Dynamic Event-Triggered Output Feedback Control for Networked Systems Subject to Multiple Cyber Attacks

Lijuan Zha, Rongfei Liao, Jinliang Liu, Xiangpeng Xie, Engang Tian, and Jinde Cao, *Fellow, IEEE*

***Abstract*—This article is concerned with the problem of the H_∞ output feedback control for a class of event-triggered networked systems subject to multiple cyber attacks. Two dynamic event-triggered generators are equipped at sensor and observer sides, respectively, to lower the frequency of unnecessary data transmission. The sensor-to-observer (STO) channel and observer-to-controller (OTC) channel are subject to deception attacks and Denial-of-Service (DoS) attacks, respectively. The aim of the addressed problem is to design an output feedback controller, with the consideration of the effects of dynamic event-triggered schemes (DETSs) and multiple cyber attacks. Sufficient condition is derived, which can guarantee that the resulted closed-loop system is asymptotically mean-square stable (AMSS) with a prescribed H_∞ performance. Moreover, we provide the desired output feedback controller design method. Finally, the effectiveness of the proposed method is demonstrated by an example.**

***Index Terms*—Dynamic event-triggered schemes (DETSs), networked control systems (NCSs), observer-based control, stochastic cyber attacks.**

I. Introduction

In recent years, networked control systems (NCSs) have been widely concerned due to the advantages of high reliability and low maintenance cost, flexible configuration, and simple installation. Significant attention has been paid and many important results are achieved [1]–[5]. Considering the fact that the full information of the system state is difficult to be obtained in some practical control systems, the output feedback control is very necessary in these circumstances and has been implemented in some appealing works. For example, considering the existence of interval time-varying delay, He *et al.* [6] provided an output feedback control method for a linear discrete-time system. In [7], the output feedback distributed containment controller was designed for high-order nonlinear multiagent systems. Mu *et al.* [8] studied the finite-time H_∞ control problem for networked semi-Markovian jump systems based on a reliable observer.

Though the introduction of wireless communication network into control systems has many advantages, it also may cause some challenging problems, such as network-induced delays and packet dropouts, which are mainly resulted by the bandwidth limitation of communication networks. Nowadays, event-triggered schemes (ETSs) are popular with researchers because of their superiority in reducing the networked transmission amount while maintaining the expected system performance [9]–[12]. It has been proved by many investigations that ETSs are more effective to cope with the bandwidth-limitation issue compared with the periodic transmission schemes [13]–[15]. In the literature, various different ETSs can be available, under which the inputs of the controllers or state estimators are updated when the predesigned triggering conditions are violated [16]–[20]. It should be mentioned that either fixed or dynamic thresholds are devised in most of the existing event-triggered approaches [21]–[23]. For instance, Liu *et al.* [21] addressed the leader–follower consensus problems for nonlinear multiagent systems under event-/self-triggered strategies. In [22], a team-triggered control strategy was proposed for fixed-time consensus of double-integrator agents with uncertain disturbance. The problem of impulsive control was investigated for the hybrid event-triggered multiagent system under switching topologies in [23]. However, the majority of the current control methods are based on the periodic ETSs and ignore the negative impact of the cyber attacks on the NCSs, which motivates us to investigate the resilient dynamic event-triggered control problem for NCSs undergoing cyber attacks.

Nowadays, the security issue of NCSs has received broad interest due to the fact that the signal transmission in NCSs

Manuscript received 6 May 2021; revised 2 September 2021; accepted 1 November 2021. Date of publication 19 November 2021; date of current version 18 November 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61903182 and Grant 61973152; in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20190794 and Grant BK20211290; in part by the China Postdoctoral Science Foundation under Grant 2019M651651; and in part by the Qinglan Project of Jiangsu Province of China. This article was recommended by Associate Editor C.-M. Lin. *(Corresponding author: Jinliang Liu.)*

Lijuan Zha is with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China, and also with the School of Mathematics, Southeast University, Nanjing 210096, China (e-mail: zhalijuan@vip.163.com).

Rongfei Liao and Jinliang Liu are with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: liaorongfei110@163.com; liujinliang@vip.163.com).

Xiangpeng Xie is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: xiexiangpeng1953@163.com).

Engang Tian is with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: tianengang@163.com).

Jinde Cao is with the School of Mathematics and the Research Center for Complex Systems and Network Sciences, Southeast University, Nanjing 210096, China (e-mail: jdcao@seu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCYB.2021.3125851.

Digital Object Identifier 10.1109/TCYB.2021.3125851

is implemented via a shared wireless network, which is vulnerable to different types of hostile attacks generated by adversaries. Once the attackers complete the malicious actions to the control system, it will cause harm to the NCSs, leading to tremendous financial and security effects [24]–[28]. Therefore, to protect NCSs from malicious attacks, it is of great importance to enhance the system counter-attack ability. Recently, increasing attention has been paid to deal with the security problem of NCSs [29]–[32]. For example, Gao *et al.* [29] researched the deception attacks for discrete Markov jump control systems with ETS. In [30], considering Denial-of-Service (DoS) jamming attacks, the distributed set-membership filtering problem for discrete-time systems with fading measurements was investigated. In [31], the presence of cyber attacks was considered for connected vehicle discrete-time systems with an interaction network. In [32], under the influence of dual-terminal cyber attacks, a decentralized control method was developed for event-triggered switched systems with quantization. Based on the above observations, it makes great sense to investigate the stability and control performance for NCSs that are vulnerable to attack.

To the best of our knowledge, the results about the observer-based dynamic ETSs (DETSs) control problem with multiple cyber attacks are not fully investigated. Motivated by all the aforementioned analysis, in this article, we focus on output feedback control problem for event-triggered NCSs subject to multiple cyber attacks. The goal of this article is to design a secure output feedback controller for the addressed system, which can guarantee the prescribed system performance and tolerate the cyber attacks. The novelties of this article are summarized as follows.

1) Two independent DETSs are introduced to economize the communication network resources. Dynamic thresholds are designed for the DETSs to reduce the bandwidth usage of the communication networks.
2) A new model of the output feedback control system is constructed with the consideration of the two-channel DETSs, external disturbances, unmeasured states, and randomly occurring malicious cyber attacks, simultaneously.
3) An new output feedback control strategy is presented to guarantee the augmented system is asymptotically mean-square stable (AMSS) with the prescribed H_∞ performance.

The remainder of this article is organized as follows. Section II describes the observer-based dynamic event-triggered NCS and gives some preliminaries. Section III presents the main results of this article. Simulation results are given in Section IV. Finally, we conclude this article in Section V.

Notation: $\mathbb{R}^{m\times n}$ and $\mathbb{R}^m$ stand for, respectively, the set of $m \times n$ real matrices and the m-dimensional Euclidean space, I is the identity matrix of appropriate dimension, and 0 represents the zero matrix of compatible dimensions. The superscript T stands for matrix transposition. diag$\{\cdots\}$ represents a block-diagonal matrix, and the symbol $*$ stands for the symmetric term in a symmetric block matrix. The notation $P > 0 (P \geq 0)$ means that matrix P is a symmetric positive-definite (semipositive definite) matrix. $\|\cdot\|$ is the Euclidean norm of a vector and its induced norm of a matrix.

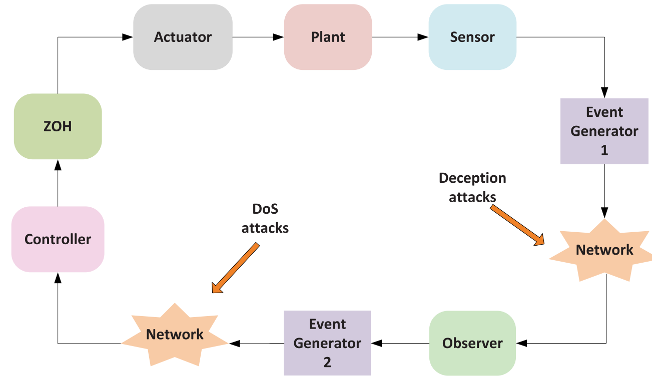


Fig. 1. Structure of the dynamic event-triggered output feedback control for networked systems with multiple attacks.

II. System Description

Consider the following discrete-time system described by:

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + D_1\omega_k \\ y_k = Cx_k \\ z_k = Ex_k + Bu_k + D_2\omega_k \end{cases} \tag{1}$$

where $x_k \in \mathbb{R}^m$, $y_k \in \mathbb{R}^p$, and $z_k \in \mathbb{R}^q$ $(k = 0, 1, 2, \ldots)$ are the system state vector, measured output, and control output, respectively. $u_k \in \mathbb{R}^n$ is the control input. ω_k is the external disturbance, which belongs to $L_2[0, \infty)$. A, B, C, E, D_1, and D_2 are known constant matrices with compatible dimensions.

As the system state vector x_k is not fully measurable, the aim of this article is to design an output feedback controller as follows:

$$\begin{cases} \hat{x}_{k+1} = A_c\hat{x}_k + L_c\tilde{y}_k \\ u_k = K_c\tilde{x}_k \end{cases} \tag{2}$$

where $\hat{x}_k \in \mathbb{R}^m$ is the observation of the system state vector x_k, and $\tilde{y}_k \in \mathbb{R}^p$ and $\tilde{x}_k \in \mathbb{R}^m$ are the real observer input and controller input, respectively. A_c, L_c, and K_c are the controller gain matrices to be determined.

In order to reduce the unnecessary data transmission and save the limited communication resources, as shown in Fig. 1, two dynamic event generators are used to determine whether the latest measured output and the observer state signal should be released and transmitted to the observer and controller, respectively.

Event generator 1 is set to reduce the unnecessary data transmission of the sensor-to-observer (STO) channel. As shown in Fig. 1, the sensor periodically samples the signal of the plant and sends them to event generator 1. Whether the sampled measured outputs need to be sent to a remote observer via a wireless network channel is determined by the following dynamic event-triggered condition:

$$\frac{1}{\theta_1}\zeta_{1,k} + \sigma_1 y_k^T\Omega_1 y_k - \phi_k^T\Omega_1\phi_k \leq 0 \tag{3}$$

where $\phi_k = y_k - y_{i_k}$, y_{i_k} is the signal released by event generator 1, σ_1 and θ_1 are given positive scalars, Ω_1 is a positive-definite weighting matrix to be designed later, and $\zeta_{1,k}$ is the internal dynamic variable satisfying

$$\zeta_{1,k+1} = \lambda_1 \zeta_{1,k} + \sigma_1 y_k^T \Omega_1 y_k - \phi_k^T \Omega_1 \phi_k \quad (4)$$

with $\zeta_{1,0} = \zeta_1^0 \geq 0$ being the initial condition and $\lambda_1 \in (0, 1)$ being a given constant satisfying $\lambda_1 \theta_1 \geq 1$.

If i_k is the latest triggering instant, then the next triggering instant i_{k+1} is defined as

$$i_{k+1} = \min\{k \in \mathbb{N} | k > i_k, k \text{ satisfying}(3)\}. \quad (5)$$

Remark 1: It is observed that the adaptive ETS in [33] and the DETSs in this article are different in some aspects. In [33], the adaptive ETS is designed for continuous networked systems, in which the threshold parameter can be dynamically adjusted dependent on the error between filter input updates. Whereas, in this article, the DETSs are designed for discrete-time networked systems. An additional internal dynamical variable is introduced for (3) in this article, which has perceptible influence on dynamically regulating the amount of the released data and the interevent time.

Remark 2: In (3), when $\theta_1 \rightarrow \infty$, the dynamic event-triggered condition (3) will reduce to the static event-triggered condition in particular as follows:

$$\sigma_1 y_k^T \Omega_1 y_k - \phi_k^T \Omega_1 \phi_k \leq 0. \quad (6)$$

Remark 3: It is noted that for any $k \in [i_k, i_{k+1})$, because there are no new triggered signals, the signal received by the observer keeps y_{i_k} and the following constraint holds:

$$\frac{1}{\theta_1}\zeta_{1,k} + \sigma_1 y_k^T \Omega_1 y_k - \phi_k^T \Omega_1 \phi_k > 0. \quad (7)$$

As shown in Fig. 1, we assume that the STO channel is attacked by the deception attacks. The occurrence of the deception attacks has impacts on the signal $\tilde{y}_k$ received by the observer as follows (see [10], [34] for example):

$$\tilde{y}_k = \alpha_k\big[\delta(y_{i_k}) - y_{i_k}\big] + y_{i_k} \quad (8)$$

where $\delta(y_k)$ is a nonlinear function. The stochastic variable α_k, which accounts for the probabilistic occurrence of the deception attacks, is a Bernoulli distributed variable taking values on $\{0, 1\}$ with the following probabilities:

$$\text{Prob}\{\alpha_k = 1\} = \bar{\alpha}, \text{Prob}\{\alpha_k = 0\} = 1 - \bar{\alpha} \quad (9)$$

where $\bar{\alpha} \in [0, 1)$ is a known positive constant and $\text{Prob}(\alpha_k - \bar{\alpha})^2 = \bar{\alpha}(1 - \bar{\alpha})$, obviously.

Remark 4: In (8), when $\alpha_k = 1$, the system is subject to the deception attacks, and the actual signal received by the observer is $\tilde{y}_k = \delta(y_{i_k})$. When $\alpha_k = 0$, cyber attacks are absent in the network, and the actual signal received by the observer is y_{i_k}.

As shown in Fig. 1, event generator 2 at the observer side is set up to further reduce the unnecessary data transmission and make better use of the limited communication resources. The triggering condition in event generator 2 is designed as follows:

$$\frac{1}{\theta_2}\zeta_{2,k} + \sigma_2 \hat{x}_k^T \Omega_2 \hat{x}_k - \varphi_k^T \Omega_2 \varphi_k \leq 0 \quad (10)$$

where $\varphi_k = \hat{x}_k - \hat{x}_{t_k}$, $\hat{x}_{t_k}$ is the signal released by event generator 2, σ_2 and θ_2 are given positive scalars, Ω_2 is a positive-definite weighting matrix to be designed later, and $\zeta_{2,k}$ is the internal dynamic variable satisfying

$$\zeta_{2,k+1} = \lambda_2 \zeta_{2,k} + \sigma_2 \hat{x}_k^T \Omega_2 \hat{x}_k - \varphi_k^T \Omega_2 \varphi_k \quad (11)$$

with $\zeta_{2,0} = \zeta_2^0 \geq 0$ being the initial condition and $\lambda_2 \in (0, 1)$ being a given constant satisfying $\lambda_2 \theta_2 \geq 1$.

If t_k is the latest triggered instant of event generator 2, then the next triggering instant t_{k+1} is expressed as

$$t_{k+1} = \min\{k \in \mathbb{N} | k > t_k, k \text{ satisfying}(10)\}. \quad (12)$$

Remark 5: As stated in article [35], [37], in order to keep $\zeta_{i,k} \geq 0 (i = 1, 2)$, the parameters λ_i and θ_i in DETSs (3) and (10) should satisfy $\lambda_i \theta_i \geq 1$.

Remark 6: Motivated by the DETSs in [36] and [37], in this article, the value of $\zeta_{i,k}$ for $i = 1, 2$ in (3) and (10) can be adjusted real time according to the information of the current measurement y_k (or the observer state $\hat{x}_k$) and the latest released measurement y_{i_k} (or the latest transmitted observer state $\hat{x}_{t_k}$). With the implementation of the two DETSs (3) and (10), the rate of the utilization of the limited network resources can be improved.

In the observer-to-controller (OTC) channel, we assume that DoS attacks may occur, which will block the communication channel. Based on the DETS (10) and DoS jamming attacks, the signal received by the controller in (2) can be written as

$$\tilde{x}_k = \beta_k \hat{x}_{t_k} \quad (13)$$

where β_k is a Bernoulli distributed white variable taking values on $\{0, 1\}$ with the following probabilities:

$$\text{Prob}\{\beta_k = 1\} = \bar{\beta}, \text{Prob}\{\beta_k = 0\} = 1 - \bar{\beta} \quad (14)$$

where $\bar{\beta} \in [0, 1)$ is a known positive constant and $\text{Prob}(\beta_k - \bar{\beta})^2 = \bar{\beta}(1 - \bar{\beta})$, obviously.

Remark 7: In (13), when $\beta_k = 0$, the system is subject to the DoS attacks, and the signal received by the controller is zero. When $\beta_k = 1$, it means data transmission in the OTC channel is normal, and the actual signal received by the controller is $\hat{x}_{t_k}$.

Defining the error of observation as $e_k = x_k - \hat{x}_k$, we can derive x_{k+1} from (1), (2), and (13)

$$\begin{aligned} x_{k+1} = &\big[A + \bar{\beta}BK_c\big]\hat{x}_k + Ae_k - \bar{\beta}BK_c\varphi_k + D_1\omega_k \\ &+ \big(\beta_k - \bar{\beta}\big)BK_c\big(\hat{x}_k - \varphi_k\big). \end{aligned} \quad (15)$$

From (2) and (8), one can obtain

$$\begin{aligned} \hat{x}_{k+1} = &[A_c + (1 - \bar{\alpha})L_cC]\hat{x}_k + (1 - \bar{\alpha})L_cCe_k \\ &- (1 - \bar{\alpha})L_c\phi_k + \bar{\alpha}L_c\delta(y_{i_k}) \\ &+ (\alpha_k - \bar{\alpha})L_c\big[\delta(y_{i_k}) - C(\hat{x}_k + e_k) + \phi_k\big]. \end{aligned} \quad (16)$$

Hence

$$\begin{aligned} e_{k+1} &= x_{k+1} - \hat{x}_{k+1} \\ &= \big[A + \bar{\beta}BK_c - A_c - (1 - \bar{\alpha})L_cC\big]\hat{x}_k \\ &\quad + [A - (1 - \bar{\alpha})L_cC]e_k + (1 - \bar{\alpha})L_c\phi_k \\ &\quad - \bar{\beta}BK_c\varphi_k - \bar{\alpha}L_c\delta(y_{i_k}) + D_1\omega_k \end{aligned}$$

$$
\begin{aligned}
&+ (\alpha_k - \bar{\alpha})L_c\big[C\hat{x}_k + Ce_k - \phi_k - \delta(y_{i_k})\big]\\
&+ \big(\beta_k - \bar{\beta}\big)BK_c(\hat{x}_k - \varphi_k). \qquad (17)
\end{aligned}
$$

Let $\eta_k = \begin{bmatrix}\hat{x}_k\\ e_k\end{bmatrix}$, we derive the following augmented system:

$$
\begin{cases}
\eta_{k+1} = \tilde{A}\eta_k - (1-\bar{\alpha})\tilde{L}\phi_k - \bar{\beta}\tilde{B}\varphi_k + \bar{\alpha}\tilde{L}\delta(y_{i_k})\\
\qquad +(\alpha_k - \bar{\alpha})\Big[\tilde{C}\eta_k + \tilde{L}\phi_k + \tilde{L}\delta(y_{i_k})\Big]\\
\qquad +\big(\beta_k - \bar{\beta}\big)\big(\tilde{K}\eta_k - \tilde{B}\varphi_k\big) + \tilde{D}\omega_k\\
z_k \quad = \big(E\tilde{I} + \bar{\beta}BK_c\bar{I}\big)\eta_k - \bar{\beta}BK_c\varphi_k + D_2\omega_k\\
\qquad +\big(\beta_k - \bar{\beta}\big)\big[BK_c\bar{I}\eta_k - BK_c\varphi_k\big]
\end{cases} \qquad (18)
$$

where

$$
\begin{aligned}
\tilde{A} &= \begin{bmatrix} A_c + (1-\bar{\alpha})L_cC & (1-\bar{\alpha})L_cC\\ A - A_c + \bar{\beta}BK_c - (1-\bar{\alpha})L_cC & A - (1-\bar{\alpha})L_cC\end{bmatrix}\\
\tilde{B} &= \begin{bmatrix}0\\ BK_c\end{bmatrix}, \tilde{L} = \begin{bmatrix}L_c\\ -L_c\end{bmatrix}, \tilde{D} = \begin{bmatrix}0\\ D_1\end{bmatrix}, \tilde{K} = \begin{bmatrix}0 & 0\\ BK_c & 0\end{bmatrix}\\
\tilde{C} &= \begin{bmatrix}-L_cC & -L_cC\\ L_cC & L_cC\end{bmatrix}, \tilde{I} = \big[I\ I\big], \bar{I} = \big[I\ 0\big].
\end{aligned}
$$

Remark 8: In this article, the NCSs under multiple cyber attacks are described by a discrete-time linear system (1) with input and external disturbance. The input of the observer is modeled as (8), which reflects the effect of the deception attacks. The control input subject to DoS attacks is expressed as (13). The Bernoulli-distributed sequences α_k and β_k account for the successful ratio of the cyber attacks [9].

The objective of this article is to design an output feedback controller in the form of (2) such that the following requirements are satisfied.

1) The augmented system (18) with $\omega_k = 0$ is AMSS.
2) Under the zero-initial condition, the control output z_k satisfies

$$
E\left\{\sum_{k=0}^{+\infty}\|z_k\|^2\right\} < \gamma^2\sum_{k=0}^{+\infty}\|\omega_k\|^2 \qquad (19)
$$

for all nonzero ω_k, where $\gamma > 0$ is the given attenuation level.

The following lemma and assumptions are necessary in the derivation of the main results.

Assumption 1: $\forall y \in \mathbb{R}^p$, $\delta(y)$ is a nonlinear function, which is assumed to satisfy

$$
\delta\big(y_{i_k}\big)^T\delta\big(y_{i_k}\big) \le y_{i_k}^T\Gamma^T\Gamma y_{i_k} \qquad (20)
$$

where Γ is a known matrix.

Assumption 2: B is assumed to be a matrix with full column rank.

Lemma 1: For the full rank matrix $\operatorname{rank}(B) = n$, $B \in R^{m\times n}$, the singular value decomposition (SVD) for B can be described as $B = O\begin{bmatrix}S\\ 0\end{bmatrix}V^T$, where $O^T\cdot O = I$ and $V^T\cdot V = I$. Let matrices $P > 0$, $M \in R^{m\times m}$, $N \in R^{n\times m}$. Then, there exits P_1 such that $PB = BP_1$ if and only if the following condition holds:

$$
P = O\begin{bmatrix}M & 0\\ 0 & N\end{bmatrix}O^T. \qquad (21)
$$

III. Main Results

In this section, a sufficient condition is derived to guarantee that the augmented system (18) is AMSS with a weighted H_∞ performance and then the desired H_∞ output feedback controller gains are designed by solving a certain linear matrix inequality (LMI).

Theorem 1: Given scalars $\bar{\alpha} \in (0,1)$, $\bar{\beta} \in (0,1)$, and $\mu > 0$, feedback gain matrix K_c, and observer gain matrices A_c and L_c, system (18) (with $\omega_k = 0$) is AMSS under the DETSs (3) and (10), if there exists a positive-definite symmetric matrix P such that

$$
\Sigma_1 = \begin{bmatrix}
\Xi & * & * & * & *\\
P\bar{A} & -P & * & * & *\\
\sqrt{\bar{\alpha}(1-\bar{\alpha})}P\bar{C} & 0 & -P & * & *\\
\sqrt{\bar{\beta}(1-\bar{\beta})}P\bar{B} & 0 & 0 & -P & *\\
\mu\Gamma\bar{D} & 0 & 0 & 0 & -\mu I
\end{bmatrix} < 0 \qquad (22)
$$

where

$$
\begin{aligned}
\Xi &= \begin{bmatrix}
\Psi_{11} & * & * & *\\
0 & \Psi_{22} & * & *\\
0 & 0 & \Psi_{33} & *\\
0 & 0 & 0 & -\mu I
\end{bmatrix}\\
\Psi_{11} &= -P + m_1\sigma_1\tilde{I}^TC^T\Omega_1C\tilde{I} + m_2\sigma_2\bar{I}^T\Omega_2\bar{I}\\
\Psi_{22} &= -m_1\Omega_1\\
\Psi_{33} &= -m_2\Omega_2\\
m_1 &= 1 - \lambda_1 + \frac{1}{\theta_1}\\
m_2 &= 1 - \lambda_2 + \frac{1}{\theta_2}\\
\bar{A} &= \big[\tilde{A}\ -(1-\bar{\alpha})\tilde{L}\ -\bar{\beta}\tilde{B}\ \bar{\alpha}\tilde{L}\big]\\
\bar{B} &= \big[\tilde{K}\quad 0\quad -\tilde{B}\quad 0\big]\\
\bar{C} &= \big[\tilde{C}\quad \tilde{L}\quad 0\quad \tilde{L}\big]\\
\bar{D} &= \big[C\tilde{I}\quad -I\quad 0\quad 0.\big]
\end{aligned}
$$

Proof: Construct a Lyapunov–Krasovskii function as

$$
V_k = \eta_k^TP\eta_k + \frac{1}{\theta_1}\zeta_{1,k} + \frac{1}{\theta_2}\zeta_{2,k}. \qquad (23)
$$

According to (4) and (11), with $\omega_k = 0$, the forward difference of V_k defined as $\Delta V_k = V_{k+1} - V_k$ along the trajectory of (18) is calculated as

$$
\begin{aligned}
\mathbb{E}\{\Delta V_k\} &= \mathbb{E}\{V_{k+1} - V_k\}\\
&\le \mathbb{E}\{\Big[\tilde{A}\eta_k - (1-\bar{\alpha})\tilde{L}\phi_k - \bar{\beta}\tilde{B}\varphi_k + \bar{\alpha}\tilde{L}\delta(y_{i_k})\Big]^TP\\
&\quad \Big[\tilde{A}\eta_k - (1-\bar{\alpha})\tilde{L}\phi_k - \bar{\beta}\tilde{B}\varphi_k + \bar{\alpha}\tilde{L}\delta(y_{i_k})\Big]\\
&\quad + (\alpha_k - \bar{\alpha})^2\Big[\tilde{C}\eta_k + \tilde{L}\phi_k + \tilde{L}\delta(y_{i_k})\Big]^TP\\
&\quad \Big[\tilde{C}\eta_k + \tilde{L}\phi_k + \tilde{L}\delta(y_{i_k})\Big]\\
&\quad + \big(\beta_k - \bar{\beta}\big)^2\big[\tilde{K}\eta_k - \tilde{B}\varphi_k\big]^TP\big[\tilde{K}\eta_k - \tilde{B}\varphi_k\big]\\
&\quad - \eta_k^TP\eta_k\\
&\quad + \frac{1}{\theta_1}\big[(\lambda_1 - 1)\zeta_{1,k} + \sigma_1y_k^T\Omega_1y_k - \phi_k^T\Omega_1\phi_k\big]\\
&\quad + \frac{1}{\theta_2}\big[(\lambda_2 - 1)\zeta_{2,k} + \sigma_2\hat{x}_k^T\Omega_2\hat{x}_k - \varphi_k^T\Omega_2\varphi_k\big]. \qquad (24)
\end{aligned}
$$

Define $\xi_k = \left[\eta_k^T \ \phi_k^T \ \varphi_k^T \ \delta^T(y_{i_k})\right]^T$. By combining (20) and the triggering condition (3) and (10), we have

$$\begin{aligned}\mathbb{E}\{\Delta V_k\} \le\ & \xi_k^T\big[\bar{A}^T P\bar{A} + \bar{\alpha}(1-\bar{\alpha})\bar{C}^T P\bar{C} \\ & +\ \bar{\beta}(1-\bar{\beta})\bar{B}^T P\bar{B}\big]\xi_k - \mathbb{E}\{\eta_k^T P\eta_k\} \\ & +\ \mathbb{E}\left\{\left(1-\lambda_1+\frac{1}{\theta_1}\right)\left[\sigma_1 y_k^T\Omega_1 y_k - \phi_k^T\Omega_1\phi_k\right]\right\} \\ & +\ \mathbb{E}\left\{(1-\lambda_2+\frac{1}{\theta_2})\left[\sigma_2\hat{x}_k^T\Omega_2\hat{x}_k - \varphi_k^T\Omega_2\varphi_k\right]\right\} \\ & -\ \mu\left[\delta^T(y_{i_k})\delta(y_{i_k}) - y_{i_k}^T\Gamma^T\Gamma y_{i_k}\right] \\ =\ & \mathbb{E}\{\xi_k^T\big[\Xi + \bar{A}^T P\bar{A} + \bar{\alpha}(1-\bar{\alpha})\bar{C}^T P\bar{C} \\ & +\ \bar{\beta}(1-\bar{\beta})\bar{B}^T P\bar{B} + \mu\bar{D}^T\Gamma^T\Gamma\bar{D}\big]\xi_k\}. \quad (25)\end{aligned}$$

It is clear that $\Sigma_1 < 0$ indicates there exists a sufficiently small scalar $\iota > 0$ such that

$$\Sigma_1 + \iota\mathrm{diag}\{I_{2m\times 2m}, 0\} < 0. \quad (26)$$

By the Schur complement, one can derive that (26) can ensure

$$\begin{aligned}&\Xi + \iota\mathrm{diag}\{I_{2m\times 2m}, 0\} + \bar{A}^T P\bar{A} + \bar{\alpha}(1-\bar{\alpha})\bar{C}^T P\bar{C} \\ &+\bar{\beta}(1-\bar{\beta})\bar{B}^T P\bar{B} + \mu\bar{D}^T\Gamma^T\Gamma\bar{D} < 0. \quad (27)\end{aligned}$$

It follows from (25) and (27) that:

$$\mathbb{E}\{\Delta V_k\} \le -\iota\mathbb{E}\left\{\|\eta_k\|^2\right\}. \quad (28)$$

Summing up both sides of (28) from 0 to ∞ with respect to k, we can derive that

$$\mathbb{E}\left\{\sum_{k=0}^{\infty}\|\eta_k\|^2\right\} \le \frac{1}{\iota}\mathbb{E}\{V_0\}. \quad (29)$$

Let $\rho_{\max} = \lambda_{\max}(P)$, it is obvious that

$$\mathbb{E}\left\{\sum_{k=0}^{\infty}\|\eta_k\|^2\right\} \le \frac{1}{\iota}\left\{\rho_{\max}\mathbb{E}\{\|\eta_0\|^2 + \frac{1}{\theta_1}\zeta_{1,0} + \frac{1}{\theta_2}\zeta_{2,0}\}\right\}. \quad (30)$$

Then, the augmented system (18) with $\omega_k = 0$ is AMSS.

Now, we are in a position to analyze the H_∞ performance of the augmented system (18).

Theorem 2: Given scalars γ, $\bar{\alpha} \in (0,1)$, $\bar{\beta} \in (0,1)$ and $\mu > 0$, feedback gain matrix K_c, and observer gain matrices A_c and L_c, system (18) is AMSS with a guaranteed H_∞ performance index γ under the DETSs (3) and (10), if there exists a positive-definite symmetric matrix P such that

$$\Sigma_2 = \begin{bmatrix} \bar{\Xi} & * & * & * & * & * & * \\ P\mathcal{A} & -P & * & * & * & * & * \\ \epsilon_1 P\mathcal{C} & 0 & -P & * & * & * & * \\ \epsilon_2 P\mathcal{B} & 0 & 0 & -P & * & * & * \\ \mu\Gamma\mathcal{D} & 0 & 0 & 0 & -\mu I & * & * \\ \mathcal{E} & 0 & 0 & 0 & 0 & -I & * \\ \epsilon_2\Lambda & 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \quad (31)$$

where

$$\begin{aligned}\bar{\Xi} &= \begin{bmatrix} \Psi_{11} & * & * & * & * \\ 0 & \Psi_{22} & * & * & * \\ 0 & 0 & \Psi_{33} & * & * \\ 0 & 0 & 0 & -\mu I & * \\ 0 & 0 & 0 & 0 & -\gamma^2 I \end{bmatrix} \\ \mathcal{A} &= \left[\tilde{A} \ -(1-\bar{\alpha})\tilde{L} \ -\bar{\beta}\tilde{B} \ \bar{\alpha}\tilde{L} \ \tilde{D}\right] \\ \mathcal{B} &= \left[\tilde{K} \ 0 \ -\tilde{B} \ 0 \ 0\right] \\ \mathcal{C} &= \left[\tilde{C} \ \tilde{L} \ 0 \ \tilde{L} \ 0\right] \\ \mathcal{D} &= \left[C\tilde{I} \ -I \ 0 \ 0 \ 0\right] \\ \mathcal{E} &= \left[E\tilde{I} + \bar{\beta}BK_c\bar{I} \ 0 \ -\bar{\beta}BK_c \ 0 \ D_2\right] \\ \Lambda &= \left[BK_c\bar{I} \ 0 \ -BK_c \ 0 \ 0\right] \\ \epsilon_1 &= \sqrt{\bar{\alpha}(1-\bar{\alpha})}, \epsilon_2 = \sqrt{\bar{\beta}(1-\bar{\beta})}.\end{aligned}$$

Other symbols are given in Theorem 1.

Proof: For all nonzero ω_k, selecting the same Lyapunov function as in Theorem 1, by similar derivation as in Theorem 1, one has

$$\begin{aligned}\mathbb{E}\{\Delta V_k\} \le\ & \mathbb{E}\{\varsigma_k^T\big[\Xi_1 + \mathcal{A}^T P\mathcal{A} + \bar{\alpha}(1-\bar{\alpha})\mathcal{C}^T P\mathcal{C} \\ & + \bar{\beta}(1-\bar{\beta})\mathcal{B}^T P\mathcal{B} + \mu\mathcal{D}^T\Gamma^T\Gamma\mathcal{D}\big]\varsigma_k\} \quad (32)\end{aligned}$$

where

$$\begin{aligned}\varsigma_k &= \left[\eta_k^T \quad \phi_k^T \quad \varphi_k^T \quad \delta^T(y_{i_k}) \quad \omega_k^T\right]^T \\ \Xi_1 &= \begin{bmatrix} \Psi_{11} & * & * & * & * \\ 0 & \Psi_{22} & * & * & * \\ 0 & 0 & \Psi_{33} & * & * \\ 0 & 0 & 0 & -\mu I & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.\end{aligned}$$

Adding the zero term $\mathbb{E}\{z_k^T z_k - \gamma^2\omega_k^T\omega_k - (z_k^T z_k - \gamma^2\omega_k^T\omega_k)\}$ to $\mathbb{E}\{\Delta V_k\}$ yields

$$\begin{aligned}\mathbb{E}\{\Delta V_k\} \le\ & \mathbb{E}\{\varsigma_k^T\big[\bar{\Xi} + \mathcal{A}^T P\mathcal{A} + \bar{\alpha}(1-\bar{\alpha})\mathcal{C}^T P\mathcal{C} + \mu\mathcal{D}^T\Gamma^T\Gamma\mathcal{D} \\ & + \bar{\beta}(1-\bar{\beta})\mathcal{B}^T P\mathcal{B} + \mathcal{E}^T\mathcal{E} + \bar{\beta}(1-\bar{\beta})\Lambda^T\Lambda\big]\varsigma_k\} \\ & -\ \mathbb{E}\left\{z_k^T z_k - \gamma^2\omega_k^T\omega_k\right\}. \quad (33)\end{aligned}$$

Under the zero-initial condition, summing up (33) on both sides from 0 to T with respect to k, we can derive that

$$\begin{aligned}&\sum_{k=0}^{T}\mathbb{E}\{\Delta V_k\} \\ &\le \sum_{k=0}^{T}\mathbb{E}\{\varsigma_k^T\big[\bar{\Xi} + \mathcal{A}^T P\mathcal{A} + \bar{\alpha}(1-\bar{\alpha})\mathcal{C}^T P\mathcal{C} + \mu\mathcal{D}^T\Gamma^T\Gamma\mathcal{D} \\ &\qquad + \bar{\beta}(1-\bar{\beta})\mathcal{B}^T P\mathcal{B} + \mathcal{E}^T\mathcal{E} + \bar{\beta}(1-\bar{\beta})\Lambda^T\Lambda\big]\varsigma_k\} \\ &\quad -\sum_{k=0}^{T}\mathbb{E}\{z_k^T z_k\} + \sum_{k=0}^{T}\gamma^2\omega_k^T\omega_k \quad (34)\end{aligned}$$

and hence

$$\begin{aligned}&\mathbb{E}\left\{\sum_{k=0}^{T}\|z_k\|^2 - \gamma^2\sum_{k=0}^{T}\|\omega_k\|^2\right\} \\ &\le \sum_{k=0}^{T}\mathbb{E}\{\varsigma_k^T\big[\bar{\Xi} + \mathcal{A}^T P\mathcal{A} + \bar{\alpha}(1-\bar{\alpha})\mathcal{C}^T P\mathcal{C}\end{aligned}$$

$$+\bar{\beta}(1-\bar{\beta})\mathcal{B}^T P\mathcal{B}+\mathcal{E}^T\mathcal{E}+\bar{\beta}(1-\bar{\beta})\Lambda^T\Lambda$$
$$+\mu\mathcal{D}^T\Gamma^T\Gamma\mathcal{D}\big]\varsigma_k\big\}-\mathbb{E}\{V_{T+1}\}. \tag{35}$$

Based on the Schur complement lemma, noticing (31), it is easy to derive $\mathbb{E}\{\sum_{k=0}^{T}\|z_k\|^2-\gamma^2\sum_{k=0}^{T}\|\omega_k\|^2\}<0$. Letting $T\to+\infty$, then H_∞ performance constraint (19) is met, which completes the proof. ■

It is noted that due to some nonlinear terms in (31), it is difficult to obtain the observer-based controller parameters from Theorem 2. In order to deal with this problem, the following theorem is provided to convert the nonlinear matrix inequality (31) into LMI.

Theorem 3: For given parameters γ, $\bar{\alpha}\in(0,1)$, $\bar{\beta}\in(0,1)$, $\mu>0$, for the augmented system (18) , if there exists a symmetric positive-definite matrix $P\triangleq \mathrm{diag}\{\bar{P},\bar{P}\}$ such that the following LMI holds:

$$\Sigma_4=\begin{bmatrix}\bar{\Xi} & * & * & * & * & * & * \\ \Sigma_{21} & -P & * & * & * & * & * \\ \Sigma_{31} & 0 & -P & * & * & * & * \\ \Sigma_{41} & 0 & 0 & -P & * & * & * \\ \Gamma\Sigma_{51} & 0 & 0 & 0 & -\mu I & * & * \\ \Sigma_{61} & 0 & 0 & 0 & 0 & \Sigma_{66} & * \\ \Sigma_{71} & 0 & 0 & 0 & 0 & 0 & \Sigma_{77}\end{bmatrix}<0 \tag{36}$$

where

$$\Sigma_{21}=\begin{bmatrix}\Theta_{21} & -\epsilon_3\Theta_{22} & -\bar{\beta}\Theta_{23} & \bar{\alpha}\Theta_{24} & \Theta_{27}\end{bmatrix}$$
$$\Sigma_{31}=\begin{bmatrix}\epsilon_1\Theta_{31} & \epsilon_1\Theta_{32} & 0 & \epsilon_1\Theta_{34} & 0\end{bmatrix}$$
$$\Sigma_{41}=\begin{bmatrix}\epsilon_2\Theta_{41} & 0 & -\epsilon_2\Theta_{43} & 0 & 0\end{bmatrix}$$
$$\Sigma_{51}=\begin{bmatrix}\mu C\tilde{I} & -\mu I & 0 & 0 & 0\end{bmatrix},$$
$$\Sigma_{61}=\begin{bmatrix}\bar{P}E\tilde{I}+\bar{\beta}BT & 0 & -\bar{\beta}BT & 0 & \bar{P}D_2\end{bmatrix}$$
$$\Sigma_{71}=\begin{bmatrix}\epsilon_2BT\bar{I} & 0 & -\epsilon_2BT & 0 & 0\end{bmatrix}$$
$$\Theta_{21}=\begin{bmatrix}A_1+\epsilon_3L_1C & \epsilon_3L_1C\\ \bar{P}A-A_1+\bar{\beta}BT-\epsilon_3L_1C & \bar{P}A-\epsilon_3L_1C\end{bmatrix}$$
$$\Theta_{22}=\Theta_{24}=\Theta_{32}=\Theta_{34}=\begin{bmatrix}L_1\\ -L_1\end{bmatrix}\Theta_{23}=\Theta_{43}=\begin{bmatrix}0\\ BT\end{bmatrix}$$
$$\Theta_{27}=\begin{bmatrix}0\\ \bar{P}D_1\end{bmatrix}\Theta_{31}=\begin{bmatrix}-L_1C & -L_1C\\ L_1C & L_1C\end{bmatrix}$$
$$\Theta_{41}=\begin{bmatrix}0 & 0\\ BT & 0\end{bmatrix}$$
$$\Sigma_{55}=-\mu I,\ \Sigma_{66}=\Sigma_{77}=-2\varepsilon\bar{P}+\varepsilon^2I$$

$$\epsilon_1=\sqrt{\bar{\alpha}(1-\bar{\alpha})},\ \epsilon_2=\sqrt{\bar{\beta}(1-\bar{\beta})},\ \epsilon_3=1-\bar{\alpha}.$$

Other symbols are given in Theorem 2.

Proof: Set $P=\mathrm{diag}\{\bar{P},\bar{P}\}$, and define $A_1=\bar{P}A_c$, $L_1=\bar{P}L_c$ and $T=P_1K_c$. According to Lemma 1, for $\bar{P}=O\begin{bmatrix}M & *\\ 0 & N\end{bmatrix}O^T$, there exists $P_1=VS^{-1}MSV^T$ satisfying $\bar{P}B=BP_1$. Premultiplying and postmultiplying (31) by $\mathrm{diag}\{\underbrace{I,\ldots,I}_{9},\bar{P},\bar{P}\}$, replace $\bar{P}A_c$, $\bar{P}L_c$, and P_1K_c by A_1, L_1, and T, respectively, then we can obtain

$$\Sigma_3=\begin{bmatrix}\Xi_4 & * & * & * & * & * & * \\ \Sigma_{21} & -P & * & * & * & * & * \\ \Sigma_{31} & 0 & -P & * & * & * & * \\ \Sigma_{41} & 0 & 0 & -P & * & * & * \\ \Sigma_{51} & 0 & 0 & 0 & \Sigma_0 & * & * \\ \Sigma_{61} & 0 & 0 & 0 & 0 & -\bar{P}^2 & * \\ \Sigma_{71} & 0 & 0 & 0 & 0 & 0 & -\bar{P}^2\end{bmatrix}<0. \tag{37}$$

For $\forall\varepsilon>0$, from

$$\left(I-\varepsilon^{-1}\bar{P}\right)\left(I-\varepsilon^{-1}\bar{P}\right)\geq 0 \tag{38}$$

we can obtain

$$-\bar{P}^2\leq -2\varepsilon\bar{P}+\varepsilon^2I. \tag{39}$$

Replacing $-\bar{P}^2$ by $-2\varepsilon\bar{P}+\varepsilon^2I$ in (37), then (37) can be guaranteed by (36). This completes the proof.

Remark 9: In this article, the dynamic event-triggered output feedback control problem is addressed for networked systems subject to multiple cyber attacks. There are four factors that complicate the observer-based controller design method, that is, the two dynamic event-triggered control approach, the DoS attacks, and the deception attacks. In Theorem 3, the observer-based controller and the dynamic event-triggering matrices are co-designed, which reflect the influences of the four factors.

IV. Simulation Examples

In this section, a simulation example is presented to illustrate the validity of the proposed output feedback controller.

Consider the system (1) with

$$A=\begin{bmatrix}0.2335 & -0.0672 & 0\\ 2.0570 & -0.2967 & 0\\ 0 & 0 & 0.4\end{bmatrix},B=\begin{bmatrix}1 & 0\\ 1 & 1\\ 0 & 1\end{bmatrix}$$
$$D_1=\begin{bmatrix}0.1\\ 0\\ 0.1\end{bmatrix}E=\begin{bmatrix}0.1 & 0 & 0\\ 0.2 & 0 & 0.2\\ 0 & 0.1 & 0.2\end{bmatrix},D_2=\begin{bmatrix}0.11\\ 0.03\\ 0.09\end{bmatrix}$$
$$C=\begin{bmatrix}0.1 & 0.8 & 0.7\\ -0.6 & 0.9 & 0.6\end{bmatrix}.$$

For the DETS of (3) and (10), let $\lambda_1=0.1$, $\lambda_2=0.8$, $\theta_1=\theta_2=10$, $\sigma_1=0.1$, and $\sigma_2=0.7$, the initial conditions of $\zeta_{1,k}$ and $\zeta_{2,k}$ are $\zeta_1^0=10$ and $\zeta_2^0=15$, respectively.

The occurrence probabilities of cyber attacks are chosen as $\bar{\alpha}=0.3$ and $\bar{\beta}=0.7$, and the nonlinear function is as follows:

$$\delta(y_{ik})=\begin{bmatrix}0.7\sin(i_k) & 0\\ 0 & 0.7\sin(i_k)\end{bmatrix}\times y_{i_k}$$

then we can obtain $\delta(y_{i_k})^T\delta(y_{i_k})\leq y_{i_k}^T\Gamma^T\Gamma y_{i_k}$, where $\Gamma=\mathrm{diag}\{0.7,0.7\}$.

By solving condition (36), the feedback gain matrix, the observer gains, and the triggering matrices are obtained as

$$A_c=\begin{bmatrix}0.1544 & -0.0376 & 0.0202\\ 1.4913 & -0.2123 & 0.0255\\ -0.0022 & 0.0014 & 0.1800\end{bmatrix}$$

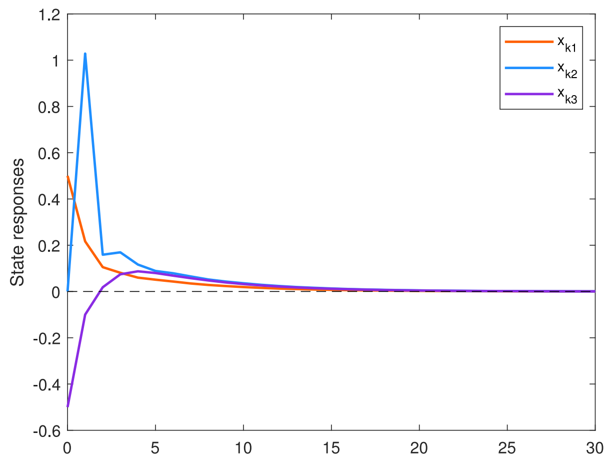


Fig. 2. State responses.

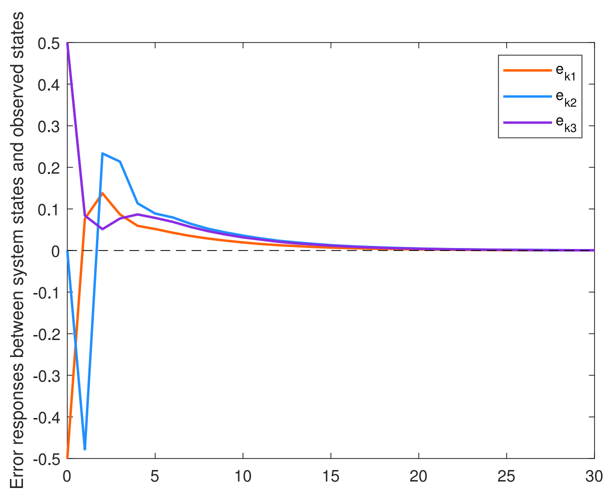


Fig. 3. Error responses between system states and observed states.

$$L_c = \begin{bmatrix} 0.0077 & -0.0143 \\ 0.0799 & -0.1078 \\ 0.0074 & -0.0008 \end{bmatrix}$$

$$K_c = \begin{bmatrix} -0.1550 & 0.0643 & 0.1801 \\ -0.1177 & -0.0318 & -0.2217 \end{bmatrix}$$

$$\Omega_1 = \begin{bmatrix} -0.1550 & 0.0643 & 0.1801 \\ -0.1177 & -0.0318 & -0.2217 \end{bmatrix}$$

$$\Omega_2 = \begin{bmatrix} 271.2308 & -19.1228 & 5.1005 \\ -19.1228 & 65.5148 & -16.0926 \\ 5.1005 & -16.0926 & 240.7276 \end{bmatrix}.$$

Given the initial conditions as $x_0^T = \begin{bmatrix} 0.5 & 0 & -0.5 \end{bmatrix}$ and $\hat{x}_0^T = \begin{bmatrix} 1 & 0 & -1 \end{bmatrix}$, the external disturbance is $\omega_k = e^{-0.2k}$.

According to the initial conditions and above-obtained parameters, the state responses of system (1) under multiple attacks and DETSs are depicted in Fig. 2, which illustrates that the system state is AMSS even when the multiple attacks are present intermittently. The error responses e_k are shown in Fig. 3. We can see the error gradually decreases to zero as expected.

The released instants in the STO channel based on DETS and static ETS (SETS) are depicted in Fig. 4, respectively. During the simulation time, the events are triggered 16 times under DETS and 25 times under SETS. From the comparison, we can easily obtain the conclusion that the DETSs can reduce the unnecessary data transmission more effectively than SETS.

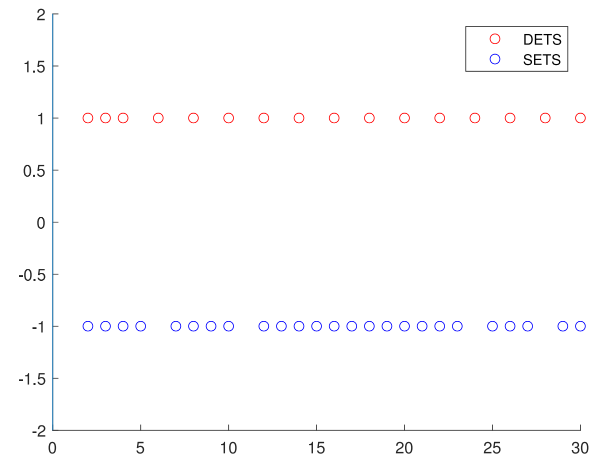


Fig. 4. Release instants.

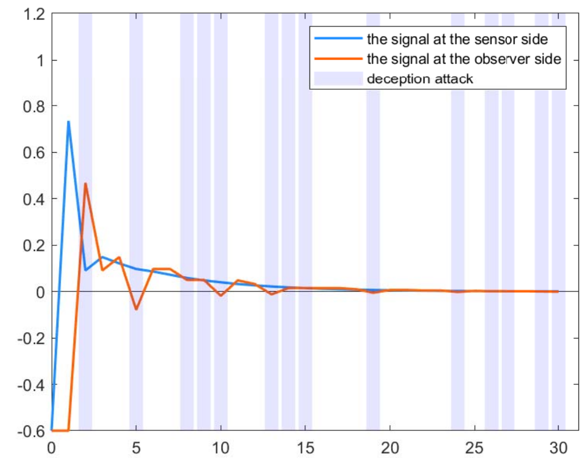


Fig. 5. Signal received by observer under deception attacks.

Fig. 5 shows the signal received by an observer under deception attacks, which will make the signal suddenly stray from the original path. Especially at the instant of $k = 5$, the deception attacks result in serious system deterioration. However, even though there are random deception attacks occurring, the signal reaches stability gradually. Fig. 6 depicts the control input subject to DoS attacks. When DoS attacks occur, the control input will turn out to be zero. The control input is also tending toward stability under stochastic DoS jamming attacks.

Based on the simulation results above, the proposed event-triggered output feedback control method performs very well.

Remark 10: The similar DETSs have been proposed in [36] and [37]. Whereas, the DETS proposed in [36] for observer-based control is in the continuous context. In [37], the DETS was designed for the distributed set-membership estimation for a discrete-time linear time-varying system. In contrast, in this article, the DETSs are exploited to study

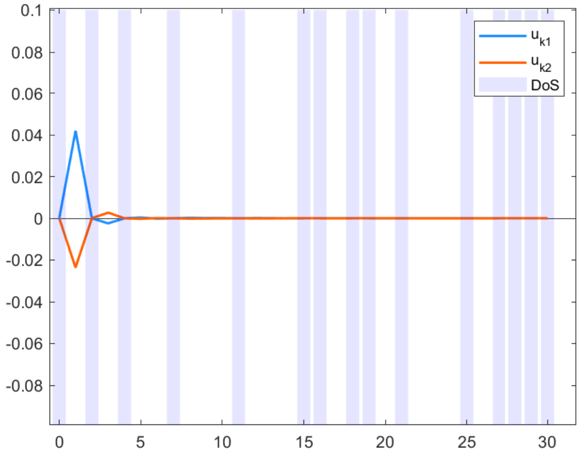


Fig. 6. Control input u_k under DoS attacks.

the observer-based control for networked systems subject to multiple cyber attacks.

V. Conclusion

In this article, we have investigated the dynamic event-triggered output feedback control for NCSs with multiple cyber attacks. A novel two-channel DETSs has been proposed to enhance the utilization efficiency of network resources. Considering the characteristics of the randomly occurring deception attacks and DoS jamming attacks, an observer error system model is constructed. Tractable LMI-based stability analysis and control design criteria for the co-design of the observer and controller gains have been derived while preserving satisfactory control performance despite the presence of deception attacks and DoS jamming attacks. Finally, a numerical example has been exploited to demonstrate the effectiveness of the proposed dynamic event-triggered output feedback controller design method.

Future research directions will include the problem of an observer-based dynamic event-triggering consensus control for multiagent systems with multiple cyber attacks.

References

[1] S. Hu, D. Yue, Q.-L. Han, X. Xie, X. Chen, and C. Dou, "Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1952–1964, May 2020.

[2] H. Sun, J. Sun, and J. Chen, "Analysis and synthesis of networked control systems with random network-induced delays and sampling intervals," *Automatica*, vol. 125, Mar. 2021, Art. no. 109385.

[3] L. Wang, Z. Wang, G. Wei, and F. E. Alsaadi, "Observer-based consensus control for discrete-time multiagent systems with coding-decoding communication protocol," *IEEE Trans. Cybern.*, vol. 49, no. 12, pp. 4335–4345, Dec. 2019.

[4] X. Wang, X. Wang, H. Su, and J. Lam, "Coordination control for uncertain networked systems using interval observers," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 4008–4019, Sep. 2020.

[5] C. Wu, X. Zhao, W. Xia, J. Liu, and T. Baar, "L_2-gain analysis for dynamic event-triggered networked control systems with packet losses and quantization," *Automatica*, vol. 129, Jul. 2021, Art. no. 109587.

[6] Y. He, M. Wu, G.-P. Liu, and J.-H. She, "Output feedback stabilization for a discrete-time system with a time-varying delay," *IEEE Trans. Autom. Control*, vol. 53, no. 10, pp. 2372–2377, Nov. 2008

[7] Y. Li, C. Hua, S. Wu, and X. Guan, "Output feedback distributed containment control for high-order nonlinear multiagent systems," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 2032–2043, Aug. 2017

[8] X. Mu, X. Li, J. Fang, and X. Wu, "Reliable observer-based finite-time H_∞ control for networked nonlinear semi-Markovian jump systems with actuator fault and parameter uncertainties via dynamic event-triggered scheme," *Inf. Sci.*, vol. 546, pp. 573–595, Feb. 2021.

[9] J. Liu, Y. Wang, J. Cao, D. Yue, and X. Xie, "Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack," *IEEE Trans. Cybern.*, vol. 51, no. 8, pp. 4000–4010, Aug. 2021.

[10] J. Liu, T. Yin, J. Cao, D. Yue, and H. R. Karimi, "Security control for T-S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 10, pp. 6544–6554, Oct. 2021.

[11] J. Lian, C. Li, and B. Xia, "Sampled-data control of switched linear systems with application to an F-18 aircraft," *IEEE Trans. Ind. Electron.*, vol. 64, no. 2, pp. 1332–1340, Feb. 2017.

[12] G. Ran, Z. Lu, F. Xu, and J. Lu, "Event-triggered dynamic output feedback control for networked T-S fuzzy systems with asynchronous premise variables," *IEEE Access*, vol. 6, pp. 78740–78750, 2018

[13] J. Liu, W. Suo, X. Xie, D. Yue, and J. Cao, "Quantized control for a class of neural networks with adaptive event-triggered scheme and complex cyber-attacks," *Int. J. Robust Nonlinear Control*, vol. 31, no. 10, pp. 4705–4728, 2021.

[14] J. Sun, J. Yang, S. Li, and Z. Zeng, "Predictor-based periodic event-triggered control for dual-rate networked control systems with disturbances," *IEEE Trans. Cybern.*, early access, Feb. 2, 2021, doi: 10.1109/TCYB.2021.3050329.

[15] M. Wang, J. Sun, and J. Chen, "Stabilization of perturbed continuous-time systems using event-triggered model predictive control," *IEEE Trans. Cybern.*, early access, Sep. 7, 2020, doi: 10.1109/TCYB.2020.3011177.

[16] T. Feng, Y. Wang, L. Liu, and B. Wu, "Observer-based event-triggered control for uncertain fractional-order systems," *J. Franklin Inst.*, vol. 357, no. 14, pp. 9423–9441, 2020.

[17] D. Wang, Z. Wang, Z. Wang, and W. Wang, "Design of hybrid event-triggered containment controllers for homogeneous and heterogeneous multiagent systems," *IEEE Trans. Cybern.*, vol. 51, no. 10, pp. 4885–4896, Oct. 2021.

[18] W. He, B. Xu, Q.-L. Han, and F. Qian, "Adaptive consensus control of linear multiagent systems with dynamic event-triggered strategies," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 2996–3008, Jul. 2020.

[19] A.-Y. Lu and G.-H. Yang, "Observer-based control for cyber-physical systems under denial-of-service with a decentralized event-triggered scheme," *IEEE Trans. Cybern.*, vol. 5, no. 12, pp. 4886–4895, Dec. 2020.

[20] W. Wang and S. Tong, "Distributed adaptive fuzzy event-triggered containment control of nonlinear strict-feedback systems," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3973–3983, Sep. 2020.

[21] J. Liu, Y. Zhang, Y. Yu, and C. Sun, "Fixed-time leader-follower consensus of networked nonlinear systems via event/self-triggered control," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 11, pp. 5029–5037, Nov. 2020

[22] J. Liu, Y. Yu, H. He, and C. Sun, "Team-triggered practical fixed-time consensus of double-integrator agents with uncertain disturbance," *IEEE Trans. Cybern.*, vol. 51, no. 6, pp. 3263–3272, Jun. 2021

[23] T. Hu, X. Liu, Z. He, X. Zhang, and S. Zhong, "Hybrid event-triggered and impulsive control strategy for multiagent systems with switching topologies," *IEEE Trans. Cybern.*, early access, Dec. 7, 2020, doi: 10.1109/TCYB.2020.3035713.

[24] J. Cao, D. Ding, J. Liu, E. Tian, S. Hu, and X. Xie, "Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks," *Inf. Sci.*, vol. 548, pp. 69–84, Feb. 2021.

[25] M. Li, Y. Chen, and Y. Liu, "Sliding-mode secure control for jump cyber-physical systems with malicious attacks," *J. Franklin Inst.*, vol. 358, no. 7, pp. 3424–3440, 2021.

[26] E. Mousavinejad, X. Ge, Q. Han, F. Yang, and L. Vlacic, "Resilient tracking control of networked control systems under cyber attacks," *IEEE Trans. Cybern.*, vol. 51, no. 4, pp. 2107–2119, Apr. 2021.

[27] P. S. P. Pessim, M. L. C. Peixoto, R. M. Palhares, and M. J. Lacerda, "Static output-feedback control for cyber-physical LPV systems under DoS attacks," *Inf. Sci.*, vol. 563, pp. 241–255, Jul. 2021.

[28] E. Tian and C. Peng, "Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4610–4618, Nov. 2020.

[29] J. Gao, Z. Zhao, J. Wang, T. Tan, and M. Ma, "Event-triggered output feedback control for discrete Markov jump systems under deception attack," *J. Franklin Inst.*, vol. 357, no. 11, pp. 6435–6452, 2020.

[30] X. Li, G. Wei, and L. Wang, "Distributed set-membership filtering for discrete-time systems subject to denial-of-service attacks and fading measurements: A zonotopic approach," *Inf. Sci.*, vol. 547, pp. 49–67, Feb. 2021.

[31] Y. Liu, Z. Li, and Z. Shen, "Resilient consensus of discrete-time connected vehicle systems with interaction network against cyber-attacks," *J. Franklin Inst.*, vol. 358, no. 5, pp. 2780–2800, 2021.

[32] Y. Qi, Y. Tang, Z. Ke, Y. Liu, X. Xu, and S. Yuan, "Dual-terminal decentralized event-triggered control for switched systems with cyber attacks and quantization," *ISA Trans.*, vol. 110, pp. 15–27, Apr. 2021.

[33] J. Liu, G. Ran, Y. Huang, C. Han, Y. Yu, and C. Sun, "Adaptive event-triggered finite-time dissipative filtering for interval type-2 fuzzy Markov jump systems with asynchronous modes," *IEEE Trans. Cybern.*, early access, Mar. 5, 2021, doi: 10.1109/TCYB.2021.3053627.

[34] J. Liu, Y. Wang, L. Zha, X. Xie, and E. Tian, "An event-triggered approach to security control for networked systems using hybrid attack model," *Int. J. Robust Nonlinear Control*, vol. 31, no. 12, pp. 5796–5812, 2021.

[35] Q. Li, Z. Wang, W. Sheng, F. E. Alsaadi, and F. E. Alsaadi, "Dynamic event-triggered mechanism for H_∞ non-fragile state estimation of complex networks under randomly occurring sensor saturations," *Inf. Sci.*, vol. 509, pp. 304–316, Jan. 2020.

[36] S. Hu, D. Yue, Z. Cheng, E. Tian, X. Xie, and X. Chen, "Co-design of dynamic event-triggered communication scheme and resilient observer-based control under aperiodic DoS attacks," *IEEE Trans. Cybern.*, vol. 51, no. 9, pp. 4591–4601, Sep. 2021.

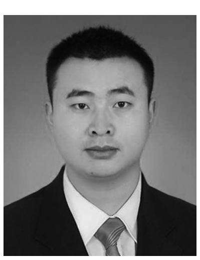
[37] X. Ge, Q.-L. Han, and Z. Wang, "A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks," *IEEE Trans. Cybern.*, vol. 49, no. 1, pp. 171–183, Jan. 2019.

Lijuan Zha received the Ph.D. degree from Donghua University, Shanghai, China, in 2018.

She is currently an Associate Professor with the Nanjing University of Finance and Economics, Nanjing, China, and a Postdoctoral Research Associate with the School of Mathematics, Southeast University, Nanjing, in 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, where she is currently pursuing the M.Sc. degree with the College of Information Engineering.

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, and a Visiting Professor with the College of Automation Electronic Engineering, Qingdao University of Science and Technology, Qingdao, China. His research interests include networked control systems, complex dynamical networks, and time-delay systems.

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.

Prof. Xie serves as an Associate Editor for the *International Journal of Fuzzy Systems* and *International Journal of Control, Automation, and Systems*.

Engang Tian received the B.S. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Postdoctoral Research Fellow with the Hong Kong Polytechnic University, Hong Kong. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2008 to 2018, he was an Associate Professor and then a Professor with the School of Electrical and Automation Engineering, Nanjing Normal University. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, and joined the University of Shanghai for Science and Technology, Shanghai, where he is currently a Professor with the School of Optical-Electrical and Computer Engineering. He has published more than 100 papers in refereed international journals. His research interests include networked control systems, cyber attack, as well as nonlinear stochastic control and filtering.

Jinde Cao (Fellow, IEEE) received the B.S. degree in mathematics/applied mathematics from Anhui Normal University, Wuhu, China, in 1986, the M.S. degree in mathematics/applied mathematics from Yunnan University, Kunming, China, in 1989, and the Ph.D. degree in mathematics/applied mathematics from Sichuan University, Chengdu, China, in 1998.

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. From 2001 to 2002, he was a Postdoctoral Research Fellow with the Chinese University of Hong Kong, Hong Kong.

Dr. 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 member of the Academy of Europe and European Academy of Sciences and Arts and a Fellow of Pakistan Academy of Sciences.