Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 358 (2021) 9325–9345

www.elsevier.com/locate/jfranklin

H_∞ filter design for discrete-time networked systems with adaptive event-triggered mechanism and hybrid cyber attacks

Jinliang Liu[a,b], Nan Zhang[a], Yan Li[a,*], Xiangpeng Xie[c]

[a] *College of information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210023, China*

[b] *College of Automation Electronic Engineering, Qingdao University of Science and Technology, Qingdao, Shandong 266061, China*

[c] *Institute of Advanced Technology, Nanjing University of Post and Telecommunications, Nanjing, Jiangsu 210023, China*

Received 1 May 2021; received in revised form 17 August 2021; accepted 13 September 2021
Available online 17 September 2021

Abstract

This paper focuses on the design of H_∞ filter for a class of discrete-time networked systems. Given that the network communication resources are becoming limited with the ever-increasing network traffic, an adaptive event-triggered mechanism (AETM) is adopted for the systems to mitigate the pressure of network bandwidth. The considered discrete-time networked systems are envisioned to suffer from both Deception attacks and denial-of-service (DoS) attacks, thereby a novel hybrid cyber attacks model is firstly constructed to integrate the two kinds of attacks. Then, a filtering error system model is established for the discrete-time networked systems under AETM and hybrid cyber attacks. Based on the constructed model, the sufficient conditions that guaranteeing the asymptotic stability and H_∞ performance of the concerned filtering error system are analyzed based on Lyapunov–Krasovskii stability theory. Furthermore, the corresponding parameters of the designed filter are derived by solving a set of linear matrix inequalities (LMIs). The effectiveness of the designed filter is finally demonstrated by conducting a numerical example.

* Corresponding author.
E-mail address: ylnjue@163.com (Y. Li).

https://doi.org/10.1016/j.jfranklin.2021.09.010

1. Introduction

Over the past few decades, the filtering issue plays an important role in networked control field and thus attracts persistent research attentions. Up to now, fruitful results on the issue have been presented in literatures [1–7]. To specifically mention a few, the authors in Gu et al. [1] solved the filtering problem over a class of interconnected systems; focusing on T-S fuzzy systems, the robust filter design problem was tackled in Shi et al. [3]; by taking input constraints and network anomaly into considerations, the authors in Liu et al. [4] proposed an effective filtering method for networked control systems. The aforementioned works were all conducted based on continuous-time model. However, given that continuous-time systems tend to be digitally implemented in practice [8], the filtering problem on discrete-time networked systems is gaining rapid research concerns (see [2,9–12]). For instance, a Kalman filtering approach was proposed in Zhong and Liu [9] to realize intermittent observations for wireless sensor networks. Nevertheless, Kalman filtering always assumes that the spectral densities of external noise are known in advance to minimize the estimation error, which is hardly to be achieved [11]. Accordingly, many new filtering schemes, such as H_2 filtering and H_∞ filtering, are exploited to deal with system uncertainties. Comparing with H_2 filtering, H_∞ filtering is more applicable since that it is not necessary to predetermine the attenuation level of the envisioned filter but which is needed for H_2 filtering. Therefore, this paper will focus on designing H_∞ filter for discrete-time networked systems.

While designing an effective filter, the mismatch between the ever-increasing volume of system data and the limited bandwidth capacity of communication network brings significant challenges. In view of this, many triggered mechanisms have been investigated to reduce the transmission of sampling signals, and guarantee the system performance [13–18]. Among which, time-triggered schemes where the sampled data is periodically transmitted are commonly used in the early stage. However, when the system is stable, which means that the current sampling data is almost same with the latest transmitted data, time-triggered methods will result in a lot of redundant traffic. Thus, event-triggered schemes are consequently proposed with the aim to avoid unnecessary signal transportation [19–25]. Among these literatures, the event-triggered mechanism presented in Yue et al. [23] attracts wide attentions, in which whether the current sampling data is released was determined by a predefined threshold. Based on [23], many kinds of event-triggered methods are designed for various systems and applications. For instance, to handle the synchronization problem of neural networks, the authors in Yan et al. [21] employed an event-triggered scheme with a constant parameter to control the rate of data transmission; for state-dependent uncertain systems, a fixed-parameter-based event-triggered method was used to reduce the bandwidth pressure on communication network in Liu et al. [22]. But it is hard to give an appropriate constant triggering threshold considering the fluctuation of system status. Therefore, adaptive event-triggered mechanisms (AETMs) where the triggering threshold is dynamically adjusted during the system operations are consequently proposed [26–32]. For example, the authors in Gu et al. [26] designed a novel AETM for nonlinear networked interconnected control systems; in Peng et al. [28], another AETM was presented to save network bandwidth for network-based power systems. Given the good adaptability of AETMs to the changes of system states, this paper will introduce an AETM into the design of filter for discrete-time networked systems to respond to the limited network bandwidth.

In networked systems, besides of the limited network resources, the system performance is also affected by various of cyber attacks given the openness of communication networks.

The randomly occurring attacks can interrupt the data transmission, destroy the stability or even availability of networked systems. Such security issue inevitably increases the complexity of handling filtering problem. In the existed studies, a lot of concerns are concentrated on two typical attacks, i.e., denial-of-service (DoS) attacks [33–35] and Deception attacks [36–39]. DoS attacks suspend the regular signal transmission by exhausting network resources. Taking DoS attacks into considerations, the distributed resilient filtering problem for a class of power systems was addressed in Chen et al. [33]. For nonlinear stochastic systems with DoS attacks, the distributed filtering problem based on probabilistic constraints was investigated in Tian et al. [34]. Deception attacks degrade the system performance by injecting fake information into the network. With Deception attacks, the filtering problem over stochastic nonlinear time-varying complex networks was studied in Shen et al. [36]. The authors in Xiao et al. [37] designed a distributed finite-time filter for discrete-time networked systems with Deception attacks. In practice, DoS attacks and Deception attacks may be launched simultaneously, which will result in more severe damage of networked systems. Thus, the hybrid DoS and Deception attacks are considered in this paper.

On the basis of the above investigations, this paper dedicates to design an effective H_∞ filter for discrete-time networked systems with AETM and hybrid cyber attacks. To the best of our knowledge, none of the existed researches studies the H_∞ filtering problem over discrete-time networked systems under the limited bandwidth and hybrid cyber attacks scenario. Meanwhile, the main contributions of this paper are listed as below:

- In order to save limited network resources, an AETM is applied into the considered discrete-time networked systems to adaptively reduce redundant data transmission.
- Based on the employed AETM, a filtering error system model is established under the hybrid cyber attacks scenario.
- By recurring to Lyapunov stability theory and linear matrix inequalities (LMIs) technology, a H_∞ filter with guaranteed stability is designed for the formulated filtering error system.

The remaining parts of this paper are organized as follows. The mathematical model of filtering error system under the AETM and hybrid cyber attacks scenario is established in Section 2. The sufficient conditions that guaranteeing the asymptotic stability of the filtering error system are derived and the algorithm designing parameters of the filter is obtained in Section 3. In Section 4, the effectiveness of the work is verified via a simulated example.

Notation: In this paper, $\mathbb{R}^m$, $\mathbb{R}^n$, $\mathbb{R}^p$, $\mathbb{R}^q$ and $\mathbb{R}^l$ are used to denote the Euclidean space with appropriate dimensions, and N is the set of all non-negative integers. 0 represents matrix of compatible dimensions zero. The symbol $\|.\|$ means the Euclidean norm. The superscript T represents matrix transposition and the asterisk $*$ in a matrix stands for the term induced by summery. I refers to the identity matrix with appropriate dimensions. $\mathbb{L}_2[0,\infty)$ is the space of square summable vector-valued functions. Matrices, if not specified explicitly, are assumed to have compatible dimensions. $Pr\{.\}$ represents the probability.

2. System model and problem formulation

Given that the H_∞ filtering problem over discrete-time networked systems is exploited in this paper, the considered networked linear system model with discrete-time is firstly given

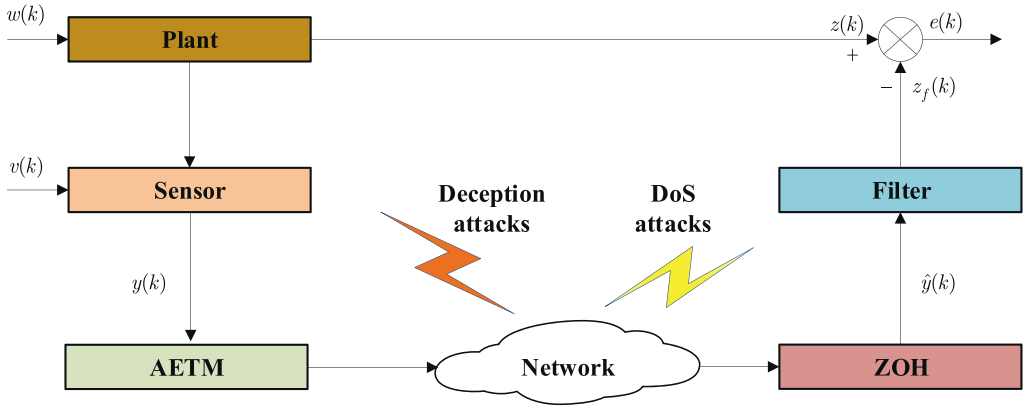

Fig. 1. The framework of discrete-time networked systems with AETM and hybrid cyber attacks.

as follows:

$$\begin{cases} x(k+1) = Ax(k) + Bw(k), \\ y(k) = Cx(k) + Dv(k), \\ z(k) = Lx(k). \end{cases} \tag{1}$$

In Eq. (1), $x(k) \in \mathbb{R}^m$, $y(k) \in \mathbb{R}^n$ and $z(k) \in \mathbb{R}^p$ are the system state, measured output and estimated signal, respectively; $w(k) \in \mathbb{R}^l$ and $v(k) \in \mathbb{R}^q$ are the disturbance input and measurable outside noise, and both of them belong to $\mathbb{L}_2[0, \infty)$. A, B, C, D, L are known constant matrices with appropriate dimensions.

Based on the above system model, the framework of the envisioned discrete-time networked systems with AETM and hybrid cyber attacks is then presented in Fig. 1. As shown, whether the signal sent out by the sensor, i.e., $y(k)$, is released is determined by the AETM. Considering that the released data is transferred through the communication network, which is assumed to suffer from Deception attacks, DoS attacks and the zero-order-holder (ZOH), the $\hat{y}(k)$ is used to indicate the signal that finally arrived at the filter, the specific constitution of which will be introduced shortly.

According to the framework, the filter to be designed in this paper can be given as:

$$\begin{cases} x_f(k+1) = A_f x_f(k) + B_f \hat{y}(k), \\ z_f(k) = C_f x_f(k), \end{cases} \tag{2}$$

where, $x_f(k) \in \mathbb{R}^m$ and $z_f(k) \in \mathbb{R}^p$ are the state and output of the filter; A_f, B_f, C_f are the filtering parameters which will be designed later.

2.1. Adaptive event-triggered mechanism

In the progress of designing an effective filter, an AETM is adopted to relieve data transmission pressure of communication network. Let $k_0 \le k_1 \le \ldots \le k_s \le \ldots$ be the sequence of the triggered instants, then the next trigging instant can be depicted as:

$$k_{s+1} = k_s + \min_{i \in N} \left\{ i \mid \frac{1}{\theta} q(k) + \sigma y^T(k_s + i) y(k_s + i) - \phi^T(k)\phi(k) \le 0 \right\}. \tag{3}$$

In Eq. (3), θ and σ are the given positive scalars; $\phi(k) = y(k_s) - y(k_s + i)$, $y(k_s)$ and $y(k_s + i)$ are the measurable outputs at the latest triggered instant k_s and the current sampling instant $k_s + i$, respectively; $q(k)$ is the triggering threshold, which satisfies adaptive control law as follows:

$$q(k+1) = \lambda q(k) + \sigma y^T(k_s + i)y(k_s + i) - \phi^T(k)\phi(k). \tag{4}$$

where $\lambda \in (0, 1)$ is a given constant and $q(0) \geq 0$ denotes the initial condition.

Remark 1. Inspired by Li et al. [40], an AETM is adopted into the design of filter for discrete-time networked linear systems in this paper. Noting that the threshold $q(k)$ of AETM Eq. (3) is a dynamic parameter, which is adaptively adjusted according to the adaptive control law Eq. (4). Meanwhile, the AETM Eq. (3), in which the triggering condition changes depending on the states of system, shows the advantage on adaptively reducing the transmission of redundant data.

Remark 2. During data transmission, if the triggering condition Eq. (3) is satisfied, the new measurable signal $y(k_s + i)$ will be released into the communication network by the sensor, and vice versa. It is also would like to note that if $\theta \to +\infty$, the AETM will reduce to a static event-triggered mechanism, i.e.,

$$k_{s+1} = k_s + \min_{i \in N} \left\{ i \mid \sigma y^T(k_s + i)y(k_s + i) - \phi^T(k)\phi(k) \leq 0 \right\}. \tag{5}$$

2.2. Hybrid cyber attacks modeling

Before modeling the hybrid cyber attacks occurred in the communication network, the network-induced delay is firstly investigated. Similar to Yue et al. [23], the time interval $[k_s + \tau_{k_s}, k_{s+1} + \tau_{k_{s+1}})$ can be divided into $n + 1$ $(n = k_{s+1} - k_s - 1)$ subintervals:

$$[k_s + \tau_{k_s}, k_{s+1} + \tau_{k_{s+1}}) = \cup_{m=0}^{n} W_m^{k_s}. \tag{6}$$

where $\tau_{k_s} \in [0, \tau_M]$ is the network-induced delay of $y(k_s)$ and $W_m^{k_s} = [k_s + m + \tau_{k_s+m}, k_s + m + 1 + \tau_{k_s+m+1})$.

Defining $d(k) = k - k_s - m$ $(k \in W_m^{k_s})$, then it can be obtained:

$$0 \leq d(k) \leq \tau_M + 1 = d_M. \tag{7}$$

By introducing $d(k)$, the transmitted signal under network-induced delay can be denoted as:

$$\tilde{y}(k) = y(k - d(k)) + \phi(k). \tag{8}$$

Based on Eq. (8), we then try to model the considered hybrid cyber attacks, where the Deception attacks are always assumed to be launched before the DoS attacks. Under the Deception attacks, the real measurement signal, denoted by $\check{y}(k)$, can be defined as:

$$\check{y}(k) = (1 - \rho_k)\tilde{y}(k) + \rho_k h(\tilde{y}(k)). \tag{9}$$

where, ρ_k is a Bernoulli distributed white sequence used to represent the probability of the Deception attacks occurrence, it takes values on $\{0, 1\}$, i.e., $\rho_k = 1$ indicates that the Deception attacks occur in the network and vice versa. The probability distribution of ρ_k satisfies $Pr\{\rho_k = 1\} = \bar{\rho}$ and $Pr\{\rho_k = 0\} = 1 - \bar{\rho}$ $(0 \leq \bar{\rho} \leq 1)$; $h(\tilde{y}(k))$ is the false data while the Deception attacks appear and it follows:

$$h^T(\tilde{y}(k))h(\tilde{y}(k)) \leq \tilde{y}^T(k)G^T G\tilde{y}(k), \tag{10}$$

in which G is a given constant matrix with appropriate dimension.

By further considering the DoS attacks and ZOH, the signal arrived at the filter, i.e., $\hat{y}(k)$, can be given as:

$$\hat{y}(k) = (1 - r_k)\check{y}(k) = (1 - r_k)\big[(1 - \rho_k)\tilde{y}(k) + \rho_k h(\tilde{y}(k))\big]. \tag{11}$$

Similar to ρ_k in the Deception attacks Eq. (9), r_k in Eq. (11) is a random variable satisfying Bernoulli distribution, which is used to denote the probability of the DoS attacks occurrence. It takes values in the set $\{0, 1\}$, i.e., $r_k = 1$ indicates that the DoS attacks occur in the network and vice versa. Besides, the probability distribution of r_k satisfies $Pr\{r_k = 1\} = \bar{r}$ and $Pr\{r_k = 0\} = 1 - \bar{r}$ $(0 \le \bar{r} \le 1)$.

Specially, in practical systems, the attacks may be launched by different adversaries, and one attacker generally does not know the existence of the other attackers. In view of this, we do not consider the influence of one type of attacks on the other type of attacks in this study.

Remark 3. Comparing with the single type of attacks, i.e., DoS attacks or Deception attacks, the considered hybrid cyber attacks will inevitably complicate the control of the envisioned system given that the system may be affected by different types of attacks at different instants. Then, the filtering methods focused on the single type of attacks will become inefficient, which impels the research of filtering strategy under the hybrid cyber attacks.

Remark 4. Deception attacks are a type of integrity attacks that can pass detectors. Thus, many researches have been presented to design effective detectors so as to identify or defense various forms of Deception attacks [41,42]. Although the Deception attacks are also considered in this study, but we follow a different research route that to design effective control strategy so as to guarantee the stability of the envisioned system compromised by the Deception attacks.

Remark 5. In practical systems, the specific order of cyber attacks occurrence is unknown in advance. In this paper, it is assumed that the hybrid cyber attacks occur in the following order: the Deception attacks $\rightarrow$ the DoS attacks. By simply extending the above proposed modeling approach, the hybrid cyber attacks model can also be designed for the circumstance that the DoS attacks occur before the Deception attacks.

Remark 6. In Eq. (11), the hybrid cyber attacks are depicted by two random variables, i.e., ρ_k and r_k, $\rho_k = 1$ and $r_k = 1$ indicate that both of the Deception attacks and DoS attacks are launched by hackers relatively, $\rho_k = 0$ and $r_k = 0$ represent that the communication network is secure without danger of attacks, $\rho_k = 1$ and $r_k = 0$ ($\rho_k = 0$ and $r_k = 1$) denote that only the Deception attacks (the DoS attacks) occur in the network.

2.3. Formulation of the filtering error system

Let $\xi(k) = \begin{bmatrix} x^T(k) & x_f^T(k) \end{bmatrix}^T$, $e(k) = z(k) - z_f(k)$, then the filtering error system resulting from Eqs. (1), (2), (3), (8) and (11) can be formulated as:

$$\begin{cases} \xi(k+1) = \bar{A}\xi(k) + \bar{B}\xi(k - d(k)) + \bar{C}\hat{w}(k) + \bar{D}_1\phi(k) + \bar{D}_2 h(k), \\ e(k) = \bar{E}\xi(k), \end{cases} \tag{12}$$

where,

$$\bar{A} = \begin{bmatrix} A & 0 \\ 0 & A_f \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} 0 & 0 \\ (1 - r_k)(1 - \rho_k)B_f C & 0 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} B & 0 \\ 0 & (1 - r_k)(1 - \rho_k)B_f D \end{bmatrix},$$

$$\hat{w}(k)=\begin{bmatrix} w(k) \\ v(k-d(k)) \end{bmatrix},\quad \bar{D}_1=\begin{bmatrix} 0 \\ (1-r_k)(1-\rho_k)B_f \end{bmatrix},\quad \bar{D}_2=\begin{bmatrix} 0 \\ \rho_k(1-r_k)B_f \end{bmatrix},$$
$$\bar{E}=\begin{bmatrix} L & -C_f \end{bmatrix},\quad h(k)=h(y(k-d(k))+\phi(k)).$$

For easy description, define $y(k-d(k))=\bar{F}_1\xi(k-d(k))+\bar{F}_2\hat{w}(t)$, where $\bar{F}_1=\begin{bmatrix} C & 0 \end{bmatrix}$ and $\bar{F}_2=\begin{bmatrix} 0 & D \end{bmatrix}$.

Before giving the main results derived in this study, the following definition and lemmas should be firstly introduced.

Definition 1 [43]**.** Let $\gamma>0$ be a given attenuation level, then for all nonzero $\hat{w}(k)\in\mathbb{L}_2[0,\infty)$, the filtering error system Eq. (12) is asymptotic stable and the H_∞ performance is guaranteed only when $e(k)$ and $\hat{w}(k)$ satisfy:

$$\sum_{k=0}^{+\infty}\mathbb{E}\{\|e(k)\|^2\}\le\gamma^2\sum_{k=0}^{+\infty}\mathbb{E}\{\|\hat{w}(k)\|^2\}. \tag{13}$$

Lemma 1 [44]**.** *For any scalars $x,\ y\in\mathbb{R}^n$ and positive definite matrix $Z\in\mathbb{R}^{n\times n}$, it can be obtained that:*

$$2x^Ty\le x^TZx+y^TZ^{-1}y. \tag{14}$$

Lemma 2 [43]**.** *For given matrices $\Omega,\ \Omega_1,\ \Omega_2$ with appropriate dimensions and $\tau(k)\in[\tau_1,\tau_2]$, $(\tau(k)-\tau_1)\Omega_1+(\tau_2-\tau(k))\Omega_2+\Omega<0$ holds only while:*

$$\begin{cases}(\tau_2-\tau_1)\Omega_1+\Omega<0,\\ (\tau_2-\tau_1)\Omega_2+\Omega<0.\end{cases} \tag{15}$$

3. Main results

The main results of this paper are presented in form of two theorems in this section with their corresponding proofs. By using Lyapunov–Krasovskii stability theory and LMI techniques, the sufficient conditions guaranteeing the asymptotic stability of the filtering error system Eq. (12) and the algorithm designing parameters of filter will be obtained in Theorems 1 and 2, respectively.

3.1. Stability and H_∞ performance analysis

Theorem 1. *For given scalars $\theta,\ \sigma,\ \lambda,\ \bar{r},\ \bar{\rho},\ d_M,\ \gamma$ and matrices $A_f,\ B_f,\ C_f$, if there exist positive definite matrices $P,\ Q,\ R$ and free weighting matrices $M,\ N$ with appropriate dimensions such that the following matrices inequalities:*

$$\begin{bmatrix} \Gamma_{11} & (*) & (*) & (*) & (*) & (*) & (*) \\ \Gamma_{21}(s) & -R & (*) & (*) & (*) & (*) & (*) \\ \Gamma_{31} & 0 & -P & (*) & (*) & (*) & (*) \\ \Gamma_{41} & 0 & 0 & -R & (*) & (*) & (*) \\ \Gamma_{51} & 0 & 0 & 0 & -bI & (*) & (*) \\ \Gamma_{61} & 0 & 0 & 0 & 0 & -I & (*) \\ \Gamma_{71} & 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix}<0,\qquad s=1,2, \tag{16}$$

hold, in which,

$$a = 1 + \frac{1}{\theta} - \lambda, \quad b = \frac{1}{(1 + \frac{1}{\theta} - \lambda)\sigma}, \quad c = \sqrt{d_M + 1},$$

$$\Gamma_{11} = \begin{bmatrix} -P + Q + N_1 + N_1^T & (*) & (*) & (*) & (*) & (*) \\ N_2 - N_1^T + M_1^T & -N_2 - N_2^T + M_2 + M_2^T & (*) & (*) & (*) & (*) \\ N_3 - M_1^T & -N_3 + M_3 - M_2^T & -Q - M_3 - M_3^T & (*) & (*) & (*) \\ 0 & 0 & 0 & -\gamma^2 I & (*) & (*) \\ 0 & 0 & 0 & 0 & -aI & (*) \\ 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix},$$

$$\Gamma_{21}(1) = \begin{bmatrix} \sqrt{d_M} N_1^T & \sqrt{d_M} N_2^T & \sqrt{d_M} N_2^T & 0 & 0 & 0 \end{bmatrix},$$

$$\Gamma_{21}(2) = \begin{bmatrix} \sqrt{d_M} M_1^T & \sqrt{d_M} M_2^T & \sqrt{d_M} M_3^T & 0 & 0 & 0 \end{bmatrix},$$

$$\Gamma_{41} = \begin{bmatrix} c(R\bar{A} - R) & cR\bar{B} & 0 & cR\bar{C} & cR\bar{D}_1 & cR\bar{D}_2 \end{bmatrix},$$

$$\Gamma_{31} = \begin{bmatrix} P\bar{A} & P\bar{B} & 0 & P\bar{C} & P\bar{D}_1 & P\bar{D}_2 \end{bmatrix},$$

$$\Gamma_{51} = \begin{bmatrix} 0 & \bar{F}_1 & 0 & \bar{F}_2 & 0 & 0 \end{bmatrix}, \quad \Gamma_{61} = \begin{bmatrix} 0 & G\bar{F}_1 & 0 & G\bar{F}_2 & G & 0 \end{bmatrix},$$

$$\Gamma_{71} = \begin{bmatrix} \bar{E} & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

then the augmented filtering error system Eq. (12) is asymptotic stable and satisfies the H_∞ performance under zero initial condition.

Proof. Constructing the following Lyapunov function:

$$V(k) = \sum_{i=1}^{4} V_i(k), \tag{17}$$

with

$$\begin{cases} V_1(k) = \xi^T(k) P \xi(k), \\ V_2(k) = \sum_{s=k-d_M}^{k-1} \xi^T(s) Q \xi(s), \\ V_3(k) = \sum_{s=-d_M}^{-1} \sum_{l=k+s}^{k-1} \delta^T(l) R \delta(l), \\ V_4(k) = \frac{1}{\theta} q(k), \end{cases} \tag{18}$$

where $\delta(l) = \xi(l+1) - \xi(l)$. Then, taking derivative of $V_i(k)$, it can be gotten:

$$\begin{cases} \triangle V_1(k) = \xi^T(k+1) P \xi(k+1) - \xi^T(k) P \xi(k), \\ \triangle V_2(k) = \xi^T(k) Q \xi(k) - \xi^T(k - d_M) Q \xi(k - d_M), \\ \triangle V_3(k) = (d_M + 1)\delta^T(k) R \delta(k) - \sum_{l=k-d_M}^{k} \delta^T(l) R \delta(l), \\ \triangle V_4(k) = \frac{1}{\theta}(q(k+1) - q(k)). \end{cases} \tag{19}$$

For $\triangle V_3(k)$, adopting the free weighting matrix method [45,46], it is clear that:

$$\triangle V_3(k) = \quad (d_M + 1)\delta^T(k) R \delta(k) - \sum_{l=k-d_M}^{k} \delta^T(l) R \delta(l) + \Upsilon_1 + \Upsilon_2, \tag{20}$$

where $\Upsilon_1 = 2\eta^T(k) N \left[\xi(k) - \xi(k - d(k)) - \sum_{j=k-d(k)}^{k} \delta(j) \right] = 0$, $\Upsilon_2 = 2\eta^T(k) M \left[\xi(k - d(k)) - \xi(k - d_M) - \sum_{k-d_M}^{k-d(k)} \delta(j) \right] = 0$, $\eta^T(k) = \left[\xi(k) \quad \xi(k - d(k)) \quad \xi(k - d_M) \right]^T$, $N = \begin{bmatrix} N_1 & N_2 & N_3 \end{bmatrix}$, $M = \begin{bmatrix} M_1 & M_2 & M_3 \end{bmatrix}$.

According to Lemma 1, it can be obtained that:

$$\begin{cases} -2\eta^T(k)N\sum_{j=k-d(k)}^{k}\delta(j) \le d(k)\eta^T(k)NR^{-1}N^T\eta(k) + \sum_{j=k-d(k)}^{k}\delta^T(j)R\delta(j), \\ -2\eta^T(k)M\sum_{j=k-d(k)}^{k-d(k)}\delta(j) \le (d_M - d(k))\eta^T(k)MR^{-1}M^T\eta(k) + \sum_{j=k-d_M}^{k-d(k)}\delta^T(j)R\delta(j). \end{cases} \tag{21}$$

Thus, combining Eqs. (20) and (21), it is obvious that:

$$\begin{aligned} \triangle V_3(k) \le & (d_M+1)\delta^T(k)R\delta(k) + 2\eta^T(k)N[\xi(k) - \xi(k-d(k))] \\ & + 2\eta^T(k)M[\xi(k-d(k)) - \xi(k-d_M)] \\ & + d(k)\eta^T(k)NR^{-1}N^T\eta(k) + (d_M - d(k))\eta^T(k)MR^{-1}M^T\eta(k). \end{aligned} \tag{22}$$

For $\triangle V_4(k)$, based on the introduced AETM Eq. (5) and adaptive control law Eq. (4), we have:

$$\begin{aligned} \triangle V_4(k) = & \frac{1}{\theta}(\lambda q(k) + \sigma y^T(k-d(k))y(k-d(k)) - \phi^T(k)\phi(k) - q(k)) \\ = & \frac{1}{\theta}(\lambda-1)q(k) + \frac{1}{\theta}(\sigma y^T(k-d(k))y(k-d(k)) - \phi^T(k)\phi(k)) \\ \le & (\lambda-1)(\phi^T(k)\phi(k) - \sigma y^T(k-d(k))y(k-d(k))) \\ & + \frac{1}{\theta}(\sigma y^T(k-d(k))y(k-d(k)) - \phi^T(k)\phi(k)) \\ \le & (\lambda - 1 - \frac{1}{\theta})\phi^T(k)\phi(k) - (\lambda - 1 - \frac{1}{\theta})\sigma y^T(k-d(k))y(k-d(k)). \end{aligned} \tag{23}$$

Based on Eqs. (17), (19), (22), (23) and (10), it is obtained:

$$\begin{aligned} \mathbb{E}\{\triangle V(k)\} = & \sum_{i=1}^{4}\mathbb{E}\{\triangle V_i(k)\} \\ \le & \mathbb{E}\{\xi^T(k+1)P\xi(k+1) - \xi^T(k)P\xi(k) + \xi^T(k)Q\xi(k) + (d_M+1)\delta^T(k)R\delta(k) \\ & - \xi^T(k-d_M)Q\xi(k-d_M) + 2\eta^T(k)N[\xi(k) - \xi(k-d(k))] \\ & + 2\eta^T(k)M[\xi(k-d(k)) - \xi(k-d_M)] + d(k)\eta^T(k)NR^{-1}N^T\eta(k) \\ & + (d_M - d(k))\eta^T(k)MR^{-1}M^T\eta(k) + (\lambda - 1 - \frac{1}{\theta})\phi^T(k)\phi(k) \\ & - (\lambda - 1 - \frac{1}{\theta})\sigma y^T(k-d(k))y(k-d(k)) \\ & - h^T(y(k-d(k)) + \phi(k))h(y(k-d(k)) + \phi(k)) \\ & + \left[y(k-d(k)) + \phi(k)\right]^T G^T G\left[y(k-d(k)) + \phi(k)\right]\} \\ = & \mathbb{E}\{\zeta^T(k)\Phi_1\zeta(k) + d(k)\eta^T(k)NR^{-1}N^T\eta(k) + (d_M - d(k))\eta^T(k)MR^{-1}M^T\eta(k)\}, \end{aligned} \tag{24}$$

where $\zeta^T(k) = \left[\xi(k) \quad \xi(k-d(k)) \quad \xi(k-d_M) \quad \hat{w}(k) \quad \phi(k) \quad h(k)\right]^T$,

$$\Phi_1 = \begin{bmatrix} \Lambda_{11} & (*) & (*) & (*) & (*) \\ \Gamma_{31} & -P & (*) & (*) & (*) \\ \Gamma_{41} & 0 & -R & (*) & (*) \\ \Gamma_{51} & 0 & 0 & -bI & (*) \\ \Gamma_{61} & 0 & 0 & 0 & -I \end{bmatrix},$$

in which,

$$\Lambda_{11}=\begin{bmatrix} -P+Q+N_1+N_1^T & (*) & (*) & (*) & (*) & (*) \\ N_2-N_1^T+M_1^T & -N_2-N_2^T+M_2+M_2^T & (*) & (*) & (*) & (*) \\ N_3-M_1^T & -N_3+M_3-M_2^T & -Q-M_3-M_3^T & (*) & (*) & (*) \\ 0 & 0 & 0 & 0 & (*) & (*) \\ 0 & 0 & 0 & 0 & -aI & (*) \\ 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix}.$$

Then the $\mathbb{E}\{\triangle V(k)\}$ can be rewritten as:

$$\begin{aligned}\mathbb{E}\{\triangle V(k)\} &= \mathbb{E}\left\{\triangle V(k)+e^T(k)e(k)-\gamma^2\hat{w}^T(k)\hat{w}(k)\right\}-\mathbb{E}\left\{e^T(k)e(k)-\gamma^2\hat{w}^T(k)\hat{w}(k)\right\}\\ &\le \mathbb{E}\left\{\zeta^T(k)\Phi_2\zeta(k)+d(k)\eta^T(k)NR^{-1}N^T\eta(k)+(d_M-d(k))\eta^T(k)MR^{-1}M^T\eta(k)\right\}\\ &\quad-\mathbb{E}\left\{e^T(k)e(k)-\gamma^2\hat{w}^T(k)\hat{w}(k)\right\}, \end{aligned} \tag{25}$$

where,

$$\Phi_2=\begin{bmatrix} \Gamma_{11} & (*) & (*) & (*) & (*) & (*) \\ \Gamma_{31} & -P & (*) & (*) & (*) & (*) \\ \Gamma_{41} & 0 & -R & (*) & (*) & (*) \\ \Gamma_{51} & 0 & 0 & -bI & (*) & (*) \\ \Gamma_{61} & 0 & 0 & 0 & -I & (*) \\ \Gamma_{71} & 0 & 0 & 0 & 0 & -I \end{bmatrix}.$$

So, for $k\in[0,T]$, it can be obtained that:

$$\begin{aligned}&\sum_{k=0}^{T}\mathbb{E}\{\triangle V(k)\}\\ &\le\sum_{k=0}^{T}\mathbb{E}\left\{\zeta^T(k)\Phi_2\zeta(k)+d(k)\eta^T(k)NR^{-1}N^T\eta(k)+(d_M-d(k))\eta^T(k)MR^{-1}M^T\eta(k)\right\}\\ &-\sum_{k=0}^{T}\mathbb{E}\{e^T(k)e(k)\}+\sum_{k=0}^{T}\mathbb{E}\{\gamma^2\hat{w}^T(k)\hat{w}(k)\},\end{aligned} \tag{26}$$

which means that:

$$\begin{aligned}&\mathbb{E}\left\{\sum_{k=0}^{T}\|e(k)\|^2\right\}-\gamma^2\mathbb{E}\left\{\sum_{k=0}^{T}\|\hat{w}(k)\|^2\right\}\\ &\le\sum_{k=0}^{T}\mathbb{E}\left\{\zeta^T(k)\Phi_2\zeta(k)+d(k)\eta^T(k)NR^{-1}N^T\eta(k)+(d_M-d(k))\eta^T(k)MR^{-1}M^T\eta(k)\right\}\\ &\quad-\mathbb{E}\{V(k+1)\}+\mathbb{E}\{V(0)\}.\end{aligned} \tag{27}$$

Given the zero initial condition, i.e., $V(0)=0$, then it is clear that:

$$\begin{aligned}&\mathbb{E}\left\{\sum_{k=0}^{T}\|e(k)\|^2\right\}-\gamma^2\mathbb{E}\left\{\sum_{k=0}^{T}\|\hat{w}(k)\|^2\right\}\\ &\le\sum_{k=0}^{T}\mathbb{E}\left\{\zeta^T(k)\Phi_2\zeta(k)+d(k)\eta^T(k)NR^{-1}N^T\eta(k)+(d_M-d(k))\eta^T(k)MR^{-1}M^T\eta(k)\right\}\end{aligned}$$

$$
\begin{aligned}
&-\mathbb{E}\{V(k+1)\}\\
&\le \sum_{k=0}^{T}\mathbb{E}\left\{\zeta^T(k)\Phi_2\zeta(k)+d(k)\eta^T(k)NR^{-1}N^T\eta(k)+(d_M-d(k))\eta^T(k)MR^{-1}M^T\eta(k)\right\}. \qquad (28)
\end{aligned}
$$

Let $T\to+\infty$, it can be further gotten:

$$
\begin{aligned}
&\sum_{k=0}^{+\infty}\mathbb{E}\left\{\|e(k)\|^2\right\}-\gamma^2\sum_{k=0}^{+\infty}\mathbb{E}\left\{\|\hat{w}(k)\|^2\right\}\\
&\le \sum_{k=0}^{+\infty}\mathbb{E}\left\{\zeta^T(k)\Phi_2\zeta(k)+d(k)\eta^T(k)NR^{-1}N^T\eta(k)+(d_M-d(k))\eta^T(k)MR^{-1}M^T\eta(k)\right\}. \qquad (29)
\end{aligned}
$$

Based on Eq. (29) and Definition 1, the filtering error system is asymptotic stable and satisfies H_∞ performance only while:

$$
\sum_{k=0}^{+\infty}\mathbb{E}\left\{\zeta^T(k)\Phi_2\zeta(k)+d(k)\eta^T(k)NR^{-1}N^T\eta(k)+(d_M-d(k))\eta^T(k)MR^{-1}M^T\eta(k)\right\}\le 0. \qquad (30)
$$

According to Lemma 2, inequality Eq. (30) holds only if:

$$
\begin{cases}
\zeta^T(k)\Phi_2\zeta(k)+d_M\eta^T(k)NR^{-1}N^T\eta(k)\le 0,\\
\zeta^T(k)\Phi_2\zeta(k)+d_M\eta^T(k)MR^{-1}M^T\eta(k)\le 0.
\end{cases} \qquad (31)
$$

By using Schur implement theory, noting that if inequalities in Eq. (16) are satisfied, then the Eq. (31) hold, that is to say, the filtering error system Eq. (12) is asymptotic stable and satisfies H_∞ performance. So far, the theorem is proved. □

In Theorem 1, the sufficient conditions that guaranteeing the asymptotic stability and H_∞ performance of the considered filtering error system Eq. (12) are derived. In the next subsection, the algorithm to design A_f, B_f, C_f based on the deductions above will be proposed.

3.2. H_∞ filter design

Theorem 2. *For given scalars θ, σ, λ, $\bar{r}$, $\bar{\rho}$, d_M and γ, if there exist matrices $P_1>0$, $P_2>0$, $Q_1>0$, $Q_2>0$, $R_1>0$, $R_2>0$, P_3, Q_3, R_3, M_i, N_i $(i\in\{1,2,3\})$, $\hat{Y}_j$, $\bar{Y}_j$ $(j\in\{1,2,3,4\})$ and Y_c with appropriate dimensions, such that the following LMIs:*

$$
\begin{bmatrix}
\Pi_{11} & (*) & (*) & (*) & (*) & (*) & (*)\\
\Pi_{21}(s) & -R & (*) & (*) & (*) & (*) & (*)\\
\Pi_{31} & 0 & -P & (*) & (*) & (*) & (*)\\
\Pi_{41} & 0 & 0 & -R & (*) & (*) & (*)\\
\Pi_{51} & 0 & 0 & 0 & -bI & (*) & (*)\\
\Pi_{61} & 0 & 0 & 0 & 0 & -I & (*)\\
\Pi_{71} & 0 & 0 & 0 & 0 & 0 & -I
\end{bmatrix}<0,\quad s=1,2, \qquad (32)
$$

are satisfied, where,

$$\Pi_{11}=\begin{bmatrix} -P+Q+N_1+N_1^T & (*) & (*) & (*) & (*) & (*) \\ N_2-N_1^T+M_1^T & -N_2-N_2^T+M_2+M_2^T & (*) & (*) & (*) & (*) \\ N_3-M_1^T & -N_3+M_3-M_2^T & -Q-M_3-M_3^T & (*) & (*) & (*) \\ 0 & 0 & 0 & -\gamma^2 I & (*) & (*) \\ 0 & 0 & 0 & 0 & -aI & (*) \\ 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix},$$

$$P=\begin{bmatrix} P_1 & (*) \\ P_3 & P_2 \end{bmatrix},\quad Q=\begin{bmatrix} Q_1 & (*) \\ Q_3 & Q_2 \end{bmatrix},\quad R=\begin{bmatrix} R_1 & (*) \\ R_3 & R_2 \end{bmatrix},$$

$$\Pi_{21}(1)=\begin{bmatrix} \sqrt{d_M}N_1^T & \sqrt{d_M}N_2^T & \sqrt{d_M}N_3^T & 0 & 0 & 0 \end{bmatrix},$$

$$\Pi_{21}(2)=\begin{bmatrix} \sqrt{d_M}M_1^T & \sqrt{d_M}M_2^T & \sqrt{d_M}M_3^T & 0 & 0 & 0 \end{bmatrix},$$

$$\Pi_{31}=\begin{bmatrix} \Pi_{311} & \Pi_{312} & \Pi_{313} \end{bmatrix},$$

$$\Pi_{311}=\begin{bmatrix} P_1A & \hat{Y}_2 & (1-\bar{r})(1-\bar{\rho})\bar{Y}_2C & 0 \\ P_3A & \hat{Y}_1 & (1-\bar{r})(1-\bar{\rho})\bar{Y}_1C & 0 \end{bmatrix},\quad \Pi_{312}=\begin{bmatrix} 0 & 0 & P_1B & (1-\bar{r})(1-\bar{\rho})\bar{Y}_2D \\ 0 & 0 & P_3B & (1-\bar{r})(1-\bar{\rho})\bar{Y}_1D \end{bmatrix},$$

$$\Pi_{313}=\begin{bmatrix} (1-\bar{r})(1-\bar{\rho})\bar{Y}_2 & \bar{\rho}(1-\bar{r})\bar{Y}_2 \\ (1-\bar{r})(1-\bar{\rho})\bar{Y}_1 & \bar{\rho}(1-\bar{r})\bar{Y}_1 \end{bmatrix},\quad \Pi_{41}=\begin{bmatrix} \Lambda_1 & \Lambda_2 & 0 & \Lambda_3 & \Lambda_4 \end{bmatrix},$$

$$\Lambda_1=\begin{bmatrix} c(R_1A-R_1) & c(\hat{Y}_4-R_3^T) \\ c(R_3A-R_3) & c(\hat{Y}_3-R_2) \end{bmatrix},\quad \Lambda_2=\begin{bmatrix} c(1-\bar{r})(1-\bar{\rho})\bar{Y}_4C & 0 \\ c(1-\bar{r})(1-\bar{\rho})\bar{Y}_3C & 0 \end{bmatrix},$$

$$\Lambda_3=\begin{bmatrix} cR_1B & c(1-\bar{r})(1-\bar{\rho})\bar{Y}_4D \\ cR_3B & c(1-\bar{r})(1-\bar{\rho})\bar{Y}_3D \end{bmatrix},\quad \Lambda_4=\begin{bmatrix} c(1-\bar{r})(1-\bar{\rho})\bar{Y}_4 & c\bar{\rho}(1-\bar{r})\bar{Y}_4 \\ c(1-\bar{r})(1-\bar{\rho})\bar{Y}_3 & c\bar{\rho}(1-\bar{r})\bar{Y}_3 \end{bmatrix},$$

$$\Pi_{51}=\begin{bmatrix} 0 & 0 & C & 0 & 0 & 0 & 0 & D & 0 & 0 \end{bmatrix},$$

$$\Pi_{61}=\begin{bmatrix} 0 & 0 & GC & 0 & 0 & 0 & 0 & GD & G & 0 \end{bmatrix},$$

$$\Pi_{71}=\begin{bmatrix} L & -Y_c & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

then the augmented filtering error system Eq. (12) is asymptotic stable and satisfies H_∞ performance under zero initial condition, and the parameters of the designed filter are:

$$\begin{cases} A_f=P_2^{-1}\hat{Y}_1, \\ B_f=P_2^{-1}\bar{Y}_1, \\ C_f=Y_c, \end{cases} \tag{33}$$

Proof. Based on Theorem 1, defining the following matrices:

$$\begin{cases} P_2A_f=\hat{Y}_1, \\ P_3^TA_f=\hat{Y}_2, \\ R_2A_f=\hat{Y}_3, \\ R_3^TA_f=\hat{Y}_4, \end{cases}\quad \begin{cases} P_2B_f=\bar{Y}_1, \\ P_3^TB_f=\bar{Y}_2, \\ R_2B_f=\bar{Y}_3, \\ R_3^TB_f=\bar{Y}_4, \end{cases}\quad C_f=Y_c, \tag{34}$$

by using the above definitions, the matrices inequalities in Eq. (16) can be transformed into LMIs in Eq. (32) and the parameters of the designed filter can be expressed as: $A_f=P_2^{-1}\hat{Y}_1$, $B_f=P_2^{-1}\bar{Y}_1$ and $C_f=Y_c$. Thus, the theorem can be obtained. □

Remark 7. The H_∞ filtering problem has been widely exploited in literatures [47–50]. For instance, under the limited network resources scenario, H_∞ filters were designed for switch-based filtering networks and nonlinear networked systems in Zhang et al. [47] and Zhao

et al. [48], respectively; while considering the existence of cyber-attacks, the authors in Gong et al. [49] designed an asynchronous distributed H_∞ filter for sensor networks with hidden Markovian switching policy, and the authors in Cheng et al. [50] proposed a hierarchical structure approach to design H_∞ filter for fuzzy Markov switching systems. However, differing from these existed works, our study takes both limited network resources and hybrid cyber attacks, i.e., Deception attacks and DoS attacks, into accounts, and then designs an efficient H_∞ filter for discrete-time networked systems. Under such complicated network environment and specific research objective, different system model, analysis and validation processes are further presented in the paper.

4. Numerical example

In this section, an example is given to demonstrate the effectiveness and applicability of the designed H_∞ filter. For this, given a discrete-time networked linear system Eq. (1) with the following parameters:

$$A=\begin{bmatrix}-0.5 & -0.4\\ 1 & -0.1\end{bmatrix},\quad B=\begin{bmatrix}0.1\\ 0.4\end{bmatrix},\quad C=\begin{bmatrix}1 & -0.2\end{bmatrix},\quad D=0.6,\quad L=\begin{bmatrix}-0.1 & 0.5\end{bmatrix}.$$

The employed AETM and constructed hybrid cyber attacks model are depicted by: $\theta=1.5$, $\lambda=0.8$, $\sigma=0.9$, $q(0)=0$, $d_M=2$, $\bar{r}=0.4$, $\bar{\rho}=0.3$, the matrix G in Deception attacks is given as $G=[0.1\quad 0.1]^T$, and the H_∞ performance level γ is set to be 1.6733.

Based on the above settings, by solving the LMIs Eq. (32) in Theorem 2, it can be gotten that:

$$P_2=\begin{bmatrix}78.8614 & -0.0876\\ -0.0876 & 78.8174\end{bmatrix},\bar{Y}_1=\begin{bmatrix}0.0822\\ -0.3907\end{bmatrix},\hat{Y}_1=\begin{bmatrix}-1.7340 & -2.6489\\ 2.1603 & -0.5855\end{bmatrix},$$
$$Y_c=\begin{bmatrix}0.0549 & -0.3271\end{bmatrix}.$$

According to Eq. (33), then the parameters of H_∞ filter can be derived as follows:

$$A_f=\begin{bmatrix}-0.0220 & -0.0336\\ 0.0274 & -0.0075\end{bmatrix},\quad B_f=\begin{bmatrix}0.0010\\ -0.0050\end{bmatrix},\quad C_f=\begin{bmatrix}0.0549 & -0.3271\end{bmatrix}.$$

Next, the initial conditions are assumed that: $x(0)=\begin{bmatrix}-0.21 & 0.3\end{bmatrix}^T$, $x_f(0)=\begin{bmatrix}-0.05 & 0.15\end{bmatrix}^T$, and the disturbance input and measurable noise function are given as:

$$w(k)=2*e^{-0.1*k},\quad v(k)=-e^{-0.2*k}.$$

Meanwhile, the function of Deception attacks is assumed to be:

$$h(y(k-d(k))+\phi(k))=0.1*\sin(-k)*(y(k-d(k))+\phi(k)).$$

The final simulation results are obtained by using MATLAB. From Figs. 2 and 3, it can be seen that the system tends to be stable and the filtering error changes to zero along the time, which represents the robust filtering performance on estimating the output of the origin system, and thus validates the effectiveness of the study. Furthermore, the adaptive control law $q(k)$, data release instants and intervals are shown in Figs. 4 and 5. It is clear that the $q(k)$ changes to zero when the system achieves stability. Besides, the simulated DoS attacks and Deception attacks are presented in Figs. 6 and 7, respectively.

Figs. 8 and 9 are given to verify the statement presented in Remark 3. In Figs. 8 and 9, we show the filtered signals under a strategy focused on the DoS (Deception) attacks, denoted

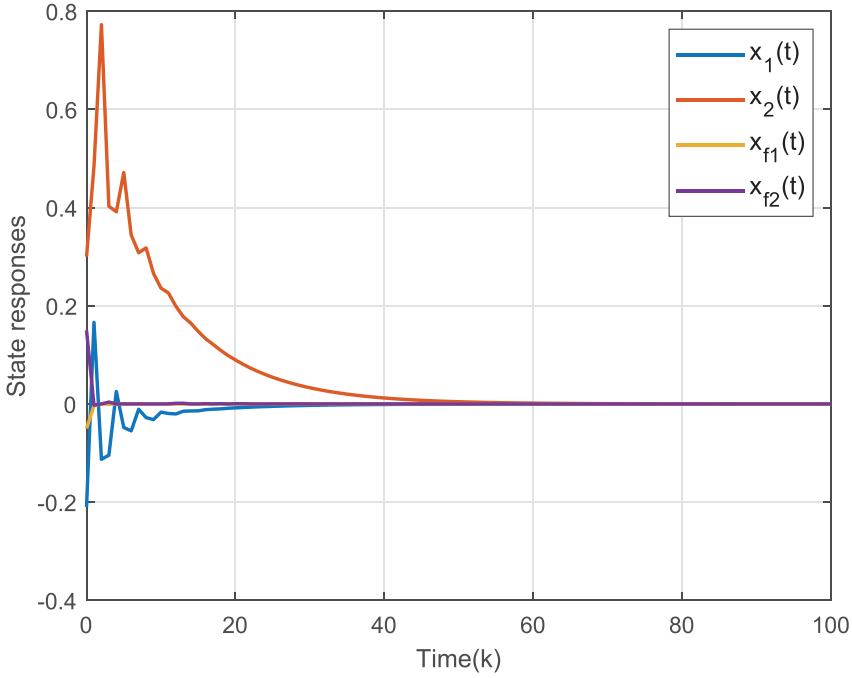

Fig. 2. State responses.

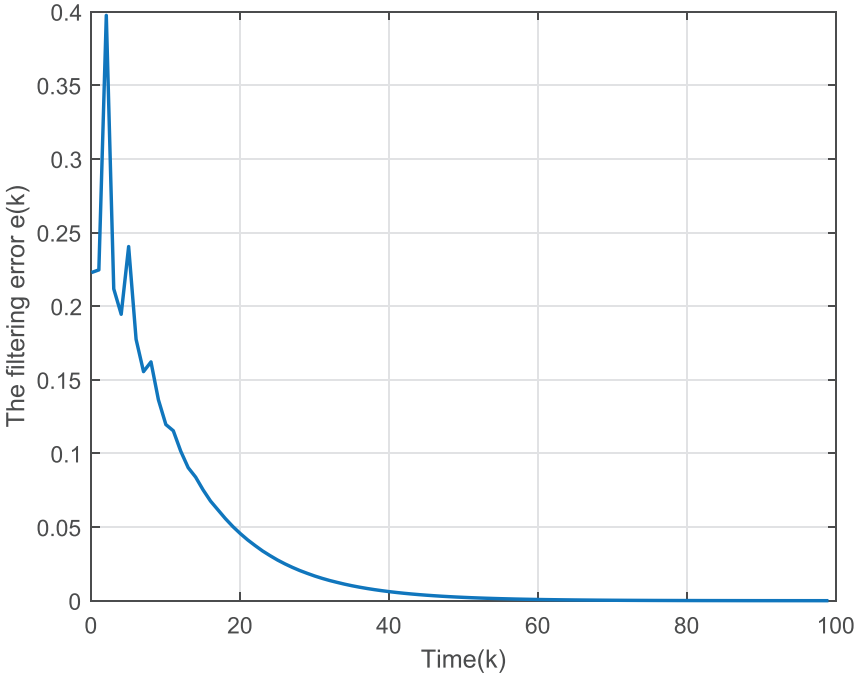

Fig. 3. Filtering error $e(k)$.

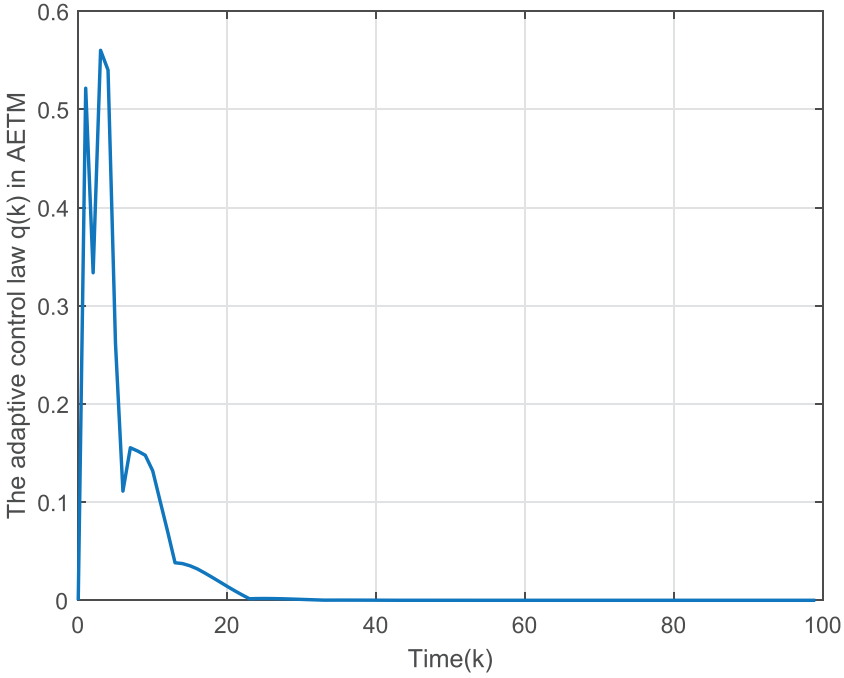

Fig. 4. The adaptive control law $q(k)$.

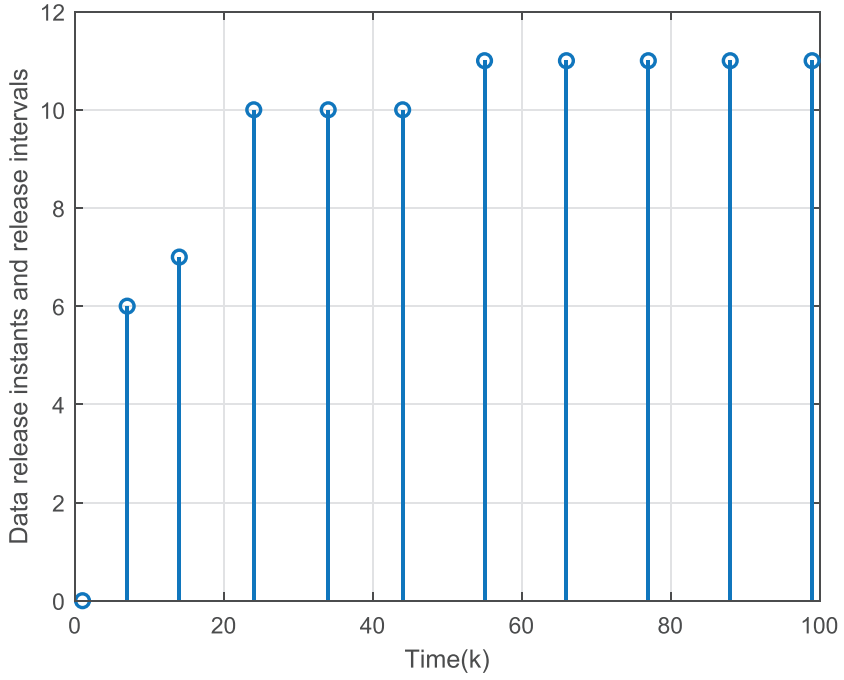

Fig. 5. Triggering instants and intervals.

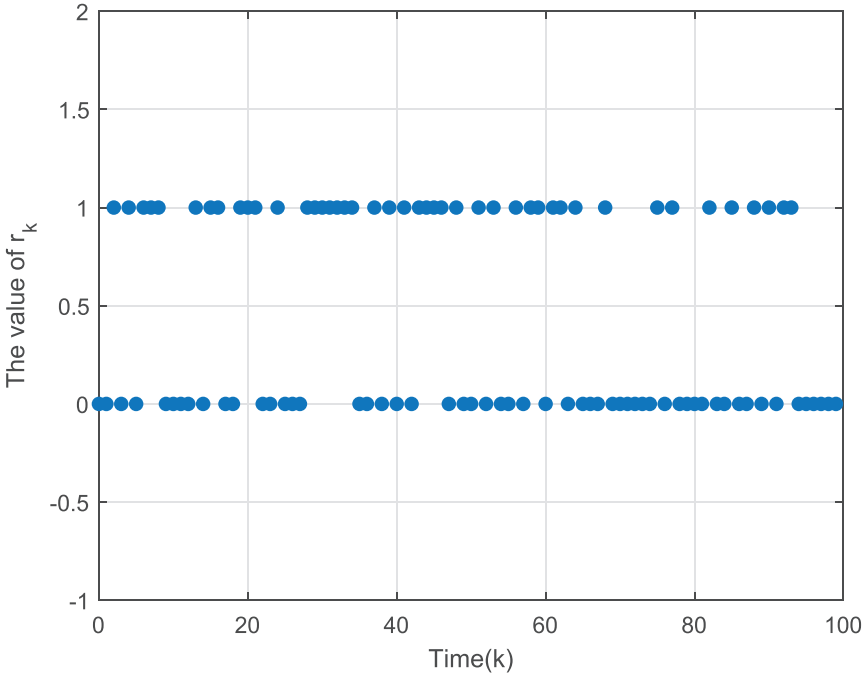

Fig. 6. Instants of the DoS attacks occurrence.

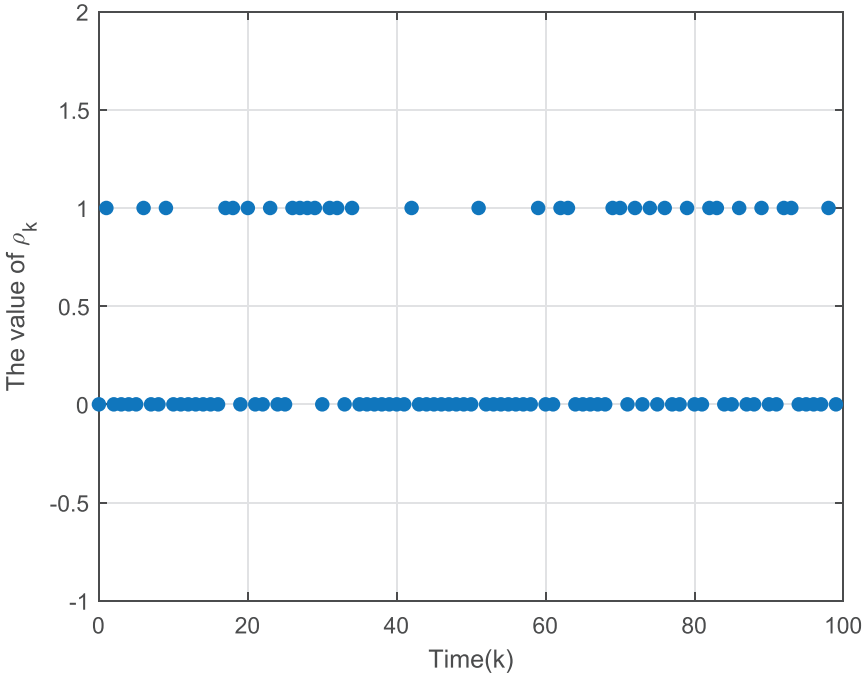

Fig. 7. Instants of the Deception attacks occurrence.

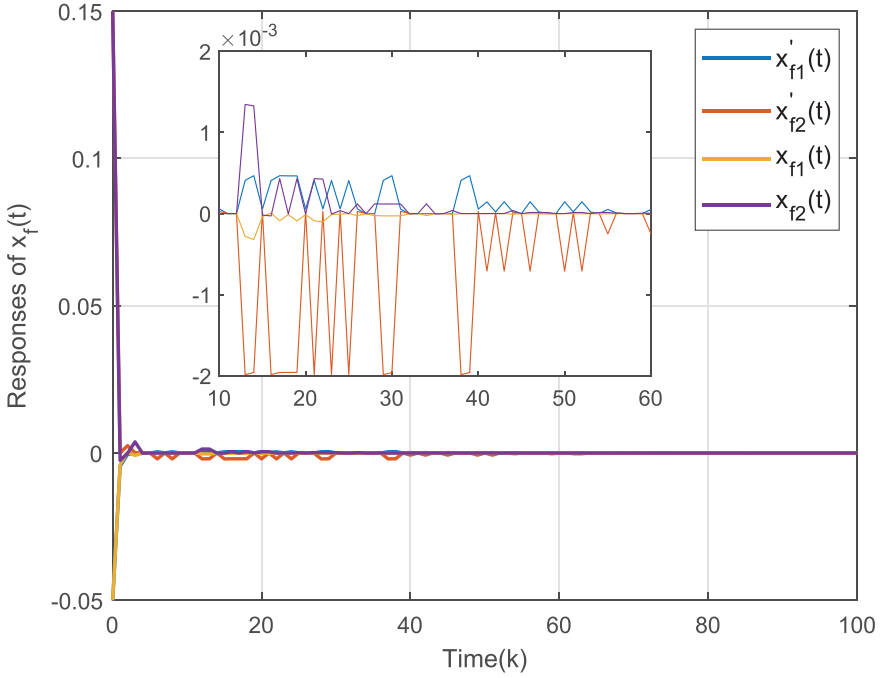

Fig. 8. Filtered signals under the strategy focused on the DoS attacks and the proposed strategy.

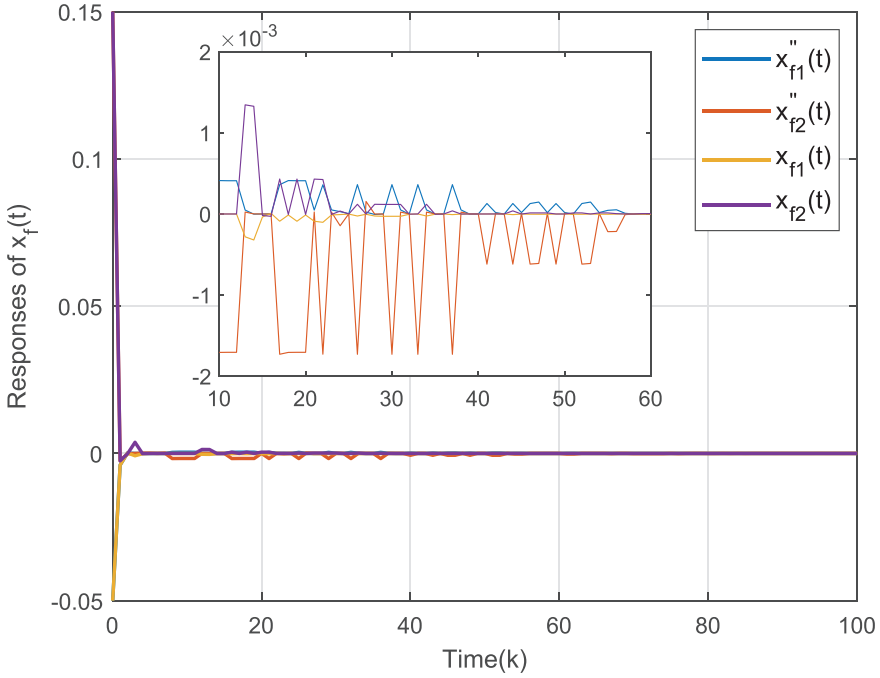

Fig. 9. Filtered signals under the strategy focused on the Deception attacks and the proposed strategy.

by $x'_{f1}(t)$ $(x''_{f1}(t))$ and $x'_{f2}(t)$ $(x''_{f2}(t))$, and that under the proposed strategy focused on the hybrid cyber attacks, i.e., $x_{f1}(t)$ and $x_{f2}(t)$. The strategy focused on the DoS (Deception) attacks is constructed by ignoring the Deception (DoS) attacks in the proposed method. As presented, the fluctuations of the filtered signals under the proposed strategy are much smaller than that under the strategies focused on the single type of attacks at the transient process, which confirms the significance of studying the hybrid cyber attacks.

5. Conclusion

In this paper, the H_∞ filtering problem is studied over discrete-time networked systems which lack sufficient network resources and suffer from various cyber attacks. To save the limited network bandwidth, an AETM is firstly introduced to reduce the transmission of redundant signals. In the AETM, the triggering threshold can be adaptively adjusted to response to the changes of system status. Then, a hybrid cyber attacks model is employed to depict the Deception attacks and DoS attacks occurred simultaneously. Based on the AETM and hybrid cyber attacks model, the considered filtering problem is formulated by establishing a filtering error system model. The sufficient conditions on the asymptotic stability and H_∞ performance of the constructed filtering error system are obtained by using Lyapunov stability theory, and the specific filtering parameters are also derived via LMI technique. Simulation results show that the robustness of the designed filter can be guaranteed under hybrid cyber attacks scenario. Given that the hybrid cyber attacks model is constructed based on fixed probabilities in this paper, a more realistic scenario is to construct a detector-based hybrid cyber attacks model, which will be the future work of us. Apparently, this work lays a good foundation for the future study.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grants 61973152 and 61903182, in part by Natural Science Foundation of Jiangsu Province of China under Grant BK20211290, in part by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 19KJA510005, in part by Fundamental Research on Advanced Leading Technology Project of Jiangsu Province under Grants BK20202011 and BK20192004C, and in part by the Qinglan Project of Jiangsu Province of China.

References

[1] Z. Gu, P. Shi, D. Yue, Z. Ding, Decentralized adaptive event-triggered H_∞ filtering for a class of networked nonlinear interconnected systems, IEEE Trans. Cybern. 49 (5) (2019) 1570–1579, doi:10.1109/TCYB.2018.2802044.

[2] P. Cheng, S. He, X. Luan, F. Liu, Finite-region asynchronous H_∞ control for 2D Markov jump systems, Automatica 129 (2021) 109590, doi:10.1016/j.automatica.2021.109590.

[3] P. Shi, X. Su, F. Li, Dissipativity-based filtering for fuzzy switched systems with stochastic perturbation, IEEE Trans. Autom. Control 61 (6) (2016) 1694–1699, doi:10.1109/TAC.2015.2477976.
[4] J. Liu, Y. Wang, J. Cao, D. Yue, X. Xie, Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack, IEEE Trans. Cybern. 51 (8) (2021) 4000–4010, doi:10.1109/TCYB.2020.3003752.
[5] E. Tian, W.K. Wong, D. Yue, T.-C. Yang, H_∞ filtering for discrete-time switched systems with known sojourn probabilities, IEEE Trans. Autom. Control 60 (9) (2015) 2446–2451, doi:10.1109/TAC.2015.2409909.
[6] X. Zhang, S. He, V. Stojanovic, X. Luan, F. Liu, Finite-time asynchronous dissipative filtering of conic-type nonlinear Markov jump systems, Sci. China Inf. Sci. 64 (5) (2021) 152206.
[7] W. Zhang, Q.-L. Han, Y. Tang, Y. Liu, Sampled-data control for a class of linear time-varying systems, Automatica 103 (2019) 126–134, doi:10.1016/j.automatica.2019.01.027.
[8] Z. Ke, B. Jiang, V. Cocquempot, H. Zhang, A framework of robust fault estimation observer design for continuous/discrete time system, Optim. Control Appl. Methods 34 (4) (2013) 442–457, doi:10.1002/oca.2031.
[9] Y. Zhong, Y. Liu, Flexible optimal Kalman filtering in wireless sensor networks with intermittent observations, J. Frankl. Inst. 358 (9) (2021) 5073–5088, doi:10.1016/j.jfranklin.2021.03.025.
[10] E. Tian, Z. Wang, L. Zou, D. Yue, Chance-constrained H_∞ control for a class of time-varying systems with stochastic nonlinearities: the finite-horizon case, Automatica 107 (2019) 296–305, doi:10.1016/j.automatica.2019.05.039.
[11] X. Chang, Z. Li, J.H. Park, Fuzzy generalized H_2 filtering for nonlinear discrete-time systems with measurement quantization, IEEE Trans. Syst., Man, Cybern. 48 (12) (2018) 2419–2430, doi:10.1109/TSMC.2017.2743012.
[12] Y. Shi, E. Tian, S. Shen, X. Zhao, Adaptive memory-event-triggered H_∞ control for network-based T-S fuzzy systems with asynchronous premise constraints, IET Control Theory Appl. 15 (4) (2021) 534–544, doi:10.1049/cth2.12059.
[13] J. Liu, M. Yang, X. Xie, C. Peng, H. Yan, Finite-time H_∞ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks, IEEE Trans. Circuits Syst. I 67 (3) (2020) 1021–1034, doi:10.1109/TCSI.2019.2949014.
[14] Z. Gu, J.H. Park, D. Yue, Z.-G. Wu, X. Xie, Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks, IEEE Trans. Syst., Man, Cybern. 51 (10) (2021) 6197–6206, doi:10.1109/TSMC.2019.2960115.
[15] Q. Liu, Z. Wang, X. He, D.H. Zhou, Event-based recursive distributed filtering over wireless sensor networks, IEEE Trans. Autom. Control 60 (9) (2015) 2470–2475, doi:10.1109/TAC.2015.2390554.
[16] K. Wang, E. Tian, J. Liu, L. Wei, D. Yue, Resilient control of networked control systems under deception attacks: a memory-event-triggered communication scheme, Int. J. Robust Nonlinear Control 30 (4) (2020) 1534–1548, doi:10.1002/rnc.4837.
[17] Z. Gu, P. Shi, D. Yue, S. Yan, X. Xie, Memory-based continuous event-triggered control for networked T-S fuzzy systems against cyber-attacks, IEEE Trans. Fuzzy Syst. (2020), doi:10.1109/TFUZZ.2020.3012771.
[18] W. Zhang, Y. Tang, Y. Liu, J. Kurths, Event-triggering containment control for a class of multi-agent networks with fixed and switching topologies, IEEE Trans. Circuits Syst. I 64 (3) (2017) 619–629, doi:10.1109/TCSI.2016.2618944.
[19] D. Ding, Z. Wang, Q. Han, A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks, IEEE Trans. Autom. Control 65 (4) (2020) 1792–1799, doi:10.1109/TAC.2019.2934389.
[20] J. Liu, T. Yin, M. Shen, X. Xie, J. Cao, State estimation for cyber physical systems with limited communication resources, sensor saturation and denial-of-service attacks, ISA Trans. 104 (2020) 101–114, doi:10.1016/j.isatra.2018.12.032.
[21] S. Yan, S.K. Nguang, Z. Gu, H_∞ weighted integral event-triggered synchronization of neural networks with mixed delays, IEEE Trans. Ind. Inf. 17 (4) (2021) 2365–2375, doi:10.1109/TII.2020.3004461.
[22] J. Liu, M. Yang, E. Tian, J. Cao, S. Fei, Event-based security control for state-dependent uncertain systems under hybrid-attacks and its application to electronic circuits, IEEE Trans. Circuits Syst. I 66 (12) (2019) 4817–4828, doi:10.1109/TCSI.2019.2930572.
[23] D. Yue, E. Tian, Q. Han, A delay system method for designing event-triggered controllers of networked control systems, IEEE Trans. Autom. Control 58 (2) (2013) 475–481, doi:10.1109/TAC.2012.2206694.
[24] P. Cheng, S. He, V. Stojanovic, X. Luan, F. Liu, Fuzzy fault detection for Markov jump systems with partly accessible hidden information: an event-triggered approach, IEEE Trans. Cybern. (2021), doi:10.1109/TCYB.2021.3050209.
[25] J. Liu, Y. Wang, L. Zha, X. Xie, E. Tian, An event-triggered approach to security control for networked systems using hybrid attack model, Int. J. Robust Nonlinear Control 31 (12) (2021) 5796–5812, doi:10.1002/rnc.5570.

[26] Z. Gu, D. Yue, E. Tian, On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems, Inf. Sci. 422 (2018) 257–270, doi:10.1016/j.ins.2017.09.005.
[27] M. Wang, Z. Wang, Y. Chen, W. Sheng, Adaptive neural event-triggered control for discrete-time strict-feedback nonlinear systems, IEEE Trans. Cybern. 50 (7) (2020) 2946–2958, doi:10.1109/TCYB.2019.2921733.
[28] C. Peng, J. Zhang, H. Yan, Adaptive event-triggering H_∞ load frequency control for network-based power systems, IEEE Trans. Ind. Electron. 65 (2) (2018) 1685–1694, doi:10.1109/TIE.2017.2726965.
[29] J. Cao, D. Ding, J. Liu, E. Tian, S. Hu, X. Xie, Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks, Inf. Sci. 548 (2021) 69–84, doi:10.1016/j.ins.2020.09.046.
[30] Z. Gu, P. Shi, D. Yue, An adaptive event-triggering scheme for networked interconnected control system with stochastic uncertainty, Int. J. Robust Nonlinear Control 27 (2) (2017) 236–251, doi:10.1002/rnc.3570.
[31] J. Liu, T. Yin, J. Cao, D. Yue, H.R. Karimi, Security control for T-S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks, IEEE Trans. Syst., Man, Cybern. 51 (10) (2021) 6544–6554, doi:10.1109/TSMC.2019.2963143.
[32] J. Liu, W. Suo, X. Xie, D. Yue, J. Cao, Quantized control for a class of neural networks with adaptive event-triggered scheme and complex cyber-attacks, Int. J. Robust Nonlinear Control 31 (10) (2021) 4705–4728, doi:10.1002/rnc.5500.
[33] W. Chen, D. Ding, H. Dong, G. Wei, Distributed resilient filtering for power systems subject to denial-of-service attacks, IEEE Trans. Syst., Man, Cybern. 49 (8) (2019) 1688–1697, doi:10.1109/TSMC.2019.2905253.
[34] E. Tian, X. Wang, C. Peng, Probabilistic-constrained distributed filtering for a class of nonlinear stochastic systems subject to periodic DoS attacks, IEEE Trans. Circuits Syst. I 67 (12) (2020) 5369–5379, doi:10.1109/TCSI.2020.3007953.
[35] S. Hu, D. Yue, C. Dou, X. Xie, Y. Ma, L. Ding, Attack-resilient event-triggered fuzzy interval type-2 filter design for networked nonlinear systems under sporadic denial-of-service jamming attacks, IEEE Trans. Fuzzy Syst. (2020), doi:10.1109/TFUZZ.2020.3033851.
[36] B. Shen, Z. Wang, D. Wang, Q. Li, State-saturated recursive filter design for stochastic time-varying nonlinear complex networks under deception attacks, IEEE Trans. Neural Netw. Learn. Syst. 31 (10) (2020) 3788–3800, doi:10.1109/TNNLS.2019.2946290.
[37] S. Xiao, Q.-L. Han, X. Ge, Y. Zhang, Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks, IEEE Trans. Cybern. 50 (3) (2020) 1220–1229, doi:10.1109/TCYB.2019.2900478.
[38] Y. Sun, J. Yu, X. Yu, H. Gao, Decentralized adaptive event-triggered control for a class of uncertain systems with deception attacks and its application to electronic circuits, IEEE Trans. Circuits Syst. I 67 (12) (2020) 5405–5416, doi:10.1109/TCSI.2020.3027678.
[39] J. Wu, C. Peng, J. Zhang, B. Zhang, Event-triggered finite-time H_∞ filtering for networked systems under deception attacks, J. Frankl. Inst. 357 (6) (2020) 3792–3808, doi:10.1016/j.jfranklin.2019.09.002.
[40] Q. Li, Z. Wang, W. Sheng, F.E. Alsaadi, F.E. Alsaadi, Dynamic event-triggered mechanism for H_∞ non-fragile state estimation of complex networks under randomly occurring sensor saturations, Inf. Sci. 509 (2020) 304–316, doi:10.1016/j.ins.2019.08.063.
[41] D. Wang, J. Huang, Y. Tang, F. Li, A watermarking strategy against linear deception attacks on remote state estimation under kl divergence, IEEE Trans. Ind. Inf. 17 (5) (2021) 3273–3281, doi:10.1109/TII.2020.3009874.
[42] W. Zhang, S. Mao, J. Huang, L. Kocarev, Y. Tang, Data-driven resilient control for linear discrete-time multi-agent networks under unconfined cyber-attacks, IEEE Trans. Circuits Syst. I 68 (2) (2021) 776–785, doi:10.1109/TCSI.2020.3037242.
[43] E. Tian, D. Yue, Y. Zhang, Delay-dependent robust H_∞ control for T-S fuzzy system with interval time-varying delay, Fuzzy Sets Syst. 160 (12) (2009) 1708–1719, doi:10.1016/j.fss.2008.10.014.
[44] Y. Wang, L. Xie, C.E. de Souza, Robust control of a class of uncertain nonlinear systems, Syst. Control Lett. 19 (2) (1992) 139–149, doi:10.1016/0167-6911(92)90097-C.
[45] S. Hu, X. Yin, Y. Zhang, Y. Ma, Further results on memory control of nonlinear discrete-time networked control systems with random input delay, Nonlinear Dyn. 77 (4) (2014) 1531–1545, doi:10.1007/s11071-014-1397-y.
[46] Y. He, M. Wu, J. She, G. Liu, Parameter-dependent Lyapunov functional for stability of time-delay systems with polytopic-type uncertainties, IEEE Trans. Autom. Control 49 (5) (2004) 828–832, doi:10.1109/TAC.2004.828317.
[47] H. Zhang, Z. Wang, H. Yan, F. Yang, X. Zhou, Adaptive event-triggered transmission scheme and H_∞ filtering co-design over a filtering network with switching topology, IEEE Trans. Cybern. 49 (12) (2019) 4296–4307, doi:10.1109/TCYB.2018.2862828.

[48] X. Zhao, C. Lin, B. Chen, Q.-G. Wang, Z. Ma, Adaptive event-triggered fuzzy H_∞ filter design for nonlinear networked systems, IEEE Trans. Fuzzy Syst. 28 (12) (2020) 3302–3314, doi:10.1109/TFUZZ.2019.2949764.

[49] C. Gong, G. Zhu, P. Shi, R.K. Agarwal, Asynchronous distributed finite-time H_∞ filtering in sensor networks with hidden Markovian switching and two-channel stochastic attacks, IEEE Trans. Cybern. (2020), doi:10.1109/TCYB.2020.2989320.

[50] J. Cheng, W. Huang, J.H. Park, J. Cao, A hierarchical structure approach to finite-time filter design for fuzzy Markov switching systems with deception attacks, IEEE Trans. Cybern. (2021), doi:10.1109/TCYB.2021.3049476.