

Distributed Event-Triggered Consensus Control of Multi-Agent Systems under Denial-of-Service Jamming Attacks

Mingyue Xiong · Xin Wang · Jun Cheng

Received: date / Accepted: date

Abstract This work focuses on the consensus problem of multi-agent systems (MASs) under event-triggered control (ETC) subject to denial-of-service (DoS) jamming attacks. To reduce the cost of communication networks, a novel event-triggering mechanism (ETM) is applied to the sleeping interval to determine whether the sampled signal should be transmitted or not. Unlike periodic DoS attacks model, the DoS attacks occurrence are irregular, where attack attributes such as attack frequency and attack duration are taken into account. Moreover, compared with the fixed topological graph, the communication topologies may change due to DoS jamming attacks in this work. In view of this, based on the piecewise Lyapunov functional, sufficient conditions are derived to guarantee that consensus problem of the MASs can be solved. Finally, the effectiveness and correctness of the theoretical results are verified by a numerical example.

Keywords Multi-agent Systems · Event-triggering mechanism · DoS jamming attacks · Consensus

1 Introduction

In recent years, the consensus control issue of MASs has been diffusely investigated and received tremendous attention in many domains, such as teaming of robots, traffic control, formation control and so on [1–6].

M. Xiong · X. Wang (✉)
College of Electronic and Information Engineering, Southwest University, Chongqing 400715, China
E-mail: xinwang201314@126.com

J. Cheng
College of Mathematics and Statistics, Guangxi Normal University, Guilin 541006, China
E-mail: jcheng6819@126.com

Generally speaking, consensus control aims to design a valid distributed control protocol that uses the information of adjacent agents in the system to make the state of all agents reach an agreement. Until now, various distributed control schemes have been developed for leader-following consensus problems [7, 8] and leaderless consensus problems [9–12].

However, when discussing the consensus problems of MASs, some existing results are based on ideal conditions of infinite network resources [9–12]. To minimize the waste of communication and computing resources, a time-triggering mechanism was first proposed for MASs in [13], which transmits measurements after fixed time intervals. Unfortunately, this strategy may still cause unnecessary communication and consumption of computing resources. To further address this issue, various ETC strategies were proposed [14–19], where the data will be broadcasted depends whether the pre-designed event-triggering condition is met or not. For example, the authors in [14] proposed a centralized output feedback ETC to achieve consensus of linear MASs. By applying the centralized ETC protocol, leader-following consensus issue of MASs with different structure of topologies was investigated in [15]. Wang et al. [16] introduced a centralized ETC scheme with internal dynamic variables to investigate the consensus issue of MASs. It is noteworthy that centralized ETC approaches require information from all agents of MASs, which may cause unnecessary waste of resources. To improve the limited network resources, distributed ETC strategies were proposed for MASs in [17–20]. A new iterative event-triggered analysis method was proposed in [17] to avoid continuous sampling transmission between adjacent states in MASs. In [18], the authors proposed a new event-triggered distributed predictive control method, which not only realizes the asynchronous

exchange of information, but also achieves the balance between efficient resource utilization and control performance. To solve the issue of robust cooperative output regulation for uncertain linear MASs with and without extra disturbances, two adaptive ETC protocols based on internal model theories were proposed in [19], where the frequency of information exchange between agents is greatly reduced and Zeno behavior is excluded.

Furthermore, with the development of spatially distributed technology, MASs are usually considered to be a class of networked control systems that are brittle to cyber-attacks [21]. The communication channel between agents is easily interrupted or broken due to cyber-attacks, which will lead to the unavailability of information exchange between agents and system instability [22]. Therefore, it is essential to discuss the impacts of cyber-attacks in the investigation of various MASs [23–26]. In general, cyber-attacks can be categorized into deception attacks [27–29], replay attacks [30–32] and DoS jamming attacks [33–35]. Among them, DoS jamming attack is the most important and difficult to address. The authors considered asynchronous DoS jamming attacks in [36], where MASs can achieve consensus by restricting the frequency and duration of valid DoS jamming attacks. In [37], the authors established a hybrid dynamic model for the formation control of nonlinear MASs under DoS jamming attacks, which gives the calculation method of transmission interval with DoS attacks. Based on a novel security controller, the frequency and duration of DoS jamming attacks were obtained in [7] to guarantee that the tracking error system converges to zero for MASs under the DoS jamming attacks. The authors in [8] developed a distributed security consensus control method for leader-following MASs with DoS jamming attacks, which successfully overcome the issue of inaccurate control input calculation within the attacking periods. By taking the DoS jamming attacks into account, leader-following robust H_∞ consensus of heterogeneous MASs was presented in [33]. However, how to design a distributed event-triggered controller to achieve consensus of MASs in the presence of DoS jamming attacks, which still an open challenge issue and motivates this work.

In this article, we investigate the consensus issue of MASs under DoS jamming attacks by a distributed event-triggered controller. The main contributions of this paper are summarized as follows.

1) Compared with [22,38,39] where the periodic DoS jamming attacks are considered, the aperiodic DoS jamming attacks are proposed by a time-sequence way in this work, which are more general in practice.

2) Different from the centralized ETC approaches in [14–16], a distributed discrete ETC method is pro-

posed in this work to avoid continuous information exchange among adjacent agents, which not only improves the network communication but also achieves consensus control for MASs under DoS jamming attacks.

3) Different from [21,40] where the DoS jamming attacks active/sleeping periods need to known, this work does not need such restrictions as the attack frequency and duration of DoS jamming attacks are analyzed.

Notations:

\mathbb{R}^n	n -dimensional real vector space
$\mathbb{R}^{n \times m}$	$n \times m$ real matrix
T	matrix transposition
$\ \cdot\ $	2-norm
I_N	N -dimensional identity matrix
I	identity matrix with appropriate dimension
\otimes	Kronecker product
$\lambda_{max}(X)$	the maximum eigenvalue of X
$\lambda_{min}(X)$	the minimum eigenvalue of X
\mathbb{N}	the set of non-negative integers
$P > 0$	real symmetric matrix P is positive definite

2 Preliminary and Problem Formulation

2.1 Graph theory

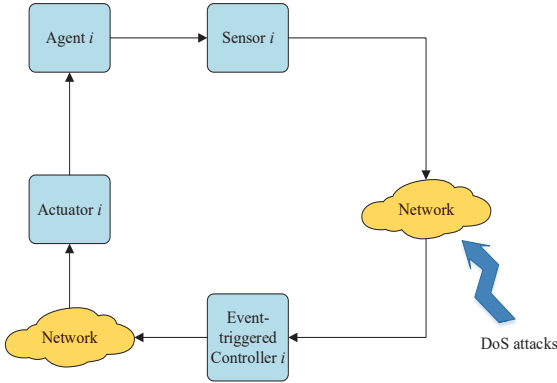
A directed graph is represented by $\mathbb{G} = (\mathbb{P}, \mathbb{B}, \mathbb{W})$ where $\mathbb{P} = \{1, 2, \dots, N\}$ denotes a set of nodes, $\mathbb{B} \subseteq \{(i, j), i, j \in \mathbb{P}\}$ denotes a set of edges, and $\mathbb{W} = [w_{ij}]_{N \times N}$ denotes a weighted adjacency matrix with non-negative element w_{ij} , $i, j = 1, 2, \dots, N$. The ordered pair of nodes (p_i, p_j) represents an edge b_{ij} in the graph \mathbb{G} , and $b_{ij} \in \mathbb{B}$ if and only if $w_{ij} > 0$. And an element $\{b_{ij} = (p_i, p_j)\} \in \mathbb{B}$ denotes that node i can obtain information from node j . Laplacian matrix $L = [l_{ij}]_{N \times N}$ of \mathbb{G} as $L = \bar{W} - \mathbb{W}$ where $\bar{W} = \text{diag}\{W_1, \dots, W_N\}$ with $W_i = \sum_{j \in N_i} w_{ij}$. If there exists one node that can reach any other node through a directed path, we can say \mathbb{G} has a directed spanning tree.

2.2 System Model

Consider the MASs consisting of N agents, a model of the i th agent shown in Fig. 1 can be represented as:

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t) + Cf(x_i(t)), \quad (1)$$

where $x_i(t) \in \mathbb{R}^n$ is the state variable, $u_i(t) \in \mathbb{R}^m$ is the control input of the i th agent. A , B , and C are real matrices with appropriate dimensions. $f(x_i(t))$ is a nonlinear vector-valued function satisfying the following assumption.


 Fig. 1: Structure of ETC for agent i .

Assumption 1: The nonlinear function $f(x_i(t))$ satisfies the following condition:

$$\|f(x_i(t))\| \leq \|Hx_i(t)\|,$$

where H is a known constant matrix representing the upper bound of the nonlinearity.

2.3 Denial-of-Service Attack Model

As a result of the openness of networks, the communication channels are easily destroyed by malicious attacks, which is one of the main factors threatening the security of the system. Then, the sampled data transmitted over the communication networks may be lost and the whole network may collapse in serious cases. In addition, the cyber-attacks may also destroy the communication topology of MASSs.

This paper considers the case that the communication networks are disrupted by DoS jamming attacks when transmitting the measurement signals. It should be noted that DoS jamming attacks require a certain amount of energy. Assume that malicious attackers will consume a certain amount of energy when sending DoS jamming signals. Therefore, the attackers need to enter a sleep state to save energy for the next attacks. Fig. 2 shows an example of signal transmission via an event-triggering mechanism (ETM) under the DoS jamming attacks model.

Let $\{l_n\}_{n \in \mathbb{N}}$ denote the time sequence of the DoS jamming attacks, and a DoS jamming attack is launched at time instants l_n . $L_{1,n} = [l_n, l_n + \Delta_n)$ denotes the interval of the $(n+1)$ -th DoS jamming attacks, where Δ_n indicates the length of the $(n+1)$ -th DoS jamming attacks satisfying $l_{n+1} > l_n + \Delta_n$. $L_{2,n} = [l_n + \Delta_n, l_{n+1})$ represent the sleeping period of the DoS jamming attacks.

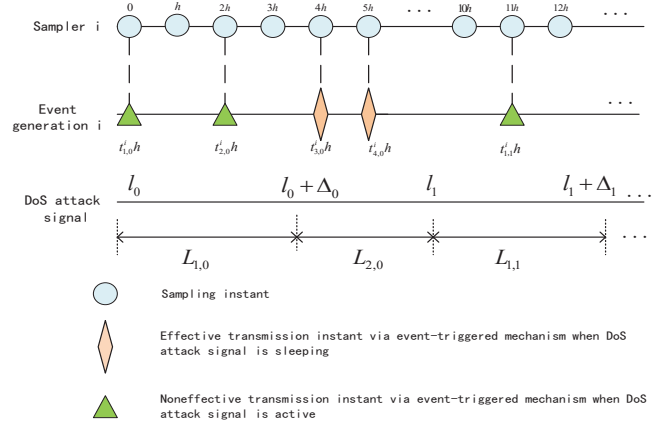


Fig. 2: Example of transmitted signals via an ETM under DoS jamming attacks.

Similar to [41], for given t and ι

$$F_a(\iota, t) = \bigcup_{n \in \mathbb{N}} L_{1,n} \cap [\iota, t), \quad (2)$$

$$F_c(\iota, t) = [\iota, t) \setminus F_a(\iota, t). \quad (3)$$

$F_a(\iota, t)$ and $F_c(\iota, t)$ denote sets of time intervals for the active and sleeping intervals of DoS jamming attacks, respectively.

The following assumptions are introduced to describe the attack duration and the attack frequency.

Assumption 2: (Attack Duration [42]) For any $\mathbb{T}_2 > \mathbb{T}_1 > t_0$, $F_a(\mathbb{T}_1, \mathbb{T}_2) \leq \mathbb{T}_0 + \frac{\mathbb{T}_2 - \mathbb{T}_1}{\tau_a}$ represent attack duration over $[\mathbb{T}_1, \mathbb{T}_2)$ for all $\mathbb{T}_0 \geq 0$ and $\tau_a > 0$.

Assumption 3: (Attack Frequency [42]) For any $\mathbb{T}_2 > \mathbb{T}_1 > t_0$, $N_f(\mathbb{T}_1, \mathbb{T}_2)$ represent the total number of DoS jamming attack occurring over $[\mathbb{T}_1, \mathbb{T}_2)$. Then, $F_f(\mathbb{T}_1, \mathbb{T}_2) = \frac{N_f(\mathbb{T}_1, \mathbb{T}_2)}{\mathbb{T}_2 - \mathbb{T}_1}$ denote the attack frequency over $[\mathbb{T}_1, \mathbb{T}_2)$ for all $\mathbb{T}_2 > \mathbb{T}_1 > t_0$.

2.4 A Distributed Event-Triggered Consensus Protocol

In order to alleviate the communication load of the networks, inspired by [40], a distributed ETM is designed. By using this mechanism, sample data of each agent will not be transmitted through the network unless the event-triggering condition is met. Under the mechanism, the triggering instant is described by:

$$t_{k+1,n}h = t_{k,n}h + \min_{m \geq 1} \left\{ mh | (\psi_{k,n}^i(t))^\top \Omega_i \psi_{k,n}^i(t) > \sigma x_i^\top(t_{k,n}h + mh) \Omega_i x_i(t_{k,n}h + mh) \right\}, \quad (4)$$

where parameter $\sigma \in [0, 1)$, $\Omega_i > 0$, $m \in \mathbb{N}^+$, $mh \in (t_{k,n}h, t_{k+1,n}h]$ denotes the m -th sampling instant, and $\psi_{k,n}^i(t) = x_i(t_{k,n}h) - x_i(t_{k,n}h + mh)$, $t_{k,n}h$ as the k th triggered instant in $L_{2,n}$, $k \in \{1, 2, \dots, k_m\}$, $k_m = \sup\{k | t_{k,n}h < l_{n+1}\}$, denote $t_{1,n}h = l_n + \Delta_n$, $t_{k_m+1,n}h = l_{n+1}$.

Remark 1: From (4), we can see that only the sampled data satisfying the triggering condition will be transmitted through the network, which greatly reduces the network resources. Note that h denotes the discrete sampling period of the sensors, so-called Zeno behavior will not happen here. If $\sigma = 0$, then the proposed ETM will turn into a time-triggering mechanism.

Remark 2: Combined with the more common scenario in practice, assuming that the triggering condition is not met in $L_{2,n}$, there will be a situation that $t_{k_m+1,n}h$ does not exist. Compared with [22] and [43] where the above case is not considered, we define $t_{k_m+1,n}h = l_{n+1}$ when the triggering condition is invalid in this paper, which makes the article more organized.

Partitioning $L_{2,n}$ into the triggering interval $\varpi_{k,n} = [t_{k,n}h, t_{k+1,n}h)$, $k = 1, 2, \dots, k_m$. Then it has $\Theta_{k,n} = \varpi_{k,n} \cap L_{2,n}$, we can get $L_{2,n} = \bigcup_{k=1}^{k_m} \Theta_{k,n}$. Then $\varpi_{k,n}$ can be divided as $\varpi_{k,n} = \bigcup_{L=0}^{L_m} \Xi_{L,k}$ where $\Xi_{L,k} = [t_{k,n}h + Lh, t_{k,n}h + (L+1)h)$, $L \in \{0, 1, \dots, L_m\}$, $L_m = \sup\{L | t_{k,n}h + Lh < t_{k+1,n}h\}$. It is obvious that $L_{2,n} = \bigcup_{k=1}^{k_m} \bigcup_{L=0}^{L_m} \Xi_{L,k} \cap \Theta_{k,n}$.

According to the above analysis, the ETC is described by:

$$u_i(t) = \begin{cases} \alpha K \sum_{j \in N_i} w_{ij}^{\sigma(t)} (x_j(t_{k,n}h) - x_i(t_{k,n}h)), & \text{if } t \in \Xi_{L,k} \cap \Theta_{k,n} \cap L_{2,n}, \\ 0, & \text{if } t \in L_{1,n}, \end{cases} \quad (5)$$

where $\alpha > 0$ denotes the coupling strength of the MASs, K is the controller gain, $\sigma(t)$ is a piecewise function, $\sigma(t) : [0, +\infty) \rightarrow S = \{1, 2, \dots, s\}$ is utilized to describe the switching signal, and $\mathbb{G}^{\sigma(t)} \in \tilde{\mathbb{G}}$, for $t \in \Xi_{L,k} \cap \Theta_{k,n} \cap L_{2,n}$, where $\tilde{\mathbb{G}} = \{\mathbb{G}^1, \mathbb{G}^2, \dots, \mathbb{G}^s\}$, $s > 1$, represents the set of all possible topological graphs when the MASs recover from DoS attacks. $w_{ij}^{\sigma(t)}$ stands for the adjacency element of $\mathbb{G}^{\sigma(t)}$. $x_i(t_{k,n}h)$ is the latest broadcast state of agent i with a time sequence $\{t_{k,n}h\}_{k \in \mathbb{N}}$.

In what follows, we can define $\tau_{L,k}(t) \in [0, h)$ as time varying delay variable

$$\tau_{L,k}(t) = \begin{cases} t - t_{k,n}h & t \in \Xi_{0,k} \\ \vdots & \\ t - t_{k,n}h - (L_m - 1)h & t \in \Xi_{L,k} \\ t - t_{k,n}h - L_m h & t \in \Xi_{L_m,k} \end{cases}$$

and

$$\psi_{k,n}^i(t) = \begin{cases} 0 & t \in \Xi_{0,k} \\ \vdots & \\ x_i(t_{k,n}h) - x_i(t_{k,n}h + (L_m - 1)h) & t \in \Xi_{L,k} \\ x_i(t_{k,n}h) - x_i(t_{k,n}h + L_m h) & t \in \Xi_{L_m,k} \end{cases}$$

Further, the event-triggered sampled states $x_i(t_{k,n}h)$ and $x_j(t_{k,n}h)$ can be given as follows:

$$\begin{cases} x_i(t_{k,n}h) = \psi_{k,n}^i(t) + x_i(t - \tau_{L,k}(t)), \\ x_j(t_{k,n}h) = \psi_{k,n}^j(t) + x_j(t - \tau_{L,k}(t)). \end{cases} \quad (6)$$

Then, the controller (5) can be rewritten as

$$u_i(t) = \begin{cases} \alpha K \sum_{j \in N_i} w_{ij}^{\sigma(t)} (\psi_{k,n}^j(t) + x_j(t - \tau_{L,k}(t))) \\ -\psi_{k,n}^i(t) - x_i(t - \tau_{L,k}(t)), & \text{if } t \in \Xi_{L,k} \cap \Theta_{k,n} \cap L_{2,n}, \\ 0, & \text{if } t \in L_{1,n}. \end{cases} \quad (7)$$

Substituting (7) into (1), we have

$$\dot{x}(t) = \begin{cases} (I_N \otimes A)x(t) - \alpha(L^{\sigma(t)} \otimes BK)x(t - \tau_{L,k}(t)) \\ -\alpha(L^{\sigma(t)} \otimes BK)\psi_{k,n}(t) + (I_N \otimes C)F(x(t)), & \text{if } t \in \Xi_{L,k} \cap \Theta_{k,n} \cap L_{2,n}, \\ (I_N \otimes A)x(t) + (I_N \otimes C)F(x(t)), & \text{if } t \in L_{1,n}, \end{cases} \quad (8)$$

where $F(x(t)) = [f^T(x_1(t)), \dots, f^T(x_N(t))]^T$, $L^{\sigma(t)} = [l_{ij}^{\sigma(t)}]_{N \times N}$, $\psi_{k,n}(t) = [(\psi_{k,n}^1(t))^T, \dots, (\psi_{k,n}^N(t))^T]^T$, $x(t - \tau_{L,k}(t)) = [x_1^T(t - \tau_{L,k}(t)), \dots, x_N^T(t - \tau_{L,k}(t))]^T$, and $x(t) = [x_1^T(t), \dots, x_N^T(t)]^T$. And $\phi(t)$ is the supplemented initial condition of the state $x(t)$ with $\phi(0) \triangleq \phi_0$.

The aim of this article is to devise an event-triggering controller to converge the states of all agents to a consistent level. In view of this, we need the following lemma.

Lemma 1: [44] For any matrices $F \in \mathbb{R}^{n \times n}$ and $\Lambda \in \mathbb{R}^{n \times n}$ that satisfy $\begin{bmatrix} F & * \\ \Lambda^T & F \end{bmatrix} \geq 0$, the following inequality holds for $\kappa(t) \in [0, \bar{\kappa}]$:

$$\begin{aligned} & -\bar{\kappa} \int_{t-\bar{\kappa}}^t \dot{\delta}^T(s) F \delta(s) ds \\ & \leq \delta(t)^T \begin{bmatrix} -F & * & * \\ F^T - \Lambda^T & -2F + \Lambda + \Lambda^T & * \\ \Lambda^T & F^T - \Lambda^T & -F \end{bmatrix} \delta(t) \end{aligned}$$

where $\tilde{o}(t) = \begin{bmatrix} o(t) \\ o(t - \kappa(t)) \\ o(t - \bar{\kappa}) \end{bmatrix}$, and $*$ is utilized to depict the entries implied by symmetry.

3 Main results

The following section mainly consists of two theorems, before given Theorem 1, we first present the Lemma 2. Then, sufficient conditions are derived to guarantee the exponential stability of the closed-loop system (8) under DoS jamming attacks in Theorem 1. In Theorem 2, we solve the problem of system parameters.

Consider following piecewise Lyapunov functional:

$$V_f(t) = V_{f1}(t) + V_{f2}(t) + V_{f3}(t), \quad (9)$$

where $f = 1$, when $t \in [\Xi_{L,k} \cap \Theta_{k,n} \cap L_{2,n})$, and $f = 2$, when $t \in L_{1,n}$,

$$V_{f1}(t) = x^T(t)(I_N \otimes P_f)x(t)$$

$$V_{f2}(t) = \int_{t-h}^t e^{(-1)^f \mu_f(t-\theta)} x^T(\theta) R_f x(\theta) d\theta$$

$$V_{f3}(t) = h \int_{t-h}^t \int_{\theta}^t e^{(-1)^f \mu_f(t-\varphi)} \dot{x}^T(\varphi) Z_f \dot{x}(\varphi) d\varphi d\theta$$

Lemma 1 For given scalars $h > 0$, $\mu_1 > 0$, $\mu_2 > 0$, $\sigma > 0$, and matrices K , H , the functions defined in (9) satisfy

$$\begin{aligned} V_1(t) &\leq e^{-\mu_1(t-(l_n+\Delta_n))} V_1(l_n + \Delta_n), \\ V_2(t) &\leq e^{\mu_2(t-l_n)} V_2(l_n), \end{aligned} \quad (10)$$

if there exist matrices $P_f > 0$, $R_f > 0$, $Z_f > 0$, and $\Omega > 0$, U_f with appropriate dimensions satisfying :

$$\omega_f < 0, \quad (11)$$

$$0 < \begin{bmatrix} Z_f & * \\ U_f & Z_f \end{bmatrix}, \quad f = 1, 2, \quad (12)$$

where the elements of ω_f are described in detail in Appendix A.

Proof See Appendix B.

Based on Lemma 2, we will analyze of exponential stability of system (8) under DoS jamming attacks.

Theorem 1. For given scalars $h > 0$, $\mu_1 > 0$, $\mu_2 > 0$, $\lambda_1 > 0$, $\lambda_2 > 0$, and matrices K , H , if Lemma 2 holds and there exist matrices $P_f > 0$, $R_f > 0$, $Z_f > 0$, $f = 1, 2$ and $\Omega > 0$, U_f with compatible dimensions satisfying the following conditions:

$$I_N \otimes P_1 < \lambda_2(I_N \otimes P_2), \quad (13)$$

$$I_N \otimes P_2 < \lambda_1 e^{(\mu_1 + \mu_2)h} (I_N \otimes P_1),$$

$$R_f - \lambda_{3-f} R_{3-f} < 0, \quad (14)$$

$$Z_f - \lambda_{3-f} Z_{3-f} < 0 \quad (15)$$

and

Attack Frequency:

$$F_f(0, t) = \frac{N_f(0, t)}{t} \leq \frac{\mu_1^* + T_D}{\ln(\lambda_1 \lambda_2) + (\mu_1 + \mu_2)h}, \quad (16)$$

where $\mu_1^* \in (0, \mu_1)$, $\mu_1 - \mu_1^* \geq T_D \geq 0$.

Attack Duration:

$$\tau_a \geq \frac{\mu_1 + \mu_2}{\mu_1 - \mu_1^* - T_D}. \quad (17)$$

Then, the closed-loop system (8) is exponential stable with the ETC under DoS jamming attacks.

Proof $V_1(t)$ and $V_2(t)$ are describable at different time intervals, it follows that:

$$V(t) = \begin{cases} e^{-\mu_1(t-l_{n-1}-\Delta_{n-1})} V_1(l_{n-1} + \Delta_{n-1}), & \text{if } t \in [l_{n-1} + \Delta_{n-1}, l_n), \\ e^{\mu_2(t-l_n)} V_2(l_n) & \text{if } t \in [l_n, l_n + \Delta_n). \end{cases} \quad (18)$$

If $t \in [l_{n-1} + \Delta_{n-1}, l_n)$, we can get

$$\begin{aligned} V(t) &\leq \lambda_2 e^{-\mu_1(t-l_{n-1}-\Delta_{n-1})} V_1((l_{n-1} + \Delta_{n-1})^-) \\ &\quad \vdots \\ &\leq e^{n[\ln(\lambda_1 \lambda_2) + (\mu_1 + \mu_2)h]} e^{\mu_2 |F_a(0,t)|} e^{-\mu_1 |F_c(0,t)|} V_1(0). \end{aligned} \quad (19)$$

If $t \in [l_n, l_n + \Delta_n)$, it leads to

$$\begin{aligned} V(t) &\leq \lambda_1 e^{\mu_2(t-l_n)} e^{(\mu_1 + \mu_2)h} V_2(l_n^-) \\ &\quad \vdots \\ &\leq e^{(n+1)[\ln(\lambda_1 \lambda_2) + (\mu_1 + \mu_2)h]} e^{\mu_2 |F_a(0,t)|} e^{-\mu_1 |F_c(0,t)|} V_1(0). \end{aligned} \quad (20)$$

Combining (19) and (20), it is easy to get:

$$\begin{aligned} V(t) &\leq e^{(n+1)[\ln(\lambda_1 \lambda_2) + (\mu_1 + \mu_2)h]} \\ &\quad \times e^{\mu_2 |F_a(0,t)|} e^{-\mu_1 |F_c(0,t)|} V_1(0). \end{aligned} \quad (21)$$

Besides, according to the property of the Assumption 3, we can know the number of DoS jamming attacks in the interval $[0, t]$ is $N_f(0, t) = n + 1$. Therefore, one obtains

$$V(t) \leq e^{N_f(0,t)[In(\lambda_1\lambda_2)+(\mu_1+\mu_2)h]} \times e^{\mu_2|\hat{F}_a(0,t)|} e^{-\mu_1|\hat{F}_c(0,t)|} V_1(0). \quad (22)$$

Note that

$$\hat{F}_a(0, t) = F_a(0, t), \quad (23)$$

$$\hat{F}_c(0, t) = t - \hat{F}_a(0, t). \quad (24)$$

Substituting (23) and (24) into (22) yields

$$V(t) \leq e^{N_f(0,t)[In(\lambda_1\lambda_2)+(\mu_1+\mu_2)h]} \times e^{\mu_2|\hat{F}_a(0,t)|} e^{-\mu_1|t-\hat{F}_a(0,t)|} V_1(0). \quad (25)$$

Based on (16) and (17), (25) can be written as

$$V(t) \leq e^{o_1} e^{-o_2 t} V_1(0), \quad (26)$$

where $o_1 = (\mu_1 + \mu_2)T_0$, and $o_2 = \mu_1 - \mu_1^* - \frac{\mu_1 + \mu_2}{\tau_a} - T_D$.

Define $c_1 = \min\{\lambda_{\min}(P_1), \lambda_{\min}(P_2)\}$, $c_2 = \max\{\lambda_{\max}(P_1), \lambda_{\max}(P_2)\}$, $c_3 = c_2 + h\lambda_{\max}(R_1) + \frac{h^2}{2}\lambda_{\max}(Z_2)$. Further, we can get

$$V(t) \geq c_1 \|x(t)\|^2, V(0) \leq c_3 \|\phi(0)\|^2. \quad (27)$$

Combining (26) and (27), we can obtain

$$\|x(t)\| \leq \sqrt{\frac{c_3}{c_1}} e^{o_1} e^{-\frac{o_2}{2}t} \|\phi(0)\|, \quad (28)$$

which implies that the system (8) is exponentially stable under DoS jamming attacks. This proof is completed.

In Theorem 1, we assume that the controller gain K is known. In Theorem 2, the unknown controller gain K of MASs can be derived on the basis of the foregoing research.

Theorem 2. For given scalars $h > 0$, $\mu_1 > 0$, $\mu_2 > 0$, $\lambda_1 > 0$, $\lambda_2 > 0$, a_{sr} , $s = 1, 2, 3$, $r = 1, 2$, system (8) is exponential stable, if there exist matrices $\bar{R}_f > 0$, $\bar{Z}_f > 0$, $f = 1, 2$ and $\bar{\Omega} > 0$, \bar{U}_f with appropriate dimensions and the following conditions hold:

$$\bar{\omega}_f < 0, \quad f = 1, 2, \quad (29)$$

$$0 < \begin{bmatrix} \bar{Z}_f & * \\ \bar{U}_f & \bar{Z}_f \end{bmatrix}, \quad (30)$$

$$\begin{bmatrix} -\lambda_2(I_N \otimes X_2) & * \\ I_N \otimes X_2 & -I_N \otimes X_1 \end{bmatrix} < 0 \quad (31)$$

$$\begin{bmatrix} -e^{(\mu_1+\mu_2)h}\lambda_1(I_N \otimes X_1) & * \\ I_N \otimes X_1 & -I_N \otimes X_2 \end{bmatrix} < 0 \quad (32)$$

$$\begin{bmatrix} -\lambda_f \bar{R}_f & * \\ I_N \otimes X_f - 2a_{3(3-f)}(I_N \otimes X_{3-f}) + a_{3(3-f)}^2 \bar{R}_{3-f} \end{bmatrix} < 0 \quad (33)$$

$$\begin{bmatrix} -\lambda_f \bar{Z}_f & * \\ I_N \otimes X_f - 2a_{1(3-f)}(I_N \otimes X_{3-f}) + a_{1(3-f)}^2 \bar{Z}_{3-f} \end{bmatrix} < 0 \quad (34)$$

where the element of $\bar{\omega}_f$ is given in Appendix C.

Moreover, the consensus protocol and ETC parameters can be calculated as follows:

$$K = YX_1^{-1}, \Omega = (I_N \otimes X)^{-1}\bar{\Omega}(I_N \otimes X)^{-1}$$

Proof For any positive scalars a_{sr} , due to $(S - a_{sr}^{-1}T)S^{-1}(S - a_{sr}^{-1}T) \geq 0$, we can obtain that

$$-TS^{-1}T \leq -2a_{sr}T + a_{sr}^2S$$

Let $X_1 = P_1^{-1}$, $\bar{X}_1 = I_N \otimes X_1$, one has

$$\begin{aligned} Z_1^{-1} &\leq a_{11}^2 \bar{Z}_1 - 2a_{11} \bar{X}_1, \\ -\bar{X}_1 I \bar{X}_1 &\leq a_{21}^2 I - 2a_{21} \bar{X}_1, \\ R_1^{-1} &\leq a_{31}^2 \bar{R}_1 - 2a_{31} \bar{X}_1. \end{aligned} \quad (35)$$

When $f = 1$, define $\Delta_1 = \text{diag}\{I_5 \otimes \bar{X}_1, I, \bar{X}_1\}$, $\Delta_2 = \text{diag}\{I_2 \otimes \bar{X}_1\}$, then pre-multiply and post-multiply both side of $\omega_1 < 0$ by Δ_1 and both side of (12) by Δ_2 . Define new variables $\bar{Z}_1 = \bar{X}_1 Z_1 \bar{X}_1$, $\bar{R}_1 = \bar{X}_1 R_1 \bar{X}_1$, $\bar{U}_1 = \bar{X}_1 U_1 \bar{X}_1$, $Y = KX_1$. According to schur complement lemma, $\bar{\omega}_1 < 0$ is equivalent to $\omega_1 < 0$ and (30) is equivalent to (12). Thus, we can derive that (29) and (30) can guarantee (11) and (12) hold.

Furthermore, let $X_2 = P_2^{-1}$, $\bar{X}_2 = I_N \otimes X_2$, one has

$$\begin{aligned} Z_2^{-1} &\leq a_{12}^2 \bar{Z}_2 - 2a_{12} \bar{X}_2, \\ -\bar{X}_2 I \bar{X}_2 &\leq a_{22}^2 I - 2a_{22} \bar{X}_2, \\ -R_2^{-1} &\leq a_{32}^2 \bar{R}_2 - 2a_{32} \bar{X}_2. \end{aligned} \quad (36)$$

When $f = 2$, denote $\Delta_3 = \text{diag}\{I_4 \otimes \bar{X}_2, I, \bar{X}_2\}$, $\Delta_4 = \text{diag}\{I_2 \otimes \bar{X}_2\}$, then pre-multiply and post-multiply both side of $\omega_2 < 0$ by Δ_3 and both side of (12) by Δ_4 . Define new variables $\bar{Z}_2 = \bar{X}_2 Z_2 \bar{X}_2$, $\bar{R}_2 = \bar{X}_2 R_2 \bar{X}_2$, $\bar{U}_2 = \bar{X}_2 U_2 \bar{X}_2$. Similarly, employing the schur complement lemma, $\bar{\omega}_2 < 0$ is equivalent to $\omega_2 < 0$ and (30) is equivalent to (12). Thus, we can derive that (29) and (30) can guarantee (11) and (12) hold. In addition, pre-multiply and post-multiply the first inequality in (13) and the second inequality in (13) by \bar{X}_2 and \bar{X}_1 , respectively, and applying the Schur complement lemma, (31) is equivalent to the first inequality in (13) and (32) is

equivalent to the second inequality in (13), respectively. By using similar derivations, we can derive that the LMIs (33) and (34) ensure the (14) and (15) hold, respectively. According to the results of Theorem 1 and the above analysis, the system (8) can achieve exponential stable. Due to $Y = KX_1$, the consensus controller gain can be computed as $K = YX_1^{-1}$.

This completes the proof.

4 Numerical example

In this section, we will provide a numerical simulation to illustrate the feasibility of the obtained results. Similar to [38], consider a nonlinear MAS described by

$$(8) \text{ with } A = \begin{bmatrix} -1.175 & 0.9871 \\ -0.8458 & -0.8776 \end{bmatrix}, \quad B = \begin{bmatrix} -0.194 \\ -10.29 \end{bmatrix},$$

$$C = \begin{bmatrix} 0.1 & 0.2 \\ 0 & 0.1 \end{bmatrix} \text{ and}$$

$$f(x_i(t)) = \begin{bmatrix} \tanh(0.4x_{i1}(t)) \\ \sin(0.3x_{i2}(t)) \end{bmatrix}.$$

According to the topology graph shown in Fig. 3, the L can be obtained as follows:

$$L = \begin{bmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ -1 & 2 & 0 & 0 & -1 & 0 \\ -1 & 0 & 2 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 0 & 0 & 1 \end{bmatrix}$$

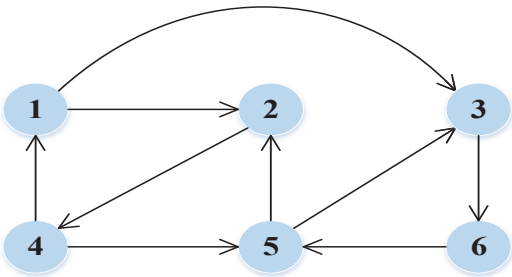


Fig. 3: Topology graph.

The other designed parameters are set as $\mu_1 = 0.4689$, $\mu_2 = 1.5311$, $\sigma = 0.1$, $\alpha = 1.5$, $\lambda_1 = 1.05$, $\lambda_2 = 1.05$, $h = 0.01$, $a_{11} = 1$, $a_{12} = 1$, $a_{21} = 1$, $a_{31} = 1$, $a_{32} = 1$. By solving the LMIs in MATLAB, the distributed event-triggering matrices are obtained as $\Omega_1 = \Omega_2 = \Omega_3 = \Omega_4 = \Omega_5 = \Omega_6 = \begin{bmatrix} 0.0432 & -0.0016 \\ -0.0016 & 0.0439 \end{bmatrix}$. Then, by applying Theorem 2, we can get the controller gain $K = \begin{bmatrix} 0.0007 \\ 0.0093 \end{bmatrix}^T$.

The initial conditions of the agents are described as follows $x_1(0) = [0.1 \ 1]^T$, $x_2(0) = [0.7 \ 0.3]^T$, $x_3(0) = [0.4 \ -0.2]^T$, $x_4(0) = [-0.6 \ 0.8]^T$, $x_5(0) = [0.5 \ -0.1]^T$, $x_6(0) = [0.9 \ -1]^T$.

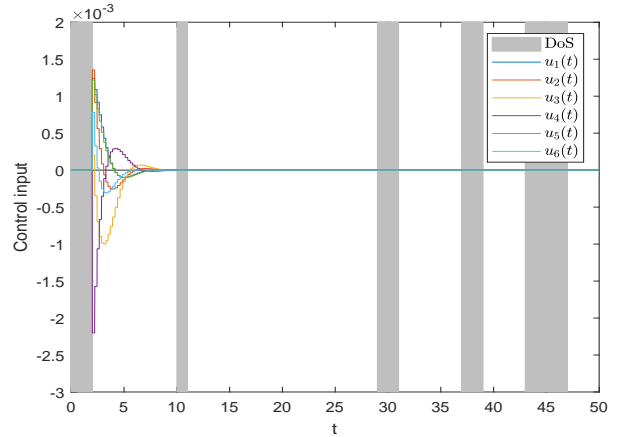


Fig. 4: Control input under DoS jamming attacks.

In this example, suppose that the DoS jamming attacks occur in $[0, 2)$, $[10, 11)$, $[29, 31)$, $[37, 39)$ and $[43, 47)$, respectively. According to Theorem 1, when choose $\mu_1^* = 0.0311$ and $T_D = 0.1$, the attack frequency and attack duration of DoS jamming attacks can be obtained as

$$F_f(0, t) \leq \frac{0.0311 + 0.1}{0.7419 + 2 * 0.01} = 0.172,$$

$$\tau_a \geq \frac{0.4689 + 1.5311}{0.4689 - 0.0311 - 0.1} = 5.921.$$

Fig. 4 denotes the control input under DoS jamming attacks. It can be seen that the control inputs are piecewise continuous during sleeping intervals of DoS jamming attacks, while the control inputs become zero during the active intervals of DoS jamming attacks. Besides, the triggering instants under DoS jamming attacks are depicted in Fig. 5. Based on the proposed ETC protocol, the states responses of all agents under DoS jamming attacks are described in Fig. 6, which shows that MASs can achieve consensus under the DoS jamming attacks.

5 Conclusion

In this paper, the event-triggered consensus problem of MASs under DoS jamming attacks has been investigated. The communication topologies may change due to DoS jamming attacks. To mitigate the cost of

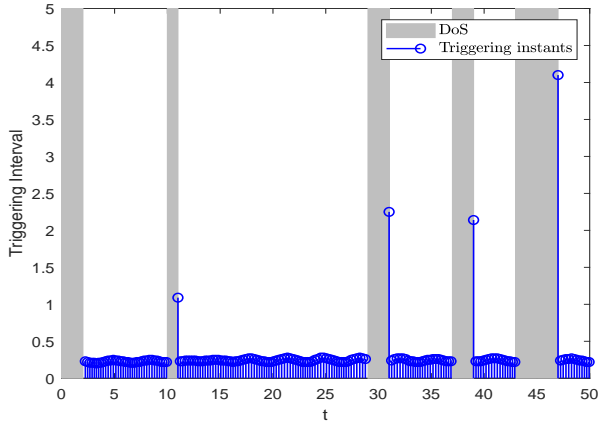


Fig. 5: Triggering instants under DoS jamming attacks.

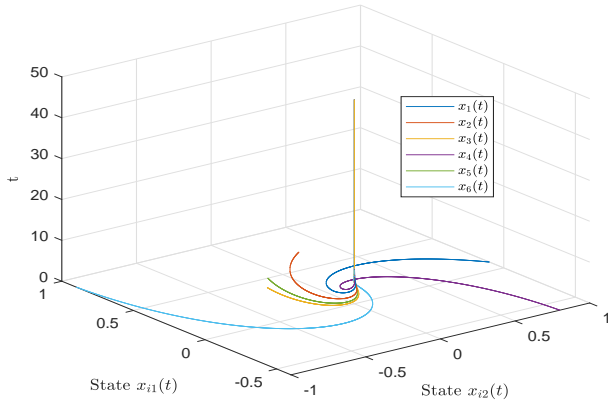


Fig. 6: State responses of agent $x_i(t)$.

communication networks, a novel ETC protocol is proposed to guarantee that consensus performance of the MASs can be realized under the DoS jamming attacks. The attack frequency and attack duration of DoS jamming signals are discussed. Then, by using piecewise Lyapunov functional, sufficient conditions are derived to guarantee that consensus problem of MASs can be solved. In addition, controller gains have been obtained in terms of linear matrix inequalities. Finally, a numerical example is given to verify the effectiveness of the proposed method. Future work will be directed to heterogeneous MASs with multiple cyber-attacks by ETC scheme.

Appendix A

Elements of ω_f in Lemma 2.

$$\omega_1 = \begin{bmatrix} \Pi_1 & * & * \\ hM_1 - Z_1^{-1} & * & * \\ M_3 & 0 & -I \end{bmatrix} \quad (37)$$

$$\omega_2 = \begin{bmatrix} \Pi_2 & * & * \\ hM_2 - Z_2^{-1} & * & * \\ M_4 & 0 & -I \end{bmatrix} \quad (38)$$

$$\Pi_1 = \begin{bmatrix} \Gamma_{11}^1 & * & * & * & * \\ \Gamma_{21}^1 & \Gamma_{22}^1 & * & * & * \\ \Gamma_{31}^1 & \Gamma_{32}^1 & \Gamma_{33}^1 & * & * \\ \Gamma_{41}^1 & 0 & 0 & -I & * \\ \Gamma_{51}^1 & 0 & 0 & 0 & -\Omega \end{bmatrix}$$

$$\Pi_2 = \begin{bmatrix} \Gamma_{11}^2 & * & * & * \\ \Gamma_{21}^2 & \Gamma_{22}^2 & * & * \\ \Gamma_{31}^2 & \Gamma_{32}^2 & \Gamma_{33}^2 & * \\ \Gamma_{41}^2 & 0 & 0 & -I \end{bmatrix}$$

$$\Gamma_{11}^1 = \mu_1(I_N \otimes P_1) + R_1 + (I_N \otimes P_1 A) + (I_N \otimes A^T P_1) - e^{-\mu_1 h} Z_1$$

$$\Gamma_{21}^1 = -\left(\alpha(L^{\sigma(t)} \otimes P_1 B K)^T + e^{-\mu_1 h}(Z_1 - U_1^T)\right)$$

$$\Gamma_{22}^1 = \sigma \Omega + e^{-\mu_1 h}(-2Z_1 + U_1 + U_1^T)$$

$$\Gamma_{31}^1 = e^{-\mu_1 h} U_1^T$$

$$\Gamma_{32}^1 = e^{-\mu_1 h}(Z_1 - U_1^T)$$

$$\Gamma_{33}^1 = -e^{-\mu_1 h}(R_1 + Z_1)$$

$$\Gamma_{41}^1 = (I_N \otimes P_1 C)^T$$

$$\Gamma_{51}^1 = -\left(\alpha(L^{\sigma(t)} \otimes P_1 B K)\right)^T$$

$$M_1 = [I_N \otimes A, -\alpha(L^{\sigma(t)} \otimes B K), 0, I_N \otimes C, -\alpha(L^{\sigma(t)} \otimes B K)]$$

$$M_3 = [I_N \otimes H, 0, 0, 0, 0]$$

$$\Gamma_{11}^2 = -\mu_2(I_N \otimes P_2) + R_2 + (I_N \otimes P_2 A) + (I_N \otimes A^T P_2) - e^{\mu_2 h} Z_2$$

$$\Gamma_{21}^2 = e^{\mu_2 h}(Z_2 - U_2^T)$$

$$\Gamma_{22}^2 = e^{\mu_2 h}(-2Z_2 + U_2 + U_2^T)$$

$$\Gamma_{31}^2 = e^{\mu_2 h}(U_2^T)$$

$$\Gamma_{32}^2 = e^{\mu_2 h}(Z_2 - U_2^T)$$

$$\Gamma_{33}^2 = -e^{\mu_2 h}(R_2 + Z_2)$$

$$\Gamma_{41}^2 = (I_N \otimes P_2 C)^T$$

$$M_2 = [I_N \otimes A, 0, 0, I_N \otimes C]$$

$$M_4 = [I_N \otimes H, 0, 0, 0]$$

Appendix B

The proof of Lemma 2.

The following cases with $f = 1$ and $f = 2$ will be given, respectively.

When $f = 1$, for $t \in [\Xi_{L,k} \cap \Theta_{k,n} \cap L_{2,n}]$, taking the derivative of $V_1(t)$, one has

$$\dot{V}_{11}(t) = 2x^T(t)(I_N \otimes P_1)\dot{x}(t), \quad (39)$$

$$\begin{aligned} \dot{V}_{12}(t) = & -\mu_1 \int_{t-h}^t e^{-\mu_1(t-\theta)} x^T(\theta) R_1 x(\theta) d\theta \\ & + x^T(t) R_1 x(t) - e^{-\mu_1 h} x^T(t-h) R_1 x(t-h), \end{aligned} \quad (40)$$

$$\begin{aligned} \dot{V}_{13}(t) = & -\mu_1 h \int_{t-h}^t \int_{\theta}^t \dot{x}^T(\varphi) Z_1 e^{-\mu_1(t-\varphi)} \dot{x}(\varphi) d\varphi d\theta \\ & - h \int_{t-h}^t \dot{x}^T(\theta) Z_1 e^{-\mu_1(t-\theta)} \dot{x}(\theta) d\theta \\ & + h^2 \dot{x}^T(t) Z_1 \dot{x}(t). \end{aligned} \quad (41)$$

Then, according to (39)-(41), we can get

$$\begin{aligned} \dot{V}_1(t) \leq & -\mu_1 V_1(t) + \mu_1 x^T(t)(I_N \otimes P_1)x(t) \\ & + x^T(t) R_1 x(t) - x^T(t-h) R_1 e^{-\mu_1 h} x(t-h) \\ & + h^2 \dot{x}^T(t) Z_1 \dot{x}(t) - h \int_{t-h}^t \dot{x}^T(\theta) Z_1 e^{-\mu_1 h} \dot{x}(\theta) d\theta \\ & + 2x^T(t)(I_N \otimes P_1)\dot{x}(t). \end{aligned} \quad (42)$$

By using Lemma 1, for Z_1 and U_1 satisfying (12), we can obtain that

$$-h \int_{t-h}^t \dot{x}^T(\theta) Z_1 \dot{x}(\theta) d\theta \leq \zeta_1^T(t) \Upsilon_1 \zeta_1(t), \quad (43)$$

where $\zeta_1(t) = [x^T(t) \ x^T(t - \tau_{L,k}(t)) \ x^T(t-h)]^T$ and

$$\Upsilon_1 = \begin{bmatrix} -Z_1 & * & * \\ Z_1 - U_1^T & -2Z_1 + U_1 + U_1^T & * \\ U_1^T & Z_1 - U_1^T & -Z_1 \end{bmatrix}.$$

From Assumption 1, one can get

$$x^T(t)(I_N \otimes H)^T(I_N \otimes H)x(t) - F^T(x(t))F(x(t)) \geq 0. \quad (44)$$

Moreover, according to the triggering algorithm (4), one has

$$\sigma x^T(t - \tau_{L,k}(t)) \Omega x(t - \tau_{L,k}(t)) - \psi_{k,n}^T(t) \Omega \psi_{k,n}(t) \geq 0, \quad (45)$$

where $\Omega = \text{diag}\{\Omega_1, \Omega_2, \dots, \Omega_N\}$.

Combining (42)-(45), we obtain

$$\begin{aligned} \dot{V}_1(t) \\ \leq -\mu_1 V_1(t) + \xi_1^T(t) [\Pi_1 + h^2 M_1^T Z_1 M_1 + M_3^T I M_3] \xi_1(t), \end{aligned} \quad (46)$$

where $\xi_1(t) = [x^T(t), x^T(t - \tau_{L,k}(t)), x^T(t-h), F^T(x(t)), \psi_{k,n}^T(t)]^T$.

Due to $\omega_1 < 0$, which implies, for all $t \in [l_{n-1} + \Delta_{n-1}, l_n]$

$$V_1(t) \leq e^{-\mu_1(t-(l_{n-1}+\Delta_{n-1}))} V_1(l_{n-1} + \Delta_{n-1}). \quad (47)$$

When $f = 2$, $t \in L_{1,n}$. Similarly, we can get

$$\begin{aligned} \dot{V}_2(t) \leq & \mu_2 V_2(t) - \mu_2 x^T(t)(I_N \otimes P_2)x(t) \\ & + 2x^T(t)(I_N \otimes P_2)\dot{x}(t) \\ & + x^T(t) R_2 x(t) - x^T(t-h) R_2 e^{\mu_2 h} x(t-h) \\ & + h^2 \dot{x}^T(t) Z_2 \dot{x}(t) - h \int_{t-h}^t \dot{x}^T(\theta) Z_2 e^{\mu_2 h} \dot{x}(\theta) d\theta. \end{aligned} \quad (48)$$

Similarly, it can be achieved that

$$-h \int_{t-h}^t \dot{x}^T(\theta) Z_2 \dot{x}(\theta) d\theta \leq \zeta_1^T(t) \Upsilon_2 \zeta_1(t), \quad (49)$$

$$\text{where } \Upsilon_2 = \begin{bmatrix} -Z_2 & * & * \\ Z_2 - U_2^T & -2Z_2 + U_2 + U_2^T & * \\ U_2^T & Z_2 - U_2^T & -Z_2 \end{bmatrix}.$$

Combining (44), (48) and (49), we obtain

$$\begin{aligned} \dot{V}_2(t) \leq & \mu_2 V_2(t) \\ & + \xi_2^T(t) [\Pi_2 + h^2 M_2^T Z_2 M_2 + M_4^T I M_4] \xi_2(t), \end{aligned} \quad (50)$$

where $\xi_2(t) = [x^T(t), x^T(t - \tau_{L,k}(t)), x^T(t-h), F^T(x(t))]^T$.

According to (38), and by applying Schur complement, one has

$$V_2(t) \leq e^{\mu_2(t-l_n)} V_2(l_n), \quad t \in [l_n, l_n + \Delta_n]. \quad (51)$$

This proof is completed.

Appendix C

Element of $\bar{\omega}_f$ in Theorem 2.

$$\bar{\omega}_1 = \begin{bmatrix} \bar{\Pi}_1 & * & * \\ h\bar{M}_1 & a_{11}^2 \bar{Z}_1 - 2a_{11} \bar{X}_1 & * \\ \bar{M}_3 & 0 & a_{21}^2 I - 2a_{21} \bar{X}_1 \end{bmatrix} \quad (52)$$

$$\bar{\omega}_2 = \begin{bmatrix} \bar{\Pi}_2 & * & * \\ h\bar{M}_2 & a_{12}^2 \bar{Z}_2 - 2a_{12} \bar{X}_2 & * \\ \bar{M}_4 & 0 & a_{22}^2 I - 2a_{22} \bar{X}_2 \end{bmatrix} \quad (53)$$

$$\bar{\Pi}_1 = \begin{bmatrix} \bar{\Gamma}_{11}^1 & * & * & * & * \\ \bar{\Gamma}_{21}^1 & \bar{\Gamma}_{22}^1 & * & * & * \\ \bar{\Gamma}_{31}^1 & \bar{\Gamma}_{32}^1 & \bar{\Gamma}_{33}^1 & * & * \\ \bar{\Gamma}_{41}^1 & 0 & 0 & a_{21}^2 I - 2a_{21} \bar{X}_1 & * \\ \bar{\Gamma}_{51}^1 & 0 & 0 & 0 & -\bar{\Omega} \end{bmatrix}$$

$$\bar{\Pi}_2 = \begin{bmatrix} \bar{\Gamma}_{11}^2 & * & * & * \\ \bar{\Gamma}_{21}^2 & \bar{\Gamma}_{22}^2 & * & * \\ \bar{\Gamma}_{31}^2 & \bar{\Gamma}_{32}^2 & \bar{\Gamma}_{33}^2 & * \\ \bar{\Gamma}_{41}^2 & 0 & 0 & a_{22}^2 I - 2a_{22} \bar{X}_2 \end{bmatrix}$$

$$\bar{\Gamma}_{11}^1 = \mu_1(I_N \otimes X_1) + \bar{R}_1 + (I_N \otimes AX_1) + (I_N \otimes X_1 A^T) - e^{-\mu_1 h} \bar{Z}_1$$

$$\bar{\Gamma}_{21}^1 = -\left(\alpha(L^{\sigma(t)} \otimes BY)^T + e^{-\mu_1 h}(\bar{Z}_1 - \bar{U}_1^T)\right)$$

$$\bar{\Gamma}_{22}^1 = \sigma \bar{\Omega} + e^{-\mu_1 h}(-2\bar{Z}_1 + \bar{U}_1 + \bar{U}_1^T)$$

$$\bar{\Gamma}_{31}^1 = e^{-\mu_1 h} \bar{U}_1^T$$

$$\bar{\Gamma}_{32}^1 = e^{-\mu_1 h}(\bar{Z}_1 - \bar{U}_1^T)$$

$$\bar{\Gamma}_{33}^1 = -e^{-\mu_1 h}(\bar{R}_1 + \bar{Z}_1)$$

$$\bar{\Gamma}_{41}^1 = (I_N \otimes CX_1)^T$$

$$\bar{\Gamma}_{51}^1 = -\left(\alpha(L^{\sigma(t)} \otimes BY)\right)^T$$

$$\bar{M}_1 = [I_N \otimes AX_1, -\alpha(L^{\sigma(t)} \otimes BY), 0, I_N \otimes CX_1, -\alpha(L^{\sigma(t)} \otimes BY)]$$

$$\bar{M}_3 = [I_N \otimes HX_1, 0, 0, 0, 0]$$

$$\bar{\Gamma}_{11}^2 = -\mu_2(I_N \otimes X_2) + \bar{R}_2 + (I_N \otimes AX_2) + (I_N \otimes X_2 A^T) - e^{\mu_2 h} \bar{Z}_2$$

$$\bar{\Gamma}_{21}^2 = e^{\mu_2 h}(\bar{Z}_2 - \bar{U}_2^T)$$

$$\bar{\Gamma}_{22}^2 = e^{\mu_2 h}(-2\bar{Z}_2 + \bar{U}_2 + \bar{U}_2^T)$$

$$\bar{\Gamma}_{31}^2 = e^{\mu_2 h} \bar{U}_2^T$$

$$\bar{\Gamma}_{32}^2 = e^{\mu_2 h}(\bar{Z}_2 - \bar{U}_2^T)$$

$$\bar{\Gamma}_{33}^2 = -e^{\mu_2 h}(\bar{R}_2 + \bar{Z}_2)$$

$$\bar{\Gamma}_{41}^2 = (I_N \otimes CX_2)^T$$

$$\bar{M}_2 = [I_N \otimes AX_2, 0, 0, I_N \otimes CX_2]$$

$$\bar{M}_4 = [I_N \otimes HX_2, 0, 0, 0]$$

Compliance with ethical standards

Conflict of interest

The authors declare that they have no conflict of interest.

Data Availability Statement

All data generated or analyzed during this study are included in this article.

References

1. Beard, R.W., Lawton, J., Hadaegh, F.Y.: A coordination architecture for spacecraft formation control. *IEEE Transactions on Control Systems Technology* **9**(6), 777–790 (2001)
2. Cai, Y., Tang, Z., Ding, Y., Qian, B.: Theory and application of multi-robot service-oriented architecture. *IEEE/CAA Journal of Automatica Sinica* **3**(1), 15–25 (2016)
3. Lawton, J.R., Beard, R.W.: Synchronized multiple spacecraft rotations. *Automatica* **38**(8), 1359–1364 (2001)
4. Fax, J., Murray, R.: Information flow and cooperative control of vehicle formations. *IEEE Transactions on Automatic Control* **49**(9), 1465–1476 (2004)
5. Park, J.H., Shen, H., Chang, X.H., Lee, T.H.: Recent advances in control and filtering of dynamic systems with constrained signals. Springer (2019)
6. Sun, D., Liao, Q., Gu, X., Li, C., Ren, H.: Multilateral teleoperation with new cooperative structure based on reconfigurable robots and type-2 fuzzy logic. *IEEE Transactions on Cybernetics* **49**(8), 2845–2859 (2019)
7. Dong, T., Gong, Y.: Leader-following secure consensus for second-order multi-agent systems with nonlinear dynamics and event-triggered control strategy under dos attack. *Neurocomputing* **416**, 95–102 (2020)
8. Yang, Y., Li, Y., Yue, D., Tian, Y.C., Ding, X.: Distributed secure consensus control with event-triggering for multi-agent systems under dos attacks. *IEEE Transactions on Cybernetics* **51**(6), 2916–2928 (2021)
9. Olfati-Saber, R., Fax, J.A., Murray, R.M.: Consensus and cooperation in networked multi-agent systems. *Proceedings of the IEEE* **95**(1), 215–233 (2007)
10. Ren, W., Beard, R.: Consensus seeking in multiagent systems under dynamically changing interaction topologies. *IEEE Transactions on Automatic Control* **50**(5), 655–661 (2005)
11. Zheng, Y., Ma, J., Wang, L.: Consensus of hybrid multi-agent systems. *IEEE Transactions on Neural Networks and Learning Systems* **29**(4), 1359–1365 (2018)
12. Tian, Y.P., Liu, C.L.: Consensus of multi-agent systems with diverse input and communication delays. *IEEE Transactions on Automatic Control* **53**(9), 2122–2128 (2008)
13. Hayakawat, T., Matsuzawat, T., Harat, S.: Formation control of multi-agent systems with sampled information relationship between information exchange structure and control performance. In: *Proceedings of the 45th IEEE Conference on Decision and Control*, pp. 4333–4338 (2006)
14. Zhang, H., Feng, G., Yan, H., Chen, Q.: Observer-based output feedback event-triggered control for consensus of multi-agent systems. *IEEE Transactions on Industrial Electronics* **61**(9), 4885–4894 (2013)
15. Xu, W., Ho, D.W., Li, L., Cao, J.: Event-triggered schemes on leader-following consensus of general linear multiagent systems under different topologies. *IEEE Transactions on Cybernetics* **47**(1), 212–223 (2015)
16. Wang, S., Zhang, P., Fan, Y.: Centralized event-triggered control of multi-agent systems with dynamic triggering mechanisms. In: *The 27th Chinese Control and Decision Conference (2015 CCDC)*, pp. 2183–2187 (2015)
17. Fan, Y., Feng, G., Wang, Y., Song, C.: Distributed event-triggered control of multi-agent systems with combinatorial measurements. *Automatica* **49**(2), 671–675 (2013)
18. Zou, Y., Su, X., Li, S., Niu, Y., Li, D.: Event-triggered distributed predictive control for asynchronous coordination of multi-agent systems. *Automatica* **99**, 92–98 (2019)
19. Yang, R., Zhang, H., Feng, G., Yan, H., Wang, Z.: Robust cooperative output regulation of multi-agent systems via adaptive event-triggered control. *Automatica* **102**, 129–136 (2019)
20. Dimarogonas, D.V., Frazzoli, E.: Distributed event-triggered control strategies for multi-agent systems. In: *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 906–910 (2009)

21. Ye, D., Yang, X.: Distributed event-triggered consensus for nonlinear multi-agent systems subject to cyber attacks. *Information Sciences* **473**, 178–189 (2019)
22. Xu, Y., Fang, M., Shi, P., Wu, Z.G.: Event-based secure consensus of multiagent systems against dos attacks. *IEEE Transactions on Cybernetics* **50**(8), 3468–3476 (2020)
23. Choi, I.S., Hong, J., Kim, T.W.: Multi-agent based cyber attack detection and mitigation for distribution automation system. *IEEE Access* **8**, 183,495–183,504 (2020)
24. Mousavinejad, E., Yang, F., Han, Q.L., Vlacic, L.: A novel cyber attack detection method in networked control systems. *IEEE Transactions on Cybernetics* **48**(11), 3254–3264 (2018)
25. Meng, M., Xiao, G., Li, B.: Adaptive consensus for heterogeneous multi-agent systems under sensor and actuator attacks. *Automatica* **122**, 109,242 (2020)
26. Mustafa, A., Modares, H.: Attack analysis and resilient control design for discrete-time distributed multi-agent systems. *IEEE Robotics and Automation Letters* **5**(2), 369–376 (2019)
27. He, W., Gao, X., Zhong, W., Qian, F.: Secure impulsive synchronization control of multi-agent systems under deception attacks. *Information Sciences* **459**, 354–368 (2018)
28. Zhao, L., Yang, G.H.: Cooperative adaptive fault-tolerant control for multi-agent systems with deception attacks. *Journal of the Franklin Institute* **357**(6), 3419–3433 (2020)
29. Gu, Z., Zhou, X., Zhang, T., Yang, F., Shen, M.: Event-triggered filter design for nonlinear cyber-physical systems subject to deception attacks. *ISA Transactions* **104**, 130–137 (2020)
30. Ye, D., Zhang, T.Y., Guo, G.: Stochastic coding detection scheme in cyber-physical systems against replay attack. *Information Sciences* **481**, 432–444 (2019)
31. Zhu, M., Martinez, S.: On the performance analysis of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control* **59**(3), 804–808 (2013)
32. Chen, B., Ho, D.W., Hu, G., Yu, L.: Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. *IEEE Transactions on Cybernetics* **48**(6), 1862–1876 (2017)
33. Zhang, D., Feng, G.: A new switched system approach to leader-follower consensus of heterogeneous linear multiagent systems with dos attack. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (2019)
34. Wang, J.S., Yang, G.H.: Data-driven methods for stealthy attacks on tcp/ip-based networked control systems equipped with attack detectors. *IEEE Transactions on Cybernetics* **49**(8), 3020–3031 (2018)
35. Yang, H., Ye, D.: Observer-based fixed-time secure tracking consensus for networked high-order multiagent systems against dos attacks. *IEEE Transactions on Cybernetics* (2020)
36. Chang, B., Mu, X., Yang, Z., Fang, J.: Event-based secure consensus of multi-agent systems under asynchronous dos attacks. *Applied Mathematics and Computation* **401**, 126,120 (2021)
37. Tang, Y., Zhang, D., Shi, P., Zhang, W., Qian, F.: Event-based formation control for nonlinear multiagent systems under dos attacks. *IEEE Transactions on Automatic Control* **66**(1), 452–459 (2021)
38. Zha, L., Liu, J., Cao, J.: Resilient event-triggered consensus control for nonlinear multi-agent systems with dos attacks. *Journal of the Franklin Institute* **356**(13), 7071–7090 (2019)
39. Hu, S., Yue, D., Han, Q.L., Xie, X., Chen, X., Dou, C.: Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. *IEEE Transactions on Cybernetics* **50**(5), 1952–1964 (2020)
40. Liu, J., Yin, T., Yue, D., Karimi, H.R., Cao, J.: Event-based secure leader-following consensus control for multi-agent systems with multiple cyber attacks. *IEEE Transactions on Cybernetics* **51**(1), 162–173 (2020)
41. Xu, Y., Fang, M., Wu, Z.G., Pan, Y.J., Chadli, M., Huang, T.: Input-based event-triggering consensus of multiagent systems under denial-of-service attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **50**(4), 1455–1464 (2018)
42. Feng, Z., Wen, G., Hu, G.: Distributed secure coordinated control for multiagent systems under strategic attacks. *IEEE Transactions on Cybernetics* **47**(5), 1273–1284 (2016)
43. Cheng, Z., Yue, D., Hu, S., Ge, H., Chen, L.: Distributed event-triggered consensus of multi-agent systems under periodic dos jamming attacks. *Neurocomputing* **400**, 458–466 (2020)
44. Peng, C., Ma, S., Xie, X.: Observer-based non-pdc control for networked t-s fuzzy systems with an event-triggered communication. *IEEE transactions on Cybernetics* **47**(8), 2279–2287 (2017)