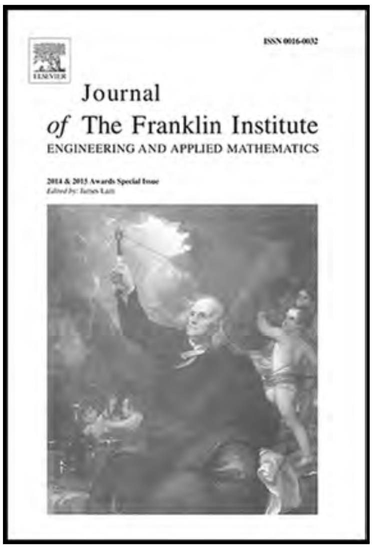

Periodic Event-Triggered Resilient Control for Cyber-Physical Systems Under Denial-of-Service Attacks

Yuan-Cheng Sun, Guang-Hong Yang

PII: S0016-0032(18)30412-5
DOI: 10.1016/j.jfranklin.2018.06.009
Reference: FI 3504

To appear in: *Journal of the Franklin Institute*

Received date: 20 January 2018
Revised date: 21 May 2018
Accepted date: 6 June 2018

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 00 (2018) 1–17

Journal
of The
Franklin Institute

Periodic Event-Triggered Resilient Control for Cyber-Physical Systems Under Denial-of-Service Attacks

Yuan-Cheng Sun[a], Guang-Hong Yang[a,b,*]

[a] *College of Information Science and Engineering, Northeastern University, Shenyang, 110819, PR China*
[b] *State Key Laboratory of Synthetical Automation of Process Industries, Northeastern University, Shenyang, 110819, PR China*

Abstract

This paper studies the problem of designing a resilient control strategy for cyber-physical systems (CPSs) under denial-of-service (DoS) attacks. By constructing an H_∞ observer-based periodic event-triggered control (PETC) framework, the relationship between the event-triggering mechanism and the prediction error is obtained. Then, inspired by the maximum transmission interval, the input-to-state stability of the closed-loop system is proved. Compared with the existing methods, a Zeno-free periodic PETC scheme is designed for a continuous-time CPS with the external disturbance and measurement noise. In particular, the objective of maximizing the frequency and duration of the DoS attacks is achieved without losing robustness. Finally, two examples are given to verify the effectiveness of the proposed approach.

Keywords: Cyber-physical systems; periodic event-triggered control; denial-of-service attack; input-to-state stability

1. Introduction

In recent years, cyber-physical systems (CPSs) have been widely used in various engineering fields owing to advances in computing and communication technologies. However, the use of networks and heterogeneous digital elements has made these CPSs vulnerable to various cyber attacks, such as deception attacks, replay attacks, bias injection attacks, zero-dynamics attacks, denial-of-service (DoS) attacks and so on. Unlike traditional systems where attacks limit their impact to the cyber level, malicious attacks to CPSs can impact the physical world [1].Thus these is a strong demand for analysis, synthesis and design methods to guarantee the security and reliability of CPSs despite the presence of malicious attacks[2, 3].

Among the various malicious attacks, DoS attacks make the actuator and sensor data to be blocked rather than reach their respective destinations and lead to the absence of data for the related components. Such kind of attack is very common in network communications, and a lot of works have been made for the CPSs under DoS attacks [4–8]. A basic research field on security problem of CPSs is the stability analysis under DoS attacks. In [9], the authors characterize frequency and duration of the DoS attacks under which input-to-state stability of the closed-loop system can be presented, and the transmission times is scheduled. A resilient control method is presented in [10] to maximize frequency and duration of the DoS attacks under which closed-loop stability is not destroyed. In [11], based on the studies on [10], a control architecture that approximate co-location while enable remote implementation is designed.

[*] Corresponding author.
Email addresses: dksyc294@126.com (Yuan-Cheng Sun), yangguanghong@ise.neu.edu.cn (Guang-Hong Yang)

The input-to-state stable (ISS) control problem for CPSs with multiple transmission channels under DoS attacks is concerned in [12]. In [13], a systematic design framework for output-based dynamic event-triggered control (ETC) systems under DoS attacks is proposed for a class of nonlinear systems using a hybrid model.

The traditional control methods are implemented in a time-triggered method where the sampling and the signal transmission are executed periodically, such as sampled-data control [14]. Usually, the wireless communication units of CPSs are power restricted, and the network is often shared with multiple devices. Hence communication resource utilization is needed to be considered. ETC scheme which helps reduce the network utilization has been widely investigated on networked control systems [15–19]. In [20], a state-dependent triggering method is proposed for network-based interconnected systems with delays and packet losses. In [21], periodic event-triggered control (PETC) strategy for linear systems is proposed. By combining time-triggered control and ETC, the event-triggering condition is verified periodically in PETC, and whether or not to compute or to transmit new measurements and control signals is decided at every periodic sampling instant. In [22], a model-based PETC strategy for linear discrete systems is presented, and both sensor-to-controller channels and the controller-to-actuator channels of the systems are communicated through networks. However, the ETC scheme for CPSs under DoS attacks has not been fully investigated. On the other hand, the DoS attacks occurred at the event-triggering intervals are invalid, thus the tolerable DoS attacks can be increased by using the ETC strategy. These are the major motivations of this study.

In this paper, a CPS which the sensor-to-controller channel is networked under DoS attacks is concerned, and both the disturbance and measurement noise are considered. An H_∞ observer-based ETC framework is constructed for the linear continuous-time plant, and the event-triggering mechanism (ETM) is verified periodically. The relationship between the event-triggering coefficient and the lower bound of inter-event times is given. Based on the input-to-state stability analysis framework, the stability is proved whether or not the DoS attacks are presented. The main contributions of this paper are characterized as follows: First, the advanced PETC method is used to continuous-time CPSs under DoS attacks, communication resources are saved, and the lower bounded of inter-event times is proposed to guarantee that the ETM is triggered at most once at each period. Second, the traditional static state feedback control using in [9] requires the availability of full-state information, and this is a strong assumption. In this paper, the assumption is relaxed and the influence of disturbance and noise can be restrained by using the H_∞ observer. Besides, compared with the method in [10], the measurement noise will not be amplified. Third, the maximum prediction error is calculated, and based on the convergence of the error, the objective of tolerating DoS attacks as much as possible is achieved without compromising the robustness.

The rest is organized as follows. In Section 2, the process is described, and the problem formulation is presented. In Section 3, input-to-state stability of the PETC strategy is proved without DoS attacks. Section 4 gives the PETC strategy under DoS attacks, and the main theorem is obtained. In Section 5, a numerical simulation and a batch reactor system simulation are provided. Section 6 concludes this paper.

Notation: Donate by $\mathbb{R}$ the set of reals, $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, and given $\alpha \in \mathbb{R}$, let $\mathbb{R}_{\geq\alpha}$ be the set of reals greater than or equal to α. Let $\mathbb{N}$ denote the set of natural number and $\mathbb{N}_0$ is defined as $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Given a vector $x \in \mathbb{R}^n$, $\|x\|$ indicates its Euclidean norm. Given a matrix A, let A^T denote its transpose, $\|A\|$ its spectral norm, μ_A its logarithmic norm [23], and $\mu_A = \max\left\{\lambda|\lambda \in \text{spectrum}\left\{\frac{A+A^T}{2}\right\}\right\}$. Given two sets S_1 and S_2, let $S_2 \backslash S_1$ be the relative complement of S_1 in S_2. For an interval $T = [t_1, t_2)$, its length is defined as $|T(t_1, t_2)| = t_2 - t_1$. Given a measurable time function $f(t)$ and a time interval $[0, t)$, the $\mathcal{L}_\infty$ norm of $f(\cdot)$ on $[0, t)$ is formulated as $\|f_t\|_\infty = ess\ \sup_{s\in[0,t)} \|f(s)\|$.

2. Preliminaries and Problem Statement

2.1. System description

Consider the CPS process shown in Fig. 1. The sensor system transmits the measurement information to the controller system over a shared wireless network, where communication resources (the batteries for the wireless devices, for instance) are limited. At the same time, the network of the CPS may be attacked by DoS attacks. The linear continuous-time plant is described as follows

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + \omega(t) \\ y(t) &= Cx(t) + \nu(t) \end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state variable of the physical plant, $u(t) \in \mathbb{R}^{m_u}$ is the input from the feedback controller. $y(t) \in \mathbb{R}^{m_y}$ is the output of the physical plant sending to the sensor system. $\omega(t) \in \mathbb{R}^n$ is a bounded disturbance, $\nu(t) \in \mathbb{R}^{m_y}$ is bounded measurement noise, where $\|\omega(t)\| \leq \kappa_\omega$, $\|\nu(t)\| \leq \kappa_\nu$. The bounds are known constants. A, B and C are matrices of appropriate sizes. Assume that the system is observable, and there exist no time-delay or random packet loss in the network communication, and the computation time is zero.

Remark 1. The noises considered here includes non-Gaussian noises [24, 25]. The only constraint is that the noises are bounded.

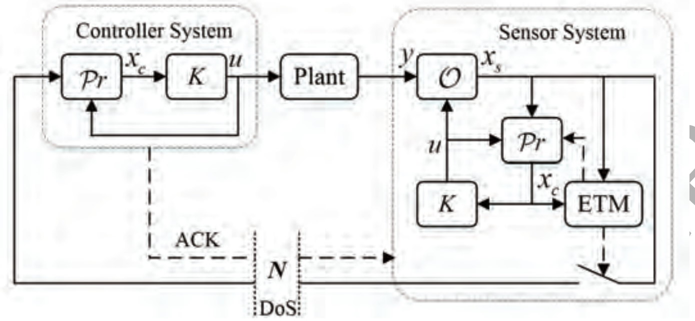

Fig. 1. The framework of PETC system under DoS.

In order to reduce the transmissions over the network as much as possible while still guaranteeing the desirable closed-loop behavior and stability, a smart sensor system with PETC strategy is designed. The smart sensor system consists of an observer $\mathcal{O}$ and an ETM that determines when information should be transmitted to the controller system. Besides, the controller system consists of a predictor $\mathcal{P}r$ which can predict the state information using the transmitted signals. There is a copy of the controller system maintained in the sensor system to provide information for the decision of ETM. The observer is given as

$$\mathcal{O} : \quad \dot{x}_s(t) = Ax_s(t) + Bu(t) + L\tilde{y}(t) \tag{2}$$

where $x_s(t)$ is the estimated state of the sensor system, and $\tilde{y}(t) = y(t) - Cx_s(t)$. The predictor is given as

$$\mathcal{P}r : \begin{cases} \dot{x}_c(t) = Ax_c(t) + Bu(t), & x_s(t) \; is \; not \; sent \\ x_c(t) = x_s(t), & x_s(t) \; is \; sent \end{cases} \tag{3}$$

Whether $x_s(t)$ is sent is decided by the ETM given as follows

$$x_s(t) is \; sent \Leftrightarrow \|x_s(t) - x_c(t)\| > \sigma_s \|x_s(t)\| + \sigma_c \rho \tag{4}$$

where $\rho = \lambda \|C\| \kappa + \kappa_\nu$, $\sigma_s > 0$, $\sigma_c > 0$ and λ are suitable parameters to be designed later, $\kappa = \kappa_\omega + \kappa_\nu$. Besides, an acknowledgment signal (ACK) is needed to confirm the success of the transmission attempt when the ETM (4) is satisfied.

Let T_P be the verification period of the ETM (4), and $\{t_k\}_{k \in \mathbb{N}_0}$ be the sequence of data update transmission attempt, then the interval Δ_k between two consecutive signal transmission attempts satisfies

$$0 < \underline{\Delta} \leq t_{k+1} - t_k = \Delta_k \leq \bar{\Delta} \tag{5}$$

where $\underline{\Delta}$ and $\bar{\Delta}$ are the lower and upper bounds of the transmission attempts interval, respectively.

Remark 2. The transmission attempts interval Δ_k is determined by the ETM (4). Because of the feature of PETC strategy, the ETM is verified periodically, and the period T_P is defined less than or equal to the lower bound $\underline{\Delta}$ which is obtained later. The upper bound is used to compel the sensor system to transmit a signal to the controller system when the ETM is not triggered for a long time. The pre-specified upper bound can also be seen in [17].

2.2. Control objective

Definition 1 [26]. System (1) under a control input $u(t)$ is said to be ISS if there exist a $\mathcal{KL}$-function f_1 and a $\mathcal{K}_\infty$-function f_2 such that

$$\|x(t)\| \le f_1(\|x(0)\|, t) + f_2(\|d_t\|_\infty) \tag{6}$$

holds for all $t \in \mathbb{R},\ t \ge 0$, and each $d(t) \in \mathcal{L}_\infty(\mathbb{R}_{\ge 0})$, $x(0) \in \mathbb{R}^n$, where $d(t) = [\omega^T(t)\ \ \nu^T(t)]^T$. If (6) holds for $d(t) \equiv 0$, then the system (1) is said to be globally asymptotically stable (GAS).

The objectives of this paper are as follows: First, design the observer-based control framework and the ETM (4) to guarantee that the system is ISS with both the disturbance and measurement noise, and that the PETC strategy can save the communication resources. Then, design the advanced PETC strategy that can tolerate the DoS attacks as much as possible without loosing the closed-loop system stability.

3. Stability analysis of PETC strategy

In order to restrain the disturbance and noise, an H_∞ observer is designed. For any $t \in \mathbb{R}_{\ge 0}$, the observation error is defined as $e_s(t) = x(t) - x_s(t)$, then

$$\dot{e}_s(t) = \Phi_1 e_s(t) + \Upsilon d(t) \tag{7}$$

where $\Phi_1 = A - LC$, $\Upsilon = [I \quad -L]$, $d(t) = [\omega^T(t)\ \ \nu^T(t)]^T$. By employing the bounded real lemma for continuous-time systems [27], the observer gain matrix L can be obtained from the following LMI (8), and the H_∞ performance $\|e_s(t)\| < \lambda\|d(t)\|_\infty$ is achieved, where P_1 is a positive definite symmetric matrix, λ is a positive number.

$$\begin{bmatrix} P_1\Phi_1 + \Phi_1^T P_1 & P_1\Upsilon & I \\ * & -\lambda I & 0 \\ * & * & -\lambda I \end{bmatrix} < 0 \tag{8}$$

The sensor system sends the current estimated state to the predictor by network to update the prediction state at $\{t_k\}_{k\in\mathbb{N}_0}$, yields $x_c(t_k) = x_s(t_k)$. When $t \in [t_k, t_{k+1})$, $x_c(t_k) = x_s(t_k)$ is the initial value for the predictor, then $x_c(t)$ can be predicted by (3) dynamically, the control input can be calculated by the following state feedback controller

$$u(t) = Kx_c(t) \tag{9}$$

where K is the controller gain matrix. Let $\Phi_2 = A + BK$, where K is designed in such a way that all the eigenvalues of Φ_2 have negative real part.

Define the error between the current state $x(t)$ and the prediction state $x_c(t)$ as

$$e(t) = x_c(t) - x(t) \tag{10}$$

where $t \in \mathbb{R}_{\ge 0}$, then the closed-loop system is formulated as

$$\dot{x}(t) = \Phi_2 x(t) + BKe(t) + \omega(t) \tag{11}$$

Choose $V(t) = x^T(t)Px(t)$ as the Lyapunov function [9], where P is the unique solution of the following Lyapunov equation

$$P\Phi_2 + \Phi_2^T P + Q = 0 \tag{12}$$

and Q is an any given positive definite symmetric matrix. Then for any $t \in \mathbb{R}_{\ge 0}$, it can be obtained that

$$\alpha_2 \|x(t)\| \le V(t) \le \alpha_1 \|x(t)\| \tag{13}$$

$$\dot{V}(t) \le -\gamma_1\|x(t)\|^2 + \gamma_2 \|x(t)\| \|e(t)\| + \gamma_3 \|x(t)\| \|\omega(t)\| \tag{14}$$

where α_1 and α_2 represent the largest and smallest eigenvalues of P, respectively. γ_1 is the smallest eigenvalue of Q, $\gamma_2 = \|2PBK\|$ and $\gamma_3 = \|2P\|$. For any $t \in [t_k, t_{k+1})$, $\|x_s(t) - x_c(t)\| \le \sigma_s \|x_s(t)\| + \sigma_c\rho$ always holds, then based on the triangle inequality and $\|e_s(t)\| = \|x(t) - x_s(t)\| < \lambda \|d(t)\|_\infty$, it can be obtained that

$$\|x(t) - x_c(t)\| \le \sigma_s \|x(t)\| + \sigma_c\rho + \lambda \|d(t)\|_\infty \tag{15}$$

then $\|d(t)\|_\infty \le \kappa_\omega + \kappa_\nu = \kappa$ yields

$$\|e(t)\| = \|x(t) - x_c(t)\| \le \sigma_s \|x(t)\| + \sigma_\kappa\kappa \tag{16}$$

where $\sigma_\kappa = \lambda\sigma_c \|C\| + \lambda + \sigma_c$. Then substituting (16) into (14) yields $\dot{V}(t) \le -(\gamma_1 - \sigma_s\gamma_2)\|x(t)\|^2 + (\gamma_3 + \sigma_\kappa\gamma_2) \|x(t)\| \kappa$, it can be proven that when $\gamma_1 - \sigma_s\gamma_2 > 0$ is satisfied, and

$$V(x(t)) \le e^{-\theta_1 t} V(x(0)) + \gamma_4\kappa^2 \tag{17}$$

where, $\theta_1 = \frac{\gamma_5}{2\alpha_1}$, $\gamma_4 = \frac{(\gamma_3+\sigma_\kappa\gamma_2)^2}{2\gamma_5\theta_1}$, $\gamma_5 = \gamma_1 - \sigma_s\gamma_2$. Then for any $\underline{\Delta} \le t_{k+1} - t_k = \Delta_k$, it can be concluded from Definition 1 that the system is ISS. The use of the predictor allows the controller to predict the system state value, and the error generated during the transmission interval is reduced. For any $t \in [t_k, t_{k+1})$, it can be obtained from (10) that

$$\dot{e}(t) = Ae(t) - \omega(t) \tag{18}$$

then $x_c(t_k) = x_s(t_k)$ yields $\|e(t_k)\| = \|e_s(t_k)\|$, and by employing $\left\|e^{At}\right\| \le e^{\mu_A t}$ for $t \in \mathbb{R}_{\ge 0}$, it can be obtained that

$$\begin{aligned} \|e(t)\| &\le \int_{t_k}^{t} e^{\mu_A(t-\tau)}(\|A\| \|e_s(t_k)\| + \|\omega(\tau)\|)d\tau \\ &< f(t - t_k)(\lambda \|A\| \kappa + \kappa_\omega) \\ &= \varepsilon(\lambda \|A\| \kappa + \kappa_\omega) \end{aligned} \tag{19}$$

where $f(t - t_k) = \int_{t_k}^{t} e^{\mu_A(t-\tau)} d\tau$, μ_A is the logarithmic norm of A and $\varepsilon = \begin{cases} \Delta_k, & \mu_A \le 0 \\ \frac{1}{\mu_A}(e^{\mu_A\Delta_k} - 1), & \mu_A > 0 \end{cases}$.

Because the ETM (4) is verified periodically while the system process is continuous, the triggering time sequence $\{t_k\}_{k\in\mathbb{N}_0}$ is needed to study to exclude continuous triggering of each verification period.

Theorem 1. *Consider the control system (1) with the observer $\mathcal{O}$ and the predictor $\mathcal{P}r$, and the control input (9) with the ETM (4), the inter-event times Δ_k, $k \in \mathbb{N}_0$ defined in (5) are lower bounded by $\underline{\Delta}$ which satisfies*

$$\underline{\Delta} = \begin{cases} \frac{\sigma_c}{\|L\|}, & \mu_A \le 0 \\ \frac{1}{\mu_A}\log(\frac{\mu_A\sigma_c}{\|L\|} + 1), & \mu_A > 0 \end{cases} \tag{20}$$

where σ_c is defined in (4).

Proof. Denote $e_c(t) = x_s(t) - x_c(t)$, then it can be obtained that

$$\dot{e}_c(t) = Ae_c(t) + L\tilde{y}(t) \tag{21}$$

where $\tilde{y}(t) = Ce_s(t) + \nu(t)$. For any $t \in [t_k, t_{k+1})$, $e_c(t_k) = 0$, then

$$\begin{aligned} \|e_c(t)\| &\le \int_{t_k}^{t} e^{\mu_A(t-\tau)} \|L\| \|\tilde{y}(\tau)\| d\tau \\ &\le \|L\| \int_{t_k}^{t} e^{\mu_A(t-\tau)} d\tau(\|C\| \|e_s(t)\| + \|\nu(t)\|_\infty) \\ &\le \begin{cases} (t - t_k) \|L\|\rho, & \mu_A \le 0 \\ \frac{\|L\|}{\mu_A}(e^{\mu_A(t-t_k)} - 1)\rho, & \mu_A > 0 \end{cases} \end{aligned}$$

where $\rho = \lambda \|C\| \kappa + \kappa_v$ as in (4). Then it can be seen that for any $\sigma_c > 0$, the ETM (4) cannot be triggered if $t \in [t_k, t_k + \underline{\Delta})$, which completes the proof. □

4. Resilient control under DoS attacks

4.1. DoS attack

In this paper, a general DoS model is considered that constrains the attacker action in time by only restricting the frequency of DoS attacks and their duration. Let $\{h_n\}_{n\in\mathbb{N}_0}$ with $h_0 \geq 0$ be the sequence of DoS off/on transitions, which are the time instants at which DoS transforms from zero (transmission attempts can be successful) to one (transmission attempts fail)[10]. The nth DoS time-interval is given by $H_n = \{h_n\} \cup [h_n, h_n + \tau_n)$, with $\tau_n \in \mathbb{R}_{\geq 0}$ being its length. If $\tau_n = 0$, then H_n degenerates to a single pulse. Suppose that $\{H_n\}_{n\in\mathbb{N}_0}$ has no overlap, then for any interval $[t_1, t_2]$, $0 \leq t_1 < t_2$, let

$$\mathcal{D}(t_1, t_2) = \underset{n\in\mathbb{N}_0}{\cup} H_n \cap [t_1, t_2] \tag{22}$$

$$\mathcal{H}(t_1, t_2) = [t_1, t_2] \backslash \mathcal{D}(t_1, t_2) \tag{23}$$

be the subset of $[t_1, t_2]$ when the network is in DoS status and healthy status, respectively. Let $n(t_1, t_2)$ be the number of DoS off/on transitions over $[t_1, t_2]$.

Assumption 1. [9] For any $0 \leq t_1 < t_2$, there exist $\eta \in \mathbb{R}_{\geq 0}$ and $\tau_D \in \mathbb{R}_{\geq \underline{\Delta}}$ such that

$$n(t_1, t_2) \leq \eta + \frac{t_2 - t_1}{\tau_D} \tag{24}$$

Assumption 2. [9] For any $0 \leq t_1 < t_2$, there exist $\varsigma \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{\geq 1}$ such that

$$|\mathcal{D}(t_1, t_2)| \leq \varsigma + \frac{t_2 - t_1}{T} \tag{25}$$

Remark 3. It is necessary to limit the frequency and duration of DoS attacks. Consider the worst situations without these assumptions: first, if $n(t_1, t_2)$ is sufficiently large, every transmission attempt may be covered by DoS pulses; second, if $|\mathcal{D}(t_1, t_2)|$ is sufficiently large, a DoS attack may fully occupies the interval $[t_1, t_2]$. In either case, all the transmission attempts may fail, the control performance cannot be guaranteed. On the other hand, the two assumptions can be explained from the view of energy. It is reasonable to suppose that the adversaries have limited energy to implement DoS attacks, the available energy is direct proportion to the length of time interval $[t_1, t_2]$, and the proportionality coefficient can be set as 1. The energy consumed for each DoS off/on transitions is τ_D, and for per unit of time, the energy consumed of maintaining a DoS attack is T. Besides, η and ς can be regarded as regularization parameters to guarantee the existence of (24) and (25).

4.2. Control update policy under DoS attacks

Let

$$T_k = \inf\{t \in \mathbb{R}_{>t_k} | \, \|x_s(t) - x_c(t)\| \geq \sigma_s \|x_s(t)\| + \sigma_c \rho\} \tag{26}$$

be the first time instant which the ETM is satisfied after a successful transmission attempt at t_k, and $\mathcal{T} = \{t \in \mathbb{R}_{>t_k} | \, \|x_s(t) - x_c(t)\| \geq \sigma_s \|x_s(t)\| + \sigma_c \rho\}$. If a transmission attempt at T_k is presented in a DoS interval H_n, it will fail. Denote by $\mathcal{F} = \{k \in \mathbb{N}_0 | t_k \in \underset{n\in\mathbb{N}_0}{\cup} H_n\}$ the set of integers related to a transmission attempt occurring under DoS. During DoS intervals, the system is transformed to use the periodic update policy, and the periodic control update interval is smaller than the ETC update interval in order to reduce the transmission delay caused by DoS. For each $k \in \mathbb{N}_0$, the transmission attempt times is given as follows

$$t_{k+1} = \begin{cases} t_k + \Delta_*, & if\ k \in \mathcal{F} \wedge\ t_k \in \mathcal{T} \\ t_k + \bar{\Delta}, & if\ k \notin \mathcal{F} \wedge\ \bar{\Delta} < T_k - t_k \\ T_k, & \text{otherwise} \end{cases} \tag{27}$$

where Δ_* is the periodic data update interval during DoS intervals, and $0 < \Delta_* < \bar{\Delta}$.

Remark 4. (27) gives the PETC update policy under DoS attacks. The sensor system sends the update data $x_s(t_k)$ at t_k, if the control system receives the data, it will send an ACK back to the sensor system, the transmission attempt at t_k is successful. Then the ETM (4) is verified at $t_k + T_P$, the next transmission attempt will occur at T_k when $\bar{\Delta} \geq T_k - t_k$. Otherwise, the next transmission attempt will occur at $t_k + \bar{\Delta}$. If the sensor system does not receive the ACK, it means that a DoS off/on transition occurred in the interval $(t_{k-1}, t_k]$, the transmission will be attempted at a periodic update rate specified by Δ_* from t_k until the sensor system receives an ACK again or the ETM is violated.

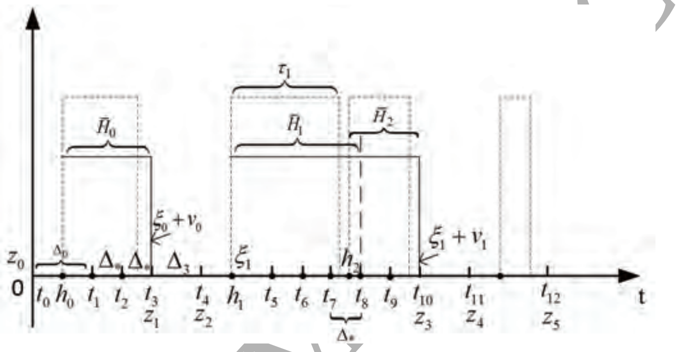

Fig. 2. An example of DoS attacks.

For any $0 \leq t_1 < t_2$, the interval $[t_1, t_2]$ is the disjoint union of $\bar{\mathcal{H}}(t_1, t_2)$ and $\bar{\mathcal{D}}(t_1, t_2)$, where $\bar{\mathcal{H}}(t_1, t_2)$ is the union of sub-intervals of $[t_1, t_2]$ over which the ETM (4) is not satisfied, that is the union of healthy sub-intervals of $[t_1, t_2]$. $\bar{\mathcal{D}}(t_1, t_2)$ is the union of valid DoS sub-intervals which is defined as the intervals leading to (4) be satisfied, and $\bar{\mathcal{D}}(t_1, t_1) = [t_1, t_1] \backslash \bar{\mathcal{H}}(t_1, t_1)$. The valid DoS sub-interval means that there is at least one transmission attempt occurs at the DoS sub-interval. On the other hand, the invalid DoS is that the DoS interval has no influence to the transmission attempts, such as the DoS occurs during $[t_{11}, t_{12}]$ in Fig. 2. But consider the worst case, the DoS on/off instant may cover the transmission instant such as t_{12} leading to a delay Δ_*. Define

$$\lambda_n = \begin{cases} 0, & \text{if } \mathcal{F} = \emptyset \\ t_{\sup\{k \in \mathbb{N}_0 | k \in \mathcal{F}\}} - h_n, & otherwise \end{cases} \tag{28}$$

then the nth valid DoS sub-interval is as follows

$$\bar{H}_n = \{h_n\} \cup [h_n, h_n + \lambda_n + \Delta_*) \tag{29}$$

Notice that $\bar{H}_n$ and $\bar{H}_{n+1}$ may overlap each other in that h_{n+1} may belong to $\bar{H}_n$, as shown in Fig. 2. For convenience, the overlapping sub-interval can be regarded as a single valid DoS sub-interval. Denote by $\{\xi_m\}_{m \in \mathbb{N}_0}$ the sequence of off/on transitions of the mth valid DoS interval as follows

$$\xi_0 = h_0,\ \xi_{m+1} = \inf\{h_n > \xi_m | h_n > h_{n-1} + \lambda_{n-1} + \Delta_*\} \tag{30}$$

and the length of the mth valid DoS interval is $v_m = \sum_{\substack{n\in\mathbb{N}_0 \\ \xi_m \le h_n < \xi_{m+1}}} \left|\bar{H}_n \backslash \bar{H}_{n+1}\right|$, then

$$\bar{\mathcal{D}}(t_1, t_2) = \bigcup_{m\in\mathbb{N}_0} [\xi_m, \xi_m + v_m) \cap [t_1, t_2] \tag{31}$$

$$\bar{\mathcal{H}}(t_1, t_2) = \bigcup_{m\in\mathbb{N}_0} [\xi_m + v_m, \xi_{m+1}) \cap [t_1, t_2] \tag{32}$$

From Assumption 1 and 2 it can be obtained that

$$\begin{aligned} \left|\bar{\mathcal{D}}(t_1, t_2)\right| &\le |\mathcal{D}(t_1, t_2)| + (n(t_1, t_2) + 1)\Delta_* \\ &\le \varsigma_* + \tfrac{t_2 - t_1}{T_*} \end{aligned} \tag{33}$$

where $\varsigma_* = \varsigma + (\eta + 1)\Delta_*$, $\frac{1}{T_*} = \frac{\Delta_*}{\tau_D} + \frac{1}{T}$.

Lemma 1. *Denote by $\{z_m\}_{m\in\mathbb{N}_0}$ the sequence of successful transmission attempts. Consider a transmission policy as (27), and the DoS attacks satisfying Assumption 1 and 2, then $\{z_m\}_{m\in\mathbb{N}_0}$ satisfies $z_0 \le \Psi$ and $z_{m+1} - z_m \le \Psi + \bar{\Delta}$, where $\Psi = (\varsigma + \eta\Delta_*)(1 - \frac{\Delta_*}{\tau_D} - \frac{1}{T})^{-1}$.*

Remark 5. A similar lemma is proved in [10]. In this paper, the event-triggered time interval during H_n is unknown, but the upper bound of the transmission attempt interval $\bar{\Delta}$ is known. Obviously, $\frac{1}{T_*} < 1$ is needed, and it is the best bound for which closed-loop stability can be achieved under any DoS attacks as discussed in [10].

Based on Lemma 1, it can be obtained from (18) and (19) that for any $t \in [z_m, z_{m+1})$

$$\|e(t)\|_\infty < \bar{\varepsilon}(\lambda \|A\| \kappa + \kappa_\omega) \tag{34}$$

where $\bar{\varepsilon} = \begin{cases} \Psi + \bar{\Delta}, & \mu_A \le 0 \\ \frac{1}{\mu_A}(e^{\mu_A(\Psi+\bar{\Delta})} - 1), & \mu_A > 0 \end{cases}$. It implies that the error between prediction state $x_c(t)$ and the actual state $x(t)$ is bound under DoS attacks. Exploiting (34), the following result is obtained.

Theorem 2. *Consider the control system (1) with the observer $\mathcal{O}$ (2) and the predictor $\mathcal{P}r$ (3), the control input (9) with the ETM (4) and (5), and $\gamma_1 - \sigma_s\gamma_2 > 0$ is satisfied. For any DoS attacks satisfying Assumption 1 and 2 with arbitrary ς and η, and with τ_D and T such that*

$$\frac{\Delta_*}{\tau_D} + \frac{1}{T} < 1 \tag{35}$$

where Δ_* is a nonnegative constant satisfying $T_P \le \Delta_* \le \bar{\Delta}$, the closed-loop system is ISS under the transmission policy (27).

Proof. For clarity of exposition, the following part is divided into two steps.

Step 1. Stability analysis of the closed-loop system in the healthy sub-interval $[\xi_m + v_m, \xi_{m+1})$ and the valid DoS sub-interval $[\xi_m, \xi_m + v_m)$ is proposed, respectively.

Choose $V(t) = x^T(t)Px(t)$ as the Lyapunov function, the matrices P and Q are obtained as in (12). For any $t \in [\xi_m + v_m, \xi_{m+1}),\ m \in N_0$, notice that $\|x(t) - x_c(t)\| \le \sigma_s \|x(t)\| + \sigma_c\rho$ holds, then it can be obtained from (17) that

$$V(x(t)) \le e^{-\theta_1(t-\xi_m-v_m)}V(x(\xi_m + v_m)) + \gamma_4\kappa^2 \tag{36}$$

where $\sigma_\kappa = \lambda(\sigma_c \|C\| + \sigma_s + 1) + \sigma_c$, $\kappa = \kappa_\omega + \kappa_v$, $\theta_1 = \frac{\gamma_5}{2\alpha_1}$, $\gamma_4 = \frac{(\gamma_3+\sigma_\kappa\gamma_2)^2}{2\gamma_5\theta_1}$, $\gamma_5 = \gamma_1 - \sigma_s\gamma_2$.

Consider any valid DoS interval $t \in [\xi_m, \xi_m + v_m),\ m \in \mathbb{N}_0$. In this interval, $\|x(t) - x_c(t)\| \le \sigma_s \|x(t)\| + \sigma_c\rho$ may not hold, but the time instant when the ETM is satisfied cannot be known. Notice $\|e(t)\| < \bar{\varepsilon}(\lambda \|A\| \kappa + \kappa_\omega)$ from (34), then it can be obtained from (14) that

$$\begin{aligned}\dot{V}(x(t)) &\le -\gamma_1\|x(t)\|^2 + \gamma_2\bar{\varepsilon}\,\|x(t)\|\,(\lambda\,\|A\|\,\kappa + \kappa_\omega) + \gamma_3\,\|x(t)\|\,\|\omega(t)\| \\ &\le -\gamma_1\|x(t)\|^2 + (\gamma_2\bar{\varepsilon} + \gamma_3)\,\|x(t)\|\,\kappa_e\end{aligned} \tag{37}$$

where $\kappa_e = \lambda\,\|A\|\,\kappa + \kappa_\omega$. Using the following inequation

$$(\gamma_2\bar{\varepsilon} + \gamma_3)\,\|x(t)\|\,\kappa_e \le \frac{\gamma_1}{2}\|x(t)\|^2 + \frac{(\gamma_2\bar{\varepsilon} + \gamma_3)^2}{2\gamma_1}\kappa_e^2 \tag{38}$$

one can obtain

$$\begin{aligned}\dot{V}(x(t)) &\le -\tfrac{\gamma_1}{2}\|x(t)\|^2 + \tfrac{(\gamma_2\bar{\varepsilon}+\gamma_3)^2}{2\gamma_1}\kappa_e^2 \\ &\le -\theta_2 V(x(t)) + \gamma_6\kappa_e^2\end{aligned} \tag{39}$$

where $\theta_2 = \frac{\gamma_1}{2\alpha_1}$, $\gamma_6 = \frac{(\gamma_2\bar{\varepsilon}+\gamma_3)^2}{2\gamma_1}$. Then for any $t \in [\xi_m, \xi_m + \nu_m),\ m \in \mathbb{N}_0$,

$$V(x(t)) \le e^{-\theta_2(t-\xi_m)}V(x(\xi_m)) + \gamma_7\kappa_e^2 \tag{40}$$

holds, where $\gamma_7 = \frac{\gamma_6}{\theta_2}$.

Step 2. Stability analysis for any $t \in \mathbb{R}_{>0}$.

For any interval $[0, t)$, by iterations, we have

$$V(x(t)) \le e^{-\theta_1\left|\bar{\mathcal{H}}(0,t)\right|}e^{-\theta_2\left|\bar{\mathcal{D}}(0,t)\right|}V(x(0)) + \gamma_*(1 + \sum_{\substack{m\in\mathbb{N}_0;\\ \xi_m\le t}} e^{-\theta_1\left|\bar{\mathcal{H}}(\xi_m+\nu_m,t)\right|}e^{-\theta_2\left|\bar{\mathcal{D}}(\xi_m,t)\right|})\kappa_*^2 \tag{41}$$

where $\gamma_* = \max\{\gamma_4, \gamma_7\}$ and $\kappa_* = \max\{\kappa, \kappa_e\}$. Using (33), we have

$$\left|\bar{\mathcal{D}}(\xi_m, t)\right| \le \varsigma_* + \frac{t - \xi_m}{T_*} \tag{42}$$

holds for any $t \in \mathbb{R}, t > \xi_m$. Then notice that $\bar{\mathcal{D}}(\tau, t) = [t_1, t_2]\backslash\bar{\mathcal{H}}(t_1, t_2)$ and $\bar{\mathcal{H}}(\xi_m + \nu_m, t) = 0$ when $t < \xi_m + \nu_m$, it can be obtained that

$$\bar{\mathcal{H}}(\xi_m + \nu_m, t) = t - \xi_m - \left|\bar{\mathcal{D}}(\xi_m, t)\right| \tag{43}$$

For any $t \in \mathbb{R}, t > \xi_m + \nu_m$, notice that $\left|\bar{\mathcal{D}}(\xi_m + \nu_m, t)\right| = 0$, $\left|\bar{\mathcal{D}}(\xi_m, t)\right| = \nu_m$ holds, then it can be obtained that $\bar{\mathcal{H}}(\xi_m + \nu_m, t) = t - \xi_m - \nu_m = t - \xi_m - \left|\bar{\mathcal{D}}(\xi_m, t)\right|$. Thus,

$$\sum_{\substack{m\in\mathbb{N}_0;\\ \xi_m\le t}} e^{-\theta_1\left|\bar{\mathcal{H}}(\xi_m+\nu_m,t)\right|}e^{-\theta_2\left|\bar{\mathcal{D}}(\xi_m,t)\right|} \le e^{-(\theta_2-\theta_1)\varsigma_*}\sum_{\substack{m\in\mathbb{N}_0;\\ \xi_m\le t}} e^{-a(t-\xi_m)} \tag{44}$$

where $a = \theta_1 + \frac{\theta_2-\theta_1}{T_*}$, $\varsigma_* = \varsigma + (\eta + 1)\Delta_*$. It is obvious that $\frac{1}{T_*} < 1$ ensures $a > 0$. The same as (44), the first term of the right hand side of (41) can be bounded by $e^{-(\theta_2-\theta_1)\varsigma_*}e^{-at}V(x(0))$, then we have

$$V(x(t)) \le e^{-(\theta_2-\theta_1)\varsigma_*}e^{-at}V(x(0)) + \gamma_*(1 + e^{-(\theta_2-\theta_1)\varsigma_*}\sum_{\substack{m\in\mathbb{N}_0;\\ \xi_m\le t}} e^{-a(t-\xi_m)})\kappa_*^2 \tag{45}$$

From the result in [9], we have $\sum\limits_{\substack{m\in\mathbb{N}_0;\\ \xi_m\leq t}} e^{-a(t-\xi_m)} \leq \frac{e^{a\eta\tau_D}}{1-e^{-a\tau_D}}$, then it can be obtained that

$$\|x(t)\| \leq \sqrt{\frac{\alpha_1}{\alpha_2}} e^{\frac{-(\theta_2-\theta_1)\varsigma_*}{2}} e^{-\frac{at}{2}} \|x(0)\| + \sqrt{\frac{\gamma_*}{\alpha_2}(1+\frac{e^{a\eta\tau_D}}{1-e^{-a\tau_D}} e^{-(\theta_2-\theta_1)\varsigma_*})}\kappa_* \tag{46}$$

Notice that the parameters of (46) are independent of the process initial condition and the disturbance, thus the closed-loop system is ISS, which completes the proof. □

Remark 6. The conservativeness of the results in [9] comes from the decomposition of the time axis. As is shown in Fig. 2, the intervals $[h_0, t_1)$ and $[h_1, t_5)$ are regarded as the sub-intervals of valid DoS intervals in [9]. In fact, in these sub-intervals the ETM is still violated, that is $\|x_s(t) - x_c(t)\| < \sigma_s \|x_s(t)\| + \sigma_c\rho$. The real valid DoS intervals should be $[t_1, t_3)$ and $[t_5, t_{10})$, where the ETM is satisfied and the transmission attempts fail. Because the time when the DoS off/on transition occurs is unknown to us, the conservativeness cannot be reduced by decomposing the time axis. Employing the maximum disturbance-induced error which is obtained from (34), the process can be reversely understood as the error converges from the maximum value to $\sigma_s \|x_s(t_k)\| + \sigma_c\rho, k = \inf\{k \in \mathcal{F} | t_k \in \bigcup\limits_{n\in\mathbb{N}_0} H_n\}$, then the best bound of the tolerable DoS attacks can be obtained.

5. Simulation Examples

5.1. Numerical Simulation

In this section, a simple numerical simulation is given to verify the proposed results. Consider an open-loop unstable system which the parameter matrices is given as $A = \begin{bmatrix} 0 & 1 \\ -2 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. The disturbance $\omega(t)$ is a random signal with uniform distribution in $[-0.5, 0.5]$ and the noise $v(t)$ uniformly distributes in $[-0.3,\ 0.3]$. The initial conditions are $x(0) = x_c(0) = [2, -2]^T$. The H_∞ performance index $\lambda = 1.67$, the observer gain matrix L and the state-feedback gain matrix K are given as $L = \begin{bmatrix} 3 & 1 \\ -2 & 8 \end{bmatrix}$, $K = \begin{bmatrix} -2 & -6 \end{bmatrix}$. By solving the Lyapunov equation (12) with $Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, it can be obtained that $\gamma_1 = 1$, $\gamma_2 = 12.2927$, $\gamma_3 = 2.4474$, $\alpha_1 = 1.2237$, $\alpha_2 = 0.1929$ and $\mu_A = 3.0811$. Thus σ_s must be selected such that $\sigma_s < 0.0813$, and $\sigma_s = 0.08$ is chosen. Let $\bar{\Delta} = 1s$ and $\underline{\Delta} = 0.06s$, Δ_* and T_P are selected as $\Delta_* = T_P = 0.01s$, then σ_c can be obtained from (20) that $\sigma_c = 0.0326$.

When the DoS attacks are absent, the closed-loop state response, the evolution of the inter-event times and the values of $\|x_s(t) - x_c(t)\|$ and $\sigma_s \|x_s(t)\| + \sigma_c\rho$ are given in Fig. 3, Fig. 4 and Fig. 5, respectively. As shown in Fig. 5, because the ETM is verified periodically, the event error may exceed the threshold at the period intervals.

When the DoS attacks are presented, the PETC strategy is as (27). Over the simulation horizon of 10 s, the DoS attacks yield $|\mathcal{D}(0, 10)| = 6.54s$ and $n(0, 10) = 9$, randomly. This corresponds to values of $\tau_D \approx 1.111$ and $T \approx 1.529$, and $\frac{\Delta_*}{\tau_D} + \frac{1}{T} \approx 0.663$. Then the closed-loop state response, the evolution of the inter-event times and the values of $\|x_s(t) - x_c(t)\|$ and $\sigma_s \|x_s(t)\| + \sigma_c\rho$ are given in Fig. 6, Fig. 7 and Fig. 8, respectively.

From Fig. 6, it can be seen that the PETC strategy proposed in this paper has strong robustness to the disturbance, noise and DoS attacks. In Fig. 7 and Fig. 8, it can be seen that when the DoS attack stopped, the successful transmission makes $\|x_s(t) - x_c(t)\| < \sigma_s \|x_s(t)\| + \sigma_c\rho$ hold again. When a new DoS off/on transition is occurred , $\|x_s(t) - x_c(t)\| < \sigma_s \|x_s(t)\| + \sigma_c\rho$ is still satisfied, the sensor system is unconscious of the occurrence of the DoS attack. Until the ETM (4) is satisfied during the DoS interval, the transmission attempt failed, the sensor system begins to transmit signals periodically, and the shorter transmission attempt interval leading the shorter delay. Then the transmission attempt interval is $\Delta_* = 0.01s$ as the selection. Then the first transmission attempt after the DoS on/off transition is successful, the system returns to normal.

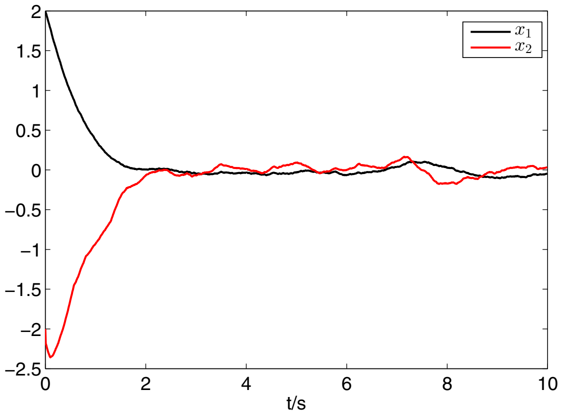

Fig. 3. State responses.

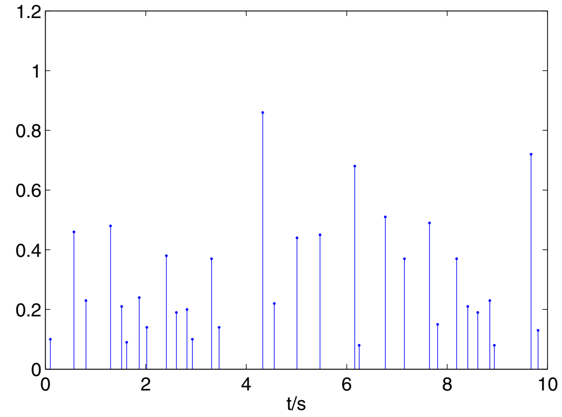

Fig. 4. The inter-event times of the PETC strategy.

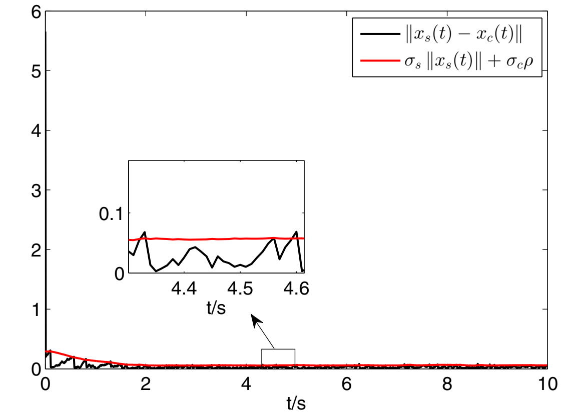

Fig. 5. The evolution of $\|x_s(t) - x_c(t)\|$ and $\sigma_s \|x_s(t)\| + \sigma_c \rho$.

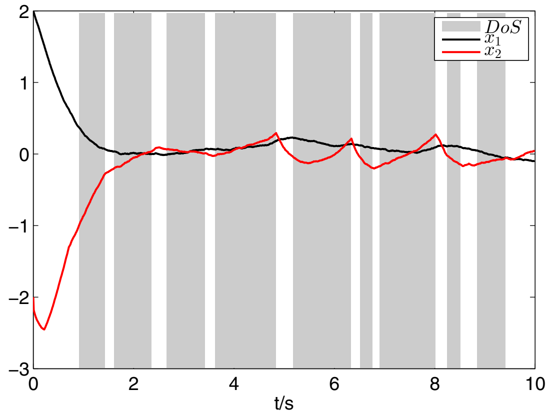

Fig. 6. State responses under DoS attacks.

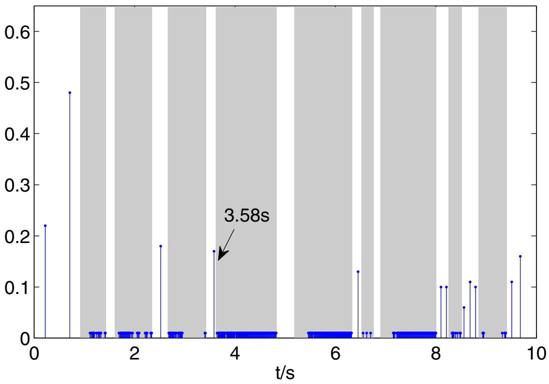

Fig. 7. The inter-event times of the PETC strategy under DoS attacks.

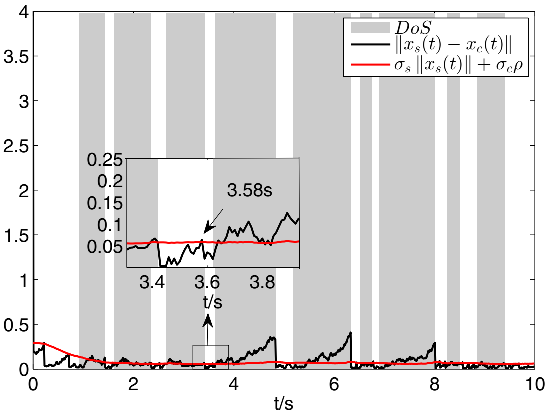

Fig. 8. The evolution of $\|x_s(t) - x_c(t)\|$ and $\sigma_s \|x_s(t)\| + \sigma_c\rho$ under DoS attacks.

5.2. Batch Reactor System Simulation

In this section, a batch reactor model proposed in [28] is considered. The open-loop unstable process is a coupled two-input , two-output network control system. The system matrices are shown as follows

$$A = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

The disturbance $\omega(t)$ is a random signal with uniform distribution in $[-0.2, 0.2]$ and the noise $v(t)$ is $v(t) = a\sin(\frac{\pi}{3}t)$, where a is a random number defined on $[0,\ 0.02]$. The initial conditions are $x(0) = x_c(0) = [0.8, -1, 0, 0.5]^T$. Setting $\lambda = 5.19$, then the observer gain matrix and state-feedback gain matrix can be obtained as follows

$$L = \begin{bmatrix} 10.7992 & -0.9969 \\ 2.3459 & 2.7804 \\ 12.6039 & 11.1471 \\ 11.8514 & 10.3365 \end{bmatrix},\ K = \begin{bmatrix} -0.7299 & -0.5116 & -1.2459 & 0.1511 \\ 2.3638 & 0.1773 & 1.6615 & -2.7389 \end{bmatrix}.$$

The relative parameters can be obtained that $\|\Phi_2\| = 19.1481$, $\alpha_1 = 2.1581$, $\alpha_2 = 0.0466$, $\gamma_1 = 1$, $\gamma_2 = 33.3192$, $\gamma_3 = 4.3162$. Thus σ_s must be selected such that $\sigma_s < 0.03$, and $\sigma_s = 0.027$ is chosen. Let $\bar{\Delta} = 1.5s$ and $\underline{\Delta} = 0.02s$, Δ_* and T_P are selected as $\Delta_* = T_P = 0.01s$, then σ_c can be obtained from (20) that $\sigma_c = 0.011$, then the closed-loop state response and the evolution of the inter-event times are given in Fig. 9 and the top of Fig. 10 , respectively, when the DoS attacks are absent,and the average inter-event time is 0.385s. The bottom of Fig.10 gives the inter-event times of the PETC strategy of [22], where the ETM is the same as (4) in [22] with $\sigma_s = 0.135$, and the disturbance and the measurement noise are the same as in this paper. The average inter-event time is 0.014s. As the contrast, the advanced PETC method has stronger robustness and saves much more communication resources.

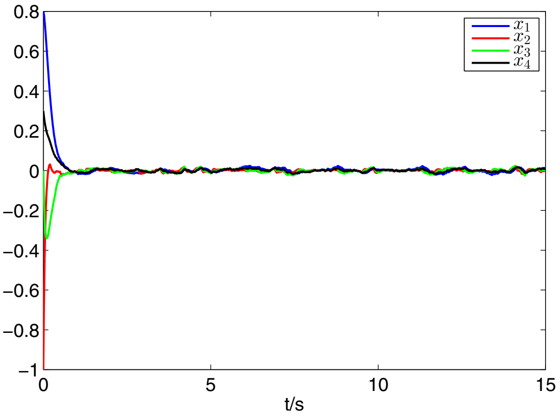

Fig. 9. State responses without DoS attacks.

When the DoS attacks are presented, the PETC strategy is as (27). Over the simulation horizon of 15s, the DoS attacks yield $|\mathcal{D}(0, 15)| = 10.93s$ and $n(0, 15) = 12$, randomly. This corresponds to values of $\tau_D \approx 1.25$ and $T \approx 1.3724$, and 73% of communication failures (the same as in [10]), then $\frac{\Delta_*}{\tau_D} + \frac{1}{T} \approx 0.7367$. Then the closed-loop state response, the evolution of the inter-event times and the values of $\|x_s(t) - x_c(t)\|$ and $\sigma_s\|x_s(t)\| + \sigma_c\rho$ are given in Fig. 11, Fig. 13 and Fig. 14, respectively.

Fig. 12 shows the simulation results of the algorithm in [10] with the same disturbance, noise and DoS attacks, meanwhile, the used observer gain matrix is the same as obtained in this paper, the feedback gain matrix is as in [10]. In [10], the measurement noise is neglected because of the noise will be amplified by the algorithm. Compared with the existing simulations in [10], the disturbance considered in this paper is much bigger, and the noise-induced

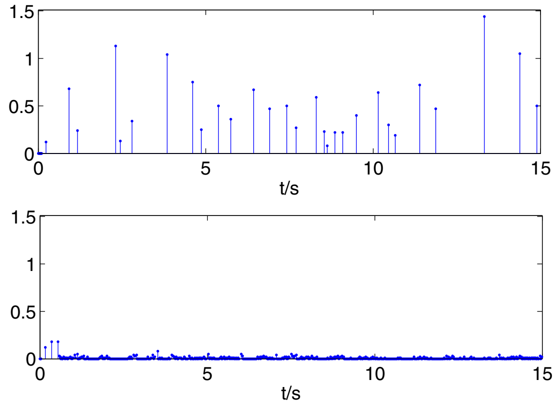

Fig. 10. Top: The inter-event times of the PETC strategy in this paper. Bottom: The inter-event times of [22].

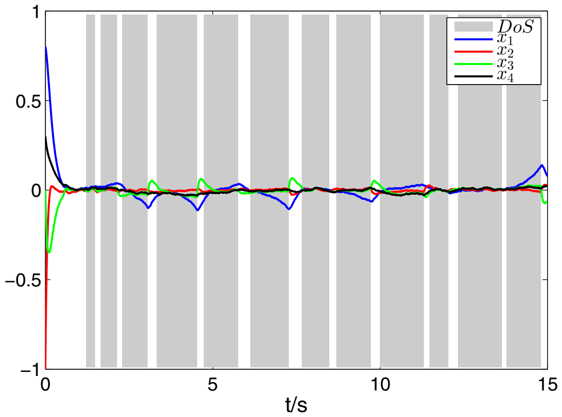

Fig. 11. State responses under DoS attacks.

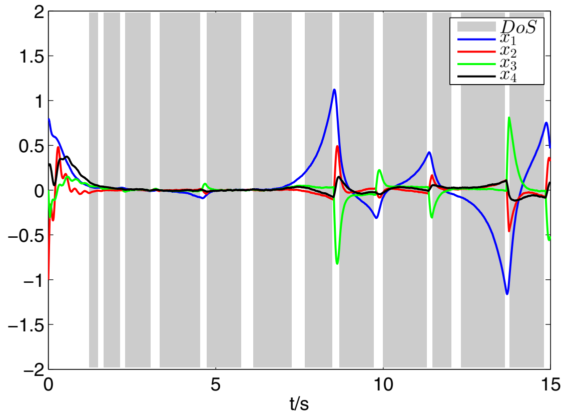

Fig. 12. Simulation results for (39)-(40) in [10].

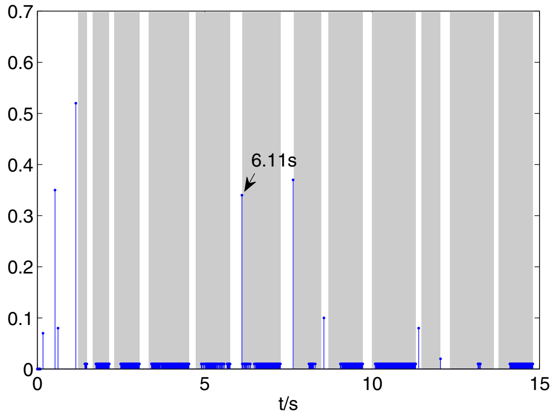

Fig. 13. The inter-event times of the PETC strategy under DoS attacks.

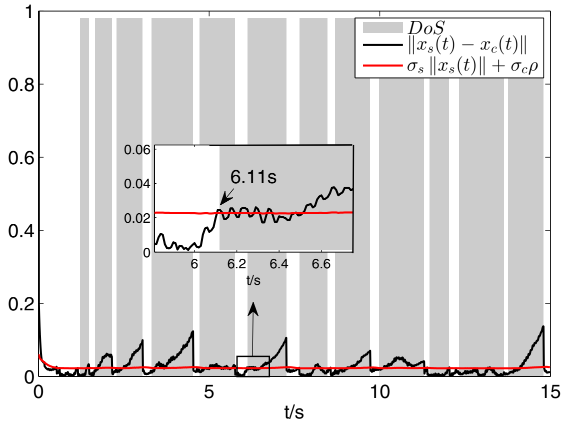

Fig. 14. The evolution of $\|x_s(t) - x_c(t)\|$ and $\sigma_s \|x_s(t)\| + \sigma_c\rho$ under DoS attacks.

error can be restricted by the H_∞ observer. In [9], because of the limitation of inequation (22), only a small part of communication can be jammed. In this paper, this limitation is reduced as shown in the examples. From Fig. 6 and Fig. 11, it can be seen that the PETC strategy proposed in this paper has stronger robustness to the disturbance, noise and DoS attacks. In Fig. 7 and Fig. 13, it can be seen that the PETC strategy in this paper can greatly saving the communication resources, at the same time, the control effect is not compromised.

6. Conclusions

In this paper, the periodic event-triggered control strategy for CPSs under DoS attacks is investigated. An H_∞ observer is used to relax the assumption of full-state information available and restrict the influence of the disturbance and noise. A predictor is designed to predict the system state in the interval between any two continuous event-triggering. Besides, the lower bounded of the inter-event times is obtained to exclude continuous triggering of each verification period. In this way, the transmission interval is extended, and the communication resources are saved. Input-to-state stability analysis is proposed when sufficient condition on the duration and frequency of the DoS attacks is satisfied, and using the upper bound of the prediction error, the conservativeness of the tolerable of DoS attacks is reduced. Finally, a simple numerical simulation and a batch reactor system simulation have been given to illustrate the effectiveness of the proposed control strategy.

Acknowledgement

This work was supported in part by the Funds of the National Natural Science Foundation of China (Grant Nos. 61621004 and 61420106016), and the Research Fund of State Key Laboratory of Synthetical Automation for Process Industries (Grant no. 2013ZCX01).

References

[1] A. Teixeira, I. Shames, H. Sandberg and K. H. Johansson, A secure control framework for resource-limited adversaries, Automatica 51 (2015) 135–148.

[2] H. Sandberg, S. Amin, K. H. Johansson, Cyberphysical Security in networked control systems: An introduction to the issue, IEEE Control Systems Magazines 35 (1) (2015) 20–23.

[3] Y. Yuan, P. Zhang, L. Guo, H. J. Yang, Towards quantifying the impact of randomly occurred attacks on a class of networked control systems, Journal of the Franklin Institute 354 (12) (2017) 4966–4988.

[4] W. Y. Xu, K. Ma, W. Trappe, Y. Y. Zhang, Jamming sensor networks: Attack and defense strategies, IEEE Network 20 (3) (2006) 41–47.

[5] Y. Z. Li, L. Shi, P. Cheng, J. M. Chen, D. E. Quevedo, Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach, IEEE Transactions on Automatic Control 60 (10) (2015) 2831–2836.

[6] H. Zhang, P. Cheng, L. Shi, J. M. Chen, Optimal Denial-of-Service attack scheduling with energy constraint, IEEE Transactions on Automatic Control 60 (11) (2015) 3023–3028.

[7] D. Wang, Z. D. Wang, B. Shen, F. E. Alsaadi, T. Hayat, Recent advances on filtering and control for cyber-physical systems under security and resource constraints, Journal of the Franklin Institute 353 (11) (2016) 2451–2466.

[8] L. Zhao, G. H. Yang, Adaptive sliding mode fault tolerant control for nonlinearly chaotic systems against DoS attack and network faults, Journal of the Franklin Institute 354 (15) (2017) 6520–6535.

[9] C. D. Persis, P. Tesi, Input-to-state stabilizing control under Denial-of-Service, IEEE Transactions on Automatic Control 60 (11) (2015) 2930–2944.

[10] S. Feng, P. Tesi, Resilient control under Denial-of-Service: Robust design, Automatica 79 (2017) 42–51.

[11] S. Feng, P. Tesi. Networked control systems under Denial-of-Service: Co-located vs. remote architures, Systems & Control letters 108 (2017) 40–47.

[12] A. Y. Lu, G. H. Yang, Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial-of-service, IEEE Transactions on Automatic Control DOI: 10.1109/TAC.2017.2751999 (2017).

[13] V. S. Dolk, P. Tesi, C. D. Persis, W. P. M. H. Heemels, Event-triggered control systems under Denial-of-Service attacks, IEEE Transactions on Control of Network Systems 4 (1) (2017) 93–105.

[14] J. Mao, J. Guo, Z. R. Xiang, Sampled-data control of a class of uncertain switched nonlinear systems in nonstrict-feedback form, International Journal of Robust and Nonlinear Control 28 (3) (2018) 918–939.

[15] P. Tabuada, Event-triggered real-time scheduling of stabilizing control tasks, IEEE Transaction Automatic Control 52 (9) (2007) 1680–1684.

[16] D. Yue, E. G. Tian, Q. L. Han, A delay system method for designing event-triggered controllers of networked control systems, IEEE Transactions on Automatic Control 58 (2) (2013) 475–481.

[17] H. Yu, F. Hao, Input-to-state stability of integral-based event-triggered control for linear plants, Automatica 85 (2017) 248–255.

[18] Y. N. Pan, G. H. Yang, Event-triggered fuzzy control for nonlinear networked control systems, Fuzzy Sets and Systems 329 (15) (2017) 91–107.

[19] W. C. Zou, Z. R. Xiang, Event-triggered distributed containment control of heterogeneous linear multi-agent systems by an output regulation approach, International Journal of Systems Science 48 (10) (2017) 2041–2054.

[20] E. G. Tian, D. Yue, Decentralized control of network-based interconnected systems: A state-dependent triggering method, International Journal of Robust and Nonlinear Control 25 (2015) 1126-1144.

[21] W. P. M. H. Heemels, M. C. F. Donkers, A. R. Teel, Periodic event-triggered control for linear systems, IEEE Transaction Automatic Control 58 (4) (2013) 847–861.

[22] M. C. F. Donkers, W. P. M. H. Heemels, Model-based periodic event-triggered control for linear systems, Automatica 49 (2013) 698–711.

[23] T. Strom, On logarithmic norm, SIAM Journal on Numerical Analysis 12 (5) (1975) 741–753.

[24] V. Filipovic, N. Nedic, V. Stojanovic, Robust identification of pneumatic servo actuators in the real situations, Forschung im Ingenieurwesen 75 (2011) 183–196.

[25] V. Stojanovic, N. Nedic, Robust identification of OE model with constrained output using optimal input design, Journal of the Franklin Institute 353 (2016) 576–593.

[26] H. K. Khalil, Nonlinear Systems, New Jersey: Prentice Hall, 2002.

[27] Y. C. Sun, L. N. Yao, Robust fault diagnosis and fault-tolerant control for non-Gaussian uncertain stochastic distribution control systems, International Journal of Robust and Nonlinear Control 27 (10) (2017) 1709-1725.

[28] G. C. Walsh, H. Ye, Scheduling of networked control systems, IEEE Control Systems Magazine 21 (1) (2001) 57–65.