion estimation problem for cyber-physical systems with bandwidth constraints and replay attacks. However, secure control for state-dependent uncertain systems has not received enough attention, which motivates this work.

The rest of this paper is organized as follows: In Section II, the model for networked uncertain systems with state-dependent uncertainties and hybrid-attacks is constructed. Section III presents the main results concerning the sufficient conditions for networked state-dependent uncertain systems. In Section IV, two practical examples are utilized to show the usefulness and applicability of designed method.

Notation: $\mathbb{N}$ is the set of all non-negative integers and $\mathbb{R}^n$ denotes the n-dimensional Euclidean space; the T is matrix transposition; I stands for the identity matrix of appropriate dimension; $X > 0 (X \geq 0)$ indicates that the matrix X is real symmetric positive definite (positive semi-definite). For symmetric matrix $\begin{bmatrix} A & * \\ B & C \end{bmatrix}$ with a matrix B and two symmetric matrices A, C, $*$ is the entries implied by symmetry.

II. System Description

A. Model Description

This paper is concerned with the event-based security control for networked control system under hybrid-attacks. As shown in Fig.1, the sampled signals are delivered to controller through event-triggered scheme and the network. It is assumed that the sampled signals are sifted by an event generator before it transmits to the unreliable communication network. On the other hand, the network may be subject to hybrid-attacks which contain two kinds of attacks: replay attack and DoS attacks. In particular, the packet dropouts induced by attacks occur in a certain random way when the data is sent to the controller through the communication network.

The model of continuous-time uncertain system can be expressed as follows:

$$\begin{cases} \dot{x}(t) = A(\sigma(x(t), \chi(t)))x(t) + B(\sigma(x(t), \chi(t)))u(t) \\ y(t) = C(\sigma(x(t), \chi(t)))x(t) \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^{n_x}$ denotes the state vector, $u(t) \in \mathbb{R}^{n_u}$ represents the control input, $y(t) \in \mathbb{R}^{n_y}$ is the measurement; $\sigma(x(t), \chi(t)) \in \mathbb{R}^{n_\sigma}$ denotes the uncertain parameter vector function, which contains the common time-varying parameters $\chi(t) \in \mathbb{R}^{n_\chi}$ and the state-dependent parametric perturbations with components $\sigma_i\left(x^i(t), \chi^i(t)\right) \in \mathbb{R}^{n_\sigma}$. Moreover, $\sigma(x(t), \chi(t))$ belongs to the following set

$$\mathbb{D} = \Big\{\sigma(x(t), \chi(t)) \mid \sum_{i=1}^{m} \sigma_i\left(x^i(t), \chi^i(t)\right) = 1, \\ \sigma_i\left(x^i(t), \chi^i(t)\right) \geq 0, i \in J_m = \{1, 2, \ldots, m\}\Big\} \tag{2}$$

where $\chi^i(t)$ is a vector whose entries are the elements of $\chi(t)$ and the entries of vector $x^i(t)$ are the elements of $x(t)$. Consequently, $A(\sigma(x(t), \chi(t)))$, $B(\sigma(x(t), \chi(t)))$ and $C(\sigma(x(t), \chi(t)))$ are system matrices and belong to the following convex polytopic set:

$$\mathbb{X} = \Big\{X(\sigma(x(t), \chi(t))) \mid X(\sigma(x(t), \chi(t))) \\ = \sum_{i=1}^{m} \sigma_i\left(x^i(t), \chi^i(t)\right) X_i, X_i \in \{A_i, B_i, C_i\}\Big\} \tag{3}$$

where $\sigma(x(t), \chi(t)) \in \mathbb{D}$; A_i, B_i and C_i $(i \in J_m)$ denote vertices of the corresponding uncertainty polytope, and all are known constant real matrices with appropriate dimensions.

Thus, any system in the form of (1) can be represented as follows:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{m} \sigma_i\left(x^i(t), \chi^i(t)\right)[A_i x(t) + B_i u(t)] \\ y(t) = \sum_{i=1}^{m} \sigma_i\left(x^i(t), \chi^i(t)\right)[C_i x(t)] \end{cases} \tag{4}$$

The purpose of this paper is to design the following output feedback controller:

$$u(t) = K\hat{y}(t) \tag{5}$$

where K and $\hat{y}(t)$ denote the controller gain to be designed and the real input of controller, respectively.

Remark 1: The state-dependent models have aroused wide interest because of its applications in various fields, for instance, spring damping systems, tunnel diode electronic circuit systems, Chuas circuits, mechanical systems [32]–[34]. Compare with previous state-dependent models which only contain the state-dependent polytopic uncertainties, the model (1) involves general uncertain time-varying parameters. In this paper, an event-based security controller design problem of the state-dependent uncertain system is investigated under the consideration of hybrid-attacks.

B. Design of Event-Triggered Scheme

For the purpose of saving the limited resources and decreasing the pressure of network bandwidth, an event-triggered scheme is introduced in this paper, which is a high effective strategy based on event protocol to sift out the sampled data. As shown in Fig.1, the event generator is employed between the sensor and the controller. Under the action of the event generator, assume that $t_k h$ denotes the latest transmission instant, and the next transmission instant $t_{k+1}h$ can be regarded as follows:

$$t_{k+1}h = t_k h + \inf_{j\in\mathbb{N}} \Big\{ jh | e_k(t_k h)^T \Omega e_k(t_k h) > \varrho^2 y(t_k h + jh)^T \Omega y(t_k h + jh) \Big\} \quad (6)$$

where h represents the sample period, $j = 1, 2, \ldots, J$, $J = t_{k+1} - t_k - 1$, $\Omega > 0$ is a positive definite matrix, $\varrho \in [0, 1)$ denotes a threshold coefficient and

$$e_k(t_k h) = y(t_k h) - y(t_k h + jh) \quad (7)$$

where $y(t_k h)$ denotes the latest transmitted data and $y(t_k h + jh)$ is the current sampling data.

Then, the sampled signals are transmitted to the communication network only when the following event-triggered condition is satisfied [14]:

$$e_k^T(t_k h)\Omega e_k(t_k h) > \varrho^2 y^T(t_k h + jh)\,\Omega y(t_k h + jh) \quad (8)$$

C. Hybrid-Attacks Model

Due to the openness of the network and the complexity of network environment, the threats of cyber-attacks can no longer be neglected. For simplicity of analysis, consider that a newer type of hybrid-attacks can damage the normal transmission of data between the sensor to the controller, and the controller to the actuator. As shown in Fig.1, the new hybrid-attacks model is proposed which includes the replay attacks and DoS attacks. Under the hybrid-attacks model, assume that the replay attacks occur in a random manner, and the length and frequency of DoS attacks are limited.

When the released data is transmitted to network, we will begin by considering the replay attacks. In this paper, the intercepted transmission signals will replace the normal transmission data if the network is subject to replay attacks. Then, inspired by [35], the real transmitted data under replay attacks can be expressed as follows

$$y_2(t) = \alpha(t) y_r(t) + (1 - \alpha(t))\, y_1(t) \quad (9)$$

where $\alpha(t)$ is a Bernouli variable with $\alpha(t) \in [0, 1]$, $\bar{\alpha}$ stands for the expectation of $\alpha(t)$, $y_r(t) = y_1(t_r)$, $y_1(t_r)$ is used to represent the replay signals at time instant t_r, and $y_1(t)$ is the signal via the designed event-triggered scheme.

Moreover, by taking the influence of DoS attacks into consideration, the attacker has the limited energy to block the communication channels in an active-period. Specifically, the time interval $\mathcal{H}_n$ of n_{th} DoS attacks is defined as follows

$$\mathcal{H}_n = \big[\hbar_n + L_n, \hbar_{n+1}\big) \quad (10)$$

where $\{\hbar_n\}_{n\in\mathbb{N}}$ is the sequence of the DoS attacks, $\hbar_0$ represents the start interval of attackers, $L_n > 0$ is the length of n_{th} period when the jammer is sleeping and one has $(\hbar_n + L_n) < \hbar_{n+1}$.

Inspired by [36] and [37], given $t \in \mathbb{R}$, $\tau \in \mathbb{R}$, for each interval $[\tau, t]$, let

$$\Phi_a(\tau, t) = \bigcup_{n\in\mathbb{N}} \mathcal{H}_n \bigcap [\tau, t] \quad (11)$$

$$\Phi_s(\tau, t) = [\tau, t] \backslash \Phi_s(\tau, t) \quad (12)$$

where $\Phi_a(\tau, t)$ represents the set of time instant for rejecting communication in each interval $[\tau, t]$, the communication is normal in the set of time instant $\Phi_s(\tau, t)$ for each interval $[\tau, t]$, and $\Phi_s(\tau, t) = \{\bar{t} | \bar{t} \in [\tau, t], \bar{t} \notin \Phi_a(\tau, t)\}$.

To be more precise, we introduce the following assumptions, which will be helpful to discuss DoS attacks.

Assumption 1 (DoS Attacks Frequency) [36]: For any $0 < \tau < t$, assume that $n(t)$ is the total number of DoS attacks occurring over interval $[\tau, t)$. There exist a_1, $\tau_d \in \mathbb{R}$, the DoS attacks frequency over $[\tau, t)$ satisfies

$$n(t) \le a_1 + \frac{t - \tau}{\tau_d} \quad (13)$$

for all τ, $t \in \mathbb{R}$.

Assumption 2 (DoS Duration) [37]: Suppose that a unified lower bound $L_{\min}$ denotes the lengths of the periods while communication is normal, and a unified upper bound $b_{\max}$ represents the lengths of the periods while communication is interrupted, then the $L_{\min}$ and $b_{\max}$ satisfy

$$\begin{cases} L_{\min} \ge \inf_{n\in\mathbb{N}}\{L_n\} \\ b_{\max} \ge \sup_{n\in\mathbb{N}}\{\hbar_n - \hbar_{n-1} - L_n\} \end{cases} \quad (14)$$

Remark 2: In practical applications, networked control system is vulnerable to various kinds of attacks resulting from the fragility of network. To the best of the authors knowledge, there are few studies about the impact of two or more kinds of cyber-attacks on the system. In view of this, the main purpose of the present paper is to design and investigate a kind of hybrid-attacks which include the replay attacks and the DoS attacks.

Remark 3: According to the equality (9), a Bernoulli distribution $\alpha(t)$ is introduced to show the randomness of replay attacks. When $\alpha(t) = 1$, the previous released signals will replace the normal signals transmission. That is, the equality (9) can be rewritten as $y_2(t) = y_1(t_r)$ where $y_1(t_r)$ denotes the replay signals chosen by attacker at instant t. Otherwise, when $\alpha(t) = 0$, the released signals are transmitted via the communication network without replay attacks.

Remark 4: Different from some existing replay attack models (see [38]), the replay attack model (9) is applied to a certain instant rather than to a certain time interval. That is to say, suppose the attacker only selects one of the captured signals as the malicious signal at a time.

Furthermore, both kinds of attack can occur stochastically. To reflect such a realistic situation, the real input of output feedback controller is described as follows:

$$\hat{y}(t) = \triangle(t) y_2(t) = \triangle(t)\,[\alpha(t) y_r(t) + (1 - \alpha(t))\, y_1(t)] \quad (15)$$

where $\triangle(t)$ denotes the signal for DoS attack occurrence and

$$\triangle(t) = \begin{cases} 1, & t \in [\hbar_n, \hbar_n + L_n) \\ 0, & t \in [\hbar_n + L_n, \hbar_{n+1}). \end{cases}$$

Remark 5: From (15), we can get the following three special cases by selecting the different values of $\alpha(t)$: (I) the networked control systems suffer from the DoS attacks when $\Delta(t) = 0$ and the controller cannot receive the transmitted signals; (II) the networked control systems are subject to the replay attacks when $\Delta(t) = 1$ and $\alpha(t) = 1$; (III) the event-trigger generator measurements are transmitted normally when $\Delta(t) = 1$ and $\alpha(t) = 0$. Moreover, it should be pointed out that case I can reflect the packet dropouts phenomenon and case II represents the time delays. In other words, the designed hybrid-attacks model regards packet dropouts and time delays as its special cases.

D. Event-Based Controller Design

Because of the action of the non-periodic DoS attacks, the event-triggered scheme (8) is not suitable, so the transmission scheme need to be modified. On the basis of the above conditions and considering the impact of DoS attacks, the event-triggering instant can be expressed as

$$t_k^n h = \left\{ t_{k_j} h \text{ satisfying (8)} \mid t_{k_j} h \in \Phi_s(0, t) \right\} \cup \{\hbar_n\} \quad (16)$$

where $n,\ j,\ t_{k_j} h,\ k_j \in \mathbb{N}$, k represents the sets of triggering times in the nth DoS period, $\mathcal{K}^n = \{1, 2, \ldots, k(n)\}$, $k \in \mathcal{K}^n$ with $n \in \mathbb{N}$ and

$$k(n) = \sup\{k \in \mathbb{N} \mid (\hbar_{n-1} + L_{n-1}) \geq t_k^n h\}$$

Similar to [37], let

$$\Upsilon_s(0, t) = \cup_{k=0}^{k(n)} \left\{ \Phi_s(0, t) \cap \mathcal{M}_k^n \right\} \quad (17)$$

where $\lambda_k^n = \sup\left\{ j \in \mathbb{N} \mid t_k^{n+1} h + jh < t_{k+1}^{n+1} h \right\}$, $\mathcal{M}_k^n = \cup_{j=1}^{\lambda_k^n} [t_k^{n+1} h + (j-1)h, t_k^{n+1} h + jh) \cup \left[t_k^{n+1} h + \lambda_k^n h, t_{k+1}^{n+1} h \right)$.

Then, the interval $\Upsilon_s(0, t)$ can be rewritten as

$$\Upsilon_s(0, t) = \cup_{k=0}^{k(n)} \cup_{j=1}^{\lambda_k^n + 1} \left\{ \Phi_s(0, t) \cap [t_k^{n+1} h + (j-1)h, t_k^{n+1} h + jh) \right\} \quad (18)$$

Define

$$\tau_k^n(t) = t - t_k^{n+1} h - \lambda_k^n h \quad (19)$$

$$e_k^n(t) = x\left(t_k^{n+1} h\right) - x\left(t_k^{n+1} h + \lambda_k^n h\right) \quad (20)$$

with $t \in \Upsilon_s(0, t) \cap [t_k^{n+1} h + \lambda_k^n h, t_{k+1}^{n+1} h)$.

Combine the inequality (8) and the definition of $\tau_k^n(t)$ and $e_k^n(t)$, the event-triggered condition can be derived as

$$\left(e_k^n(t)\right)^T \Omega e_k^n(t) > \varrho^2 y^T \left(t - \tau_k^n(t)\right) \Omega y \left(t - \tau_k^n(t)\right) \quad (21)$$

The successful signal $y_1(t_k^n h)$ via event-triggered scheme can be expressed as

$$y_1(t) = y\left(t - \tau_k^n(t)\right) + e_k^n(t), t \in \bar{\Phi}_s(0, t) \quad (22)$$

where $\bar{\Phi}_s(0, t) = \Upsilon_s(0, t) \cap \mathcal{M}_k^n$, $k \in \mathcal{K}^n$.

Recalling (5), (15), (22) and $y_r(t) = y_1(t_r)$, the real control input $u(t)$ under hybrid-attacks can be represented as

$$u(t) = \begin{cases} \alpha(t) K \left[e_k^n(t_r) + y\left(t_r - \tau_k^n(t_r)\right)\right] + (1- \\ \alpha(t))\, K \left[e_k^n(t) + y\left(t - \tau_k^n(t)\right)\right], \quad t \in \bar{\Phi}_s(0, t) \\ 0, t \in \Phi_a(0, t) \end{cases} \quad (23)$$

By combining (4) and (23), the output feedback control system can be expressed as

$$\begin{cases} \dot{x}(t) = \begin{cases} \displaystyle\sum_{i=1}^m \sum_{j=1}^m \sigma_i \hat{\sigma}_j \Big\{ A_i x(t) + B_i K \big[\alpha(t) y_r(t) \\ \quad + (1 - \alpha(t))(e_k^n(t) + C_j x\left(t - \tau_k^n(t)\right)) \big] \Big\} \\ t \in \bar{\Phi}_s(0, t) \\ \displaystyle\sum_{i=1}^m \sigma_i \left[A_i x(t) \right], \quad t \in \Phi_a(0, t) \end{cases} \\ x(t) = \phi(t), \quad t \in [-h, 0] \end{cases} \quad (24)$$

where $\sigma_i = \sigma_i\left(x^i(t), \chi^i(t)\right)$, $\hat{\sigma}_j = \hat{\sigma}_j(x^j(t - \tau_k^n(t)), \chi^j(t - \tau_k^n(t)))$ and $\phi(t)$ is the initial condition of the state $x(t)$.

Remark 6: By taking the influence of hybrid-attacks into consideration, sufficient conditions are derived to co-design both security output feedback controller and event-triggered scheme for state-dependent uncertain systems. To the best of the authors knowledge, the event-based security output feedback controller design for the state-dependent uncertain systems with hybrid-attacks is firstly investigated in this paper.

The following definition and lemmas are proposed which will be helpful to develop the main results.

Definition 1 [39]: For given scalars $a \geq 0$ and $b > 0$, if the following inequality (25) holds, the zero solution of (24) is considered to be exponentially mean-square stable (EMS-stability) with the initial functions ϕ.

$$a e^{-bt} \|\phi\|^2 \geq \mathbb{E}\left[\|x(t)\|^2 | \phi \right], \quad \forall t \geq 0 \quad (25)$$

Lemma 1 [40] (Jensen s Inequality): Assume a function $\tau(t)$ is subject to the interval $[0, \bar{\tau}]$ and vector $\dot{x} : [0, \bar{\tau}] \to \mathbb{R}$. For any matrix $R \in \mathbb{R}^{n \times n}$ and $V \in \mathbb{R}^{n \times n}$ satisfying $\begin{bmatrix} R & * \\ V & R \end{bmatrix} > 0$, the following inequality holds:

$$-\int_{t-\bar{\tau}}^{t} \dot{x}^T(s) R \dot{x}(s) ds \leq \frac{1}{\bar{\tau}} \mathbb{C}^T(t) \Theta \mathbb{C}(t) \quad (26)$$

where

$$\mathbb{C} = \begin{bmatrix} x(t) \\ x(t - \tau(t)) \\ x(t - \bar{\tau}) \end{bmatrix}, \quad \Theta = \begin{bmatrix} -R & * & * \\ R - V & -2R + V + V^T & * \\ V & R - V & -R \end{bmatrix}$$

Lemma 2 [41]: Let $H = L\digamma V^T$ be a singular value decomposition of matrix with full column rank, where L and V represent the orthogonal matrices, and $\digamma$ denotes an $m \times n$ rectangular diagonal matrix with positive real numbers on the diagonal in decreasing order of magnitude. Suppose that $S \in n \times n$ is a symmetric matrix. Then, there exists a matrix $X \in m \times m$ such that $SH = HX$ if and only if the following equality holds

$$S = L \begin{bmatrix} \Delta_1 & * \\ 0 & \Delta_2 \end{bmatrix} L^T$$

where $\Delta_1 \in \mathbb{R}^{m\times m}$, $\Delta_2 \in \mathbb{R}^{m\times(n-m)}$.

III. Main Results

In this section, by resorting to Lyapunov-Krasocskii stability theory and linear matrix inequality techniques, the sufficient conditions can be established which ensure the system (24) is EMS-stability. The main results are shown in the following theorem.

Theorem 1: For given positive parameters ρ_i, γ_s, $\psi_s(s = 1, 2)$, $\bar{\alpha}$, μ, sampling period h, trigger parameter ϱ, matrix K, DoS parameters a_1, ω_d, $L_{\min}$, $b_{\max}$, the system (24) is EMS-stability if there exist matrices $P_s > 0$, $Q_{sk} > 0$, $R_{sk} > 0$, $Z_{sk} > 0$, $\Omega > 0$, $M_i^s > 0$, U_{sk} and $V_{sk}(s = 1, 2)$ with appropriate dimensions, such that for any $i, j, k \in J_m$, the following inequalities hold with $\hat{\sigma}_j - \rho_j\sigma_j \geq 0$

$$\Pi_{ijk}^s - M_i^s < 0 \quad (27)$$

$$\rho_i\Pi_{iik}^s - \rho_i M_i^s + M_i^s < 0 \quad (28)$$

$$\rho_j\Pi_{ijk}^s + \rho_i\Pi_{jik}^s - \rho_j M_i^s - \rho_i M_j^s + M_i^s + M_j^s < 0 \quad (i < j) \quad (29)$$

$$P_1 \leq \psi_2 P_2, \quad P_2 \leq \psi_1 e^{2(\gamma_1+\gamma_2)h} P_1 \quad (30)$$

$$Q_{sk} \leq \psi_{3-s} Q_{(3-s)k}, \quad R_{sk} \leq \psi_{3-s} R_{(3-s)k}$$
$$Z_{sk} \leq \psi_{3-s} Z_{(3-s)k}, \quad \varpi > 0 \quad (31)$$

$$\begin{bmatrix} R_{sk} & * \\ V_{sk} & R_{sk} \end{bmatrix} \geq 0, \quad \begin{bmatrix} Z_{sk} & * \\ U_{sk} & Z_{sk} \end{bmatrix} \geq 0 \quad (32)$$

where the matrix Π_{ijk}^s is given in Appendix A.

Proof: See Appendix B. ■

In Theorem 1, sufficient conditions which can guarantee the EMS-stability of the state-dependent uncertain systems (24) have been obtained. Furthermore, on the basis of Theorem 1, the nonlinear terms will be treated in the following section and the desired controller gain will be given.

Theorem 2: For given positive parameters ρ_i, γ_s, ψ_s, e_{s1}, $e_{s2}(s = 1, 2)$, $\bar{\alpha}$, μ, sampling period h, trigger parameter ϱ, DoS parameters a_1, ω_d, $L_{\min}$, $b_{\max}$, the system (24) is EMS-stability if there exist matrices $P_s > 0$, Y, $Q_{sk} > 0$, $R_{sk} > 0$, $Z_{sk} > 0$, $\Omega > 0$, $M_i^s > 0$, U_{sk} and $V_{sk}(s = 1, 2)$ with appropriate dimensions, such that for any $i, j, k \in J_m$, the following linear matrix inequalities and conditions (30)-(32) hold with $\hat{\sigma}_j - \rho_j\sigma_j \geq 0$.

$$\bar{\Pi}_{ijk}^s - M_i^s < 0 \quad (33)$$

$$\rho_i\bar{\Pi}_{iik}^s - \rho_i M_i^s + M_i^s < 0 \quad (34)$$

$$\rho_j\bar{\Pi}_{ijk}^s + \rho_i\bar{\Pi}_{jik}^s - \rho_j M_i^s - \rho_i M_j^s + M_i^s + M_j^s < 0 \quad (i < j) \quad (35)$$

where the matrix $\bar{\Pi}_{ijk}^s$ is given in Appendix C.

Moreover, the output feedback controller gain for state-dependent uncertain systems can be given by

$$K = (B_i^T P_1 B_i)^{-1} B_i^T B_i Y \quad (36)$$

Proof: See Appendix D. ■

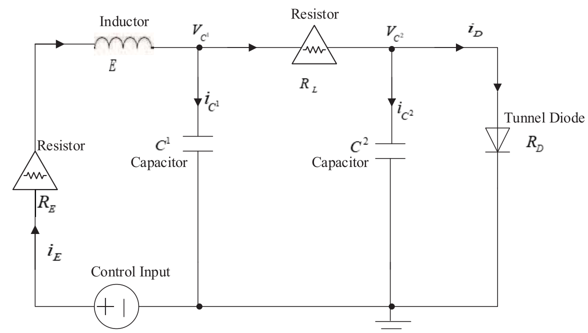

Fig. 2. The application circuit of tunnel diode.

IV. Simulation Examples

In this section, two practical engineering examples are utilized to illustrate the feasibility of designed output feedback control system in this paper.

Example 1: The mathematical model adopted in (1)-(4) can be applied to describe many practical applications. Considering the tunnel diode circuit system as shown in Fig.2, its characteristics are expressed by

$$\begin{cases} C^1\dfrac{dV_{C^1(t)}}{dt} = -\dfrac{V_{C^1(t)} - V_{C^2(t)}}{R_L} + i_E(t) \\ C^2\dfrac{dV_{C^2(t)}}{dt} = \dfrac{V_{C^1(t)} - V_{C^2(t)}}{R_L} - i_D(t) \\ E\dfrac{di_E(t)}{dt} = -V_{C_1(t)} - R_E i_E(t) + u(t) \end{cases}$$

where C^1, C^2 denote the capacitor, R_L, R_E are the linear resistance, E is inductor and R_D represents the impedance of tunnel diode.

In practice, R_D is time-varying uncertain which depends on V_D [6], and we suppose that $\frac{1}{R_D} = \frac{i_D(t)}{V_D(t)} = s_1 + s_2 V_D^2(t)$, where s_1, s_2 denote the known scalars. Select $x_1(t) = V_{C^1}(t)$, $x_2(t) = V_{C^2}(t)$, $x_3(t) = i_E(t)$ as the state variables, where $x_1(t) \in [m_1, m_2]$, $m_1 = \max\{m_1^2, m_2^2\}$, then the tunnel diode circuit can be governed by

$$\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \\ \dot{x}_3(t) \end{bmatrix} = \begin{bmatrix} -\dfrac{1}{R_L C^1} & \dfrac{1}{R_L C^1} & \dfrac{1}{C^1} \\ \dfrac{1}{R_L C^2} & -\dfrac{s_1 + s_2 x_1^2(t)}{C^2} - \dfrac{1}{R_L C^2} & 0 \\ -\dfrac{1}{E} & 0 & -\dfrac{R_E}{E} \end{bmatrix} \times \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \dfrac{1}{E} \end{bmatrix} u(t)$$

The above equations can be described in polytopic form as follows

$$\begin{cases} \dot{x}(t) = \displaystyle\sum_{i=1}^{2} \left(\sigma_i\left(x^i(t), \chi\right)\right)[A_i x(t) + B_i u(t)] \\ y(t) = \displaystyle\sum_{i=1}^{2} \left(\sigma_i\left(x^i(t), \chi\right)\right)[C_i x(t)] \end{cases}$$

where $\sigma_1\left(x^1(t),\chi\right) = \frac{x_1^2(t)}{m_1}$, $\sigma_2\left(x^2(t),\chi\right) = 1 - \frac{x_1^2(t)}{m_1}$ are the uncertain parameter vector, $x(t) = [x_1(t), x_2(t), x_3(t)]^T$, $y(t) = [V_{C^1}(t), V_{C^2}(t), i_E(t)]^T$ and the vertices $A_i(i = 1, 2)$ of corresponding uncertainty polytope can be given by

$$A_1 = \begin{bmatrix} -\frac{1}{R_L C^1} & \frac{1}{R_L C^1} & \frac{1}{C^1} \\ \frac{1}{R_L C^2} & -\frac{s_1 + s_2 m_1}{C^2} - \frac{1}{R_L C^2} & 0 \\ -\frac{1}{E} & 0 & -\frac{R_E}{E} \end{bmatrix}$$

$$A_2 = \begin{bmatrix} -\frac{1}{R_L C^1} & \frac{1}{R_L C^1} & \frac{1}{C^1} \\ \frac{1}{R_L C^2} & -\frac{s_1}{C^2} - \frac{1}{R_L C^2} & 0 \\ -\frac{1}{E} & 0 & -\frac{R_E}{E} \end{bmatrix}$$

$$B_1 = B_2 = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{E} \end{bmatrix}, \quad C_i = I$$

Then, the tunnel diode circuit system can be expressed in a polytopic form with the following parameters:

$$A_1 = \begin{bmatrix} -1 & 1 & 1 \\ 10 & -10.52 & 0 \\ -0.05 & 0 & 0 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} -1 & 1 & 1 \\ 10 & -10.02 & 0 \\ -0.05 & 0 & 0 \end{bmatrix}$$

$$B_1 = B_2 = \begin{bmatrix} 0 \\ 0 \\ 0.05 \end{bmatrix}, \quad C_i = I$$

where $s_1 = 0.002$, $s_2 = 0.01$, $C^1 = 1F$, $C^2 = 0.1F$, $E = 20H$, $R_E = 0\Omega$, $R_L = 1\Omega$ and $x_1(t) = [-5, 5]$.

Set $L_{\min} = 2$, $\psi_1 = 1.01$, $\psi_2 = 1.01$, $\gamma_1 = 0.13$, $\gamma_2 = 0.4$, $e_{11} = e_{12} = e_{21} = e_{22} = 4$, the parameter of event-triggered scheme $\varrho^2 = 0.4$, $\rho_1 = 0.75$, $\rho_2 = 0.95$ which can guarantee $\hat{\sigma}_j - \rho_j \sigma_j \geq 0$. Then, the following two cases are considered by setting different values of $\bar{\alpha}$. In Case 1 and Case 2, by setting different occurring probability of attacks, the problems of event-based security controller design for tunnel diode circuit system with single attack or with hybrid-attacks are discussed.

Based on (36) and (40), the controller gain is given as

$$K = \begin{bmatrix} -4.1284 & -1.9967 & -41.858 \end{bmatrix} \quad (37)$$

Cases 1: Let $\bar{\alpha} = 0.04$, $b_{\max} = 0.2$, which means that hybrid-attacks are discussed in the networked control system with event-triggered scheme.

The following matrices can be obtained by using Theorem 2:

$$\begin{cases} Y = 10^3 \times \begin{bmatrix} -0.1891 & -0.0916 & -0.0916 \end{bmatrix} \\ P_1 = \begin{bmatrix} 44.3621 & -7.5459 & -2.7756 \\ -7.5459 & 24.4492 & -1.2883 \\ -2.7756 & -1.2883 & 44.1381 \end{bmatrix} \end{cases} \quad (38)$$

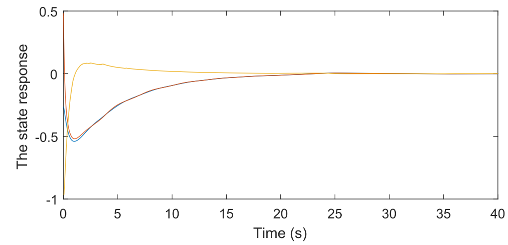

Fig. 3. State response of $x(t)$ in Case 1 of Example 1.

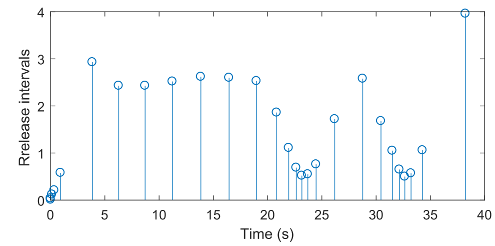

Fig. 4. Release intervals in Case 1 of Example 1.

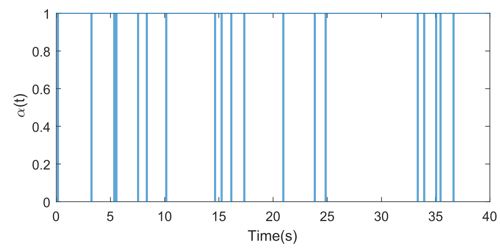

Fig. 5. Bernoulli distribution variables for replay attacks in Case 1 of Example 1.

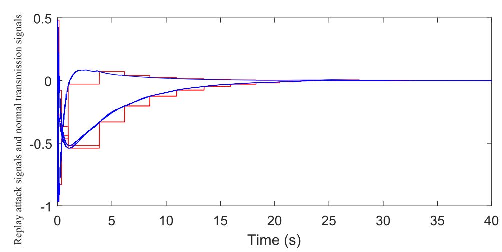

Fig. 6. Relationship between replay attack signals and normal transmission signals in Case 1 of Example 1.

According to (36) and (38), the gain of the output feedback controller is obtained as follows

$$K = \begin{bmatrix} -4.2845 & -2.0760 & -43.3155 \end{bmatrix} \quad (39)$$

Set the initial state $x_0 = [-0.264, 0.482, -0.965]^T$ and the sampling period $h = 0.01s$, the simulation results are depicted from Fig.3 to Fig.6.

The response of $x(t)$ is shown in Fig.3, which indicates that the event-based tunnel diode circuit system under hybrid-attacks is stable, and the desired algorithm is feasible. Fig.4 denotes the release instants and interval of the event-triggered scheme. The Bernoulli distribution variable for replay attacks is depicted in Fig.5 and relationship between the signals under replay attacks and normal transmission signals are shown in

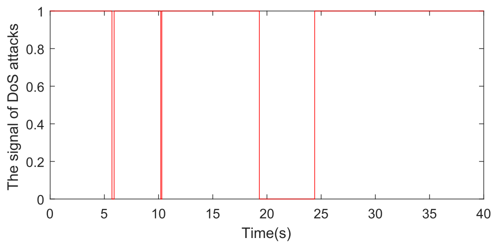

Fig. 7. Sequence of DoS attacks Case 1 of Example 1.

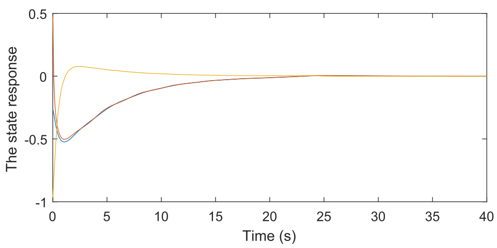

Fig. 8. State response of $x(t)$ in Case 2 of Example 1.

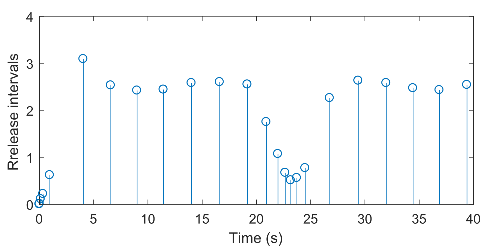

Fig. 9. Release intervals in Case 2 of Example 1.

Fig.6, respectively. Fig.7 depicts the sequence of DoS attacks with a varying way.

Cases 2: Let $\bar{\alpha} = 0$, $b_{\max} = 0.2$, which means that only DoS attacks are discussed in the networked control system with event-triggered scheme.

By solving Theorem 2 through MATLAB, it can be obtained that:

$$\begin{cases} Y = 10^3 \times \begin{bmatrix} -0.1823 & -0.0882 & -1.8481 \end{bmatrix} \\ P_1 = \begin{bmatrix} 44.3632 & -7.5463 & -2.7648 \\ -7.5463 & 24.4483 & -1.2855 \\ -2.7648 & -1.2855 & 44.1523 \end{bmatrix} \end{cases} \tag{40}$$

Taking the sampling period $h = 0.01s$ and the initial condition of the tunnel diode circuit system is chosen as $x_0 = [-0.264, 0.482, -0.965]^T$, the Fig.8-Fig.10 can be obtained through the simulation.

Fig.8 denotes the state response of $x(t)$, which is shown in Fig.8 that the tunnel diode circuit system is stable. Based on the event-triggered condition, the release instants and interval of the event-triggered scheme are shown in Fig.9. Fig.10 denotes the sequence of DoS attacks.

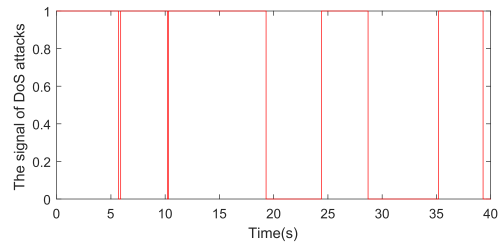

Fig. 10. Sequence of DoS attacks in Case 2 of Example 1.

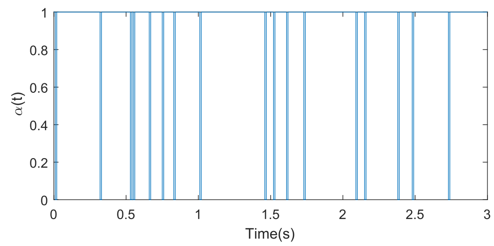

Fig. 11. Bernoulli distribution variables for replay attacks in Example 2.

Example 2: Consider the tunnel diode circuit system with slight modification [6]:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{2} \left(\sigma_i \left(x^i(t), \chi\right)\right) [A_i x(t) + B_i u(t)] \\ y(t) = \sum_{i=1}^{2} \left(\sigma_i \left(x^i(t), \chi\right)\right) [C_i x(t)] \end{cases}$$

the tunnel diode circuit system is described with the following parameters matrices:

$$A_1 = \begin{bmatrix} -40.1 & 40 \\ 0.025 & -10 \end{bmatrix}, \quad A_2 = \begin{bmatrix} -0.1 & 40 \\ 0.025 & -10 \end{bmatrix}$$

$$B_1 = B_2 = \begin{bmatrix} 0 \\ 0.05 \end{bmatrix}, \quad C_i = [10]$$

$$\sigma_1(x^1(t)) = \frac{x_1^2(t)}{100}, \quad \Sigma_2(x^2(t)) = 1 - \frac{x_1^2(t)}{100}$$

Set $L_{\min} = 1.78$, $b_{\max} = 0.2$, $\psi_1 = 1.03$, $\psi_2 = 1.03$, $\gamma_1 = 0.16$, $\gamma_2 = 0.5$, $e_{11} = e_{12} = e_{21} = e_{22} = 10$, the parameter of event-triggered scheme $\varrho^2 = 0.4$, $\bar{\alpha} = 0.05$, $\rho_1 = 0.75$, $\rho_2 = 0.95$ which can guarantee $\hat{\sigma}_j - \rho_j \sigma_j \geq 0$.

By solving (30)-(35) in Theorem 2, the matrices are obtained as follow:

$$\begin{cases} Y = 10^4 \times \begin{bmatrix} -1.593 & -16.447 \end{bmatrix} \\ P_1 = 10^3 \times \begin{bmatrix} 18.025 & -2.463 \\ -2.463 & 1.441 \end{bmatrix} \end{cases} \tag{41}$$

By combining (36) and (41), the following output feedback controller gain can be obtained

$$K = \begin{bmatrix} -0.8836 & -9.1243 \end{bmatrix} \tag{42}$$

For illustration purpose, we perform the sampling period $h = 0.01s$ and the initial condition $x_0 = [-0.3, 8]^T$, the simulation results are shown in Fig.11-Fig.15. Fig.11 shows the occurring probability of the replay attack and Fig.12

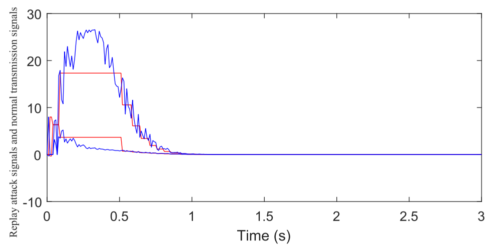

Fig. 12. Relationship between replay attack signals and normal transmission signals in Example 2.

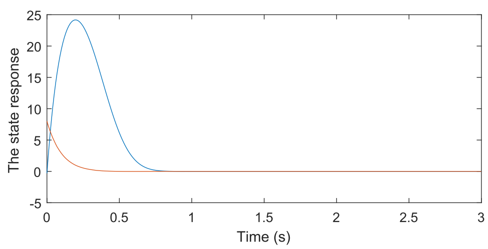

Fig. 13. State response of $x(t)$ in Example 2.

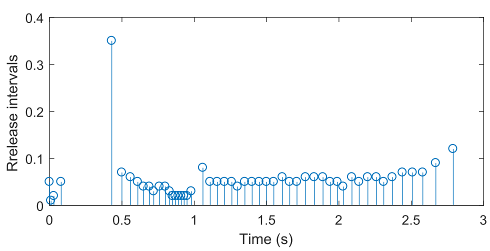

Fig. 14. Release intervals in Example 2.

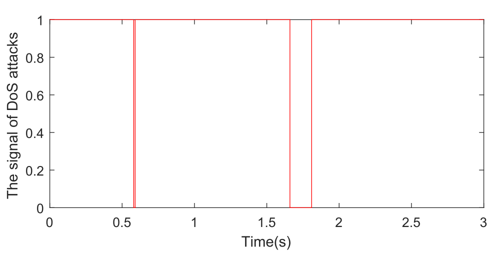

Fig. 15. Sequence of DoS attacks in Example 2.

describes the relationship between signals via replay attacks and normal transmission signals. The response of $x(t)$ is depicted in Fig.13, and Fig.14 represents the event-triggered instants and intervals. Fig.15 denotes the response of DoS attacks. From Fig.13 and Fig.14, the event-based security control for tunnel diode circuit system can be stable under hybrid-attacks, and the proposed algorithm is feasible.

V. Conclusion

In this paper, the problem of event-based security controller design is investigated for state-dependent uncertain systems under hybrid-attacks. In order to resolve resource limitation problem of networked control systems, an event-trigger scheme is introduced to reduce data redundancies and the network burden. Meanwhile, a novel hybrid-attacks model, which consists of replay attack and DoS attacks, is proposed to examine the impact of cyber-attacks on the system security. Further, for the purpose of guaranteeing the state-dependent uncertain system being EMS-stability, sufficient conditions are derived and the output feedback controller gain is also expressed by applying Lyapunov-Krasocskii stability theory and LMI techniques. Finally, a simulation example and an electronic circuit about tunnel diode are shown to illustrate the efficiency of proposed method. Our future research will include the event-based security control and attack detection for state-dependent uncertain systems with hybrid cyber-attacks.

Appendix A
The Elements of the Matrix Π^s_{ijk} in Theorem 1

$$\Pi^1_{ijk} = \begin{bmatrix} \Sigma^1_{11ik} & * & * & * & * & * \\ \Sigma^1_{21ijk} & \Sigma^1_{22ijk} & * & * & * & * \\ \Sigma^1_{31ijk} & \Sigma^1_{32k} & \Sigma^1_{33jk} & * & * & * \\ \Sigma^1_{41i} & 0 & 0 & \Sigma^1_{44j} & * & * \\ \Sigma^1_{51i} & \Sigma^1_{52ij} & \Sigma^1_{53ij} & \Sigma^1_{54i} & \Sigma^1_{55} & * \\ \Sigma^1_{61i} & \Sigma^1_{62ij} & \Sigma^1_{63ij} & \Sigma^1_{64i} & 0 & \Sigma^1_{66k} \end{bmatrix}$$

$$\Pi^2_{ijk} = \begin{bmatrix} \Sigma^2_{11ik} & * & * & * \\ \Sigma^2_{21k} & \Sigma^2_{22k} & * & * \\ \Sigma^2_{31k} & \Sigma^2_{32k} & \Sigma^2_{33k} & * \\ \Sigma^2_{41i} & 0 & 0 & \Sigma^2_{44k} \end{bmatrix}$$

$$\Sigma^1_{11ik} = 2\gamma_1 P_1 + P_1 A_i + A_i^T P_1 + Q_{1k} - \frac{1}{h}(R_{1k} + Z_{1k})$$

$$\Sigma^1_{21ijk} = \bar{\alpha}_1 C_j^T K^T B_i^T P_1 + \frac{1}{h}(R_{1k} - U_{1k} + Z_{1k} - V_{1k})$$

$$\bar{\alpha}_1 = 1 - \bar{\alpha}, \ \Sigma^1_{22ijk} = \varrho^2 C_j^T \Omega C_j + \frac{1}{h}(-2R_{1k} + U_{1k} + U_{1k}^T - 2Z_{1k} + V_{1k} + V_{1k}^T),$$

$$\Sigma^1_{31ijk} = \begin{bmatrix} \frac{1}{h}(U_{1k} + V_{1k}) \\ \bar{\alpha} C_j^T K^T B_i^T P_1 \end{bmatrix}$$

$$\Sigma^1_{32k} = \begin{bmatrix} \frac{1}{h}(R_{1k} - U_{1k} + Z_{1k} - V_{1k}) \\ 0 \end{bmatrix}$$

$$\Sigma^1_{33jk} = diag\{-e^{-2\gamma_1 h} Q_{1k} - \frac{1}{h}(R_{1k} + Z_{1k}), \quad \varrho^2 C_j^T \Omega C_j\}$$

$$\Sigma^1_{41i} = \begin{bmatrix} \bar{\alpha} K^T B_i^T P_1 \\ \bar{\alpha}_1 K^T B_i^T P_1 \end{bmatrix}, \quad \Sigma^1_{44} = \begin{bmatrix} -\Omega & * \\ 0 & -\Omega \end{bmatrix}$$

$$\Sigma^1_{51i} = \begin{bmatrix} \sqrt{h} P_1 A_i \\ \sqrt{h} P_1 A_i \end{bmatrix}, \quad \Sigma^1_{52ij} = \begin{bmatrix} \sqrt{h}\bar{\alpha}_1 P_1 B_i K C_j \\ \sqrt{h}\bar{\alpha}_1 P_1 B_i K C_j \end{bmatrix}$$

$$\Sigma^1_{54i} = \begin{bmatrix} \sqrt{h}\bar{\alpha} P_1 B_i K & \sqrt{h}\bar{\alpha}_1 P_1 B_i K \\ \sqrt{h}\bar{\alpha} P_1 B_i K & \sqrt{h}\bar{\alpha}_1 P_1 B_i K \end{bmatrix}$$

$$\Sigma^1_{53ij} = \begin{bmatrix} 0 & \sqrt{h}\bar{\alpha} P_1 B_i K C_j \\ 0 & \sqrt{h}\bar{\alpha} P_1 B_i K C_j \end{bmatrix},$$

$$\Sigma^1_{62ij} = \begin{bmatrix} -\sqrt{h}\mu P_1 B_i K C_j \\ -\sqrt{h}\mu P_1 B_i K C_j \end{bmatrix}$$

$$\Sigma^1_{63ij} = \sqrt{h} \begin{bmatrix} 0 & \mu\bar{\alpha} P_1 B_i K C_j \\ 0 & \mu\bar{\alpha} P_1 B_i K C_j \end{bmatrix}$$

$$\Sigma^1_{64i} = \begin{bmatrix} \sqrt{h}\mu\bar{\alpha} P_1 B_i K & -\sqrt{h}\mu\bar{\alpha} P_1 B_i K \\ \sqrt{h}\mu\bar{\alpha} P_1 B_i K & -\sqrt{h}\mu\bar{\alpha} P_1 B_i K \end{bmatrix}$$

$$\Sigma^1_{55k} = \Sigma^1_{66k} = diag\{-P_1 R_{1k}^{-1} P_1, -P_1 Z_{1k}^{-1} P_1\}$$

$$\Sigma^2_{11ik} = -2\gamma_2 P_2 + P_2 A_i + A_i^T P_2 + Q_{2k} - \frac{1}{h}(R_{2k} + Z_{2k})$$
$$\Sigma^2_{21k} = \frac{1}{h}(R_{2k} - U_{2k} + Z_{2k} - V_{2k})$$
$$\Sigma^2_{22k} = \frac{1}{h}\left(-2R_{2k} + U_{2k} + U_{2k}^T - 2Z_{2k} + V_{2k} + V_{2k}^T\right)$$
$$\Sigma^2_{31k} = \frac{1}{h}(U_{2k} + V_{2k}), \quad \Sigma^2_{32k} = \frac{1}{h}(R_{2k} - U_{2k} + Z_{2k} - V_{2k})$$
$$\Sigma^2_{33k} = -e^{2\gamma_2 h} Q_{2k} - \frac{1}{h}(R_{2k} + Z_{2k}), \quad \Sigma^2_{41i} = \begin{bmatrix}\sqrt{h}P_2A_i \\ \sqrt{h}P_2A_i\end{bmatrix}$$
$$\Sigma^2_{44k} = diag\{-P_2R_{2k}^{-1}P_2, -P_2Z_{2k}^{-1}P_2\}$$
$$\varpi = \frac{2\gamma_1 L_{\min} - 2(\gamma_1+\gamma_2)h - 2\gamma_2 b_{\max} - \ln\psi_1\psi_2}{\omega_d}$$

Appendix B
The proof of Theorem 1

Consider the Lyapunov-Krasovskii functional as follows

$$V_{\Psi(t)}(t) = V_{1\Psi(t)}(t) + V_{2\Psi(t)}(t) + V_{3\Psi(t)}(t) \tag{43}$$

where

$$V_{1\Psi(t)}(t) = x^T(t)P_{\Psi(t)}x(t)$$
$$V_{2\Psi(t)}(t) = \int_{t-h}^{t} \mathrm{e}(\cdot)x^T(s)\left(\sum_{k=1}^{m}\sigma_k\left(x^k(t),\chi^k(t)\right)Q_{\Psi(t)k}\right)\times x(s)ds$$
$$V_{3\Psi(t)}(t) = \int_{-h}^{0}\int_{t+\theta}^{t} \mathrm{e}(\cdot)\dot{x}^T(s)\left(\sum_{k=1}^{m}\sigma_k\left(x^k(t),\chi^k(t)\right)R_{\Psi(t)k}\right)\times\dot{x}(s)dsd\theta + \int_{-h}^{0}\int_{t+\theta}^{t} \mathrm{e}(\cdot)\dot{x}^T(s)\left(\sum_{k=1}^{m}\sigma_k\left(x^k(t),\chi^k(t)\right)\times Z_{\Psi(t)k}\right)\dot{x}(s)dsd\theta$$

in which $\mathrm{e}(\cdot) = e^{2(-1)^{\Psi(t)}\gamma_{\Psi(t)}(t-s)}$, $Q_{\Psi(t)k}$, $Z_{\Psi(t)k}$, $R_{\Psi(t)k}$, $P_{\Psi(t)}$ are symmetric positive matrices and $\Psi(t) = \begin{cases}1, & t\in\bar{\Phi}_s(0,t)\\ 2, & t\in\Phi_a(0,t)\end{cases}$.

To lighten the notation, σ_k is used to represent $\sigma_k\left(x^k(t),\chi^k(t)\right)$. First, for the case of $\Psi(t)=1$, taking the time derivative and mathematical expectation of (43) along the system (24) yields

$$\mathbb{E}\left[\dot{V}_1(t)\right] \le 2\gamma_1 x^T(t)P_1x(t) + x^T(t)\left(\sum_{k=1}^{m}\sigma_k Q_{1k}\right)x(t) + 2\mathbb{E}\left[x^T(t)P_1\dot{x}(t)\right] - 2\gamma_1 V_1(t) + h\mathbb{E}\left[\dot{x}^T(t)\left(\sum_{k=1}^{m}\sigma_k(R_{1k}+Z_{1k})\right)\dot{x}(t)\right] - e^{-2\gamma_1 h}x^T(t-h)\left(\sum_{k=1}^{m}\sigma_k Q_{1k}\right)x(t-h) - \int_{t-h}^{t}\dot{x}^T(s)\left(\sum_{k=1}^{m}\sigma_k Z_{1k}\right)\dot{x}(s)ds - \int_{t-h}^{t}\dot{x}^T(s)\left(\sum_{k=1}^{m}\sigma_k R_{1k}\right)\dot{x}(s)ds \tag{44}$$

Notice that

$$\mathbb{E}\left[\dot{x}^T(t)\mathbb{R}\dot{x}(t)\right] = \mathcal{A}_0^T\mathbb{R}\mathcal{A}_0 + \mu^2\mathcal{A}_1^T\mathbb{R}\mathcal{A}_1 \tag{45}$$

where $\mathcal{A}_0 = (1-\bar{\alpha})B_iK\left[C_jx(t-\tau_k^n(t)) + e_k^n(t)\right] + A_ix(t) + \bar{\alpha}B_iK\left[C_jx\left(t_r-\tau_k^n(t_r)\right) + e_k^n(t_r)\right]$, $\mathcal{A}_1 = B_iK[C_jx(t_r - \tau_k^n(t_r)) + e_k^n(t_r)] - B_iK\left[C_jx(t-\tau_k^n(t) + e_k^n(t)\right]$ and $\mathbb{R} = \sum_{k=1}^{m}\sigma_k(R_{1k}+Z_{1k})$.

According to the condition (21) of event-triggered scheme, one can obtain

$$\mathcal{T}(t) = \varrho^2 y^T\left(t-\tau_k^n(t)\right)C_j^T\Omega C_j y\left(t-\tau_k^n(t)\right) - \left(e_k^n(t)\right)^T\Omega e_k^n(t) \ge 0 \tag{46}$$

Moreover, by using Lemma 1 to deal with the integral item in (44) and apply Schur complement, one can get from (43)-(46)

$$\mathbb{E}\left[\dot{V}_1(t)\right] + 2\gamma_1V_1(t) \le \mathbb{E}\left[\dot{V}_1(t)\right] + 2\gamma_1V_1(t) + \mathcal{T}(t) \le \vartheta_1^T(t)\left(\sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{k=1}^{m}\sigma_i\hat{\sigma}_j\sigma_k\Pi^1_{ijk}\right)\vartheta_1(t) \tag{47}$$

where $\vartheta^T(t) = \left[\vartheta_1^T(t)\ I\ I\ I\ I\right]$, $\vartheta_1^T(t) = \left[\vartheta_2^T(t)\ x^T\left(t_r-\tau_k^n(t_r)\right)\ \left(e_k^n(t_r)\right)^T\ \left(e_k^n(t)\right)^T\right]$, $\vartheta_2^T(t) = \left[x^T(t)\ x^T\left(t-\tau_k^n(t)\right)\ x^T(t-h)\right]$.

Second, similar to [42], according to the slack matrix M_i^1, the following equalities hold

$$\sum_{i=1}^{m}\sum_{j=1}^{m}\sigma_i\left(\sigma_j-\hat{\sigma}_j\right)M_i^1 = \sum_{i=1}^{m}\sigma_i\left(\sum_{j=1}^{m}\sigma_j - \sum_{j=1}^{m}\hat{\sigma}_j\right)M_i^1 = \sum_{i=1}^{m}\sigma_i(1-1)M_i^1 = 0 \tag{48}$$

where $M_i^1 = (M_i^1)^T \in \mathbb{R}^{n\times n} > 0$, $i\in J_m$. Then, the inequality (47) can be described as

$$\begin{aligned}\mathbb{E}\left[\dot{V}_1(t)\right] &\le \sum_{i=1}^{m}\sum_{j=1}^{m}\sigma_i\hat{\sigma}_j\vartheta^T(t)\Pi^1_{ijk}\vartheta(t) - 2\gamma_1V_1(t)\\ &= \sum_{i=1}^{m}\sum_{j=1}^{m}\sigma_i\left(\sigma_j-\hat{\sigma}_j+\rho_j\sigma_j-\rho_j\sigma_j\right)\vartheta^T(t)\times M_i^1\vartheta(t) + \sum_{i=1}^{m}\sum_{j=1}^{m}\sigma_i\hat{\sigma}_j\vartheta^T(t)\Pi^1_{ijk}\vartheta(t) - 2\gamma_1V_1(t)\\ &\le -2\gamma_1V_1(t) + \sum_{i=1}^{m}\sigma_i^2\vartheta^T(t)\left(\rho_i\Pi^1_{iik} - \rho_iM_i^1 + M_i^1\right)\vartheta(t) + \sum_{i=1}^{m}\sigma_i\left(\hat{\sigma}_j-\rho_j\sigma_j\right)\vartheta^T(t)\times\left(\Pi^1_{ijk}-M_i^1\right)\vartheta(t) + \sum_{i=1}^{m}\sum_{i<j}\vartheta^T(t)\left(\rho_j\Pi^1_{ijk} + \rho_i\Pi^1_{jik} - \rho_jM_i^1 - \rho_iM_j^1 + M_i^1 + M_j^1\right)\vartheta(t)\end{aligned} \tag{49}$$

According to the conditions (27)-(29) and (49), it can be derived that

$$\mathbb{E}\left[\dot{V}_1(t)\right] + 2\gamma_1 V_1(t) < 0 \tag{50}$$

with $\hat{\sigma}_j - \rho_j\sigma_j \geq 0$ for all j.

Third, for another case of $\Psi(t) = 2$, taking the time derivative and mathematical expectation of (43) in the same way, one has that

$$\mathbb{E}\left[\dot{V}_2(t)\right] - 2\gamma_2 V_2(t) \leq \vartheta_2^T(t)\left(\sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{k=1}^{m}\sigma_i\hat{\sigma}_j\sigma_k\Pi_{ijk}^2\right)\vartheta_2(t) \tag{51}$$

Based on the conditions (27)-(29) and (49), we obtain that $\mathbb{E}\left[\dot{V}_2(t)\right] - 2\gamma_2 V_2(t) < 0$.

Fourth, inspired by [37], from the inequalities (50) and (51), it is clear that

$$\mathbb{E}[V(t)] \leq \begin{cases} e^{-2\gamma_1(t-\hbar_n)}\mathbb{E}[V_1(\hbar_n)], \\ t \in [\hbar_n, \hbar_n + L_n) \\ e^{2\gamma_2(t-\hbar_n-L_n)}\mathbb{E}[V_2(\hbar_n + L_n)], \\ t \in \left[\hbar_n + L_n, \hbar_{n+1}\right) \end{cases} \tag{52}$$

Based on (29)-(31), one can get

$$\begin{cases} \mathbb{E}[V(\hbar_n)] \leq \psi_2\mathbb{E}\left[V_2\left(\hbar_n^-\right)\right] \\ \mathbb{E}[V(\hbar_n + L_n)] \leq \psi_1 e^{2(\gamma_1+\gamma_2)h}\mathbb{E}\left[V_2\left(\hbar_n^- + L_n^-\right)\right] \end{cases} \tag{53}$$

Assuming $t \in [\hbar_n, \hbar_n + L_n)$, it follows from (52)-(53) that

$$\begin{aligned} \mathbb{E}[V_1(t)] &\leq e^{-2\gamma_1(t-\hbar_n)}\psi_2\mathbb{E}\left[V_2\left(\hbar_n^-\right)\right] \\ &\leq e^{2\gamma_2(\hbar_n-\hbar_{n-1}-L_{n-1})-2\gamma_1(t-\hbar_n)}\psi_2 \\ &\quad \times \mathbb{E}\left[V_2(\hbar_{n-1} + L_{n-1})\right] \\ &\leq \ldots \\ &\leq e^{pn(t)}(\psi_1\psi_2)^{n(t)}\mathbb{E}[V_1(\hbar_0)] \end{aligned} \tag{54}$$

where $p = 2(\gamma_1 + \gamma_2)h - 2\gamma_1[(t - \hbar_n) + (\hbar_{n-1} + L_{n-1} - \hbar_{n-1}) + \ldots + (\hbar_0 - \hbar_0 - L_0)] + 2\gamma_2[(\hbar_n - \hbar_{n-1} - L_{n-1}) + (\hbar_{n-1} - \hbar_{n-2} - L_{n-2}) + \ldots + (\hbar_1 - \hbar_0 - L_0)]$.

Assuming $t \in \left[\hbar_n + L_n, \hbar_{n+1}\right)$, one can obtain from (52)-(53) that

$$\begin{aligned} \mathbb{E}[V_2(t)] &\leq e^{2\gamma_2(t-\hbar_n-L_n)}\psi_1\mathbb{E}\left[V_1\left(\hbar_n^- + L_n^-\right)\right] \\ &\leq e^{-2\gamma_1(\hbar_n+L_n-\hbar_{n-1})+2\gamma_2(t-\hbar_n-L_n)}\psi_1 \\ &\quad \times \mathbb{E}\left[V_1(\hbar_{n-1})\right] \\ &\leq \ldots \\ &\leq \frac{e^{q(n(t)+1)}}{\psi_2}\psi_1^{n(t)+1}\psi_2^{n(t)}\mathbb{E}[V_1(\hbar_0)] \end{aligned} \tag{55}$$

where $q = 2(\gamma_1 + \gamma_2)h - 2\gamma_1 L_{\min} + 2\gamma_2 b_{\max}$.

Based on the nature of DoS attacks frequency in Assumption 2, it can be obtained from (54) and (55) that

$$\begin{aligned} \mathbb{E}[V(t)] &\leq \max\left\{e^{b1}, \frac{e^{b2}}{\psi_2}\right\}e^{-\varpi t}\mathbb{E}[V_1(\hbar_0)] \\ &= \max\left\{e^{b_1}, \frac{e^{b_2}}{\psi_2}\right\}e^{-\varpi t}\mathbb{E}[V_1(0)] \end{aligned} \tag{56}$$

where $b_1 = d_1\left[2(\gamma_1 + \gamma_2)h + \ln(\psi_1\psi_2) + 2\gamma_2 b_{\max} - 2\gamma_1 L_{\min}\right]$ and $b_2 = (d_1+1)[2(\gamma_1+\gamma_2)h+\ln(\psi_1\psi_2)+2\gamma_2 b_{\max}-2\gamma_1 L_{\min}]$.

From the definition of $V(t)$, it yields that

$$f\|x(t)\|^2 \leq \mathbb{E}[V(t)],\ g\|\phi\|_h^2 \geq \mathbb{E}[V_1(0)] \tag{57}$$

where $f = \min\{\lambda_{\min}(P_s)\}$, $g = \max\{\lambda_{\max}(P_s) + \frac{h^2}{2}\lambda_{\max}(R_{1k} + Z_{1k})\}$.

On the basis of the above inequalities (56) and (57), one can get

$$\mathbb{E}[V(t)] \leq \sqrt{\frac{g\max\left\{e^{b_1}, \frac{e^{b_2}}{\psi_2}\right\}}{f}e^{-\frac{\varpi}{2}t}\|\phi\|_h^2} \tag{58}$$

According to Definition 1 and the inequality (58), we can conclude that if (27)-(32) are satisfied, the system (24) is EMS-stability with decay rate $\frac{\varpi}{2}$. This completes the proof.■

Appendix C
The Elements of the Matrix $\bar{\Pi}_{ijk}^s$ in Theorem 2

$$\bar{\Pi}_{ijk}^1 = \begin{bmatrix} \Sigma_{11ik}^1 & * & * & * & * & * \\ \bar{\Sigma}_{21ijk}^1 & \Sigma_{22ijk}^1 & * & * & * & * \\ \bar{\Sigma}_{31ijk}^1 & \Sigma_{32k}^1 & \Sigma_{33jk}^1 & * & * & * \\ \bar{\Sigma}_{41i}^1 & 0 & 0 & \Sigma_{44j}^1 & * & * \\ \Sigma_{51i}^1 & \bar{\Sigma}_{52ij}^1 & \bar{\Sigma}_{53ij}^1 & \bar{\Sigma}_{54i}^1 & \bar{\Sigma}_{55}^1 & * \\ \Sigma_{61i}^1 & \bar{\Sigma}_{62ij}^1 & \bar{\Sigma}_{63ij}^1 & \bar{\Sigma}_{64i}^1 & 0 & \bar{\Sigma}_{66k}^1 \end{bmatrix}$$

$$\Pi_{ijk}^2 = \begin{bmatrix} \Sigma_{11ik}^2 & * & * & * \\ \Sigma_{21k}^2 & \Sigma_{22k}^2 & * & * \\ \Sigma_{31k}^2 & \Sigma_{32k}^2 & \Sigma_{33k}^2 & * \\ \Sigma_{41i}^2 & 0 & 0 & \bar{\Sigma}_{44k}^2 \end{bmatrix}$$

$$\Sigma_{11ik}^1 = 2\gamma_1 P_1 + P_1 A_i + A_i^T P_1 + Q_{1k} - \frac{1}{h}(R_{1k} + Z_{1k})$$

$$\bar{\Sigma}_{21ijk}^1 = \bar{\alpha}_1 C_j^T Y^T B_i^T + \frac{1}{h}(R_{1k} - U_{1k} + Z_{1k} - V_{1k})$$

$$\bar{\alpha}_1 = 1 - \bar{\alpha},\ \Sigma_{22ijk}^1 = \varrho^2 C_j^T\Omega C_j + \frac{1}{h}\left(-2R_{1k} + U_{1k} + U_{1k}^T - 2Z_{1k} + V_{1k} + V_{1k}^T\right),$$

$$\bar{\Sigma}_{31ijk}^1 = \begin{bmatrix} \frac{1}{h}(U_{1k} + V_{1k}) \\ \bar{\alpha}C_j^T Y^T B_i^T \end{bmatrix}$$

$$\Sigma_{32k}^1 = \begin{bmatrix} \frac{1}{h}(R_{1k} - U_{1k} + Z_{1k} - V_{1k}) \\ 0 \end{bmatrix}$$

$$\Sigma_{33jk}^1 = diag\{-e^{-2\gamma_1 h}Q_{1k} - \frac{1}{h}(R_{1k} + Z_{1k}), \varrho^2 C_j^T\Omega C_j\}$$

$$\bar{\Sigma}_{41i}^1 = \begin{bmatrix} \bar{\alpha}Y^T B_i^T \\ \bar{\alpha}_1 Y^T B_i^T \end{bmatrix},\quad \Sigma_{44}^1 = \begin{bmatrix} -\Omega & * \\ 0 & -\Omega \end{bmatrix}$$

$$\Sigma_{51i}^1 = \begin{bmatrix} \sqrt{h}P_1 A_i \\ \sqrt{h}P_1 A_i \end{bmatrix},\quad \bar{\Sigma}_{52ij}^1 = \begin{bmatrix} \sqrt{h}\bar{\alpha}_1 B_i Y C_j \\ \sqrt{h}\bar{\alpha}_1 B_i Y C_j \end{bmatrix}$$

$$\bar{\Sigma}_{53ij}^1 = \begin{bmatrix} 0 & \sqrt{h}\bar{\alpha}B_i Y C_j \\ 0 & \sqrt{h}\bar{\alpha}B_i Y C_j \end{bmatrix},\quad \bar{\Sigma}_{62ij}^1 = \begin{bmatrix} -\sqrt{h}\mu B_i Y C_j \\ -\sqrt{h}\mu B_i Y C_j \end{bmatrix}$$

$$\bar{\Sigma}_{54i}^1 = \sqrt{h}\begin{bmatrix} \bar{\alpha}B_i Y & \bar{\alpha}_1 B_i Y \\ \bar{\alpha}B_i Y & \bar{\alpha}_1 B_i Y \end{bmatrix},\quad \bar{\Sigma}_{63ij}^1 = \begin{bmatrix} 0 & \sqrt{h}\mu\bar{\alpha}B_i Y C_j \\ 0 & \sqrt{h}\mu\bar{\alpha}B_i Y C_j \end{bmatrix}$$

$$\bar{\Sigma}_{64i}^1 = \begin{bmatrix} \sqrt{h}\mu\bar{\alpha}B_i Y & -\sqrt{h}\mu\bar{\alpha}B_i Y \\ \sqrt{h}\mu\bar{\alpha}B_i Y & -\sqrt{h}\mu\bar{\alpha}B_i Y \end{bmatrix}$$

$$\bar{\Sigma}_{55k}^1 = diag\{-2e_{11}P_1 + e_{11}^2 R_{1k}, -2e_{12}P_1 + e_{12}^2 Z_{1k}\}$$

$$\Sigma_{11ik}^2 = -2\gamma_2 P_2 + P_2 A_i + A_i^T P_2 + Q_{2k} - \frac{1}{h}(R_{2k} + Z_{2k})$$
$$\Sigma_{21k}^2 = \frac{1}{h}(R_{2k} - U_{2k} + Z_{2k} - V_{2k}), \quad \bar{\Sigma}_{66k}^1 = \bar{\Sigma}_{55k}^1$$
$$\Sigma_{22k}^2 = \frac{1}{h}\left(-2R_{2k} + U_{2k} + U_{2k}^T - 2Z_{2k} + V_{2k} + V_{2k}^T\right)$$
$$\Sigma_{31k}^2 = \frac{1}{h}(U_{2k} + V_{2k}), \quad \Sigma_{41i}^2 = \begin{bmatrix} \sqrt{h} P_2 A_i \\ \sqrt{h} P_2 A_i \end{bmatrix}$$
$$\Sigma_{32k}^2 = \frac{1}{h}(R_{2k} - U_{2k} + Z_{2k} - V_{2k})$$
$$\Sigma_{33k}^2 = -e^{2\gamma_2 h} Q_{2k} - \frac{1}{h}(R_{2k} + Z_{2k})$$
$$\bar{\Sigma}_{44k}^2 = diag\{-2e_{21}P_2 + e_{21}^2 R_{2k}, -2e_{22}P_2 + e_{22}^2 Z_{2k}\}$$

Appendix D
The Proof of Theorem 2

According to Lemma 2, let B_i be a matrix with the singular value decomposition, then we have the following equalities:

$$B_i^T B_i = V_i^T \begin{bmatrix} \check{B}_i & 0 \end{bmatrix} L_i^T L_i \begin{bmatrix} \check{B}_i \\ 0 \end{bmatrix} V_i = V_i^T \check{B}_i^2 V_i \quad (59)$$

$$\begin{aligned} B_i^T P_1 B_i &= V_i^T \begin{bmatrix} \check{B}_i & 0 \end{bmatrix} L_i^T L_i \mathrm{diag}\{P_1^1, P_1^2\} \\ &\quad \times L_i^T L_i \begin{bmatrix} \check{B}_i \\ 0 \end{bmatrix} V_i \\ &= V_i^T \check{B}_i P_1^1 \check{B}_i V_i \end{aligned} \quad (60)$$

where $P_1 = L_i \begin{bmatrix} P_1^1 & * \\ 0 & P_1^2 \end{bmatrix} L_i^T$, $B_i = L_i \begin{bmatrix} \check{B}_i \\ 0 \end{bmatrix} V_i$.

Combining the equalities (59) and (60), one can get

$$\begin{aligned} (B_i^T B_i)^{-1} B_i^T P_1 B_i &= V_i^T \check{B}_i^{-2} V_i V_i^T \check{B}_i P_1^1 \check{B}_i V_i \\ &= V_i^T \check{B}_i^{-1} P_1^1 \check{B}_i V_i \end{aligned} \quad (61)$$

Based on the above equalities (59)-(61), it yields that

$$\begin{aligned} P_1 B_i K &= L_i \begin{bmatrix} P_1^1 \check{B}_i \\ 0 \end{bmatrix} V_i K \\ &= L_i \begin{bmatrix} \check{B}_i \\ 0 \end{bmatrix} V_i V_i^T \check{B}_i^{-1} P_1^1 \check{B}_i V_i K \\ &= B_i (B_i^T B_i)^{-1} B_i^T P_1 B_i K \end{aligned} \quad (62)$$

Denoting $Y = (B_i^T B_i)^{-1} B_i^T P_1 B_i K$ and noticing that (62), one has that $P_1 B_i K = B_i Y$.

In addition, for any positive scalars e_{s1}, e_{s2}, due to

$$\begin{cases} \left(R_{sk} - e_{s1}^{-1} P_s\right) R_{sk}^{-1} \left(R_{sk} - e_{s1}^{-1} P_s\right) \geq 0 \\ \left(Z_{sk} - e_{s2}^{-1} P_s\right) Z_{sk}^{-1} \left(Z_{sk} - e_{s2}^{-1} P_s\right) \geq 0, \quad (s = 1, 2) \end{cases} \quad (63)$$

Then by simple calculations, (63) can be rewritten as

$$\begin{cases} -P_1 R_{1k}^{-1} P_1 \leq -2e_{11} P_1 + e_{11}^2 R_{1k} \\ -P_1 Z_{2k}^{-1} P_1 \leq -2e_{12} P_1 + e_{12}^2 Z_{2k} \\ -P_2 R_{1k}^{-1} P_2 \leq -2e_{21} P_2 + e_{21}^2 R_{1k} \\ -P_2 Z_{2k}^{-1} P_2 \leq -2e_{22} P_2 + e_{22}^2 Z_{2k} \end{cases} \quad (64)$$

Based on (64) and $P_1 B_i K = B_i Y$, by replacing Σ_{55k}^1, Σ_{66k}^1, Σ_{44k}^2, $P_1 B_i K$ in (27) with $\bar{\Sigma}_{55k}^1$, $\bar{\Sigma}_{66k}^1$, $\bar{\Sigma}_{44k}^2$ and $B_i Y$, respectively, then (27) can be rewritten as (33). Similar operation to (28) and (29), the inequalities (34) and (35) can be obtained. Therefore, it can be seen that (30)-(35) hold implies (27)-(32) hold. Then, if the conditions (27)-(32) in Theorem 1 hold, we can get $\mathbb{E}\left[\dot{V}(t)\right] < 0$, which means the system (24) is EMS-stability. Recalling $Y = (B_i^T B_i)^{-1} B_i^T P_1 B_i K$, the desired output controller gains can be reformed as (36).

That completes the proof. ■

References

[1] S. Xu and J. Lam, "New positive realness conditions for uncertain discrete descriptor systems: Analysis and synthesis," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 9, pp. 1897–1905, Sep. 2004.

[2] J. Feng, N. Li, and H. Zhao, "Event-driven H_∞ control for state-dependent uncertain systems in the sense of ISS," *IET Control Theory Appl.*, vol. 11, no. 7, pp. 962–972, 2017.

[3] X. Zhao, L. Zhang, P. Shi, and H. R. Karimi, "Novel stability criteria for T–S fuzzy systems," *IEEE Trans. Fuzzy Syst.*, vol. 22, no. 2, pp. 313–323, Apr. 2014.

[4] D. Yang, X. Li, and J. Qiu, "Output tracking control of delayed switched systems via state-dependent switching and dynamic output feedback," *Nonlinear Anal., Hybrid Syst.*, vol. 32, pp. 294–305, May 2019.

[5] J. Zhang, Y. Xia, and P. Shi, "Parameter-dependent robust H_∞ filtering for uncertain discrete-time systems," *Automatica*, vol. 45, no. 2, pp. 560–565, 2009.

[6] X. Zhao, L. Zhang, P. Shi, and H. R. Karimi, "Robust control of continuous-time systems with state-dependent uncertainties and its application to electronic circuits," *IEEE Trans. Ind. Electron.*, vol. 61, no. 8, pp. 4161–4170, Aug. 2014.

[7] Y. Sun, J. Yu, and Z. Li, "Event-triggered finite-time robust filtering for a class of state-dependent uncertain systems with network transmission delay," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 3, pp. 1076–1089, Mar. 2019.

[8] M. Zhang, P. Shi, L. Ma, J. Cai, and H. Su, "Network-based fuzzy control for nonlinear Markov jump systems subject to quantization and dropout compensation," *Fuzzy Sets Syst.*, vol. 371, pp. 96–109, Sep. 2019.

[9] H. Jiao, L. Zhang, Q. Shen, J. Zhu, and P. Shi, "Robust gene circuit control design for time-delayed genetic regulatory networks without SUM regulatory logic," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 15, no. 6, pp. 2086–2093, Nov. 2018.

[10] M. Zhang, C. Shen, Z.-G. Wu, and D. Zhang, "Dissipative filtering for switched fuzzy systems with missing measurements," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/tcyb.2019.2908430.

[11] Q. Shen, P. Shi, J. Zhu, and L. Zhang, "Adaptive consensus control of leader-following systems with transmission nonlinearities," *Int. J. Control*, vol. 92, no. 2, pp. 317–328, 2019.

[12] W. Zhang, Y. Tang, T. Huang, and J. Kurths, "Sampled-data consensus of linear multi-agent systems with packet losses," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 11, pp. 2516–2527, Nov. 2017.

[13] Q. Shen, P. Shi, Y. Shi, and J. Zhang, "Adaptive output consensus with saturation and dead-zone and its application," *IEEE Trans. Ind. Electron.*, vol. 6, no. 6, pp. 5025–5034, Jun. 2017.

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

[15] S. Wen, Z. Zeng, M. Z. Q. Chen, and T. Huang, "Synchronization of switched neural networks with communication delays via the event-triggered control," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2334–2343, Oct. 2017.

[16] Z. Gu, P. Shi, D. Yue, and Z. Ding, "Decentralized adaptive event-triggered H_∞ filtering for a class of networked nonlinear interconnected systems," *IEEE Trans. Cybern.*, vol. 49, no. 5, pp. 1570–1579, May 2019.

[17] S. Wen, T. Huang, X. Yu, M. Z. Q. Chen, and Z. Zeng, "Aperiodic sampled-data sliding-mode control of fuzzy systems with communication delays via the event-triggered method," *IEEE Trans. Fuzzy Syst.*, vol. 24, no. 5, pp. 1048–1057, Oct. 2016.

[18] Z.-G. Wu, Y. Xu, Y.-J. Pan, H. Su, and Y. Tang, "Event-triggered control for consensus problem in multi-agent systems with quantized relative state measurements and external disturbance," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 7, pp. 2232–2242, Jul. 2018.

[19] Q. Jia and W. K. S. Tang, "Event-triggered protocol for the consensus of multi-agent systems with state-dependent nonlinear coupling," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 2, pp. 723–732, Feb. 2018.

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

[21] S. Wen, X. Yu, Z. Zeng, and J. Wang, "Event-triggering load frequency control for multiarea power systems with communication delays," *IEEE Trans. Ind. Electron.*, vol. 63, no. 2, pp. 1308–1317, Feb. 2016.

[22] J. Liu, L. Wei, X. Xie, E. Tian, and S. Fei, "Quantized stabilization for T–S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 6, pp. 3820–3834, Dec. 2018.

[23] J. Liu, Y. Gu, X. Xie, D. Yue, and J. H. Park, "Hybrid-driven-based H_∞ control for networked cascade control systems with actuator saturations and stochastic cyber attacks," *IEEE Trans. Syst., Man Cybern., Syst.*, to be published. doi: 10.1109/tsmc.2018.2875484.

[24] S. Lai, B. Chen, T. Li, and L. Yu, "Packet-based state feedback control under DoS attacks in cyber-physical systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, to be published. doi: 10.1109/tcsii.2018.2881984.

[25] A. W. Al-Dabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 8, pp. 1049–1053, Aug. 2018.

[26] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *IEEE Trans. Cybern.*, vol. 48, no. 6, pp. 1862–1876, Jun. 2018.

[27] L. Zha, J. Liu, and J. Cao, "Resilient event-triggered consensus control for nonlinear muti-agent systems with DoS attacks," *J. Franklin Inst.*, to be published. doi: 10.1016/j.jfranklin.2019.06.014.

[28] J. Liu, L. Wei, J. Cao, and S. Fei, "Hybrid-driven H_∞ filter design for T–S fuzzy systems with quantization," *Nonlinear Anal.-Hybrid Syst.*, vol. 31, pp. 135–152, Feb. 2019.

[29] J. Liu, E. Tian, X. Xie, and H. Lin, "Distributed event-triggered control for networked control systems with stochastic cyber-attacks," *J. Franklin Inst.*, to be published. doi: 10.1016/j.jfranklin.2018.01.048.

[30] J. Liu, Y. Gu, L. Zha, Y. Liu, and J. Cao, "Event-triggered H_∞ load frequency control for multi-area power systems under hybrid cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1665–1678, Aug. 2019.

[31] J. Liu, T. Yin, M. Shen, X. Xie, and J. Cao, "State estimation for cyber–physical systems with limited communication resources, sensor saturation and denial-of-service attacks," *ISA Trans.*, to be published. doi: 10.1016/j.isatra.2018.12.032.

[32] S. Khaledian, F. Farzami, D. Erricolo, and B. Smida, "A full-duplex bidirectional amplifier with low DC power consumption using tunnel diodes," *IEEE Microw. Wireless Compon. Lett.*, vol. 27, no. 12, pp. 1125–1127, Dec. 2017.

[33] Y. Li, H. R. Karimi, Q. Zhang, D. Zhao, and Y. Li, "Fault detection for linear discrete time-varying systems subject to random sensor delay: A Riccati equation approach," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 5, pp. 1707–1716, May 2018.

[34] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Mar. 2001.

[35] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[36] 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.

[37] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/tcyb.2018.2861834.

[38] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[39] W. Zhang, Q.-L. Han, Y. Tang, and Y. Liu, "Sampled-data control for a class of linear time-varying systems," *Automatica*, vol. 103, pp. 126–134, May 2019.

[40] J. Liu, L. Wei, X.-P. Xie, and D. Yue, "Distributed event-triggered state estimators design for sensor networked systems with deception attacks," *IET Control Theory Appl.*, to be published. doi: 10.1049/iet-cta.2018.5868.

[41] Q.-L. Han, Y. Liu, and F. Yang, "Optimal communication network-based H_∞ quantized control with packet dropouts for a class of discrete-time neural networks with distributed time delay," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 2, pp. 426–434, Feb. 2016.

[42] H. Li, C. Wu, S. Yin, and H. K. Lam, "Observer-based fuzzy control for nonlinear networked systems under unmeasurable premise variables," *IEEE Trans. Fuzzy Syst.*, vol. 24, no. 5, pp. 1233–1245, Oct. 2016.

Jinliang Liu received the Ph.D. degree in networked control systems from Donghua University, Shanghai, China, in 2011.

From December 2013 to June 2016, he was a Post-Doctoral Research Associate with the School of Automation, Southeast University, Nanjing, China. From October 2016 to October 2017, he was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, The University of Hong Kong. From November 2017 to January 2018, he was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, South Korea. He is currently a Professor with the Nanjing University of Finance and Economics, and a Visiting Professor with the College of Automation Electronic Engineering, Qingdao University of Science and Technology. His research interests include networked control systems, complex dynamical networks, and time delay systems.

Meng Yang received the B.Eng. degree from the Nanjing Forest Police College, Nanjing, China, in 2017.

She is currently pursuing the M.S. degree with the College of Information Engineering, Nanjing University of Finance and Economics. Her research interests include networked control systems, T-S fuzzy systems, and time delay systems.

Engang Tian received the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

He is currently a Professor with the University of Shanghai for Science and Technology, Shanghai. His research interests include networked control systems, as well as nonlinear stochastic control and filtering.

Jie Cao received the doctor's degree from Southeast University in 2003. He is currently a Professor with the Nanjing University of Finance and Economics, Nanjing, China. His main research interests are complex dynamical networks, data mining, business intelligence, and recommendation system.

Shumin Fei received the Ph.D. degree in nonlinear systems from the Beijing University of Aeronautics and Astronautics, Beijing, China, in 1995.

From 1995 to 1997, he was a Postdoctoral Researcher with the Research Institute of Automation, Southeast University, Nanjing, China. He is currently a Professor with Southeast University. He has published more than 70 journal papers. His research interests include nonlinear systems, time delay system, complex systems, and so on.