Information Sciences 612 (2022) 306–321

Contents lists available at ScienceDirect

Information Sciences

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

Event-based security tracking control for networked control systems against stochastic cyber-attacks

Jinliang Liu [a], Yanhui Dong [a], Lijuan Zha [a,*], Engang Tian [b], Xiangpeng Xie [c]

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

ARTICLE INFO

Article history:
Received 1 June 2022
Received in revised form 22 August 2022
Accepted 24 August 2022
Available online 30 August 2022

Keywords:
Dynamic event-triggered communication approach (DETCA)
stochastic cyber-attacks
networked control systems (NCSs)
security tracking control

ABSTRACT

This paper investigates the security tracking controller design for discrete-time networked control systems (NCSs) with stochastic cyber-attacks via dynamic event-triggered communication approach (DETCA). The DETCA is introduced to adjust the amount of data transmission in the network based on variation of the tracking error while keeping the tracking performance of the system. Stochastic cyber-attacks such as the denial-of-service and deception attacks are assumed to be encountered during the signal transmitted in the network. A sufficient condition to guarantee the asymptotical stability of the tracking error system is achieved with the Lyapunov stability theory. The tracking controller gain and the event-triggering parameter are co-designed by solving a linear matrix inequality. Finally, two simulation examples are given to verify the availability of theoretical results.

1. Introduction

Cyber-physical system(CPS) is known as an advanced generation system in which the physical processes, the computing, communication technologies are integrated, presenting high efficiency [1–3]. These systems have received extensive attention in the fields of power grids, civil infrastructure, autonomous vehicles, and sensor networks [4–7]. Even though the networked communications in such systems can highly improve the communication efficiency when the components in physical systems are interacting with each other, it also brings some research challenges. In particular, the application of open networked communication make the attackers accessible to gather information of the system measurement and the control input, which may corrupt the stability of the CPS and degrade the system performance, if the attackers block or modify the true data [8,9]. Therefore, it is of paramount importance to investigate the security of the CPS. The state estimation, filter design, consensus tracking issue of CPS have been addressed by some researchers, see [10–12] for example. In this article, the secure tracking control problem is focused for the CPS.

As is well known that the limited network bandwidth in CPSs may result in unexpected phenomenon such as data packet loss and network-induced time delay, which have negative impacts on system performance and should be paid much attention to. How to handle the limited network bandwidth issue has been a research frontier in recent years [13–17]. Many experts have devoted themselves to economizing scarce network bandwidth resources and put forward some effective

[*] Corresponding author.
E-mail address: zhalijuan@vip.163.com (L. Zha).

https://doi.org/10.1016/j.ins.2022.08.085
0020-0255/© 2022 Elsevier Inc. All rights reserved.

event-triggered mechanisms (ETMs) [18–21]. For example, the authors in [18] proposed adaptive event-triggered mechanism for NCSs, in which its threshold will be adjusted spontaneously as the environment changes. The output feedback controller was designed for switched linear systems with self-triggered mechanism in [19]. In [20], the authors designed a dynamic triggering scheme to devise a reliable controller for continuous-time nonlinear system. Nonetheless, aiming at the tracking control problem, there are few related studies on event-triggered control in which the triggering parameters can adjust automatically with tracking errors, which motivates this article.

Network security is another significant problem that should be taken into account in analysis and control for NCSs. Due to the openness of wireless networks, data transmission will inevitably be blocked or destroyed by DoS, deception and replay attacks sent by attackers [22–25]. As for DoS attacks, the assailants attempt to clog the transmission channels, resulting that data fail to reach the controller at particular instants [26]. When deception attacks happen, the current transmitted data is replaced by the attackers with wrong packets [27,28]. Under the replay attacks, the attacker deceives the system by replacing real data with previous data in network. There have been many achievements about cyber-attacks, for example, Wang *et al.* [29] studied the event-based controller for CPSs with periodic DoS jamming attacks. To defend against DoS attacks, the authors proposed a design state feedback control method for NCSs in [30]. In [31], considering deception attacks, the distributed filter design problem for discrete-time systems were addressed. An adaptive controller was proposed in [32] for a set of nonlinear systems with replay attacks. Although some preliminary achievements have been made on secure tracking control of NCSs, most of the available results only take one type of cyber-attacks into consideration [33–37]. However, the attackers may launch stochastic cyber-attacks to realize their attacking purposes, it is practical to discuss the event-based tracking control problem for NCSs under stochastic cyber-attacks. This is another motivation of this paper.

Enlightened by the above discussions, the security tracking control issue is investigated for discrete-time NCSs with stochastic heterogeneous cyber-attacks in this study. The primary works of the paper are summarized below:

1) Considering the impact of DoS and deception attacks, a DETCA is introduced to reduce the networked transmission burden based on variation of the tracking error, which is not considered in the vast majority of tracking control literatures.
2) A novel dynamic event-based tracking error model is established for discrete-time NCSs, which is firstly taken both the stochastic cyber-attacks and DETCA into a unified framework.
3) A sufficient condition for the asymptotic stability of the tracking error model is acquired. Meanwhile, the precise expression of the tracking controller gain is acquired with solving the linear matrix inequality (LMI).

The rest of this work is arranged as follows. The model description of each module and a tracking error model are founded in Section 2. The main results are shown in Section 3 based on stochastic cyber-attacks and DETCA. Section 4 gives two simulation examples and various cases analysis. Section 5 concludes the research work of the paper.

Notations: $\mathbb{R}^n$ is the n-dimensional vector space; X^T and X^{-1} represent transpose and inverse of matrix X respectively; $X > 0$ denotes the matrix is positive definite and $X < 0$ shows negative definiteness, similarly; I_n is the identity matrix. $\Pr\{z\}$ is the occurrence probability of event z. $E\{\cdot\}$ represents expectation of $\cdot$. $*$ indicates the corresponding symmetric term in symmetric matrices. $\mathrm{diag}\{\cdots\}$ expresses a block-diagonal matrix.

2. Problem formulation

The framework of security tracking control for the NCS based on the DETCA is placed in Fig. 1. The sensor is connected with the controller via an unprotected network. The aim of this article is to propose a secure tracking controller to ensure the tracking performance of the system under DETCA and stochastic cyber-attacks.

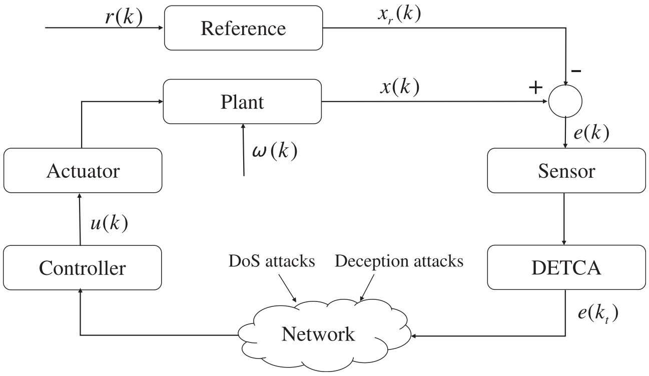

Fig. 1. Structure of the NCS with DETCA and stochastic cyber-attacks.

Consider the discrete-time NCS

$$x(k+1) = Ax(k) + Bu(k) + D\omega(k) \tag{1}$$

where $x(k) \in \mathbb{R}^n$ denotes the system state; $u(k) \in \mathbb{R}^q$ indicates the control input vector; $\omega(k)$ is the external disturbance; A, B and D are known system matrices.

The reference model is considered as below

$$x_r(k+1) = A_r x_r(k) + B_r r(k) \tag{2}$$

where $x_r(k) \in \mathbb{R}^m$ is the state vector of the reference model and $r(k) \in \mathbb{R}^p$ is the bounded reference input. A_r and B_r are constant matrices with suitable dimensions.

Inspired by [18], a DETCA is introduced to overcome the problem of resource constraints in this paper, as shown in Fig. 1. The packets with little change being considered as ”unnecessary” data will be discarded by DETCA, and the remaining “necessary” sampling packets can arrive at the controller, which should meet the following triggering condition

$$\frac{1}{\theta}\epsilon(k) + \sigma e^T(k)e(k) - \eta_e^T(k)\eta_e(k) \leqslant 0 \tag{3}$$

where $\eta_e(k) = e(k) - e(k_t), e(k_t)$ is the sampled data at the latest transmitted instant, $e(k)$ is the tracking error which will be given later; θ and σ are known positive scalars; and the positive time-dependent threshold function $\epsilon(k)$ is defined as

$$\epsilon(k+1) = \lambda\epsilon(k) + \sigma e^T(k)e(k) - \eta_e^T(k)\eta_e(k) \tag{4}$$

with $\lambda \in (0, 1)$ is a given constant.

Remark 1. In this paper, the DETCA in (3) is motivated by some existing results (see [15,19] for example). However, the DETCA in (3) is different from the existing ones in some aspects. Particularly, in [15], the threshold can be adjusted on the basis of measurement output. Whereas, the tracking error has a significant impact on the dynamic adjustment threshold. It is observed that the DETCA in [19] is designed for continuous NCSs, in this paper, the DETCA is introduced for discrete-time NCSs. There are no available results to solve the tracking control problem for NCSs with stochastic attacks and DETCA, which motivates the current study.

The opening character of the communication network brings risks to the NCSs undergoing DoS and deception attacks. In order to make the NCSs tolerable to stochastic cyber-attacks, a resilient controller will be devised in the following.

If the communication network suffers deception attacks, the actual signal reach the controller is expressed as follows

$$\tilde{e}(k) = \beta_d(k)e(k_t) + (1 - \beta_d(k))h(e(k_t)) \tag{5}$$

where the nonlinear deception attacks function $h(e(k_t))$ satisfies

$$h^T(e(k_t))h(e(k_t)) \leqslant e^T(k_t)G^T Ge(k_t) \tag{6}$$

and G is a known constant matrix.

In addition, consider the scenario that communication channel is jammed by DoS attacks, the practical controller input $\vec{e}(k)$ is denoted as

$$\vec{e}(k) = \alpha_d(k)\tilde{e}(k) = \alpha_d(k)[\beta_d(k)e(k_t) + (1 - \beta_d(k))h(e(k_t))] \tag{7}$$

In (5) and (7), the stochastic variables $\alpha_d(k)$ and $\beta_d(k)$ are assumed to be mutually independent and obey the Bernoulli distribution. At the same time, the range of values in $\{0, 1\}$ and the corresponding probabilities are

$$\begin{aligned} Pr\{\alpha_d(k) = 1\} = &\ \bar{\alpha}_d, Pr\{\alpha_d(k) = 0\} = 1 - \bar{\alpha}_d \\ Pr\{\beta_d(k) = 1\} = &\ \bar{\beta}_d, Pr\{\beta_d(k) = 0\} = 1 - \bar{\beta}_d \end{aligned} \tag{8}$$

with $0 \leqslant \bar{\alpha}_d \leq 1, 0 \leqslant \bar{\beta}_d \leq 1$.

Remark 2. It is noticed that, the model (7) describes the practical controller input that affected by randomly appearing DoS and deception attacks, which occur or not are described by the variable $\alpha_d(k)$ and $\beta_d(k)$ respectively. Specifically, $\alpha_d(k)\beta_d(k) = 1$ represents an ideal transmission channel from sensor to controller, $\alpha_d(k) = 0$ and $\beta_d(k) = 1$ stands for the network which under DoS attacks, $\alpha_d(k) = 1$ and $\beta_d(k) = 0$ indicates the channel which is under the deception attacks.

Remark 3. In fact, the type and sequence of attacks are unpredictable, but the information of the attacks can be detected by some attack detection mechanisms, see [38,39] for example. In this work, it is assumed that deception attacks happen firstly, and the DoS attacks happen later. If the sequence of the two cyber-attacks is reversed, the analysis and control method is similar to this paper.

Hence, considering effect of the stochastic cyber-attacks, the following control method is proposed

$$u(k) = K\vec{e}(k) = \alpha_d(k)[\beta_d(k)K(e(k) - \eta_e(k)) + (1 - \beta_d(k))Kh(e(k) - \eta_e(k))]. \tag{9}$$

For easing description, $h(e(k) - \eta_e(k))$ is written as $\bar{h}(k)$ in the rest of the article.

Taking (9) into (1), we can obtain

$$x(k+1) = Ax(k) + \alpha_d(k)\beta_d(k)BK(e(k) - \eta_e(k)) + \alpha_d(k)(1 - \beta_d(k))BK\bar{h}(k) + D\omega(k) \tag{10}$$

Define the tracking error $e(k) \triangleq x(k) - x_r(k)$, from (1) (2) (10), it can be obtained that

$$\begin{aligned} e(k+1) = \; & Ax(k) + \alpha_d(k)\beta_d(k)BK(e(k) - \eta_e(k)) - A_r x_r(k) + D\omega(k) - B_r r(k) \\ & + \alpha_d(k)(1 - \beta_d(k))BK\bar{h}(k) \\ = \; & (A + \bar{\alpha}_d\bar{\beta}_d BK)e(k) - \bar{\alpha}_d\bar{\beta}_d BK\eta_e(k) + V_{e(k)} + \bar{\alpha}_d(1 - \bar{\beta}_d)BK\bar{h}(k) \\ & + (\alpha_d(k)\beta_d(k) - \bar{\alpha}_d\bar{\beta}_d)BKe(k) - (\alpha_d(k)\beta_d(k) - \bar{\alpha}_d\bar{\beta}_d)BK\eta_e(k) + (\alpha_d(k) - \bar{\alpha}_d)BK\bar{h}(k) \\ & - (\alpha_d(k)\beta_d(k) - \bar{\alpha}_d\bar{\beta}_d)BK\bar{h}(k) \end{aligned} \tag{11}$$

where $V_{e(k)} = (A - A_r)x_r(k) + D\omega(k) - B_r r(k)$.

Remark 4. In recent years, the tracking control issues have been researched owing to their wide range of applications [40–42]. Inspired by the above literature, the tracking control issue considering networked security and resource constraints is discussed in this paper. The purpose of the paper is to propose a tracking controller to make the error system (11) possesses asymptotic stability with the condition of tracking performance (12).

The following Definition, Lemma and Assumptions are needed to carry out the subsequent analysis.

Definition 1. ([43]) The tracking error system (11) has tracking performance under the DETCA and stochastic cyber-attacks if

$$E\left\{\sum_{k=0}^{\infty} e^T(k)e(k)\right\} < \gamma^2 E\left\{\sum_{k=0}^{\infty} V_{e(k)}^T V_{e(k)}\right\} \tag{12}$$

where $\gamma > 0$ denotes tracking performance level and k is finite.

Lemma 1. ([44]) *For given positive-definite matrices P, R and any positive scalar $\delta > 0$, the following inequality holds*

$$-PR^{-1}P \leqslant \delta^2 R - 2\delta P$$

Assumption 1. ([45]) The completely loss of transmission signal will happen if the communication channel is under DoS attacks.

Assumption 2. ([45]) The deception attacks have the ability to know and randomly modify the exact value of the controller input in real time.

3. Main results

By using Lyapunov–Krasovskii functional approach, sufficient condition will be given in Theorem 1, guaranteeing the asymptotic stability of tracking error system (11) and satisfy the tracking performance (12). The controller gain will be derived in Theorem 2.

Theorem 1. *For given scalars $\lambda, \bar{\alpha}_d, \bar{\beta}_d, \gamma, \delta, \theta, \sigma$ and matrix K, the error system (11) is asymptotically stable under the condition of tracking performance (12) if there exists a symmetric matrix $P > 0$, such that the following inequality holds*

$$\Omega = \begin{bmatrix} \Xi_{11} & * & * & * & * \\ \Xi_{21} & -P & * & * & * \\ \Xi_{31} & 0 & -P & * & * \\ \Xi_{41} & 0 & 0 & -P & * \\ \Xi_{51} & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{13}$$

where

$$
\begin{aligned}
\Xi_{11} &= \begin{bmatrix} -P-\sigma aI+I & * & * & * \\ 0 & aI & * & * \\ 0 & 0 & -\gamma^2 I & * \\ 0 & 0 & 0 & -I \end{bmatrix}, \\
\Xi_{21} &= \begin{bmatrix} PA+\bar{\alpha}_d\bar{\beta}_d PBK & -\bar{\alpha}_d\bar{\beta}_d PBK & P & \bar{\alpha}_d(1-\bar{\beta}_d)PBK \end{bmatrix}, \\
\Xi_{31} &= \begin{bmatrix} \bar{\mu}PBK & -\bar{\mu}PBK & 0 & -\bar{\mu}PBK \end{bmatrix}, \\
\Xi_{41} &= \begin{bmatrix} \bar{\phi}\sqrt{\bar{\beta}_d}PBK & -\bar{\phi}\sqrt{\bar{\beta}_d}PBK & 0 & \bar{\phi}(\sqrt{1-\bar{\beta}_d})PBK \end{bmatrix}, \\
\Xi_{51} &= \begin{bmatrix} G & -G & 0 & 0 \end{bmatrix}
\end{aligned}
$$

with $\bar{\mu} = \bar{\alpha}_d\sqrt{\bar{\beta}_d(1-\bar{\beta}_d)}, \bar{\phi} = \sqrt{\bar{\alpha}_d(1-\bar{\alpha}_d)}, a = \lambda - 1 - \frac{1}{\theta}$

Proof. The Lyapunov–Krasovskii functional for system (11) is constructed as follows

$$
\mathrm{V}(k) = e^T(k)Pe(k) + \frac{1}{\theta}\epsilon(k) \tag{14}
$$

Let $\triangle\mathrm{V}(k) = \mathrm{V}(k+1) - \mathrm{V}(k)$, it is calculated that

$$
\begin{aligned}
E\{\triangle\mathrm{V}(k)\} &= E\{\mathrm{V}(k+1) - \mathrm{V}(k)\} \\
&= E\{e^T(k+1)Pe(k+1) - e^T(k)Pe(k) + \tfrac{1}{\theta}[\epsilon(k+1) - \epsilon(k)]\}
\end{aligned} \tag{15}
$$

Notice that $E\left\{[\alpha_d(k)\beta_d(k) - \bar{\alpha}_d\bar{\beta}_d]^2\right\} = \bar{\alpha}_d\bar{\beta}_d(1-\bar{\alpha}_d\bar{\beta}_d), E\{[\alpha_d(k) - \bar{\alpha}_d][\alpha_d(k)\beta_d(k) - \bar{\alpha}_d\bar{\beta}_d]\} = \bar{\alpha}_d\bar{\beta}_d(1-\bar{\alpha}_d)$ and $E\left\{[\alpha_d(k) - \bar{\alpha}_d]^2\right\} = \bar{\alpha}_d(1-\bar{\alpha}_d)$, the following can be obtained

$$
\begin{aligned}
E\{e^T(k+1)Pe(k+1)\} &= E\{\mathscr{A}^T P\mathscr{A}\} + E\left\{(\alpha_d(k)\beta_d(k) - \bar{\alpha}_d\bar{\beta}_d)^2\mathscr{B}^T P\mathscr{B}\right\} + E\left\{(\alpha_d(k) - \bar{\alpha}_d)^2\mathscr{C}^T P\mathscr{C}\right\} \\
&\quad +2E\{(\alpha_d(k) - \bar{\alpha}_d)(\alpha_d(k)\beta_d(k) - \bar{\alpha}_d\bar{\beta}_d)\mathscr{B}^T P\mathscr{C}\} \\
&\leqslant E\{\mathscr{A}^T P\mathscr{A}\} + \bar{\alpha}_d(1-\bar{\alpha}_d)(\sqrt{\bar{\beta}_d}\mathscr{B} + \mathscr{C})^T P(\sqrt{\bar{\beta}_d}\mathscr{B} + \mathscr{C}) + \bar{\alpha}_d{}^2\bar{\beta}_d(1-\bar{\beta}_d)\mathscr{B}^T P\mathscr{B}
\end{aligned} \tag{16}
$$

where $\mathscr{A} = (A + \bar{\alpha}_d\bar{\beta}_d BK)e(k) - \bar{\alpha}_d\bar{\beta}_d BK\eta_e(k) + V_{e(k)} + \bar{\alpha}_d(1-\bar{\beta}_d)BK\bar{h}(k)$, $\mathscr{B} = BK(e(k) - \eta_e(k) - \bar{h}(k))$ and $\mathscr{C} = BK\bar{h}(k)$.

Recalling the event-triggered condition (3), it can be represented as

$$
\frac{1}{\theta}\epsilon(k) \leqslant \eta_e(k)^T\eta_e(k) - \sigma e(k)^T e(k) \tag{17}
$$

Obviously, combining (4) and (17), we can get

$$
\begin{aligned}
E\{\tfrac{1}{\theta}[\epsilon(k+1) - \epsilon(k)]\} &= E\{\tfrac{1}{\theta}[\lambda\epsilon(k) + \sigma e^T(k)e(k) - \eta_e^T(k)\eta_e(k) - \epsilon(k)]\} \\
&= \tfrac{1}{\theta}[(\lambda-1)\epsilon(k) + \sigma e^T(k)e(k) - \eta_e^T(k)\eta_e(k)] \\
&\leqslant (\lambda - 1 - \tfrac{1}{\theta})\eta_e^T(k)\eta_e(k) - \sigma(\lambda - 1 - \tfrac{1}{\theta})e^T(k)e(k)
\end{aligned} \tag{18}
$$

Based on inequality (6), it is clear that

$$
\bar{h}^T(k)\bar{h}(k) \leqslant (e(k) - \eta_e(k))^T G^T G(e(k) - \eta_e(k)) \tag{19}
$$

Combining (16), (18) and (19), the expression of $E\{\triangle V(k)\}$ is

$$
\begin{aligned}
E\{\triangle\mathrm{V}(k)\} \leqslant\ & E\{\mathscr{A}^T P\mathscr{A}\} + \bar{\alpha}_d{}^2\bar{\beta}_d(1-\bar{\beta}_d)\mathscr{B}^T P\mathscr{B} + \bar{\alpha}_d(1-\bar{\alpha}_d)(\sqrt{\bar{\beta}_d}\mathscr{B} + \mathscr{C})^T P(\sqrt{\bar{\beta}_d}\mathscr{B} + \mathscr{C}) \\
& -e^T(k)Pe(k) - \sigma(\lambda - 1 - \tfrac{1}{\theta})e^T(k)e(k) + (\lambda - 1 - \tfrac{1}{\theta})\eta_e^T(k)\eta_e(k) \\
& +(e(k) - \eta_e(k))^T G^T G(e(k) - \eta_e(k)) - \bar{h}^T(k)\bar{h}(k)
\end{aligned} \tag{20}
$$

One can easily deduce that (20) is equal to (21)

$$
E\left\{\triangle\mathrm{V}(k) + e^T(k)e(k) - \gamma^2 V_{e(k)}^T V_{e(k)}\right\} \leqslant E\{\vartheta^T(k)\Psi\vartheta(k)\} \tag{21}
$$

where $\vartheta(k) = [e^T(k) \quad \eta_e^T(k) \quad V_{e(k)}^T \quad h^T(e(k) - \eta_e(k))]^T$ and $\Psi = \Xi_{11} + \Xi_{21}^T P^{-1}\Xi_{21} + \Xi_{31}^T P^{-1}\Xi_{31} + \Xi_{41}^T P^{-1}\Xi_{41} + \Xi_{51}^T\Xi_{51}$.

According to Schur complement, $E\left\{\triangle\mathrm{V}(k) + e^T(k)e(k) - \gamma^2 V_{e(k)}^T V_{e(k)}\right\} \leqslant 0$ can be ensured by (13). Based on the zero initial condition and analysis, it is derived that

$$\begin{aligned}\sum_{k=0}^{\infty}E\{e^T(k)e(k)\} &< \gamma^2\sum_{k=0}^{\infty}E\left\{V_{e(k)}^TV_{e(k)}\right\}-\sum_{k=0}^{\infty}E\{\triangle\mathrm{V}(k)\}\\ &=\gamma^2\sum_{k=0}^{\infty}E\left\{V_{e(k)}^TV_{e(k)}\right\}-\{E\{\mathrm{V}(\infty)\}-E\{\mathrm{V}(0)\}\}\\ &=\gamma^2\sum_{k=0}^{\infty}E\left\{V_{e(k)}^TV_{e(k)}\right\}-E\{\mathrm{V}(\infty)\}\\ &<\gamma^2\sum_{k=0}^{\infty}E\left\{V_{e(k)}^TV_{e(k)}\right\}\end{aligned} \tag{22}$$

which implies the H_∞ tracking performance (12) is guaranteed. This completes the proof. ■

Based on Theorem 1, the tracking controller design method shall be proposed in Theorem 2.

Theorem 2. *For given $\lambda,\bar{\alpha}_d,\bar{\beta}_d,\gamma,\delta,\theta$ and σ , the error system (11) with controller in (9) is asymptotically stable under the condition of tracking performance (12), if there exist matrices $X>0$and Y such that the following LMI holds*

$$\bar{\Omega}=\begin{bmatrix}\bar{\Xi}_{11} & * & * & * & *\\ \bar{\Xi}_{21} & -X & * & * & *\\ \bar{\Xi}_{31} & 0 & -X & * & *\\ \bar{\Xi}_{41} & 0 & 0 & -X & *\\ \bar{\Xi}_{51} & 0 & 0 & 0 & -I\end{bmatrix}<0 \tag{23}$$

where

$$\bar{\Xi}_{11}=\begin{bmatrix}-X+(\sigma a-1)(-2\delta X+\delta^2I) & * & * & *\\ 0 & -a(-2\delta X+\delta^2I) & * & *\\ 0 & 0 & -\gamma^2I & *\\ 0 & 0 & 0 & -2\delta X+\delta^2I\end{bmatrix},$$

$$\bar{\Xi}_{21}=\begin{bmatrix}AX+\bar{\alpha}_d\bar{\beta}_dBY & -\bar{\alpha}_d\bar{\beta}_dBY & I & \bar{\alpha}_d(1-\bar{\beta}_d)BY\end{bmatrix},$$

$$\bar{\Xi}_{31}=[\,\bar{\mu}BY \quad -\bar{\mu}BY \quad 0 \quad -\bar{\mu}BY\,],$$

$$\bar{\Xi}_{41}=\left[\bar{\phi}\sqrt{\bar{\beta}}BY \quad -\bar{\phi}\sqrt{\bar{\beta}_d}BY \quad 0 \quad \bar{\phi}(\sqrt{1-\bar{\beta}_d})BY\right],$$

$$\bar{\Xi}_{51}=[\,GX \quad -GX \quad 0 \quad 0\,]$$

with $\bar{\mu}=\bar{\alpha}_d\sqrt{\bar{\beta}_d(1-\bar{\beta}_d)},\bar{\phi}=\sqrt{\bar{\alpha}_d(1-\bar{\alpha}_d)},a=\lambda-1-\frac{1}{\theta}.$

Moreover, tracking controller gain is determined as

$$K=YX^{-1} \tag{24}$$

Proof. Let $X=P^{-1},\Sigma=diag\{X,X,I,X,X,X,X,I\}$. Then pre- and post-multipling Ω in (13) by Σ and Σ^T, one can get

$$\tilde{\Omega}=\begin{bmatrix}\tilde{\Xi}_{11} & * & * & * & *\\ \bar{\Xi}_{21} & -X & * & * & *\\ \bar{\Xi}_{31} & 0 & -X & * & *\\ \bar{\Xi}_{41} & 0 & 0 & -X & *\\ \bar{\Xi}_{51} & 0 & 0 & 0 & -I\end{bmatrix}<0 \tag{25}$$

where

$$\tilde{\Xi}_{11}=\begin{bmatrix}-X-(\sigma a-1)XX & * & * & *\\ 0 & aXX & * & *\\ 0 & 0 & -\gamma^2I & *\\ 0 & 0 & 0 & -XX\end{bmatrix}$$

According to Lemma 1, the following inequality can be obtained

$$-XX\leqslant-2\delta X+\delta^2I \tag{26}$$

Define $Y = KX$, replace the items $-XX$ in (25) with $-2\delta X + \delta^2 I$ [44], (23) can ensure (13) holds. Then, the controller gain K is calculated as (24). This completes the proof. ■

In Theorem 1 and Theorem 2, the security tracking control issue for discrete-time NCSs has been investigated under stochastic cyber-attacks. However, the same kind of attacks also exist in the actual systems, which can be handled by the same way in this paper.

If $\alpha_d(k) \equiv 1$, which means the tracking error system (11) is only subject to deception attacks, then the tracking error system is expressed as

$$\begin{aligned} e(k+1) &= Ax(k) + \beta_d(k)BK(e(k) - \eta_e(k)) - A_r x_r(k) + D\omega(k) - B_r r(k) \\ &\quad + (1 - \beta_d(k))BK\bar{h}(k) \\ &= (A + \bar{\beta}_d BK)e(k) - \bar{\beta}_d BK\eta_e(k) + V_{e(k)} + (1 - \bar{\beta}_d)BK\bar{h}(k) \\ &\quad + (\beta_d(k) - \bar{\beta}_d)BKe(k) - (\beta_d(k) - \bar{\beta}_d)BK\eta_e(k) - (\beta_d(k) - \bar{\beta}_d)BK\bar{h}(k) \\ &= \mathscr{A} + (\beta_d(k) - \bar{\beta}_d)\mathscr{B} \end{aligned} \tag{27}$$

where $V_{e(k)} = (A - A_r)x_r(k) + D\omega(k) - B_r r(k), \mathscr{A} = (A + \bar{\beta}_d BK)e(k) - \bar{\beta}_d BK\eta_e(k) + V_{e(k)} + (1 - \bar{\beta}_d)BK\bar{h}(k)$ and $\mathscr{B} = BK(e(k) - \eta_e(k) - \bar{h}(k))$.

On the other hand, if $\beta_d(k) \equiv 1$, which means only DoS attacks occur, the tracking error system (11) can be represented as

$$\begin{aligned} e(k+1) &= Ax(k) + \alpha_d(k)BK(e(k) - \eta_e(k)) - A_r x_r(k) + D\omega(k) - B_r r(k) \\ &= (A + \bar{\alpha}_d BK)e(k) - \bar{\alpha}_d BK\eta_e(k) + V_{e(k)} + (\alpha_d(k) - \bar{\alpha}_d)BKe(k) - (\alpha_d(k) - \bar{\alpha}_d)BK\eta_e(k) \\ &= \mathscr{A} + (\alpha_d(k) - \bar{\alpha}_d)\mathscr{B} \end{aligned} \tag{28}$$

where $V_{e(k)} = (A - A_r)x_r(k) + D\omega(k) - B_r r(k), \mathscr{A} = (A + \bar{\alpha}_d BK)e(k) - \bar{\alpha}_d BK\eta_e(k) + V_{e(k)}$ and $\mathscr{B} = BK(e(k) - \eta_e(k))$.

The following Corollary 1 and Corollary 2 can be derived by using the same method as the Theorem 2 respectively.

Corollary 1. For given $\lambda, \bar{\alpha}_d, \bar{\beta}_d, \gamma, \delta, \theta$ and σ, the error system (27) is asymptotically stable under the condition of tracking performance (12) if there are matrices $X > 0$ and Y such that

$$\hat{\Omega} = \begin{bmatrix} \hat{\Xi}_{11} & * & * & * \\ \hat{\Xi}_{21} & -X & * & * \\ \hat{\Xi}_{31} & 0 & -X & * \\ \hat{\Xi}_{41} & 0 & 0 & -I \end{bmatrix} < 0 \tag{29}$$

where

$$\begin{aligned} \hat{\Xi}_{11} &= \begin{bmatrix} -X + (\sigma a - 1)(-2\delta X + \delta^2 I) & * & * & * \\ 0 & -a(-2\delta X + \delta^2 I) & * & * \\ 0 & 0 & -\gamma^2 I & * \\ 0 & 0 & 0 & -2\delta X + \delta^2 I \end{bmatrix}, \\ \hat{\Xi}_{21} &= \begin{bmatrix} AX + \bar{\beta}_d BY & -\bar{\beta}_d BY & I & (1 - \bar{\beta}_d)BY \end{bmatrix}, \\ \hat{\Xi}_{31} &= [\, \bar{\varphi} BY \quad -\bar{\varphi} BY \quad 0 \quad -\bar{\varphi} BY \,], \\ \hat{\Xi}_{41} &= [\, GX \quad -GX \quad 0 \quad 0 \,] \end{aligned}$$

with $\bar{\varphi} = \sqrt{\bar{\beta}_d(1 - \bar{\beta}_d)}, a = \lambda - 1 - \frac{1}{\theta}$. ■

In this case, the tracking controller gain can be computed by $K = YX^{-1}$.

Corollary 2. For given scalars $\lambda, \bar{\alpha}_d, \bar{\beta}_d, \gamma, \delta, \theta$ and σ. The error system (28) is asymptotically stable under the condition of tracking performance (12) if there exist matrices $X > 0$ and Y, such that

$$\vec{\Omega} = \begin{bmatrix} \vec{\Xi}_{11} & * & * \\ \vec{\Xi}_{21} & -X & * \\ \vec{\Xi}_{31} & 0 & -X \end{bmatrix} < 0 \tag{30}$$

where

$$\vec{\Xi}_{11} = \begin{bmatrix} -X + (\sigma a - 1)(-2\delta X + \delta^2 I) & * & * \\ 0 & -a(-2\delta X + \delta^2 I) & * \\ 0 & 0 & -\gamma^2 I \end{bmatrix},$$

$$\vec{\Xi}_{21} = [AX + \bar{\alpha}_d BY \quad -\bar{\alpha}_d BY \quad I],$$

$$\vec{\Xi}_{31} = [\,\bar{\phi}BY \quad -\bar{\phi}BY \quad 0\,]$$

with $\bar{\phi} = \sqrt{\bar{\alpha}_d(1-\bar{\alpha}_d)}, a = \lambda - 1 - \frac{1}{\theta}$.■

In this case, the tracking controller gain can be obtained through $K = YX^{-1}$.

4. Numerical examples

In what following, two examples will be taken to verify the feasibility and usefulness of the presented theoretical results.

Example 1. . An F-404 aircraft engine system is taken as a simulation example to verify the proposed secure tracking control method. As discussed in [46–48], the matrix parameters of F-404 aircraft engine system is

$$A = \begin{bmatrix} 1.4600 & 0 & 2.4280 \\ 0.1643 & -0.4000 & -0.3788 \\ 0.3107 & 0 & -2.2300 \end{bmatrix}$$

By setting the sampling period as 1 s, the discretized nominal system matrices in (1) are shown as follows

$$A = \begin{bmatrix} 0.4529 & -0.1000 & 1.3951 \\ -0.1570 & -0.5000 & 0.3603 \\ -0.5800 & 0.0899 & -1.0975 \end{bmatrix}, B = \begin{bmatrix} -2 \\ 1 \\ 0 \end{bmatrix}, D = \begin{bmatrix} 0.3 & 0.2 & 0 \\ 0.4 & 0.5 & 0 \\ 0.1 & 0 & 1 \end{bmatrix}$$

The reference model (2) is expressed as

$$x_r(k+1) = \begin{bmatrix} -0.1 & 0.2 & 0 \\ 0 & -0.24 & 0 \\ 0 & 0 & -0.2 \end{bmatrix} x_r(k) + \begin{bmatrix} -0.45 & 0 & 0 \\ 0 & 0.4 & 0 \\ 0 & 0 & 0.5 \end{bmatrix} r(k)$$

where the bounded reference input $r(k)$ is chosen as

$$r(k) = \begin{bmatrix} -1.6\sin(0.75 - 0.4k) \\ -1.1\sin(0.65 - 0.4k) \\ -0.8\sin(0.25 - 0.4k) \end{bmatrix}$$

The initial values are $x(0) = [-0.9\ 0.6\ 0.8]^T, x_r(0) = [0.2\ \ -0.1\ 0.3]^T$. The deception attacks is $h(e(k_t)) = 0.1\sin(-0.4e(k_t))$, which can satisfy the condition of (6), where $G = diag\{0.05, 0.1, 0.15\}$. Suppose that the disturbance $\omega(k) = [-0.5\sin(0.4k)\ 1.5\sin(0.4 - 0.4k)\ \ -0.8\sin(0.5 - 0.4k)]^T$.

The occurence probability of cyber-attacks are set as $\bar{\alpha}_d = 0.85, \bar{\beta}_d = 0.9$ and the H_∞ tracking performance index $\gamma = 2.09$. For given $\sigma = 0.7, \theta = 2, \lambda = 0.9, \delta = 0.1$, from the LMI (23), we can obtain the following parameters

$$Y = [0.0141 \quad 0.0277 \quad -0.0472], X = \begin{bmatrix} 2.8032 & 0.3025 & -1.4048 \\ 0.3025 & 2.1457 & 0.3402 \\ -1.4048 & 0.3402 & 1.2847 \end{bmatrix}$$

the controller gain is derived from (24)

$$K = [-0.0485 \quad 0.0355 \quad -0.0992]$$

With the tracking performance index γ, one can see from Fig. 2 that the state vector $x(k)$ is well tracked on the reference model $x_r(k)$. To further illustrate the effectiveness of the proposed method, the response trajectory of tracking error $e(k)$ is shown in Fig. 3, which converge to a very small region around zero. Fig. 4 carries out the response of control input $u(k)$ under random cyber-attacks. Fig. 5 depicts the event-triggering instants and intervals, it is easy to see that the sampling releasing instants decrease drastically after 5 times.

Example 2. . Consider the system (1) with parameters given as

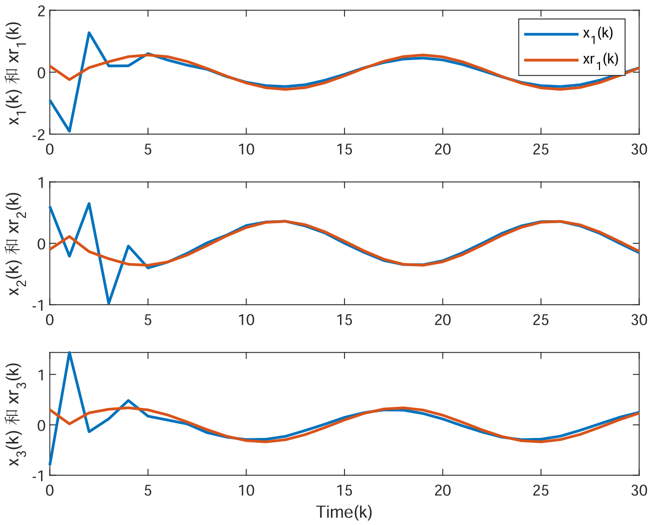

Fig. 2. State responses in Example 1.

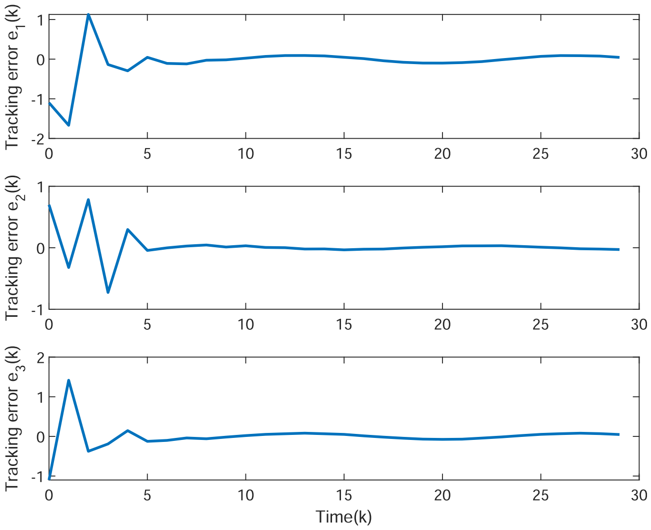

Fig. 3. Tracking error $e(k)$ in Example 1.

$$A = \begin{bmatrix} -0.1 & 0.1 \\ 0.2 & -0.12 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, D = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and the parameters of reference model (2) is selected as

$$A_r = \begin{bmatrix} -0.8 & 0 \\ 0 & -0.8 \end{bmatrix}, D_r = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Set the bounded reference input

$$r(k) = \begin{bmatrix} -1.8\sin(0.25 - 0.4k) \\ -1.8\sin(0.65 - 0.4k) \end{bmatrix}$$

and the relevant parameters σ, θ, λ and γ are the same as the Example 1. The deception attacks is chosen to be $h(e(k_t)) = 0.1\sin(-0.4e(k_t))$, where $G = diag\{-0.1, 0.5\}$.

Next, the validity of the results obtained will be illustrated with three related cases.

Case 1. Given the occurence probability of cyber-attacks are $\bar{\alpha}_d = 0.85, \bar{\beta}_d = 0.9$ and $\gamma = 2.00$.

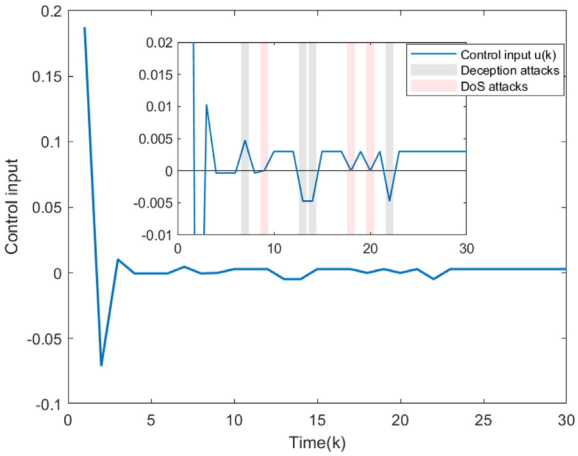

Fig. 4. Control input $u(k)$ under stochastic cyber-attacks in Example 1.

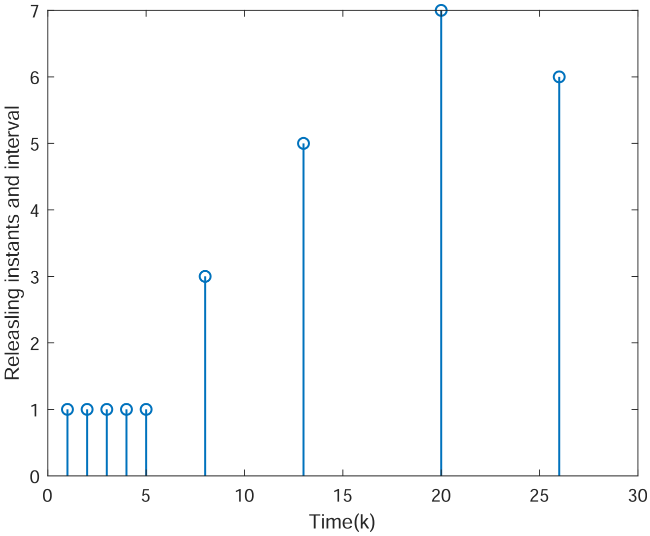

Fig. 5. The releasing instants and the releasing intervals under DETCA in Example 1.

The following parameters can be obtained by solving the LMI (23) in Theorem 2

$$Y = [-0.0305 \quad 0.0051], X = \begin{bmatrix} 0.9769 & -0.0041 \\ -0.0041 & 0.3093 \end{bmatrix}$$

According to (24), the controller gain is derived as

$$K = [-0.0312 \quad 0.0160]$$

Simulation results of are given in Fig. 6 - Fig. 9. The state vector $x(k)$ and the tracking signal $x_r(k)$ are shown in Fig. 6, which implies that the tracking signal is basically the same as the state response trajectory after twenty seconds. Fig. 7 displays the tracking error $e(k)$ approaches zero gradually. Fig. 8 shows the response of control input $u(k)$ under random cyber-attacks. Fig. 9 indicates the releasing instants and intervals under DETCA.

Case 2. In this case, let $\alpha_d(k) = 1, \bar{\beta}_d = 0.9$ and $\gamma = 1.81$, which means that only deception attacks occur.

The following matrices can be obtained by Corollary 1

$$Y = [-0.0096 \quad 0.0052], X = \begin{bmatrix} 0.3843 & -0.0111 \\ -0.0111 & 0.3300 \end{bmatrix}$$

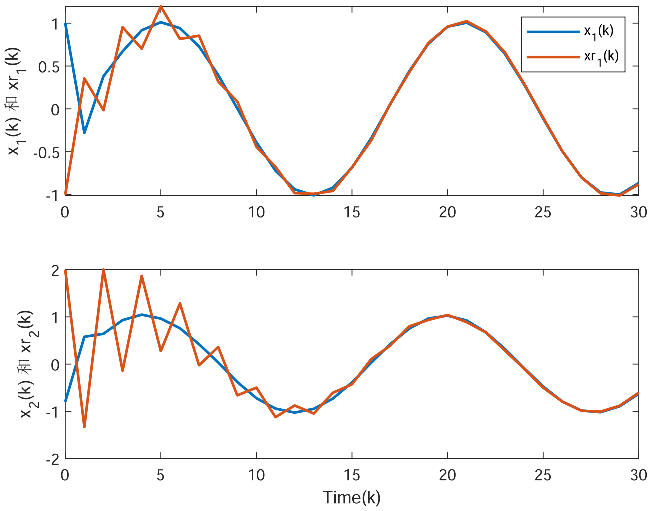

Fig. 6. State responses in Case 1.

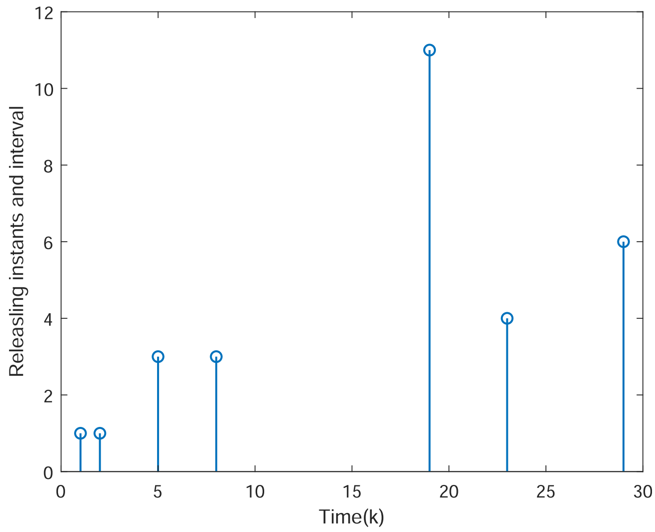

Fig. 9. The releasing instants and the releasing intervals under DETCA in Case 1.

In the light of (24), the following control gain can be obtained

$$K = [-0.0247 \quad 0.0148]$$

Fig. 10 depicts the trajectory of $x(k)$ and the response of $x_r(k)$. From Fig. 10, we observe that the state tracks the reference state well. The $e(k)$ variation curve is given in Fig. 11, which can gradually converge to a very small region near zero. It can be concluded from Fig. 12 that only 23% signals are transmitted to the controller under the DETCA.

Case 3. In this case, set $\beta_d(k) = 1, \bar{\alpha}_d = 0.54$, and $\gamma = 0.45$, which indicate that only DoS attacks appear.

We can get the following values by Corollary 2

$$Y = [-0.1774 \quad 0.1101], X = \begin{bmatrix} 4.0465 & 0.0173 \\ 0.0173 & 4.1156 \end{bmatrix}$$

By calculating (24), the controller gain is given as

$$K = [-0.0440 \quad 0.0269]$$

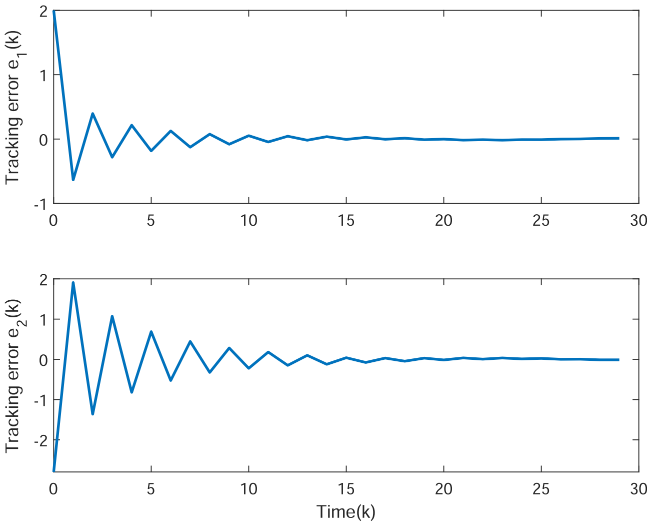

Fig. 7. Tracking error $e(k)$ in Case 1.

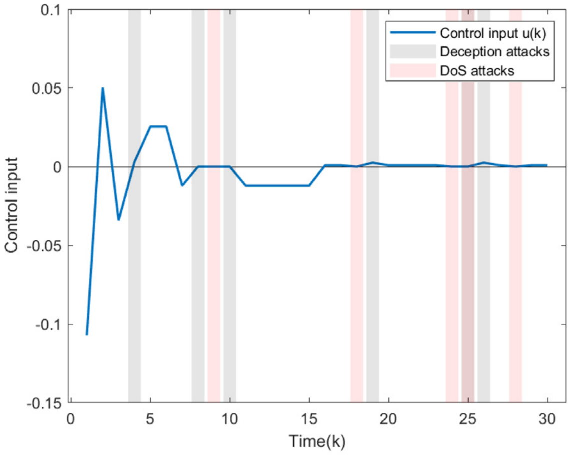

Fig. 8. Control input $u(k)$ under stochastic cyber-attacks in Case 1.

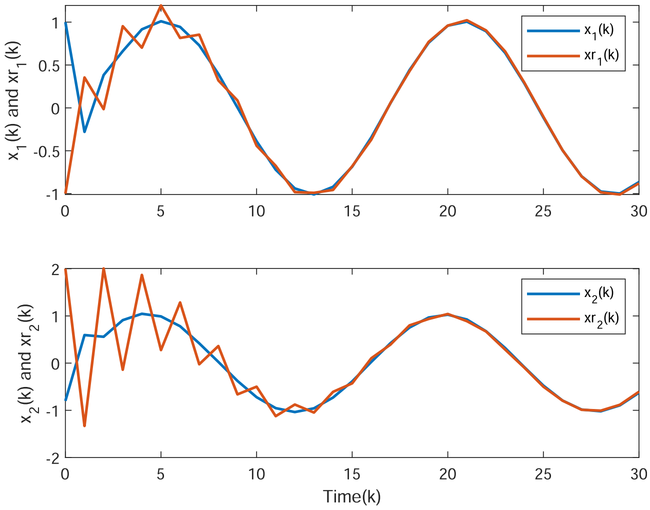

Fig. 10. State responses in Case 2.

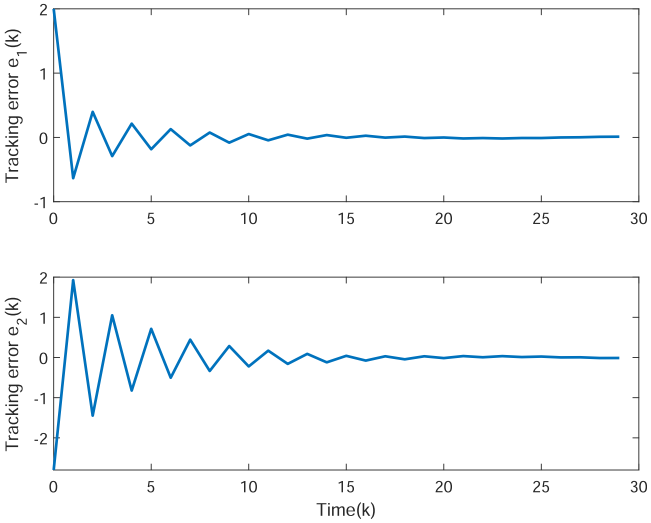

Fig. 11. Tracking error $e(k)$ in Case 2.

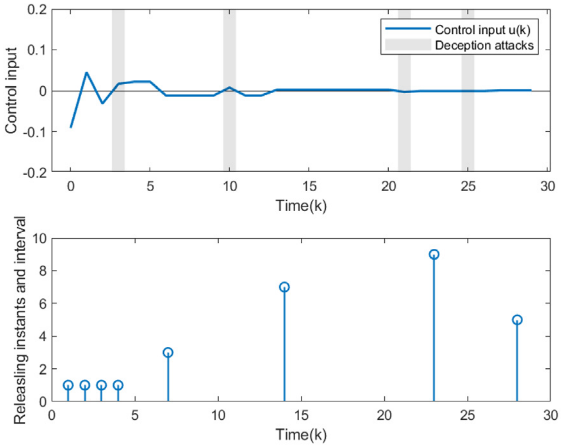

Fig. 12. Control input $u(k)$ and release intervals in Case 2.

Through Fig. 13 and Fig. 14, the tracking error can be asymptotically stabilized in about 20 times after large fluctuations in the early stage. Moreover, it is obvious from Fig. 15 that the DETCA reduces triggering data and then effectively lightens the network burden.

5. Conclusions

In this paper, a security tracking controller for discrete-time NCSs has been investigated with DETCA and stochastic cyber-attacks. In order to reduce the load of communication channel, the DETCA is introduced to adjust the amount of data transmission based on the variation of tracking error. The threshold of the ETM is adjustable according to a dynamic pre-designed condition. In addition, a novel model is presented that considers the influence of stochastic cyber-attacks. A security tracking control strategy is proposed for the discrete-time NCSs when networked security is affected. Moreover, by means of Lyapunov stability theory, a sufficient condition to guarantee the stability of the tracking error system and H_∞ tracking performance is achieved, the controller gain is obtained by LMI technique. In the end, the correctness and feasibility of the theoretical results has been verified by two simulation examples.

Our future directions mainly includes the tracking control problem for networked systems using the reinforcement learning algorithm, such as neural network algorithm and Q-learning algorithm.

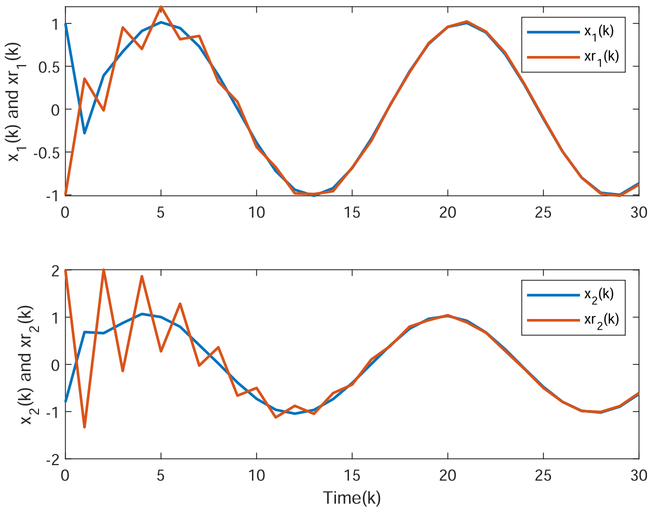

Fig. 13. State responses in Case 3.

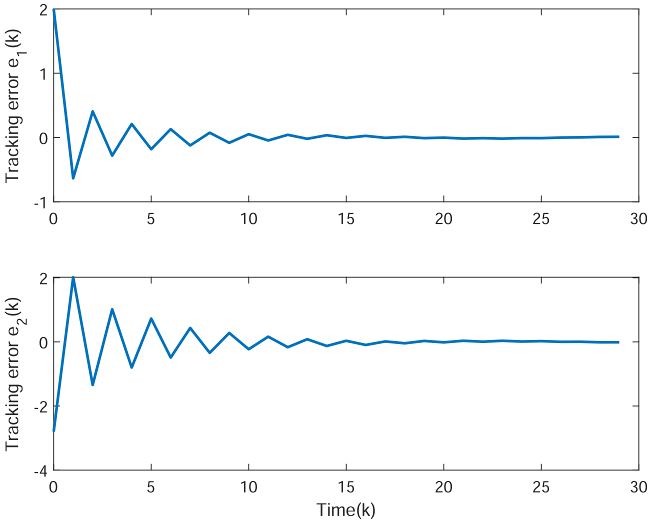

Fig. 14. Tracking error $e(k)$ in Case 3.

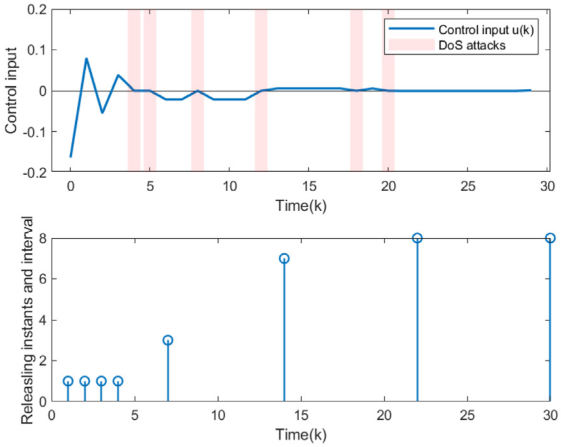

Fig. 15. Control input $u(k)$ and release intervals in Case 3.

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.

Acknowledgement

This work is 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; in part by the Qinglan Project of Jiangsu Province of China, and in part by the Postgraduate Research and practice Innovation Program of Jiangsu Province under Grant DYHXW21001.

References

[1] Y.-S. Ma, W.-W. Che, C. Deng, Dynamic event-triggered model-free adaptive control for nonlinear CPSs under aperiodic DoS attacks, Inf. Sci. 589 (2022) 790–801.
[2] A. Karbasi, A. Farhadi, A cyber-physical system for building automation and control based on a distributed MPC with an efficient method for communication, Eur. J. Control 61 (8) (2021) 151–170.
[3] 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, Inf. Sci. 544 (2021) 298–307.
[4] Z. Li, J. Zhao, Resilient adaptive control of switched nonlinear cyber-physical systems under uncertain deception attacks, Inf. Sci. 543 (2021) 398–409.
[5] Y. Yang, J. Huang, X. Su, B. Deng, Adaptive control of cyber-physical systems under deception and injection attacks, J. Franklin Inst. 358 (12) (2021) 6174–6194.
[6] H.L. Gawand, A.K. Bhattacharjee, K. Roy, Securing a cyber physical system in nuclear power plants using least square approximation and computational geometric approach, Nucl. Eng. Technol. 49 (3) (2017) 484–494.
[7] A. Fu, J.A. McCann, Dynamic decentralized periodic event-triggered control for wireless cyber-physical systems, IEEE Trans. Control Syst. Technol. 29 (4) (2021) 1783–1790.
[8] N. Zhao, P. Shi, W. Xing, J. Chambers, Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks, IEEE Trans. Control Network Syst. 8 (1) (2021) 158–167.
[9] J. Cao, D. Ding, J. Liu, E. Tian, S. Hu, X. Xie, Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks, Inf. Sci. 548 (2021) 69–84.
[10] R. Nadafi, M. Kabganian, Robust nonlinear attitude tracking control of an underactuated spacecraft under saturation and time-varying uncertainties, Eur. J. Control 63 (2022) 133–142.
[11] S. Xiao, X. Ge, Q.-L. Han, Y. Zhang, Z. Cao, Distributed guaranteed two-target tracking over heterogeneous sensor networks under bounded noises and adversarial attacks, Inf. Sci. 535 (2020) 187–203.
[12] 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 Trans. Cybern. 51 (1) (2021) 162–173.
[13] J. Liu, D. Yue, Event-triggering in networked systems with probabilistic sensor and actuator faults, Inf. Sci. 240 (2013) 145–160.
[14] W. He, Z. Mo, Q.L. Han, F. Qian, Secure impulsive synchronization in lipschitz-type multi-agent systems subject to deception attacks, IEEE/CAA J. Automatica Sinica 7 (5) (2020) 1326–1334.
[15] Q. Li, Z. Wang, W. Sheng, A. Fawaz E, and A. Fuad E, “Dynamic event-triggered mechanism for H_∞ non-fragile state estimation of complex networks under randomly occurring sensor saturations,” Information Sciences, vol. 509, pp. 304–316, 2020.
[16] Y. Li, F. Song, J. Liu, X. Xie, E. Tian, Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks, Int. J. Robust Nonlinear Control 3 (32) (2022) 1633–1653.
[17] D. Ding, Z. Wang, Q.-L. Han, A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks, IEEE Trans. Autom. Control 65 (4) (2020) 1792–1799.
[18] Z. Gu, D. Yue, E. Tian, On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems, Inf. Sci. 422 (2017) 257–270.
[19] Y. Wang, Z. Jia, Z. Zuo, Dynamic event-triggered and self-triggered output feedback control of networked switched linear systems, Neurocomputing 314 (2018) 39–47.
[20] S. Yan, M. Shen, G. Zhang, S.K. Nguang, Reliable H_∞ output control of nonlinear systems with dynamic event-triggered scheme, J. Franklin Inst. 356 (1) (2019) 58–79.
[21] W. He, B. Xu, Q.-L. Han, F. Qian, Adaptive consensus control of linear multiagent systems with dynamic event-triggered strategies, IEEE Trans. Cybern. 50 (7) (2020) 2996–3008.
[22] J. Liu, Y. Wang, L. Zha, X. Xie, E. Tian, An event-triggered approach to security control for networked systems using hybrid attack model, Int. J. Robust Nonlinear Control 31 (12) (2021) 5796–5812.
[23] D. Ding, Z. Wang, Q.-L. Han, G. Wei, Security control for discrete-time stochastic nonlinear systems subject to deception attacks, IEEE Trans. Syst., Man, Cybern.: Syst. 48 (5) (2018) 779–789.
[24] S. Hu, D. Yue, X. Xie, X. Chen, X. Yin, Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks, IEEE Trans. Cybern. 49 (12) (2019) 4271–4281.
[25] M.M. Hossain, C. Peng, Observer-based event triggering H_∞ LFC for multi-area power systems under DoS attacks, Inf. Sci. 543 (2021) 437–453.
[26] L. Zha, R. Liao, J. Liu, X. Xie, E. Tian, J. Cao, Dynamic event-triggered output feedback control for networked systems subject to multiple cyber-attacks, IEEE Trans. Cybern. (2021), https://doi.org/10.1109/TCYB.2021.3125851.
[27] J. Liu, W. Suo, X. Xie, D. Yue, J. Cao, Quantized control for a class of neural networks with adaptive-event-triggered scheme and complex cyber-ttacks, Int. J. Robust Nonlinear Control 31 (10) (2021) 4705–4728.
[28] C. Peng, H. Sun, M. Yang, Y.L. Wang, A survey on security communication and control for smart grids under malicious cyber attacks, IEEE Trans. Syst., Man, Cybern.: Syst. 49 (8) (2019) 1554–1569.
[29] P.-B. Wang, X.-M. Ren, D.-D. Zheng, Event-triggered resilient control for cyber-physical systems under periodic DoS jamming attacks, Inf. Sci. 577 (2021) 541–556.
[30] X.M. Zhang, Q.L. Han, X. Ge, L. Ding, Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks, IEEE Trans. Cybern. 50 (8) (2020) 3616–3626.
[31] S. Xiao, Q.L. Han, X. Ge, Y. Zhang, Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks, IEEE Trans. Cybern. 50 (3) (2020) 1220–1229.
[32] J. Huang, L. Zhao, Q.-G. Wang, Adaptive control of a class of strict feedback nonlinear systems under replay attacks, ISA Trans. 107 (2020) 134–142.

[33] B. Wei, E. Tian, J. Liu, X. Zhao, Probabilistic-constrained tracking control for stochastic time-varying systems under deception attacks: A Round-Robin protocol, J. Franklin Inst. 358 (17) (2021) 9135–9157.

[34] J. Liu, T. Yin, M. Shen, X. Xie, J. Cao, State estimation for cyber-physical systems with limited communication resources, sensor saturation and denial-of-service attacks, ISA Trans. 104 (2020) 101–114.

[35] J. Liu, Y. Wang, J. Cao, D. Yue, X. Xie, Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack, IEEE Trans. Cybern. 51 (8) (2021) 4000–4010.

[36] S. Xiao, X. Ge, Q.-L. Han, Y. Zhang, Secure distributed adaptive platooning control of automated vehicles over vehicular Ad-Hoc networks under denial-of-service attacks, IEEE Trans. Cybern. (2021), https://doi.org/10.1109/TCYB.2021.3074318.

[37] X. Li, C. Wen, J. Wang, C. Chen, C. Deng, Resilient leader tracking for networked Lagrangian systems under DoS attacks, Inf. Sci. 577 (2021) 622–637.

[38] K. Han, Y. Duan, R. Jin, Z. Ma, H. Wang, W. Wu, B. Wang, X. Cai, Attack detection method based on bayesian hypothesis testing principle in CPS, Procedia Comput. Sci. 187 (2021) 474–480.

[39] 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 Trans. 116 (2021) 1–16.

[40] Z. Du, Y. Kao, J.H. Park, Tracking control design for interval type-2 fuzzy nonlinear unreliable networked control systems, J. Franklin Inst. 358 (8) (2021) 4159–4177.

[41] X. Zhao, X. Zheng, B. Niu, L. Liu, Adaptive tracking control for a class of uncertain switched nonlinear systems, Automatica 52 (2015) 185–191.

[42] P. Gong, Q.-L. Han, W. Lan, Finite-time consensus tracking for incommensurate fractional-order nonlinear multiagent systems with directed switching topologies, IEEE Trans. Cybern. 52 (1) (2022) 65–76.

[43] Z. Gu, D. Yue, J. Liu, Z. Ding, H_∞ tracking control of nonlinear networked systems with a novel adaptive event-triggered communication scheme, J. Franklin Inst. 354 (8) (2017) 3540–3553.

[44] C. Peng, D. Yue, M.R. Fei, Relaxed stability and stabilization conditions of networked fuzzy control systems subject to asynchronous grades of membership, IEEE Trans. Fuzzy Syst. 22 (5) (2014) 1101–1112.

[45] E. Mousavinejad, X. Ge, Q.-L. Han, Y. Zhang, Resilient tracking control of networked control systems under cyber attacks, IEEE Trans. Cybern. 51 (4) (2021) 2107–2119.

[46] Y. Gu, J.H. Park, M. Shen, D. Liu, Event-triggered control of markov jump systems against general transition probabilities and multiple disturbances via adaptive-disturbance-observer approach, Inf. Sci. 608 (2022) 1113–1130.

[47] X. Zhao, C. Liu, E. Tian, Finite-horizon tracking control for a class of stochastic systems subject to input constraints and hybrid cyber attacks, ISA Trans. 104 (2020) 93–100.

[48] R.W. Eustace, B.A. Woodyatt, G.L. Merrington, A. Runacres, Fault signatures obtained from fault implant tests on an F-404 engine, J. Eng. Gas Turbines Power 116 (1) (1994) 178–183.