Resilient H_∞ Filtering for Event-Triggered Networked Systems Under Nonperiodic DoS Jamming Attacks

Songlin Hu, Dong Yue, *Senior Member, IEEE*, Xiaoli Chen, Zihao Cheng, and Xiangpeng Xie

***Abstract*—This paper focuses on the resilient H_∞ filter design for event-triggered networked systems subject to nonperiodic denial-of-service (DoS) jamming attacks. In this paper, a new resilient event-triggered transmission strategy is first proposed to improve the efficiency of network resource utilization while counteracting the nonperiodic DoS jamming attacks. Then, by using a time-delay approach, the filtering error system is modeled as a switched system, which characterizes the effects of the event-triggering scheme and nonperiodic DoS jamming attacks simultaneously. Based on the established model, by using the piecewise Lyapunov–Krasovskii functional method, linear matrix inequality (LMI)-based sufficient conditions are formulated to achieve the globally exponential stability as well as the weighted H_∞ performance of the resulting switched system under the DoS jamming attacks. Consequently, the co-design method for the desired filter parameters and event-triggering parameters can be formulated provided that the above LMIs are feasible. Finally, the effectiveness of the proposed method is demonstrated by a practical example.**

***Index Terms*—H_∞ filtering, networked systems, nonperiodic denial-of-service (DoS) jamming attacks, piecewise Lyapunov–Krasovskii functional.**

I. Introduction

IN THE past decade, networked systems have been widely used in a broad range of areas, including critical infrastructures, such as electric power systems, transportation systems, and water resource management systems. As one of the core contents in the research of network systems, the state filtering or state estimation problem has attracted much attention from the scientific community in the past few years (see [1]–[4] and survey paper [5]). In particular, the networked H_∞ filtering problem has gained more attention in recent years, since there is no need to know the statistic property of the external disturbance in H_∞ filtering compared to classical Kalman filtering.

Nowadays, owing to the increasing openness of networks, the wired network has been gradually replaced by the wireless network in many practical applications. In this context, the sensor information is transmitted via wireless communication, where the energy consumption becomes a critical issue. In fact, there are peaks of energy consumption for the transmission/reception of data [6]. Hence, to prolong the lifetime of the network, for the battery powered sensor node, it is of significance to reduce the number of messages sent through the wireless network. This, in turn, triggers attention toward H_∞ filtering of networked systems under an event-triggering mechanism, which seems more natural than the commonly used periodic triggering scheme and has more advantages in saving energy and communication resources. The event-based H_∞ filtering problem of networked systems has been extensively investigated, and many important results have been reported in [7]–[16] and the survey paper [17].

Although great progress has been made in the study of event-triggered H_∞ filtering and the estimation of networked systems in recent years, there is another point in connection with wireless communications that need careful consideration. Note that wireless communications operate over a shared medium and are thus vulnerable to cyber attacks, such as denial-of-service (DoS) attacks since the availability of the medium can be interrupted by an attacker [18]. In this case, the data transmission from the sensor node to the filter node may suffer from packet dropouts, which inevitably degrade the filtering performance. If not well handled in the filter/estimator design, the data losses resulted from the DoS attacks may cause instability in the worst case. Therefore, it is of great importance to take the effect of the DoS attacks into account in the analysis and synthesis of event-triggered networked filtering systems [19]. It is worth pointing out that, recently, event-triggered control problems for networked control systems (NCSs) under cyber attacks have become an active research topic in the control community, see [20]–[27] for DoS attacks; [28]–[32] for deception

Manuscript received May 4, 2018; revised October 15, 2018; accepted January 18, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61673223, Grant 61533010, Grant 61773221, and Grant 61633016, in part by the Six Talent Peaks Project of Jiangsu Province of China under Grant RLD201810, in part by the Qing Lan Project of Jiangsu Province of China under Grant QL04317006, in part by NUPTSF under Grant XJKY15001, and in part by the 1311 Talent Project of Nanjing University of Posts and Telecommunications, China. This paper was recommended by Associate Editor C.-C. Lim. *(Corresponding author: Dong Yue.)*

S. Hu, D. Yue, and X. Xie are with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: songlin621@126.com; medongy@vip.163.com; xiexiangpeng1953@163.com).

X. Chen is with the School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: chenxiaoli_206@126.com).

Z. Cheng is with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: oranice7@163.com).

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

Digital Object Identifier 10.1109/TSMC.2019.2896249

attacks; and [33] for replay attacks. However, to the best of our knowledge, there is no work on the event-triggered H_∞ filtering problem for networked systems in the presence of DoS attacks reported yet. It is, therefore, the main motivation of this paper to shorten such a gap by initiating a systematic study.

Summarizing the above discussions, in this paper, we consider the event-triggered H_∞ filtering for networked systems under nonperiodic DoS jamming attacks (when the attacker broadcasts a signal over a wireless medium to intentionally block the availability of the wireless channel, referred to as jamming attack [18]). The main contributions of this paper can be summarized as follows.

1) A new event-triggering transmission scheme that is resilient to the nonperiodic DoS jamming attacks is proposed.
2) An explicit characterization of the sampling period, decay rate, the minimal "sleeping" periods, and the maximal "active" periods of DoS jamming attacks is developed.
3) A novel weighted H_∞ filter will be developed to guarantee that the resultant switched filtering error system is globally exponentially stable (GES) and resilient to nonperiodic DoS jamming attacks as well, by using the piecewise Lyapunov functional approach. The weighted H_∞ performance analysis and filter design results will be formulated in terms of linear matrix inequalities (LMIs), which can be conveniently checked by the standard software.

Notation: The notations used in this paper are quite standard. $\mathbb{N}$ represents the set of non-negative integers. $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, $\mathbb{R}^{n\times m}$ is the set of real $n \times m$ matrices, n, $m \in \mathbb{N}$. The notation $X > 0$ ($X < 0$) for any $X \in \mathbb{R}^{n\times m}$ means that the matrix X is a real symmetric positive definite (negative definite). I is an identity matrix with appropriate dimension. For a real matrix B and two real symmetric matrices A and C of appropriate dimensions, $\begin{bmatrix} A & \star \\ B & C \end{bmatrix}$ denotes a real symmetric matrix, where $\star$ denotes the entries implied by symmetry. $\text{diag}\{\cdots\}$ stands for a block-diagonal matrix. The superscript T stands for matrix transposition. The space of squareintegrable vector functions over $[0, +\infty)$ is denoted by $L_2[0, +\infty)$, and for $w = \{w(t)\} \in L_2[0, +\infty)$, its norm is given by $\|w\|_2 = \sqrt{\int_0^{+\infty} |w(t)|^2 dt}$. Throughout this paper, if not explicitly stated, matrices are assumed to have compatible dimensions.

II. Problem Formulation

A typical networked filtering system under nonperiodic DoS jamming attacks and an event-triggering scheme in the continuous-time domain is shown in Fig. 1, where the system consists of a physical plant, a sensor, a remote filter, and a wireless network channel. For the sake of brevity, in this paper, we assume that the signal is transmitted as a single packet in network channel, packet loss and communication delay are negligible.

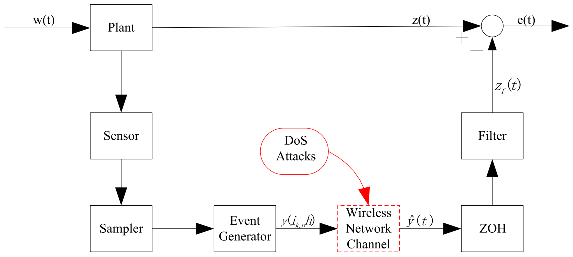


Fig. 1. Framework for networked filtering under DoS jamming attacks.

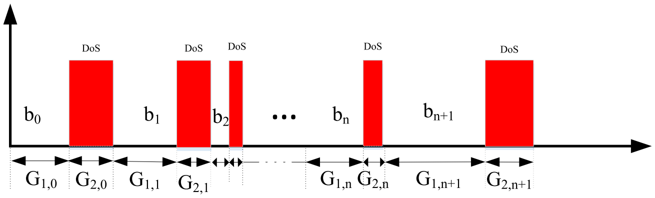


Fig. 2. Timing diagram of DoS jamming attacks.

A. Physical Plant

The physical plant is described by the following time-invariant linear system:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bw(t) \\ y(t) = Cx(t) + Dv(t) \\ z(t) = Lx(t) \end{cases} \quad (1)$$

where $x(t) \in \mathbb{R}^{n_x}$ is the state vector, $y(t) \in \mathbb{R}^m$ is the measured output, $z(t) \in \mathbb{R}^p$ is the signal to be estimated, and $w(t) \in \mathbb{R}^l$ and $v(t) \in \mathbb{R}^q$ are the input signal and measurement noise, respectively, which belong to $L_2[0, +\infty)$. n_x, m, p, l, and $q \in \mathbb{N}$. The problem considered in this paper is to estimate $z(t)$ by a full-order filter of the following form:

$$\begin{cases} \dot{x}_f(t) = A_f x_f(t) + B_f \hat{y}(t) \\ z_f(t) = C_f x_f(t) \end{cases} \quad (2)$$

where $x_f(t) \in \mathbb{R}^{n_x}$ is the filter state vector; $z_f(t)$ is the estimate of $z(t)$; $\hat{y}(t)$ is the real input of the filter; and A_f, B_f, and C_f are the filter gain matrices with appropriate dimensions.

B. Nonperiodic DoS Jamming Attacks

In this paper, we consider a type of power-constraint jammer signal, blocking the communication channels as in [23] (see Fig. 2)

$$S_{\text{DoS}}(t) = \begin{cases} 0, & t \in [g_{n-1}, g_{n-1} + b_{n-1}) \\ 1, & t \in [g_{n-1} + b_{n-1}, g_n) \end{cases} \quad (3)$$

where the sequences of real numbers $\{g_n\}_{n\in\mathbb{N}}$ and $\{b_n\}_{n\in\mathbb{N}}$, satisfy $0 \le g_0 < g_0 + b_0 \le g_1 < g_1 + b_1 \le g_2 < \cdots < g_{n-1} < g_{n-1} + b_{n-1} \le g_n < \cdots$ for $n \in \mathbb{N}$. Based on these parameters, the intervals $\cup_{n\in\mathbb{N}}[g_n, g_n + b_n)$ determine when the signal is sleeping and communication is allowed, while the intervals $\cup_{n\in\mathbb{N}}[g_n + b_n, g_{n+1})$ denote the time intervals where the jammer is active and communication is denied and, thus, no data can be transmitted. Given the power-constrained nature of the DoS jamming attack signal (3), it is reasonable to make the following assumption.

Assumption 1: For time interval $\mathcal{G}_{1,n} \triangleq [g_n, g_n + b_n)$, there exists a positive scalar $b_{\min}$ satisfying

$$\inf_{n\in\mathbb{N}}\{b_n\} \geq b_{\min}. \tag{4}$$

For time interval $\mathcal{G}_{2,n} \triangleq [g_n + b_n, g_{n+1})$, there exists a positive scalar $c_{\max}$ satisfying

$$\sup_{n\in\mathbb{N}}\{g_{n+1} - g_n - b_n\} \leq c_{\max}. \tag{5}$$

Remark 1: Assumption 1 is reasonable for the resilient filter design problem under DoS jamming attacks. From a practical perspective, it is natural to require that communication is allowed to continue for some time after DoS jamming attacks stop. In addition, the DoS duration cannot last too long. This means that the settings for the parameters b_n and $g_{n+1}-g_n-b_n$ ($\forall n \in \mathbb{N}$) should ensure there is no overlap between a DoS jamming attack's finish time and another one's start time.

Remark 2: Notice that in general the nonperiodic DoS jamming attacks (3) do occur in the nth jamming period. That is to say, the case $b_n \to \infty$ will not happen, i.e., $g_n + b_n < g_{n+1} < \infty \; \forall n \in \mathbb{N}$. Therefore, there always exists a positive scalar $b_{\max} = \sup_{n\in\mathbb{N}}\{b_n\}$. This property will be used in the H_∞ performance analysis in Section IV.

Remark 3: Note that some previous works on security of NCSs under DoS attacks, such as [21], [22], [24], [26], [34], and [35] are based on some constraints on the DoS duration and DoS frequency, which play an important role in deducing the main results. However, it is worth pointing out that these constraints are focused on the distribution of the DoS attack occurrences in the time interval $[0, \infty)$, the corresponding stability criterion is difficult to be checked or satisfied in real applications, as the real DoS attacks often happen randomly and are difficult to be predicted. Thus, to improve the existing methods based on the distribution of DoS attack occurrences, the main results proposed in this paper depend on the constraints on sleeping and active intervals of DoS jamming attacks as shown in Assumption 1. The two intervals describe the individual behavior for DoS attacks in different states, and they can be estimated by analyzing the pattern and properties of the DoS jamming signal [23]. Moreover, given that the sleeping and active time intervals of the DoS jamming attacks may be different in different attack statuses and they are difficult to be precisely predicted beforehand. Therefore, to accord with actual and without loss of generality, it is assumed that the lower bound $b_{\min}$ of the sleeping periods of the DoS jamming attacks and the upper bound $c_{\max}$ of the active periods of the DoS jamming attacks are known in advance.

As already mentioned, the sensor output is transmitted to the filter over the wireless network channel. In the absence of the DoS jamming attacks, the measured output $y(t_{k,n}h)$ is successfully transmitted to the filter, $\hat{y}(t) = y(t_{k,n}h)$, otherwise the input is set to zero, i.e., $\hat{y}(t) = 0$. Thus, the input $\hat{y}(t)$ of the filter (2) can be rewritten as

$$\hat{y}(t) = \begin{cases} y\big(t_{k,n}h\big), & t \in \big[t_{k,n}h, t_{k+1,n}h\big) \cap \mathcal{G}_{1,n-1} \\ 0, & t \in \mathcal{G}_{2,n-1} \end{cases} \tag{6}$$

where $\{t_{k,n}h\}$ denotes the sequence of the successful transmission instants ($t_{0,n}h \triangleq g_{n-1}$), which are generated by the event-triggering mechanism to be designed, $h(< b_{\min})$ is the sampling period, $k \in \{0, 1, \ldots, k(n)\} \triangleq \mathcal{K}(n)$ with $n \in \mathbb{N}$ and

$$k(n) = \sup\big\{k \in \mathbb{N} | t_{k,n}h \leq g_{n-1} + b_{n-1}\big\}.$$

Substituting (6) into (2) yields

$$\begin{cases} \dot{x}_f(t) = A_{f_i}x_f(t) + B_{f_i}\hat{y}(t) \\ z_f(t) = C_{f_i}x_f(t), \quad i \in \{1, 2\} \end{cases} \tag{7}$$

which implies that when the attack signal is sleeping or inactive, the filter gain matrices are denoted by A_{f_1}, B_{f_1}, and C_{f_1}. While when the attack signal is present, the filter gain matrices are denoted by A_{f_2}, B_{f_2}, and C_{f_2}. Therefore, system (7) is actually a switching one with two distinct modes. Specifically, for $t \in \mathcal{G}_{1,n}$, the first subsystem is operating. For $t \in \mathcal{G}_{2,n}$, the second subsystem is active. Intuitively, the stability of system (7) will depend on the choice of event-triggering instants $t_{0,n}, t_{1,n}, \ldots, t_{k(n),n}$, the filter gain matrices A_{f_i}, B_{f_i}, and C_{f_i}, and the frequency and duration of the DoS jamming attacks.

Based on the above analysis, when $t \in [t_{k,n}h, t_{k+1,n}h) \cap \mathcal{G}_{1,n-1}$, i.e., in the absence of the DoS jamming attacks, the filter is described as

$$\begin{cases} \dot{x}_f(t) = A_{f_1}x_f(t) + B_{f_1}\hat{y}(t) \\ z_f(t) = C_{f_1}x_f(t) \\ \hat{y}(t) = y\big(t_{k,n}h\big). \end{cases} \tag{8}$$

When $t \in \mathcal{G}_{2,n-1}$, i.e., in the presence of the DoS jamming attack, the filter can be expressed as

$$\begin{cases} \dot{x}_f(t) = A_{f_2}x_f(t) + B_{f_2}\hat{y}(t) \\ z_f(t) = C_{f_2}x_f(t) \\ \hat{y}(t) = 0. \end{cases} \tag{9}$$

In what follows, for easy of exposition, define $\mathcal{R}_{k,n} \triangleq [t_{k,n}h, t_{k+1,n}h)$, $k \in \mathcal{K}(n)$, $n \in \mathbb{N}$.

C. Design of Attack-Resilient Event-Triggered Communication Scheme

Recall that when the DoS jamming attacks are not considered in a network environment, the following event-triggering condition has been used to study the event-triggered H_∞ filtering problem (see [7]):

$$\begin{aligned} &\big[y(t_kh + jh) - y(t_kh)\big]^{\mathrm{T}} W \big[y(t_kh + jh) - y(t_kh)\big] \\ &\quad > \sigma y^{\mathrm{T}}(t_kh) W y(t_kh) \end{aligned} \tag{10}$$

where $\sigma \in [0, 1)$ is a design parameter and $W > 0$ is a weighting matrix to be determined later. t_kh denotes the last event-triggering instant, $t_kh + jh$ ($k, j \in \mathbb{N}$) denotes the subsequent sampling instant. However, in this paper, we mainly consider the effect of the DoS jamming attacks and, thus, the event-triggering scheme (10) cannot be directly used. In addition, notice that the DoS jamming attacks are capable of intercepting the input signal of filter over the jamming time intervals. Therefore, we must redesign the triggering scheme (10) to counteract the effect of the nonperiodic DoS jamming attacks (3).

Definition 1: The event-triggering instant shown in (6) in the presence of nonperiodic DoS jamming signal is defined as follows:

$$t_{k,n+1}h = \left\{t_{k_j}h \text{ satisfying (10)} \mid t_{k_j}h \in \mathcal{G}_{1,n}\right\} \cup \{g_{n+1}\} \tag{11}$$

where n, t_{k_j}, $k_j \in \mathbb{N}$, and k denotes the number of triggering times occurring in $(n+1)$th jammer action interval.

Remark 4: It is worth emphasizing that the triggering instants determined by (11) include the time instants satisfying (10) while falling in the interval $\mathcal{G}_{1,n}$. Specifically, if there is no event occurring in $\mathcal{G}_{1,n}$, then the only triggering instant is g_{n+1}. In addition, the so-called Zeno behavior (i.e., occurring infinite times in a finite time interval) will not happen here. Since the proposed event-triggering condition is implemented in the context of periodic sampling, which implies that the minimum triggering interval in this paper is actually one sampling period h. That is, the event will be triggered at each sampling time instant in the worst-case scenario.

D. Event-Based Switched Filtering Error System Formulation

In this section, we analyze the system stability by the well-developed theories on time delay systems and switched systems. First, the system, combining (1) and (7), is transformed into an equivalent switching time delay system with an event-triggering strategy (11). To this end, we divide the event intervals $\mathcal{R}_{k,n}$ shown in (7) into sampling interval-like subintervals

$$\begin{aligned}\mathcal{R}_{k,n} = {} & \left\{\cup_{m=1}^{\lambda_{k,n}}\left[t_{k,n}h + (m-1)h,\, t_{k,n}h + mh\right)\right\}\\ & \cup \left[t_{k,n}h + \lambda_{k,n}h,\, t_{k+1,n}h\right)\end{aligned} \tag{12}$$

where $k \in \mathcal{K}(n)$, $n \in \mathbb{N}$, and

$$\lambda_{k,n} \triangleq \sup\left\{m \in \mathbb{N}\middle| t_{k,n}h + mh < t_{k+1,n}h\right\}.$$

Let

$$\begin{cases}\mathcal{F}_{k,n}^{m} = \left[t_{k,n}h + (m-1)h,\, t_{k,n}h + mh\right)\\ \qquad m \in \left\{1, 2, \ldots, \lambda_{k,n}\right\}\\ \mathcal{F}_{k,n}^{\lambda_{k,n}+1} = \left[t_{k,n}h + \lambda_{k,n}h,\, t_{k+1,n}h\right).\end{cases} \tag{13}$$

Note that

$$\mathcal{G}_{1,n-1} = \cup_{k=0}^{k(n)}\left\{\mathcal{R}_{k,n} \cap \mathcal{G}_{1,n-1}\right\} \subseteq \cup_{k=0}^{k(n)}\mathcal{R}_{k,n}. \tag{14}$$

Combining (12)–(14), the interval $\mathcal{G}_{1,n-1}$ can be rewritten as

$$\mathcal{G}_{1,n-1} = \cup_{k=0}^{k(n)} \cup_{m=1}^{\lambda_{k,n}} \left\{\mathcal{F}_{k,n}^{m} \cap \mathcal{G}_{1,n-1}\right\}.$$

Set

$$\Omega_{k,n}^{m} = \mathcal{F}_{k,n}^{m} \cap \mathcal{G}_{1,n-1} \tag{15}$$

then

$$\mathcal{G}_{1,n-1} = \cup_{k=0}^{k(n)} \cup_{m=1}^{\lambda_{k,n}+1} \Omega_{k,n}^{m}.$$

Now, for $k \in \mathcal{K}(n)$, $n \in \mathbb{N}$, define two piecewise functions as follows:

$$\tau_{k,n}(t) = \begin{cases} t - t_{k,n}h, & t \in \Omega_{k,n}^{1}\\ t - t_{k,n}h - h, & t \in \Omega_{k,n}^{2}\\ \vdots & \\ t - t_{k,n}h - \lambda_{k,n}h, & t \in \Omega_{k,n}^{\lambda_{k,n}+1}\end{cases} \tag{16}$$

and

$$e_{k,n}(t) = \begin{cases} 0, & t \in \Omega_{k,n}^{1}\\ y\left(t_{k,n}h\right) - y\left(t_{k,n}h + h\right), & t \in \Omega_{k,n}^{2}\\ \vdots & \\ y\left(t_{k,n}h\right) - y\left(t_{k,n}h + \lambda_{k,n}h\right), & t \in \Omega_{k,n}^{\lambda_{k,n}+1}.\end{cases} \tag{17}$$

Based on the above two definitions, it can be seen that

$$\tau_{k,n}(t) \in [0, h),\ \ t \in \mathcal{G}_{1,n-1} \cap \mathcal{R}_{k,n}. \tag{18}$$

The event-triggered sampled state $y(t_{k,n}h)$ can be rewritten as

$$y\left(t_{k,n}h\right) = y\left(t - \tau_{k,n}(t)\right) + e_{k,n}(t),\, t \in \mathcal{G}_{1,n-1} \cap \mathcal{R}_{k,n}$$

with which the systems (8) and (9) can be represented as

$$\begin{cases}\dot{x}_f(t) = A_{f_1}x_f(t) + B_{f_1}y\left(t - \tau_{k,n}(t)\right) + B_{f_1}e_{k,n}(t)\\ z_f(t) = C_{f_1}x_f(t), \quad t \in \mathcal{G}_{1,n-1} \cap \mathcal{R}_{k,n},\ \ n \in \mathbb{N}\end{cases} \tag{19}$$

where the error vector $e_{k,n}(t)$ satisfies

$$\begin{aligned}e_{k,n}^{\mathrm{T}}(t)We_{k,n}(t) \le {} & \sigma\left[y\left(t - \tau_{k,n}(t)\right) + e_{k,n}(t)\right]^{\mathrm{T}}\\ & \times W\left[y\left(t - \tau_{k,n}(t)\right) + e_{k,n}(t)\right]\end{aligned} \tag{20}$$

and

$$\begin{cases}\dot{x}_f(t) = A_{f_2}x_f(t)\\ z_f(t) = C_{f_2}x_f(t)\\ t \in \mathcal{G}_{2,n-1}, \quad n \in \mathbb{N}.\end{cases} \tag{21}$$

Define $e(t) = z(t) - z_f(t)$, $\xi(t)[\,x^{\mathrm{T}}(t) \ \ x_f^{\mathrm{T}}(t)\,]^{\mathrm{T}}$, $\omega(t) = [\,w^{\mathrm{T}}(t) \ \ v^{\mathrm{T}}(t - \tau_{k,n}(t))\,]^{\mathrm{T}}$, combining (1) and (19)–(21), the filtering error system can be written as

$$\begin{cases}\dot{\xi}(t) = \begin{cases} A_1\xi(t) + \mathcal{B}_1 H\xi\left(t - \tau_{k,n}(t)\right) & \\ \ + \mathcal{B}_{e_1}e_{k,n}(t) + \mathcal{B}_{w_1}\omega(t), & t \in \mathcal{G}_{1,n-1} \cap \mathcal{R}_{k,n}\\ A_2\xi(t) + \mathcal{B}_{w_2}\omega(t), & t \in \mathcal{G}_{2,n-1}, n \in \mathbb{N}\end{cases}\\ e(t) = \begin{cases} C_1\xi(t),\ t \in \mathcal{G}_{1,n-1} \cap \mathcal{R}_{k,n}\\ C_2\xi(t),\ t \in \mathcal{G}_{2,n-1}, n \in \mathbb{N}\end{cases}\\ \xi(t) = \Psi(t), \quad t \in [-h, 0]\end{cases} \tag{22}$$

where

$$\begin{aligned}& A_1 = \begin{bmatrix} A & 0\\ 0 & A_{f_1}\end{bmatrix},\ \ A_2 = \begin{bmatrix} A & 0\\ 0 & A_{f_2}\end{bmatrix},\ \ \mathcal{B}_1 = \begin{bmatrix} 0\\ B_{f_1}C\end{bmatrix}\\ & \mathcal{B}_2 = 0,\ \ \mathcal{B}_{e_1} = \begin{bmatrix} 0\\ B_{f_1}\end{bmatrix},\ \ \mathcal{B}_{e_2} = 0,\ \ \mathcal{B}_{w_1} = \begin{bmatrix} B & 0\\ 0 & B_{f_1}D\end{bmatrix}\\ & \mathcal{B}_{w_2} = \begin{bmatrix} B & 0\\ 0 & 0\end{bmatrix},\ \ C_1 = \begin{bmatrix} L & -C_{f_1}\end{bmatrix},\ C_2 = \begin{bmatrix} L & -C_{f_2}\end{bmatrix}\\ & H = \begin{bmatrix} I & 0\end{bmatrix}\end{aligned}$$

and $e_{k,n}(t)$ satisfies (20).

Before proceeding further, we need the following definitions.

Definition 2 [36]: The switched filtering error system (22) is said to be GES with a weighted H_∞ disturbance attenuation level γ, if the following two conditions hold.

1) The switched filtering error system (22) with $\omega(t) = 0$ is GES, that is, there exist constants $\epsilon > 0$ and $\rho > 0$ such that $\|\xi(t)\| \le \epsilon e^{-\rho t}\|\Psi_0\|_h$ for all $t \ge 0$. Here, $\|\Psi_0\|_h = \sup_{-h\le\theta\le 0}\{\|\xi(\theta)\|, \|\dot{\xi}(\theta)\|\}$ and ρ is called the decay rate.

2) For given scalar $\gamma > 0$, the switched system (22) achieves a weighed H_∞ performance level γ, if it is GES and under zero initial condition, the filtering error $e(t)$ satisfies $\|e(t)\|_2 \leq \gamma\|\omega(t)\|_2$ for any nonzero $\omega(t) \in L_2[0, +\infty)$.

Definition 3 [22], [26]: Let $n(0, t)$ denote the number of DoS off/on transitions occurring on the interval $[0, t)$, i.e., $n(0, t) = \text{card}\{n \in \mathbb{N} \mid t > g_n + b_n\}$, where card denotes the number of the elements in the set. We say that the sequence of DoS attacks specified by $\mathcal{G}_{2,n}$ satisfies the DoS frequency constraint for a given $\tau_a \in \mathbb{R}_{>0}$, and arbitrary $\delta \in \mathbb{R}_{\geq 0}$, if for all $t \in \mathbb{R}_{\geq 0}$

$$n(0, t) \leq \delta + \frac{t}{\tau_a}. \tag{23}$$

We are now in a position to state our resilient H_∞ filtering problem as follows.

Resilient H_∞ Filtering Problem: Design a filter in the form of (7) such that the switched system (22) is GES and achieves a weighted H_∞ performance level in the presence of the nonperiodic DoS jamming attacks (3).

III. Stability Analysis

In this section, we first introduce a technical lemma and its corresponding proof, which will be essential in deriving the subsequent results.

Lemma 1: Consider the switched filtering error system (22) without disturbance $\omega(t)$, if for some prescribed scalars $\alpha_i \in (0, +\infty)$, $\sigma \in (0, 1)$, and $h \in (0, b_{\min})$, there exist symmetric positive definite matrices $P_i \in \mathbb{R}^{2n\times 2n}$, $Q_i \in \mathbb{R}^{n\times n}$, $R_i \in \mathbb{R}^{n\times n}$, $i \in \{1, 2\}$, and $W \in \mathbb{R}^{1\times 1}$, and matrices $M_1 \in \mathbb{R}^{(4n+1)\times n}$, $M_2 \in \mathbb{R}^{4n\times n}$, $N_1 \in \mathbb{R}^{(4n+1)\times n}$, and $N_2 \in \mathbb{R}^{4n\times n}$ such that the following matrix inequalities hold:

$$\Sigma_i = \begin{bmatrix} \Sigma_{11}^i & \star & \star \\ \Sigma_{21(l)}^i & \Sigma_{22}^i & \star \\ \Sigma_{31}^i & 0 & \Sigma_{33}^i \end{bmatrix} < 0, \quad l = 1, 2 \tag{24}$$

where $\Sigma_{11}^i = \Pi_{i1} + \Pi_{i2} + \Pi_{i2}^{\mathrm{T}}$, $\Sigma_{21(1)}^i = \sqrt{h}M_i^{\mathrm{T}}$, $\Sigma_{21(2)}^i = \sqrt{h}N_i^{\mathrm{T}}$, $\Sigma_{22}^1 = -e^{-2\alpha_1 h}R_1$, $\Sigma_{22}^2 = -R_2$, $\Sigma_{31}^1 = \sqrt{h}R_1H[A_1 \;\; \mathcal{B}_1 \;\; 0 \;\; \mathcal{B}_{e_1}]$, $\Sigma_{31}^2 = \sqrt{h}R_2H[A_2 \;\; 0 \;\; 0]$, $\Sigma_{33}^i = -R_i$, with

$$\Pi_{11} = \begin{bmatrix} \Lambda_{11} & \star & \star & \star \\ \mathcal{B}_1^{\mathrm{T}}P_1 & \sigma C^{\mathrm{T}}WC & \star & \star \\ 0 & 0 & \Lambda_{33} & \star \\ \mathcal{B}_{e_1}^{\mathrm{T}}P_1 & \sigma WC & 0 & \Lambda_{44} \end{bmatrix}$$

where $\Lambda_{11} = 2\alpha_1 P_1 + P_1A_1 + A_1^{\mathrm{T}}P_1 + H^{\mathrm{T}}Q_1H$, $\Lambda_{33} = -e^{-2\alpha_1 h}Q_1$, and $\Lambda_{44} = \sigma W - W$

$$\Pi_{12} = \begin{bmatrix} -M_1H & M_1 - N_1 & N_1 & 0 \end{bmatrix}$$

and

$$\Pi_{21} = \begin{bmatrix} \begin{array}{c} -2\alpha_2P_2 + P_2A_2 \\ +A_2^{\mathrm{T}}P_2 + H^{\mathrm{T}}Q_2H \end{array} & \star & \star \\ 0 & 0 & \star \\ 0 & 0 & -e^{2\alpha_2 h}Q_2 \end{bmatrix}$$

$$\Pi_{22} = \begin{bmatrix} -M_2H & M_2 - N_2 & N_2 \end{bmatrix}$$

hold, then along the trajectory of the switched system (22), it follows that for $t \in \mathcal{G}_{1,n}$, $n \in \mathbb{N}$:

$$V_1(t) \leq e^{-2\alpha_1(t-g_n)}V_1(g_n) \tag{25}$$

for $t \in \mathcal{G}_{2,n}$, $n \in \mathbb{N}$

$$V_2(t) \leq e^{2\alpha_2(t-g_n-b_n)}V_2(g_n + b_n). \tag{26}$$

Proof: First, choose the following piecewise Lyapunov–Krasovskii functional for the switched system (22):

$$V(t) = \begin{cases} V_1(t), & t \in \mathcal{G}_{1,n-1} \cap \mathcal{R}_{k,n} \\ V_2(t), & t \in \mathcal{G}_{2,n-1} \end{cases}$$

where

$$\begin{aligned} V_i(t) = {} & \xi^{\mathrm{T}}(t)P_i\xi(t) + \int_{t-h}^{t} \xi^{\mathrm{T}}(s)H^{\mathrm{T}}e^*Q_iH\xi(s)ds \\ & + \int_{-h}^{0}\int_{t+\theta}^{t} \dot{\xi}^{\mathrm{T}}(s)H^{\mathrm{T}}e^*R_iH\dot{\xi}(s)dsd\theta \end{aligned} \tag{27}$$

with $P_i > 0$, $Q_i > 0$, $R_i > 0$, $\alpha_i > 0$, and $e^* = e^{2(-1)^i\alpha_i(t-s)}$. Then, following the proof of Lemma 1 in [37], it is not difficult to give a decay estimation of $V_i(t)$ along the trajectory of the system (22). Due to page limitations, the details are omitted here. ■

Based on Lemma 1, the GES of the switched filtering error system (22) is established and summarized below.

Theorem 1: Consider the switched filtering error system (22) without disturbance $\omega(t)$ under the nonperiodic DoS jamming attacks (3), if for some prescribed scalars $\alpha_i \in (0, +\infty)$, $\mu_i \in (0, +\infty)$, $\sigma \in (0, 1)$, $b_{\min} \in (0, +\infty)$, $c_{\max} \in (0, +\infty)$, $\tau_a \in (0, +\infty)$, and $h \in (0, b_{\min})$ satisfying

$$2\alpha_1 b_{\min} - 2(\alpha_1 + \alpha_2)h - 2\alpha_2 c_{\max} - \ln(\mu_1\mu_2) > 0 \tag{28}$$

with $\mu_1\mu_2 > 1$, there exist symmetric positive definite matrices $P_i \in \mathbb{R}^{2n\times 2n}$, $Q_i \in \mathbb{R}^{n\times n}$, $R_i \in \mathbb{R}^{n\times n}$, $i \in \{1, 2\}$, and $W \in \mathbb{R}^{1\times 1}$, and matrices $M_1 \in \mathbb{R}^{(4n+1)\times n}$, $M_2 \in \mathbb{R}^{4n\times n}$, $N_1 \in \mathbb{R}^{(4n+1)\times n}$, and $N_2 \in \mathbb{R}^{4n\times n}$ such that (24) and the following conditions hold:

$$P_1 \leq \mu_2 P_2 \tag{29}$$

$$P_2 \leq \mu_1 e^{2(\alpha_1+\alpha_2)h}P_1 \tag{30}$$

$$Q_i \leq \mu_{3-i}Q_{3-i} \tag{31}$$

$$R_i \leq \mu_{3-i}R_{3-i}. \tag{32}$$

Then the event-based switched filtering system (22) under the nonperiodic DoS jamming attacks (3) is GES with decay rate $\rho \overset{\triangle}{=} (\lambda/2)$, where $\lambda \overset{\triangle}{=} ([2\alpha_1 b_{\min} - 2(\alpha_1 + \alpha_2)h - 2\alpha_2 c_{\max} - \ln(\mu_1\mu_2)]/\tau_a)$.

Proof: Construct a piecewise Lyapunov functional candidate as in Lemma 1: $V(t) = V_i(t)$, $i \in \{1, 2\}$. Then along the same lines as in the proof of the GES shown in [38], it is easy to finish the proof. ■

Remark 5: It is worth pointing out that the conditions (24) and (29)–(32) given in Theorem 1 are linear in P_i, Q_i, R_i, W, M_1, M_2, N_1, and N_2 for fixed filter gain matrices A_{f_i}, B_{f_i}, and C_{f_i}, adjustable parameters $\alpha_i \in (0, +\infty)$, $\mu_i \in (0, +\infty)$, $b_{\min} \in (0, +\infty)$, $c_{\max} \in (0, +\infty)$, and $h \in (0, b_{\min})$. Therefore, when the filter gain matrices A_{f_i}, B_{f_i},

C_{f_i}, and triggering parameters $\sigma \in (0, 1)$ are given in advance, feasible solutions can be searched by iterating over a set of values for $\alpha_i \in (0, +\infty)$, $\mu_i \in (0, +\infty)$, $b_{\min} \in (h, +\infty)$, $c_{\max} \in (0, +\infty)$, and $h \in (0, b_{\min})$ satisfying (28), $i \in \{1, 2\}$.

Remark 6: It follows from the relation (28) in Theorem 1 that the switched filtering error system (22) is GES despite the presence of the nonperiodic DoS jamming attacks (3) if the matrix inequalities (29)–(32) hold and the following condition (C1) or (C2) is satisfied.

(C1) The maximal DoS duration time $c_{\max}$ is smaller than a certain upper bound $\bar{c}_{\max}$. In fact, the equality (28) is equivalent to

$$\begin{aligned} 2\alpha_2 c_{\max} &< 2\alpha_1 b_{\min} - 2(\alpha_1 + \alpha_2)h - \ln(\mu_1\mu_2) \\ &\Leftrightarrow c_{\max} < \bar{c}_{\max} \end{aligned} \tag{33}$$

where $\bar{c}_{\max} \triangleq ([2\alpha_1(b_{\min} - h) - \ln(\mu_1\mu_2)]/2\alpha_2) - h$.

(C2) The minimal sleeping time $b_{\min}$ of DoS attacks is no less than a certain lower bound $b^*_{\min}$. Similar to the preceding analysis, from (28), one has

$$\begin{aligned} 0 &< 2\alpha_1 b_{\min} - 2(\alpha_1 + \alpha_2)h - 2\alpha_2 c_{\max} - \ln(\mu_1\mu_2) \\ &\Leftrightarrow 2\alpha_1 b_{\min} > 2\alpha_2 c_{\max} + 2(\alpha_1 + \alpha_2)h + \ln(\mu_1\mu_2) \\ &\Leftrightarrow b_{\min} > b^*_{\min} \end{aligned} \tag{34}$$

where $b^*_{\min} \triangleq ([2\alpha_2 c_{\max} + 2(\alpha_1 + \alpha_2)h + \ln(\mu_1\mu_2)]/2\alpha_1)$.

Further investigation reveals that the relations (33) and (34) characterize some interesting properties of the DoS attack parameters $b_{\min}$ and $c_{\max}$, the sampling period h, and adjustable parameters $\alpha_i \in (0, +\infty)$ and $\mu_i \in (0, +\infty)$, $i \in \{1, 2\}$. For example, based on the expression for $\bar{c}_{\max}$ in (33), it can be seen that for given scalars $\alpha_i \in (0, +\infty)$, $\mu_i \in (0, +\infty)$, and $h \in (0, b_{\min})$, $\bar{c}_{\max}$ is a linear monotonic increasing function of the minimal sleeping time $b_{\min}$ of DoS jamming attacks (during this sleeping period, the wireless channel is DoS free). That is, the larger the $b_{\min}$, the larger the $\bar{c}_{\max}$. This is consistent with the expected result, since a larger sleeping time of DoS jamming attacks naturally tolerates a larger DoS attack time. Moreover, when $\alpha_i \in (0, +\infty)$ and $\mu_i \in (0, +\infty)$ (or $\alpha_i \in (0, +\infty)$, $\mu_i \in (0, +\infty)$, and $h \in (0, +\infty)$) are fixed, $\bar{c}_{\max}$ is a linear monotonic decreasing function of the sampling period h. A similar analysis can be applied to $b^*_{\min}$.

IV. Weighted H_∞ Filtering Performance Analysis

Based on Theorem 1, sufficient conditions ensuring the weighted H_∞ disturbance attenuation level $\bar{\gamma}$ for the filtering error system (22) are obtained in terms of LMIs.

Theorem 2: For given scalars $\sigma \in (0, 1)$, $\gamma \in (0, +\infty)$, $\alpha_i \in (0, +\infty)$, $\mu_i \in (0, +\infty)$, $b_{\min} \in (0, +\infty)$, $b_{\max} \in (0, +\infty)$, $c_{\max} \in (0, +\infty)$, and $h \in (0, b_{\min})$, the event-based switched filtering error system (22) is GES with a weighted H_∞ disturbance attenuation level $\bar{\gamma} = \sqrt{(\rho_2/\rho_1)}\gamma$ under the nonperiodic DoS jamming attacks (3), where $\rho_1 = \min\{(1/\mu_2), 1\}$ and $\rho_2 = \max\{(1/\mu_2)e^{2\alpha_1 b_{\max}}, e^{2\alpha_2 c_{\max}}\}$, if there exist symmetric positive definite matrices $P_i \in \mathbb{R}^{2n\times 2n}$, $Q_i \in \mathbb{R}^{n\times n}$, $R_i \in \mathbb{R}^{n\times n}$, $i \in \{1, 2\}$, and $W \in \mathbb{R}^{1\times 1}$, and matrices $\hat{M}_1 \in \mathbb{R}^{(4n+3)\times n}$, $\hat{M}_2 \in \mathbb{R}^{(4n+2)\times n}$, $\hat{N}_1 \in \mathbb{R}^{(4n+3)\times n}$, and $\hat{N}_2 \in \mathbb{R}^{(4n+2)\times n}$ such that (28) and (29) and the following matrix inequalities hold:

$$\hat{\Sigma}_i = \begin{bmatrix} \hat{\Sigma}^i_{11} & \star & \star & \star \\ \hat{\Sigma}^i_{21(l)} & \hat{\Sigma}^i_{22} & \star & \star \\ \hat{\Sigma}^i_{31} & 0 & \hat{\Sigma}^i_{33} & \star \\ \hat{\Sigma}^i_{41} & 0 & 0 & -I \end{bmatrix} < 0, \quad l = 1, 2 \tag{35}$$

where $\hat{\Sigma}^i_{11} = \hat{\Pi}_{i1} + \hat{\Pi}_{i2} + \hat{\Pi}^{\mathrm{T}}_{i2}$, $\hat{\Sigma}^i_{21(1)} = \sqrt{h}\hat{M}^{\mathrm{T}}_i$, $\hat{\Sigma}^i_{21(2)} = \sqrt{h}\hat{N}^{\mathrm{T}}_i$, $\hat{\Sigma}^1_{22} = -e^{-2\alpha_1 h}R_1$, $\hat{\Sigma}^2_{22} = -R_2$, $\hat{\Sigma}^1_{31} = \sqrt{h}R_1 H[A_1 \;\; \mathcal{B}_1 \;\; 0 \;\; \mathcal{B}_{e_1} \;\; \mathcal{B}_{w_1}]$, $\hat{\Sigma}^2_{31} = \sqrt{h}R_2 H[A_2 \;\; 0 \;\; 0 \;\; \mathcal{B}_{w_2}]$, $\hat{\Sigma}^i_{33} = -R_i$, $\hat{\Sigma}^1_{41} = [C_1 \;\; 0 \;\; 0 \;\; 0 \;\; 0]$, and $\hat{\Sigma}^2_{41} = [C_2 \;\; 0 \;\; 0 \;\; 0]$

$$\hat{\Pi}_{11} = \begin{bmatrix} \Lambda_{11} & \star & \star & \star & \star \\ \mathcal{B}^{\mathrm{T}}_1 P_1 & \sigma C^{\mathrm{T}} W C & \star & \star & \star \\ 0 & 0 & \Lambda_{33} & \star & \star \\ \mathcal{B}^{\mathrm{T}}_{e_1} P_1 & \sigma W C & 0 & \Lambda_{44} & \star \\ \mathcal{B}^{\mathrm{T}}_{w_1} P_1 & \sigma \hat{D}^{\mathrm{T}} W C & 0 & \sigma \hat{D}^{\mathrm{T}} W & \Lambda_{55} \end{bmatrix}$$

$$\hat{\Pi}_{12} = \begin{bmatrix} -\hat{M}_1 H & \hat{M}_1 - \hat{N}_1 & \hat{N}_1 & 0 & 0 \end{bmatrix}$$

$$\hat{\Pi}_{21} = \begin{bmatrix} \Lambda_{21} & \star & \star & \star \\ 0 & 0 & \star & \star \\ 0 & 0 & -e^{2\alpha_2 h} Q_2 & \star \\ \mathcal{B}^{\mathrm{T}}_{w2} P_2 & 0 & 0 & -\gamma^2 I \end{bmatrix}$$

$$\hat{\Pi}_{22} = \begin{bmatrix} -\hat{M}_2 H & \hat{M}_2 - \hat{N}_2 & \hat{N}_2 & 0 \end{bmatrix}$$

with $\Lambda_{11} = 2\alpha_1 P_1 + P_1 A_1 + A^{\mathrm{T}}_1 P_1 + H^{\mathrm{T}} Q_1 H$, $\Lambda_{33} = -e^{-2\alpha_1 h} Q_1$, $\Lambda_{44} = \sigma W - W$, $\Lambda_{55} = \sigma \hat{D}^{\mathrm{T}} W \hat{D} - \gamma^2 I$, $\hat{D} = [0 \;\; D]$, and $\Lambda_{21} = -2\alpha_2 P_2 + P_2 A_2 + A^{\mathrm{T}}_2 P_2 + H^{\mathrm{T}} Q_2 H$.

Proof: See the Appendix. ■

Based on the weighted H_∞ performance analysis results in Theorem 2, sufficient conditions for the existence of the weighted H_∞ filter of the form (22) are presented in Theorem 3.

V. Weighted H_∞ Filter Synthesis

Theorem 3: For given scalars $\sigma \in (0, 1)$, $\gamma \in (0, +\infty)$, $\alpha_i \in (0, +\infty)$, $\mu_i \in (0, +\infty)$, $b_{\min} \in (0, +\infty)$, $b_{\max} \in (0, +\infty)$, $c_{\max} \in (0, +\infty)$, and $h \in (0, b_{\min})$ satisfying (28), there exists an event-based switched H_∞ filter in the form of (7) such that the switched filtering error system (22) under the nonperiodic DoS jamming attacks (3) is GES with a weighted H_∞ noise attenuation level $\bar{\gamma}$, where $\bar{\gamma}$ is defined in Theorem 2, if there exist some symmetric definite matrices $P_{i1} \in \mathbb{R}^{n\times n}$, $Q_i \in \mathbb{R}^{n\times n}$, $R_i \in \mathbb{R}^{n\times n}$, $V_i \in \mathbb{R}^{n\times n}$, $i \in \{1, 2\}$, $W \in \mathbb{R}^{1\times 1}$, $\tilde{M}_1 \in \mathbb{R}^{(4n+3)\times n}$, $\tilde{M}_2 \in \mathbb{R}^{(4n+2)\times n}$, $\tilde{N}_1 \in \mathbb{R}^{(4n+3)\times n}$, $\tilde{N}_2 \in \mathbb{R}^{(4n+2)\times n}$, $\bar{A}_{f_i} \in \mathbb{R}^{n\times n}$, $\bar{B}_{f_i} \in \mathbb{R}^{n\times 1}$, and $\bar{C}_{f_i} \in \mathbb{R}^{1\times n}$, such that $P_{i1} - V_i > 0$, and the following linear matrix inequalities hold:

$$\tilde{\Sigma}_i = \begin{bmatrix} \tilde{\Sigma}^i_{11} & \star & \star & \star \\ \tilde{\Sigma}^i_{21(l)} & \tilde{\Sigma}^i_{22} & \star & \star \\ \tilde{\Sigma}^i_{31} & 0 & \tilde{\Sigma}^i_{33} & \star \\ \tilde{\Sigma}^i_{41} & 0 & 0 & -I \end{bmatrix} < 0, \quad l = 1, 2 \tag{36}$$

$$\begin{bmatrix} P_{11} - \mu_2 P_{21} & \star \\ Y^{\mathrm{T}}_2 - \mu_2 V_2 & Z_2 - \mu_2 V^{\mathrm{T}}_2 \end{bmatrix} \leq 0 \tag{37}$$

$$\begin{bmatrix} P_{21}-\mu_1 e^{2(\alpha_1+\alpha_2)h}P_{11} & \star \\ Y_1^{\mathrm{T}}-\mu_1 e^{2(\alpha_1+\alpha_2)h}V_1 & Z_1-\mu_1 e^{2(\alpha_1+\alpha_2)h}V_1^{\mathrm{T}} \end{bmatrix} \le 0 \quad (38)$$

$$Q_i-\mu_{3-i}Q_{3-i}\le 0 \quad (39)$$

$$R_i-\mu_{3-i}R_{3-i}\le 0 \quad (40)$$

where $\tilde{\Sigma}_{11}^{i}=\tilde{\Pi}_{i1}+\tilde{\Pi}_{i2}+\tilde{\Pi}_{i2}^{\mathrm{T}}$, $\tilde{\Sigma}_{21(1)}^{i}=\sqrt{h}\tilde{M}_i^{\mathrm{T}}$, $\tilde{\Sigma}_{21(2)}^{i}=\sqrt{h}\tilde{N}_i^{\mathrm{T}}$, $\tilde{\Sigma}_{22}^{1}=-e^{-2\alpha_1 h}R_1$, $\tilde{\Sigma}_{22}^{2}=-R_2$, $\tilde{\Sigma}_{31}^{1}=\sqrt{h}[R_1A\ \ 0\ \ 0\ \ 0\ \ 0\ \ R_1B\ \ 0]$, $\tilde{\Sigma}_{31}^{2}=\sqrt{h}[R_2A\ \ 0\ \ 0\ \ 0\ \ R_2B\ \ 0]$, $\tilde{\Sigma}_{33}^{i}=-R_i$, $\tilde{\Sigma}_{41}^{1}=[L\ \ -\bar{C}_{f_1}\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0]$, and $\tilde{\Sigma}_{41}^{2}=[L\ \ -\bar{C}_{f_2}\ \ 0\ \ 0\ \ 0\ \ 0]$ with

$$\tilde{\Pi}_{11}=\begin{bmatrix} \Lambda_{111} & \star & \star & \star & \star & \star & \star \\ \Lambda_{121} & \Lambda_{122} & \star & \star & \star & \star & \star \\ C^{\mathrm{T}}\bar{B}_{f_1}^{\mathrm{T}} & C^{\mathrm{T}}\bar{B}_{f_1}^{\mathrm{T}} & \sigma C^{\mathrm{T}}WC & \star & \star & \star & \star \\ 0 & 0 & 0 & \Lambda_{144} & \star & \star & \star \\ \bar{B}_{f_1}^{\mathrm{T}} & \bar{B}_{f_1}^{\mathrm{T}} & \sigma WC & 0 & \Lambda_{155} & \star & \star \\ B^{\mathrm{T}}P_{11} & B^{\mathrm{T}}V_1 & 0 & 0 & 0 & -\gamma^2 I & \star \\ D^{\mathrm{T}}\bar{B}_{f_1}^{\mathrm{T}} & D^{\mathrm{T}}\bar{B}_{f_1}^{\mathrm{T}} & \sigma D^{\mathrm{T}}WC & 0 & \sigma D^{\mathrm{T}}W & 0 & \Lambda_{177} \end{bmatrix}$$

$$\tilde{\Pi}_{12}=\begin{bmatrix} -\tilde{M}_1 & 0 & \tilde{M}_1-\tilde{N}_1 & \tilde{N}_1 & 0 & 0 & 0 \end{bmatrix}$$

and

$$\tilde{\Pi}_{21}=\begin{bmatrix} \Lambda_{211} & \star & \star & \star & \star & \star \\ \Lambda_{221} & \Lambda_{222} & \star & \star & \star & \star \\ 0 & 0 & 0 & \star & \star & \star \\ 0 & 0 & 0 & \Lambda_{244} & \star & \star \\ B^{\mathrm{T}}P_{21} & B^{\mathrm{T}}V_2^{\mathrm{T}} & 0 & 0 & -\gamma^2 I & \star \\ 0 & 0 & 0 & 0 & 0 & -\gamma^2 I \end{bmatrix}$$

$$\tilde{\Pi}_{22}=\begin{bmatrix} -\tilde{M}_2 & 0 & \tilde{M}_2-\tilde{N}_2 & \tilde{N}_2 & 0 & 0 \end{bmatrix}$$

where $\Lambda_{111}=2\alpha_1P_{11}+Q_1+P_{11}A+A^{\mathrm{T}}P_{11}$, $\Lambda_{121}=2\alpha_1V_1+V_1A+\bar{A}_{f_1}^{\mathrm{T}}$, $\Lambda_{122}=2\alpha_1V_1^{\mathrm{T}}+\bar{A}_{f_1}+\bar{A}_{f_1}^{\mathrm{T}}$, $\Lambda_{144}=-e^{-2\alpha_1 h}Q_1$, $\Lambda_{155}=(\sigma-1)W$, $\Lambda_{177}=-\gamma^2I+\sigma D^{\mathrm{T}}WD$, $\Lambda_{211}=-2\alpha_2P_{21}+Q_2+P_{21}A+A^{\mathrm{T}}P_{21}$, $\Lambda_{221}=-2\alpha_2V_2+V_2A+\bar{A}_{f_2}^{\mathrm{T}}$, $\Lambda_{222}=-2\alpha_2V_2^{\mathrm{T}}+\bar{A}_{f_2}+\bar{A}_{f_2}^{\mathrm{T}}$, and $\Lambda_{244}=-e^{2\alpha_2 h}Q_2$.

If the above conditions are feasible, the matrices for a resilient H_∞ filter (7) are given by

$$A_{f_i}=\bar{A}_{f_i}V_i^{-1},\ \ B_{f_i}=\bar{B}_{f_i},\ \ C_{f_i}=\bar{C}_{f_i}V_i^{-1}. \quad (41)$$

Proof: This theorem can be proved by using the standard H_∞ filter design technique (see [7]) for networked systems without DoS attacks and, hence, the detailed procedure is omitted here. ■

Remark 7: Note that although many parameters are involved in Theorem 3 [see (36)–(40)], some positive parameters, such as $\sigma < 1$, γ, $b_{\min}$, $b_{\max}$, and $c_{\max}$ can be set in advance and, thus, the feasibility of the proposed design conditions is mainly dependent on the values of parameters α_i, μ_i, and h, which should be carefully chosen in the application of Theorem 3. First, the selection of the sampling period h can be referred to Remark 6. Then, based on Theorem 1, it can be inferred that ρ and $\bar{c}_{\max}$ are monotonic increasing functions of α_1, and are monotonic decreasing functions of α_2, μ_1, and μ_2. In view of this, if the matrix inequalities (36)–(40) are feasible, α_1 should be chosen as large as possible while α_2, μ_1, and μ_2 should be chosen as small as possible to get large values of ρ and $\bar{c}_{\max}$. On the other hand, from (36)–(40), it is seen that a smaller α_1 and larger values of α_2, μ_1, and μ_2 are beneficial to the solvability of the inequalities (36)–(40). Therefore, an iterative method can be used to select the appropriate values of α_1, α_2, μ_1, and μ_2 that guarantee the feasibility of the inequalities (36)–(40).

Remark 8: According to Remark 7, once the values of some related parameters shown in Theorem 3 are chosen properly, the existence conditions for the event-triggered filters become strict LMIs which are convex in the scalar γ^2. Therefore, one may solve the following optimization problem to obtain the event-triggered filter gain matrices in (7) and the corresponding weighting matrix in resilient event-triggering scheme (11) that minimize the H_∞ disturbance attenuation level for given $b_{\min}$, $c_{\max}$, α_1, α_2, μ_2, $b_{\max}$

$$\min\ \bar{\gamma}\quad \text{subjects to (28) and (36)–(40) with } \bar{\gamma}=\gamma^2. \quad (42)$$

If the above optimization problem admits an optimal solution $\bar{\gamma}^*$, then the designed event-triggering scheme (11) and the corresponding event-triggered filters (7) guarantee that the filtering error system (22) achieves the optimal weighted H_∞ performance index $\hat{\gamma}^*=\sqrt{\bar{\gamma}^*(\rho_2/\rho_1)}$, where ρ_1 and ρ_2 are defined in Theorem 2.

Remark 9: Compared with the existing resilient control/estimation methods under DoS attacks (see [22], [26], [34], [35], [39], [40]), our proposed method has some strong and weak points. As regards the construction of the Lyapunov function, the piecewise Lyapunov–Krasovskii functional proposed in this paper provides more freedom in choosing the Lyapunov function candidates and may obtain less conservative results than that of the common quadratic Lyapunov function used in [21], [22], [24], [26], [34], and [35]. On the other hand, the developed piecewise Lyapunov–Krasovskii functional method needs to determine the additional parameters μ_1 and μ_2 to estimate the values of the piecewise Lyapunov–Krasovskii functional at the switching instants. According to (28), the value of $\mu_1 \times \mu_2$ has to be chosen greater than 1 and, thus, might lead to conservative results.

VI. Illustrative Example

In this section, an illustrative example is presented to show the effectiveness of the proposed resilient H_∞ filter design method under DoS attacks. Consider a quarter-car model with an active suspension system that appeared in [16] and [41], from which it can be seen that the state-space realization of the above system can be written as (1) with

$$A=\begin{bmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \\ -k_s/m_s & 0 & -c_s/m_s & c_s/m_s \\ k_s/m_u & -k_u/m_u & c_s/m_u & -c_s/m_u \end{bmatrix}$$

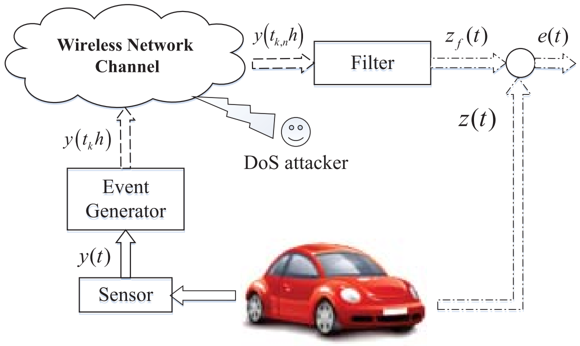


Fig. 3. Framework of active vehicle suspension system.

$$B = \begin{bmatrix} 0 \\ 0 \\ -2\pi q_0\sqrt{G_0 \nu} \\ 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix},\ D = 0.1,\ L = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}$$

where $m_s = 973$ kg, $k_s = 42720$ N/m, $c_s = 3000$ Ns/m, $k_u = 101115$ N/m, $m_u = 114$ kg, $G_0 = 512 \times 10^{-6}$ m^3, $q_0 = 0.1$ m^{-1}, and $\nu = 12.5$ m/s.

Inspired by [16], the structure of active vehicle suspension system over wireless network is depicted in Fig. 3. The data sampled by sensors is fed into the event generator, which is responsible for determining whether to transmit the sampled data or not based on the predefined triggering condition through unreliable wireless networks, which may be subject to nonperiodic DoS jamming attacks. Filters are placed at the remote side to estimate vehicle suspension states based on the vehicle aggregate information.

A. Co-Design of Triggering Parameter and Resilient H_∞ Filter

First, we shall co-design the event-triggering parameters (σ, W) and event-based switched filter parameters A_{f_i}, B_{f_i}, and C_{f_i}, in the form of (8) and (9) such that the switched filtering error system (22) is GES in the presence of the unknown DoS jamming attacks. To this end, we consider the unknown DoS jamming attacks, imposing signal $\mathcal{S}_{\text{DoS}}(t)$ (3), where g_n and b_n satisfying (28). The DoS attacks intervals are generated randomly as shown in Fig. 4, i.e., $\mathcal{G}_{2,n} = \{[1.54, 2.49], [4.97, 5.88], [6.69, 7.98], [8.05, 8.25], [8.58, 9.09], [10.48, 10.86], [11.16, 12.97], [14.51, 15.24], [15.38, 15.60], [17.20, 17.74], [19.16, 22.38], [23.69, 23.73], [24.59, 25.47], [25.59, 26.22], [26.65, 29.27]\}$.

Choosing $\mu_1 = \mu_2 = 1.01$, $\alpha_1 = 0.15$, $\alpha_2 = 0.1$, $h = 0.01$, and $\sigma = 0.2$, by solving Theorem 3, it is obtained that the minimum weighted H_∞ disturbance attenuant level is $\gamma^* = 0.2020$, and the corresponding event-triggering parameter W and the filter gain matrices A_{f_i}, B_{f_i}, and C_{f_i} are given by $W = 6.6087$ and

$$A_{f_1} = \begin{bmatrix} -0.2583 & 13.3626 & 42.6504 & -443.9631 \\ 0.0130 & -29.3653 & -0.3572 & 866.9857 \\ -0.9034 & 0.5522 & -0.7517 & -15.8511 \\ 1.0253 & -0.6307 & -3.8348 & -15.5147 \end{bmatrix}$$

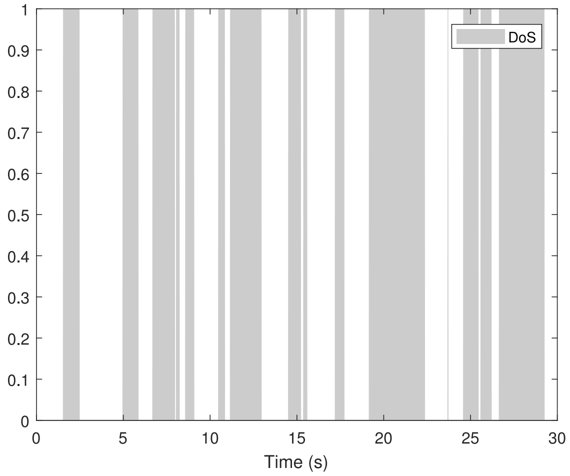


Fig. 4. Nonperiodic DoS jamming attacks signal.

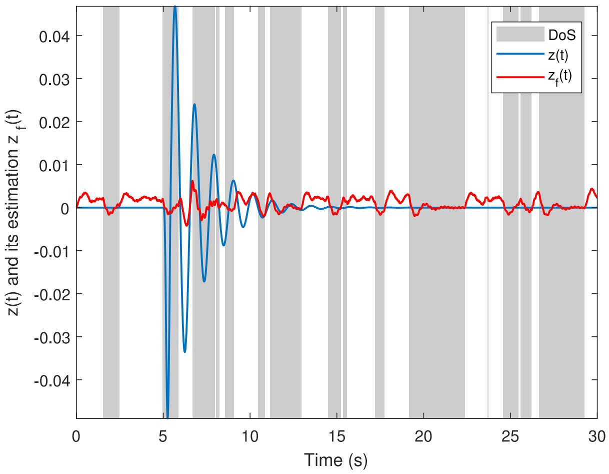


Fig. 5. Estimation signals $z(t)$ and $z_f(t)$ under nonperiodic DoS attacks.

$$B_{f_1} = \begin{bmatrix} 0.6269 & 0.1526 & -0.1046 & -1.8976 \end{bmatrix}^{\mathrm{T}}$$

$$C_{f_1} = \begin{bmatrix} 0.1038 & -0.0261 & -3.7477 & -1.2968 \end{bmatrix}$$

$$A_{f_2} = \begin{bmatrix} -1.2234 & 12.7580 & 46.1348 & -387.7221 \\ 2.4912 & -30.4990 & -4.6758 & 880.6353 \\ -0.9902 & 0.7187 & -0.4404 & -24.4561 \\ 1.0425 & -1.3597 & -2.7149 & 19.0540 \end{bmatrix}$$

$$C_{f_2} = \begin{bmatrix} 0.1070 & -0.0833 & -3.6128 & -0.5875 \end{bmatrix}.$$

To illustrate the H_∞ performance of the designed filter, let us select a set of input signals as follows:

$$\omega(t) = \begin{cases} \frac{\alpha\pi\nu}{l}\sin\left(\frac{2\pi\nu}{l}t\right), & 5 \le t \le 5 + \frac{l}{\nu} \\ 0, & \text{elsewhere.} \end{cases} \tag{43}$$

The disturbance $\nu(t)$ is assumed to be uniformly distributed within $[0, 0.1]$ for the time interval $[0, 20]$. Fig. 5 depicts $z(t)$ and $z_f(t)$, Fig. 6 depicts the estimation error $e(t) = z(t) - z_f(t)$, and Fig. 7 shows the release time intervals under nonperiodic DoS attacks. From these simulations, it can be seen that the proposed event-based switched filter has counteracted the effect of the nonperiodic DoS jamming attacks shown in Fig. 4. Furthermore, by calculation, we have $\|\omega\|_2^2 = 49.3480$,

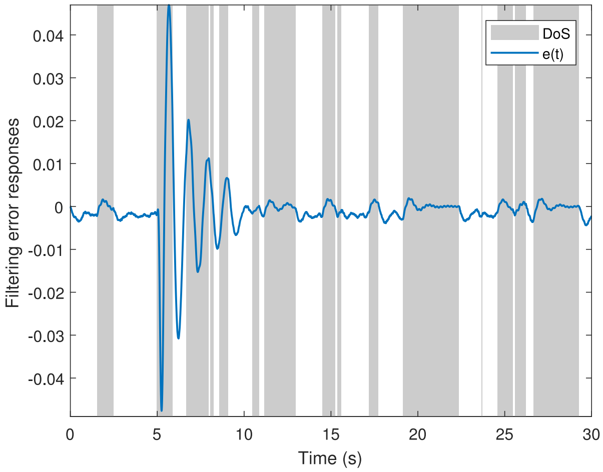


Fig. 6. Estimation error $e(t)$ under nonperiodic DoS attacks.

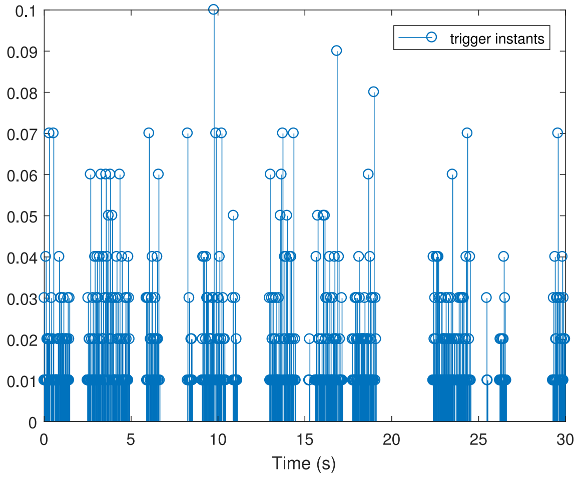


Fig. 7. Release time intervals under nonperiodic DoS attacks.

$\|v\|_2^2 = 10.0228$, and $\|e\|_2^2 = 0.1553$, which yields

$$\sqrt{\frac{\|e\|_2^2}{\|\omega\|_2^2 + \|v\|_2^2}} = 0.0511 < \gamma^* = 0.2020$$

showing the effectiveness of the proposed resilient H_∞ filter design method.

B. Relationship Between the Minimal Sleeping Period b_{min} and Maximal Activating Period c^*_{max} of Attack

Now, to show the relationship between the minimal sleeping period $b_{\min}$ and maximal activating period $c^*_{\max}$, we solve the following optimization problem for different values of $c_{\max}$ in the interval [0, 30 s] (the parameters μ_i, α_i, σ, h, and γ^* are chosen as the same before):

$$c^*_{\max} = \max\{c_{\max} \mid c_{\max} \text{ satisfying (28)}\}$$
$$\text{subject to LMIs (36)–(40).}$$

From Table I, it can be seen that the maximal activating period $c^*_{\max}$ monotonically increases as the minimal sleeping period $b_{\min}$ increases, which is an expected result because a larger sleeping period naturally provides more tolerance on attacks,

TABLE I
$c^*_{\max}$ FOR DIFFERENT VALUES OF $b_{\min}$

b_{min}	1	3	5	7	9
c^*_{max}	1.3	4.3	7.3	10.3	13.3

TABLE II
VALUES OF ρ FOR DIFFERENT VALUES OF $c^*_{\max}$

c^*_{max}	7	5	3	1	0.5
ρ	0.0188	0.1188	0.2188	0.3188	0.3438

TABLE III
VALUES OF ρ FOR DIFFERENT VALUES OF $b_{\min}$

$b_{\min}$	0.8	1.5	2.2	3	5.5
ρ	0.0038	0.0563	0.1088	0.1688	0.2063

TABLE IV
$\gamma_{\min}$ AND FOR $\bar{\gamma}$ DIFFERENT VALUES OF σ

σ	0.1	0.2	0.3	0.4	0.5
$\gamma_{\min}$	0.2008	0.2020	0.2082	0.2166	0.2246
$\bar{\gamma}$	0.5738	0.5772	0.5951	0.6190	0.6417

i.e., a larger $c^*_{\max}$. That is to say, the system can relatively tolerate more malicious attacks. In addition, from Table I, we know that $c^*_{\max} = 7.3$ for given $b_{\min} = 5$ and $\tau_a = 2$ (the other parameters remain unchanged). In order to show the relationship between $c^*_{\max}$ and the decay rate ρ, some calculations are listed in Table II for given $b_{\min} = 5$, from which it is observed that the smaller the $c^*_{\max}$, the larger the ρ. The relationship between $b_{\min}$ and the decay rate ρ are shown in Table III ($c^*_{\max} = 1$, the other parameters are fixed). It is observed that the larger the $b_{\min}$, the larger the ρ, which validates the statement of Remark 7.

C. Influence of the Triggering Parameter σ

Assume that $\mu_1 = \mu_2 = 1.01$, $\alpha_1 = 0.14$, $\alpha_2 = 0.5$, $b_{\min} = 5$, $c^*_{\max} = 7.3$, and $h = 0.01$, and other parameters are chosen as the same before. For given $b_{\max} = 7$, the effect of the triggering parameter σ on the H_∞ performance level $\gamma_{\min}$ is shown in Table IV. It can be seen from Table IV that the larger the σ and the bigger the $\gamma_{\min}$, the worse the noise attenuation level. Finally, for a fixed $\gamma = 1.5$, other parameters are the same as before, the maximin allowable sampling period $h_{\max}$ for different σ are listed in Table V. From Table V, we find that with the increase of the triggering parameter σ (which means the reduction utilization in communication resources is more), the maximum allowable sampling period $h_{\max}$ becomes smaller and, correspondingly, the maximal activating period $c^*_{\max}$ increases. Thus, Remark 6 is verified by the computations. Moreover, it can be observed from Table V that there exists a tradeoff between attack tolerance and communication resources.

TABLE V
$h_{\max}$ AND $c^*_{\max}$ FOR DIFFERENT VALUES OF σ WITH $\gamma = 1.5$

σ	0.1	0.2	0.3	0.4	0.5
c_{max}	3	3	4	5	6
h_{max}	1.6	1.7	1.3	0.9	0.5
c^*_{max}	3.4005	3.1505	4.1505	5.1505	6.1505

VII. Conclusion

In this paper, the event-based weighted H_∞ filter design method for networked systems under nonperiodic DoS jamming attacks has been presented. A novel event-triggering transmission scheme, which is resilient to the DoS jamming attacks, has been proposed to reduce the unnecessary data transmissions over the networks while guaranteeing the desired filter performance. A new switched filtering error system model has been established which has integrated the event-triggering transmission scheme and DoS jamming attacks together. By means of the piecewise Lyapunov–Krasovskii functional approach, sufficient conditions for the GES of the switched filtering error system have been derived and the weighted H_∞ performance level has been guaranteed. The desired filter parameters and event-triggering parameter have been obtained as well. A practical example has been provided to show the effectiveness of the proposed filter design method. In particular, the simulation results show that the proposed method is capable of making the tradeoff among H_∞ performance index, exponential decay rate, event-triggering frequency, and tolerance for nonperiodic DoS jamming attacks by taking full advantage of the design flexibility.

Since the piecewise Lyapunov–Krasovskii functional approach provides a new perspective for investigating the security state estimation of NCSs under DoS attacks, within the proposed generic framework, the method can be further extended to nonlinear NCSs, distributed NCSs, multiagent systems, and so on, which are left for our future work.

Appendix
Proof of Theorem 2

Following the proof of Lemma 1, for any given $n \in \mathbb{N}$, calculating the derivation of $V_1(t)$ with respect to time $t \in \mathcal{G}_{1,n}$ along the trajectory of the system (22) with $i = 1$, we have

$$\dot{V}_1(t) + 2\alpha_1 V_1(t) + e^{\mathrm{T}}(t)e(t) - \gamma^2\omega^{\mathrm{T}}(t)\omega(t) \leq 0. \tag{44}$$

Similarly, differentiating $V_2(t)$ with respect to $t \in \mathcal{G}_{2,n}$ along the trajectories of the system (22) with $i = 2$ yields

$$\dot{V}_2(t) - 2\alpha_2 V_2(t) + e^{\mathrm{T}}(t)e(t) - \gamma^2\omega^{\mathrm{T}}(t)\omega(t) \leq 0. \tag{45}$$

For any given $t \in [0, g_{n+1})$, define $\upsilon_{1n}(t) = (1/\mu_2)e^{-2\alpha_1(g_n-t)}$, $\upsilon_{2n}(t) = e^{2\alpha_2(g_{n+1}-t)}$, $\vartheta_k = (2\alpha_1+2\alpha_2)h+2\alpha_2(g_{k+1}-g_k-b_k)$. Using Lemma 1, one has

$$\begin{aligned}
&\sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)\big[\dot{V}_1(t)+2\alpha_1 V_1(t)\big]dt \\
&\quad+\sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)\big[\dot{V}_2(t)-2\alpha_2 V_2(t)\big]dt \\
&\geq \sum_{k=0}^{n}\bigg[\frac{1}{\mu_2}e^{2\alpha_1 b_k}V_1(g_k+b_k)-\frac{1}{\mu_2}V_1(g_k) \\
&\qquad +\frac{1}{\mu_2}V_1(g_{k+1})-\mu_1 e^{\vartheta_k}V_1(g_k+b_k)\bigg] \\
&= \sum_{k=0}^{n}\frac{1}{\mu_2}\big[V_1(g_{k+1})-V_1(g_k)\big] \\
&\quad +\sum_{k=0}^{n}\bigg[\frac{1}{\mu_2}e^{2\alpha_1 b_k}-\mu_1 e^{\vartheta_k}\bigg]V_1(g_k+b_k) \\
&= \frac{1}{\mu_2}\big[V_1(g_{n+1})-V_1(0)\big] \\
&\quad +\sum_{k=0}^{n}\bigg[\frac{1}{\mu_2}e^{2\alpha_1 b_k}-\mu_1 e^{\vartheta_k}\bigg]V_1(g_k+b_k).
\end{aligned} \tag{46}$$

It follows from (28), we can obtain $(1/\mu_1)e^{2\alpha_1 b_{\min}-(2\alpha_1+2\alpha_2)h} - \mu_2 e^{2\alpha_2 c_{\max}} \geq 0$, which implies that $(1/\mu_2)e^{2\alpha_1 b_k} - \mu_1 e^{\vartheta_k} \geq 0$, where we have used Assumption 1. Therefore, with zero initial condition and noting that $V_1(0) = 0$ and $V_1(t) \geq 0$, we have

$$\sum_{k=0}^{n}\left(\begin{array}{l}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)\big[\dot{V}_1(t)+2\alpha_1 V_1(t)\big]dt \\ +\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)\big[\dot{V}_2(t)-2\alpha_2 V_2(t)\big]dt\end{array}\right) > 0. \tag{47}$$

From (44) and (45), it follows that:

$$\begin{aligned}
&\sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)\Big[-e^{\mathrm{T}}(t)e(t)+\gamma^2\omega^{\mathrm{T}}(t)\omega(t)\Big]dt \\
&\quad\geq \sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)\big[\dot{V}_1(t)+2\alpha_1 V_1(t)\big]dt
\end{aligned} \tag{48}$$

and

$$\begin{aligned}
&\sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)\Big[-e^{\mathrm{T}}(t)e(t)+\gamma^2\omega^{\mathrm{T}}(t)\omega(t)\Big]dt \\
&\quad\geq \sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)\big[\dot{V}_2(t)-2\alpha_2 V_2(t)\big]dt.
\end{aligned} \tag{49}$$

Adding both sides of the inequalities (48) and (49) and noting (47), one has

$$\begin{aligned}
&\sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)\Big[-e^{\mathrm{T}}(t)e(t)+\gamma^2\omega^{\mathrm{T}}(t)\omega(t)\Big]dt \\
&\quad+\sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)\Big[-e^{\mathrm{T}}(t)e(t)+\gamma^2\omega^{\mathrm{T}}(t)\omega(t)\Big]dt \\
&\geq 0
\end{aligned} \tag{50}$$

which means that

$$\begin{aligned}
&\sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)e^{\mathrm{T}}(t)e(t)dt+\sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)e^{\mathrm{T}}(t)e(t)dt \\
&\leq \sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)\gamma^2\omega^{\mathrm{T}}(t)\omega(t)dt \\
&\quad+\sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)\gamma^2\omega^{\mathrm{T}}(t)\omega(t)dt.
\end{aligned} \tag{51}$$

Based on the definitions of ρ_1 and ρ_2 together with (51), one has

$$\begin{aligned}\sum_{k=0}^{n}\int_{g_k}^{g_{k+1}}\rho_1 e^{\mathrm{T}}(t)e(t)dt &\leq \sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)e^{\mathrm{T}}(t)e(t)dt\\ &\quad+\sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)e^{\mathrm{T}}(t)e(t)dt\\ &\leq \sum_{k=0}^{n}\int_{g_k}^{g_k+b_k}\upsilon_{1k}(t)\gamma^2\omega^{\mathrm{T}}(t)\omega(t)dt\\ &\quad+\sum_{k=0}^{n}\int_{g_k+b_k}^{g_{k+1}}\upsilon_{2k}(t)\gamma^2\omega^{\mathrm{T}}(t)\omega(t)dt\\ &\leq \sum_{k=0}^{n}\int_{g_k}^{g_{k+1}}\rho_2\gamma^2\omega^{\mathrm{T}}(t)\omega(t)dt \qquad (52)\end{aligned}$$

which implies that

$$\int_0^{g_{n+1}} e^{\mathrm{T}}(t)e(t)dt \leq \frac{\rho_2}{\rho_1}\gamma^2\int_0^{g_{n+1}}\omega^{\mathrm{T}}(t)\omega(t)dt.$$

Let $n \to \infty (g_{n+1} \to \infty)$, it follows that:

$$\int_0^{\infty} e^{\mathrm{T}}(t)e(t)dt \leq \bar{\gamma}^2\int_0^{\infty}\omega^{\mathrm{T}}(t)\omega(t)dt$$

that is, $\|e(t)\|_2 \leq \bar{\gamma}\|\omega(t)\|_2$ with $\bar{\gamma} = \gamma\sqrt{(\rho_2/\rho_1)}$, for $\omega(t) \in L_2[0, +\infty)$. When $\omega(t) \equiv 0$, it is not difficult to prove the exponential stability of the system (22) based on the preceding derivations. The proof is completed.

References

[1] L. Zhang, Z. Ning, and Z. Wang, "Distributed filtering for fuzzy time-delay systems with packet dropouts and redundant channels," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 4, pp. 559–572, Apr. 2016.

[2] D. Zhang, H. Song, and L. Yu, "Robust fuzzy-model-based filtering for nonlinear cyber-physical systems with multiple stochastic incomplete measurements," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 8, pp. 1826–1838, Aug. 2017.

[3] J. Dong and G.-H. Yang, "H_∞ filtering for continuous-time T–S fuzzy systems with partly immeasurable premise variables," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 8, pp. 1931–1940, Aug. 2017.

[4] H. Yan, Q. Yang, H. Zhang, F. Yang, and X. Zhan, "Distributed H_∞ state estimation for a class of filtering networks with time-varying switching topologies and packet losses," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 12, pp. 2047–2057, Dec. 2018.

[5] X.-M. Zhang, Q.-L. Han, and X. Yu, "Survey on recent advances in networked control systems," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1740–1752, Oct. 2016.

[6] S. Tarbouriech, A. Seuret, J. M. G. D. Silva, and D. Sbarbaro, "Observer-based event-triggered control co-design for linear systems," *IET Control Theory Appl.*, vol. 10, no. 18, pp. 2466–2473, Dec. 2016.

[7] S. Hu and D. Yue, "Event-based H_∞ filtering for networked system with communication delay," *Signal Process.*, vol. 92, no. 9, pp. 2029–2039, Sep. 2012.

[8] C. Peng and M.-R. Fei, "Networked H_∞ filtering for discrete linear systems with a periodic event-triggering communication scheme," *IET Signal Process.*, vol. 7, no. 8, pp. 754–765, Oct. 2013.

[9] X. Meng and T. Chen, "Event triggered robust filter design for discrete-time systems," *IET Control Theory Appl.*, vol. 8, no. 2, pp. 104–113, Jan. 2014.

[10] H. Dong, Z. Wang, S. X. Ding, and H. Gao, "Event-based H_∞ filter design for a class of nonlinear time-varying systems with fading channels and multiplicative noises," *IEEE Trans. Signal Process.*, vol. 63, no. 13, pp. 3387–3395, Jul. 2015.

[11] X. Ge and Q.-L. Han, "Distributed event-triggered H_∞ filtering over sensor networks with communication delays," *Inf. Sci.*, vol. 291, pp. 128–142, Jan. 2015.

[12] X.-M. Zhang and Q.-L. Han, "Event-based H_∞ filtering for sampled-data systems," *Automatica*, vol. 51, pp. 55–69, Jan. 2015.

[13] J. Liu, S. Fei, E. Tian, and Z. Gu, "Co-design of event generator and filtering for a class of T–S fuzzy systems with stochastic sensor faults," *Fuzzy Sets Syst.*, vol. 273, pp. 124–140, Aug. 2015.

[14] C. Zhang, J. Hu, J. Qiu, and Q. Chen, "Event-triggered nonsynchronized H_∞ filtering for discrete-time T–S fuzzy systems based on piecewise Lyapunov functions," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 8, pp. 2330–2341, Aug. 2017.

[15] X. Xiao, L. Zhou, and G. Lu, "Event-triggered H_∞ filtering of continuous-time switched linear systems," *Signal Process.*, vol. 141, pp. 343–349, Dec. 2017.

[16] H. Zhang *et al.*, "Co-design of event-triggered and distributed H_∞ filtering for active semi-vehicle suspension systems," *IEEE/ASME Trans. Mechatronics*, vol. 22, no. 2, pp. 1047–1058, Apr. 2017.

[17] X.-M. Zhang, Q.-L. Han, and B.-L. Zhang, "An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 4–16, Feb. 2017.

[18] B. DeBruhl and P. Tague, "Digital filter design for jamming mitigation in 802.15.4 communication," in *Proc. Int. Conf. Comput. Commun. Netw.*, 2011, pp. 1–6.

[19] D. Wang, Z. Wang, B. Shen, F. E. Alsaadi, and T. Hayat, "Recent advances on filtering and control for cyber-physical systems under security and resource constraints," *J. Frankl. Inst.*, vol. 353, no. 11, pp. 2451–2466, Jul. 2016.

[20] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. Int. Conf. Hybrid Syst. Comput. Control*, San Francisco, CA, USA, 2009, pp. 31–45.

[21] C. D. Persis and P. Tesi, "Resilient control under denial-of-service," *IFAC Proc. Vol.*, vol. 47, no. 3, pp. 134–139, 2014.

[22] 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.

[23] H. S. Foroush and S. Martínez, "On triggering control of single-input linear systems under pulse-width modulated DoS signals," *SIAM J. Control Optim.*, vol. 54, no. 6, pp. 3084–3105, Nov. 2016.

[24] C. D. Persis and P. Tesi, "Networked control of nonlinear systems under denial-of-service," *Syst. Control Lett.*, vol. 96, pp. 124–131, Oct. 2016.

[25] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1786–1794, Oct. 2016.

[26] V. S. Dolk, P. Tesi, C. D. 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.

[27] C. Peng, J. Li, and M. R. Fei, "Resilient event-triggered H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4110–4118, Sep. 2017.

[28] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sep. 2012.

[29] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.

[30] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.

[31] D. Wang, Z. Wang, B. Shen, and F. E. Alsaadi, "Security-guaranteed filtering for discrete-time stochastic delayed systems with randomly occurring sensor saturations and deception attacks," *Int. J. Robust Nonlin. Control*, vol. 27, no. 7, pp. 1194–1208, May 2017.

[32] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, Jan. 2018.

[33] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, 2009, pp. 911–918.

[34] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2434–2449, May 2017.

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

[36] S. Hu, *et al.*, "Observer-based event-triggered control for networked linear systems subject to denial-of service attacks," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/TCYB.2019.2903817.

[37] S. Hu, Y. Han, X. Chen, and Z. Cheng, "Event-triggered H_∞ filtering over wireless sensor networks under unknown periodic DoS jamming attacks," in *Proc. 30th Chin. Control Decis. Conf.*, Shenyang, China, 2018, pp. 1433–1438.

[38] 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.

[39] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231–240, Apr. 2017.

[40] J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attacks," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1086–1101, Mar. 2015.

[41] H. Gao, W. Sun, and P. Shi, "Robust sampled-data H_∞ control for vehicle active suspension systems," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 1, pp. 238–245, Jan. 2010.

Songlin Hu received the Ph.D. degree in control science and engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2012.

Since 2013, he has been with the College of Automation, Nanjing University of Posts and Telecommunications, Nanjing, China, where he is currently an Associate Professor with the Institute of Advanced Technology. His current research interests include networked/event-triggered control, T-S fuzzy systems, and time delay systems.

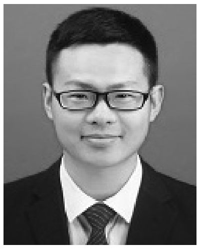
Dong Yue (SM'08) received the Ph.D. degree in control science and engineering from the South China University of Technology, Guangzhou, China, in 1995.

He is currently a Professor and the Dean of the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China, and also a Changjiang Professor with the Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He has published over 100 papers in international journals. His current research interests include analysis and synthesis of networked control systems, multiagent systems, optimal control of power systems, and Internet of Things.

Dr. Yue is currently an Associate Editor of the IEEE Control Systems Society Conference Editorial Board and the IEEE Transactions on Neural Networks and Learning Systems, *Journal of the Franklin Institute*, and *International Journal of Systems Science*.

Xiaoli Chen received the B.Sc. degree in applied mathematics from Xiangfan University, Xiangyang, China, in 2005. She is currently pursuing the Ph.D. degree in telecommunications and information engineering with the Nanjing University of Posts and Telecommunications, Nanjing, China.

Her current research interests include analysis and synthesis of networked control systems, fuzzy systems, interconnected systems, and power systems.



Zihao Cheng received the M.S. degree in control theory and control engineering from the School of Electrical Engineering and Automation, Henan Polytechnic University, Jiaozuo, China, in 2016. He is currently pursuing the Ph.D. degree in information security with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China.

His current research interests include analysis and synthesis of networked control system and its security control, multiagent systems, fuzzy control system, and power system.

Xiangpeng Xie received the B.S. and Ph.D. degrees in engineering from Northeastern University, Shenyang, China, in 2004 and 2010, respectively.

From 2012 to 2014, he was a Post-Doctoral Fellow with the Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is currently an Associate Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.