Neurocomputing 500 (2022) 405–412

Contents lists available at ScienceDirect

Neurocomputing

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

Dynamic event-triggered security control of cyber-physical systems against missing measurements and cyber-attacks ☆

Lijuan Zha [a,b], Rongfei Liao [b], Jinliang Liu [b], Jinde Cao [c,d,*], Xiangpeng Xie [e]

[a] School of Mathematics, Southeast University, Nanjing 210096, China
[b] College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China
[c] School of Mathematics, Southeast University, Nanjing 210096, China
[d] Yonsei Frontier Lab, Yonsei University, Seoul 03722, South Korea
[e] Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

ARTICLE INFO

Article history:
Received 22 January 2022
Revised 8 April 2022
Accepted 23 May 2022
Available online 26 May 2022

Keywords:
Observer-based control
dynamic event-triggered scheme
cyber-attacks
missing measurements

ABSTRACT

The security control approach is presented for cyber-physical systems (CPSs) with missing measurements and cyber-attacks based on an improved dynamic event-triggered scheme (DETS). The DETS is proposed to decrease the communication workload and reduce the effects of mutation data which may be erroneous. The sensor measurements are assumed to be lost randomly due to the unreliable network. In this paper, an observer-based controller is derived which can be tolerant towards the impacts of the missing measurements and cyber-attacks. The observer-based controller parameters and event-triggered parameter are co-designed. Finally, simulation results verify the validity of the proposed approach.

1. Introduction

Increased attention has been attracted to cyber-physical systems (CPSs), which are complex systems integrated the functions of the computation, communication, and control. These systems have broad application prospects in various areas, such as intelligent transportation systems, power grids, and industrial process control [1]. With the advancement of networked communication and computational abilities, the CPSs can quickly adjust to new situation and provide significant improvement in sensing, actuation and computation [2,3]. However, the signals transmitted among the various components of the system are via wireless network, which are vulnerable to malicious cyber-attacks [4–7]. There is no doubt that severe attacks on CPSs can cause huge economic loss and even threaten human life. Thus, the investigation of the security control issues for CPSs would be of great significance.

Security concerns of CPSs have aroused the enthusiasm of the scholars in science and engineering [8–10]. Since the saboteurs may launch denial-of-service (DoS) attacks [11] and deception attacks [12,13] to destroy the target system by interfering the data transmission. The DoS attacks aim to corrupt the stability of the system by blocking the communication channel, while the deception attacks corrupt the control systems by tempering the transmitted information maliciously [14,15]. For example, in [14], a disturbance rejection controller was developed for nonlinear network control systems (NCSs) under physical and DoS attacks. A distributed attack detection approach was addressed for sensor networks under deception attacks and unknown disturbance and noise in [16]. Until now, a vast amount of energy has been invested into the cyber-attacks against CPSs and a number of control or estimation methods of networked systems have been developed against various types of cyber-attacks. Among the wealth results about cyber-attacks in CPSs, there appear to be a few publications about observer-based control for continuous CPSs subject to DoS attacks [17–19], these approaches fail to work for discrete CPSs in presence of deception attacks and missing measurements, which motivates this article.

Since the networked computation and information exchange are essential in CPSs, it is of great need to make the most efficient use of the constrained bandwidth. Various methods have been

☆ This work is supported by the National Natural Science Foundation of China under Grant 61903182 and Grant 61973152, in part by Natural Science Foundation of Jiangsu Province of China under Grant BK20190794 and Grant BK20211290, in part by China Postdoctoral Science Foundation under Grant 2019M651651, in part by Qinglan Project of Jiangsu Province of China, in part by the Postgraduate Research and practice Innovation Program of Jiangsu Province of China under Grant LRFXW21001 (Corresponding author: Jinde Cao.)

* Corresponding author at: School of Mathematics, Southeast University, Nanjing 210096, China.

E-mail addresses: zhalijuan@vip.163.com (L. Zha), liaorongfei110@163.com (R. Liao), liujinliang@vip.163.com (J. Liu), jdcao@seu.edu.cn (J. Cao), xiexiangpeng1953@163.com (X. Xie).

https://doi.org/10.1016/j.neucom.2022.05.096
0925-2312/

derived to well utilize the limited network resources [20–24]. Especially, as one effective means to save network resources, event-triggered (ET) schemes are popular with many researchers [25–27]. To mention a few works, two resilient adaptive ET schemes are designed in [28] to avoid some unnecessary data traveling across the network. In [29], a resilient ET scheme was proposed to reduce the bandwidth pressure between the sensor and the filter. A learning-based ET scheme is applied in [30] to economize bandwidth of the network, the triggering threshold of which can be automatically adjusted in response to the variations of latest vehicle state. An ET scheme is applied to investigate the secure leader-following consensus control problem for multi-agent systems with multiple attacks by Liu et al.[31]. However, the dynamic ET control method for NCSs has not been developed to resist the cyber-atacks and randomly missing output measurements, which is still a challenging task.

Motivated by the above analysis, taking malicious cyber-attacks and missing output measurement into account, we are concerned with the stability analysis of a class of discrete NCSs in this article. Note that the network resources have the characteristic of resources-starved and all the system states may be difficult to be measured directly. Our objective is to design an resilient observer-based output feedback controller for the addressed NCSs, which can put up with the cyber-attacks and missing output measurements. The main contributions of this article are as follows. (1) An improved dynamic event-triggered scheme (DETS) is proposed to reduce the network congestion while avoiding some unnecessary abrupt data transmission. (2) A new closed-loop system model is established, which taking into account of the impacts of the cyber-attacks and the missing output measurements. (3) The co-design approach of the observer/controller gains and the triggering matrix of the DETS are presented to guarantee the desired system performance.

2. Preliminaries

The framework of the NCSs under randomly missing output measurements and cyber attacks is given in Fig. 1, where the information flows from sensor to observer and from observer to controller are via unreliable wireless network. For the sake of reducing data update frequency of observer, a DETS is introduced to discard some 'unnecessary' packets with little variation.

The dynamics of the physical plant in Fig. 1 can be modeled as:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) \\ y(k) = Cx(k) \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$ and $y(k) \in \mathbb{R}^{n_y}$ represent the system state vector and the output measurement, respectively. $u(k) \in \mathbb{R}^{n_u}$ stands for the control input. $A \in \mathbb{R}^{n_x \times n_x}, B \in \mathbb{R}^{n_x \times n_u}$ and $C \in \mathbb{R}^{n_y \times n_x}$ are known constant matrices.

The main intend of this article is to design a controller based on the observed state $\hat{x}(k)$. The observer-based controller model is constructed as follows:

$$\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + Bu(k) + L(\tilde{y}(k) - C\hat{x}(k)) \\ u(k) = K\tilde{x}(k) \end{cases} \tag{2}$$

where $\hat{x}(k) \in \mathbb{R}^{n_x}$ represents the observer state, $\tilde{x}(k) \in \mathbb{R}^{n_x}$ stands for the signal received by controller and $\tilde{y}(k) \in \mathbb{R}^{n_y}$ is the data received by observer. The models of $\tilde{x}(k)$ and $\tilde{y}(k)$ will be given later. $L \in \mathbb{R}^{n_x \times n_y}$ and $K \in \mathbb{R}^{n_u \times n_x}$ are observer gain and controller gain to be determined.

Remark 1. Notice that the randomly occurring information missing and cyber-attacks are often encountered in many practical systems. The output measurement $y(k)$ and the observer state

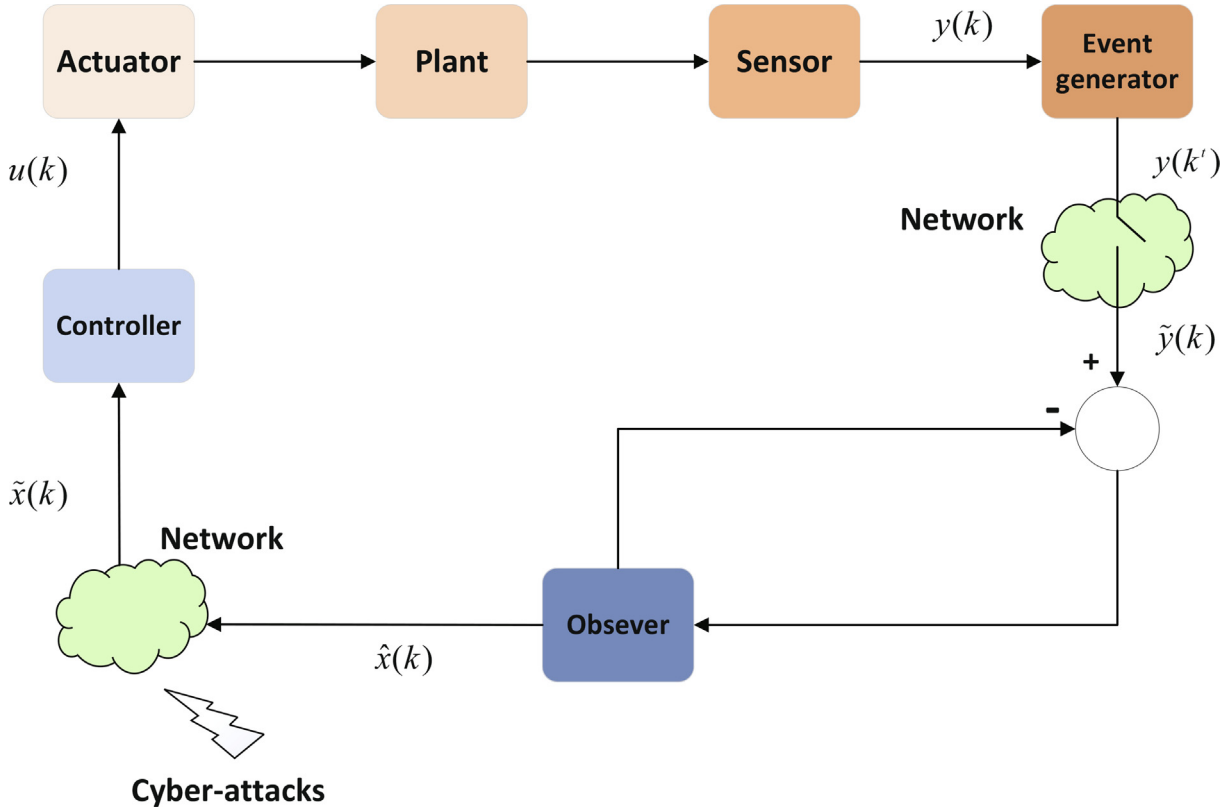


Fig. 1. The structure of dynamic ET NCSs with cyber-attacks and missing output measurements.

$\hat{x}(k)$being transmitted via the unreliable network may be different with the real observer input $\bar{y}(k)$and the controller input $\bar{x}(k)$, that is, $\bar{y}(k)$ is not equal to $y(k)$and $\bar{x}(k)$ is not equal to $\hat{x}(k)$.

A dynamic ET generator is introduced between the sensor and the observer to reduce the frequency of signals released into the network as shown in Fig. 1. The following condition is employed for event-based update of the observer:

$$\begin{cases} \lambda\phi(k) > \theta(k) \\ \phi(k) = e^T(k)Me(k) - \delta y^T\left(k^t\right)My\left(k^t\right) \end{cases} \tag{3}$$

where δ and λ are known positive constants, $e(k) = y\left(k^t\right) - y\left(k^t + \Delta\right)$ in which

$$y\left(k^t + \Delta\right) \triangleq \mu\left[y(k) - y\left(k^t\right)\right] + y\left(k^t\right) \tag{4}$$

with μ is an adjustment factor satisfying $\mu \in (0, 1]$, k^t stands for the triggering instant, $y\left(k^t\right)$ denotes the latest signal released by the dynamic ET generator, and the auxiliary offset variable $\theta(k)$ is denoted as:

$$\begin{cases} \theta(k+1) = \sigma\theta(k) - \phi(k) \\ \theta(0) \geqslant 0 \end{cases} \tag{5}$$

with σ is a constant in $(0, 1)$, λ and σ satisfy $\lambda\sigma \geqslant 1$ which can ensure $\theta(k) \geqslant 0$ for any $k \in \mathbb{N}, \mathbb{N} = \{1, 2, 3, \cdots\}$ according to Lemma 1 in [25].

If the dynamic ET condition (3) is met, the "required" output measurement will be put into the wireless network, while the data with a little variation will be dropped. Then we obtain the next triggering time k^{t+1} as follows:

$$k^{t+1} = \min\left\{k \in \mathbb{N} | k > k^t, k \text{ satisfying } (3)\right\} \tag{6}$$

Remark 2. From the definition of k^t, one can easily see that the set of triggering times $\left\{k^t | t \in \mathbb{N}\right\}$ is the subset of $\mathbb{N}$.

Remark 3. Considering that the mutation data may be easier to satisfy dynamic ET condition (3) than normal data, one set the error $e(k) = y\left(k^t\right) - y\left(k^t + \Delta\right)$ with the definition of $y\left(k^t + \Delta\right)$ in (4) rather than $e(k) = y\left(k^t\right) - y(k)$ to avoid the mutation data being mistakenly released into the network.

Remark 4. In (4), if we let $\mu = 1, y\left(k^t + \Delta\right)$ will be equal to $y(k)$ and the error $e(k) = y\left(k^t\right) - y\left(k^t + \Delta\right)$ will be $e(k) = y\left(k^t\right) - y(k)$, that is, the triggering condition (3) becomes the case in [32]. If $0 < \mu < 1$, the value of $y\left(k^t + \Delta\right)$ will range from $y\left(k^t\right)$ to $y(k)$. In particular, if $\mu = \frac{1}{2}, y\left(k^t + \Delta\right)$ will equal to the average between $y\left(k^t\right)$ and $y(k)$. Consequently, the designed triggering condition (3) can avoid the erroneous events in some extent.

Since the information losses may occur during being transmitted via the Sensor-to-Observer communication channel, the stochastic variable $\alpha(k)$ is applied to account for this phenomenon. The presentation of the observer input is:

$$\tilde{y}(k) = \alpha(k)y\left(k^t\right) = \alpha(k)\left[Cx(k) + \frac{1}{\mu}e(k)\right] \tag{7}$$

where $\alpha(k) \in \{0, 1\}$ satisfying the following constraints:

$$\mathbb{E}(\alpha(k)) = \bar{\alpha}, \mathbb{E}(1 - \alpha(k)) = 1 - \bar{\alpha} \tag{8}$$

In the presence of malicious cyber-attacks, the transmitted data over the network will be modified and the controller cannot receive the real observer state. A nonlinear function (NF) $\varrho(\hat{x}(k))$ is utilized to characterize the cyber-attacks sent by the malicious opponent. The controller input can be expressed as

$$\tilde{x}(k) = \hat{x}(k) + \beta(k)\varrho(\hat{x}(k)) \tag{9}$$

where $\beta(k) \in \{0, 1\}$ and

$$\mathbb{E}(\beta(k)) = \bar{\beta}, \mathbb{E}(1 - \beta(k)) = 1 - \bar{\alpha}, \tag{10}$$

Remark 5. It should be noted that $\beta(k) = 1$ in (9) represents that the system is subject to cyber-attacks which will tamper the real data packets, in this case, the real controller input is denoted by (9). Otherwise, $\beta(k) = 0$, this means the network does not experience the cyber-attacks, and the input of the controller is $\hat{x}(k)$.

Define $\epsilon(k) \triangleq x(k) - \hat{x}(k)$, from (1), (2) and (9), the system state $x(k+1)$ can be computed as:

$$\begin{aligned} x(k+1) = {} & (A + BK)\hat{x}(k) + A\epsilon(k) + \bar{\beta}BK\varrho(\hat{x}(k)) \\ & + \left(\beta(k) - \bar{\beta}\right)BK\varrho(\hat{x}(k)) \end{aligned} \tag{11}$$

and observer state $\hat{x}(k+1)$ can be obtained from (2), (7) and (9):

$$\begin{aligned} \hat{x}(k+1) = {} & [A + BK + (\bar{\alpha} - 1)LC]\hat{x}(k) + \bar{\alpha}LC\epsilon(k) + \frac{\bar{\alpha}}{\mu}Le(k) \\ & + \bar{\beta}BK\varrho(\hat{x}(k)) + (\alpha(k) - \bar{\alpha}) \\ & \times \left[LC\hat{x}(k) + LC\epsilon(k) + \frac{1}{\mu}Le(k)\right] \\ & + \left(\beta(k) - \bar{\beta}\right)BK\varrho(\hat{x}(k)). \end{aligned} \tag{12}$$

Then, we can derive the error $\epsilon(k+1)$ from (11) and (12):

$$\begin{aligned} \epsilon(k+1) = {} & -(\bar{\alpha} - 1)LC\hat{x}(k) + (A - \bar{\alpha}LC)\epsilon(k) - \frac{\bar{\alpha}}{\mu}Le(k) \\ & - (\alpha(k) - \bar{\alpha})\left[LC\hat{x}(k) + LC\epsilon(k) + \frac{1}{\mu}Le(k)\right]. \end{aligned} \tag{13}$$

Let $\eta(k) = \begin{bmatrix} \hat{x}^T(k) & \epsilon^T(k) \end{bmatrix}^T$, the following augmented system can be derived

$$\begin{aligned} \eta(k+1) = {} & \bar{A}\eta(k) + \frac{\bar{\alpha}}{\mu}\bar{L}e(k) + \bar{\beta}\bar{B}\varrho(\hat{x}(k)) + \left(\beta(k) - \bar{\beta}\right)\bar{B}\varrho(\hat{x}(k)) \\ & + (\alpha(k) - \bar{\alpha})\left[\bar{L}_c\eta(k) + \frac{1}{\mu}\bar{L}e(k)\right], \end{aligned} \tag{14}$$

where

$$\bar{A} = \begin{bmatrix} A + BK + (\bar{\alpha} - 1)LC & \bar{\alpha}LC \\ -(\bar{\alpha} - 1)LC & A - \bar{\alpha}LC \end{bmatrix}, \bar{L} = \begin{bmatrix} L \\ -L \end{bmatrix}, \bar{B} = \begin{bmatrix} BK \\ 0 \end{bmatrix},$$

$$\bar{L}_c = \begin{bmatrix} LC & LC \\ -LC & -LC \end{bmatrix}.$$

Then, the dynamic ET control issue for NCSs (1) with missing measurements and cyber-attacks is transformed into the stability issue of (14). In deriving our main results, the following lemma and assumption are needed.

Lemma 1. [32] For $B \in \mathbb{R}^{n_x \times n_u}, rank(B) = n_u$, the singular value decomposition of B is $B = U\begin{bmatrix} S^T & 0 \end{bmatrix}^T V^T$, where $U^T U = I, V^T V = I$. For $\overline{P} \triangleq UP_1U^T, P_1 = \begin{bmatrix} M & * \\ 0 & N \end{bmatrix}, M \in \mathbb{R}^{n_q \times n_q}, N \in \mathbb{R}^{(n_x - n_q) \times (n_x - n_q)}$, there exists $\widetilde{P} = \left(V^T\right)^{-1}S^{-1}MSV^T$ satisfying $\overline{P}B = B\widetilde{P}$.

Assumption 1. The matrix B is a full rank matrix.

Assumption 2. The NF $\varrho(\hat{x}(k))$ satisfies the following condition

$$\varrho^T(\hat{x}(k))\varrho(\hat{x}(k)) \leqslant \hat{x}^T(k)\Gamma^T\Gamma\hat{x}(k). \tag{15}$$

where Γ is a known matrix.

Remark 6. Compared with the event-triggered scheme with preset triggering parameter in [5,25,33,34], an auxiliary variable $\theta(k)$ is introduced into the DETS in this paper to adjust the amount of data transmission via network. Larger trigger interval will be determined by DETS than that by event-triggered scheme with preset triggering parameter which has been proved in [35].

3. Main Results

A new ET observer-based control algorithm is developed in this section for the augmented system (14). Moreover, the co-design approach of controller gain, the observer gain, and dynamic ET parameter will be shown.

Theorem 1. *For given scalars $\lambda > 0, \delta > 0, \mu \in (0,1], \sigma \in (0,1)$ $\bar{\alpha} \in (0,1)$ and $\bar{\beta} \in (0,1)$ and matrix Γ, the augmented system (14) is asymptotic stable if there exist matrices $\bar{P} > 0, M > 0, Y$ and Z such that*

$$\Sigma_2 = \begin{bmatrix} \Omega_{11} & * & * & * & * \\ \Omega_{21} & \mathcal{P} & * & * & * \\ \rho_\beta\Omega_{31} & 0 & \mathcal{P} & * & * \\ \rho_\alpha\Omega_{41} & 0 & 0 & \mathcal{P} & * \\ \Omega_{51} & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{16}$$

where

$$\Omega_{11} = \begin{bmatrix} -\bar{P}^T - \delta\kappa C^T MC & * & * & * \\ -\delta\kappa C^T MC & -\bar{P}^T - \delta\kappa C^T MC & * & * \\ -\frac{\delta}{\mu}\kappa MC & -\frac{\delta}{\mu}\kappa MC & \kappa\left(1-\frac{\delta}{\mu^2}\right)M & * \\ 0 & 0 & 0 & -I \end{bmatrix},$$

$$\Omega_{21} = \begin{bmatrix} \bar{P}^T A + BY + (\bar{\alpha}-1)ZC & \bar{\alpha}ZC & \frac{\bar{\alpha}}{\mu}Z & \bar{\beta}BY \\ -(\bar{\alpha}-1)ZC & \bar{P}^T A - \bar{\alpha}ZC & -\frac{\bar{\alpha}}{\mu}Z & 0 \end{bmatrix},$$

$$\Omega_{31} = \begin{bmatrix} 0 & 0 & 0 & BY \\ 0 & 0 & 0 & 0 \end{bmatrix}, \Omega_{41} = \begin{bmatrix} ZC & ZC & \frac{1}{\mu}ZC & 0 \\ -ZC & -ZC & -\frac{1}{\mu}ZC & 0 \end{bmatrix},$$

$$\Omega_{51} = [\Gamma \quad 0 \quad 0 \quad 0],$$

$$\rho_\beta = \sqrt{(1-\bar{\beta})\bar{\beta}}, \rho_\alpha = \sqrt{(1-\bar{\alpha})\bar{\alpha}}, \kappa = \sigma - 1 - \frac{1}{\lambda},$$

$$\mathcal{P} = diag\{-\bar{P}, -\bar{P}\}.$$

Then, the observer-based controller gains can be designed as

$$K = \widetilde{P}^{-1}Y \tag{17}$$

$$L = \bar{P}^{-1}Z \tag{18}$$

where $\widetilde{P} = \left(V^T\right)^{-1}S^{-1}MSV^T$ and the symbols V, S and M are given in Lemma 1.

Proof. Construct the following Lyapunov functional candidate for system (14)

$$V(k) = \eta^T(k)P\eta(k) - \frac{1}{\lambda}\theta(k) \tag{19}$$

Define the forward difference of $V(k)$ as $\Delta V(k) \triangleq V(k+1) - V(k)$. The expectation of $\Delta V(k)$ is

$$\begin{aligned} \mathbb{E}\{\Delta V(k)\} &= \left[\overline{A}\eta(k) + \tfrac{\bar{\alpha}}{\mu}\overline{L}e(k) + \bar{\beta}\overline{B}\varrho(\hat{x}(k))\right]^T \\ &\quad \times P\left[\overline{A}\eta(k) + \tfrac{\bar{\alpha}}{\mu}\overline{L}e(k) + \bar{\beta}\overline{B}\varrho(\hat{x}(k))\right] \\ &\quad + \bar{\alpha}(1-\bar{\alpha})\left[\overline{L}_c\eta(k) + \tfrac{1}{\mu}\overline{L}e(k)\right]^T P\left[\overline{L}_c\eta(k) + \tfrac{1}{\mu}\overline{L}e(k)\right] \\ &\quad + \bar{\beta}(1-\bar{\beta})\varrho^T(\hat{x}(k))\overline{B}^T P\overline{B}\varrho(\hat{x}(k)) - \eta^T(k)P\eta(k) \\ &\quad + \tfrac{1}{\lambda}(\sigma-1)\theta(k) - \tfrac{1}{\lambda}\left[e^T(k)Me(k) - \delta y\left(k^t\right)My\left(k^t\right)\right] \\ &= \xi^T(k)\Big[\Theta_1 + \mathcal{A}^T P\mathcal{A} + \bar{\beta}(1-\bar{\beta})\mathcal{B}^T P\mathcal{B} \\ &\quad + \bar{\alpha}(1-\bar{\alpha})\mathcal{C}^T P\mathcal{C}\Big]\xi(k) + \tfrac{1}{\lambda}(\sigma-1)\theta(k) \end{aligned} \tag{20}$$

where $\mathcal{A} = \begin{bmatrix} \overline{A} & \frac{\bar{\alpha}}{\mu}\overline{L} & \bar{\beta}\overline{B} \end{bmatrix}, \mathcal{B} = \begin{bmatrix} 0 & 0 & \overline{B} \end{bmatrix}, \mathcal{C} = \begin{bmatrix} \overline{L}_c & \frac{1}{\mu}\overline{L} & 0 \end{bmatrix}, \xi(k) = \begin{bmatrix} \eta^T(k) & e^T(k) & \varrho^T(\hat{x}(k)) \end{bmatrix}^T$, and

$$\Theta_1 = \begin{bmatrix} -P + \frac{\delta}{\lambda}I_{12}^T C^T MCI_{12} & * & * \\ \frac{\delta}{\mu\lambda}MCI_{12} & \frac{1}{\lambda}\left(\frac{\delta}{\mu^2}-1\right)M & * \\ 0 & 0 & 0 \end{bmatrix},$$

with $I_{12} = [I \quad I]$.

Notice that $0 < \sigma < 1$, the following inequality can be easily deduced from (3):

$$\frac{1}{\lambda}(\sigma-1)\theta(k) \leqslant (\sigma-1)\left[e^T(k)Me(k) - \delta y\left(k^t\right)My\left(k^t\right)\right] \tag{21}$$

Combining (3), (15) and (21), one can obtain

$$\begin{aligned} \mathbb{E}\{\Delta V(k)\} &\leqslant \xi^T(k)\Big[\Theta_1 + \mathcal{A}^T P\mathcal{A} + \bar{\beta}(1-\bar{\beta})\mathcal{B}^T P\mathcal{B} \\ &\quad + \bar{\alpha}(1-\bar{\alpha})\mathcal{C}^T P\mathcal{C}\Big]\xi(k) \\ &\quad + (\sigma-1)\Big\{e^T(k)Me(k) - \delta\left[CI_{12}\eta(k) + \tfrac{1}{\mu}e(k)\right]^T \\ &\quad \times M\left[CI_{12}\eta(k) + \tfrac{1}{\mu}e(k)\right]\Big\} - \eta^T(k)P\eta(k) \\ &\quad + \eta^T(k)I_1^T\Gamma^T\Gamma I_1\eta(k) - \varrho^T(\hat{x}(k))\varrho(\hat{x}(k)) \\ &= \xi^T(k)\Big[\Theta_2 + \mathcal{A}^T P\mathcal{A} + \bar{\beta}(1-\bar{\beta})\mathcal{B}^T P\mathcal{B} \\ &\quad + \bar{\alpha}(1-\bar{\alpha})\mathcal{C}^T P\mathcal{C} + \mathcal{D}^T\mathcal{D}\Big]\xi(k) \end{aligned} \tag{22}$$

where

$$\Theta_2 = \begin{bmatrix} -P - \delta(\sigma - 1 - \frac{1}{\lambda})I_{12}^T C^T MCI_{12} & * & * \\ -\frac{\delta}{\mu}(\sigma - 1 - \frac{1}{\lambda})MCI_{12} & (\sigma - 1 - \frac{1}{\lambda})\left(1 - \frac{\delta}{\mu^2}\right)M & * \\ 0 & 0 & -I \end{bmatrix},$$

and $\mathcal{D} = [\Gamma I_1 \quad 0 \quad 0], I_1 = [I \quad 0]$.

According to schur complement, we can conclude that $\mathbb{E}\{\Delta V(k)\} \leqslant 0$ from the following inequality

$$\Sigma_1 = \begin{bmatrix} \Theta_2 & * & * & * & * \\ P\mathcal{A} & -P & * & * & * \\ \rho_\beta P\mathcal{B} & 0 & -P & * & * \\ \rho_\alpha P\mathcal{C} & 0 & 0 & -P & * \\ \mathcal{D} & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{23}$$

then the asymptotic stability of system (14) can be ensured.

In the following, the explicit form of the observer-based controller gains will be presented. Let $P = \begin{bmatrix} \bar{P} & * \\ 0 & \bar{P} \end{bmatrix}$. For $B \in \mathbb{R}^{n_x \times n_u}, rank(B) = n_u$, By using Lemma 1, there exists

$\widetilde{P} = \left(V^T\right)^{-1} S^{-1} M S V^T$ satisfying $\overline{P}B = B\widetilde{P}$. Define $Y \triangleq \widetilde{P}K$ and $Z \triangleq \overline{P}L$, then (16) can be derived from (23). This completes the proof.

When the network channel between the observer and controller works normally, which means the cyber-attacks are in absent, the closed loop system model (14) can be rewritten as

$$\eta(k+1) = \overline{A}\eta(k) + \frac{\bar{\alpha}}{\mu}\overline{L}e(k) + (\alpha(k) - \bar{\alpha})\left[\overline{L}_c\eta(k) + \frac{1}{\mu}\overline{L}e(k)\right]. \tag{24}$$

The expressions of $\overline{A}, \overline{L}$ and $\overline{L}_c$ are given in (14).

By the same derivation process as Theorem 1, based on (24), the observer-based controller design approach can be derived for system (1) with missing output measurements and DETS.

Corollary 1. *For given scalars $\lambda > 0, \delta > 0, \mu \in (0,1], \sigma \in (0,1)$ and $\bar{\alpha} \in (0,1)$ and matrix Γ, the augmented system (24) is asymptotic stable if there exist matrices $\bar{P} > 0, M > 0, Y$ and Z such that*

$$\Sigma_3 = \begin{bmatrix} \Phi_{11} & * & * \\ \Phi_{21} & \mathcal{P} & * \\ \rho_\alpha \Phi_{31} & 0 & \mathcal{P} \end{bmatrix} < 0 \tag{25}$$

where

$$\Phi_{11} = \begin{bmatrix} -\bar{P}^T - \delta\kappa C^T M C & * & * \\ -\delta\kappa C^T M C & -\bar{P}^T - \delta\kappa C^T M C & * \\ -\frac{\delta}{\mu}\kappa M C & -\frac{\delta}{\mu}\kappa M C & \kappa\left(1 - \frac{\delta}{\mu^2}\right)M \end{bmatrix},$$

$$\Phi_{21} = \begin{bmatrix} \bar{P}A + BY + \left(\bar{\alpha} - 1\right)ZC & \bar{\alpha}ZC & \frac{\bar{\alpha}}{\mu}Z \\ -\left(\bar{\alpha} - 1\right)ZC & \bar{P}A - \bar{\alpha}ZC & -\frac{\bar{\alpha}}{\mu}Z \end{bmatrix},$$

$$\Phi_{31} = \begin{bmatrix} ZC & ZC & \frac{1}{\mu}Z \\ -ZC & -ZC & -\frac{1}{\mu}Z \end{bmatrix},$$

$$\rho_\alpha = \sqrt{\bar{\alpha}\left(1 - \bar{\alpha}\right)}, \kappa = \sigma - 1 - \tfrac{1}{\lambda}, \mathcal{P} = diag\left\{-\bar{P}, -\bar{P}\right\}.$$

The observer-based controller gains are designed as (17) and (18).

Remark 7. The main challenges in deriving the control method in Theorem 1 is how to construct an dynamic event-triggered scheme to reduce the network congestion while avoiding some unnecessary abrupt data transmission, and how to deal with the impacts of the cyber-attacks and the missing output measurements. Inspired by References [25,33], the difficulties are overcome and a secure co-design approach of the observer/controller gains and the DETS matrix are presented to guarantee the desired system performance.

4. Numerical simulation

A numerical instance is utilized to verify the feasibility of the proposed control methods. Consider system (1) with the following parameters:

$$A = \begin{bmatrix} 0.1 & 0.2 & 0.6 & 0.1 \\ 0.5 & 0.2 & -0.2 & 0.1 \\ 0.7 & 0.5 & 0.4 & -0.3 \\ 0.2 & 0.1 & 0.3 & 0.6 \end{bmatrix}, B = \begin{bmatrix} 0.1 & 0.2 \\ 2.679 & 1 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix},$$

$$C = \begin{bmatrix} 0.6 & 0.5 \\ 0.8 & 0.9 \\ 0.3 & 0.7 \\ -0.2 & 1 \end{bmatrix}^T.$$

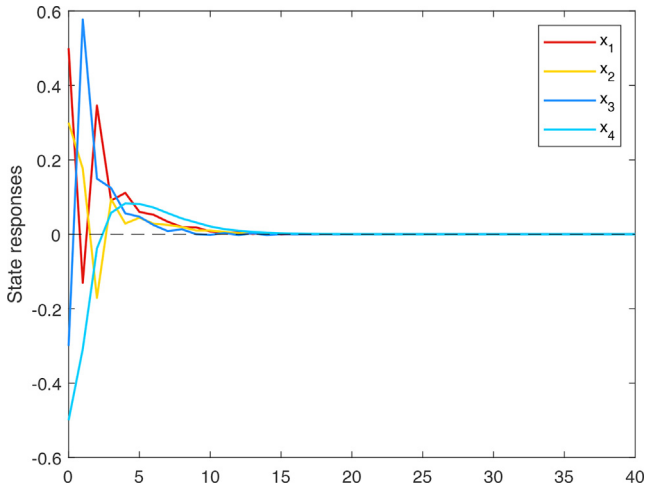


Fig. 2. State response.

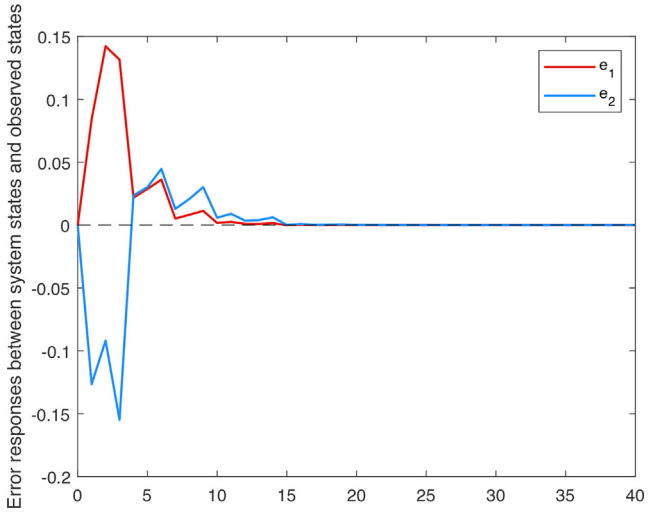


Fig. 3. Error responses between system states and observed states.

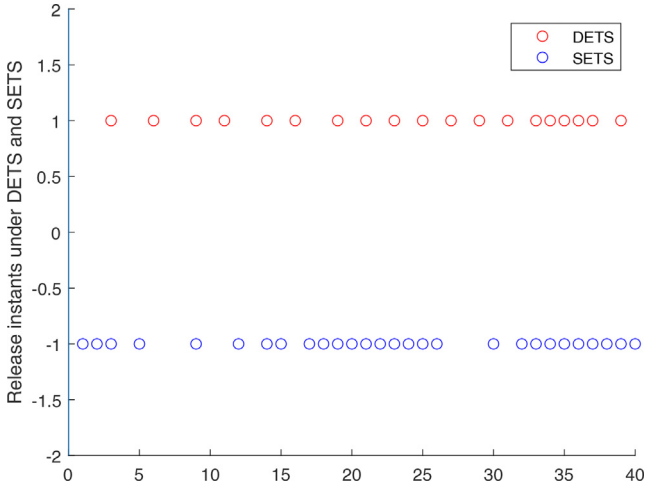


Fig. 4. Triggering instants under DETM and SETM.

The dynamic ET parameters are $\lambda = 10, \delta = 0.03, \sigma = 0.2, \mu = \frac{1}{3}$ and the initial auxiliary offset variable $\theta(0) = 10$. $\bar{\alpha} = 0.7, \bar{\beta} = 0.3$, and

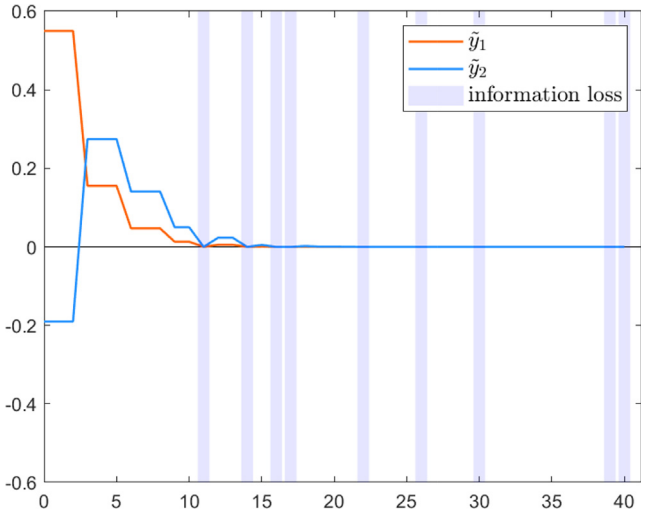


Fig. 5. The observer input with random information losses.

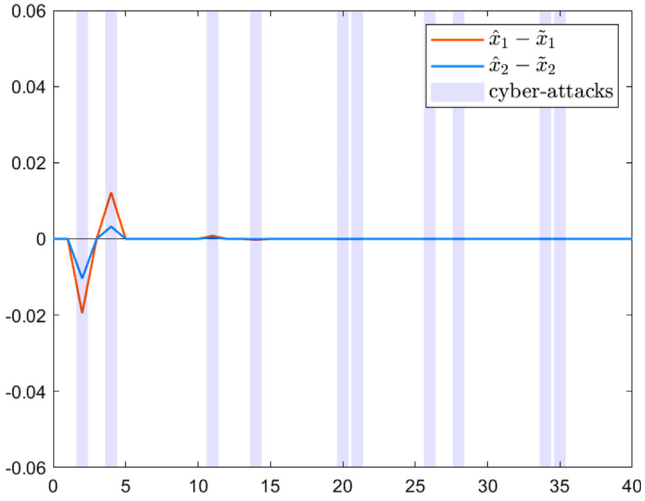


Fig. 6. The error between the signals at the observer side and the controller side subject to cyber-attacks.

the initial state and the initial observer state are $x(0) = [0.5 \quad 0.3 \quad -0.3 \quad -0.5]^T$, $\hat{x}(0) = [1 \quad 0 \quad -1 \quad 0]^T$. The NF meeting Assumption 2 is $\varrho(\hat{x}(k)) = diag\{0.2\sin(k), 0.1\sin(k), 0.3\sin(k), 0.2sin(k)\} \times \hat{x}(k)$with $\Gamma = diag\{0.2, 0.1, 0.3, 0.2\}$

Then, by solving LMI conditions given by Theorem 1, dynamic ET matrix M, observer gain L and controller gain K can be calculated as

$$M = \begin{bmatrix} 1.6665 & -0.4617 \\ -0.4617 & 0.8610 \end{bmatrix},$$

$$L = \begin{bmatrix} 0.0366 & 0.0272 & 0.0917 & 0.0145 \\ 0.0151 & 0.0332 & 0.0532 & 0.0389 \end{bmatrix}^T,$$

$$K = \begin{bmatrix} -0.0634 & -0.0365 & -0.0210 & -0.0332 \\ 0.0853 & 0.0846 & 0.1157 & -0.0158 \end{bmatrix}.$$

The simulation results are given in Fig. 2–6. Fig. 2 shows the system state converges to zero which illustrates the designed controller can ensure the stability of the augmented system. Fig. 3 depicts the error between system state and observer state which implies the effectiveness of the observer. The releasing instants of DETS and static ET scheme are shown in Fig. 4. Within the simulation interval, 28 data have been triggered under static ET scheme, while only 19 signals have been released into the wireless network under DETS. In other words, 47.5% signals takes up bandwidth resources under DETS, while 70% sampled signals are released under static ET scheme. The observer input $\tilde{y}(k)$ with random information loss is depicted in Fig. 5, from which we can see the observer input $\tilde{y}(k)$ will turn to zero when information missing happens. The error between the signals at the observer side $\hat{x}(k)$ and the controller side $\tilde{x}(k)$ subject to cyber-attacks is displayed in Fig. 6. Under the influence of malicious attacks, the signal $\tilde{x}(k)$ will suddenly deviate from the normal value $\hat{x}(k)$. From the above simulation results, we can see the validity and merit of the proposed methods is illustrated.

5. Conclusions

In this article, the problem of dynamic ET observer-based control has been solved for a class of NCSs with missing output measurements and malicious cyber-attacks. A novel DETS is developed to make effective use of the constrained network resources. Considering the situation of unreliable communication network and limited networked resources, a new model has been proposed to reflect the phenomena of the missing output measurements and randomly occurring cyber-attacks under the adopted DETS. The observer gain, controller gain, and the parameters of the DETS have been co-designed. Finally, the validity of the proposed control algorithm has been checked by the simulation results. In the future, we will extend the proposed DETS into the consensus control of mutiagent systems and sensor networks.

CRediT authorship contribution statement

Lijuan Zha: Conceptualization, Methodology, Investigation, Formal analysis, Resources, Writing - original draft, Writing - review & editing. **Rongfei Liao:** Writing - original draft, Data curation, Validation, Formal analysis. **Jinliang Liu:** Investigation, Resources, Formal analysis, Writing - review & editing. **Jinde Cao:** Conceptualization, Supervision, Methodology, Project administration. **Xiangpeng Xie:** Investigation, Writing - 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.

References

[1] W. Song, Z. Wang, J. Wang, J. Shan, Particle filtering for a class of cyber-physical systems under round-robin protocol subject to randomly occurring deception attacks, Information Sciences 544 (2021) 298–307.
[2] D. Ding, Q.-L. Han, X. Ge, J. Wang, Secure state estimation and control of cyber-physical systems: A survey, IEEE Transactions on Systems, Man, and Cybernetics: Systems 51 (1) (2021) 176–190.
[3] Y.-G. Li, G.-H. Yang, Optimal stealthy switching location attacks against remote estimation in cyber-physical systems, Neurocomputing 421 (2021) 183–194.
[4] S. Yuan, C. Yu, J. Sun, Adaptive event-triggered consensus control of linear multi-agent systems with cyber attacks, Neurocomputing 442 (2021) 1–9.
[5] W. Xu, Z. Wang, L. Hu, J. Kurths, State estimation under joint false data injection attacks: dealing with constraints and insecurity, IEEE Transactions on Automatic Control (2021), https://doi.org/10.1109/tac.2021.3131145.
[6] C. Zhao, J. Lam, H. Lin, State estimation of CPSs with deception attacks: stability analysis and approximate computation, Neurocomputing 423 (2021) 318–326.
[7] 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, Information Sciences 548 (2021) 69–84.
[8] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, A.V. Vasilakos, A survey on attack detection, estimation and control of industrial cyber-physical systems, ISA Transactions 116 (2021) 1–16.

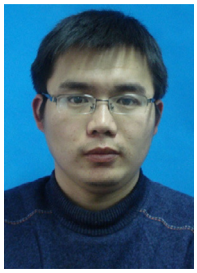
[9] M. Wang, Y. Liu, B. Xu, Observer-based $H_{-\infty}$ control for cyber-physical systems encountering DoS jamming attacks: an attack-tolerant approach, ISA Transactions 104 (2020) 1–14.
[10] Y. Xu, G. Guo, Event triggered control of connected vehicles under multiple cyber attacks, Information Sciences 582 (2022) 778–796.
[11] D. Zhao, Z. Wang, D.W.C. Ho, G. Wei, Observer-based PID security control for discrete time-delay systems under cyber-attacks, IEEE Transactions on Systems, Man, and Cybernetics: Systems 51 (6) (2021) 3926–3938.
[12] B. Shen, Z. Wang, D. Wang, Q. Li, State-saturated recursive filter design for stochastic time-varying nonlinear complex networks under deception attacks, IEEE Transactions on Neural Networks and Learning Systems 31 (10) (2020) 3788–3800.
[13] H. Yan, J. Wang, H. Zhang, H. Shen, X. Zhan, Event-based security control for stochastic networked systems subject to attacks, IEEE Transactions on Systems, Man, and Cybernetics: Systems 50 (11) (2020) 4643–4654.
[14] Y. Yang, Y. Yuan, Event-triggered active disturbance rejection control for nonlinear network control systems subject to DoS and physical attacks, ISA Transactions 104 (2020) 73–83.
[15] D. Ding, Z. Wang, D.W. Ho, G. Wei, Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks, Automatica 78 (2017) 231–240.
[16] X. Ge, Q.-L. Han, M. Zhong, X.-M. Zhang, Distributed krein space-based attack detection over sensor networks under deception attacks, Automatica 109 (2019) 108557.
[17] P.-B. Wang, X.-M. Ren, D.-D. Zheng, Event-triggered resilient control for cyber-physical systems under periodic dos jamming attacks, Information Sciences 577 (2021) 541–556.
[18] Y. Deng, H. Lu, W. Zhou, Security event-triggered control for Markovian jump neural networks against actuator saturation and hybrid cyber attacks, Journal of the Franklin Institute 358 (14) (2021) 7096–7118.
[19] J. Liu, Y. Wang, J. Cao, D. Yue, X. Xie, Secure adaptive-event-triggered filter design with input constraint and hybrid cyber-attack, IEEE Transactions on Cybernetics 51 (8) (2021) 4000–4010.
[20] X.-M. Zhang, Q.-L. Han, B.-L. Zhang, An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems, IEEE Transactions on Industrial Informatics 13 (1) (2017) 4–16.
[21] L. Ding, Q.-L. Han, X. Ge, X.-M. Zhang, An overview of recent advances in event-triggered consensus of multiagent systems, IEEE Transactions on Cybernetics 48 (4) (2018) 1110–1123.
[22] X. Tang, M. Wu, M. Li, and B. Ding, "On designing the event-triggered multistep model predictive control for nonlinear system over networks with packet dropouts and cyber attacks," IEEE Transactions on Cybernetics, doi:10.1109/tcyb.2021.3062056.
[23] H. Zhang, J. Zhang, Y. Cai, S. Sun, and J. Sun, "Leader-following consensus for a class of nonlinear multiagent systems under event-triggered and edge-event triggered mechanisms," IEEE Transactions on Cybernetics, doi:10.1109/tcyb.2020.3035907.
[24] M. Zhong, S.X. Ding, D. Zhou, X. He, An H_i/H_∞ optimization approach to event-triggered fault detection for linear discrete time systems, IEEE Transactions on Automatic Control 65 (10) (2020) 4464–4471.
[25] X. Ge, Q.-L. Han, Z. Wang, A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks, IEEE Transactions on Cybernetics 49 (1) (2019) 171–183.
[26] Q. Li, Z. Wang, W. Sheng, F.E. Alsaadi, F.E. Alsaadi, Dynamic event-triggered mechanism for $H_{-\infty}$ non-fragile state estimation of complex networks under randomly occurring sensor saturations, Information Sciences 509 (2020) 304–316.
[27] V. Rezaei, M. Stefanovic, Event-triggered cooperative stabilization of multiagent systems with partially unknown interconnected dynamics, Automatica 130 (2021) 109657.
[28] N. Zhao, P. Shi, W. Xing, and C.P. Lim, "Resilient adaptive event-triggered fuzzy tracking control and filtering for nonlinear networked systems under denial of service attacks," IEEE Transactions on Fuzzy Systems, doi:10.1109/tfuzz.2021.3106674.
[29] 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 Transactions on Fuzzy Systems 30 (1) (2022) 190–204.
[30] Z. Gu, T. Yin, Z. Ding, Path tracking control of autonomous vehicles subject to deception attacks via a learning-based event-triggered mechanism, IEEE Transactions on Neural Networks and Learning Systems 32 (12) (2021) 5644–5653.
[31] J. Liu, T. Yin, D. Yue, H.R. Karimi, J. Cao, Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks, IEEE Transactions on Cybernetics 51 (1) (2021) 162–173.
[32] L. Zha, R. Liao, J.L. Liu, X. Xie, E. Tian, and J. Cao, "Dynamic event-triggered output feedback control for networked systems subject to multiple cyber-attacks," IEEE Transactions on Cybernetics, doi:10.1109/tcyb.2021.3125851.
[33] Z. Gu, C.K. Ahn, D. Yue and X. Xie, Event-triggered H_∞ filtering for T-S fuzzy-model-based nonlinear networked systems with multisensors against DoS attacks, IEEE Transactions on Cybernetics, doi: 10.1109/tcyb.2020.3030028.
[34] 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 Transactions on Circuits and Systems I: Regular Papers 67 (3) (2020) 1021–1034.
[35] A. Girard, Dynamic triggering mechanisms for event-triggered control, IEEE Transactions Automatic Control 60 (7) (2015) 1992–1997.

Lijuan Zha received the Ph.D. degree from Donghua University in 2018. She is currently an Associate Professor at Nanjing University of Finance and Economics, Nanjing, China and a post doctoral research associate in School of Mathematics, Southeast University, Nanjing, China, from December 2018. Her current research interests include networked control systems, neural networks, and complex dynamical systems.

Rongfei Liao received the B.S. degree in Applied Mathematics from the Nanjing University of Finance and Economics, Nanjing, China, in 2019. She is currently pursuing the M.Sc. degree in the College of Information Engineering, Nanjing University of Finance and Economics. Her research interests include T-S fuzzy systems and networked secure control.

Jinliang Liu received the Ph.D. degree in automatic control from the School of Information Science and Technology, Donghua University, Shanghai, China, in 2011. He was a Postdoctoral Research Associate with the School of Automation, Southeast University, Nanjing, China, from 2013 to 2016. He was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, University of Hong Kong, Hong Kong, from 2016 to 2017. He was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea, from 2017 to 2018. He is currently a Professor with the Nanjing University of Finance and Economics, Nanjing. His research interests include networked control systems, complex dynamical networks, and time-delay systems.

Jinde Cao received the B.S. degree from Anhui Normal University, Wuhu, China, the M.S. degree from Yunnan University, Kunming, China, and the Ph.D. degree from Sichuan University, Chengdu, China, all in mathematics/applied mathematics, in 1986, 1989, and 1998, respectively. He joined the School of Mathematics, Southeast University, Nanjing, China, in 2000, where he is an Endowed Chair Professor, the Dean of the School of Mathematics and the Director of the Research Center for Complex Systems and Network Sciences. From 1989 to 2000, he was with Yunnan University, Kunming, China. From 2001 to 2002, he was a Post-Doctoral Research Fellow with the Chinese University of Hong Kong, Hong Kong. Prof. Cao was a recipient of the National Innovation Award of China in 2017 and the Highly Cited Researcher Award in Engineering, Computer Science, and Mathematics by Thomson Reuters/Clarivate Analytics. He was an Associate Editor of the IEEE Transactions on Neural Networks and Neurocomputing. He is an Associate Editor of the IEEE Transactions on Cybernetics, IEEE Transactions on Cognitive and Developmental Systems, Journal of the Franklin Institute, Mathematics and Computers in Simulation, Cognitive Neurodynamics, and Neural Networks. He is a fellow of IEEE, a member of the Academy of Europe and European Academy of Sciences and Arts, and a Fellow of Pakistan Academy of Sciences.



Xiangpeng Xie received the B.S. and Ph.D. degrees in engineering from Northeastern University, Shenyang, China, in 2004 and 2010, respectively. From 2010 to 2014, he was a Senior Engineer with the Metallurgical Corporation of China Ltd., Beijing, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms. Dr. Xie serves as an Associate Editor for the International Journal of Fuzzy Systems and International Journal of Control, Automation, and Systems.