KYBERNETIKA — VOLUME *56* (2020), NUMBER 2, PAGES 340–362

EVENT-TRIGGERED CONTROL OF CYBER-PHYSICAL SYSTEMS UNDER ASYNCHRONOUS DENIAL OF SERVICE ATTACKS

Huaye Peng, Chen Peng, Yong Shao, and Deliang Zeng

This paper addresses event-triggered control cyber-physical systems under asynchronous denial of service attacks. First, a general attack model is given, which allows us to conveniently model the asynchronous denial of service attacks within measurement and control channels in a unified framework. Then, under a delicate event triggered communication mechanism, a refined switching control mechanism is proposed to account for various attack intervals and non-attack intervals. Furthermore, sufficient conditions are derived for guaranteeing the input to state stability (ISS) of the resulting closed-loop system. Finally, a simulation example of unmanned ground vehicle (UGV) is given to demonstrate the validity of the proposed main results.

Keywords: DoS attack, event-triggered mechanism, cyber-physical system

Classification: 93A99

1. INTRODUCTION

In recent years, due to the computer's computing processing capabilities and the long-distance communication capabilities of communication networks, cyber-physical systems that combine computing sources, communication networks, and physical objects have received increasing attention [5, 14, 26, 27, 33]. Numerous practical applications, such as smart grids, water distribution systems and unmanned ground vehicles, have testified the prospects of cyber-physical systems in modern critical infrastructure. However, due to the openness and insufficient protection of various communication networks [34], the reliability of communication is generally difficult to guarantee during the operation and control of the physical object. It is thus possible that real-world attackers can launch malicious cyber attacks on the network medium [7]. The occurrences of cyber attacks can often lead to damages or even collapses of physical objects [23, 20]. This has been fully demonstrated in recent years such as the StuxNet computer worm [6] and the Ukrainian blackout [16]. Therefore, the security control problem of cyber-physical systems has received intensive attention in recent several years, see, e. g., [1, 2, 3, 21] and the references therein.

DOI: 10.14736/kyb-2020-2-0340

Among the many types of cyber attacks, there are two main categories that have been widely studied: *false data injection attacks* and *denial of service (DoS) attacks*. There are fruitful results dealing with such a type of attacks in different cyber-physical systems, see, e. g., [4, 10, 15, 31, 32] and the references therein. The latter is a more common and easy-to-implement type of attacks, mainly causing congestion in the communication network and resulting in prevented data exchanges or data losses among distributed system components [27, 35]. DoS attacks can either interrupt the sensor channels [18], block the acquisition of sensor data, or block both the sensor channels and the controller channels [27]. As testified by the networked control literature, an event-triggered mechanism provide an effective and efficient solution for reducing the frequency of sensor/controller data packet transmissions or updates [8, 9, 11, 19, 22, 30], thus potentially contributing to the saving of limited communication resources in practical networked systems. There is no doubt that employing suitable event-triggered mechanism to deal with DoS attacks for practical networked systems is also an interesting research topic in the control society [13, 25]. For example, to combat DoS attacks with limited energy, a resilient trigger mechanism is designed for load frequency control (LFC) in [24]. An observer-based event trigger control mechanism is proposed in [12] under consideration of the periodic congestion attacks. However, the above results require that the DoS attacks occur at the same time when data are transmitted over the communication channels from the sensor to the controller and the controller to the actuator [29], thereby leading to the so-called synchronous DoS attacks. From the perspective of the system designers, such a requirement may facilitate the analysis and design of practical networked systems. However, this may also increase the detectability of such attacks and thus the possibility of being removed by the system designers, which violates the intension of a real-world cunning attacker. A more practical scenario is that a sophisticated adversary launches asynchronous DoS attacks on the sensor-to-controller communication channel and the controller-to-actuator communication channel to disrupt the data exchanges. How to further the research of secure control for practical cyber-physical systems motivates the current study.

Under consideration of the asynchronous attacks in the communication channels from the sensor to the controller and the controller to the actuator, a unified model for asynchronous denial of service attacks is firstly established, which is inspired by [27] and [12]. Then under a carefully designed event-triggered communication scheme, a refined switching control mechanism is proposed to deal with the attack interval and non-attack interval respectively. Two sufficient conditions are further derived for guaranteing the input to state stability (ISS) of studied system. Compared with some existing works, the main contributions of this paper are summarized as follows:

1) An asynchronous attack model has been introduced to make the attack model more general. For the asynchronous DoS attacks in the measurement channel and the control channel, it is equivalent to replace it with the DoS attacks in the control channel; and

2) Two sufficient conditions have been derived for the analysis and synthesis of the studied system under DoS attacks by using an new Lyapunov functional. Different from the open loop control in [12], in this work, the control inputs are kept as the last received data until there are new arrived data.

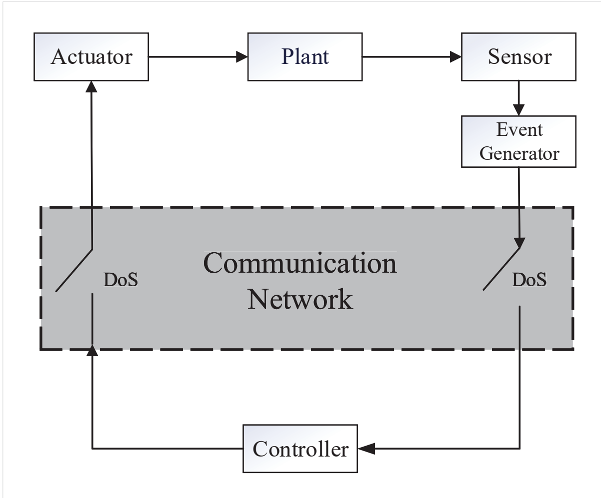

Fig. 1. Block diagram of closed-loop system.

Notation. We denote by $\mathbb{R}^n$ the set of n dimensional real vector. Given $\alpha \in \mathbb{R}$, we let $\mathbb{R}_{>\alpha}(\mathbb{R}_{\geq\alpha})$ denote the set of reals greater than (greater than or equal to) α. Given $v \in \mathbb{R}^n$, $\|v\|$ is its Euclidean norm. We let $\mathbb{N}$ denote the set of natural numbers and denote $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Given a matrix M, then $\|M\|$ is its spectral norm. Given two sets A and B, we denote by $A \backslash B$ the relative complement of B in A. And we denote $\|w(t)\|_\infty = \sup_{s\in[0,t]}\{w(s)\}$ and $\|x(t)\|_h = \sup_{-h\leq\theta\leq 0}\{x(t+\theta), \dot{x}(t+\theta)\}$.
The remainder of this paper is organized as follows. In Section 2, we describe the framework of the system and the formulate of the control problem. In Section 3, the stability of the closed loop system is analyzed. In addition, the trigger matrix and the controller gain matrix is obtained by solving a set of LMIs. In Section 4, the effectiveness of the proposed control strategy is demonstrated by a practical example. The conclusions are drawn in Section 5.

2. PROBLEM FORMULATION

2.1. System equation

The schematic of a cyber-physical system under asynchronous DoS attacks is shown in Figure 1, where the system model is given as follows:

$$\dot{x}(t) = Ax(t) + Bu(t) + w(t) \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $u(t) \in \mathbb{R}^m$ is the control input, $w(t) \in \mathbb{R}^n$ is an unknown disturbance. A, B are matrices of appropriate size. Throughout this paper, we assume (A, B) is controllable. The sensor and the controller are connected to each other by the network, as are the controller and the actuator. The state feedback is concerned in this paper, so the sensor directly measures the state vector of the system.

2.2. Event trigger mechanism

In this work, we employ the following event triggering mechanism [17]:

$$p_{j+1}h = p_j h + \inf\{lh|e^T((p_j + l)h)\Omega e((p_j + l)h) > \sigma x^T(p_j h)\Omega x(p_j h)\} \tag{2}$$

where h is the sampling period of sensor, $e(t) = x(p_j h) - x(t)$, Ω is a positive definite weighting matrix, and σ is a preselected constant. The successfully received control sequence at the actuator is described by the set $S_1 = \{0, t_1 h, t_2 h, \ldots, t_k h\}$, the transmitted sequence is described by the set $S_2 = \{0, p_1 h, p_2 h, \ldots, p_j h\}$, We can obtain $S_1 \subseteq S_2$, and $S_3 = \{0, h, 2h, \ldots, nh\}$ is the set of the sampled sequence.

As shown in Figure 1, the sensor sends data to the remotely located controller through the communication network for calculating suitable control commands, and then the control commands are transmitted over the communication network again to the actuator so as to act on the physical system (plant). In this paper, we assume that the transmitted data is received immediately without delay. The control input applied to the process can be expressed as

$$v(t) = Kx(t_k^s h), t \in [t_k^s h, t_{k+1}^s h) \tag{3}$$

$$u(t) = v(t_k^c h), t \in [t_k^c h, t_{k+1}^c h) \tag{4}$$

where K is the state-feedback matrix, $v(t)$ is the controller output, $t_k^i h (i = s, c)$ represents the successful sensor (s) or control (c) update instants sequence, respectively. Since the controller receives the sensor datas only at each triggering time, it is simultaneously transmitted to the actuator, so the actuator only receives the controller outputs at the triggering time. Then we have $\{t_k^c\} \subset \{t_k^s\}$. In this paper, only the actuator could hold the control input, so the sensor sending data unsuccessfully is equivalent to the sensor sending successfully but the controller failed to send the data. So let $t_k h$ be the instants sequence when the actuator last successfully received the data. Then we get

$$u(t) = Kx(t_k h). \tag{5}$$

2.3. General DoS attack

Let $\{h_n\}_{n\in\mathbb{N}_0}$ denote the sequence of DoS *off/on* transitions, i. e., the time instants at which DoS exhibits a transition from zero (communication is possible) to one (communication is interrupted) [27], τ_n represents the nth DoS attack duration. Then we have

$$\mathcal{H}_n = [h_n, h_n + \tau_n]\,. \tag{6}$$

For a period $[\tau, t]\,, \tau \in [0, t)$, it can be divided into the following subintervals

$$\Xi(\tau, t) := \bigcup_{n\in\mathbb{N}_0} \mathcal{H}_n \bigcap [\tau, t] \tag{7}$$

$$\Theta(\tau, t) := [\tau, t] \backslash \Xi(\tau, t). \tag{8}$$

Where $\Xi(\tau, t)$ is the sum of all attacked periods within $[\tau, t]$, and $\Theta(\tau, t)$ is the sum of all unattacked periods within $[\tau, t]$. However, due to energy constraints and other constraints, it is assumed that the attack is not arbitrary, as in [27], introducing constraints on attack duration and frequency. Let $n(\tau, t)$ denote the number of DoS *off/on* transitions occurring on the interval $[\tau, t)$

Assumption 1 – (DoS Duration): There exist $\kappa \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{>1}$ that

$$|\Xi(\tau,t)| \leq \kappa + \frac{t-\tau}{T}. \tag{9}$$

Assumption 2 – (DoS Frequency): There exist $\eta \in \mathbb{R}_{\geq 0}$ and $\tau_D \in \mathbb{R}_{>\underline{\Delta}}$ that

$$n(\tau,t) \leq \eta + \frac{t-\tau}{\tau_D} \tag{10}$$

where $\underline{\Delta} < t_{k+1}h - t_k h, k \in \mathbb{N}_0$.

Remark 2.1. Duration and frequency of occurrence are the main features of the attack. The longer the duration, the longer the communication channel is blocked, and the constraint duration cannot be long enough to completely block the communication channel. T indicate the ratio of the attack duration to the discussed duration. Another constraint is that for the frequency of occurrence, the constrained frequency must not be greater than the frequency of data transmission. Otherwise, each data transmission may just be attacked, resulting in no data transmission success. So, τ_D means the approximate period of attack.

2.4. Asynchronous DoS attack

The above attacks are only for one communication channel. However, the actual system has two communication channels, one is from the sensor to the controller and the other is from the controller to the actuator. Especially when the attack is not synchronized, it is necessary to establish an asynchronous attack model.
For asynchronous DoS attack, the measurement channel and the control channel are attacked separately. Then

$$\mathcal{H}_n^s = [h_n^s, h_n^s + \tau_n^s], \mathcal{H}_n^c = [h_n^c, h_n^c + \tau_n^c] \tag{11}$$

represent the attack duration of the measurement channel (sensor-to-controller) and the control channel (controller-to-actuator), respectively. And as long as any channel is attacked, the packet will not be received successfully. Then let

$$\mathcal{H}_n^* = \mathcal{H}_n^s \cup \mathcal{H}_n^s \tag{12}$$

denote the total time period during which any channel is attacked.
According to assumption 1 and assumption 2, we have

$$|\Xi_s(\tau,t)| \leq \kappa_1 + \frac{t-\tau}{T_1}, n_s(\tau,t) \leq \eta_1 + \frac{t-\tau}{\tau_D^1} \tag{13}$$

$$|\Xi_c(\tau,t)| \leq \kappa_2 + \frac{t-\tau}{T_2}, n_c(\tau,t) \leq \eta_2 + \frac{t-\tau}{\tau_D^2} \tag{14}$$

where $\Xi_i(\tau,t)$ and $n_i(\tau,t)(i = s,c)$ represent the attack duration and the number of attacks of the sensor channel or the actuator channel in time period $[\tau,t)$, respectively. Then we have

$$|\Xi_*(\tau,t)| \leq |\Xi_s(\tau,t)| + |\Xi_c(\tau,t)| = (\kappa_1+\kappa_2) + (t-\tau)\left(\frac{1}{T_1} + \frac{1}{T_2}\right) \tag{15}$$

and

$$n_*(\tau,t) \le n_s(\tau,t) + n_c(\tau,t) \le (\eta_1+\eta_2) + (t-\tau)\left(\frac{1}{\tau_D^1} + \frac{1}{\tau_D^2}\right) \tag{16}$$

where $\Xi_*(\tau,t)$ and $n_*(\tau,t)$ represent the duration and the number of attacks after merging the two channels, that is, attacking any one channel is considered an attack on the network. Let

$$\kappa_* = \kappa_1 + \kappa_2, \frac{1}{T_*} = \frac{1}{T_1} + \frac{1}{T_2} \tag{17}$$

and

$$\eta_* = \eta_1 + \eta_2, \frac{1}{\tau_D^*} = \frac{1}{\tau_D^1} + \frac{1}{\tau_D^2}. \tag{18}$$

Then we get

$$|\Xi_*(\tau,t)| \le \kappa_* + \frac{t-\tau}{T_*} \tag{19}$$

and

$$n_*(\tau,t) \le \eta_* + \frac{t-\tau}{\tau_D^*}. \tag{20}$$

Since the combined overall attack has the possibility of simultaneous attacks on two channels, the duration overlap rate λ and the attack occurrence merge rate φ are defined for this purpose. The duration overlap rate λ represents the ratio of the simultaneous attack duration of two channels to the duration of the attack of the two channels. Let

$$\lambda(\tau,t) = \frac{|\Xi_s(\tau,t) \cap \Xi_c(\tau,t)|}{|\Xi_s(\tau,t)| + |\Xi_c(\tau,t)|} \tag{21}$$

and the attack occurrence merge rate φ is the ratio of the number $\bar{n}(\tau,t)$ of overlaps to the total number of attacks. We have

$$\varphi(\tau,t) = \frac{\bar{n}(\tau,t)}{n_s(\tau,t) + n_c(\tau,t)}. \tag{22}$$

Then we get

$$|\Xi_*(\tau,t)| \le (1-\lambda(\tau,t))\left(\kappa_* + \frac{t-\tau}{T_*}\right) \tag{23}$$

$$n_*(\tau,t) \le (1-\varphi(\tau,t))\left(\eta_* + \frac{t-\tau}{\tau_D^*}\right). \tag{24}$$

Define the occurrence time $\{h_n^*\}_{n\in\mathbb{N}_0}$ of the overall attack and the corresponding duration τ_n^*. Then we have $\mathcal{H}_n^* = [h_n^*, h_n^* + \tau_n^*]$.

2.5. Period division of switched controller under DoS attacks

Packets sent over the network may not all be successfully received [27], so the time period is divided into two parts, in which the controller is switched, they are $\bar{\Theta}(\tau,t)$ and $\bar{\Xi}(\tau,t)$ respectively and we use Z_m and W_m to represent the two parts, where

$$\bar{\Xi}(\tau,t) := \bigcup_{m\in\mathbb{N}_0} Z_m \cap [\tau,t] \tag{25}$$

$$\bar{\Theta}(\tau,t) := \bigcup_{m\in\mathbb{N}_0} W_{m-1}\cap[\tau,t] \tag{26}$$

$$Z_m := \{\zeta_m\}\cup[\zeta_m,\zeta_m+v_m] \tag{27}$$

$$W_m := \{\zeta_m+v_m\}\cup[\zeta_m+v_m,\zeta_{m+1}]\,. \tag{28}$$

Let

$$\bar{\mathcal{H}}_n^* := \{h_n^*\}\cup[h_n^*,h_n^*+\lambda_n+\Lambda_n] \tag{29}$$

where

$$\lambda_n := \begin{cases} \tau_n^*, & \text{if } \mathcal{S}_n=\emptyset \\ t_{\sup\{k\in\mathbb{N}_0:k\in\mathcal{S}_n\}}-h_n^*, & \text{otherwise,} \end{cases} \tag{30}$$

$$\Lambda_n := \begin{cases} 0, & \text{if } \mathcal{S}_n=\emptyset \\ \Delta_{\sup\{k\in\mathbb{N}_0:k\in\mathcal{S}_n\}}, & \text{otherwise,} \end{cases} \tag{31}$$

where $\mathcal{S}_n=\{k\in\mathbb{N}_0|p_k\in\mathcal{H}_n^*\}$ and $\Delta_k=p_{k+1}h-p_kh$. λ_n represents the length of the attack duration in each of different situations. Λ_n means the additional affected duration under the attack if there is a triggering in the attack duration [27]. Then we have

$$\zeta_0 := \inf\left\{p_kh|p_kh\geq h_0^*,p_kh\in\bar{\mathcal{H}}_0^*\right\} \tag{32}$$

$$\zeta_{m+1} := \inf\left\{p_kh|p_kh\in\bar{\mathcal{H}}_n^*,h_n^*>\zeta_m,h_n^*>h_{n-1}^*+\lambda_{n-1}+\Lambda_{n-1}\right\} \tag{33}$$

which means that the first triggering instant in the attack time period is taken as $\zeta_m, m\in\mathbb{N}_0$. Then, let

$$v_m := \sum_{\substack{n\in\mathbb{N}_0;\\ n\zeta_m\leq h_n^*<\zeta_{m+1}}} \left|\bar{\mathcal{H}}_n^*\backslash\bar{\mathcal{H}}_{n+1}^*\right|. \tag{34}$$

Since $\bar{\mathcal{H}}_n^*$ and $\bar{\mathcal{H}}_{n+1}^*$ may have overlapping portions, in order to separate the overlapping portions, the overlapping portions of $\bar{\mathcal{H}}_n^*$ and $\bar{\mathcal{H}}_{n+1}^*$ are removed in v_m, that is, the length of Z_m.

Divide the period by the instant when the trigger data is successfully received. We have

$$\mathcal{F}_k = [t_kh,t_{k+1}h), k\in\mathbb{N}_0. \tag{35}$$

Remark 2.2. In the time period $\bar{\Xi}(\tau,t)$, due to the DoS attack, although the trigger mechanism does not change, the actuator does not receive the triggered data, so the time interval between the two actual received data will contain multiple trigger instants, although they are triggered and transmitted. It can be seen from the above that the starting moments of W_m must be the triggering instants when the actuator successful received the triggers, and the starting and ending instants of Z_m are also the triggering instants.

We define μ_1 as the maximum trigger interval when $t\in W_m$, and b is the largest trigger interval for two successfully received triggers, which is also the maximum duration of the attack.

For the jth trigger instant in the kth successful trigger interval $\mathcal{F}_k$, denoted by $t_{k,j}$, then we use

$$\mathcal{F}_{k,j} = [t_{k,j}h, t_{k,j+1}h), t_{k,j} > t_k, t_{k,j+1} < t_{k+1} \tag{36}$$

denote the trigger interval for each of the unsuccessfully transmitted triggers, where $t_{k,0} = t_k$.

2.6. Event triggered control model under DoS attacks

Under consideration of cases with or without attacks, the event-triggered control scheme can be given as

$$\dot{x}(t) = \begin{cases} Ax(t) + BK_1 x(t_k h) + w(t) & t \in W_m \\ Ax(t) + BK_2 x(t_k h) + w(t) & t \in Z_m \end{cases} \tag{37}$$

where K_1 and K_2 are the controller gains need to be solved and W_m and Z_m are given in (28) and (27).

The objective of this paper is to design an event-triggered control scheme, such that the resulting closed-loop system (37) is input-to-state stable under the DoS attacks. For completeness, the definition of input-to-state stability is given as follows.

Definition 2.3. Let Σ denote the system resulting from (37), then system Σ is said to be *input-to-state stable* (ISS) if there exist a $\mathcal{KL}$-function β and a $\mathcal{K}_\infty$-function γ, for each $w \in \mathcal{L}_\infty$ that [27]

$$x(t) \le \beta(x(0), t) + \gamma(\|w(t)\|_\infty) \tag{38}$$

for all $t \in \mathbb{R}_{>0}$

3. MAIN RESULTS

Before give the main results, the follow lemma, which is helpful for deriving the main theorem, is presented.

Lemma 3.1. Given the feedback gain K and trigger parameter σ, for the system (37), if for some prescribed constants $\alpha_i \in (0, \infty)$, $\gamma_i \in (0, \infty)$, there exist symmetric positive definite matrices P_i, Q_i, R_i and matrices X_i $(i = 1, 2)$ of appropriate dimensions such that

$$\Sigma_1 < 0, \ \Re_1 > 0 \tag{39}$$

$$\Sigma_2 < 0, \ \Re_2 > 0 \tag{40}$$

where

$$\Sigma_1 = \begin{bmatrix} \Pi_1 & * \\ \mu_1 R_1 F_1 & -R_1 \end{bmatrix}, \ \Re_1 = \begin{bmatrix} \tilde{R}_1 & * \\ X_1 & \tilde{R}_1 \end{bmatrix}$$

$$\Sigma_2 = \begin{bmatrix} \Pi_2 & * \\ \mu_2 R_2 F_2 & -R_2 \end{bmatrix}, \ \Re_2 = \begin{bmatrix} \tilde{R}_2 & * \\ X_2 & \tilde{R}_2 \end{bmatrix}$$

$$\tilde{R}_1 = e^{-\alpha_1 \mu_1} \begin{bmatrix} R_1 & * \\ 0 & 3R_1 \end{bmatrix}, \ \tilde{R}_2 = \begin{bmatrix} R_2 & * \\ 0 & 3R_2 \end{bmatrix}$$

$$X_1=\begin{bmatrix} X_{11} & X_{12} \\ X_{13} & X_{14} \end{bmatrix},\ X_2=\begin{bmatrix} X_{21} & X_{22} \\ X_{23} & X_{24} \end{bmatrix}$$

$$\Pi_1=\begin{bmatrix} \Pi_1^{11} & * & * & * & * & * \\ \Pi_1^{21} & \Pi_1^{22} & * & * & * & * \\ \Pi_1^{31} & \Pi_1^{32} & \Pi_1^{33} & * & * & * \\ \Pi_1^{41} & \Pi_1^{42} & \Pi_1^{43} & \Pi_1^{44} & * & * \\ \Pi_1^{51} & \Pi_1^{52} & \Pi_1^{53} & \Pi_1^{54} & \Pi_1^{55} & * \\ \Pi_1^{61} & 0 & 0 & 0 & 0 & \Pi_1^{66} \end{bmatrix}$$

$$\Pi_2=\begin{bmatrix} \Pi_2^{11} & * & * & * & * & * \\ \Pi_2^{21} & \Pi_2^{22} & * & * & * & * \\ \Pi_2^{31} & \Pi_2^{32} & \Pi_2^{33} & * & * & * \\ \Pi_2^{41} & \Pi_2^{42} & \Pi_2^{43} & \Pi_2^{44} & * & * \\ \Pi_2^{51} & \Pi_2^{52} & \Pi_2^{53} & \Pi_2^{54} & \Pi_2^{55} & * \\ \Pi_2^{61} & 0 & 0 & 0 & 0 & \Pi_2^{66} \end{bmatrix}$$

$\Pi_1^{11}=\alpha_1 P_1 + A^T P_1 + P_1 A + Q_1 - 4R_1 e^{-\alpha_1\mu_1}$
$\Pi_1^{21} = -X_{11} - X_{12} - X_{13} - X_{14} - 2R_1 e^{-\alpha_1\mu_1}$
$\Pi_1^{22} = X_{11} - X_{12} + X_{13} - X_{14} + X_{11}^T - X_{12}^T + X_{13}^T - X_{14}^T - 8R_1 e^{-\alpha_1\mu_1} + (\sigma-1)\,\Omega$
$\Pi_1^{31} = K_1^T B^T P_1 + X_{11} + X_{12} - X_{13} - X_{14}$
$\Pi_1^{32} = -X_{11} + X_{12} + X_{13} - X_{14} - 2R_1 e^{-\alpha_1\mu_1} + \Omega$
$\Pi_1^{33} = -Q_1 e^{-\alpha_1\mu_1} - 4R_1 e^{-\alpha_1\mu_1} - \Omega, \Pi_1^{41} = 6R_1 e^{-\alpha_1\mu_1}$
$\Pi_1^{42} = 2X_{12}^T + 2X_{14}^T + 6R_1 e^{-\alpha_1\mu_1}, \Pi_1^{43} = -2X_{12}^T + 2X_{14}^T$
$\Pi_1^{44} = -12R_1 e^{-\alpha_1\mu_1}, \Pi_1^{51} = 2X_{13} + 2X_{14}$
$\Pi_1^{52} = -2X_{13} + 2X_{14} + 6R_1 e^{-\alpha_1\mu_1}, \Pi_1^{53} = 6R_1 e^{-\alpha_1\mu_1}$
$\Pi_1^{54} = -4X_{14}, \Pi_1^{55} = -12R_1 e^{-\alpha_1\mu_1}$
$\Pi_1^{61} = P_1, \Pi_1^{66} = -\gamma_1, F_1 = \begin{bmatrix} A & 0 & BK_1 & 0 & 0 & I \end{bmatrix}$
$\Pi_2^{11} = A^T P_2 + P_2 A + Q_2 - \alpha_2 P_2 - 4R_2$
$\Pi_2^{21} = -X_{21} - X_{22} - X_{23} - X_{24} - 2R_2$
$\Pi_2^{22} = X_{21} - X_{22} + X_{23} - X_{24} + X_{21}^T - X_{22}^T + X_{23}^T - X_{24}^T - 8R_2$
$\Pi_2^{31} = K_2^T B^T P_2 + X_{21} + X_{22} - X_{23} - X_{24}$
$\Pi_2^{32} = -X_{21} + X_{22} + X_{23} - X_{24} - 2R_2$
$\Pi_2^{33} = -Q_2 e^{\alpha_2 h} - 4R_2, \Pi_2^{41} = 6R_2, \Pi_2^{42} = 2X_{22}^T + 2X_{24}^T + 6R_2$
$\Pi_2^{43} = -2X_{22}^T + 2X_{24}^T, \Pi_2^{44} = -12R_2, \Pi_2^{51} = 2X_{23} + 2X_{24}$
$\Pi_2^{52} = -2X_{23} + 2X_{24} + 6R_2, \Pi_2^{53} = 6R_2, \Pi_2^{54} = -4X_{24}$
$\Pi_2^{55} = -12R_2, \Pi_2^{61} = P_2, \Pi_2^{66} = -\gamma_2, F_2 = \begin{bmatrix} A & 0 & BK_2 & 0 & 0 & I \end{bmatrix}$

then we have

$$\begin{cases} V_1(t) \le e^{-\alpha_1(t-\zeta_m-v_m)} V_1(\zeta_m+v_m) + \gamma_3 w^T(t)w(t) & t\in W_m \\ V_2(t) \le e^{\alpha_2(t-\zeta_m)} V_2(\zeta_m) + \gamma_4 e^{\alpha_2(t-\zeta_m)} w^T(t)w(t) & t\in Z_m \end{cases} \tag{41}$$

where $\gamma_3=\gamma_1/\alpha_1$, $\gamma_4=\gamma_2/\alpha_2$.

Proof. See Appendix. □

Base on Lemma 1, we now state and establish the following stability analysis result.

Theorem 3.2. Given the feedback gain K and trigger parameter σ, for the system (37), if some prescribed constants $\kappa_i, \eta_i, \tau_D^i, T_i, \delta_i, \phi_1 (i = 1, 2)$ satisfying

$$\alpha_1 > \frac{(\alpha_1 + \alpha_2)}{\bar{T}} + \frac{\bar{\varphi}\,(\phi_1 + \phi_2)}{\tau_D^*} \tag{42}$$

where $\bar{\varphi} = 1 - \varphi$, and there exist symmetric positive definite matrices P_i, Q_i, R_i and matrices X_i $(i = 1, 2)$ of appropriate dimensions satisfying (39) and (40) and the conditions below are satisfied

$$P_1 \leq \delta_2 P_2, P_2 \leq e^{\phi_1} P_1 \tag{43}$$

$$Q_1 \leq \delta_2 Q_2, Q_2 \leq \delta_1 Q_1 \tag{44}$$

$$R_1 \leq \delta_2 R_2, R_2 \leq \delta_1 R_1 \tag{45}$$

then the system (37) under the asynchronous DoS attack is ISS.

Proof. See Appendix. □

By Theorem 1, we now provide the following theorem for the co-design of the controller feedback gain K, and the weighting matrix Ω.

Theorem 3.3. Given the trigger parameter σ, for the system (37), and $\alpha_i (i = 1, 2)$ satisfying (42), if for some prescribed positive constants $\gamma_i, \delta_i, \varpi_i, \theta_i$, there exist symmetric positive definite matrices $\bar{T}_i, \bar{Q}_i, \bar{R}_i, \bar{\Omega}_i$ and matrices $\bar{X}_1, \bar{X}_2 (i = 1, 2)$ of appropriate dimensions such that

$$\bar{\Sigma}_1 < 0, \bar{\Re}_1 > 0 \tag{46}$$

$$\bar{\Sigma}_2 < 0, \bar{\Re}_2 > 0 \tag{47}$$

$$\begin{bmatrix} -\delta_2 \bar{T}_2 & \bar{T}_2 \\ \bar{T}_2 & -\bar{T}_1 \end{bmatrix} \leq 0, \begin{bmatrix} -e^{\phi_1} \bar{T}_1 & \bar{T}_1 \\ \bar{T}_1 & -\bar{T}_2 \end{bmatrix} \leq 0 \tag{48}$$

$$\begin{bmatrix} -\delta_2 \bar{Q}_2 & \bar{T}_2 \\ \bar{T}_2 & \varpi_1^2 \bar{Q}_1 - 2\varpi_1 \bar{T}_1 \end{bmatrix} \leq 0, \begin{bmatrix} -\delta_1 \bar{Q}_1 & \bar{T}_1 \\ \bar{T}_1 & \varpi_2^2 \bar{Q}_2 - 2\varpi_2 \bar{T}_2 \end{bmatrix} \leq 0 \tag{49}$$

$$\begin{bmatrix} -\delta_2 \bar{R}_2 & \bar{T}_2 \\ \bar{T}_2 & \theta_1^2 \bar{R}_1 - 2\theta_1 \bar{T}_1 \end{bmatrix} \leq 0, \begin{bmatrix} -\delta_1 \bar{R}_1 & \bar{T}_1 \\ \bar{T}_1 & \theta_2^2 \bar{R}_2 - 2\theta_2 \bar{T}_2 \end{bmatrix} \leq 0 \tag{50}$$

where

$$\bar{\Sigma}_1 = \begin{bmatrix} \bar{\Pi}_1 & * \\ \mu_1 \bar{F}_1 & -T_1 \bar{R}_1^{-1} \bar{T}_1 \end{bmatrix}, \bar{\Re}_1 = \begin{bmatrix} \bar{\tilde{R}}_1 & * \\ \bar{X}_1 & \bar{\tilde{R}}_1 \end{bmatrix}$$

$$\bar{\Sigma}_2 = \begin{bmatrix} \bar{\Pi}_2 & * \\ \mu_2 \bar{F}_2 & -T_2 \bar{R}_2^{-1} \bar{T}_2 \end{bmatrix}, \bar{\Re}_2 = \begin{bmatrix} \bar{\tilde{R}}_2 & * \\ \bar{X}_2 & \bar{\tilde{R}}_2 \end{bmatrix}$$

$$\bar{\tilde{R}}_1 = e^{-\alpha_1 \mu_1} \begin{bmatrix} \bar{R}_1 & * \\ 0 & 3\bar{R}_1 \end{bmatrix}, \bar{\tilde{R}}_2 = \begin{bmatrix} \bar{R}_2 & * \\ 0 & 3\bar{R}_2 \end{bmatrix}$$

$$\bar{X}_1 = \begin{bmatrix} \bar{X}_{11} & \bar{X}_{12} \\ \bar{X}_{13} & \bar{X}_{14} \end{bmatrix}, \bar{X}_2 = \begin{bmatrix} \bar{X}_{21} & \bar{X}_{22} \\ \bar{X}_{23} & \bar{X}_{24} \end{bmatrix}$$

$$\bar{\Pi}_1 = \begin{bmatrix} \bar{\Pi}_1^{11} & * & * & * & * & * \\ \bar{\Pi}_1^{21} & \bar{\Pi}_1^{22} & * & * & * & * \\ \bar{\Pi}_1^{31} & \bar{\Pi}_1^{32} & \bar{\Pi}_1^{33} & * & * & * \\ \bar{\Pi}_1^{41} & \bar{\Pi}_1^{42} & \bar{\Pi}_1^{43} & \bar{\Pi}_1^{44} & * & * \\ \bar{\Pi}_1^{51} & \bar{\Pi}_1^{52} & \bar{\Pi}_1^{53} & \bar{\Pi}_1^{54} & \bar{\Pi}_1^{55} & * \\ \bar{\Pi}_1^{61} & 0 & 0 & 0 & 0 & \bar{\Pi}_1^{66} \end{bmatrix}$$

$$\bar{\Pi}_2 = \begin{bmatrix} \bar{\Pi}_2^{11} & * & * & * & * & * \\ \bar{\Pi}_2^{21} & \bar{\Pi}_2^{22} & * & * & * & * \\ \bar{\Pi}_2^{31} & \bar{\Pi}_2^{32} & \bar{\Pi}_2^{33} & * & * & * \\ \bar{\Pi}_2^{41} & \bar{\Pi}_2^{42} & \bar{\Pi}_2^{43} & \bar{\Pi}_2^{44} & * & * \\ \bar{\Pi}_2^{51} & \bar{\Pi}_2^{52} & \bar{\Pi}_2^{53} & \bar{\Pi}_2^{54} & \bar{\Pi}_2^{55} & * \\ \bar{\Pi}_2^{61} & 0 & 0 & 0 & 0 & \bar{\Pi}_2^{66} \end{bmatrix}$$

$\bar{\Pi}_1^{11}=\alpha_1\bar{T}_1 + A^T\bar{T}_1 + \bar{T}_1A + \bar{Q}_1 - 4\bar{R}_1e^{-\alpha_1\mu_1}$
$\bar{\Pi}_1^{21} = -\bar{X}_{11} - \bar{X}_{12} - \bar{X}_{13} - \bar{X}_{14} - 2\bar{R}_1e^{-\alpha_1\mu_1}$
$\bar{\Pi}_1^{22} = \bar{X}_{11} - \bar{X}_{12} + \bar{X}_{13} - \bar{X}_{14} + \bar{X}_{11}^T - \bar{X}_{12}^T + \bar{X}_{13}^T - \bar{X}_{14}^T - 8\bar{R}_1e^{-\alpha_1\mu_1} + (\sigma - 1)\,\bar{\Omega}$
$\bar{\Pi}_1^{31} = Y_1^TB^T + \bar{X}_{11} + \bar{X}_{12} - \bar{X}_{13} - \bar{X}_{14}$
$\bar{\Pi}_1^{32} = -\bar{X}_{11} + \bar{X}_{12} + \bar{X}_{13} - \bar{X}_{14} - 2\bar{R}_1e^{-\alpha_1\mu_1} + \bar{\Omega}$
$\bar{\Pi}_1^{33} = -\bar{Q}_1e^{-\alpha_1\mu_1} - 4\bar{R}_1e^{-\alpha_1\mu_1} - \bar{\Omega}, \bar{\Pi}_1^{41} = 6\bar{R}_1e^{-\alpha_1\mu_1}$
$\bar{\Pi}_1^{42} = 2\bar{X}_{12}^T + 2\bar{X}_{14}^T + 6\bar{R}_1e^{-\alpha_1\mu_1}, \bar{\Pi}_1^{43} = -2\bar{X}_{12}^T + 2\bar{X}_{14}^T$
$\bar{\Pi}_1^{44} = -12\bar{R}_1e^{-\alpha_1\mu_1}, \bar{\Pi}_1^{51} = 2\bar{X}_{13} + 2\bar{X}_{14}$
$\bar{\Pi}_1^{52} = -2\bar{X}_{13} + 2\bar{X}_{14} + 6\bar{R}_1e^{-\alpha_1\mu_1}, \bar{\Pi}_1^{53} = 6\bar{R}_1e^{-\alpha_1\mu_1}$
$\bar{\Pi}_1^{54} = -4\bar{X}_{14}, \bar{\Pi}_1^{55} = -12\bar{R}_1e^{-\alpha_1\mu_1}$
$\bar{\Pi}_1^{61} = \bar{T}_1, \Pi_1^{66} = -\gamma_1, F_1 = \begin{bmatrix} A\bar{T}_1 & 0 & BY_1 & 0 & 0 & \bar{T}_1 \end{bmatrix}$
$\bar{\Pi}_2^{11} = A^T\bar{T}_2 + \bar{T}_2A + \bar{Q}_2 - \alpha_2\bar{T}_2 - 4\bar{R}_2$
$\bar{\Pi}_2^{21} = -\bar{X}_{21} - \bar{X}_{22} - \bar{X}_{23} - \bar{X}_{24} - 2\bar{R}_2$
$\bar{\Pi}_2^{22} = \bar{X}_{21} - \bar{X}_{22} + \bar{X}_{23} - \bar{X}_{24} + \bar{X}_{21}^T - \bar{X}_{22}^T + \bar{X}_{23}^T - \bar{X}_{24}^T - 8\bar{R}_2$
$\bar{\Pi}_2^{31} = Y_2^TB^T + \bar{X}_{21} + \bar{X}_{22} - \bar{X}_{23} - \bar{X}_{24}$
$\bar{\Pi}_2^{32} = -\bar{X}_{21} + \bar{X}_{22} + \bar{X}_{23} - \bar{X}_{24} - 2\bar{R}_2$
$\bar{\Pi}_2^{33} = -\bar{Q}_2e^{\alpha_2h} - 4\bar{R}_2, \bar{\Pi}_2^{41} = 6\bar{R}_2$
$\bar{\Pi}_2^{42} = 2\bar{X}_{22}^T + 2\bar{X}_{24}^T + 6\bar{R}_2, \bar{\Pi}_2^{43} = -2\bar{X}_{22}^T + 2\bar{X}_{24}^T$
$\bar{\Pi}_2^{44} = -12\bar{R}_2, \bar{\Pi}_2^{51} = 2\bar{X}_{23} + 2\bar{X}_{24}$
$\bar{\Pi}_2^{52} = -2\bar{X}_{23} + 2\bar{X}_{24} + 6\bar{R}_2, \bar{\Pi}_2^{53} = 6\bar{R}_2, \bar{\Pi}_2^{54} = -4\bar{X}_{24}$
$\bar{\Pi}_2^{55} = -12\bar{R}_2, \bar{\Pi}_2^{61} = \bar{T}_2, \Pi_2^{66} = -\gamma_2, F_2 = \begin{bmatrix} A\bar{T}_2 & 0 & BY_2 & 0 & 0 & \bar{T}_2 \end{bmatrix}$

then the system (37) with

$$K_1 = Y_1\bar{T}_1^{-1}, K_2 = Y_2\bar{T}_2^{-1} \tag{51}$$

is ISS in the presence of asynchronous DoS attack.

Proof. See Appendix. □

Remark 3.4. Since the matrix inequalities (46) and (47) contains the nonlinear term $-\bar{T}_i\bar{R}_i^{-1}\bar{T}_i(i = 1, 2)$, the basic inequality $-\bar{T}\bar{R}^{-1}\bar{T} \leq \varpi^2\bar{R} - 2\varpi\bar{T}, \varpi > 0$ can be used to linearize the nonlinear term, making it easy to use the LMI toolbox.

Remark 3.5. For the selection of the parameter $\delta_i(i = 1, 2)$, the idea in [2] is adopted. Since the theorem 1 must be satisfied, that is $\beta_* > 0$, notice that the β_* is a monotonic increasing function of α_1 and is a monotonic decreasing function of α_2, so α_1 should be chosen as large as possible while α_2 should be chosen as small as possible, until the theorem 1 are feasible. The β_* is a monotonic decreasing function for both δ_1 and δ_2, therefore, multiple attempts are required to arrive at the suitable values.

4. AN EXAMPLE

In this section, a practical example is utilized to demonstrate the effectiveness of the proposed method. Let the physical plant in Figure 1 be an unmanned ground vehicle (UGV) under DoS attacks [18].

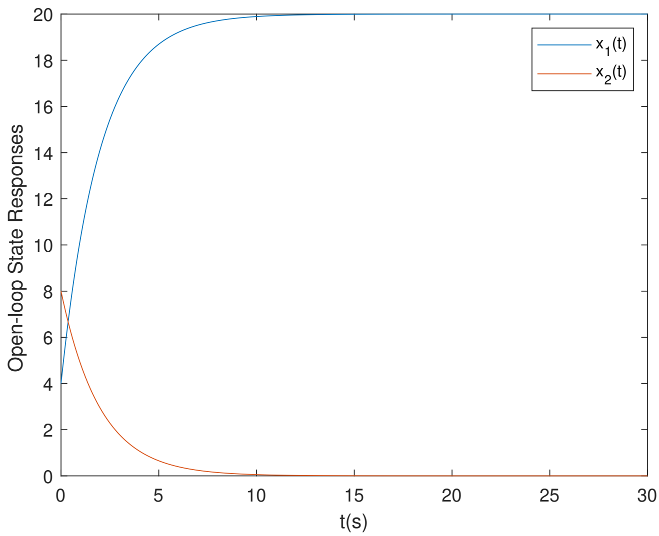

Fig. 2. State response of open-loop system.

A simplified linear dynamic model of the UGV system is described as

$$\begin{bmatrix} \dot{x} \\ \dot{v} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & \frac{-b}{M} \end{bmatrix} \begin{bmatrix} x \\ v \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{M} \end{bmatrix} F + w(t) \tag{52}$$

where x and v are the states of the UGV corresponding to position and linear velocity, respectively. M and b denote the mechanical mass and translational friction coefficient, respectively. The force F is the input and the disturbance $w(t)$ is introduced. For $M = 1, b = 0.5$, then we have

$$A = \begin{bmatrix} 0 & 1 \\ 0 & -0.5 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{53}$$

Setting $w(t) = 0.1e^{-0.1t}\sin(t), h = 0.01s, \varphi(0,t) = 0.5, \lambda(0,t) = 0.5, \kappa_*= 2, \eta_* = 1, T_* = 10, \tau_D^* = 50, \Delta_* = 0.5, \varpi = 1$ and choose $\sigma = 0.02$, then we let α_1= 0.6,α_2= 4, which

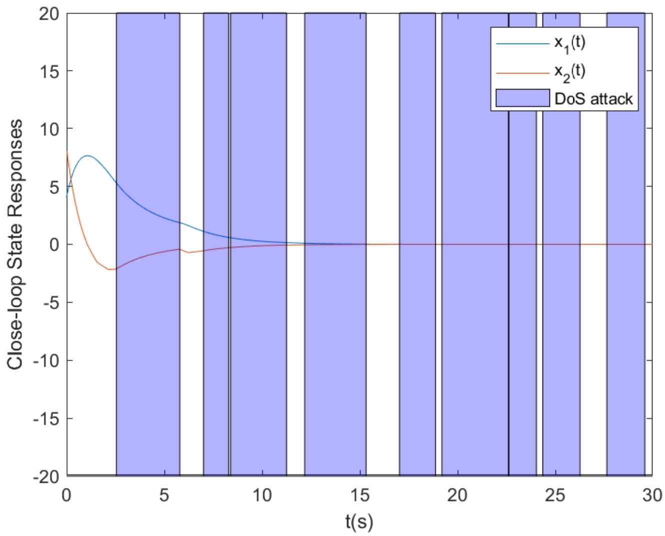

Fig. 3. State response of closed-loop system in the presence of DoS attack.

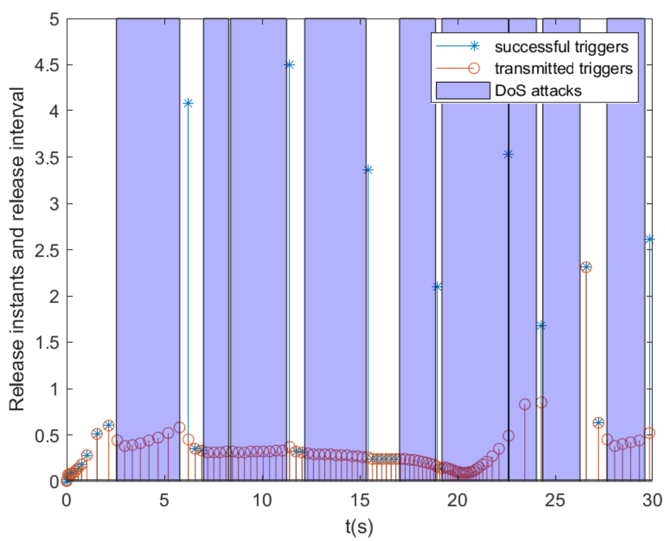

Fig. 4. Release instants and release intervals.

satisfy theorem 1. Then solving the LMIs in theorem 2, we obtain that

$$\Omega = \begin{bmatrix} 14.33 & 43.54 \\ 43.54 & 141.37 \end{bmatrix}, K_1 = \begin{bmatrix} -0.45 & -0.825 \end{bmatrix}, K_2 = \begin{bmatrix} -0.005 & -0.013 \end{bmatrix}. \quad (54)$$

The initial conditions are taken as $x_0 = \begin{bmatrix} 4 & 8 \end{bmatrix}^T$ and the simulation time is assumed to be 30 s. In the presence of the DoS attacks, the state responses of the open-loop system, the state response of the close loop system, the release time intervals between any two consecutive release instants are depicted in Figures 2 − 4, respectively.

From Figure 2 we could see the original system is not a asymptotically stable system. With the proposed controller, the close-loop system's state response is depicted in Figure 3, the states are asymptotically convergent over time. In Figure 4, the triggering instants are illustrated. The triggering instants might be dropped due to DoS attacks, that forced event generater to trigger immediately when attacks leave. The whole system is input-to-state stable. It proved that the proposed event triggering mechanism can be tolerant to some dropouts of the transmitted packets in the presence of the DoS attacks.

5. CONCLUSION

In this paper, we proposes an asynchronous DoS attacks model, which is analyzed by an equivalent synchronous attack model. The event-triggered transmitting mechanism is used to submit control signals and to maintain the most recently received data. By improving the Lyapunov functional of time-delay analysis, the sufficient conditions for the stability of the system under the asynchronous DoS attacks are given. In the future work, we will further study the observer-based feedback control under asynchronous DoS attacks. The event-triggered $\mathcal{H}_\infty$ filtering problem under such a type of asynchronous DoS attacks also a potential future topic.

6. APPENDIX

6.1. Proof of Lemma 1

Construct the following piecewise Lyapunov functional for system (37):

$$V(t) = \begin{cases} V_1(t) & t \in W_m \\ V_2(t) & t \in Z_m \end{cases} \quad (55)$$

where

$$\begin{aligned} V_1(t) &= x^T(t)P_1x(t) + \int_{t_kh}^{t} x^T(s)e^{-\alpha_1(t-s)}Q_1x(s)\,\mathrm{d}s \\ &+ \mu_1 \int_{t_kh}^{t}\int_{t-\mu_1}^{s} \dot{x}^T(s)e^{-\alpha_1(t-s)}R_1\dot{x}(s)\,\mathrm{d}\theta\mathrm{d}s \end{aligned} \quad (56)$$

$$\begin{aligned} V_2(t) = {}& x^T(t)P_2x(t) + \int_{t_kh}^{t} x^T(s)e^{\alpha_2(t-s)}Q_2x(s)\,\mathrm{d}s \\ & + \mu_2\int_{t_kh}^{t}\int_{t-\mu_2}^{s} \dot{x}^T(s)e^{\alpha_2(t-s)}R_2\dot{x}(s)\,\mathrm{d}\theta\mathrm{d}s. \end{aligned} \tag{57}$$

Where μ_1 and μ_2 are the maximum successful reception intervals when $t \in W_m$ and $t \in Z_m$, respectively. Then we have

$$\begin{aligned} \dot{V}_1(t) \le & -\alpha_1V_1(t) + \alpha_1x^T(t)P_1x(t) + \dot{x}^T(t)P_1x(t) + x^T(t)P_1\dot{x}(t) + x^T(t)Q_1x(t) \\ & - x^T(t_kh)Q_1e^{-\alpha_1\mu_1}x(t_kh) + \mu_1^2\dot{x}^T(t)R_1\dot{x}(t) \\ & - e^{-\alpha_1\mu_1}(t-t_kh)\int_{t_kh}^{t}\dot{x}^T(s)R_1\dot{x}(s)\,\mathrm{d}s \end{aligned} \tag{58}$$

and

$$\begin{aligned} \dot{V}_2(t) \le & \alpha_2V_2(t) - \alpha_2x^T(t)P_2x(t) + \dot{x}^T(t)P_2x(t) + x^T(t)P_2\dot{x}(t) + x^T(t)Q_2x(t) \\ & - x^T(t_kh)Q_2e^{\alpha_2h}x(t_kh) + \mu_2^2\dot{x}^T(t)R_2\dot{x}(t) - (t-t_kh)\int_{t_kh}^{t}\dot{x}(s)R_2\dot{x}(s)\,\mathrm{d}s. \end{aligned} \tag{59}$$

We now consider the following two cases.

Case 1: when $t \in [\zeta_m + v_m, \zeta_{m+1})$, there is no attack. We now first divide the time periods. Let

$$k_{\min}^m = \{k|t_kh = \zeta_m + v_m\}, k_{\max}^m = \sup\{k|t_kh < \zeta_{m+1}\} \tag{60}$$

then we have

$$\mathcal{F}_k^l = [t_kh + (l-1)h, t_kh + lh)\,,\ l \in \{1, 2, \ldots, \gamma_k\}\,, k \in [k_{\min}^m, k_{\max}^m] \tag{61}$$

where $\gamma_k = \inf\{l|(t_k + l)h \ge t_{k+1}h \textit{ or } (t_k + l)h \ge t_{k,1}h\}$. Let

$$\eta_k(t) = \begin{cases} t - t_kh, t \in \mathcal{F}_k^1 \\ t - t_kh - h, t \in \mathcal{F}_k^2 \\ \vdots \\ t - t_kh - (\gamma_k - 1)\,h, t \in \mathcal{F}_k^{\gamma_k} \end{cases} \tag{62}$$

and for each $k \in [k_{\min}^m, k_{\max}^m]$, we have

$$\begin{aligned} -(t-t_kh)\int_{t_kh}^{t}\dot{x}(s)R_1\dot{x}(s)\,\mathrm{d}s = & -(t-t_kh)\int_{t-\eta_k(t)}^{t}\dot{x}(s)R_1\dot{x}(s)\,\mathrm{d}s \\ & -(t-t_kh)\int_{t_kh}^{t-\eta_k(t)}\dot{x}(s)R_1\dot{x}(s)\,\mathrm{d}s. \end{aligned} \tag{63}$$

Using the inequality in [28] and [36], we have

$$\begin{aligned} & -(t-t_kh)\textstyle\int_{t-\eta_k(t)}^{t}\dot{x}(s)R_1\dot{x}(s)\,\mathrm{d}s - (t-t_kh)\int_{t_kh}^{t-\eta_k(t)}\dot{x}(s)R_1\dot{x}(s)\,\mathrm{d}s \le -\frac{(t-t_kh)}{\eta_k(t)}\Lambda_{11}^T\tilde{R}_1\Lambda_{11} \\ & -\frac{(t-t_kh)}{(t-t_kh)-\eta_k(t)}\Lambda_{12}^T\tilde{R}_1\Lambda_{12} \le -\begin{bmatrix} \Lambda_{11}^T \\ \Lambda_{12}^T \end{bmatrix}^T \begin{bmatrix} \tilde{R}_1 & X_1^T \\ X_1 & \tilde{R}_1 \end{bmatrix} \begin{bmatrix} \Lambda_{11} \\ \Lambda_{12} \end{bmatrix} \end{aligned} \tag{64}$$

where

$$\begin{bmatrix} \tilde{R}_1 & X_1^T \\ X_1 & \tilde{R}_1 \end{bmatrix} > 0 \tag{65}$$

and

$$\Lambda_{11} = \begin{bmatrix} I & -I & 0 & 0 & 0 & 0 \\ I & I & 0 & -2I & 0 & 0 \end{bmatrix} \xi_1(t), \tilde{R}_1 = \begin{bmatrix} R_1 & 0 \\ 0 & 3R_1 \end{bmatrix} \tag{66}$$

$$\Lambda_{12} = \begin{bmatrix} 0 & I & -I & 0 & 0 & 0 \\ 0 & I & I & 0 & -2I & 0 \end{bmatrix} \xi_1(t), X_1 = \begin{bmatrix} X_{11} & X_{12} \\ X_{13} & X_{14} \end{bmatrix} \tag{67}$$

where

$$\xi_1^T(t) = \begin{bmatrix} x^T(t) & x^T(t-\eta_k(t)) & x^T(t_k h) & \int_{t-\eta_k(t)}^{t} \frac{x^T(s)}{\eta_k(t)}\,\mathrm{d}s & \int_{t_k h}^{t-\eta_k(t)} \frac{x^T(s)}{h-\eta_k(t)}\,\mathrm{d}s & w^T(t) \end{bmatrix}^T. \tag{68}$$

Let

$$\Re_1 = \begin{bmatrix} \tilde{R}_1 & * \\ X_1 & \tilde{R}_1 \end{bmatrix} \tag{69}$$

using the event-triggering condition (2), we have

$$\left(x(t_k h) - x(t-\eta_k(t))\right)^T \Omega \left(x(t_k h) - x(t-\eta_k(t))\right) \leq \sigma x^T(t_k h)\Omega x(t_k h) \tag{70}$$

then we have

$$\dot{V}_1(t) \leq -\alpha_1 V_1(t) + \xi_1^T(t)\left(\Pi_1 + \mu_1^2 F_1^T R_1 F_1\right)\xi_1(t) + \gamma_1 w^T(t)w(t). \tag{71}$$

Applying the Schur complement, when the inequality (39) is satisfied, then we can obtain

$$\dot{V}_1(t) \leq -\alpha_1 V_1(t) + \gamma_1 w^T(t)w(t). \tag{72}$$

Due to the arbitrary of k, when $t \in [\zeta_m + v_m, \zeta_{m+1})$, then we have

$$V_1(t) \leq e^{-\alpha_1(t-\zeta_m - v_m)} V_1(\zeta_m + v_m) + \gamma_3 w^T(t)w(t) \tag{73}$$

where $\gamma_3 = \gamma_1/\alpha_1$.

Case 2: when $t \in [\zeta_m, \zeta_m + v_m)$, there are DoS attacks so the network might be blocked. Then following the similar steps as the ones in the proof of case 1, we let

$$j_m^k = \{j | t_{k,j}h = t_{k+1}h = \zeta_m + v_m\} \tag{74}$$

then we have

$$\mathcal{F}_{k,j}^l = [t_{k,j}h + (l-1)h, t_{k,j}h + lh), \ l \in \{1, 2, \ldots, \gamma_{k,j}\}, j \in \left[0, j_m^k\right) \tag{75}$$

where $\gamma_{k,j} = \inf\{l | (t_{k,j} + l)h \geq t_{k,j+1}h\}$. Let

$$\tau_{k,j}(t) = \begin{cases} t - t_{k,j}h, t \in \mathcal{F}_{k,j}^1 \\ t - t_{k,j}h - h, t \in \mathcal{F}_{k,j}^2 \\ \vdots \\ t - t_{k,j}h - (\gamma_{k,j} - 1)h, t \in \mathcal{F}_{k,j}^{\gamma_{k,j}} \end{cases} \tag{76}$$

for each $j \in [1, j_{\mathrm{m}}^k)$, we have

$$\begin{aligned} &-h\int_{t-\tau_{k,j}(t)}^{t} \dot{x}(s)R_2\dot{x}(s)\,\mathrm{d}s - h\int_{t_kh}^{t-\tau_{k,j}(t)} \dot{x}(s)R_2\dot{x}(s)\,\mathrm{d}s \le -\frac{h}{\tau_{k,j}(t)}\Lambda_{21}^T\tilde{R}_2\Lambda_{21} \\ &-\frac{h}{h-\tau_{k,j}(t)}\Lambda_{22}^T\tilde{R}_2\Lambda_{22} \le -\begin{bmatrix} \Lambda_{21}^T \\ \Lambda_{22}^T \end{bmatrix}^T \begin{bmatrix} \tilde{R}_2 & X_2^T \\ X_2 & \tilde{R}_2 \end{bmatrix} \begin{bmatrix} \Lambda_{21} \\ \Lambda_{22} \end{bmatrix} \end{aligned} \tag{77}$$

where

$$\begin{bmatrix} \tilde{R}_2 & X_2^T \\ X_2 & \tilde{R}_2 \end{bmatrix} > 0 \tag{78}$$

and

$$\Lambda_{21} = \begin{bmatrix} I & -I & 0 & 0 & 0 & 0 \\ I & I & 0 & -2I & 0 & 0 \end{bmatrix} \xi_2(t), \tilde{R}_2 = \begin{bmatrix} R_2 & 0 \\ 0 & 3R_2 \end{bmatrix} \tag{79}$$

$$\Lambda_{22} = \begin{bmatrix} 0 & I & -I & 0 & 0 & 0 \\ 0 & I & I & 0 & -2I & 0 \end{bmatrix} \xi_2(t), X_2 = \begin{bmatrix} X_{21} & X_{22} \\ X_{23} & X_{24} \end{bmatrix} \tag{80}$$

where

$$\begin{aligned} \xi_2^T(t) = [\ & x^T(t) \quad x^T(t-\tau_{k,j}(t)) \quad x^T(t_kh) \\ & \textstyle\int_{t-\tau_{k,j}(t)}^{t} \frac{x^T(s)}{\tau_{k,j}(t)}\,\mathrm{d}s \quad \int_{t_kh}^{t-\tau_{k,j}(t)} \frac{x^T(s)}{(t-t_kh)-\tau_{k,j}(t)}\,\mathrm{d}s \quad w^T(t)\ ]^T. \end{aligned} \tag{81}$$

Then we have

$$\dot{V}_2(t) \le \alpha_2 V_2(t) + \xi_2^T(t)\left(\Pi_2 + \mu_2^2 F_2^T R_2 F_2\right)\xi_2(t) + \gamma_2 w^T(t)w(t). \tag{82}$$

Taking the Schur complement, when the inequality (40) is satisfied and due to the arbitrary of j, when $t \in [\zeta_m, \zeta_m + v_m)$, then we can obtain

$$V_2(t) \le e^{\alpha_2(t-\zeta_m)}V_2(\zeta_m) + \gamma_4 e^{\alpha_2(t-\zeta_m)}w^T(t)w(t) \tag{83}$$

where $\gamma_4 {=} \gamma_2/\alpha_2$.

From the above analysis of cases 1 and 2, the conditions (39) and (40) guarantee the inequality (41) is satisfied. The proof is thus completed.

6.2. Proof of Theorem 1

Choose a piecewise Lyapunov functional V(t) as Lemma 1. According to (43), (44) and (45), it follows from Lemma 1 that:

$$V_1(t) \le \delta_2 V_2(t), V_2(t) \le \left(\frac{\mu_2}{\mu_1}\right)^2 e^{(\alpha_1+\alpha_2)\mu_1}\delta_1 V_1(t) \tag{84}$$

when $t = \zeta_m$, $t - t_kh \le \mu_1$ is satisfied. Then we have

$$V_1(\zeta_m + v_m) \le \delta_2 V_2(\zeta_m + v_m), V_2(\zeta_m) \le V_1(\zeta_m)\delta_1\left(\frac{\mu_2}{\mu_1}\right)^2 e^{(\alpha_1+\alpha_2)\mu_1}. \tag{85}$$

Then in time period $[0, \zeta_p]$, we have

$$
\begin{aligned}
&V(\zeta_p) = V_2(\zeta_p) \leq e^{-\alpha_1\left|\bar{\Theta}(0,\zeta_p)\right|} e^{\alpha_2\left|\bar{\Xi}(0,\zeta_p)\right|} e^{n_*(0,\zeta_p)(\phi_1+\phi_2)} V_*(0) \\
&+\gamma_* \left[1 + 2 \sum_{\substack{m\in\mathbb{N}_0;\\ \zeta_m<\zeta_p}} e^{-\alpha_1\left|\bar{\Theta}(\zeta_m+v_m,\zeta_p)\right|} e^{\alpha_2\left|\bar{\Xi}(\zeta_m,\zeta_p)\right|} e^{n_*(\zeta_m,\zeta_p)(\phi_1+\phi_2)}\right] \|w(\zeta_p)\|_\infty^2
\end{aligned} \tag{86}
$$

where $V_*(t) = \max\{V_1(t), V_2(t)\}$, $\gamma_* = \max\{\gamma_3, \gamma_4\}$, $\phi_1 = 2\left(\ln \mu_2 - \ln \mu_1\right) + \left(\alpha_1 + \alpha_2\right)\mu_1 + \ln \delta_1$, $\phi_2 = \ln \delta_2$.

When $t \in Z_m$, we have from (41)

$$
V(t) \leq e^{\alpha_2(t-\zeta_p)} e^{\phi_1} V(\zeta_p) + \gamma_* e^{\alpha_2(t-\zeta_p)} e^{\phi_1} \|w(t)\|_\infty^2 . \tag{87}
$$

Since

$$
\left|\bar{\Xi}(0,t)\right| = \left|\bar{\Xi}(0,\zeta_p)\right| + t - \zeta_p, n_*(0,t) = n_*(0,\zeta_p) + 1 \tag{88}
$$

we have

$$
\begin{aligned}
V(t) &\leq e^{-\alpha_1\left|\bar{\Theta}(0,t)\right|} e^{\alpha_2\left|\bar{\Xi}(0,t)\right|} e^{n_*(0,t)(\phi_1+\phi_2)} V(0) \\
&\quad + \gamma_*[2 \sum_{\substack{m\in\mathbb{N}_0;\\ \zeta_m\leq t}} e^{-\alpha_1\left|\bar{\Theta}(\zeta_m+v_m,t)\right|} e^{\alpha_2\left|\bar{\Xi}(\zeta_m,t)\right|} e^{n_*(\zeta_m,t)(\phi_1+\phi_2)}] \|w(t)\|_\infty^2 .
\end{aligned} \tag{89}
$$

Then when $t \in W_m$, we have

$$
V(x(t)) \leq e^{-\alpha_1(t-\zeta_p-v_p)} e^{\alpha_2 v_p} e^{\phi_2} e^{\phi_1} V\left(x\left(\zeta_p\right)\right). \tag{90}
$$

Notice that

$$
\begin{aligned}
\left|\bar{\Xi}(0,t)\right| &= v_p + \left|\bar{\Xi}(0,\zeta_p)\right|, \left|\bar{\Theta}(0,t)\right| = t - \zeta_p - v_p + \left|\bar{\Theta}(0,\zeta_p)\right| \\
n_*(0,t) &= n_*(0,\zeta_p) + 1
\end{aligned} \tag{91}
$$

we can get

$$
\begin{aligned}
V(t) &\leq e^{-\alpha_1\left|\bar{\Theta}(0,t)\right|} e^{\alpha_2\left|\bar{\Xi}(0,t)\right|} e^{n_*(0,t)(\phi_1+\phi_2)} V(0) \\
&\quad + \gamma_*[1 + 2 \sum_{\substack{m\in\mathbb{N}_0;\\ \zeta_m\leq t}} e^{-\alpha_1\left|\bar{\Theta}(\zeta_m+v_m,t)\right|} e^{\alpha_2\left|\bar{\Xi}(\zeta_m,t)\right|} e^{n_*(\zeta_m,t)(\phi_1+\phi_2)}] \|w(t)\|_\infty^2 .
\end{aligned} \tag{92}
$$

Since that

$$
|\bar{\Xi}_*(\tau,t)| \leq |\Xi_*(\tau,t)| + (1 + n_*(\tau,t))\Delta_*, \tag{93}
$$

where Δ_* is the maximum trigger interval during the attack.
Then we have

$$
\begin{aligned}
|\bar{\Xi}(\tau,t)| &\leq (1-\lambda(\tau,t))(\kappa_* + \frac{t-\tau}{T_*}) + \left(1 + (1-\varphi(\tau,t))(\eta_* + \frac{t-\tau}{\tau_D^*})\right)\Delta_* \\
&\leq [((1-\lambda(\tau,t))\kappa_* + (1 + (1-\varphi(\tau,t))\eta_*)\Delta_*)] \\
&\quad + (t-\tau)\left(\frac{(1-\lambda(\tau,t))}{T_*} + \frac{(1-\varphi(\tau,t))\Delta_*}{\tau_D^*}\right) \\
&= \bar{\kappa}(\tau,t) + \frac{t-\tau}{\bar{T}(\tau,t)}.
\end{aligned} \tag{94}
$$

Where $\bar{\kappa}(\tau,t)=((1-\lambda(\tau,t))\kappa_*+(1+(1-\varphi(\tau,t))\eta_*)\Delta_*)$,$1/\bar{T}(\tau,t)=(1-\lambda(\tau,t))/T_*+(1-\varphi(\tau,t))\Delta_*/\tau_D^*$.
Then the maximum attack duration is denoted by v_m^*, that

$$\begin{aligned}&|\bar{\Xi}(\zeta_m,\zeta_m+v_m^*)|\le\bar{\kappa}(\zeta_m,\zeta_m+v_m^*)+\frac{v_m^*}{\bar{T}(\zeta_m,\zeta_m+v_m^*)}\\&\Rightarrow v_m^*\le\bar{\kappa}(\zeta_m,\zeta_m+v_m^*)+\frac{v_m^*}{\bar{T}(\zeta_m,\zeta_m+v_m^*)}\\&\Rightarrow v_m^*\le\frac{\bar{\kappa}(\zeta_m,\zeta_m+v_m^*)\bar{T}(\zeta_m,\zeta_m+v_m^*)}{\bar{T}(\zeta_m,\zeta_m+v_m^*)-1}.\end{aligned}\tag{95}$$

Since

$$\left|\bar{\Xi}\left(\zeta_m,t\right)\right|\le\bar{\kappa}(\zeta_m,t)+\frac{t-\zeta_m}{\bar{T}(\zeta_m,t)}\tag{96}$$

and

$$\left|\bar{\Theta}\left(\zeta_m+v_m,t\right)\right|=t-\zeta_m-\left|\bar{\Xi}\left(\zeta_m,t\right)\right|.\tag{97}$$

Let

$$\alpha_*=\left(\alpha_1+\alpha_2\right)\bar{\kappa}+\left(\phi_1+\phi_2\right)\bar{\varphi}\eta_*,\beta_*=\alpha_1-\frac{\left(\alpha_1+\alpha_2\right)}{\bar{T}}-\frac{\bar{\varphi}\left(\phi_1+\phi_2\right)}{\tau_D^*}\tag{98}$$

where $\bar{\kappa}=\bar{\kappa}(0,t)$,$\bar{\varphi}=\bar{\varphi}(0,t)$ and $\bar{T}=\bar{T}(0,t)$.
We have

$$e^{-\alpha_1\left|\bar{\Theta}(0,t)\right|}e^{\alpha_2\left|\bar{\Xi}(0,t)\right|}e^{n_*(0,t)(\phi_1+\phi_2)}\le e^{\alpha_*}e^{-\beta_*t}\tag{99}$$

and

$$\sum_{\substack{m\in\mathbb{N}_0;\\\zeta_m\le t}}e^{-\alpha_1\left|\bar{\Theta}(\zeta_m+v_m,t)\right|}e^{\alpha_2\left|\bar{\Xi}(\zeta_m,t)\right|}e^{n_*(\zeta_m,t)(\phi_1+\phi_2)}\le\sum_{\substack{m\in\mathbb{N}_0;\\\zeta_m\le t}}e^{\alpha_*}e^{-\beta_*(t-\zeta_m)}.\tag{100}$$

Since that

$$t-\zeta_m\ge\tau_D^*n_*(\zeta_m,t)-\tau_D^*\eta_*\tag{101}$$

we have

$$\sum_{\substack{m\in\mathbb{N}_0;\\\zeta_m\le t}}e^{-\beta_*(t-\zeta_m)}\le e^{\beta_*\tau_D^*\eta_*}\sum_{\substack{m\in\mathbb{N}_0;\\\zeta_m\le t}}e^{-\beta_*\tau_D^*n_*(\zeta_m,t)}.\tag{102}$$

Let $m(t)=\sup\{m\in\mathbb{N}_0|\zeta_m\le t\}$, we get

$$\sum_{\substack{m\in\mathbb{N}_0;\\\zeta_m\le t}}e^{-\beta_*\tau_D^*n_*(\zeta_m,t)}=\sum_{m=0}^{m(t)}e^{-\beta_*\tau_D^*n_*(\zeta_m,t)}.\tag{103}$$

Notice that $n_*(\zeta_m,t)=m(t)-m$, we have

$$\sum_{m=0}^{m(t)}e^{-\beta_*\tau_D^*n_*(\zeta_m,t)}=\sum_{m=0}^{m(t)}e^{-\beta_*\tau_D^*(m(t)-m)}=\sum_{m=0}^{m(t)}e^{-\beta_*\tau_D^*m}\le\frac{1}{1-e^{-\beta_*\tau_D^*}}.\tag{104}$$

We have

$$V(x(t)) \leq e^{\alpha_*} e^{-\beta_* t} V_*(0) + \gamma_* \left[1 + 2e^{\alpha_*} \frac{e^{\beta_* \tau_D^* \eta_*}}{1 - e^{-\beta * \tau_D^*}}\right] \|w(t)\|_\infty^2 . \tag{105}$$

We set $x(t) = \phi(t), t \in [-h, 0]$ for the supplemented initial condition in period $[-\mu_2, 0]$. Since$V(t) \geq \lambda_{\min}\{P_1, P_2\}\|x(t)\|^2, V(0) \leq \psi \|x(0)\|_{\mu_2}^2$, and $\psi = \lambda_{\max}\{P_1, P_2\}+\mu_2\lambda_{\max}\{Q_1, Q_2\}e^{\alpha_2\mu_2} + \left(\mu_2^3/2\right) \lambda_{\max}\{R_1, R_2\}e^{\alpha_2\mu_2}$ Then we have

$$\begin{aligned}\lambda_{\min}\{P_1, P_2\}\|x(t)\|^2 &\leq e^{\alpha_*} e^{-\beta_* t} V_*(0) + \gamma_* \left[1 + 2e^{\alpha_*} \frac{e^{\beta_* \tau_D^* \eta_*}}{1 - e^{-\beta * \tau_D^*}}\right] \|w(t)\|_\infty^2 \\ &\leq e^{\alpha_*} e^{-\beta_* t} \psi \|x(0)\|_{\mu_2}^2 + \gamma_* \left[1 + 2e^{\alpha_*} \frac{e^{\beta_* \tau_D^* \eta_*}}{1 - e^{-\beta * \tau_D^*}}\right] \|w(t)\|_\infty^2 .\end{aligned} \tag{106}$$

Let ω=$\lambda_{\min}\{P_1, P_2\}$, we get

$$\|x(t)\| \leq e^{\frac{\alpha_*}{2}} e^{-\frac{\beta_*}{2} t} \sqrt{\frac{\psi}{\omega}} \|x(0)\|_{\mu_2} + \sqrt{\frac{\gamma_*}{\omega}} \left[1 + 2e^{\alpha_*} \frac{e^{\beta_* \tau_D^* \eta_*}}{1 - e^{-\beta * \tau_D^*}}\right]^{\frac{1}{2}} \|w(t)\|_\infty . \tag{107}$$

Then if

$$\beta_* > 0 \Leftrightarrow \alpha_1 > \frac{(\alpha_1 + \alpha_2)}{\bar{T}} + \frac{\bar{\varphi}\,(\phi_1 + \phi_2)}{\tau_D^*} \tag{108}$$

then the system (37) is ISS.

6.3. Proof of Theorem 2

Let $T_i = P_i^{-1}$, $\bar{Q}_i = T_i Q_i T_i$, $\bar{R}_i = T_i R_i T_i$, $\bar{\Omega}_i = T_i \Omega_i T_i$,$\bar{X}_{i1} = T_i X_{i1} T_i$, $\bar{X}_{i2} = T_i X_{i2} T_i$, $\bar{X}_{i3} = T_i X_{i3} T_i$, $\bar{X}_{i4} = T_i X_{i4} T_i$, $Y_i = K_i T_i$, define $J_1 = diag\{T, T, T, T, T, T, R^{-1}\}$ and $J_2 = diag\{T, T, T, T, T, T, R^{-1}\}$, then pre- and post-multiply J_1 and its transpose on both sides of (39), pre- and post-multiply J_1 and its transpose on both sides of (40), we can obtain (46) and (47). Utilizing the similar technique, pre- and post-multiply $T_i (i = 1, 2)$ and its transpose on both sides of the left and right inequalities in (43), (44)and (45), respectively, then by using the basic inequalities $-\bar{T}\bar{R}^{-1}\bar{T} \leq \varpi^2 \bar{R} - 2\varpi\bar{T}, \varpi > 0$ and Schur complement, we can obtain (48), (49)and (50).

ACKNOWLEDGEMENT

This work was supported by the National Natural Science Foundation of China under Grant 61833011, 61673255 and 61773356, and the Outstanding Academic Leader Project of Shanghai Science and Technology Commission under Grant 18XD1401600, the Project 111 under Grant D18003.

(Received September 15, 2019)

REFERENCES

[1] S. Amin, G. A. Schwartz, and S. Sastry: Security of interdependent and identical networked control systems. Automatica *49* (2013), 186–192. DOI:10.1016/j.automatica.2012.09.007

[2] A. A. Cardenas, S. Amin, S. Sastry et al: Secure control: Towards survivable cyber-physical systems. In: Proc. 28th International Conference on Distributed Computing Systems Workshops, Beijing 2008, pp. 495–500. DOI:10.1109/icdcs.workshops.2008.40

[3] A. Cetinkaya, H. Ishii, and T. Hayakawa: Networked control under random and malicious packet losses. IEEE Trans. Automat. Control *62* (2017), 2434–2449. DOI:10.1109/tac.2016.2612818

[4] Y. H. Chang, Q. Hu, Qie, and C. J. Tomlin: Secure estimation based Kalman filter for cyber-physical systems against sensor attacks. Automatica *95* (2018), 399–412. DOI:10.1016/j.automatica.2018.06.010

[5] D. Ding, Q.-L. Han, Z. Wang et al: A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Trans. Industr. Inform. *15* (2019), 2483–2499. DOI:10.1109/tii.2019.2905295

[6] J. P. Farwell and R. Rohozinski: Stuxnet and the future of cyber war. Survival *53* (2011), 23–40. DOI:10.1080/00396338.2011.555586

[7] S. Feng, and P. Tesi: Resilient control under denial-of-service: Robust design. Automatica *79* (2017), 42–51. DOI:10.1016/j.automatica.2017.01.031

[8] X. Ge, Q.-L. Han, and Z. Wang: A threshold-parameter-dependent approach to designing distributed event-triggered H_∞ consensus filters over sensor networks. IEEE Trans. Cybernet. *49* (2019), 1148–1159. DOI:10.1109/tcyb.2017.2789296

[9] X. Ge, Q.-L. Han, X.-M. Zhang et al: Distributed event-triggered estimation over sensor networks: A survey. IEEE Trans. Cybernet. *50* (2019), 3, 1306–1320 DOI:10.1109/tcyb.2019.2917179

[10] X. Ge, Q.-L. Han, M. Zhong, and X.-M. Zhang: Distributed Krein space-based attack detection over sensor networks under deception attacks. Automatica *109* (2019), 108557. DOI:10.1016/j.automatica.2019.108557

[11] W. P. M. H. Heemels, M. C. F. Donkers, and A. R. Teel: Periodic event-triggered control for linear systems. IEEE Trans. Automat. Control *58* (2013), 847–861. DOI:10.1109/tac.2012.2220443

[12] S. Hu, D. Yue, Q.-L. Han et al: Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. IEEE Trans. Cybernet. (2019), 1–13. DOI:10.1109/tcyb.2019.2903817

[13] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin: Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans. Cybernet. *49* (2019), 4271–4281. DOI:10.1109/tcyb.2018.2861834

[14] S. Kim, Y. Won, I.-H. Park, Y. Eun, and K.-J. Park: Cyber-physical vulnerability analysis of communication-based train control. IEEE Internet Things J. *6* (2019), 6353–6362. DOI:10.1109/jiot.2019.2919066

[15] Ch. Kwon and I. Hwang: Cyber attack mitigation for cyber-physical systems: hybrid system approach to controller design. IET Control Theory Appl. *10* (2016), 731–741. DOI:10.1049/iet-cta.2014.1013

[16] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong: The 2015 Ukraine blackout: Implications for false data injection attacks. IEEE Trans. Power Syst. *32* (2017), 3317–3318. DOI:10.1109/tpwrs.2016.2631891

[17] J. Liu, M. Yang, X. Xie et al: Finite-time H_∞ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks. IEEE Trans. Circuits Systems I: Regular Papers /2019), 1–14..

[18] A.-Y. Lu and G.-H. Yang: Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Trans. Automat. Control *63* (2018), 1813–1820. DOI:10.1109/tac.2017.2751999

[19] P. Millan, L. Orihuela, I. Jurado et al: Distributed estimation in networked systems under periodic and event-based communication policies. Int. J. Systems Sci. *46* (2015), 139–151. DOI:10.1080/00207721.2013.775387

[20] C. Peng, and H. T. Sun: Switching-like event-triggered control for networked control systems under malicious denial of service attacks. IEEE Trans. Automat. Control (2020) DOI:10.1109/tac.2020.2989773

[21] Y. Mo, S. Weerakkody, and B. Sinopoli: Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. IEEE Control Systems Mag. *35* (2015), 93–109. DOI:10.1109/mcs.2014.2364724

[22] M. Muehlebach and S. Trimpe: Distributed event-based state estimation for networked systems: An LMI approach. IEEE Trans. Automat. Control *63* (2018), 269–276. DOI:10.1109/tac.2017.2726002

[23] F. Pasqualetti, F. Dorfler, and F. Bullo: Attack detection and identification in cyber-physical systems. IEEE Trans. Automat. Control *58* (2013), 2715–2729. DOI:10.1109/tac.2013.2266831

[24] C. Peng, J. Li, and M. Fei: Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks. IEEE Trans. Power Syst. *32* (2017), 4110–4118. DOI:10.1109/tpwrs.2016.2634122

[25] C. Peng, S. Ma, and X. Xie: Observer-based non-PDC control for networked T-S fuzzy systems with an event-triggered Communication. IEEE Trans. Cybernet. *47* (2017), 2279–2287. DOI:10.1109/tcyb.2017.2659698

[26] C. Peng, H. Sun, M. Yang, and Y. Wang: A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Trans. Systems Man Cybernet.: Systems *49* (2019), 1554–1569. DOI:10.1109/tsmc.2018.2884952

[27] C. de Persis and P. Tesi: Input-to-state stabilizing control under denial-of-service. IEEE Trans. Automat. Control *60* (2015), 2930–2944. DOI:10.1109/tac.2015.2416924

[28] A. Seuret and F. Gouaisbaut: Wirtinger-based integral inequality: Application to time-delay systems. Automatica *49* (2013), 2860–2866. DOI:10.1016/j.automatica.2013.05.030

[29] Y.-Ch. Sun and G.-H. Yang: Event-triggered resilient control for cyber-physical systems under asynchronous DoS attacks. Inform. Sci. *465* (2018), 340–352. DOI:10.1016/j.ins.2018.07.030

[30] P. Tabuada: Event-triggered real-time scheduling of stabilizing control tasks. IEEE Trans. Automat. Control *52* (2007), 1680–1685. DOI:10.1109/tac.2007.904277

[31] L. Van Do, L. Fillatre, I. Nikiforov et al: Security of SCADA systems against cyber-physical attacks. IEEE Aerospace Electron. Systems Mag. *32* (2017), 28–45. DOI:10.1109/maes.2017.160047

[32] S. Xiaon, Q.-L. Han, X. Ge, and Y. Zhang: Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks. IEEE Trans. Cybernet. *50* (2019), 3, 1220–1229. DOI:10.1109/tcyb.2019.2900478

[33] X. Xie, D. Yue, and Ch. Peng: Relaxed real-time scheduling stabilization of discrete-time takagi-sugeno fuzzy systems via a alterable-weights-based ranking switching mechanism. IEEE Trans. Cybernet. *26* (2018), 3808–3819. DOI:10.1109/tfuzz.2018.2849701

[34] X.-M. Zhang, Q.-L. Han, X. Ge et al: Networked control systems: A survey of trends and techniques. IEEE/CAA J. Automat. Sinica (2019), 1–17.

[35] X.-M. Zhang, Q.-L. Han, X. Ge et al: Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks. IEEE Trans. Cybernet. (2019), 1–11.

[36] X.-M. Zhang, Q.-L. Han, A. Seuret, and F. Gouaisbaut: An improved reciprocally convex inequality and an augmented Lyapunov–Krasovskii functional for stability of linear systems with time-varying delay. Automatica *84* (2017), 221–226. DOI:10.1016/j.automatica.2017.04.048

Huaye Peng, School of Mechanical Engineering and Automation, Shanghai University, Shanghai, 200444. P. R. China.
e-mail: phuaye@shu.deu.cn

Chen Peng, School of Mechanical Engineering and Automation, Shanghai University, Shanghai, 200444. P. R. China.
e-mail: c.peng@shu.edu.cn

Yong Shao, School of Mechanical Engineering and Automation, Shanghai University, Shanghai, 200444. P. R. China.
e-mail: shaoyong@shu.edu.cn

Deliang Zeng, School of Control and Computer Engineering, North China Electric Power, Beijing 102206. P. R. China.
e-mail: zdl@ncepu.edu.cn