Nonlinear Analysis: Hybrid Systems 50 (2023) 101377

Contents lists available at ScienceDirect

Nonlinear Analysis: Hybrid Systems

journal homepage: www.elsevier.com/locate/nahs

Adaptive event-triggered control for networked interconnected systems with cyber-attacks

Jinliang Liu [a], Yan Qian [b], Lijuan Zha [b,*], Engang Tian [c], Xiangpeng Xie [d]

[a] School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, Jiangsu 210044, China
[b] College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210023, China
[c] School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China
[d] Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210023, China

ARTICLE INFO

Article history:
Received 17 April 2022
Received in revised form 17 April 2023
Accepted 8 May 2023
Available online 4 July 2023

Keywords:
Networked interconnected systems
Adaptive event-triggered mechanism
Cyber-attacks

ABSTRACT

This paper investigates the secure adaptive event-triggered controller design for networked interconnected systems (NISs) with cyber-attacks. Firstly, an adaptive event-triggered mechanism (AETM) with dynamic threshold parameter is adopted to economize the limited network bandwidth which takes the abrupt data into consideration. A model of cyber-attacks is established for NISs with consideration of the malicious cyber-attacks. On account of the model of cyber-attacks and AETM, a mathematical model of NISs is established. For the built system, the sufficient condition for the asymptotic stability of the system is obtained by making use of Lyapunov stability theory and linear matrix inequality (LMI) technique, and the design algorithm of the controller is proposed. Finally, a simulation example is given to verify the validity of the theoretical results.

1. Introduction

Interconnected systems are common large scale systems made up of several coupled subsystems which are often geographically distributed [1–4]. The systems are now widely used in many fields such as power system, economic system, communication system, computer network and so on (see [5,6] and references therein). With the development of communication network, interconnected systems based on network have become a vital research topic [7–9]. In networked interconnected systems (NISs), the information interaction among components within each subsystem can be flexibly and cost-efficiently realized via communication network. Nevertheless, the introduction of network also incurs some crucial challenges, such as network resource constraints and malicious cyber-attacks, which will significantly affect system performance [10–12].

With the increase of the scale and complexity of control systems, large amounts of transmitted data will enter the network. In order to make full use of the limited network bandwidth, scholars have done a lot of researches and put forward various data transmission schemes [13–16]. Among them, time-triggered scheme was preferably used since that it can be easily implemented. However, in such a scheme, the signal will still be transmitted periodically even if system states have little changes, which wastes the restricted network resources. In view of this, the event-triggered schemes are accordingly proposed, that is, only when the particular event occurs, the sampled data can be released to the network for transmission [17]. For example, the authors in [18] proposed an event-triggered mechanism to allow the sending

* Corresponding author.
E-mail address: zhalijuan@vip163.com (L. Zha).

https://doi.org/10.1016/j.nahs.2023.101377

of data that violates the triggering condition by monitoring the state of the system. Considering the effectiveness of the scheme proposed in [18], many improved event-triggered schemes are subsequently designed [19–23]. In the past several years, adaptive event-triggered mechanism (AETM) has attracted extensive attentions, since that it can dynamically adjust triggering conditions according to the real-time system state [24]. For instance, by combining input constraints with hybrid cyber-attacks, Liu et al. researched the secure filtering design for networked control system (NCS) with AETM in [8]. Based on T-S fuzzy model, Gu et al. [25] applied AETM to NISs and designed the controller. The authors in [26] focused on an adaptive event-triggered decentralized filtering scheme for the networked nonlinear interconnected systems.

Although the network resource constraints can be alleviated by effective data transmission schemes, the openness of network in the interconnected systems still brings the problem of network security, which will greatly damage the stability of the system. During the past decades, there has been a surge of interests in the study of cyber-attacks [27–32]. In the existing literatures, replay attacks and deception attacks are two classic forms of attacks that have gained considerable attentions. Replay attacks attempt to replay a series of previously recorded transmissions in place of the real data being transmitted over the network. As a result, system stability is affected significantly, which results in system performance deterioration [33–35]. Deception attacks usually inject malicious data into the sensor and controller, which cause data transmission interruption and information loss [36–42]. For example, in [39], with a view to deal with the impact of deception attacks, Ding et al. specifically addressed data-driven fault detection for nonlinear systems. In view of the cyber–physical systems under randomly occurring false data injection attacks, the authors in [40] studied the event-triggered adaptive sliding mode control problem. The authors in [41] mainly studied event-triggered-based security leader-follow consensus control for multi-agent systems under hybrid cyber-attacks.

However, the security control problem for NIS under AETM and cyber-attacks has not been fully exploited to the best of our knowledge. Although some of the existing control method about NIS [25,43] have adopted the event-triggered schemes to save the limited network resources, most of them did not consider the abnormal data which are triggered by the triggering condition mistakenly. Besides, it is difficult to stabilize the controlled plant when it is attacked by malicious attackers. Motivated by the above discussions, this paper investigates the secure adaptive event-triggered controller design for NISs with cyber-attacks. The innovation points of this paper are as follows.

(1) A new AETM with dynamic threshold parameter is proposed to reduce the network congestion which takes the mutation data into consideration and can avoid some unnecessary abrupt data transmission.

(2) On the basis of the AETM, considering the influence of cyber-attacks, a new model of NISs is established.

(3) The sufficient condition to ensure the stability of the augmented system is derived, and the design method of the controller is presented.

The rest of this article is organized as follows. Section 2 introduces the control model of NISs with AETM and cyber-attacks. The sufficient condition of system stability is derived, and the required controller design method is given in Section 3. In Section 4, a simulation example is given to verify the effectiveness of the design method. Section 5 presents the conclusions.

Notation: $\mathbb{R}^m$ denotes the Euclidean space with m-dimensional, and $\mathbb{R}^{m\times n}$ represents the set of $m \times n$ real matrices, respectively; I stands for the identity matrix with appropriate dimension; the notation $X > 0$, for $X \in \mathbb{R}^{m\times m}$ means that the matrix X is real symmetric positive definite ; E is the expectation operator. $\|\cdot\|$ stands for the Euclidean norm. For a symmetric matrix $\begin{bmatrix} T_1 & * \\ T_2 & T_3 \end{bmatrix}$ with a matrix T_2 and two symmetric matrices T_1 and T_3, the $*$ in the matrix is used to represent the terms derived from the symmetry.

2. System description and modeling

Consider a NIS consisted by n_s subsystems, in which the ith subsystem S_i ($i \in \{1, 2, \ldots, n_s\} \triangleq \mathcal{N}$) is depicted as:

$$\dot{x}_i(t) = A_i x_i(t) + \sum_{j\in\mathcal{N}_{-i}} D_{ij} x_j(t - \eta_{ij}(t)) + B_i u_i(t) + f_i(x_i(t), t), \tag{1}$$

where $x_i(t) \in R^{n_{x_i}}$ is the system state of S_i, and $u_i(t) \in R^{n_{u_i}}$ represents the control input vector of S_i; A_i, D_{ij} and B_i are constant matrices of appropriate dimensions; $f_i(x_i(t), t)$ represents the nonlinear perturbations with $f_i(x_i(0), 0) = 0$; $\eta_{ij}(t)$ represents the coupled delay between subsystems S_i and S_j, which satisfies $0 \leqslant \dot{\eta}_{ij}(t) \leqslant \bar{\eta}_{ij}$; $\mathcal{N}_{-i} \triangleq \{1, 2, \ldots, i-1, i+1, \ldots, n_s\}$.

It is assumed that $f_i(x_i(t), t)$ satisfies [44]:

$$\|f_i(x_i(t), t)\| \leqslant \rho_i^2 \|F_i x_i(t)\|, \tag{2}$$

where ρ_i and F_i are known positive scalar and known matrix, respectively.

Remark 1. The nonlinear perturbations $f_i(x_i(t), t)$ in this paper are assumed to have an upper bound and satisfy Eq. (2). Similar assumption has been widely used in some existing publications (see [4,44] for example). The limitation of this assumption in (2) lies that the bound information provides nothing about the inner variation information of the nonlinearities.

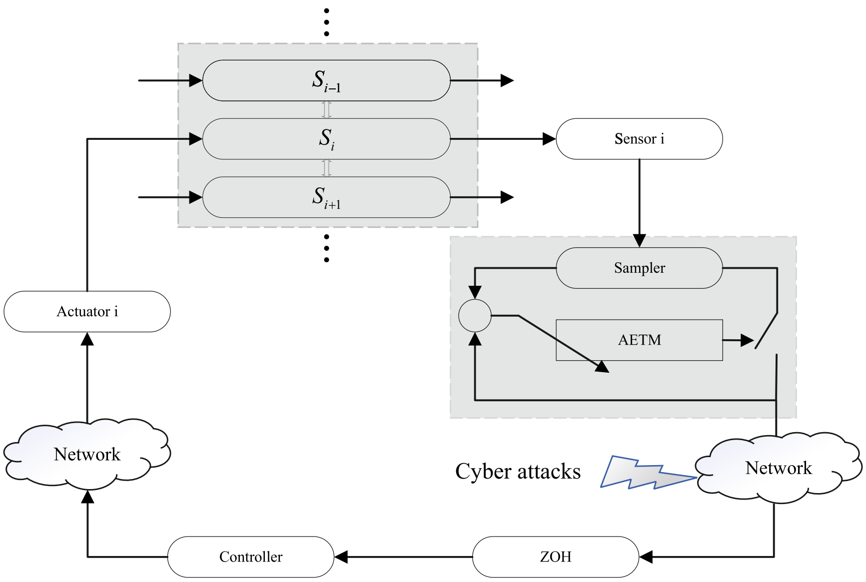

Fig. 1. The framework of the NIS subject to AETM and cyber-attacks.

The main aim of this study is to stabilize the addressed NIS (1) under AETM and cyber-attacks by a decentralized control method. For each subsystem S_i, the controller input is constructed as:

$$u_i(t) = K_i x_i(t). \tag{3}$$

The framework of the NIS under AETM and cyber-attacks is shown in Fig. 1, where the sensor, sampler, AETM, controller, and actuator are deployed in each S_i $(i \in \mathcal{N})$. Considering the fact that the abrupt data may be mistaken for necessary transmitted data with the traditional event triggered scheme, a new type of AETM is proposed to deal with the restricted network resources which aims to avoid the unnecessary transmission. The following event-triggered condition is adopted

$$\varphi_i^T(t)\Phi_i\varphi_i(t) - \sigma_i(t)x_i^T(\mu_k^i h + lh)\Phi_i x_i(\mu_k^i h + lh) \leqslant 0, \tag{4}$$

where $\varphi_i(t) = x_i(\mu_k^i h) - x_i(\mu_k^i h + \Delta h)$, $x_i(\mu_k^i h + \Delta h) = \delta_i[x_i(\mu_k^i h + lh) - x_i(\mu_k^i h)] + x_i(\mu_k^i h)$; h is the sampling period of the intelligent sensor; $\delta_i \in (0, 1]$ is an adjustment factor; $l, k \in \mathbb{N}$; $x_i(\mu_k^i h)$ and $x_i(\mu_k^i h + lh)$ represent the latest transmitted signal and the current sampling signal of sensor i, respectively; $\Phi_i > 0$ is a weight matrix; the threshold $\sigma_i(t)$ denotes an adaptive-triggered parameter satisfying the following law [24]:

$$\dot{\sigma}_i(t) = \frac{1}{\sigma_i(t)}(\frac{1}{\sigma_i(t)} - \vartheta_i)\varphi_i^T(t)\Phi_i\varphi_i(t), \tag{5}$$

where $\sigma_i(0) \in (0, 1]$ and $\vartheta_i \geqslant 1$ is a given constant.

Only when the condition (4) is broken, the sampled data will be transmitted to the network. Therefore, the next triggering instant $\mu_{k+1}^i h$ is as follows:

$$\mu_{k+1}^i h = \mu_k^i h + \min_{l \in N}\{lh \mid \varphi_i^T(t)\Phi_i\varphi_i(t) > \sigma_i(t)x_i^T(\mu_k^i h + lh)\Phi_i x_i(\mu_k^i h + lh)\}. \tag{6}$$

Define $\tau_i(t) = t - \mu_k^i h - lh$, one can find that $0 \leq \tau_1^i \leqslant \tau_i(t) < \tau_2^i$. Under the AETM (4), combine the definitions of $\tau_i(t)$ and $\varphi_i(t)$, the real transmitted data can be rewritten as

$$x_i(\mu_k^i h) = x_i(t - \tau_i(t)) + \frac{1}{\delta_i}\varphi_i(t). \tag{7}$$

Remark 2. In triggering condition (4), $\sigma_i(t)$ is an adaptive-triggered parameter that determines the frequency of the AETM. AETM can be dynamically adjusted according to real-time system state to flexibly transfer the sampled data. When the system is gradually stabilized, the adaptive law $\dot{\sigma}_i(t) \to 0$ indicates that the AETM threshold in (4) remains a constant and the AETM is converted to statical event-triggered mechanism.

In this study, we assume the triggered data are transmitted to the controller via an unreliable communication network, which is subject to randomly occurring cyber-attacks. Taking the influences of the cyber-attacks and AETM into account, the real input of the controller of subsystem S_i is expressed as

$$\bar{u}_i(\mu_k^i h) = K_i x_i(t-\tau_i(t)) + \frac{1}{\delta_i} K_i \varphi_i(t) + \alpha_i(t) K_i g_i(\mu_k^i h), \tag{8}$$

where $g_i(\cdot)$ denotes the cyber-attacks and $\alpha_i(t) \in \{0, 1\}$ is a Bernoulli variable which satisfies the following statistical properties:

$$E\{\alpha_i(t)\} = \bar{\alpha}_i,\ E\{(\alpha_i(t) - \bar{\alpha}_i)^2\} = \bar{\alpha}_i(1-\bar{\alpha}_i).$$

Remark 3. In (8), $\alpha_i(t)$ is used to describe whether the injection attacks take place or not. $\alpha_i(t) = 1$ indicates that cyber-attacks are active and the transmitted data are attacked; $\alpha_i(t) = 0$ indicates that communication network is reliable and safe.

Remark 4. The adopted AETM (4) is more general than some ones in [18,25,43]. With consideration of the mutation data, the AETM (4) is proposed to prevent the abnormal data being transmitted in this paper by introducing an artificial output instead of the current sampled state transmitted to AETM in [25,43]. The AETM (4) in this paper is capable to adjust the triggering condition and avoid mutation data transmission according to variation of the system state, only some necessary sampling packets can be transmitted via the network. By choosing $\delta_i = 1$ in the AETM, the designed AETM in this paper can include the ETM in [25,43] as a particular case, by setting $\delta_i = 1$ and $\sigma_i(t) \equiv 0$, the AETM in (4) will become the ones in [18,23]. Thus the AETM (4) is more general.

Combine (1) and (8), the mathematical model of S_i with cyber-attacks and AETM can be expressed as:

$$\begin{aligned}\dot{x}_i(t) =& A_i x_i(t) + \sum_{j\in\mathcal{N}_{-i}} D_{ij} x_j(t-\eta_{ij}(t)) + B_i K_i[x_i(t-\tau_i(t)) + \frac{1}{\delta_i}\varphi_i(t)] + \alpha_i(t) B_i K_i g_i(x_i(\mu_k^i h)) + f_i(x_i(t), t)\\ =& \mathfrak{A}_i(t) + (\alpha_i(t) - \bar{\alpha}_i) B_i K_i g_i(x_i(\mu_k^i h))\end{aligned} \tag{9}$$

where $\mathfrak{A}_i(t) = A_i x_i(t) + \sum_{j\in\mathcal{N}_{-i}} D_{ij} x_j(t-\eta_{ij}(t)) + B_i K_i[x_i(t-\tau_i(t)) + \frac{1}{\delta_i}\varphi_i(t)] + \bar{\alpha}_i B_i K_i g_i(x_i(\mu_k^i h)) + f_i(x_i(t), t)$.

Some important definition and lemmas are introduced as follows to derive the subsequent results.

Definition 1 ([4]). For given $\beta > 0$, the stability of NIS (1) with cyber-attacks is achieved in secure sense if there exist $P > 0$ and $T(\beta, x_{t_0}, P)$, such that $x(t) \in \mathcal{E}\{P, \beta\}$ for $\forall t \geq t_0 + T$, where $\mathcal{E}\{P, \beta\} = \mathcal{E}\{x^T(t) P x(t) < \beta^2\}$.

Assumption 1 ([4]). The cyber-attacks $g_i(\mu_k^i h)$ satisfy the following inequation:

$$\|g_i(\mu_k^i h)\|_2 \leqslant \beta^3. \tag{10}$$

where $\beta > 0$ is a known scalar.

Remark 5. In this paper, the deception attacks are modeled as a limited magnitude signal. In practice, some information including the probability and the bound can be tested. The bound is assumed in Assumption 1 for security requirements, which is important to derive the stability of NIS (1) with cyber-attacks in secure sense.

Lemma 1 ([45]). *Assume $\tau_i(t) \in [\tau_1^i, \tau_2^i)$, for any constant matrices $R_1^i \in \mathbb{R}^{m\times m}$, $R_2^i \in \mathbb{R}^{m\times m}$ and $U_1 \in \mathbb{R}^{m\times m}$, $U_2 \in \mathbb{R}^{m\times m}$ satisfying $\begin{bmatrix} R_\upsilon^i & * \\ U_\upsilon & R_\upsilon^i \end{bmatrix} \geqslant 0$, ($\upsilon = 1, 2$), we have:*

$$-\tau_1^i \int_{t-\tau_1^i}^{t} \dot{x}_i^T(s) R_1^i \dot{x}_i(s) ds \leqslant \varrho_i^T(t) \mathfrak{M}_1^i \varrho_i(t), \tag{11}$$

$$-(\tau_2^i - \tau_1^i) \int_{t-\tau_2^i}^{t-\tau_1^i} \dot{x}_i^T(s) R_2^i \dot{x}_i(s) ds \leqslant \varrho_i^T(t) \mathfrak{M}_2^i \varrho_i(t) \tag{12}$$

in which

$$\begin{aligned}
\varrho_i^T(t) &= \begin{bmatrix} x_i^T(t) & \varrho_{1i}^T(t) & \varrho_{2i}^T(t) \end{bmatrix}^T\\
\varrho_{1i}^T(t) &= \begin{bmatrix} x_i^T(t-\tau_1^i) & x_i^T(t-\tau_i(t)) & x_i^T(t-\tau_2^i) & \varphi_i^T(t) & g_i^T(\mu_k^i h) & f_i^T(x_i(t), t) \end{bmatrix}^T\\
\varrho_{2i}^T(t) &= \begin{bmatrix} x_1^T(t-\eta_{i1}(t)) & \cdots & x_{i-1}^T(t-\eta_{i(i-1)}(t)) & x_{i+1}^T(t-\eta_{i(i+1)}(t)) & \cdots & x_{n_s}^T(t-\eta_{in_s}(t)) \end{bmatrix}^T\\
\mathfrak{M}_1^i &= -(\Theta_1 - \Theta_2)^T R_1^i (\Theta_1 - \Theta_2),\ \mathfrak{M}_2^i = -\begin{bmatrix} \Theta_2 - \Theta_3 \\ \Theta_3 - \Theta_4 \end{bmatrix}^T \begin{bmatrix} R_2^i & * \\ U_i & R_2^i \end{bmatrix} \begin{bmatrix} \Theta_2 - \Theta_3 \\ \Theta_3 - \Theta_4 \end{bmatrix}.\\
\Theta_1 &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix},\ \Theta_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}\\
\Theta_3 &= \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & \cdots & 0 \end{bmatrix},\ \Theta_4 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}
\end{aligned}$$

Lemma 2 ([45]). *For any positive scalar ϵ and matrices $P > 0$, $R > 0$, the inequality holds as follow:*

$$-PR^{-1}P \leqslant -2\epsilon P + \epsilon^2 R. \tag{13}$$

3. Main results

Theorem 1. *For given parameters β, ρ_i, $\bar{\eta}_{ij}$, δ_i, $\bar{\alpha}_i$, ϑ_i, time delay upper bound τ_1^i, τ_2^i, matrices K_i and F_i, the system (9) is asymptotically stable in secure sense under the AETM and cyber-attacks if there exist matrices $P_i > 0$, $Q_v^i > 0$, $Q^{ij} > 0$, $R_v^i > 0$, $U_i > 0$ $(v = 1, 2)$ and $\Phi_i > 0$ with appropriate dimensions that the following inequality holds for $i \in \mathcal{N}, j \in \mathcal{N}_{-i}$*

$$\Psi_i = \begin{bmatrix} \Xi_{1i} & * & * & * & * & * \\ \Xi_{2i} & \Xi_{3i} & * & * & * & * \\ \Xi_{4i} & 0 & \Xi_{5i} & * & * & * \\ \Xi_{6i} & 0 & 0 & \Xi_{7i} & * & * \\ \Xi_{8i} & 0 & 0 & 0 & \Xi_{9i} & * \\ \Xi_{10i} & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{14}$$

$$\begin{bmatrix} R_v^i & * \\ U_v & R_v^i \end{bmatrix} \geqslant 0, (v = 1, 2) \tag{15}$$

in which

$$\Xi_{1i} = \begin{bmatrix} \Theta_{1i} & * & * & * \\ \Theta_{2i} & \Theta_{3i} & * & * \\ \Omega_i^T & \Theta_{5i} & \Theta_{6i} & * \\ 0 & U & \Theta_{7i} & \Theta_{8i} \end{bmatrix}, \Omega_i = P_i B_i K_i$$

$$\Theta_{1i} = P_i A_i + A_i^T P_i + Q_1^i + Q_2^i + \sum_{l \in \mathcal{M}_i} Q^{li} - R_1^i + \beta P_i, \Theta_{2i} = R_1^i, \Theta_{3i} = -Q_1^i - R_1^i - R_2^i$$

$$\Theta_{5i} = R_2^i - U_i, \Theta_{6i} = -2R_2^i + U_i + U_i^T + \Phi_i, \Theta_{7i} = R_2^i - U_i, \Theta_{8i} = -Q_2^i - R_2^i$$

$$\Xi_{2i} = \begin{bmatrix} \frac{1}{\delta_i}\Omega_i^T & 0 & 0 & 0 \\ \bar{\alpha}_i \Omega_i^T & 0 & 0 & 0 \\ P_i & 0 & 0 & 0 \end{bmatrix}, \Xi_{3i} = diag\{-\vartheta_i \Phi_i, -I, -I\},$$

$$\Xi_{4i} = \begin{bmatrix} D_{i1}^T P_i & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ D_{i,i-1}^T P_i & 0 & 0 & 0 \\ D_{i,i+1}^T P_i & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ D_{in_s}^T P_i & 0 & 0 & 0 \end{bmatrix}$$

$$\Xi_{5i} = diag\{-(1-\bar{\eta}_{i1})Q^{i1}, \ldots, -(1-\bar{\eta}_{i,i-1})Q^{i,i-1}, -(1-\bar{\eta}_{i,i+1})Q^{i,i+1}, \ldots, -(1-\bar{\eta}_{in_s})Q^{in_s}\}$$

$$\Xi_{6i} = \begin{bmatrix} \tau_1^i \Lambda_{1i} & \tau_1^i \Lambda_{2i} & \tau_1^i \Lambda_{3i} & \tau_1^i \Lambda_{4i} \end{bmatrix}^T, \varpi = \sqrt{\bar{\alpha}_i(1-\bar{\alpha}_i)},$$

$$\Lambda_{1i} = \begin{bmatrix} P_i A_i & 0 & \Omega_i & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \Lambda_{2i} = \begin{bmatrix} \frac{1}{\delta_i}\Omega_i & \bar{\alpha}_i \Omega_i & P_i \\ 0 & \varpi \Omega_i & 0 \end{bmatrix}$$

$$\Lambda_{3i} = \begin{bmatrix} P_i D_{i1} & \cdots & P_i D_{i,i-1} \\ 0 & \cdots & 0 \end{bmatrix}, \Lambda_{4i} = \begin{bmatrix} P_i D_{i,i+1} & \cdots & P_i D_{in_s} \\ 0 & \cdots & 0 \end{bmatrix}$$

$$\neq \Xi_{7i} = diag\{-P_i(R_1^i)^{-1}P_i, -P_i(R_1^i)^{-1}P_i\},$$

$$\Xi_{8i} = \begin{bmatrix} (\tau_2^i - \tau_1^i)\Lambda_{1i} & (\tau_2^i - \tau_1^i)\Lambda_{2i} & (\tau_2^i - \tau_1^i)\Lambda_{3i} & (\tau_2^i - \tau_1^i)\Lambda_{4i} \end{bmatrix}^T,$$

$$\Xi_{9i} = diag\{-P_i(R_2^i)^{-1}P_i, -P_i(R_2^i)^{-1}P_i\}, \Xi_{10,i} = \begin{bmatrix} \rho_i F_i & 0 & 0 & 0 \end{bmatrix}$$

Proof. See Appendix A.

The sufficient condition is given in Theorem 1, which ensures the asymptotic stability of the system (9). On basis of Theorem 1, the adaptive event-triggered controller gains of NISs under cyber-attacks will be given in the following theorem.

Theorem 2. *For given parameters ρ_i, β, $\bar{\eta}_{ij}$, ϵ_i, δ_i, $\bar{\alpha}_i$, ϑ_i, time delay upper bound τ_1^i, τ_2^i, matrix F_i, the system (9) is asymptotically stable in secure sense under the AETM and cyber-attacks if there exist matrices $X_i > 0$, $\hat{R}_v^i > 0$, $\hat{Q}_v^i > 0$, $\hat{Q}^{ij} > 0$, $\hat{U}_i > 0$,*

$\hat{\Phi}_i > 0$ and Y_i $(v = 1, 2)$ with appropriate dimensions, such that the LMI holds for $i \in \mathcal{N}, j \in \mathcal{N}_{-i}$

$$\hat{\Psi}_i = \begin{bmatrix} \hat{\Xi}_{1i} & * & * & * & * & * \\ \hat{\Xi}_{2i} & \hat{\Xi}_{3i} & * & * & * & * \\ \hat{\Xi}_{4i} & 0 & \hat{\Xi}_{5i} & * & * & * \\ \hat{\Xi}_{6i} & 0 & 0 & \hat{\Xi}_{7i} & * & * \\ \hat{\Xi}_{8i} & 0 & 0 & 0 & \hat{\Xi}_{9i} & * \\ \hat{\Xi}_{10i} & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{16}$$

$$\begin{bmatrix} \hat{R}_v^i & * \\ \hat{U}_v & \hat{R}_v^i \end{bmatrix} \geqslant 0, (v = 1, 2) \tag{17}$$

in which

$$\hat{\Xi}_{1i} = \begin{bmatrix} \hat{\Theta}_{1i} & * & * & * \\ \hat{\Theta}_{2i} & \hat{\Theta}_{3i} & * & * \\ \hat{\Omega}_i^T & \hat{\Theta}_{5i} & \hat{\Theta}_{6i} & * \\ 0 & \hat{U} & \hat{\Theta}_{7i} & \hat{\Theta}_{8i} \end{bmatrix}, \hat{\Omega}_i = B_i Y_i,$$

$$\hat{\Theta}_{1i} = A_i X_i + X_i A_i^T + \hat{Q}_1^i + \hat{Q}_2^i + \sum_{l \in \mathcal{M}_i} \hat{Q}^{li} - \hat{R}_1, \hat{\Theta}_{2i} = \hat{R}_1^i, \hat{\Theta}_{3i} = -\hat{Q}_1^i - \hat{R}_1^i - \hat{R}_2^i$$

$$\hat{\Theta}_{5i} = \hat{R}_2^i - \hat{U}_i, \hat{\Theta}_{6i} = -2\hat{R}_2^i + \hat{U}_i + \hat{U}_i^T + \hat{\Phi}_i, \hat{\Theta}_{7i} = \hat{R}_2^i - \hat{U}_i, \hat{\Theta}_{8i} = -\hat{Q}_2^i - \hat{R}_2^i$$

$$\hat{\Xi}_{2i} = \begin{bmatrix} \frac{1}{\delta_i}\hat{\Omega}_i^T & 0 & 0 & 0 \\ \bar{\alpha}_i \hat{\Omega}_i^T & 0 & 0 & 0 \\ I & 0 & 0 & 0 \end{bmatrix}, \hat{\Xi}_{3i} = diag\{-\vartheta_i \hat{\Phi}_i, -I, -I\},$$

$$\hat{\Xi}_{4i} = \begin{bmatrix} X_i D_{i1}^T & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ X_i D_{i,i-1}^T & 0 & 0 & 0 \\ X_i D_{i,i+1}^T & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ X_i D_{in_s}^T & 0 & 0 & 0 \end{bmatrix}$$

$$\hat{\Xi}_{5i} = diag\{-(1-\bar{\eta}_{i1})\hat{Q}^{i1}, \ldots, -(1-\bar{\eta}_{i,i-1})\hat{Q}^{i,i-1}, -(1-\bar{\eta}_{i,i+1})\hat{Q}^{i,i+1}, \ldots, -(1-\bar{\eta}_{in_s})\hat{Q}^{in_s}\}$$

$$\hat{\Xi}_{6i} = \begin{bmatrix} \tau_1^i \hat{\Lambda}_{1i} & \tau_1^i \hat{\Lambda}_{2i} & \tau_1^i \hat{\Lambda}_{3i} & \tau_1^i \hat{\Lambda}_{4i} \end{bmatrix}^T, \varpi = \sqrt{\bar{\alpha}_i(1-\bar{\alpha}_i)},$$

$$\hat{\Lambda}_{1i} = \begin{bmatrix} A_i X_i & 0 & \hat{\Omega}_i & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \hat{\Lambda}_{2i} = \begin{bmatrix} \frac{1}{\delta_i}\hat{\Omega}_i & \bar{\alpha}_i \hat{\Omega}_i & X_i \\ 0 & \varpi \hat{\Omega}_i & 0 \end{bmatrix}$$

$$\hat{\Lambda}_{3i} = \begin{bmatrix} D_{i1} X_i & \cdots & D_{i,i-1} X_i \\ 0 & \cdots & 0 \end{bmatrix}, \hat{\Lambda}_{4i} = \begin{bmatrix} D_{i,i+1} X_i & \cdots & D_{in_s} X_i \\ 0 & \cdots & 0 \end{bmatrix}$$

$$\hat{\Xi}_{7i} = diag\{-2\epsilon_i X_i + \epsilon_i^2 \hat{R}_1^i, -2\epsilon_i X_i + \epsilon_i^2 \hat{R}_1^i\},$$

$$\hat{\Xi}_{8i} = \begin{bmatrix} (\tau_2^i - \tau_1^i)\hat{\Lambda}_{1i} & (\tau_2^i - \tau_1^i)\hat{\Lambda}_{2i} & (\tau_2^i - \tau_1^i)\hat{\Lambda}_{3i} & (\tau_2^i - \tau_1^i)\hat{\Lambda}_{4i} \end{bmatrix}^T,$$

$$\hat{\Xi}_{9i} = diag\{-2\epsilon_i X_i + \epsilon_i^2 \hat{R}_2^i, -2\epsilon_i X_i + \epsilon_i^2 \hat{R}_2^i\}, \hat{\Xi}_{10i} = \begin{bmatrix} \rho_i F_i X_i & 0 & 0 & 0 \end{bmatrix}$$

Moreover, the expected controller gain K_i in (3) and the adaptive event-triggered matrix Φ_i of subsystem S_i are derived by

$$K_i = Y_i X_i^{-1}, \tag{18}$$

$$\Phi_i = X_i^{-1} \hat{\Phi}_i X_i^{-1}. \tag{19}$$

Proof. See Appendix B.

Remark 6. The computational complexity of the proposed method depends on the number of scalar decision variables and the size of the derived conditions in Theorem 2, which reflects the factors of the number of system nodes, the information of cyber-attacks and the AETM. It can be observed from (16) and (17) that the size of these conditions is related to the number of the subsystems and the dimensions of $x_i(t) \in R^{n_{x_i}}$, $x_j(t - \eta_{ij}(t))$, $u_i(t) \in R^{n_{u_i}}$, $f_i(x_i(t), t)$, $\varphi_i(t)$ and the cyber-attacks $g_i(\cdot)$. The larger number of the nodes and the higher dimensions of system matrices, the longer computing time will be needed to find the solution.

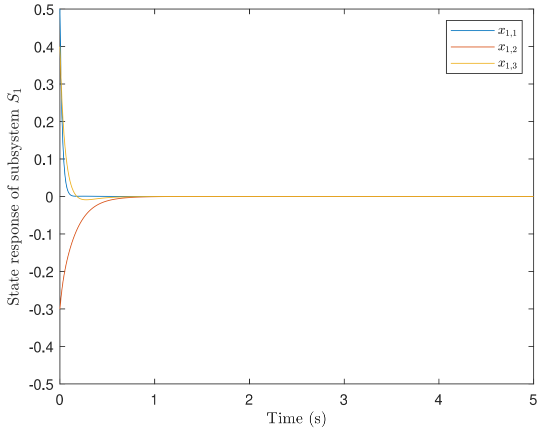

Fig. 2. State response of S_1.

4. Numerical example

A simulation example is given to verify the feasibility of the proposed adaptive event-based security control algorithm for the interconnected systems with stochastic cyber-attacks in this section.

Considering the subsystems S_1, S_2 and S_3 with the following parameters:

$$A_1=\begin{bmatrix}-38.8000 & -0.4000 & -2.0000\\ 2.8000 & -6.0000 & -0.4000\\ -3.6000 & 2.8000 & -14.8000\end{bmatrix}, A_2=\begin{bmatrix}-41.2000 & -4.0000 & -16.0000\\ -16.0000 & -6.4000 & -16.0000\\ 8.0000 & 8.0000 & -4.0000\end{bmatrix},$$
$$A_3=\begin{bmatrix}-13.0000 & -10.2000 & 1.0000\\ -0.4000 & -13.0000 & -2.5000\\ -9.5000 & -6.0000 & -6.0000\end{bmatrix} \tag{20}$$
$$B_1=\begin{bmatrix}0.4000\\ -0.8000\\ 0.1000\end{bmatrix}, B_2=\begin{bmatrix}-0.0600\\ 0.0500\\ 0.0200\end{bmatrix}, B_3=\begin{bmatrix}-0.0600\\ 0.0500\\ 0.0300\end{bmatrix},$$

Let the coupled matrix $D_{12}, D_{21}, D_{13}, D_{31}$ and the upper bound of time delay $\bar{\eta}_{12}, \bar{\eta}_{21}, \eta_{13}, \bar{\eta}_{31}$ be $D_{12} = -0.05I, D_{21} = -0.06I, D_{13} = -0.05I, D_{31} = -0.06I, \bar{\eta}_{12} = 0.4, \bar{\eta}_{21} = 0.4, \bar{\eta}_{13} = 0.4, \bar{\eta}_{31} = 0.4$, respectively, in which I is the identify matrix with appropriate dimension. Meanwhile, $F_1 = 0.01I, F_2 = 0.01I, F_3 = 0.01I$ and $\rho_1 = 0.05, \rho_2 = 0.07, \rho_3 = 0.07$. The relative parameters in event-triggered mechanism is $\delta_1 = 0.25, \delta_2 = 0.02, \delta_3 = 0.02$.

Moreover, the occurrence probability of cyber-attacks are set as $\bar{\alpha}_1 = 0.61, \bar{\alpha}_2 = 0.22, \bar{\alpha}_3 = 0.61$. $\vartheta_1 = 0.3, \vartheta_2 = 0.6, \vartheta_3 = 0.5$. $\tau_1^1 = \tau_1^2 = 0.1, \tau_2^1 = \tau_2^2 = 0.2$. $\epsilon_1 = \epsilon_2 = 1$. According to Theorem 2, the expected controller gain and event-triggered matrix can be derived as:

$$K_1=\begin{bmatrix}-0.0068 & 0.0115 & -0.0033\end{bmatrix}, K_2=\begin{bmatrix}0.0008 & -0.0007 & -0.0002\end{bmatrix}, K_3=\begin{bmatrix}0.0004 & -0.0005 & -0.0003\end{bmatrix}$$
$$\Phi_1=\begin{bmatrix}4.1676 & 0.2655 & -3.0891\\ -0.2954 & 4.2333 & -15.3513\\ 3.0754 & 15.3492 & 4.2818\end{bmatrix}, \Phi_2=\begin{bmatrix}4.2292 & 1.0750 & 0.8358\\ -0.8515 & 4.0802 & -0.1802\\ -1.2760 & 0.3705 & 3.8625\end{bmatrix},$$
$$\Phi_3=\begin{bmatrix}4.2527 & 0.4084 & 0.3491\\ -0.4408 & 4.2394 & 2.3389\\ -0.1580 & -2.1397 & 4.1093\end{bmatrix} \tag{21}$$

Set the initial states $x_1(0) = \begin{bmatrix}0.5 & -0.3 & 0.4\end{bmatrix}^T, x_2(0) = \begin{bmatrix}0.4 & -0.3 & 0.2\end{bmatrix}^T, x_3(0) = \begin{bmatrix}0.2 & -0.4 & 0.3\end{bmatrix}^T$, with the above parameters, by MATLAB simulation, the responses of each subsystem under AETM and cyber-attacks are depicted in Figs. 2–4, from which we can see the addressed system can be stabilized by the designed controller. Figs. 8–10 show the event-triggered instants and the released intervals, which shows the transmitted data are sent to the communication network according to the triggering condition. The curves of the adaptive parameter $\sigma_i(t)$ of the subsystems S_1, S_2 and S_3 are illustrated in Figs. 5–7, which are not preset constant values of each subsystem, instead, $\sigma_i(t)$ can be dynamically changed with current sampled data and the latest transmitted ones.

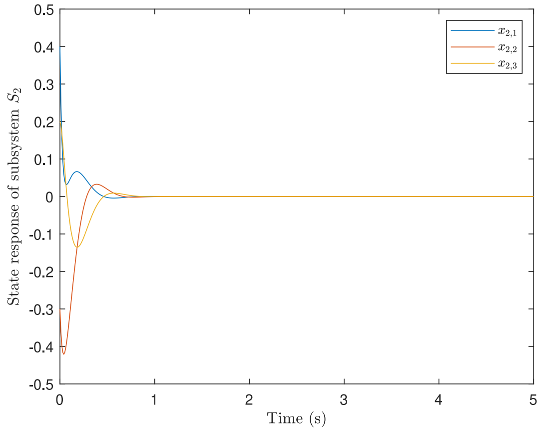

Fig. 3. State response of S_2.

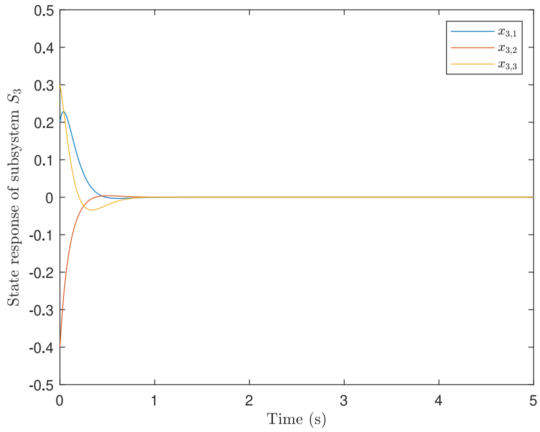

Fig. 4. State response of S_3.

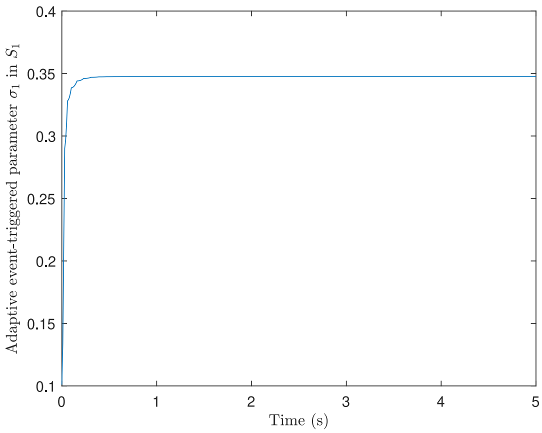

Fig. 5. Adaptive event-triggered parameter σ_1 in S_1.

5. Conclusions

The adaptive event-based security control of NISs with cyber-attacks is investigated in this article. Firstly, the AETM is adopted to economize the restricted network resources by dynamically adjusting thresholds. Then, by taking the effect of the cyber-attacks into consideration, a networked interconnected control model with AETM is established. By means of

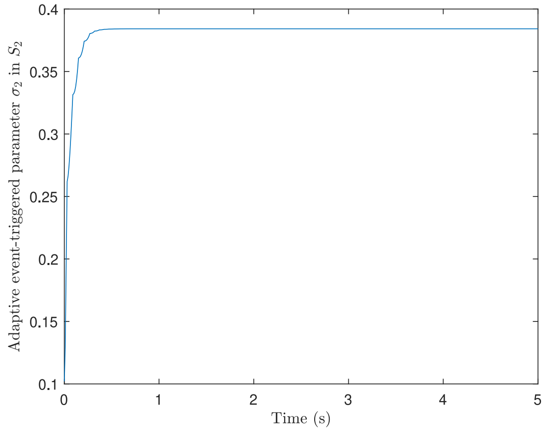

Fig. 6. Adaptive event-triggered parameter σ_1 in S_2.

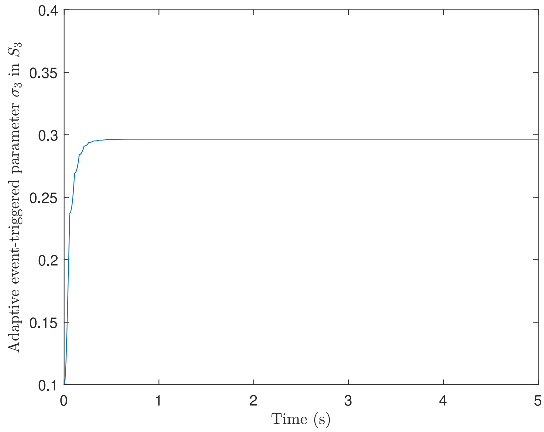

Fig. 7. Adaptive event-triggered parameter σ_2 in S_3.

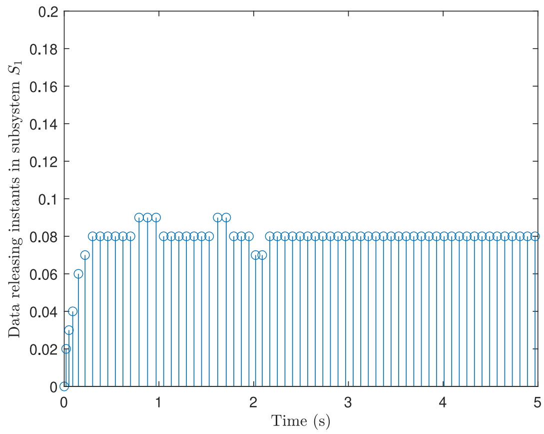

Fig. 8. Data releasing instants of S_1.

Lyapunov stability theory and LMI techniques, sufficient condition to guarantee the stability of the systems is obtained. Finally, a simulation example is given to verify the efficiency of the controller design algorithm for NISs. In addition, for the sake of improving the ability of the system in resisting cyber-attacks, we will study the outlier resistant filtering design for dynamic event-triggered NISs under hybrid attacks in the future.

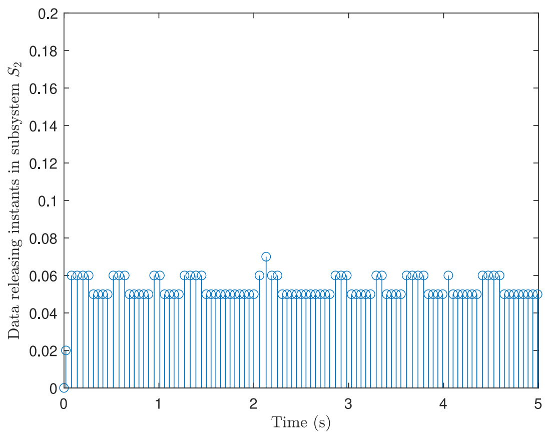

Fig. 9. Data releasing instants of S_2.

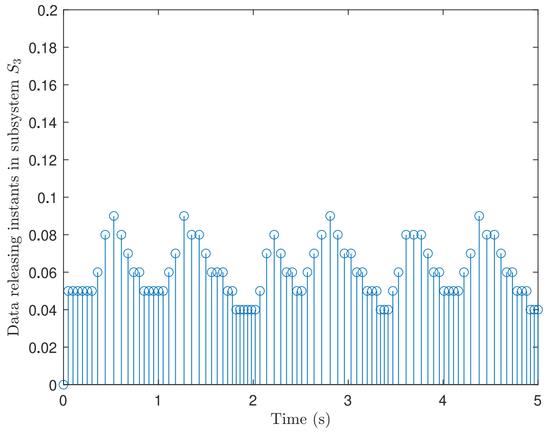

Fig. 10. Data releasing instants of S_3.

CRediT authorship contribution statement

Jinliang Liu: Methodology, Proved the main results, Performed the simulation, Writing – original draft, Investigation, Writing – review & editing. **Yan Qian:** Writing – original draft. **Lijuan Zha:** Provided the main idea, Resources, Supervision. **Engang Tian:** Review & editing, Validation. **Xiangpeng Xie:** Review & editing, Validation.

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.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 62273174, Grant 61973152 and Grant 61903182, in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20211290 and in part by the Qing Lan Project, China.

Appendix A

Choose the following Lyapunov functional candidate for the subsystem S_i as

$$V(t)=\sum_{i\in\mathcal{N}}[V_1^i(t)+V_2^i(t)+V_3^i(t)+V_4^i(t)], \tag{22}$$

where

$$\begin{aligned}
V_1^i(t) &= x_i^T(t)P_ix_i(t),\\
V_2^i(t) &= \int_{t-\tau_1^i}^{t} x_i^T(s)Q_1^ix_i(s)ds+\int_{t-\tau_2^i}^{t} x_i^T(s)Q_2^ix_i(s)ds+\sum_{j\in\mathcal{N}_{-i}}\int_{t-\eta_{ij}(t)}^{t} x_j^T(s)Q^{ij}x_j(s)ds,\\
V_3^i(t) &= \tau_1^i\int_{t-\tau_1^i}^{t}\int_{s}^{t}\dot{x}_i^T(v)R_1^i\dot{x}_i(v)dvds+(\tau_2^i-\tau_1^i)\int_{t-\tau_2^i}^{t-\tau_1^i}\int_{s}^{t}\dot{x}_i^T(v)R_2^i\dot{x}_i(v)dvds,\\
V_4^i(t) &= \frac{1}{2}\sigma_i^2(t),
\end{aligned}$$

in which $P_i>0$, $Q_1^i>0$, $Q_2^i>0$, $Q^{ij}>0$, $R_1^i>0$, $R_2^i>0$.

By taking the derivative and mathematical expectation of (22), it can be deduced that:

$$\mathrm{E}\{\mathcal{L}V_1^i(t)\} = 2x_i^T(t)P_i\mathfrak{A}_i(t), \tag{23}$$

$$\begin{aligned}
\mathrm{E}\{\mathcal{L}V_2^i(t)\} &= x_i^T(t)(Q_1^i+Q_2^i)x_i(t)-x_i^T(t-\tau_1^i)Q_1^ix_i(t-\tau_1^i)-x_i^T(t-\tau_2^i)Q_2^ix_i(t-\tau_2^i)+\sum_{j\in\mathcal{N}_{-i}}x_j^T(t)Q^{ij}x_j(t)\\
&\quad-\sum_{j\in\mathcal{N}_{-i}}(1-\dot{\eta}_{ij}(t))x_j^T(t-\eta_{ij}(t))Q_1^{ij}x_j(t-\eta_{ij}(t)),
\end{aligned} \tag{24}$$

$$\begin{aligned}
\mathrm{E}\{\mathcal{L}V_3^i(t)\} &= \mathrm{E}\left\{\dot{x}_i^T(t)[(\tau_1^i)^2R_1^i+(\tau_2^i-\tau_1^i)^2R_2^i]\dot{x}_i(t)\right\}-\tau_1^i\int_{t-\tau_1^i}^{t}\dot{x}_i^T(s)R_1^i\dot{x}_i(s)ds\\
&\quad-(\tau_2^i-\tau_1^i)\int_{t-\tau_2^i}^{t-\tau_1^i}\dot{x}_i^T(s)R_2^i\dot{x}_i(s)ds,
\end{aligned} \tag{25}$$

$$\begin{aligned}
\mathrm{E}\{\mathcal{L}V_4^i(t)\} &= \sigma_i(t)\mathrm{E}\{\mathcal{L}(\sigma_i(t))\}=\sigma_i(t)\frac{1}{\sigma_i(t)}(\frac{1}{\sigma_i(t)}-\vartheta_i)\varphi_i^T(t)\Phi_i\varphi_i(t)\\
&= \frac{1}{\sigma_i(t)}\varphi_i^T(t)\Phi_i\varphi_i(t)-\vartheta_i\varphi_i^T(t)\Phi_i\varphi_i(t).
\end{aligned} \tag{26}$$

Define $(\tau_1^i)^2R_1^i \triangleq T_1^i$, $(\tau_2^i-\tau_1^i)^2R_2^i \triangleq T_2^i$ $(k=1,2)$, it yields that

$$\mathrm{E}\{\dot{x}_i^T(t)T_k^i\dot{x}_i(t)\}=\mathfrak{A}_i(t)^TT_k^i\mathfrak{A}_i(t)+\bar{\alpha}_i(1-\bar{\alpha}_i)g_i^T(\mu_k^ih)T_k^ig_i(\mu_k^ih). \tag{27}$$

By Lemma 1, one can obtain that

$$-\tau_1^i\int_{t-\tau_1^i}^{t}\dot{x}_i^T(s)R_1^i\dot{x}_i(s)ds \leqslant \varrho_i^T(t)\mathfrak{M}_1^i\varrho_i(t), \tag{28}$$

$$-(\tau_2^i-\tau_1^i)\int_{t-\tau_2^i}^{t-\tau_1^i}\dot{x}_i^T(s)R_2^i\dot{x}_i(s)ds \leqslant \varrho_i^T(t)\mathfrak{M}_2^i\varrho_i(t) \tag{29}$$

where $\varrho_i(t)$, $\mathfrak{M}_1^i$ and $\mathfrak{M}_2^i$ have been defined in Lemma 1.

When $x(t)\mathcal{E}\{P,\beta\}$ for $\forall t\geq t_0+T$, where $\mathcal{E}\{P,\beta\}=\mathcal{E}\{x^T(t)Px(t)<\beta^2\}$

Consider the adaptive event-triggered conditions in (4), it can be rewritten as

$$\frac{1}{\sigma_i(t)}\varphi_i^T(t)\Phi_i\varphi_i(t) \leqslant x_i^T(t-\tau_i(t))\Phi_ix_i(t-\tau_i(t)). \tag{30}$$

Combine (26) and (30), then, we can derive

$$\mathrm{E}\{\mathcal{L}V_4^i(t)\} \leqslant x_i^T(t-\tau_i(t))\Phi_ix_i(t-\tau_i(t))-\vartheta_i\varphi_i^T(t)\Phi_i\varphi_i(t). \tag{31}$$

For interconnected systems (1), the following equation holds:

$$\sum_{i\in\mathcal{N}}\sum_{j\in\mathcal{N}_{-i}}x_j^T(t)Q^{ij}x_j(t)=\sum_{i\in\mathcal{N}}\sum_{l\in\mathcal{M}_i}x_i^T(t)Q^{li}x_i(t). \tag{32}$$

where $\mathcal{M}_i$ represents the set of the subsystems driven by agent i.

According to Definition 1, when $x(t)$ is out of $\mathcal{E}\{P,\beta\}$ i.e. $x^T(t)Px(t) > \beta^2$, one has

$$\beta x_i^T(t)P_i x_i(t) - g_i^T(\mu_k^i h)g_i(\mu_k^i h) \geq 0 \tag{33}$$

Combining (23)–(33), we can obtain

$$\begin{aligned}
\mathrm{E}\{\mathcal{L}V(t)\} \leqslant & \sum_{i\in\mathcal{N}} 2x_i^T(t)P_i\mathfrak{A}_i(t) + x_i^T(t)(Q_1^i+Q_2^i)x_i(t) - x_i^T(t-\tau_1^i)Q_1^i x_i(t-\tau_1^i) - x_i^T(t-\tau_2^i)Q_2^i x_i(t-\tau_2^i) \\
& + \sum_{l\in\mathcal{M}_i} x_i^T(t)Q^{li}x_i(t) - \sum_{j\in\mathcal{N}_{-i}} (1-\bar{\eta}_{ij}(t))x_j^T(t-\bar{\eta}_{ij})Q^{ij}x_j(t-\eta_{ij}(t)) + \mathfrak{A}_i(t)[(\tau_1^i)^2R_1^i + (\tau_2^i-\tau_1^i)^2R_2^i]\mathfrak{A}_i(t) \\
& + \bar{\alpha}_i(1-\bar{\alpha}_i)g_i^T(\mu_k^i h)[(\tau_1^i)^2R_1^i + (\tau_2^i-\tau_1^i)^2R_2^i]g_i(\mu_k^i h) + \varrho_i^T(t)\mathfrak{M}_1^i\varrho_i(t) + \varrho_i^T(t)\mathfrak{M}_2^i\varrho_i(t) - \varphi_i^T(t)\vartheta_i\Phi_i\varphi_i(t) \\
& + x_i^T(t-\tau_i(t))\Phi_i x_i(t-\tau_i(t)) + (\rho_iF_ix_i(t))^T(\rho_iF_ix_i(t)) - f_i^T(x_i(t),t)f_i(x_i(t),t) + \beta x_i^T(t)P_ix_i(t) - g_i^T(\mu_k^i h)g_i(\mu_k^i h)
\end{aligned} \tag{34}$$

Define $T_1^i + T_2^i \triangleq T^i$, and then, combine (23)–(32), by using the Schur complement, one can get

$$\mathrm{E}\{\mathcal{L}V(t)\} \leqslant \sum_{i\in\mathcal{N}} \left\{ \varrho_i^T(t)\Xi_{1i}\varrho_i(t) + \mathfrak{A}_i(t)^T T_k^i \mathfrak{A}_i(t) + \bar{\alpha}_i(1-\bar{\alpha}_i)g_i^T(\mu_k^i h)T_k^i g_i(\mu_k^i h) \right\}, \tag{35}$$

By using the Schur complement,(35) can be ensured by (14). This means that $\mathrm{E}\{\mathcal{L}V(t)\} \leqslant 0$.

Thus the proof is completed.

Remark 7. Due to the introduction of $\sigma_i(t)$ in (4), the Lyapunov functional $V_4^i(t)$ in (22) is constructed in this paper to reduce the conservatism of the system design, which is essential to the derivation of the results.

Appendix B

Proof. By Lemma 2, for $\epsilon_i > 0$, one can deduce that

$$\begin{cases} -P_i(R_1^i)^{-1}P_i \leq -2\epsilon_iP_i + \epsilon_i^2R_1^i, \\ -P_i(R_2^i)^{-1}P_i \leq -2\epsilon_iP_i + \epsilon_i^2R_2^i, \end{cases} \tag{36}$$

In inequality (14) of Theorem 1, substitute $-P_i(R_m^i)^{-1}P_i$ with $-2\epsilon_iP_i + \epsilon_i^2R_m^i$, $(m=1,2)$. It can be concluded that

$$\tilde{\Psi}_i = \begin{bmatrix} \Xi_{1i} & * & * & * & * & * \\ \Xi_{2i} & \Xi_{3i} & * & * & * & * \\ \Xi_{4i} & 0 & \Xi_{5i} & * & * & * \\ \Xi_{6i} & 0 & 0 & \tilde{\Xi}_{7i} & * & * \\ \Xi_{8i} & 0 & 0 & 0 & \tilde{\Xi}_{9i} & * \\ \Xi_{10i} & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{37}$$

in which $\tilde{\Xi}_{7i} = diag\{-2\epsilon_iP_i + \epsilon_i^2R_1^i, -2\epsilon_iP_i + \epsilon_i^2R_1^i\}$, $\tilde{\Xi}_{9i} = diag\{-2\epsilon_iP_i + \epsilon_i^2R^i, -2\epsilon_iP_i + \epsilon_i^2R_2^i\}$. It can be easily seen (37) is a sufficient condition to guarantee (14) holds.

Define $X_i \triangleq P_i^{-1}$, $Y_i \triangleq K_iX_i$, $\hat{Q}_1^i \triangleq X_iQ_1^iX_i$, $\hat{Q}_2^i \triangleq X_iQ_2^iX_i$, $\hat{Q}^{ij} \triangleq X_iQ^{ij}X_i$, $\hat{R}_1^i \triangleq X_iR_1^iX_i$, $\hat{R}_2^i \triangleq X_iR_2^iX_i$, $\hat{U}_i \triangleq X_iU_iX_i$, $\hat{\Phi}_i \triangleq X_i\Phi_iX_i$, $\mathbb{T}_i \triangleq diag\{X_i, X_i, X_i, X_i, X_i, X_i, I, \underbrace{X_i, \ldots, X_i}_{n_s+4}, I\}$, and then, pre- and post-multiplying both sides of (37) with $\mathbb{T}_i$ and $\mathbb{T}_i^T$, pre- and post-multiplying both sides of (15) with $diag\{X, X\}$ and its transpose, (16) and (17) can be obtained, respectively.

This completes the proof.

References

[1] G. Guo, J. Kang, R. Li, G. Yang, Distributed model reference adaptive optimization of disturbed multiagent systems with intermittent communications, IEEE Trans. Cybern. 52 (6) (2022) 5464–5473.

[2] X. Zong, T. Li, G. Yin, L.Y. Wang, J. Zhang, Stochastic consentability of linear systems with time delays and multiplicative noises, IEEE Trans. Automat. Control 63 (4) (2018) 1059–1074.

[3] G. Guo, J. Kang, Distributed optimization of multiagent systems against unmatched disturbances: A hierarchical integral control framework, IEEE Trans. Syst., Man, Cybern.: Syst. 52 (6) (2022) 3556–3567.

[4] Z. Gu, H. Ju, D. Yue, Z. Wu, X. Xie, Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks, IEEE Trans. Syst., Man, Cybern.: Syst. 51 (10) (2021) 6197–6206.

[5] G. Guo, R. Zhang, Lyapunov redesign-based optimal consensus control for multi-agent systems with uncertain dynamics, IEEE Trans. Circuits Syst. II 69 (6) (2022) 2902–2906.

[6] T.-Y. Zhang, D. Ye, G. Guo, Distributed event-triggered control for multiagent systems under denial-of-service attacked topology: Secure mode strategy, IEEE Trans. Syst., Man, Cybern.: Syst. http://dx.doi.org/10.1109/TSMC.2022.3147773.

[7] Y. Wang, P. Shi, C. Lim, Y. Liu, Event-triggered fault detection filter design for a continuous-time networked control system, IEEE Trans. Cybern. 46 (12) (2016) 3414–3426.

[8] 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.
[9] N. Zhao, P. Shi, W. Xing, Dynamic event-triggered approach for networked control systems under denial of service attacks, Internat. J. Robust Nonlinear Control 31 (5) (2021) 1774–1795.
[10] S. Zhu, E. Tian, D. Xu, J. Liu, An adaptive torus-event-based H_∞ controller design for networked T-S fuzzy systems under deception attacks, Internat. J. Robust Nonlinear Control 32 (6) (2022) 3425–3441.
[11] Y. Li, F. Song, J. Liu, X. Xie, E. Tian, Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks, Internat. J. Robust Nonlinear Control 32 (3) (2022) 1633–1653.
[12] J. Liu, Y. Dong, L. Zha, E. Tian, X. Xie, Event-based security tracking control for networked control systems against stochastic cyber-attacks, Inform. Sci. 616 (2022) 306–321.
[13] Y. Qi, X. Xu, S. Lu, Y. Yu, A waiting time based discrete event-triggered control for networked switched systems with actuator saturation, Nonlinear Anal. Hybrid Syst. 37 (2020) 100904.
[14] X. Ge, Q. Han, X. Zhang, L. Ding, F. Yang, Distributed event-triggered estimation over sensor networks: A survey, IEEE Trans. Cybern. 50 (3) (2020) 1306–1320.
[15] T. Yu, Y. Zhao, J. Wang, J. Liu, Event-triggered sliding mode control for switched genetic regulatory networks with persistent dwell time, Nonlinear Anal. Hybrid Syst. 44 (2022) 101135.
[16] J. Liu, N. Zhang, Y. Li, X. Xie, E. Tian, J. Cao, Learning-based event-triggered tracking control for nonlinear networked control systems with unmatched disturbance, IEEE Trans. Syst. Man Cybern.-Syst. http://dx.doi.org/10.1109/TSMC.2022.3224432.
[17] X. Chen, Y. Wang, S. Hu, Event-triggered quantized H_∞ control for networked control systems in the presence of denial-of-service jamming attacks, Nonlinear Anal. Hybrid Syst. 33 (2019) 265–281.
[18] D. Yue, E. Tian, Q. Han, A delay system method for designing event-triggered controllers of networked control systems, IEEE Trans. Automat. Control 58 (2) (2013) 475–481.
[19] H. Yang, H. Zhao, Y. Xia, J. Zhang, Event-triggered active MPC for nonlinear multiagent systems with packet losses, IEEE Trans. Cybern. 51 (6) (2021) 3093–3102.
[20] H. Zhang, D. Yue, C. Dou, K. Li, X. Xie, Event-triggered multiagent optimization for two-layered model of hybrid energy system with price bidding-based demand response, IEEE Trans. Cybern. 51 (6) (2021) 2068–2079.
[21] D. Zeng, R. Zhang, Ju H. Park, S. Zhong, J. Cheng, G. Wu, Reliable stability and stabilizability for complex-valued memristive neural networks with actuator failures and aperiodic event-triggered sampled-data control, Nonlinear Anal. Hybrid Syst. 39 (2021) 100977.
[22] 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, Internat. J. Robust Nonlinear Control 30 (4) (2020) 1534–1548.
[23] H. Yang, P. Li, Y. Xia, C. Yan, H_∞ Static output feedback for low-frequency networked control systems with a decentralized event-triggered scheme, IEEE Trans. Cybern. 51 (8) (2021) 4227–4236.
[24] Z. Gu, P. Shi, D. Yue, An adaptive event-triggering scheme for networked interconnected control system with stochastic uncertainty, Internat. J. Robust Nonlinear Control 27 (2) (2016) 236–251.
[25] Z. Gu, D. Yue, E. Tian, On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems, Inform. Sci. 422 (2017) 257–270.
[26] 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.
[27] H. Liu, Z. Wang, Sampled-data-based consensus of multi-agent systems under asynchronous denial-of-service attacks, Nonlinear Anal. Hybrid Syst. 39 (2021) 100969.
[28] F. Qu, E. Tian, X. Zhao, Chance-constrained H_∞ state estimation for recursive neural networks under deception attacks and energy constraints: The finite-horizon case, IEEE Trans. Neural Netw. Learn. Syst. (2022) http://dx.doi.org/10.1109/TNNLS.2021.3137426.
[29] Y. Tan, Q. Liu, J. Liu, X. Xie, S. Fei, Observer-based security control for interconnected semi-Markovian jump systems with unknown transition probabilities, IEEE Trans. Cybern. 52 (9) (2022) 9013–9025.
[30] J. Cao, D. Ding, J. Liu, E. Tian, X. Xie, Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks, Inform. Sci. 548 (10) (2021) 69–84.
[31] L. Zha, R. Liao, J. Liu, X. Xie, E. Tian, J. Cao, Dynamic event-triggered output feedback control for networked systems subject to multiple cyber-attacks, IEEE Trans. Cybern. 52 (12) (2022) 13800–13808.
[32] S. Hu, D. Yue, X. Chen, Z. Cheng, X. Xie, Resilient H_∞ filtering for event-triggered networked systems under nonperiodic DoS jamming attacks, IEEE Trans. Syst., Man, Cybern.: Syst. 51 (3) (2021) 1392–1403.
[33] B. Chen, D. Ho, G. Hu, L. Yu, Secure fusion estimation for bandwidth constrained cyber–physical systems under replay attacks, IEEE Trans. Cybern. 48 (6) (2018) 1862–1876.
[34] M. Zhu, S. Martinez, On the performance analysis of resilient networked control systems under replay attacks, IEEE Trans. Automat. Control 59 (3) (2014) 804–808.
[35] Y. Dan, A. Tyz, G. Ge, Stochastic coding detection scheme in cyber–physical systems against replay attack, Inform. Sci. 481 (2019) 432–444.
[36] D. Ding, Z. Wang, Q. Han, G. Wei, Security control for discrete-time stochastic nonlinear systems subject to deception attacks, IEEE Trans. Syst., Man, Cybern.: Syst. 48 (5) (2018) 779–789.
[37] E. Tian, C. Peng, Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks, IEEE Trans. Cybern. 50 (11) (2020) 4610–4618.
[38] F. Qu, E. Tian, X. Zhao, Chance-constrained H-infinity state estimation for recursive neural networks under deception attacks and energy constraints: The finite-horizon case, IEEE Trans. Neural Netw. Learn. Syst. (2022) http://dx.doi.org/10.1109/TNNLS.2021.3137426.
[39] 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, Internat. J. Robust Nonlinear Control 30 (4) (2020) 1534–1548.
[40] Y. Xue, W. Ren, B. Zheng, J. Han, Event-triggered adaptive sliding mode control of cyber–physical systems under false data injection attack, Appl. Math. Comput. 433 (2022) 127403.
[41] J. Liu, T. Yin, D. Yue, H. Karimi, J. Cao, Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks, IEEE Trans. Cybern. 51 (1) (2021) 162–173.
[42] 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. Regul. Pap. 67 (3) (2020) 1021–1034.
[43] H. Li, Z. Zhang, H. Yan, X. Xie, Adaptive event-triggered fuzzy control for uncertain active suspension systems, IEEE Trans. Cybern. 49 (12) (2019) 4388–4397.
[44] E. Tian, Y. Dong, Decentralized control of network-based interconnected systems: A state-dependent triggering method, Internat. J. Robust Nonlinear Control 25 (2015) 1126–1144.
[45] C. Peng, Q.-L. 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.