SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

April 2022, Vol. 65 142203:1–142203:15
https://doi.org/10.1007/s11432-020-3190-2

Resilient observer-based event-triggered control for cyber-physical systems under asynchronous denial-of-service attacks

Yifang ZHANG[1], Zheng-Guang WU[1*], Zongze WU[2] & Deyuan MENG[3,4]

[1]*State Key Laboratory of Industrial Control Technology, Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou* 310027*, China;*
[2]*School of Automation, Guangdong University of Technology, Guangzhou* 510006*, China;*
[3]*Seventh Research Division, Beihang University* (*BUAA*)*, Beijing* 100191*, China;*
[4]*School of Automation Science and Electrical Engineering, Beihang University* (*BUAA*)*, Beijing* 100191*, China*

Received 1 September 2020/Revised 16 December 2020/Accepted 2 February 2021/Published online 15 March 2022

Abstract We develop the resilient observer-based event-triggered control update strategy in this paper. It is utilized to achieve the input-to-state stability (ISS) of cyber-physical systems (CPSs) when there is an asynchronous denial-of-service (DoS) attack, which is launched by malicious adversaries both on measurement channel and control channel in a random attack strategy. To estimate the unmeasurable states while saving the limited networked bandwidth, an H_∞ observer-based event-triggered control scheme is first designed to guarantee the ISS of CPSs with economic communication. Moreover, the occurrence of Zeno behavior can be eliminated by providing the existence of a lower positive bound of any two inter-event times. Then, a recursive model of asynchronous DoS attacks is introduced. A resilient control update strategy is proposed and further analyzed to derive the stability criterion of CPSs. At last, a numerical simulation example is given to demonstrate the effectiveness of the introduced control update policy.

Keywords cyber-physical systems, input-to-state stability, asynchronous DoS attacks, H_∞ observer, event-triggered control

Citation Zhang Y F, Wu Z-G, Wu Z Z, et al. Resilient observer-based event-triggered control for cyber-physical systems under asynchronous denial-of-service attacks. Sci China Inf Sci, 2022, 65(4): 142203, https://doi.org/10.1007/s11432-020-3190-2

1 Introduction

In recent years, many researchers have paid great attention to the development of cyber-physical systems (CPSs). CPSs are highly interconnected with physical and networked world through wireless networks. They have been applied to many areas such as power grids, manufacturing, aerospace [1, 2], just to name a few. The communication network through a wireless sensor network is vulnerable to cyber threats and attacks, which makes an impact on the cyber level and physical worlds [3, 4]. Thus it is essential to analyze and synthesize the security problem of CPSs subjected to malicious adversaries.

As mentioned in [5], the major problems of security in CPSs can be categorized as denial-of-service (DoS) attacks [6–11] and deception attacks [12, 13]. In the former scenario, the availability of measurement and actuator data is violated by sending jamming signals, thus preventing the data packet from being successfully sent to its destination. In the latter scenario, the integrity, i.e., trustworthiness of data, is compromised by injecting false data without being detected. Here we focus mainly on the DoS jamming attack scenario because DoS attacks are the easiest form of attacks to implement and common in real life. DoS attacks hamper networked control communication in both measurement and control channels (sensor-control channel and control-actuator channel, respectively). Many significant studies about dynamic systems under DoS jamming attacks have been made. For example, in [6], the DoS jamming attacks restricted to frequency and duration were first characterized. The conditions on frequency and

[*] Corresponding author (email: nashwzhg@zju.edu.cn)

duration are derived to sustain the input-to-state stability (ISS) of the linear system. In [7], following the abovementioned studies, the tolerance of DoS attacks' frequency and duration was maximized as much as possible without violating the stability and robustness of the closed-loop system. In [8], the CPSs with multiple transmission channels under DoS attacks were fully investigated, where the data update policy is derived to sustain the ISS. In [14], the distributed resilient filtering problem was addressed for the power system subjected to DoS attacks that are modeled by Bernoulli distribution.

To alleviate the communication burden and achieve a more efficient utilization of the wireless network resource, event-triggered control (ETC) is proposed to sample and transmit data between units only when the specific event happens, and its advantage lies in reducing unnecessary communication times while maintaining satisfactory system performance [15–21]. Some interesting and significant results associated with ETC have been applied to different control systems such as CPSs [20, 21], multi-agent systems [22–24] and complex networked systems [25,26]. In [20], an event-triggered scheduling stabilizing task on embedded processors was settled, which is the computation core of CPSs. In [21], period ETC was investigated for networked control systems (NCSs) and global exponential stability and L_2-gain performance was achieved. In [27], based on the event-triggered communication protocol, the filtering problem of nonlinear systems was solved. However, it should be stressed that the presented results [20–23, 25, 26] considered an ideal assumption that each unit in CPSs communicates with its neighbors via a secure communication network. Wireless communication networks are vulnerable to cyber-attack, leading to poor performance or even instability. Many studies about systems under attacks are reported. For example, in [28, 29], a dynamic event-triggered control method based on internal variables is designed for nonlinear and linear systems under DoS attacks, respectively. In [30], an ETC is introduced to determine when to broadcast current subsystem's state information to its neighbors in distributed networked systems. In [31], an event-triggered condition and two different switching observers are designed to deal with stability analysis. Nevertheless, the DoS attacks are supposed to be periodic and occur in a known period, which is not practical.

In this study, an observer-based event-triggered control strategy is proposed for a linear CPS under asynchronous DoS attacks, which occur in both the measurement and control channels at different times. Compared with [6, 7], in which the measurement and control channels were interrupted simultaneously, the asynchronous DoS attack model adopted here is more practical because the DoS attacks are different on these channels under many circumstances. Asynchronous DoS attacks are such a class of attacks that the start and duration of an attack on the two channels can be different. Thus, there will be three attack scenarios: only one channel has an attack, neither channel has an attack, or both channels have an attack. The introduction of asynchronous DoS attacks can raise up new challenges to stability analysis. Unlike the DoS attacks in [14, 31] that follow a specific distribution, such as periodic distribution or Bernoulli distribution, the DoS attacks in this paper are restricted to the frequency and duration. On the other hand, most of abovementioned results [6, 28, 29] are based on full-state information to design feedback control laws which are not easy to implement, which motivates us to propose the observer to estimate the physical unmeasurable states. Moreover, the observer-based event-triggered control under asynchronous DoS attacks has not been fully investigated, which motivates this paper.

The main work and contributions of this paper are as follows. First, a system framework containing an H_∞ observer and an event-triggered mechanism is constituted for a linear continuous-time CPS. The event-triggered mechanism is used to save transmission energy. The H_∞ observer is employed to relax the condition of full-state information. Zeno behavior can be excluded by proving that there exists a lower positive bound of inter-event time. Then, asynchronous DoS attacks launched both on control channel and measurement channel are introduced, and an approximate DoS attack model is formulated by the recursive method. A resilient control update strategy is designed to achieve ISS of CPSs under asynchronous DoS attacks, and the stability condition is derived via the Lyapunov function.

2 Framework and problem formulation

Notations. The notations appearing in this paper are quite standard. For a given vector $\upsilon \in \mathbb{R}^n$, $\|\upsilon\|$ is the Euclidean norm; for a given matrix $\varPsi$, $\|\varPsi\|$ stands for its spectrum norm. The superscript "T" of a matrix represents its transpose. $\mathbb{R}$ denotes the set of real numbers and $\mathbb{R}_{\geqslant 0}$ is the set of non-negative real numbers. $\mathbb{R}^m$ denotes the m-dimensional real vector space. $\varPsi \geqslant 0$ (or $\leqslant 0$) means $\varPsi$ is a positive semidefinite (or a negative semidefinite, respectively) matrix. If a function f_1: $\mathbb{R}_{\geqslant 0} \rightarrow \mathbb{R}_{\geqslant 0}$ is continuous

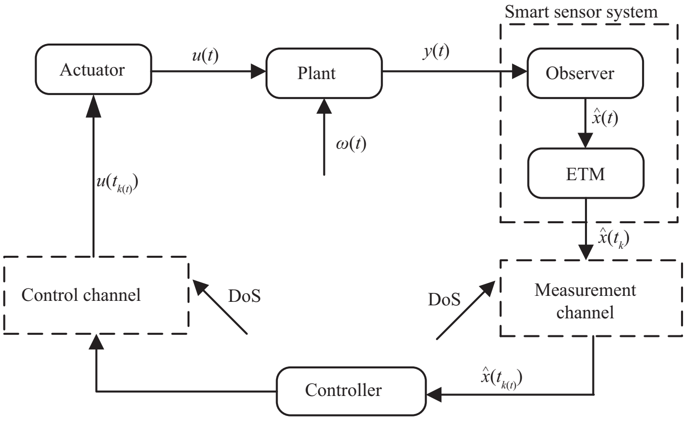

Figure 1 Framework of the system under DoS attacks.

and strictly increasing with $f_1(0) = 0$, then it is said to be of class $\mathcal{K}$. In addition, if $f_1(r) \to \infty$ as $r \to \infty$ holds, f_1 is said to be of $\mathcal{K}_\infty$. A continuous function f_2: $\mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ is said to be of class $\mathcal{KL}$ with $f_2(\cdot, s) \in \mathcal{K}$ for all $s \in \mathbb{R}_{\geqslant 0}$, and for all $r \in \mathbb{R}_{\geqslant 0}$, $f_2(r, \cdot) \in \mathcal{K}$ is strictly decreasing with respect to $f_2(r, s) \to 0$ as $s \to \infty$.

CPSs refer to a new class of systems whose normal functions depend on the close interaction between the physical and cyber worlds. Most CPSs adopt wireless communication to transmit data, which is vulnerable to malicious attacks. The malicious attackers could gain access to the transmission channels to launch DoS attacks [32]. The physical plant description, asynchronous DoS attack strategy, the smart sensor system, and the control objective are presented in this section. The framework of the system is shown in Figure 1.

2.1 Plant description

The linear continuous-time system is described as follows:

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

where $t \geqslant 0$, $x(t) \in \mathbb{R}^n$ is the system state; $u \in \mathbb{R}^{m_u}$ is the control input from the controller; $y(t) \in \mathbb{R}^{m_y}$ is the output measurement sent to the sensor system; A, B and C are the system and control matrices of appropriate size; $\omega(t) \in \mathbb{R}^n$ is the processing input disturbance which is bounded. Suppose that $\{A, B\}$ is stabilizable and $\{A, C\}$ is observable.

2.2 Asynchronous DoS attacks

As shown in Figure 1, the data transmission over a wireless network is vulnerable to DoS attacks. A DoS attack is such a phenomenon that prevents the controller and sensor data from reaching their respective destinations and results in desired data deficient [5], which may degrade the system's performance and even cause instability. Such a phenomenon may be carried out by malicious adversaries in a smart way.

We consider the scenario in which both the measurement channel and control channel are interrupted by DoS attacks asynchronously. Let $\{h_n^i\}_{n\in\mathbb{N}_0}$ denote the DoS attack transition instants, which indicate the switching from a normal state (the DoS attacks are absent and transmission attempts succeed) to an abnormal one (the DoS attacks are present and transmission attempts fail), where $i \in \{1, 2\}$ and $h_0^i \geqslant 0$. $\{h_n^1\}_{n\in\mathbb{N}_0}$ and $\{h_n^2\}_{n\in\mathbb{N}_0}$ are the transition instants for the measurement and control channels, respectively. Then

$$H_n^i = \left\{h_n^i\right\} \cup \left[h_n^i, h_n^i + \tau_n^i\right), \tag{2}$$

where H_n^1 (H_n^2) denotes the n-th DoS attack time interval for the measurement channel (control channel), τ_n^1 (τ_n^2) is the duration time of the n-th DoS attack occurring on the measurement channel (control channel).

Remark 1. The measurement and control channels are interrupted separately and asynchronously. The start and duration of asynchronous DoS attacks on both channels are not necessarily the same, which means that the DoS attacks on these channels are independent and can occur separately. Hence, there are three scenarios: either the measurement channel or control channel is attacked, both channels are attacked, or neither channel is attacked. If $h_n^1 = h_n^2$ and $\tau_n^1 = \tau_n^2$ for all $n \in \mathbb{N}_0$, the DoS attacks on both channels occur simultaneously, which reduces to the case in [6]. If $\tau_n^i = 0$, H_n^i degrades into a single pulse at time h_n^i. Suppose that the time intervals $\{H_n^i\}_{n\in\mathbb{N}_0}$ do not overlap each other.

During the attack period $[t_1, t]$, $0 \leqslant t_1 < t$, let $\Xi^i(t_1, t)$ denote the union of time that the DoS attacks are active and communication is denied, and $\Theta^i(t_1, t)$ is the complementary of $\Xi^i(t_1, t)$, which is the union of time that the DoS attacks are absent and communication is permitted.

$$\Xi^i(t_1,t) = \bigcup_{n\in\mathbb{N}_0} H_n^i \bigcap [t_1, t), \tag{3}$$

$$\Theta^i(t_1,t) = [t_1, t) \backslash \Xi^i(t_1, t). \tag{4}$$

Some appropriate assumptions of DoS attacks are adopted based on the frequency and duration constraints.

Let $n^i(t_1, t)$ denote the number of DoS attack transition instants occurring on the measurement channel $(i = 1)$ and control channel $(i = 2)$ during the time interval $[t_1, t]$.

Assumption 1 (Frequency [6]). For $0 \leqslant t_1 \leqslant t$, there exist $\nu^i \in \mathbb{R}_{\geqslant 0}$, $\tau_D^i \in \mathbb{R}_{>\underline{\Delta}}$, where $\underline{\Delta}$ stands for the lower bound of transmission attempt intervals such that

$$n^i(t_1, t) \leqslant \nu^i + \frac{t - t_1}{\tau_D^i}. \tag{5}$$

Assumption 2 (Duration [6]). For $0 \leqslant t_1 \leqslant t$, there exist $\zeta^i \in \mathbb{R}_{>0}$, $T^i \in \mathbb{R}_{>1}$ such that

$$\left|\Xi^i(t_1, t)\right| \leqslant \zeta^i + \frac{t - t_1}{T^i}. \tag{6}$$

From the above expressions, the attackers do not need to know the system information. Compared to [31], in which the DoS attacks are periodic and the period interval is known, the assumptions in this paper do not follow a specific distribution or pattern and are more practical and meaningful.

Remark 2. Assumptions 1 and 2 are inspired by the idea of the average dwell-time condition introduced in [33] for a hybrid system. These two inequalities exemplify the slow-on-the-average property of DoS attacks. τ_D^i and T^i indicate that the DoS attacks occur more slowly than $\underline{\Delta}$ on average and that the attacks cannot always be active. ν^i and ζ^i are the regularization terms to make sure the assumptions hold. Compared with [6,7], the DoS attacks are not simultaneously launched in the two channels, which introduces a new challenge to stability analysis. To overcome the difficulty in modeling asynchronous DoS attacks and analyzing the stability, the recursive method is used to describe the equivalent attack model in Section 4.

Remark 3. It is necessary to consider both frequency and duration restrictions. Taking the worst situation into account, (1) without a frequency limitation, malicious attackers could launch an infinite number of DoS attacks to interrupt every communication attempt; (2) without a duration limitation, the attackers could launch an attack at the very beginning and it lasts for the whole time, and then all the transmission attempts fail. Therefore, the performance of the system cannot be guaranteed.

2.3 Smart sensor system

In a practical system, it is common that only partial system states are physically measurable, and an observer with great computing power is exploited to estimate the physically unmeasurable states. In addition, to reduce unnecessary transmissions while maintaining the desirable closed-loop system performance and stability, an event-triggered mechanism (ETM) is adopted.

The observer is defined as follows:

$$\begin{aligned} \dot{\hat{x}}(t) &= A\hat{x}(t) + Bu(t) + L\tilde{y}(t), \\ \hat{y}(t) &= C\hat{x}(t), \end{aligned} \tag{7}$$

where $\hat{x}(t) \in \mathbb{R}^n$ is the observer estimated state, $\hat{y}(t) \in \mathbb{R}^{m_y}$ is the observer output, $\tilde{y}(t) = y(t) - \hat{y}(t)$, and L is the observer gain to be designed later.

To save limited bandwidth and achieve economic communication, an ETC is adopted to determine the triggering time sequence $\{t_k\}_{k\in\mathbb{N}_0}$, at each instant of which a control update is sent out. An ETC is proposed to sample and transmit data between units only when the specific event happens, which is concerned with the error $\hat{e}(t)$ and the estimated states. When the error between the current estimated state $\hat{x}$ and the last successfully transmitted estimated state $\hat{x}(t_{k(t)})$ exceeds the threshold on the right-hand side of the inequality in (8), the event-triggered condition, i.e., Eq. (8) is satisfied. Then the event is triggered and the current estimated state $\hat{x}$ is transmitted.

The ETC condition is designed as follows:

$$t_{k+1} = \inf\{t \in \mathbb{R}_{>t_k} | \|\hat{e}(t)\| \geqslant \sigma\|\hat{x}(t)\| + \sigma\|\omega(t)\|_\infty\}, \tag{8}$$

where $\hat{e}(t) = \hat{x}(t_{k(t)}) - \hat{x}(t)$, $\sigma \in (0,1)$,

$$k(t) = \begin{cases} -1, & \text{if } \Theta(0,t) = \emptyset, \\ \sup\{k \in \mathbb{N}_0 | t_k \in \Theta(0,t)\}, & \text{otherwise.} \end{cases} \tag{9}$$

$k(t)$ denotes the last successful update instant. $k(t) = -1$ means that the DoS attack starts at the very beginning and lasts until time t. Under such circumstances, communication is not possible from the start, and we have to assign an initial value for the estimated state $\hat{x}(t_{-1})$. We assume that $\hat{x}(t_{-1}) = 0$ by convention.

$$\Theta(0,t) = (0,t)\backslash\Xi(0,t), \quad \Xi(0,t) = \bigcup_{i=1,2} \Xi^i(0,t),$$

where $\Theta(0,t)$ denotes the healthy intervals in which the communication channels are not attacked. In contrast, $\Xi(0,t)$ denotes the intervals in which at least one of the measurement or control channels is under DoS attacks.

Accordingly, the control input based on ETM can be represented as follows:

$$u(t) = K\hat{x}(t_{k(t)}). \tag{10}$$

Remark 4. In this paper, the packet loss problem is not considered and there is no time delay in the transmitting process. Obviously, when DoS attacks are present, $k(t) \leqslant k$ holds. Note that if $h_n^i = 0$, then $k(0) = -1$, which means that at the process start-up, communication is impossible, and we should assign the initial value to control input $u(t)$. We set $u(0) = 0$ when $h_n^i = 0$.

Suppose that the update sequence has a finite sampling rate, that is, the interval Δ_k between any two adjacent transmission attempt instants satisfies

$$0 < \underline{\Delta} \leqslant \Delta_k = t_{k+1} - t_k \leqslant \bar{\Delta} \tag{11}$$

for all $k \in \mathbb{N}_0$, where $\bar{\Delta}$ and $\underline{\Delta}$ represent the upper bound and lower bound of the transmission attempt interval, respectively. The lower bound is decided later by the event-triggered condition. The upper bound is used to force the ETC to send an estimated state when there is no event triggered for a considerable amount of time.

2.4 Control objective

Definition 1 ([34])**.** Consider the linear continuous-time system (1) under the event-based control input as in (10). If there exist a $\mathcal{KL}$-function f_1 and a $\mathcal{K}_\infty$-function f_2 such that, for each $d(t) \in \mathcal{L}_\infty(\mathbb{R}_{\geqslant 0})$ and $x(0) \in \mathbb{R}^n$,

$$\|x(t)\| \leqslant f_1(\|x(0)\|, t) + f_2(\|d(t)\|_\infty) \tag{12}$$

holds for all $t \in \mathbb{R}_{\geqslant 0}$, then system (1) can achieve ISS.

The problem of designing an observer-based event-triggered control strategy is investigated in this paper. The objective is to achieve ISS for CPSs against smart malicious DoS attacks that are launched both on the measurement and control channels asynchronously.

3 Stability analysis of the observer-based ETC strategy

An H_∞ observer-based ETC strategy is employed. The condition for guaranteeing ISS of the closed-loop system is derived. By providing the existence of the lower positive bound of the inter-event time between any two consecutive triggering instants, the Zeno behavior can be eliminated.

3.1 H_∞ observer

To estimate the physically unmeasurable states, an observer is employed. By adopting the definition of H_∞ performance, the so-called H_∞ observer is designed. The H_∞ performance is defined as $\|e(t)\| < \lambda\|\omega(t)\|_\infty$, where λ is a positive scalar. Let the observation error be $e(t) = x(t) - \hat{x}(t)$. The H_∞ observer can estimate the system states accurately. Then

$$\dot{e}(t) = \Phi_1 e(t) + \omega(t), \tag{13}$$

where $\Phi_1 = A - LC$. By utilizing the bounded real lemma, the gain of the H_∞ observer L can be acquired from the following linear matrix inequality (14), where P_1 is a symmetric positive definite matrix.

$$\begin{bmatrix} \Phi_1^{\mathrm{T}} P_1 + P_1 \Phi_1 & P_1 & I \\ * & -\lambda I & 0 \\ * & * & -\lambda I \end{bmatrix} < 0. \tag{14}$$

3.2 Event-triggered control system

To alleviate the communication burden and achieve a more efficient utilization of the wireless network resources, an event-triggered control (ETC) is proposed to sample and transmit data between units only when the specific event happens. Consider the controlled system (1) under the event-based control input (10) combined with the error $\hat{e}(t)$. Therefore, the closed-loop system (1) can be rewritten as

$$\begin{aligned} &\dot{x}(t) = \Phi x(t) + BK\hat{e}(t) - BKe(t) + \omega(t), \\ &y(t) = Cx(t). \end{aligned} \tag{15}$$

Recalling the definition of $e(t) = x(t) - \hat{x}(t)$, $\Phi = (A + BK)$, where the feedback gain K is designed to ensure that the matrix $(A + BK)$ is Hurwitz.

Consider a quadratic Lyapunov function $V(t) = x^{\mathrm{T}}(t)Px(t)$, where P is a symmetric positive definite matrix.

$$\Phi^{\mathrm{T}} P + P\Phi + Q = 0, \tag{16}$$

where Q is any given positive definite matrix, $Q = Q^{\mathrm{T}} \in \mathbb{R}^{n\times n}$.

For any $t \in \mathbb{R}_{\geqslant 0}$, it is clear that $V(t)$ satisfies the following inequalities:

$$\alpha_1\|x(t)\|^2 \leqslant V(t) \leqslant \alpha_2\|x(t)\|^2, \tag{17a}$$

$$\begin{aligned} \dot{V}(t) \leqslant {} & -\gamma_1\|x(t)\|^2 + \gamma_2\|x(t)\|\|\hat{e}(t)\| \\ & + \gamma_2\|x(t)\|\|e(t)\| + \gamma_3\|x(t)\|\|\omega(t)\|, \end{aligned} \tag{17b}$$

where γ_1 is the smallest eigenvalue of matrix Q, γ_2 equals $\|2PBK\|$, and γ_3 equals $\|2P\|$. α_1 and α_2 are the smallest and largest eigenvalues of matrix P, respectively.

When there is no DoS attack, for any $t \in [t_k, t_{k+1})$, the event-triggered condition is not satisfied, i.e., $\|\hat{e}(t)\| \leqslant \sigma\|\hat{x}(t)\| + \sigma\|\omega(t)\|_\infty$ always holds. The H_∞ performance of the observer is also preserved, that is, $\|e(t)\| < \lambda\|\omega(t)\|_\infty$. Substituting the above two inequalities and inequalities (17a) into (17b), then we can obtain

$$\begin{aligned} \dot{V}(t) &\leqslant -\frac{\gamma_4}{2}\|x(t)\|^2 + \gamma_6\|\omega(t)\|_\infty^2 \\ &\leqslant -\theta_1 V(t) + \gamma_6\|\omega(t)\|_\infty^2, \end{aligned} \tag{18}$$

where $\gamma_4 = \gamma_1 - \sigma\gamma_2$, $\gamma_6 = \gamma_5^2/(2\gamma_4)$, $\gamma_5 = \gamma_2(\sigma + \lambda + \sigma\lambda) + \gamma_3$, $\theta_1 = \gamma_4/(2\alpha_2)$. By comparing the differential inequalities and using the inequality (17a), we can obtain

$$V(t) \leqslant \mathrm{e}^{-\theta_1 t} V(0) + \gamma_7\|\omega(t)\|_\infty^2, \tag{19}$$

$$\|x(t)\| \leqslant \sqrt{\frac{\alpha_2}{\alpha_1}}\mathrm{e}^{-\frac{\theta_1 t}{2}}\|x(0)\| + \sqrt{\frac{\gamma_7}{\alpha_1}}\|\omega(t)\|_\infty, \tag{20}$$

where $\gamma_7 = \gamma_6/\theta_1$.

Based on the above analysis and conclusion from Definition 1, we can prove that if $\gamma_1 - \sigma\gamma_2 > 0$, then the closed-loop system achieves ISS, for any $\underline{\Delta} \leqslant \Delta_k = t_{k+1} - t_k$.

Remark 5. The condition $\gamma_1 - \sigma\gamma_2 > 0$ can be easily satisfied by selecting σ to be sufficiently small and $\gamma_1 > 0$. A similar ETC is considered in [20] for the disturbance-free cases , and the minimum inter-event time is proven to always exist.

Note that the Zeno behavior, i.e., triggering an infinite number of times in a finite amount of time, should be excluded when adopting an ETM. Thus, the triggering instant sequence $\{t_k\}_{k\in\mathbb{N}_0}$ is needed to investigate the possibility of a lower inter-event time while the event-triggered condition holds.

Theorem 1. Consider the linear continuous-time system (1) with the H_∞ observer (7) under the event-based control input (10) and the event-triggered condition (8). When there is no DoS attack, the lower bound of inter-event time $\Delta_k, k \in \mathbb{N}_0$ defined in (11) satisfies

$$\underline{\Delta} = \begin{cases} \frac{\sigma}{\kappa_1(1+\sigma)}, & \mu_A \leqslant 0, \\ \frac{1}{\mu_A}\ln(\frac{\mu_A\sigma}{\kappa_1(1+\sigma)} + 1), & \mu_A > 0, \end{cases} \tag{21}$$

where $\kappa_1 = \max\{\|\Phi\|, \lambda\|LC\|\}$, μ_A is the logarithmic norm of A, and

$$\mu_A = \max\left\{\alpha|\alpha \in \text{spectrum}\left\{\frac{A + A^{\mathrm{T}}}{2}\right\}\right\}. \tag{22}$$

Proof. When there is no DoS attack, any control transmission attempts are successful, that is, $k(t) = k$. For any $t \in [t_k, t_{k+1})$ and $k \in \mathbb{N}_0$, t_k is constant. The dynamics of error $\hat{e}(t)$ satisfies

$$\dot{\hat{e}}(t) = A\hat{e}(t) - \Phi\hat{x}(t_k) - LCe(t). \tag{23}$$

For any $t \in [t_k, t_{k+1})$ and $k \in \mathbb{N}_0$, $\hat{e}(t_k) = 0$. By employing $\|\mathrm{e}^{At}\| \leqslant \mathrm{e}^{\mu_A t}$, for all $t \in \mathbb{R}_{\geqslant 0}$, we can obtain

$$\begin{aligned} \|\hat{e}(t)\| &< \kappa_1 \int_{t_k}^{t} \mathrm{e}^{\mu_A(t-s)}[\|\hat{x}(t_k)\| + \|\omega(t)\|_\infty]\mathrm{d}s \\ &= \kappa_1 g(t-t_k)[\|\hat{x}(t_k)\| + \|\omega(t)\|_\infty], \end{aligned} \tag{24}$$

where $g(t-t_k) = \int_{t_k}^{t} \mathrm{e}^{\mu_A(t-s)}\mathrm{d}s$. Observe that $g(0) = 0$ and $g(t - t_k)$ increases monotonically in terms of time variable t. Let $\Delta = t - t_k$, and then $g(\Delta)$ can be obtained as

$$g(\Delta) = \begin{cases} \Delta, & \mu_A \leqslant 0, \\ \frac{1}{\mu_A}(\mathrm{e}^{\mu_A\Delta} - 1)), & \mu_A > 0. \end{cases} \tag{25}$$

Notice that $\hat{x}(t_k) = \hat{e}(t) + \hat{x}(t)$. We find that

$$\begin{aligned} \|\hat{e}(t)\| \leqslant &\kappa_1 g(t-t_k)\|\hat{e}(t)\| \\ &+ \kappa_1 g(t-t_k)[\|\hat{x}(t_k)\| + \|\omega(t)\|_\infty]. \end{aligned} \tag{26}$$

By combining (25), (26), and the event-triggered condition (8), $\|\hat{e}(t)\|$ satisfies the following inequality:

$$\|\hat{e}(t)\| \leqslant \frac{\kappa_1 g(\Delta)}{1 - \kappa_1 g(\Delta)}(\|\hat{x}(t)\| + \|\omega(t)\|_\infty). \tag{27}$$

Therefore, we can observe that the event-triggered condition (8) cannot be satisfied if $t \in [t_k, t_k + \underline{\Delta})$. Eq. (21) yields the result. Therefore, Zeno behavior can be eliminated. Thus, the proof is complete.

4 Resilient control under DoS attacks

First, we propose the control update policy under DoS jamming attacks. According to time t belonging to different modes, i.e., stable and possibly unstable modes, different update strategies that are resilient to DoS attacks are adopted. Then, we characterize and discuss the class of asynchronous DoS attacks by a recursive method. The main result is derived in this section.

4.1 Resilient control update policy under DoS attacks

Note that under the DoS attacks, the control update data are not available, and we should adopt a suitable switching strategy to achieve resilient control. When there are no DoS attacks, the transmission data attempts are based on the event-triggered condition (28); once an attack occurs, the transfer data update policy is transformed into a periodic update policy with a smaller update interval than the event-based update policy to weaken the influence of the transfer delay induced by the DoS attacks.

Define

$$\varrho_k = \inf \{ t \in \mathbb{R}_{>t_k} | \|\hat{x}(t_k) - \hat{x}(t)\| \geqslant \sigma \|\hat{x}(t)\| + \sigma \|\omega(t)\|_\infty \} \tag{28}$$

for all $k \in \mathbb{N}_0$, where ρ_k is a moment at which the ETC is first satisfied after the communication is restored.

Define a set of integers associated with control update attempt instants that occur under DoS attacks as

$$\psi = \left\{ k \in \mathbb{N}_0 | t_k \in \bigcup_{n \in \mathbb{N}_0} H_n^i \right\}. \tag{29}$$

If ϱ_k occurs in the DoS attack interval, the transmission will fail. For each $k \in \mathbb{N}_0$, the transmission attempt times are given by

$$t_{k+1} = \begin{cases} t_k + \Delta_*, & \text{if } k \in \psi, \\ t_k + \bar{\Delta}, & \text{if } k \notin \psi \wedge \varrho_k - t_k > \bar{\Delta}, \\ \varrho_k, & \text{otherwise}, \end{cases} \tag{30}$$

where Δ_* is the period update interval when t_k belongs to the DoS attack interval, and $0 < \Delta_* < \underline{\Delta}$. $\bar{\Delta}$ is defined as in (11).

Remark 6. The transmission time update intervals correlated to (30) are equal to Δ_*, $\bar{\Delta}$, and $\varrho_k - t_k$ under different circumstances. First, notice that only if $k \notin \psi$ and $\varrho_k - t_k \leqslant \bar{\Delta}$, which means that any transmission attempts do not belong to the DoS attack interval and can be transmitted and triggered successfully, then $t_{k+1} = \varrho_k$. Under such a situation, $\|\hat{x}(t_k) - \hat{x}(t)\| \leqslant \sigma\|\hat{x}(t)\| + \sigma\|\omega(t)\|_\infty$ always holds, since $\hat{e}(t)$ is continuous and $\hat{e}(t_k) = 0$. However, when the inter-event time surpasses the upper bound $\bar{\Delta}$, the next transmission signal will be forced to send at time $t_k + \bar{\Delta}$. If the smart sensor system does not confirm the acknowledgement signal, which indicates that t_k occurs in the active DoS attack interval, the transmission time will be updated at a fixed rate of Δ_* from the moment t_k until the DoS attack ends and the sensor system receives the acknowledgement signal again.

From the perspective of computational complexity, the main concern is the inter-event interval. Based on the proposed resilient control update policy and taking the worst situation into account, whether the system is in an attack zone or a non-attack zone, the control signal updates at the rate of $\underline{\Delta}$. The greater the inter-event time interval is, the lower the computational complexity.

4.2 ISS under DoS attacks

To overcome the difficulty in modeling asynchronous DoS attacks and analyzing the stability, the recursive method is used to describe the equivalent attack model. Consider the time sequence $\{h_m^*\}_{m \in \mathbb{N}_0}$, which is derived from $\{h_n^i\}_{n \in \mathbb{N}_0}$ and τ_n^i $(i = 1, 2)$ as follows by recursive methods:

$$\begin{cases} h_0^* = \min\{h_0^1, h_0^2\}, \\ h_{m+1}^* = \inf_{j \in \mathbb{N}_0} \{h_j^i | h_j^i > h_m^* + \tau_m^*\}, \end{cases} \tag{31}$$

where τ_m^* refers to [29]. Let $H_n^* = \{h_n^*\} \cup [h_n^*, h_n^* + \tau_n^*)$, $\Xi(t_1, t) = \bigcup_{n \in \mathbb{N}_0} H_n \bigcap [t_1, t]$.

Owing to the DoS-induced delay, the transmission attempts cannot be immediately updated after the DoS attacks end. First, divide the time sequence into intervals where the system is in a stable mode that there are no DoS jamming attacks launched in both channels, and intervals where the system may be in an unstable mode that at least one channel is attacked. Taking the worst situation into consideration, the DoS attack transition instant happens to meet the moment of transmission attempt, which will cause a DoS-induced delay Δ_*. Thus, based on the above analysis, we need to reconsider the time sequence and decompose it into effective DoS attack intervals $\bar{H}_n^*$, which consist of H_n^* and the DoS-induced delay Δ_*, and healthy intervals over which the condition $\|\hat{x}(t_k) - \hat{x}(t)\| \leqslant \sigma\|\hat{x}(t)\| + \sigma\|\omega(t)\|_\infty$ always holds.

Let

$$\delta_n = \begin{cases} \tau_n^*, & \text{if } \psi = \emptyset, \\ t_{\sup\{k\in\mathbb{N}_0 | k\in\psi\}} - h_n^*, & \text{otherwise.} \end{cases} \tag{32}$$

Therefore, the effective DoS attack intervals are given as follows:

$$\bar{H}_n^* = \{h_n^*\} \cup [h_n^*, h_n^* + \delta_n + \Delta_*) \,. \tag{33}$$

Note that adjacent time intervals may overlap. For the convenience of stability analysis, we can treat these overlaps as a single DoS sub-interval. Define an auxiliary sequence $\{\xi_m\}_{m\in\mathbb{N}_0}$ as the transition intervals of the effective DoS attacks obtained recursively from h_n^*:

$$\begin{cases} \xi_0 = h_0^*, \\ \xi_{m+1} = \inf\left\{h_n^* > \xi_m | h_n^* > h_{n-1}^* + \delta_{n-1} + \Delta_*\right\} \end{cases} \tag{34}$$

for all $m \in \mathbb{N}$, and define the length of the m-th interval of the effective DoS attacks as

$$v_m = \sum_{\substack{n\,\in\,\mathbb{N}_0 \\ \xi_m\,\leqslant\,h_n^*\,<\,\xi_{m+1}}} |\bar{H}_n^* \backslash \bar{H}_{n+1}^*|, \tag{35}$$

where $\xi_{-1} = 0, v_{-1} = 0$. Therefore, we can construct effective DoS attack intervals as Z_m and healthy intervals as W_m listed as follows:

$$Z_m = \{\xi_m\} \cup [\xi_m, \xi_m + v_m) \,, \tag{36}$$

$$W_m = \{\xi_m + v_m\} \cup [\xi_m + v_m, \xi_{m+1}) \,. \tag{37}$$

During the period $[t_1, t]$, let $\bar{\Xi}(t_1, t)$ denote the union set of the time that the DoS attacks are effective, and $\bar{\Theta}(t_1, t)$ is the complement of $\bar{\Xi}(t_1, t)$, the union of healthy intervals. Through construction, the last successful control update occurs at time $\xi_m + v_m$ for each $m \in \mathbb{N}_0$.

$$\bar{\Xi}(t_1, t) = \bigcup_{m\in\mathbb{N}_0} Z_m \bigcap [t_1, t], \tag{38}$$

$$\bar{\Theta}(t_1, t) = \bigcup_{m\in\mathbb{N}_0} W_m \bigcap [t_1, t]. \tag{39}$$

According to Assumptions 1 and 2, it follows that

$$\begin{aligned} |\bar{\Xi}(t_1, t)| &\leqslant |\Xi(t_1, t)| + (1 + n(t_1, t))\Delta_* \\ &\leqslant \zeta^1 + \zeta^2 + \frac{t - t_1}{T^1} + \frac{t - t_1}{T^2} \\ &\quad + \left(1 + \nu^1 + \nu^2 + \frac{t - t_1}{\tau_D^1} + \frac{t - t_1}{\tau_D^2}\right)\Delta_* \\ &= \zeta + \frac{t - t_1}{T}, \end{aligned} \tag{40}$$

where $\zeta = \zeta^1 + \zeta^2 + (1 + \nu^1 + \nu^2)\Delta_*$, $\frac{1}{T} = \frac{1}{T^1} + \frac{1}{T^2} + \frac{\Delta_*}{\tau_D^1} + \frac{\Delta_*}{\tau_D^2}$.

In terms of whether the time belongs to the effective DoS attack intervals, we decompose the time axis into two modes, and then we analyze the closed-loop system stability switching between stable dynamics and possible unstable dynamics.

Theorem 2. Consider the linear continuous-time system (1) and the H_∞ observer (7) under the event-based control input (10), where there exists a feedback gain K such that the matrix $(A + BK)$ is Hurwitz along with the event-triggered condition (8) with $\gamma_1 - \sigma\gamma_2 > 0$. For asynchronous DoS jamming attacks meeting the Assumptions 1 and 2 for any ζ^i, ν^i, T^i and τ_D^i such that

$$\frac{1}{T^1} + \frac{1}{T^2} + \frac{\Delta_*}{\tau_D^1} + \frac{\Delta_*}{\tau_D^1} < \frac{\theta_1}{\theta_1 + \theta_2}, \tag{41}$$

where $0 < \Delta_* < \underline{\Delta}$, the ISS is preserved for the closed-loop system under the resilient control update strategy (30).

Proof. For the sake of simplicity, let us divide the discussion into two steps.

Step I. During effective DoS attack intervals $[\xi_m, \xi_m + v_m)$ and healthy intervals $[\xi_m + v_m, \xi_{m+1})$, stability analysis of the system is studied, respectively.

Case 1. $t \in W_m, m \in \mathbb{N}_0$, where $\|\hat{x}(t_k) - \hat{x}(t)\| \leqslant \sigma\|\hat{x}(t)\| + \sigma\|\omega(t)\|_\infty$ remains true. Then from inequality (19), it can be derived that

$$V(x(t)) \leqslant \mathrm{e}^{-\theta_1(t-\xi_m-v_m)} V(x(\xi_m + v_m)) + \gamma_7\|\omega(t)\|_\infty^2, \tag{42}$$

where $\theta_1 = \frac{\gamma_1 - \sigma\gamma_2}{2\alpha_2}, \gamma_7 = \frac{(\gamma_2(\sigma+\lambda+\sigma\lambda)+\gamma_3)^2}{(\gamma_1-\sigma\gamma_2)^2}$.

Case 2. $t \in Z_m, m \in \mathbb{N}_0$, where $\|\hat{x}(t_{k(t)}) - \hat{x}(t)\| \leqslant \sigma\|\hat{x}(t)\| + \sigma\|\omega(t)\|_\infty$ may not hold. Recall that

$$\hat{e}(t) = \hat{x}(t_{k(\xi_m)}) - \hat{x}(t), \tag{43}$$

where $\hat{x}(t_{k(\xi_m)})$ denotes the last successfully transmitted estimated state up to the time ξ_m. By the continuity of $\hat{x}$, we can obtain that

$$\hat{e}(\xi_m) \leqslant \sigma\|\hat{x}(\xi_m)\| + \sigma\|\omega(t)\|_\infty. \tag{44}$$

Hence, for all $m \in \mathbb{N}_0$,

$$\|\hat{x}(t_{k(\xi_m)})\| \leqslant (1+\sigma)\|\hat{x}(\xi_m)\| + \sigma\|\omega(t)\|_\infty. \tag{45}$$

So, for $t \in Z_m$, $\hat{e}(t)$ satisfies

$$\|\hat{e}(t)\| \leqslant (1+\sigma)\|\hat{x}(\xi_m)\| + \|\hat{x}(t)\| + \sigma\|\omega(t)\|_\infty. \tag{46}$$

Then substituting (46) into (17b), similar to the derivation of ISS in Section 3 and $\gamma_1 - \sigma\gamma_2 > 0$, we can obtain the following inequality:

$$\begin{aligned}\dot{V}(t) \leqslant\ & (\gamma_2 - \gamma_1)\|x(t)\|^2 + \gamma_1(1+\sigma)\|x(\xi_m)\| \\ & + [\gamma_2(\sigma + \sigma\lambda + 3\lambda)]\|x(t)\|\|\omega(t)\|_\infty, \\ \leqslant\ & \theta_2 \max\{V(x(\xi_m)), V(x(t))\} + \gamma_8\|\omega(t)\|_\infty^2,\end{aligned} \tag{47}$$

where $\theta_2 = 2\gamma_2/\alpha_1$,$\gamma_8 = \frac{[\gamma_2(\sigma+\sigma\lambda+3\lambda)]^2}{2(\gamma_1-\sigma\gamma_2)}$. For $t \in Z_m$, by the comparison of differential inequalities, we can get

$$V(x(t)) \leqslant \mathrm{e}^{\theta_2(t-\xi_m)} V(x(\xi_m)) + \gamma_9 \mathrm{e}^{\theta_2(t-\xi_m)}\|\omega(t)\|_\infty^2, \tag{48}$$

where $\gamma_9 = \gamma_8/\theta_2$.

Step II. For all $t \in \mathbb{R}_{\geqslant 0}$, the stability analysis of the closed-loop system is investigated. Combining (42) and (48), by iterations, it can be obtained that

$$\begin{aligned}V(x(t)) \leqslant\ & \mathrm{e}^{-\theta_1|\bar{\Xi}(0,t)|}\mathrm{e}^{\theta_2|\bar{\Theta}(0,t)|}V(x(0)) \\ & + \gamma_*\left(1 + 2\sum_{\substack{m\,\in\,\mathbb{N}_0\\ \xi_m\,\leqslant\,t}} \mathrm{e}^{-\theta_1|\bar{\Xi}(\xi_m+v_m,t)|}\mathrm{e}^{\theta_2|\bar{\Theta}(\xi_m,t)|}\right)\|\omega(t)\|_\infty^2,\end{aligned} \tag{49}$$

where $\gamma_* = \max\{\gamma_7, \gamma_9\}$.

First, we will address the sum term, when $t \in Z_m, t \leqslant \xi_m + v_m$. According to the definitions of $\bar{\Theta}$ and $\bar{\Xi}$, we have that

$$|\bar{\Xi}(\xi_m, t)| = t - \xi_m, \quad |\bar{\Theta}(\xi_m + v_m, t)| = 0. \tag{50}$$

When $t \in W_m, t \geqslant \xi_m + v_m$, $|\bar{\Xi}(\xi_m, t)| = v_m + |\bar{\Xi}(\xi_m + v_m, t)|$, we have

$$\begin{aligned}|\bar{\Theta}(\xi_m + v_m, t)| &= t - \xi_m - v_m - |\bar{\Xi}(\xi_m + v_m, t)| \\ &= t - \xi_m - |\bar{\Xi}(\xi_m, t)|.\end{aligned} \tag{51}$$

It is easy to obtain the following sum term by integrating (40) and (51):

$$\sum_{\substack{m\,\in\,\mathbb{N}_0\\ \xi_m\,\leqslant\,t}} \mathrm{e}^{-\theta_1|\bar{\Xi}(\xi_m+v_m,t)|}\mathrm{e}^{\theta_2|\bar{\Theta}(\xi_m,t)|} = \mathrm{e}_*^{\varsigma} \sum_{\substack{m\,\in\,\mathbb{N}_0\\ \xi_m\,\leqslant\,t}} \mathrm{e}^{-(t-\xi_m)\theta_*}, \tag{52}$$

where $\varsigma_* = (\theta_1+\theta_2)\varsigma$, $\theta_* = \theta_1 - \frac{\theta_1+\theta_2}{T} > 0$ from (41). From the result of [6], we obtain

$$\sum_{\substack{m\,\in\,\mathbb{N}_0\\ \xi_m\,\leqslant\,t}} \mathrm{e}^{-(t-\xi_m)\theta_*} \leqslant \frac{\mathrm{e}^{\theta_*(\tau_D^1+\tau_D^2)(\nu^1+\nu^2)}}{1-\mathrm{e}^{-\theta_*(\tau_D^1+\tau_D^2)}}. \tag{53}$$

Then, $t\in\mathbb{R}_{\geqslant 0}$, and we observe that the inequality (49) is satisfied:

$$\begin{aligned} V(x(t)) &\leqslant \mathrm{e}^{\varsigma_*}\mathrm{e}^{-t\theta_*}V(x(0)) \\ &\quad + \gamma_*\left[1+2\mathrm{e}^{\varsigma}\frac{\mathrm{e}^{\theta_*(\tau_D^1+\tau_D^2)(\nu^1+\nu^2)}}{1-\mathrm{e}^{-\theta_*(\tau_D^1+\tau_D^2)}}\right]\|\omega(t)\|_\infty^2. \end{aligned} \tag{54}$$

Using inequalities (17a) and $a^2+b^2\leqslant(a+b)^2$, it can be obtained that

$$\begin{aligned} \|x(t))\| &\leqslant \sqrt{\frac{\alpha_2}{\alpha_1}}\mathrm{e}^{\frac{\varsigma_*}{2}}\mathrm{e}^{-(\theta_*/2)t}x(0) \\ &\quad + \sqrt{\frac{\gamma_*}{\alpha_1}}\left[1+2\frac{\mathrm{e}^{\theta_*(\tau_D^1+\tau_D^2)(\nu^1+\nu^2)}}{1-\mathrm{e}^{-\theta_*(\tau_D^1+\tau_D^2)}}\right]^{\frac{1}{2}}\|\omega(t)\|_\infty. \end{aligned} \tag{55}$$

From (55), we find that the multiplier factor is independent of the input disturbance and initial state. According to Definition 1, the ISS is achieved.

Remark 7. We observe that for the inequality (55), decreasing Δ_* will elevate the ability to tolerate more (time and frequency) DoS attacks and increase the decay rate when other conditions hold.

5 Numerical simulation

The validity of the proposed results is verified by a numerical simulation. Consider a system that is open-loop and unstable as follows:

$$\begin{aligned} \dot{x}(t) &= \begin{bmatrix}1&1\\0&1\end{bmatrix}x(t)+\begin{bmatrix}1&0\\0&1\end{bmatrix}u(t)+\omega(t), \\ y(t) &= \begin{bmatrix}1&0\\0&1\end{bmatrix}x(t). \end{aligned} \tag{56}$$

The processing input disturbance $\omega(t)$ is a random signal that is uniformly distributed in $[-0.5, 0.5]$. The initial value of the state and the estimated state are $x(0)=\hat{x}(0)=[2\ \ -2]$. Set the pole assignment as $[-3.5\ \ -4]$ and the H_∞ performance index $\lambda=1.2$. By solving the LMI (14), we can get the feedback gain K and observer gain matrix L as

$$K=\begin{bmatrix}-4.5&-1.0\\0&-5.0\end{bmatrix},\quad L=\begin{bmatrix}10.42&8.75\\7.89&12.32\end{bmatrix}.$$

First, we analyze the stability of the controlled system on the basis of the H_∞ observer and ETC strategy when there are no DoS attacks. By solving the Lyapunov function (16) and setting Q as an identity matrix, we can obtain that $\alpha_1=0.3603$, $\alpha_2=0.4116$, $\gamma_1=1$, $\gamma_2=4.0916$, $\gamma_3=0.8232$, and the logarithmic norm of A is $\mu_A=1.5$. To achieve ISS, σ must be selected as $\sigma<0.1518$, so we choose $\sigma=0.08$. By Theorem 1, we can get that the lower bound of the inter-event time is $\underline{\Delta}=0.003$.

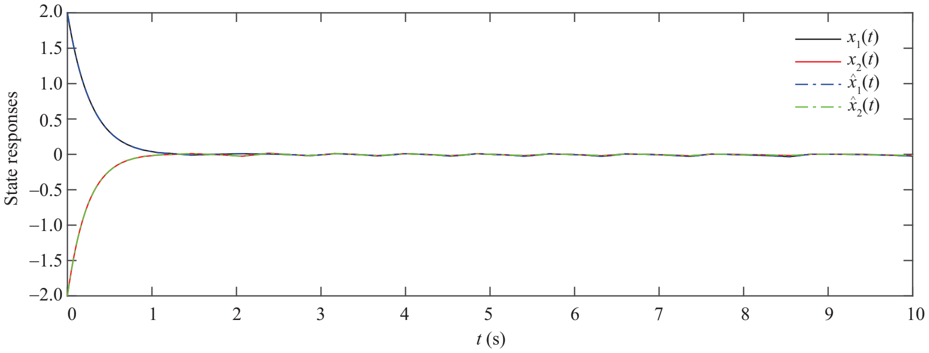

Figure 2 (Color online) State response trajectories.

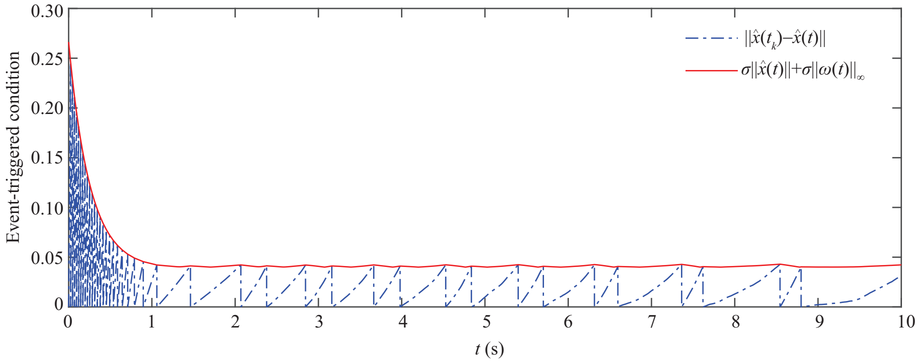

Figure 3 (Color online) The evolution of event-triggered condition.

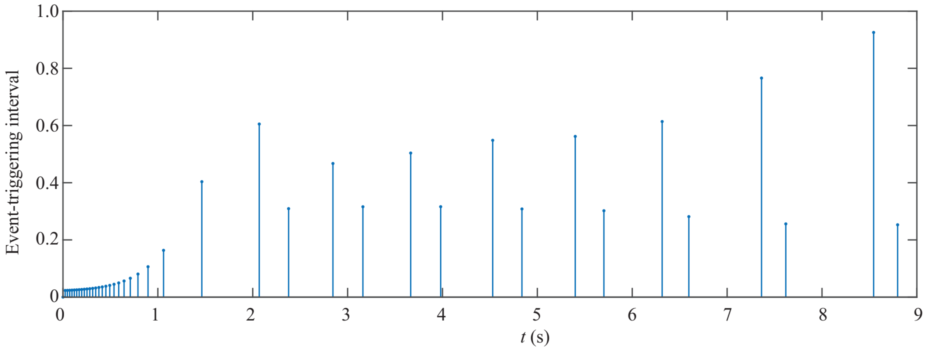

Figure 4 (Color online) The inter-time of event-triggered strategy.

When DoS attacks are not active, according to the stability analysis in Section 3, the state responses and estimated states are presented in Figure 2. The H_∞ observer can estimate the system states perfectly.

Figure 3 shows the trajectories of $\|\hat{x}(t_k)-\hat{x}(t)\|$ and $\sigma\|\hat{x}(t)\|+\sigma\|\omega(t)\|_\infty$. It is observed that the error never exceeds the threshold. Figure 4 demonstrates the inter-event intervals. The ETC can not only assure the stability performance of the controlled system, but also effectively save the communication resources.

When DoS attacks occur and satisfy Assumptions 1 and 2, the resilient control update policy is as (30). Based on the above analysis, $\frac{\theta_1}{\theta_1+\theta_2}=0.0347$, so we choose $\Delta_*=0.002$. In Figures 5–8, the legends Attack I and Attack II indicate the DoS attacks launched in the measurement channel and the control channel, respectively. Attack I/II represents the overlapping time interval between the two channels.

From Figures 5 and 6, we can observe that the control update strategy proposed in (30) is resilient to asynchronous DoS attacks and processing disturbances. And the error between the estimated states of the H_∞ observer and the system states is far below the threshold so that the proposed H_∞ observer can estimate the closed-loop system perfectly. From Figures 7 and 8, although the value of $\|\hat{x}(t_k)-\hat{x}(t)\|$ will exceed the value of $\sigma\|\hat{x}(t)\|+\sigma\|\omega(t)\|_\infty$, during the DoS attack periods, once the DoS attacks stop

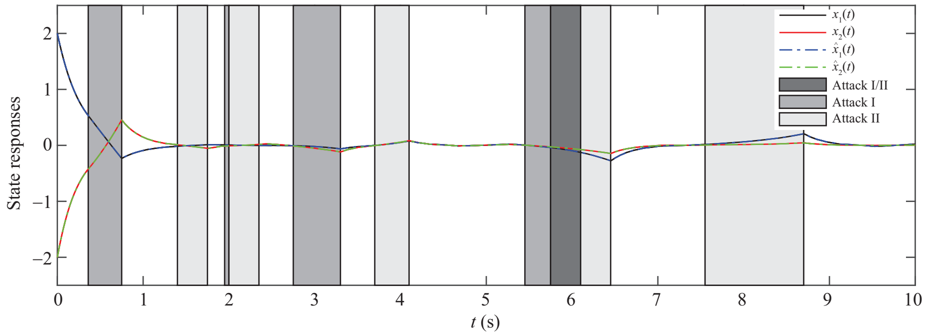

Figure 5 (Color online) The state trajectories under DoS attacks.

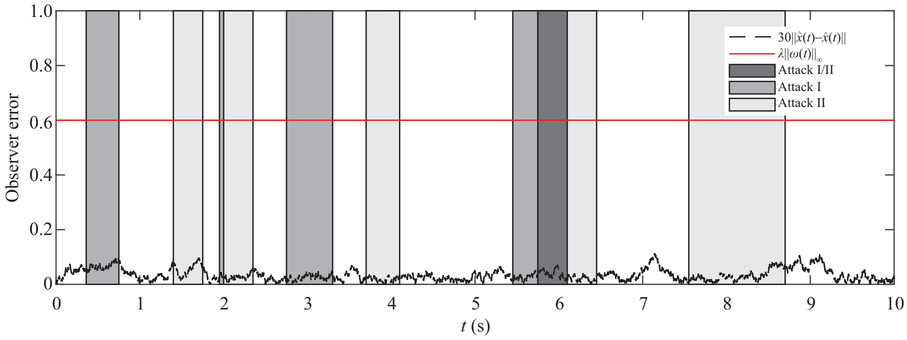

Figure 6 (Color online) The observer errors and the threshold.

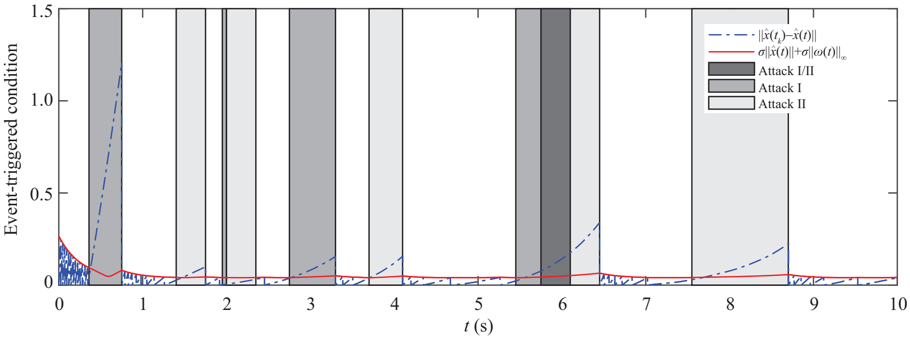

Figure 7 (Color online) The evolution of event-triggered condition under DoS attacks.

and the DoS-induced delay ends, the transmission attempts recover and succeed, and $\|\hat{x}(t_k)-\hat{x}(t)\| \leqslant \sigma\|\hat{x}(t)\|+\sigma\|\omega(t)\|_\infty$ holds again.

It can be seen that when a DoS attack transition occurs, the value of $\|\hat{x}(t_k)-\hat{x}(t)\|$ may still be smaller than the value of $\sigma\|\hat{x}(t)\|+\sigma\|\omega(t)\|_\infty$. The event has not yet been triggered until it meets the condition (28), but owing to the interruption caused by the DoS attacks, the communication cannot be reached. Then the smart sensor system will adopt the update policy and transmit data periodically with $\Delta_*=0.002$, where a shorter period leads to a shorter DoS-induced delay. When the first successful attempt is made after the DoS attacks, the system returns to normal and adopts a control update strategy again. The ETC strategy can reduce the communication times while preserving the controlled system stability even when DoS jamming attacks occur.

6 Conclusion

The problem of the resilient observer-based event-triggered control update strategy is investigated for CPSs subjected to asynchronous DoS jamming attacks restricted to frequency and duration. An H_∞ observer is used to estimate the system states that cannot be measured in practice. An ETC strategy is

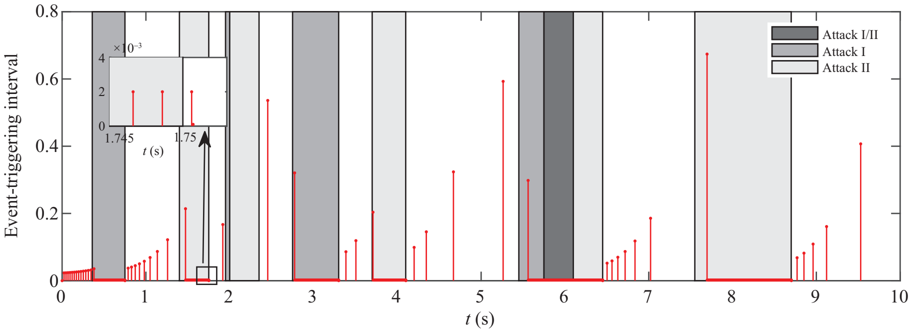

Figure 8 (Color online) The inter-time of event-triggered strategy under DoS attacks.

utilized to reduce unnecessary transmission in order to save limited bandwidth.

Based on the observer-based event-triggered model, we first analyze the stability of the closed-loop system in the absence of DoS attacks. Then we get the condition guaranteeing ISS and exclude Zeno behavior. Under DoS attacks, we adapt the control update policy to be resilient to the DoS attacks and figure out how many DoS attacks can be tolerated without losing ISS. At last, a numerical simulation is given as an example to verify the proposed methods and the validity of the proposed control update strategy. As for further research, we will focus on the effect of some common problems during information transmission, such as delay, packet losses, and quantization errors, and we will consider various engineering systems under DoS attacks, such as power systems, sensor networks, multi-agent systems, and nonlinear systems.

References

1 Schenato L, Sinopoli B, Franceschetti M, et al. Foundations of control and estimation over lossy networks. Proc IEEE, 2007, 95: 163–187

2 Ye Z, Zhang D, Wu Z G. Adaptive event-based tracking control of unmanned marine vehicle systems with DoS attack. J Franklin Institute, 2021, 358: 1915–1939

3 Teixeira A, Sou K C, Sandberg H, et al. Secure control systems: a quantitative risk management approach. IEEE Control Syst, 2015, 35: 24–45

4 de Sá A O, Carmo L F R C, Machado R C S. Covert attacks in cyber-physical control systems. IEEE Trans Ind Inf, 2017, 13: 1641–1651

5 Teixeira A, Shames I, Sandberg H, et al. A secure control framework for resource-limited adversaries. Automatica, 2015, 51: 135–148

6 de Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. IEEE Trans Automat Contr, 2015, 60: 2930–2944

7 Feng S, Tesi P. Resilient control under denial-of-service: robust design. Automatica, 2017, 79: 42–51

8 Lu A Y, Yang G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Trans Automat Contr, 2018, 63: 1813–1820

9 An L, Yang G H. Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks. IEEE Trans Cybern, 2019, 49: 827–838

10 Sun Q, Zhang K, Shi Y. Resilient model predictive control of cyber-physical systems under DoS attacks. IEEE Trans Ind Inf, 2020, 16: 4920–4927

11 Xu Y, Fang M, Pan Y J, et al. Event-triggered output synchronization for nonhomogeneous agent systems with periodic denial-of-service attacks. Int J Robust Nonlin Control, 2020, 63: rnc.5223

12 Ding D, Wang Z, Han Q L, et al. Security control for discrete-time stochastic nonlinear systems subject to deception attacks. IEEE Trans Syst Man Cybern Syst, 2018, 48: 779–789

13 Liu Y, Reiter M K, Ning P. False data injection attacks against state estimation in electric power grids. In: Proceedings of the ACM Conference on Computer and Communications Security, Chicago, 2009

14 Chen W, Ding D, Dong H, et al. Distributed resilient filtering for power systems subject to denial-of-service attacks. IEEE Trans Syst Man Cybern Syst, 2019, 49: 1688–1697

15 Heemels W P M H, Johansson K H, Tabuada P. An introduction to event-triggered and self-triggered control. In: Proceedings of IEEE 51st IEEE Conference on Decision and Control (CDC), 2012. 3270–3285

16 Chen Z, Han Q-L, Yan Y M, et al. How often should one update control and estimation: review of networked triggering techniques. Sci China Inf Sci, 2020, 63: 150201

17 Girard A. Dynamic triggering mechanisms for event-triggered control. IEEE Trans Automat Contr, 2015, 60: 1992–1997

18 Chen X L, Wang Y G. Event-triggered attack-tolerant tracking control design for networked nonlinear control systems under DoS jamming attacks. Sci China Inf Sci, 2020, 63: 150207

19 Gao Y F, Sun X M, Du X, et al. Event-based triggering mechanisms for nonlinear control systems. Sci China Inf Sci, 2020, 63: 150209

20 Tabuada P. Event-triggered real-time scheduling of stabilizing control tasks. IEEE Trans Automat Contr, 2007, 52: 1680–1685

21 Heemels W P M H, Donkers M C F, Teel A R. Periodic event-triggered control for linear systems. IEEE Trans Automat Contr, 2013, 58: 847–861

22 Yi X, Liu K, Dimarogonas D V, et al. Distributed dynamic event-triggered control for multi-agent systems. In: Proceedings of IEEE 56th Annual Conference on Decision and Control (CDC), 2017. 6683–6698

23 Xu Y, Wu Z G. Distributed adaptive event-triggered fault-tolerant synchronization for multiagent systems. IEEE Trans Ind Electron, 2021, 68: 1537–1547

24 Dong S L, Chen G R, Liu M Q, et al. Cooperative neural-adaptive fault-tolerant output regulation for heterogeneous nonlinear uncertain multiagent systems with disturbance. Sci China Inf Sci, 2021, 64: 172212

25 Zou L, Wang Z, Gao H, et al. Event-triggered state estimation for complex networks with mixed time delays via sampled data information: the continuous-time case. IEEE Trans Cybern, 2015, 45: 2804–2815

26 Li H, Liao X, Chen G, et al. Event-triggered asynchronous intermittent communication strategy for synchronization in complex dynamical networks. Neural Netw, 2015, 66: 1–10

27 Ding D, Wang Z, Han Q L. A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks. IEEE Trans Automat Contr, 2020, 65: 1792–1799

28 Dolk V S, Tesi P, de Persis C, et al. Event-triggered control systems under denial-of-service attacks. IEEE Trans Control Netw Syst, 2017, 4: 93–105

29 Zhang Z-H, Liu D, Deng C, et al. A dynamic event-triggered resilient control approach to cyber-physical systems under asynchronous DoS attacks. Inf Sci, 2020, 519: 260–272

30 Wang X, Lemmon M D. Event-triggering in distributed networked systems with data dropouts and delays. In: Hybrid Systems: Computation and Control. Berlin: Springer, 2009. 366–380

31 Hu S L, Yue D, Han Q-L, et al. Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. IEEE Trans Cybern, 2020, 50: 1952–1964

32 Wen G H, Yu W W, Yu X H, et al. Complex cyber-physical networks: from cybersecurity to security control. J Syst Sci Complex, 2017, 30: 46–67

33 Hespanha J P, Morse A S. Stability of switched systems with average dwell-time. In: Proceedings of the 38th IEEE Conference on Decision and Control, 1999. 3: 2655–2660

34 Jiang Z P, Wang Y. Input-to-state stability for discrete-time nonlinear systems. Automatica, 2001, 37: 857–869