Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 356 (2019) 10260–10276

www.elsevier.com/locate/jfranklin

Distributed event-triggered control for networked control systems with stochastic cyber-attacks

Jinliang Liu[a,*], Engang Tian[b], Xiangpeng Xie[c], Hong Lin[d]

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

[b] *School of Electrical and Automation Engineering, Nanjing Normal University, Nanjing, Jiangsu, China*

[c] *Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China*

[d] *Department of Mechanical Engineering, The University of Hong Kong, Hong Kong, China*

Received 27 October 2017; received in revised form 16 December 2017; accepted 28 January 2018
Available online 9 March 2018

Abstract

This paper is concerned with the problem of distributed event-triggered controller design for networked control systems (NCSs) with stochastic cyber-attacks. A decentralized event-triggered scheme is introduced to save the energy consumption and alleviate the transmission load of the network. Each sensor can make its own decision to determine whether the sampled data is delivered to the network or not. By taking two kinds of random cyber-attacks into consideration, a novel mathematical model is constructed for distributed event-triggered NCSs. Sufficient conditions which can guarantee the stability of the control system are obtained by applying Lyapunov stability theory, and the design method of the controller gain is presented in an exact expression. Finally, an example is given to demonstrate the effectiveness of the proposed method.

1. Introduction

NCSs consisting of sensors, controllers, actuators and networks play an increasingly significant role in the infrastructures of society, such as intelligent homes, smart grids and modern

[*] Corresponding author.
E-mail addresses: liujinliang@vip.163.com (J. Liu), teg@njnu.edu.cn (E. Tian), xiexiangpeng1953@163.com (X. Xie), linhongzju@163.com (H. Lin).

https://doi.org/10.1016/j.jfranklin.2018.01.048

public transportation systems [1–3]. There is no doubt that the insertion of network into the control systems brings about numerous advantages and convenience for its higher flexibility, lower complexity and cheaper cost in installation and maintenance [4,5]. Due to such superiorities of the NCSs, the popularity for investigations in NCSs continues and lots of fruitful results have been achieved. For example, in [6], the authors investigate the output feedback control problem for NCSs by considering signal quantization and data packet dropouts. The authors in [7] address the issue about the reliable control design for NCSs under the event-triggered scheme. In [8], the authors concentrate on the design of adaptive event-triggered scheme for nonlinear networked interconnected control systems via T-S fuzzy models. In [9], the event-triggered output feedback controller is designed for nonlinear NCSs in the framework of interval type-2 fuzzy systems.

However, the investigations of the NCSs pose some challenges in the aspects of the theories and applications [10]. As stated in [11], the problems of network-induced delay, package dropouts and external perturbations are unavoidable in NCSs. Time-triggered scheme inserted in NCSs is the first proposed transmission method in communication network. In order to alleviate the burden of the networked transmission more effectively, event-triggered scheme is proposed by lots of researchers to overcome the drawback of the time-triggered scheme. A novel event-triggered communication mechanism is proposed in [12] to determine whether the current sampled data is delivered to network or not. Motivated by the work in [12], improved event-triggered schemes are widely applied in controller and filter design problems [13]. For instances, the authors in [14] deal with the problem of an adaptive event-triggered communication scheme design for a class of T-S fuzzy control systems. In [15], the leader-following consensus problem of high-order multi-agent systems via event-triggered control is discussed. By considering the measured output quantization, the authors in [16] investigate the problem of H_∞ output feedback control for event-triggered Markovian jump systems. In [17], the authors solve the problem of event-triggered H_∞ filtering for networked systems by considering communication delay. Motivated by the aforementioned researches, this paper is concerned with the distributed event-triggered controller design for NCSs.

Recently, cyber security has become increasingly important with the development of the network and modern technology. When referring to system security, cyber-attacks may be regarded as one of the top offenders which aim to degrade the stability of the networked systems and deteriorate the system performance [18]. As described in [19], cyber-attacks are divided into three major categories including denial of service (DoS), replay attacks and deception attacks. Due to the considerable influence of the cyber-attacks, more and more scholars are interested in the investigations of cyber-attacks and achieve lots of outstanding results. In [20], the problem of fault-tolerant control for nonlinear chaotic is investigated by taking DoS attacks into consideration. The authors in [21] study the detection and isolation of replay attacks on sensor measurements for a multiplicative watermarking system. In [22], by taking the effect of deception attacks into consideration, the authors address the issue of distributed recursive filtering for a class of discrete time-delay systems. In [23], the authors investigate the problem of hybrid triggered H_∞ filter design for neural networks with deception attacks.

This paper is concerned with distributed event-triggered control for NCSs subject to two different kinds of cyber-attacks. In order to save the limited networked resources, event-triggered scheme is employed to determine whether the current sampled data is transmitted through the network. In this paper, large numbers of sensors are distributed in the cyber or physical space to sample data, and each sensor is equipped with an event-triggered scheme

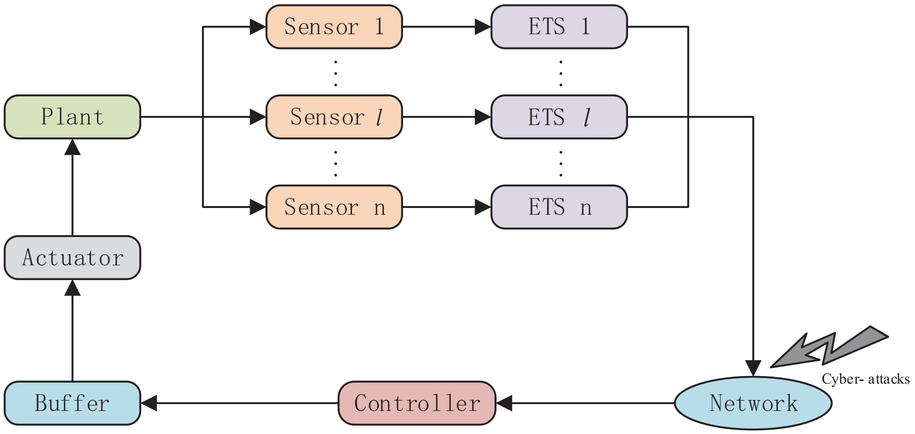

Fig. 1. The structure of distributed event-triggered networked control systems under cyber-attacks.

to make its own decision on the delivered data independently. Moreover, the influence of the cyber-attacks is also taken into consideration which is supposed as deception attacks. It should be pointed out that two different types of nonlinear functions are taken into account to describe the features of cyber-attacks. To the best of our knowledge, there is no research investigating the problem of distributed event-triggered control for NCSs with two kinds of cyber-attacks.

The rest of this paper is organized as follows. In Section 2, the problem of distributed event-triggered NCSs is described. In Section 3, sufficient conditions for the stability of the discussed system are derived by using Lyapunov stability theory, and the desired controller design method is obtained in terms of solutions to the linear matrix inequalities (LMIs). Finally, a numerical example is given to demonstrate the usefulness of the designed approach.

Notation: $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ denote the n-dimensional Euclidean space, and the set of $n\times m$ real matrices, respectively; the superscript T stands for matrix transposition; I is the identity matrix of appropriate dimension; the notation $X>0$, for $X\in\mathbb{R}^{n\times n}$ means that the matrix X is real symmetric positive definite; Prob$\{X\}$ denotes probability of event X to occur; $\mathbb{E}$ denotes the expectation operator; for a matrix B and two symmetric matrices A and C, $\begin{bmatrix} A & * \\ B & C \end{bmatrix}$ denotes a symmetric matrix, where * denotes the entries implied by symmetry.

2. Problem formulation

In this paper, the distributed event-triggered controller is designed for NCSs whose structure is shown in Fig. 1. An event-triggered generator is employed in each sensor side to save the limited network resources. The data released by the event generators is sent to the controller via an unreliable communication network subject to cyber-attacks. Considering the effect of distributed event-triggered scheme (ETS) and cyber-attacks, the stability of the distributed NCSs will be investigated.

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

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $u(t) \in \mathbb{R}^m$ is the control input vector. A and B are known matrices with appropriate dimensions.

Throughout this paper, the following assumptions are needed to facilitate the descriptions:

Assumption 1. The sensors and the controller are assumed to be connected over a communication network. The control output can be directly transmitted to the actuator through a ZOH. The communication network is facing the threats of randomly occurring cyber-attacks.

Assumption 2. The holding interval of zero-order-holder (ZOH) is $\Lambda_l = [t_k^l h + \tau_{t_k}^l, t_{k+1}^l h + \tau_{t_{k+1}}^l)$. h is the constant sampling period of each sensor, $t_k^l h$ denote the latest released instants of the event generator l. $\tau_{t_k}^l$ is the network-induced communication delay at the released instants $t_k^l h$, $\tau_M = \max_{l \in \{1,2,\ldots,n\}}\{\tau_{t_k}^l\}$.

Similar to the work in [24], the controller is designed as

$$u(t) = Kx(t_k h) \tag{2}$$

where $x(t_k h) = \begin{bmatrix} x^T(t_k^1 h) & x^T(t_k^2 h) & \cdots & x^T(t_k^n h) \end{bmatrix}^T$, $K = diag\{K_1, K_2, \ldots, K_n\}$ is the controller gain to be determined.

In this paper, suppose that the transmitted data over communication network is vulnerable to be attacked. The adversaries aim to attack the controller by modifying the control input and degrade the system performance. When the cyber-attacks are implemented, the controller can be expressed as

$$u(t) = Kx(t_k h) + \beta(t)K[\alpha(t)g(x(t-d(t))) + (1-\alpha(t))h(t-\eta(t)) - x(t_k h)] \tag{3}$$

where $d(t) \in [0, d_M]$ and $\eta(t) \in [0, \eta_M]$ represent the time delay of cyber-attacks, $d_M > 0$ and $\eta_M > 0$ denotes the maximum time delay. $\beta(t)$ and $\alpha(t)$ take values on $\{0, 1\}$ with prob$\{\beta(t) = 1\} = \bar{\beta}$ and prob$\{\alpha(t) = 1\} = \bar{\alpha}$. $\beta(t) = 1$ means the cyber-attacks occur, $\alpha(t) = 1$ means the cyber-attack function is $g(x(t-d(t)))$. $g(x(t))$ and $h(x(t))$ represent the different characteristics of the cyber-attacks.

Remark 1. In this paper, the cyber-attacks launched by a hacker are in the form $\alpha(t)g(x(t-d(t))) + (1-\alpha(t))h(t-\eta(t))$, which occur randomly and are governed by a Bernoulli distributed variable $\beta(t)$. It is possible for any hacker to modify the transmitted data in this way against the NCSs. This poses great challenge to the conventional control method. It is necessary to handle such cyber-attacks.

Remark 2. The attackers may send cyber-attacks against the communication channel for their own benefits. Due to the limited access to the system information and data authentication, the control system may be attacked randomly. $\beta(t)$ is adopted to describe the occurrence of the cyber-attacks. $\beta(t) = 1$ represents that the cyber-attacks are implemented successfully. Otherwise, $\beta(t) = 0$ means that the data is transmitted normally.

A distributed ETS is applied to reduce the communication burden of the network and the update frequency of the controller. For sensor l, when the latest released state is $x^l(t_k^l h)$, the sequence of the released time instants is determined by the following triggering condition [24]:

$$t_{k+1}^l h = t_k^l h + \min_{m^l \geq 0}\{m^l h \mid (e_k^l(t))^T \Omega_l e_k^l(t) > \sigma_l^2 (x^l(t_k^l h + m^l h))^T \Omega_l x^l(t_k^l h + m^l h)\} \tag{4}$$

in which $e_k^l(t) = x^l(t_k^l h) - x^l(t_k^l h + m^l h)$, $m^l = 0, 1, \ldots, M^l, M^l = t_{k+1}^l h - t_k^l h - 1$, Ω_l is a symmetric positive definite matrix, $\sigma_l \in [0, 1)$.

Remark 3. The sensors are supposed to be deployed geographically. Distributed event generators are provided to save the limited network-bandwidth. Whether the measurement of each sensor is transmitted or not depends on the local different triggering conditions. How frequently the sampled signals are released is determined by triggering parameter σ_l $(l = 1, \dots, n)$.

It should be remarked that each data satisfying the event-triggered condition will be time-stamped and released into the network. In order to make the proposed distributed ETS applicable, a buffer before each actuator is inserted to store a series of the control signal. Only the latest available store control signals with the same time-stamped can have access to the corresponding actuators [24].

Similar to [12], the holding interval Λ_l of ZOH can be reconstructed as $\Lambda_l = \bigcup_{m^l=0}^{M^l} \Lambda_{m^l}$, $\Lambda_{m^l} = [t_k^l h + m^l h + \tau_{t_k+m^l},\ t_k^l h + m^l h + h + \tau_{t_k+m^l+1})$. Define $\tau^l(t) = t - t_k^l h - m^l h,\ 0 \le \tau^l(t) \le \tau_M$.

Then from Eq. (4) and the definition of $\tau^l(t)$, the following event triggering condition is derived:

$$e_k^T(t)\Omega_l e_k(t) > \sigma^2 x^T(t - \tau(t))\Omega x(t - \tau(t)) \tag{5}$$

where $e_k(t) = \begin{bmatrix} e_k^1(t))^T & e_k^2(t))^T & \cdots & e_k^n(t))^T \end{bmatrix}^T$, $\sigma = \mathrm{diag}\{\sigma_1, \sigma_2, \dots, \sigma_n\}$, $\Omega = \mathrm{diag}\{\Omega_1, \Omega_2, \dots, \Omega_n\}$. $x(t - \tau(t)) = \begin{bmatrix} x^T(t - \tau^1(t)) & x^T(t - \tau^2(t)) & \cdots & x^T(t - \tau^n(t)) \end{bmatrix}^T$.

From the definitions of $e_k(t)$ and $\tau^l(t)$, the controller in Eq. (2) can be rewritten as

$$\begin{aligned} u(t) = {} & (1 - \beta(t))K[x(t - \tau(t)) + e_k(t)] + \beta(t)K\big[\alpha(t)g(x(t - d(t))) \\ & + (1 - \alpha(t))h(t - \eta(t))\big] \end{aligned} \tag{6}$$

Substituting Eq. (6) into Eq. (1) yields the following model:

$$\begin{aligned} \dot{x}(t) = {} & \Pi_0 + \bar{\beta}(\alpha(t) - \bar{\alpha})\Pi_2 + (\beta(t) - \bar{\beta})(\alpha(t) - \bar{\alpha})\Pi_2 \\ & + (\beta(t) - \bar{\beta})\Pi_1 + (\bar{\beta} - \beta(t))BK[x(t - \tau(t)) + e_k(t)] \end{aligned} \tag{7}$$

where

$$\Pi_0 = Ax(t) + (1 - \bar{\beta})BK[x(t - \tau(t)) + e_k(t)] + \bar{\beta}\Pi_1$$
$$\Pi_1 = \bar{\alpha}BKg(x(t - d(t)) + (1 - \bar{\alpha})BKh(t - \eta(t))$$
$$\Pi_2 = BKg(x(t - d(t)) - BKh(t - \eta(t))$$

Assumption 3. [25] The randomly occurring cyber-attacks $g(x(t))$ and $h(x(t))$ are assumed to be nonlinear functions satisfying

$$||g(x(t))||_2 \le ||Gx(t)||_2 \tag{8}$$

$$||h(x(t))||_2 \le ||Hx(t)||_2 \tag{9}$$

where G and H are known constant matrices representing the upper bounds of the nonlinearities.

Lemma 1. *[26] For any matrices $R \in \mathbb{R}^{n\times n}$ and $U \in \mathbb{R}^{n\times n}$ satisfying $\begin{bmatrix} R & * \\ U & R \end{bmatrix} > 0$, $\tau(t) \in [0, \tau_M]$, τ_M is a positive scalar, and vector function $\dot{x} : [-\tau_M, 0] \to \mathbb{R}^n$, the following inequality* *holds:*

$$-\tau_M \int_{t-\tau_M}^{t} \dot{x}^T(s)R\dot{x}(s)ds \leq -\varrho^T(t)\Theta\varrho(t) \tag{10}$$

where

$$\varrho(t)=\begin{bmatrix} x(t) \\ x(t-\tau(t)) \\ x(t-\tau_M) \end{bmatrix}, \Theta=\begin{bmatrix} -R & * & * \\ R-U & -2R+U+U^T & * \\ U & R-U & -R \end{bmatrix}$$

3. Main results

In this section, we are in a position to present sufficient conditions to ensure the stability of the distributed event-triggered NCSs with cyber-attacks. Then the controller design problem is solved and the controller gain is derived.

Theorem 1. *Let the Bernoulli parameters $\bar{\alpha}$, $\bar{\beta}$, trigger parameter σ, time delays d_M, η_M, τ_M and matrix K, the networked closed-loop system (7) under distributed ETS and cyber-attacks is asymptotically stable if there exist matrices $P>0$, $Q_s>0$, $R_s>0$, U_s $(s=1,2,3)$ and $\Omega>0$ with appropriate dimensions such that*

$$\begin{bmatrix} \Gamma_{11} & * & * & * & * & * & * \\ \Gamma_{21} & \mathcal{P} & * & * & * & * & * \\ \Gamma_{31} & 0 & \mathcal{P} & * & * & * & * \\ \Gamma_{41} & 0 & 0 & \mathcal{P} & * & * & * \\ \Gamma_{51} & 0 & 0 & 0 & \mathcal{P} & * & * \\ \Gamma_{61} & 0 & 0 & 0 & 0 & -I & * \\ \Gamma_{71} & 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{11}$$

$$\begin{bmatrix} R_s & * \\ U_s & R_s \end{bmatrix} > 0(s=1,2,3) \tag{12}$$

where

$$\Gamma_{11}=\begin{bmatrix} \Phi_{11} & * & * & * & * \\ \Phi_{21} & \Phi_{22} & * & * & * \\ \Phi_{31} & 0 & \Phi_{33} & * & * \\ \bar{\alpha}\bar{\beta}K^TB^TP & 0 & 0 & -I & * \\ (1-\bar{\alpha})\bar{\beta}K^TB^TP & 0 & 0 & 0 & -I \end{bmatrix}$$

$$\Phi_{11}=PA+A^TP+Q_1+Q_2+Q_3-R_1-R_2-R_3$$

$$\Phi_{21}=\begin{bmatrix} (1-\bar{\beta})K^TB^TP+R_1-U_1 \\ U_1 \\ (1-\bar{\beta})K^TB^TP \end{bmatrix}, \Phi_{22}=\begin{bmatrix} -2R_1+U_1+U_1^T+\sigma^2\Omega & * & * \\ R_1-U_1 & -Q_1-R_1 & * \\ 0 & 0 & -\Omega \end{bmatrix}$$

$$\Phi_{31}=\begin{bmatrix} R_2-U_2 \\ U_2 \\ R_3-U_3 \\ U_3 \end{bmatrix}, \Phi_{33}=\begin{bmatrix} -2R_2+U_2+U_2^T & * & * & * \\ R_2-U_2 & -Q_2-R_2 & * & * \\ 0 & 0 & -2R_3+U_3+U_3^T & * \\ 0 & 0 & R_3-U_3 & -Q_3-R_3 \end{bmatrix}$$

$$\Gamma_{21} = \begin{bmatrix} \tau_M \mathcal{F}_1 \\ d_M \mathcal{F}_1 \\ \eta_M \mathcal{F}_1 \end{bmatrix}, \Gamma_{31} = \begin{bmatrix} \tau_M \mathcal{F}_2 \\ d_M \mathcal{F}_2 \\ \eta_M \mathcal{F}_2 \end{bmatrix}, \Gamma_{41} = \begin{bmatrix} \tau_M \mathcal{F}_3 \\ d_M \mathcal{F}_3 \\ \eta_M \mathcal{F}_3 \end{bmatrix}, \Gamma_{51} = \begin{bmatrix} \tau_M \mathcal{F}_4 \\ d_M \mathcal{F}_4 \\ \eta_M \mathcal{F}_4 \end{bmatrix}$$

$$\mathcal{F}_1 = \begin{bmatrix} PA & (1-\bar{\beta})PBK & 0 & (1-\bar{\beta})PBK & 0_{1\times 4} & \bar{\alpha}\bar{\beta}PBK & (1-\bar{\alpha})\bar{\beta}PBK \end{bmatrix}$$

$$\mathcal{F}_2 = \sqrt{\delta_{\alpha}^2(\bar{\beta}^2 + \delta_{\beta}^2)}\begin{bmatrix} 0_{1\times 8} & PBK & -PBK \end{bmatrix}$$

$$\mathcal{F}_3 = \delta_{\beta}\begin{bmatrix} 0_{1\times 8} & \bar{\alpha}PBK & (1-\bar{\alpha})PBK \end{bmatrix}$$

$$\mathcal{F}_4 = \delta_{\beta}\begin{bmatrix} 0 & PBK & 0 & PBK & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\mathcal{P} = \mathrm{diag}\{-PR_1^{-1}P, -PR_2^{-1}P, -PR_3^{-1}P\}$$

$$\Gamma_{61} = \begin{bmatrix} 0_{1\times 4} & G & 0_{1\times 5} \end{bmatrix}, \Gamma_{71} = \begin{bmatrix} 0_{1\times 6} & H & 0_{1\times 3} \end{bmatrix}$$

Proof: Choose the following Lyapunov function:

$$V(t) = V_1(t) + V_2(t) + V_3(t) \tag{13}$$

$$\begin{aligned} V_1(t) &= x^T(t)Px(t) \\ V_2(t) &= \int_{t-\tau_M}^{t} x^T(s)Q_1x(s)ds + \int_{t-d_M}^{t} x^T(s)Q_2x(s)ds + \int_{t-\eta_M}^{t} x^T(s)Q_3x(s)ds \\ V_3(t) &= \tau_M \int_{t-\tau_M}^{t}\int_{s}^{t} x^T(v)Q_1x(v)dvds + d_M \int_{t-d_M}^{t}\int_{s}^{t} x^T(v)Q_2x(v)dvds \\ &\quad + \eta_M \int_{t-\eta_M}^{t}\int_{s}^{t} x^T(v)Q_3x(v)dvds \end{aligned}$$

By taking the time derivative of $V(t)$ in Eq. (13) along the trajectory of Eq. (7), it yields

$$\mathbb{E}\{\dot{V}_1(t)\} = 2x^T(t)P\Pi_0 \tag{14}$$

$$\begin{aligned} \mathbb{E}\{\dot{V}_2(t)\} &= x^T(t)(Q_1 + Q_2 + Q_3)x(t) - x^T(t-\tau_M)Q_1x(t-\tau_M) - x^T(t-d_M)Q_2x(t-d_M) \\ &\quad - x^T(t-\eta_M)Q_3x(t-\eta_M) \end{aligned} \tag{15}$$

$$\begin{aligned} \mathbb{E}\{\dot{V}_3(t)\} &= \dot{x}^T(t)\mathcal{R}\dot{x}(t) - \tau_M \int_{t-\tau_M}^{t} \dot{x}^T(s)R_1\dot{x}(s)ds - d_M \int_{t-d_M}^{t} \dot{x}^T(s)R_2\dot{x}(s)ds \\ &\quad - \eta_M \int_{t-\eta_M}^{t} \dot{x}^T(s)R_3\dot{x}(s)ds \end{aligned} \tag{16}$$

in which $\mathcal{R} = \tau_M^2 R_1 + d_M^2 R_2 + \eta_M^2 R_3$.

By Lemma 1, for matrices U_s $(s = 1, 2, 3)$ satisfying Eq. (12), we can obtain

$$-\tau_M \int_{t-\tau_M}^{t} \dot{x}^T(s)R_1\dot{x}(s)ds \le \zeta_1^T(t)\Upsilon_1\zeta_1(t) \tag{17}$$

$$-d_M \int_{t-d_M}^{t} \dot{x}^T(s)R_2\dot{x}(s)ds \le \zeta_2^T(t)\Upsilon_2\zeta_2(t) \tag{18}$$

$$-\eta_M\int_{t-\eta_M}^{t}\dot{x}^T(s)R_3\dot{x}(s)ds\le\zeta_3^T(t)\Upsilon_3\zeta_3(t)\tag{19}$$

where

$$\zeta_1(t)=\begin{bmatrix}x(t)\\x(t-\tau(t))\\x(t-\tau_M)\end{bmatrix},\zeta_2(t)=\begin{bmatrix}x(t)\\x(t-d(t))\\x(t-d_M)\end{bmatrix},\zeta_3(t)=\begin{bmatrix}x(t)\\x(t-\eta(t))\\x(t-\eta_M)\end{bmatrix}$$

$$\Upsilon_s=\begin{bmatrix}-R_s&*&*\\R_s-U_s&-2R_s+U_s+U_s^T&*\\U_s&R_s-U_s&-R_s\end{bmatrix}(s=1,2,3)$$

Notice that

$$\begin{aligned}\mathbb{E}\{\dot{x}^T(t)\mathcal{R}\dot{x}(t)\}=&\Pi_0^T\mathcal{R}\Pi_0+(\delta_\alpha^2\bar{\beta}^2+\delta_\alpha^2\delta_\beta^2)\Pi_2^T\mathcal{R}\Pi_2+\delta_\beta^2\Pi_1^T\mathcal{R}\Pi_1\\&+\delta_\beta^2(x^T(t-\tau(t))+e_k^T(t))K^TB^T\mathcal{R}BK(x(t-\tau(t))+e_k(t))\end{aligned}\tag{20}$$

By combining Eqs. (14)–(20), it is clear that

$$\begin{aligned}\mathbb{E}\{\dot{V}(t)\}\le&2x^T(t)P\Pi_0+x^T(t)(Q_1+Q_2+Q_3)x(t)-x^T(t-\tau_M)Q_1x(t-\tau_M)\\&-x^T(t-d_M)Q_2x(t-d_M)-x^T(t-\eta_M)Q_3x(t-\eta_M)\\&+\Pi_0^T\mathcal{R}\Pi_0+(\delta_\alpha^2\bar{\beta}^2+\delta_\alpha^2\delta_\beta^2)\Pi_2^T\mathcal{R}\Pi_2+\delta_\beta^2\Pi_1^T\mathcal{R}\Pi_1\\&+\delta_\beta^2(x^T(t-\tau(t))+e_k^T(t))K^TB^T\mathcal{R}BK(x(t-\tau(t))+e_k(t))\\&+\zeta_1^T(t)\Upsilon_1\zeta_1(t)+\zeta_2^T(t)\Upsilon_2\zeta_2(t)+\zeta_3^T(t)\Upsilon_3\zeta_3(t)\end{aligned}\tag{21}$$

From Assumption 3, we have

$$x^T(t-d(t))G^TGx(t-d(t))-g^T(x(t-d(t))g(x(t-d(t))>0\tag{22}$$

$$x^T(t-\eta(t))H^THx(t-\eta(t))-h^T(x(t-\eta(t)))h(x(t-\eta(t))>0\tag{23}$$

Due to Eq. (5) and Eqs. (21)–(23), it follows that:

$$\begin{aligned}\mathbb{E}\{\dot{V}(t)\}\le&\xi^T(t)\Gamma_{11}\xi(t)+\Pi_0^T\mathcal{R}\Pi_0+(\delta_\alpha^2\bar{\beta}^2+\delta_\alpha^2\delta_\beta^2)\Pi_2^T\mathcal{R}\Pi_2+\delta_\beta^2\Pi_1^T\mathcal{R}\Pi_1\\&+\delta_\beta^2(x^T(t-\tau(t))+e_k^T(t))K^TB^T\mathcal{R}BK(x(t-\tau(t))+e_k(t))\\&+x^T(t-d(t))G^TGx(t-d(t))+x^T(t-\eta(t))H^THx(t-\eta(t))\end{aligned}\tag{24}$$

where

$$\xi(t)=\begin{bmatrix}\zeta_1^T(t)&e_k^T(t)&x^T(t-d(t))&x^T(t-d_M)&x^T(t-\eta(t))&x^T(t-\eta_M)&\xi_{gh}^T(t)\end{bmatrix}^T$$
$$\xi_{gh}^T(t)=\begin{bmatrix}g^T(x(t-d(t)))&h^T(x(t-\eta(t)))\end{bmatrix}$$

By using Schur complements, one can know that Eq. (11) guarantees $\mathbb{E}\{\dot{V}(t)\}<0$. Thus the proof is completed.

Theorem 2. *Giving the positive parameters* $\bar{\alpha}$, $\bar{\beta}$, ε_r $(r=0,1,2,3)$, *trigger parameter* σ *and time delays* d_M, η_M, τ_M, *the networked closed-loop system (7) under distributed ETS and cyber-attacks is asymptotically stable with controller gain* $K=YX^{-1}$, *if there exist matrices*

$X>0$, $\bar{Q}_s>0$, $\bar{R}_s>0$, $\bar{U}_s$ $(s=1,2,3)$, Y and $\bar{\Omega}>0$ with appropriate dimensions, such that the LMIs hold:

$$\begin{bmatrix} \bar{\Gamma}_{11} & * & * & * & * & * & * \\ \bar{\Gamma}_{21} & \bar{\mathcal{P}} & * & * & * & * & * \\ \bar{\Gamma}_{31} & 0 & \bar{\mathcal{P}} & * & * & * & * \\ \bar{\Gamma}_{41} & 0 & 0 & \bar{\mathcal{P}} & * & * & * \\ \bar{\Gamma}_{51} & 0 & 0 & 0 & \bar{\mathcal{P}} & * & * \\ \bar{\Gamma}_{61} & 0 & 0 & 0 & 0 & -I & * \\ \bar{\Gamma}_{71} & 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{25}$$

$$\begin{bmatrix} \bar{R}_s & * \\ \bar{U}_s & \bar{R}_s \end{bmatrix} > 0(s=1,2,3) \tag{26}$$

where

$$\bar{\Gamma}_{11} = \begin{bmatrix} \bar{\Phi}_{11} & * & * & * & * \\ \bar{\Phi}_{21} & \bar{\Phi}_{22} & * & * & * \\ \bar{\Phi}_{31} & 0 & \bar{\Phi}_{33} & * & * \\ \bar{\alpha}\bar{\beta}Y^TB^T & 0 & 0 & -I & * \\ (1-\bar{\alpha})\bar{\beta}Y^TB^T & 0 & 0 & 0 & -I \end{bmatrix}$$

$$\bar{\Phi}_{11} = AX + XA^T + \bar{Q}_1 + \bar{Q}_2 + \bar{Q}_3 - \bar{R}_1 - \bar{R}_2 - \bar{R}_3$$

$$\bar{\Phi}_{21} = \begin{bmatrix} (1-\bar{\beta})Y^TB^T + \bar{R}_1 - \bar{U}_1 \\ \bar{U}_1 \\ (1-\bar{\beta})Y^TB^T \end{bmatrix}, \bar{\Phi}_{22} = \begin{bmatrix} -2\bar{R}_1 + \bar{U}_1 + \bar{U}_1^T + \sigma^2\bar{\Omega} & * & * \\ \bar{R}_1 - \bar{U}_1 & -\bar{Q}_1 - \bar{R}_1 & * \\ 0 & 0 & -\bar{\Omega} \end{bmatrix}$$

$$\bar{\Phi}_{31} = \begin{bmatrix} \bar{R}_2 - \bar{U}_2 \\ \bar{U}_2 \\ \bar{R}_3 - \bar{U}_3 \\ \bar{U}_3 \end{bmatrix}, \bar{\Phi}_{33} = \begin{bmatrix} -2\bar{R}_2 + \bar{U}_2 + \bar{U}_2^T & * & * & * \\ \bar{R}_2 - \bar{U}_2 & -\bar{Q}_2 - \bar{R}_2 & * & * \\ 0 & 0 & -2\bar{R}_3 + \bar{U}_3 + \bar{U}_3^T & * \\ 0 & 0 & \bar{R}_3 - \bar{U}_3 & -\bar{Q}_3 - \bar{R}_3 \end{bmatrix}$$

$$\bar{\Gamma}_{21} = \begin{bmatrix} \tau_M\bar{\mathcal{F}}_1 \\ d_M\bar{\mathcal{F}}_1 \\ \eta_M\bar{\mathcal{F}}_1 \end{bmatrix}, \bar{\Gamma}_{31} = \begin{bmatrix} \tau_M\bar{\mathcal{F}}_2 \\ d_M\mathcal{F}_2 \\ \eta_M\bar{\mathcal{F}}_2 \end{bmatrix}, \bar{\Gamma}_{41} = \begin{bmatrix} \tau_M\bar{\mathcal{F}}_3 \\ d_M\bar{\mathcal{F}}_3 \\ \eta_M\bar{\mathcal{F}}_3 \end{bmatrix}, \bar{\Gamma}_{51} = \begin{bmatrix} \tau_M\bar{\mathcal{F}}_4 \\ d_M\bar{\mathcal{F}}_4 \\ \eta_M\bar{\mathcal{F}}_4 \end{bmatrix}$$

$$\bar{\mathcal{F}}_1 = \begin{bmatrix} AX & (1-\bar{\beta})BY & 0 & (1-\bar{\beta})BY & 0_{1\times4} & \bar{\alpha}\bar{\beta}BY & (1-\bar{\alpha})\bar{\beta}BY \end{bmatrix}$$

$$\bar{\mathcal{F}}_2 = \sqrt{\delta_\alpha^2(\bar{\beta}^2 + \delta_\beta^2)}\begin{bmatrix} 0_{1\times8} & BY & -BY \end{bmatrix}$$

$$\bar{\mathcal{F}}_3 = \delta_\beta\begin{bmatrix} 0_{1\times8} & \bar{\alpha}BY & (1-\bar{\alpha})BY \end{bmatrix}$$

$$\bar{\mathcal{F}}_4 = \delta_\beta\begin{bmatrix} 0 & BY & 0 & BY & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\mathcal{P} = \mathrm{diag}\{-2\varepsilon_1X + \varepsilon_1^2R_1, -2\varepsilon_2X + \varepsilon_2^2R_2, -2\varepsilon_3X + \varepsilon_3^2R_3\}$$

$$\Gamma_{61} = \begin{bmatrix} 0_{1\times4} & GX & 0_{1\times5} \end{bmatrix}, \Gamma_{71} = \begin{bmatrix} 0_{1\times6} & HX & 0_{1\times3} \end{bmatrix}$$

Proof: For any positive scalars ε_s, due to $(R_s - \varepsilon_s^{-1}P)R_s^{-1}(R_s - \varepsilon_s^{-1}P) \geq 0$, one can obtain

$$-PR_s^{-1}P \leq -2\varepsilon_sP + \varepsilon_s^2R_s \tag{27}$$

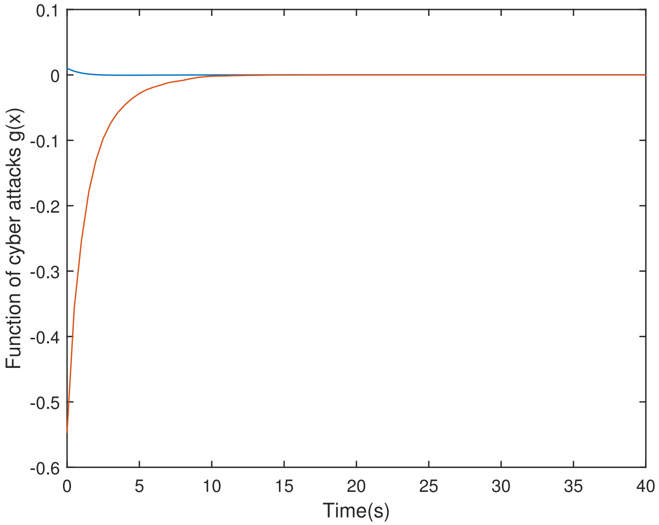

Fig. 2. The graph of cyber-attacks $g(x(t))$.

Replace $-PR_s^{-1}P$ by $-2\varepsilon_s P+\varepsilon_s^2 R_s$ $(s=1,2,3)$ in Eq. (11), Eq. (28) is a sufficient condition to ensure Eq. (11) holds.

$$\begin{bmatrix} \Gamma_{11} & * & * & * & * & * & * \\ \Gamma_{21} & \hat{\mathcal{P}} & * & * & * & * & * \\ \Gamma_{31} & 0 & \hat{\mathcal{P}} & * & * & * & * \\ \Gamma_{41} & 0 & 0 & \hat{\mathcal{P}} & * & * & * \\ \Gamma_{51} & 0 & 0 & 0 & \hat{\mathcal{P}} & * & * \\ \Gamma_{61} & 0 & 0 & 0 & 0 & -I & * \\ \Gamma_{71} & 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{28}$$

Define $X=P^{-1}$, $XR_sX=\bar{R}_s$, $XU_sX=\bar{U}_s$ $(s=1,2,3)$, $Y=KX$, $X\Omega X=\bar{\Omega}$, $J_1=\text{diag}\{\underbrace{X,\ldots,X}_{22},I,I\}$, $J_2=\text{diag}\{X,X\}$.

Pre- and post-multiplying Eqs. (28) and (12) with J_1 and J_2, respectively. From Eq. (27), it follows that $-XX\le -2\varepsilon_0 X+\varepsilon_0^2 I$. Then substitute $-2\varepsilon_0 X+\varepsilon_0^2 I$ for $-XX$, we can derive that Eqs. (25) and (26) can guarantee Eqs. (11) and (12) hold. The proof is completed.

4. Numerical examples

In this section, a numerical example will be given to demonstrate the feasibility of the proposed control approach for NCSs with stochastic cyber-attacks.

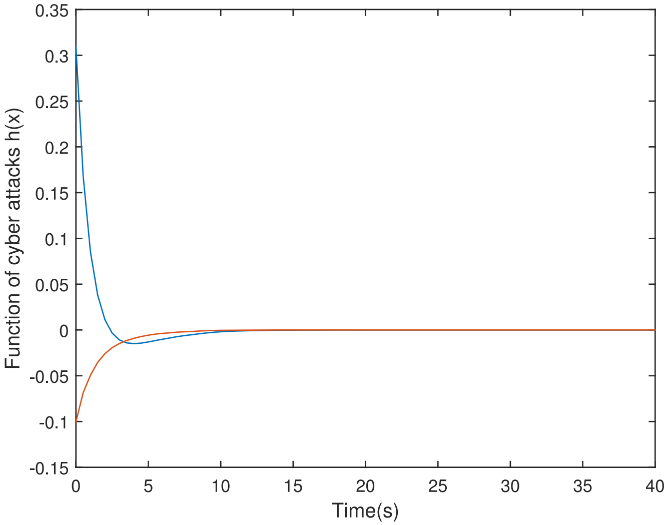

Fig. 3. The graph of cyber-attacks $h(x(t))$.

Consider system (7) with following parameters:

$$A=\begin{bmatrix}-0.72 & 0.40 & 0 & 0 & 0 & 0\\ 0.25 & -0.56 & 0 & 0 & 0 & 0\\ 0 & 0 & -0.72 & 0.40 & 0 & 0\\ 0 & 0 & 0.25 & -0.56 & 0 & 0\\ 0 & 0 & 0 & 0 & -0.72 & 0.40\\ 0 & 0 & 0 & 0 & 0.25 & -0.56\end{bmatrix}, B=\begin{bmatrix}0.1 & 0 & 0\\ 0.5 & 0 & 0\\ 0 & 0.1 & 0\\ 0 & 0.5 & 0\\ 0 & 0 & 0.1\\ 0 & 0 & 0.5\end{bmatrix}$$

Set $\tau_M=0.8$, $d_M=0.6$, $\eta_M=0.3$, the parameters of event-triggered scheme $\sigma_1^2=0.9$, $\sigma_2^2=0.5$, $\sigma_3^2=0.6$, the initial state $x(0)=\begin{bmatrix}1 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & -1 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & -1\end{bmatrix}^T$, sampling period $h=0.5$.

The above given parameters are chosen the same in the following two cases. Our purpose is to validate the usefulness of the obtained controller design method for system (7). Case 1 is used to illustrate the designed controller is useful to stabilize the augmented system even when the NCS is attacked. In case 2, the discussed system works without cyber-attacks.

Case 1. We use nonlinear functions $g(x(t))$ and $h(x(t))$ to represent the two kinds of cyber-attacks which shown in Figs. 2 and 3.

$$g(x(t))=\begin{bmatrix}-tanh(0.5x_1(t)) & 0 & 0\\ -tanh(0.01x_1(t)) & 0 & 0\\ 0 & -tanh(0.5x_2(t)) & 0\\ 0 & -tanh(0.01x_2(t)) & 0\\ 0 & 0 & -tanh(0.5x_3(t))\\ 0 & 0 & -tanh(0.01x_3(t))\end{bmatrix}$$

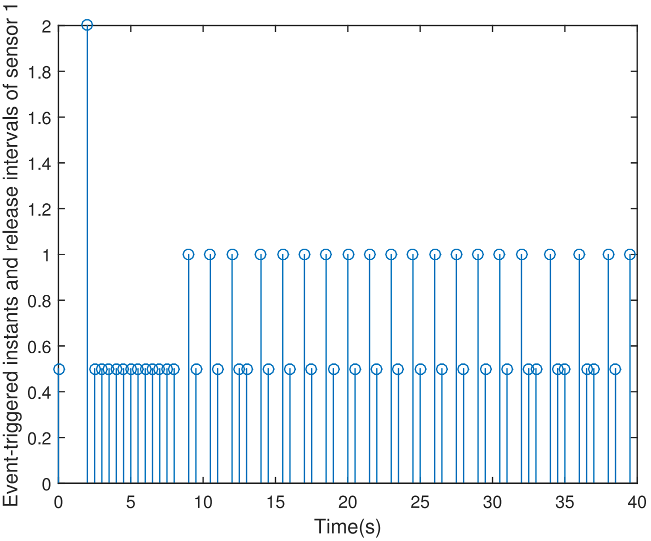

Fig. 4. Event-triggered instants and release intervals of sensor 1.

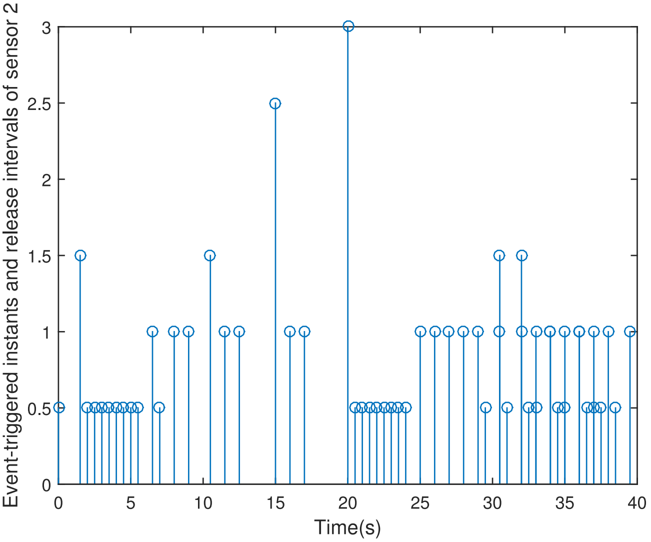

Fig. 5. Event-triggered instants and release intervals of sensor 2.

$$h(x(t)) = \begin{bmatrix} -tanh(0.1x_1(t)) & 0 & 0 \\ -tanh(0.3x_1(t)) & 0 & 0 \\ 0 & -tanh(0.1x_2(t)) & 0 \\ 0 & -tanh(0.3x_2(t)) & 0 \\ 0 & 0 & -tanh(0.1x_3(t)) \\ 0 & 0 & -tanh(0.3x_3(t)) \end{bmatrix}$$

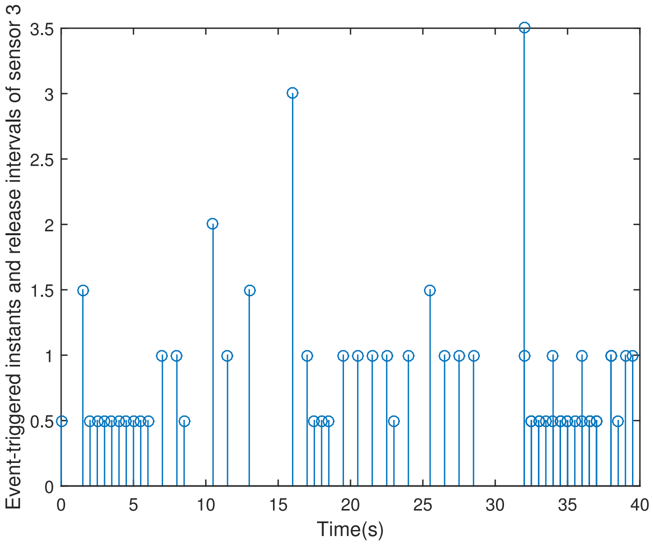

Fig. 6. Event-triggered instants and release intervals of sensor 3.

It can be seen that $g(x(t))$ and $h(x(t))$ satisfy Assumption 3 with $G = \text{diag}\{0.01, 0.5, 0.01, 0.5, 0.01, 0.5\}$ and $H = diag\{0.3, 0.1, 0.3, 0.1, 0.3, 0.1\}$.

Let $\bar{\beta} = 0.5$, $\bar{\alpha} = 0.5$, it means that the distributed control systems are subject to random cyber-attacks with the probability of 50%, and the switch probability between the two different type cyber-attacks is 50%. By applying Theorem 2, we can obtain that

$$Y = \begin{bmatrix} -3.1949 & -1.7352 & 0 & 0 & 0 & 0 \\ 0 & 0 & -5.1203 & -3.7368 & 0 & 0 \\ 0 & 0 & 0 & 0 & -5.2481 & -3.8115 \end{bmatrix}$$

$$X = \begin{bmatrix} 11.9727 & 0.6827 & 0 & 0 & 0 & 0 \\ 0.6827 & 12.4869 & 0 & 0 & 0 & 0 \\ 0 & 0 & 11.9727 & 0.6827 & 0 & 0 \\ 0 & 0 & 0.6827 & 12.4869 & 0 & 0 \\ 0 & 0 & 0 & 0 & 11.6132 & 0.3355 \\ 0 & 0 & 0 & 0 & 0.3355 & 11.4062 \end{bmatrix}$$

According to accurate expression of controller gain $K = YX^{-1}$ in Theorem 2, the distributed controller is presented as follows:

$$K = \begin{bmatrix} -0.2597 & -0.1248 & 0 & 0 & 0 & 0 \\ 0 & 0 & -0.4335 & -0.3161 & 0 & 0 \\ 0 & 0 & 0 & 0 & -0.4426 & -0.3211 \end{bmatrix}$$

Figs. 4–6 present the event-triggered instants of three sensors, respectively. The diagram of the state response of the event-triggered NCSs with cyber-attacks is shown in Fig. 7. The graph of the switching rule between the two kinds of cyber-attacks is shown in Figs. 8. The figures above demonstrate that the designed event-triggered controller is feasible when the discussed system is under stochastic cyber-attacks.

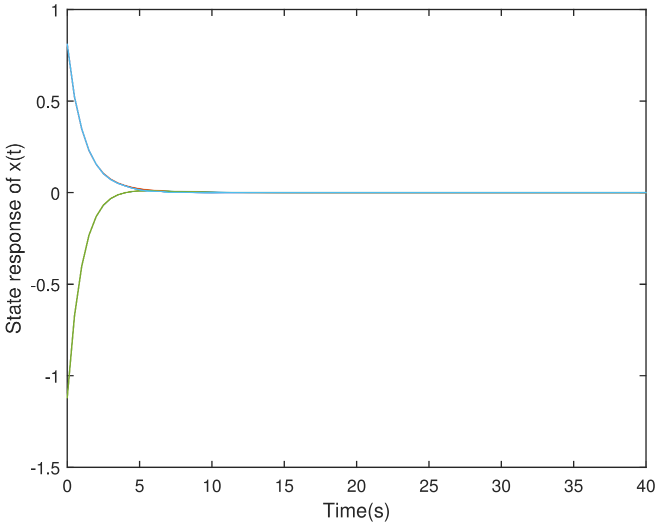

Fig. 7. State response of $x(t)$ in case 1.

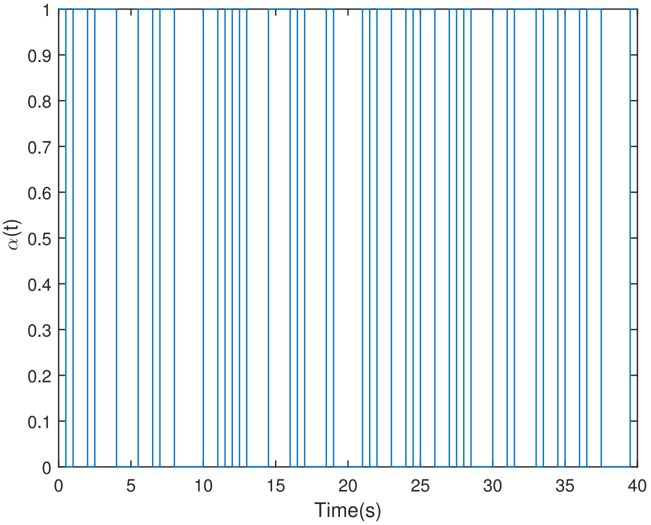

Fig. 8. The graph of switching rule $\alpha(t)$ between the cyber-attacks.

Case 2. Set $\bar{\beta} = 0$, it means that distributed event-triggered NCSs work normally without cyber-attacks. Based on Theorem 2 and LMI toolbox in MATLAB, we can obtain the following parameters:

$$Y = \begin{bmatrix} -3.6462 & -2.1763 & 0 & 0 & 0 & 0 \\ 0 & 0 & -3.9151 & -2.9008 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3.8710 & -2.8378 \end{bmatrix}$$

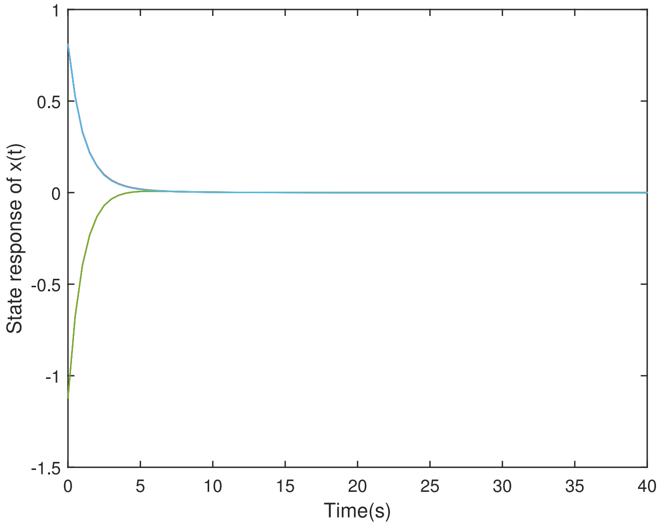

Fig. 9. State response of $x(t)$ in case 2.

$$X = \begin{bmatrix} 10.7570 & 0.6897 & 0 & 0 & 0 & 0 \\ 0.6897 & 13.0315 & 0 & 0 & 0 & 0 \\ 0 & 0 & 9.7430 & 0.0975 & 0 & 0 \\ 0 & 0 & 0.0975 & 9.4976 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9.7893 & 0.0987 \\ 0 & 0 & 0 & 0 & 0.0987 & 9.5568 \end{bmatrix}$$

From $K = YX^{-1}$ in Theorem 2, we can obtain the controller gain as follows:

$$K = \begin{bmatrix} -0.3294 & -0.1496 & 0 & 0 & 0 & 0 \\ 0 & 0 & -0.3988 & -0.3013 & 0 & 0 \\ 0 & 0 & 0 & 0 & -0.3925 & -0.2929 \end{bmatrix}$$

Fig. 9 presents the state response of $x(t)$, and it illustrates that event-triggered distributed control design approach is useful to stabilize the NCSs without cyber-attacks.

5. Conclusions

In this paper, distributed event-triggered control problem is investigated for NCSs subject to stochastic cyber-attacks. An event generator is set at each sensor side to determine whether the current sampled data is transmitted into the network or not. Based on the distributed ETS, the data redundancies are largely reduced during the networked transmission. The inner variations of the random cyber-attacks are taken into account, which are modeled as two switched nonlinear functions. By applying Lyapunov function and linear matrix inequality techniques, sufficient conditions for the stability of the discussed system are derived and the controller gain is presented by solving certain matrix inequalities. A numerical example is given in the simulation section to illustrate the usefulness of designed control scheme. Future research topics include distributed hybrid-triggered control for NCSs with stochastic cyber-attacks.

Acknowledgment

This work is partly supported by the National Key Research and Development Program of China (No. 2017YFD0700501), the National Natural Science Foundation of China (Nos. 61403185, 61773218, 61473156), the Natural Science Foundation of Jiangsu Province of China (Nos. BK20171481, BK20161561), the major project supported by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Nos. 15KJA120001, 16KJA170003), the National Science and Technology Pillar Program of Jiangsu Province of China (No. BE2016178), the National Key Technologies Research and Development Program of China (No. 2015BAD18B02), the Six Talent Peaks Project in Jiangsu Province (No. 2015-DZXX-21), the Policy Guidance Program (Cooperation of Industry, Education and Academy) of Jiangsu Province (No. BY2016009-04) and a Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD).

References

[1] A. Selivanov, E. Fridman, Distributed event-triggered control of diffusion semilinear PDEs, Automatica 68 (2016) 344–351.

[2] Z. Wu, Y. Xu, Y. Pan, H. Su, Y. Tang, Event-triggered control for consensus problem in multi-agent systems with quantized relative state measurement and external disturbance, IEEE Trans. Circuit Syst. (2017), doi:10.1109/TCSI.2017.2777504.

[3] S. Liu, P. Liu, A.E. Saddik, A stochastic security game for Kalman filtering in networked control systems under denial of service attacks, Proceedings of the 3rd IFAC International Conference on Intelligent Control and Automation Science 46(20) (2013) 106–111.

[4] J. Yan, Y. Xia, C. Wen, Quantized control for NCSs with communication constraints, Neurocomputing 267 (2017) 489–499.

[5] Z. Wu, Y. Wu, Z.G. Wu, J. Lu, Event-based synchronization of heterogeneous complex networks subject to transmission delays, IEEE Trans. Syst. Man Cybern. Syst. (2017), doi:10.1109/TSMC.2017.2723760.

[6] Y. Niu, T. Jia, X. Wang, F. Yang, Output-feedback control design for NCSs subject to quantization and dropout, Inf. Sci. 179 (21) (2009) 3804–3813.

[7] J. Liu, D. Yue, Event-triggering in networked systems with probabilistic sensor and actuator faults, Inf. Sci. 240 (10) (2013) 145–160.

[8] 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.

[9] Y. Pan, G. Yang, Event-triggered fuzzy control for nonlinear networked control systems, Fuzzy Sets Syst. 329 (2017) 91–107.

[10] Z. Wu, Y. Xu, Y. Pan, P. Shi, Q. Wang, Event-triggered pinning control for consensus of multiagent systems with quantized information, IEEE Trans. Syst. Man Cybern. Syst. (2017), doi:10.1109/TSMC.2017.2773634.

[11] D. Yue, Q. Han, J. Lam, Network-based robust protect H_∞ control of systems with uncertainty, Automatica (41) (2005) 999–1007.

[12] 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.

[13] J. Liu, L. Zha, J. Cao, S. Fei, Hybrid-driven-based stabilization for networked control systems, IET Control Theory Appl. 10 (17) (2016) 2279–2285.

[14] Z. Gu, E. Tian, J. Liu, Adaptive event-triggered control of a class of nonlinear networked systems, J. Frankl. Inst. 354 (2017) 3854–3871.

[15] Z. Wu, Y. Xu, R. Lu, Y. Wu, T. Huang, Event-triggered control for consensus of multiagent systems with fixed/switching topologies, IEEE Trans. Syst. Man Cybern. Syst. (2017), doi:10.1109/TSMC.2017.2744671.

[16] L. Zha, J. Fang, X. Li, J. Liu, Event-triggered output feedback H_∞ control for networked Markovian jump systems with quantizations, Nonlinear Anal.: Hybrid Syst. 24 (2017) 146–158.

[17] S. Hu, D. Yue, Event-based H_∞ filtering for networked system with communication delay, Signal Process. 92 (2012) 2029–2039.

[18] S. Liu, G. Wei, Y. Song, Y. Liu, Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks, Neurocomputing 207 (2016) 708–716.

[19] D. Ding, G. Wei, S. Zhang, Y. Liu, F.E. Alsaadi, On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors, Neurocomputing 219 (2017) 99–106.

[20] L. Zhao, G. Yang, Adaptive sliding mode fault tolerant control for nonlinearly chaotic systems against DoS attack and network faults, J. Frankl. Inst. 354 (2017) 6520–6535.

[21] R.M. Ferrari, A.M. Teixeira, Detection and isolation of replay attacks through sensor watermarking, Int. Fed. Autom. Control 50 (1) (2017) 7363–7368.

[22] D. Ding, Z. Wang, D.W.C. Ho, G. Wei, Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks, Automatica 78 (2017) 231–240.

[23] J. Liu, J. Xia, E. Tian, S. Fei, Hybrid-driven-based H_∞ filter design for neural networks subject to deception attacks, Appl. Math. Comput. 320 (2018) 158–174.

[24] C. Peng, E. Tian, J. Zhang, D. Du, Decentralized event-triggering communication scheme for large-scale systems under network environments, Inf. Sci. 380 (2017) 132–144.

[25] J. Liu, L. Wei, E. Tian, S. Fei, J. Cao, H_∞ filtering for networked systems with hybrid-triggered communication mechanism and stochastic cyber attacks, J. Frankl. Inst. 354 (2017) 8490–8512.

[26] C. Peng, Q. Han, D. Yue, Communication-delay-distribution-dependent decentralized control for large-scale systems with IP-based communication networks, IEEE Trans. Control Syst. Technol. 21 (3) (2013) 820–830.