Applied Mathematics and Computation 401 (2021) 126120

Contents lists available at ScienceDirect

Applied Mathematics and Computation

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

Event-based secure consensus of muti-agent systems under asynchronous DoS attacks

Beibei Chang[a], Xiaowu Mu[a], Zhe Yang[a,*], Jianyin Fang[b]

[a] School of Mathematics and Statistics, Zhengzhou University, Henan 450001, China
[b] Zhongyuan University of Technology, Henan 450007, China

ARTICLE INFO

Article history:
Received 2 September 2020
Revised 20 January 2021
Accepted 16 February 2021
Available online 26 February 2021

Keywords:
Multi-agent systems
Event-triggered resilient control
Asynchronous denial-of-service attacks
Directed topology

ABSTRACT

This paper studies the problem of event-based secure consensus for multi-agent systems subject to asynchronous denial of service attacks. The case that the communication network of multi-agent systems only contains a directed spanning tree is considered. Subsequently, we conduct a precise analysis of frequency and duration of denial of service attacks. Then, we regard the multi-agent system suffering from the invalid denial of service attack as a multi-agent system with switching topology, and adopt the control method of dealing with the switching topology to reduce the impact of invalid denial of service attacks on the multi-agent system. In addition, we propose a event-triggered resilient control mechanism, which enables multi-agent systems to reach consensus at an exponentially convergent speed, and prevents multi-agent systems from Zeno behavior, thereby avoiding continuous communication between agents. A simulation example is given to verify the correctness of the theoretical analysis.

1. Introduction

In the past few decades, the consensus problem of networked multi-agent systems (MASs) has a wide range of application scenarios, such as cooperative flight of aircraft [1], search and rescue of multi robots [2] and so on. Networked MASs are known for its low maintenance costs and high flexibility[3]. Although there are many advantages of using network MASs, MASs are more vulnerable to cyber attacks, which may cause system instability or malfunction [4]. In MASs, there are two different attack scenarios for cyber attacks, namely attack dynamic behavior and attack communication network [5]. In reality, the research on attacking communication network is more extensive. The methods of attacking communication network can be divided into deception attacks and denial-of-service (DoS) attacks [6]. Deception attacks destroy the integrity of information through illegal intrusion into information systems and malicious tampering of data [7]. DoS attacks prevent information exchange by attacking the communication networks or terminal nodes [8]. In practice, it is more common to study the latter. It should be pointed out that MASs with complex communication topology face more risks from DoS attacks [9]. Therefore, how to control the input of MASs under DoS attacks and make MASs reach consensus has become a key issue in the operation of MASs. This problem has aroused the research interest of many researchers. For example, in [10], DoS attack frequency and attack time ratio are introduced to characterize the features of DoS attacks and two types

* Corresponding author.
E-mail address: yangzhe@zzu.edu.cn (Z. Yang).

https://doi.org/10.1016/j.amc.2021.126120
0096-3003/

of novel distributed nonlinear fixed-time observers are, respectively, developed to counter connectivity-maintained/broken attacks in [11].

In addition, since the implementation of traditional communication strategies requires a continuous communication process [12], with the expansion of the system scale and the increase in system complexity, the use of traditional communication strategies inevitably leads to a large amount of information transmission. However, in many practical networked MASs, the bandwidth of the communication network will be limited [12]. As we all know, the event-triggered control (ETC) method can save network bandwidth resources while ensuring network control performance [14]. Therefore, the ETC mechanism has become an important means to reduce energy consumption and signal transmission frequency [15]. From then on, a large number of researchers have begun to study the ETC mechanism to reduce communication burden [1,12,16–21]. A distributed dynamic ETC mechanism was proposed in [21], which extends the communication topology from undirected graph to directed graph. In order to save network bandwidth resources, a hybrid event-triggered strategy associated with an improved threshold function was proposed in [22].

Therefore, how to reduce the communication burden of MASs subject to DoS attacks has attracted the attention of researchers when designing a feedback control loop [13]. In [23], researchers studied the event-triggered resilient control problem of MASs subject to energy-limited periodic DoS attacks. Event-triggered consensus problem of linear MASs interfered by periodic DoS attacks was studied in [24]. Note that the aforementioned papers assume that MASs encounter periodic DoS attacks. However, DoS attacks with an active varying period may be more common. Then, DoS attacks with an active varying period began to receive attention. In [25], distributed secure average consensus problem of linear MASs with event-based samplings was studied. Xu et al. [5] designed a novel ETC protocol based on the estimated relative state. In [26], the researchers designed a distributed secure consensus controller with a dual-terminal ETC mechanism to solve the problem of lack of precise calculation of control input during the attack. In [27], the author studied heterogeneous linear MASs with communication delays and proposed a new distributed resilient control method for it. Resilient event-triggered consensus control for nonlinear MASs was investigated in [28]. In [6], frequency and duration of DoS attacks attacking leaderless and leader-following MASs were accurately analyzed. However, in [5,23,25–28], the information interaction topology of MASs is undirected and the communication channels (information transmission channels among agents) and control channels (information transmission channels from controller to actuator) are simultaneously attacked or only one type of information channel is attacked. Note that in many practical situations, DoS attacks between communication channels and control channels may not be synchronized, which brings new challenges to stability analysis.

Inspired by the above analysis, under the ETC mechanism, we consider the consensus problem of MASs when MASs is attacked by asynchronous DoS attacks, and MASs has a general directed graph. In addition, we propose a event-triggered resilient control mechanism, which enables MASs to reach consensus at an exponentially convergent speed, and prevents multi-agent system from Zeno behavior, thereby avoiding continuous communication between agents. In addition, considering that although DoS attacks effectively prevent transmission of information on the attacked channel between agents, the communication topology between agents still contains a directed spanning tree. We call this situation ineffective DoS attacks, otherwise it is called effective DoS attacks. Taking into account the impact of the aforementioned ineffective DoS attacks, we put forward a more general assumption for the above situation to limit frequency and duration of DoS attacks. Since the communication topology in this article is restricted from connected undirected graph to directed graph containing directed spanning trees, and considering that the system may suffer from multi-channel asynchronous DoS attacks, the proof of the final convergence of consensus errors and the exclusion of the Zeno behavior are more difficult than before. This article has the following three innovations.

(1) This paper reduces the restrictions on the communication topology of MASs and relaxes the communication topology of MASs from undirected connected graph to directed graph including a spanning tree.
(2) This article considers that DoS attacks asynchronously prevent the transmission of information in the communication channel and control channel. In addition, this article reduces the Attack duration and frequency of DoS attacks. Only by limiting the frequency and duration of effective DoS attacks, MAS can achieve consensus.
(3) The event-triggered communication mechanism is applied to the design of the distributed controller of MASs under asynchronous DoS attacks. In addition, under conditions in Theorem 1, MASs under DoS attacks can achieve consensus at an exponentially convergent speed and event triggered controllers of all agents do not have Zeno behavior.

Notations: $R^{m\times n}$ and R^n denote the set of $m \times n$ real matrices and $n \times 1$ column vectors. R^+ denotes the positive constant set. Let 1_N denotes the $N \times 1$ column vector of all ones. The superscript T means the transpose for real matrices. We denote a block-diagonal matrix with c_i on its diagonal by $diag(c_1, c_2, \ldots, c_n)$. Let $\|\cdot\|$ denote the Euclidean norm for vectors and the induced 2-norm for matrices. Let $\otimes$ denote the Kronecker product. Let $num\{eig(\mathscr{L}(t))\}$ denote the number of eigenvalues of the Laplacian matrix $\mathscr{L}(t)$ equal to zero. Let $\lambda_{\max}(X)$ and $\lambda_{\min}(X)$ denote the non-zero maximum eigenvalue and non-zero minimum eigenvalue of X, respectively. Let $L \triangleq \{\mathscr{L}(t) \mid t \in \tilde{\Gamma}^C[0,t)\}$ refer to the set of all possible Laplacian matrices $\mathscr{L}(t)$ for all $t \in \tilde{\Gamma}^C[0,t)$. Let $\lambda_{\min}(L)$ and $\lambda_{\max}(L)$ denote the non-zero minimum and non-zero maximum of eigenvalues of all Laplacian matrices $\mathscr{L}(t)$ in the set L, respectively. Let $\mathscr{L}$ denote the Laplacian matrix $\mathscr{L}(t)$ when there is no dos attacks. Let ζ denote the directed graph $\zeta(t)$ when there is no dos attacks. Let ε denote the set of corresponding edge $\zeta(t)$ when there is no dos attacks. Let $r^T = [r_1, r_2, \ldots, r_N] \in R^{1\times N}$ be the left eigenvector of $\mathscr{L}$ associated with zero eigenvalue, satisfying $r^T 1_N = 1$.

2. Preliminaries and problem description

2.1. Graph theory

We represent time-varying interaction topology among agents in MASs with time-varying directed graphs $\zeta(t) = (\nu, \varepsilon(t), \mathscr{A}(t))$ where $\vartheta = 1, 2, \ldots N$ is the node set containing all agents in MASs. $\varepsilon(t) \subseteq \{(i,j)|i,j \in \nu, i \neq j\}$ is the set of corresponding edge at time t. Edge $(i,j) \in \varepsilon(t)$ implies that agent j can receive information from agent i at time t. A directed path from agent i to agent j is a sequence of ordered edges of the form $(i,i_k),(i_k,i_{k-1}),\ldots,(i_1,j)$, where $\{i_k,\ldots,i_1\} \subseteq \nu$. If there is a node in the node set, and there are directed paths from this node to every other node, we call this node the root node. If there is a root node in the node set, we say that this directed graph contains a directed spanning tree. The adjacency matrix $\mathscr{A}(t) = [a_{ij}(t)] \in R^{N\times N}$ associated with the directed graph $\zeta(t)$ is defined by $a_{ii}(t) = 0, a_{ij}(t) > 0$ if $(j,i) \in \varepsilon(t)$ and $a_{ij}(t) = 0$ otherwise. The Laplacian matrix $\mathscr{L}(t) = [l_{ij}(t)] \in R^{N\times N}$ is defined as $l_{ii}(t) = -\sum_{j=1,j\neq i}^{N} a_{ij}(t)$ and $l_{ij}(t) = a_{ij}(t), i \neq j$.

Assumption 1. (A,B) is stabilizable.

Assumption 2. The directed graph ζ contains a directed spanning tree.

Lemma 1. *[29] Based on Assumptions 2, the Laplacian matrix $\mathscr{L}$ associated with directed graph ζ has exactly one zero eigenvalue and all nonzero eigenvalues are located in the open right left plane.*

2.2. Denial-of-service attacks

This paper considers DoS attacks asynchronously destroy the information transmission in communication channels and control channels. If duration and frequency of DoS attacks are unlimited, the entire system may become unstable. From the perspective of energy limitation, attackers need to enter sleeping area after the attack to provide energy for the next attack. Therefore, this paper assumes that attackers cannot constantly attack the communication network in an active varying period due to limited energy. It is worth noting that, since the communication topology of MASs has a recovery mechanism with internal repair capabilities, it can be restored to the original topology after DoS attacks end [30].

In the case of DoS attacks attacking communication channels of MASs, Define $\Xi_k^{(i,j)} = [h_k^{ij}, h_k^{ij} + \tau_k^{ij})$ as the attack interval of the attacker's kth attacking edge (i,j). h_k^{ij} represents start instant of the kth DoS attacks attacking edge (i,j). $h_k^{ij} + \tau_k^{ij}$ represents end time instant of the kth DoS attacks attacking edge (i,j). The length of the kth DoS attacks on edge (i,j) is τ_k^{ij}. The set of time periods during which edge (i,j) is blocked by DoS attacks in time period $[t_1,t_2)$ is defined as $\Pi_D^{(i,j)}[t_1,t_2) := [t_1,t_2) \bigcap \bigcup_{k=1}^{\infty} \Xi_k^{(i,j)}$. The set of time periods in which at least one edge is attacked by DoS attacks in time period $[t_1,t_2)$ is defined as $\Pi_D[t_1,t_2) := [t_1,t_2) \bigcap \bigcup\limits_{(i,j)\in\varepsilon} \Pi_D^{(i,j)}[t_1,t_2)$. Under DoS attacks, the Laplacian matrix $\mathscr{L}$ will be changed. So, we define the following set

$$\begin{aligned} \Pi^D[t_1,t_2) &:= \{t \in [t_1,t_2) \mid num\{eig(L(t))\} = 1\}, \\ \Pi^U[t_1,t_2) &:= \Pi_D[t_1,t_2) \setminus \Pi^D[t_1,t_2), \end{aligned} \tag{1}$$

where $\Pi^U[t_1,t_2)$ and $\Pi^D[t_1,t_2)$ respectively represent the time period during which communication channels are subject to effective DoS attacks and ineffective DoS attacks in the time period $[t_1,t_2)$.

In the case of DoS attacks attacking control channels, Define $\mathcal{D}_k^i = [h_k^i, h_k^i + \tau_k^i)$ as the attack interval of the attacker's kth attacking control channel of agent i. h_k^i represent start instant of the kth DoS attacks attacking on control channel of agent i. $h_k^i + \tau_k^i$ represent end time instant of the kth DoS attacks attacking on control channel of agent i. The length of the ith DoS attacks on control channel of agent i is τ_k^i. The set of time periods during which the kth control channel is blocked by DoS attacks in time period $[t_1,t_2)$ is defined as $\Sigma_D^i[t_1,t_2) := [t_1,t_2) \bigcap \bigcup_{k=1}^{\infty} \mathcal{D}_k^i$. The set of time periods in which at least one control channel is attacked by DoS attacks in time period $[t_1,t_2)$ is defined as $\Sigma_D[t_1,t_2) := [t_1,t_2) \bigcap \bigcup\limits_{i\in\nu} \Sigma_D^i[t_1,t_2)$. Then, we describe the union of time intervals during which at least one channel is subject to effective DoS attacks. The following two sets are constructed.

$$\Gamma^U[0,t) = \Sigma_D[0,t) \bigcup \Pi^U[0,t), \quad \Gamma^C[0,t) = [0,t) \setminus \Gamma^U[0,t). \tag{2}$$

$\Gamma^U[0,t)$ and $\Gamma^C[0,t)$ respectively represent the union of subintervals when there are effective DoS attacks and when there are no effective DoS attacks in $[0,t)$. In addition, both $\Gamma^U[0,t)$ and $\Gamma^C[0,t)$ are mutually disjoint.

Assumption 3. [31] (Attack Duration): There exist constants $T > 1$ and $\varsigma > 0$ such that the attack duration $\frac{1}{T}$ satisfies

$$| \Gamma^U[t_1,t_2) | \leq \varsigma + \frac{t_2 - t_1}{T}, \quad \forall t_2 > t_1 \geq 0,$$

where $| \Gamma^U[t_1,t_2) |$ represents the Lebesgue measure of $\Gamma^U[t_1,t_2)$.

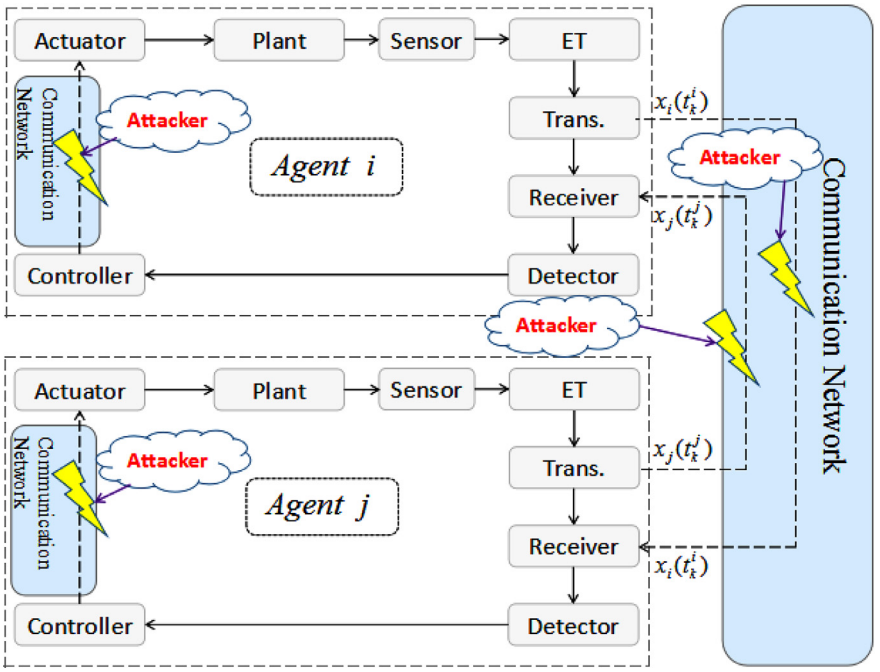


Fig. 1. Framework of MASs.

Assumption 4. [31] (Attack Frequency): There exist constants $\upsilon \geq 0$ and $\tau_D > 0$ such that the attack frequency $\frac{1}{\tau_D}$ satisfies

$$| n[t_1, t_2) | \leq \upsilon + \frac{t_2 - t_1}{\tau_D}, \quad \forall t_2 > t_1 \geq 0,$$

where $| n[t_1, t_2) |$ denotes the number of the effective DoS attacks occurring in the time interval $[t_1, t_2)$.

Remark 1. Note that [5] assumes that assumptions of attack duration and frequency are satisfied for each edge $(i, j) \in \varepsilon(t)$. However, when the communication network among agents also contains a directed spanning tree when DoS attacks attack communication channels, DoS attacks are ineffective. In particular, if attackers continuously attack the fixed side of communication channels and the communication network among agents also contains a directed spanning tree, the assumptions in [5] cannot be satisfied, while the Assumptions 3 and 4 in our article can be satisfied. Therefore, Assumptions 3 and 4 in our article are more general than assumptions about DoS attacks in [5].

Remark 2. In this paper, all networked information transmission channels may be covered by DoS attacks. Attackers attack one or more information transmission channels at different times with different attack durations. Asynchrony is reflected in the measurement and control channels will be affected by DoS separately, i.e. $h_k^{ij} \neq h_k^h$, $\tau_k^{ij} \neq \tau_k^h$, $i, j, h = 1, 2, \ldots, N$.

Remark 3. When the communication network between agents is subject to ineffective DoS attacks, the communication topology between agents changes. Switched topology is a kind of hybrid topologies that own the switching property[32], so we use the method of switching topology to deal with the situation where the communication network between agents is subject to ineffective DoS attacks.

2.3. Problem formulation

Consider the MASs consisting of N agents as shown in Fig. 1. Communication channels and control channels are all networked. MASs are subject to asynchronous DoS attacks. The dynamics of the ith agent described by

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad i = 1, 2, \ldots, N, \tag{3}$$

where $A \in R^{n\times n}$ and $B \in R^{n\times m}$ are given constant matrices. $x_i \in R^{n\times 1}$ is the state of the ith agent, $u_i(t) \in R^{m\times 1}$ denotes the control input of the ith agent.

3. Main result

In order to reduce the information transmission of the communication network, we designed a sensor system with an ETC mechanism to determine the information transmission from the sensor to the controller. We define measurement error

of agent i as

$$e_i(t) = \hat{x}_i(t) - x_i(t), \quad i = 1, 2, \ldots, N, \tag{4}$$

where $\hat{x}_i(t) \triangleq e^{A(t-t_k^i)}x_i(t_k^i)$ and $x_i(t_k^i)$ represents the state of ith agent when the last ETC mechanism update at time t.

The distributed event triggered controller is designed as

$$u_i(t) = \begin{cases} -cK\sum_{j=1}^{N} a_{ij}(t)[\hat{x}_i(t) - \hat{x}_j(t)], & t \in [t_k^i, t_{k+1}^i) \cap \Gamma^C[0,t) \\ 0, & t \in [t_k^i, t_{k+1}^i) \cap \Gamma^U[0,t) \end{cases} \tag{5}$$

where $K \in R^{m\times n}$ is feedback gain matrices, c is coupling strength. Inspired by [6], in order to ensure that there is no Zeno behavior in any of event triggers, we apply a hybrid event triggered method to determine the time when the event trigger of agent i

$$t_0^i = 0, \quad t_{k+1}^i = t_k^i + \eta_{k+1}^i, \tag{6}$$

where $\eta_{k+1}^i \triangleq \max\{\vartheta_{k+1}^i, b^i\}$ is the interevent interval, b^i is a positive scalar to be determined, and ϑ_{k+1}^i is denoted as

$$\vartheta_{k+1}^i = inf\left\{t - t_k^i \mid t \in \Gamma^C[0,t) \wedge t > t_k^i \wedge \|e_i(t)\| - \kappa_i\|\hat{z}_i(t)\| > 0 \right\}, \tag{7}$$

where $\hat{z}_i(t) \triangleq \sum_{j=1}^{N} a_{ij}(t)[\hat{x}_i(t) - \hat{x}_j(t)]$. Parameter κ_i is a positive constant selected according to Theorem 1.

Remark 4. Note that the controller will only be updated after successfully sending its control channel information. When the control channel is not subject to DoS attacks, the controller uses the data transmitted by the event trigger to update through the rules of (5). When the control channel suffers DoS attacks, unlike [33], because the control channel fails to transmit data, the controller has no data to update. Since the controller cannot be updated in time, the input of the controller may be too different from the input actually needed, and eventually the MASs cannot reach consensus. So when the control channel is attacked by DoS attacks, we set the control signal to zero before the next control channel successfully transmits information.

Remark 5. κ_i is a parameter. If κ_i is smaller, the convergence speed of MASs will be faster, and frequent information transmission is required. Otherwise, the convergence speed will slow down, but the frequency of information transmission will decrease. So the appropriate parameter κ_i can be selected according to actual needs to optimize the performance of MASs.

Putting (5) into (3) result in

$$\dot{x}(t) = \begin{cases} (I_N \otimes A + c\mathscr{L}(t) \otimes BK)x(t) \\ +(c\mathscr{L}(t) \otimes BK)e(t), & t \in [t_k^i, t_{k+1}^i) \cap \Gamma^C[0,t) \\ (I_N \otimes A)x(t), & t \in [t_k^i, t_{k+1}^i) \cap \Gamma^U[0,t) \end{cases} \tag{8}$$

where $x(t) = [x_1^{\mathrm{T}}(t), \ldots, x_N^{\mathrm{T}}(t)]^{\mathrm{T}}$, $e(t) = [e_1^{\mathrm{T}}(t), \ldots, e_N^{\mathrm{T}}(t)]^{\mathrm{T}}$.

Let $r^{\mathrm{T}}(t) = [r_1(t), \ldots, r_N(t)] \in R^{1\times N}$ be the left eigenvector of $\mathscr{L}(t)$ associated with zero eigenvalue, satisfying $r^{\mathrm{T}}(t)\mathbf{1}_N = 1$. We introduce a disagreement vector

$$\delta(t) = x(t) - (\mathbf{1}_N r^{\mathrm{T}}(t) \otimes I_n)x(t) = (\mathcal{M} \otimes I_n)x(t), \tag{9}$$

where $\mathcal{M} \triangleq I_N - \mathbf{1}_N r^{\mathrm{T}}(t)$ and $\delta \in R^{Nn\times Nn}$ satisfies $(r^{\mathrm{T}}(t) \otimes I_n)\delta = 0$. Let $Y(t) \in R^{N\times(N-1)}, W(t) \in R^{(N-1)\times N}, T(t) \in R^{N\times N}$ and upper triangular matrix $\Delta(t) \in R^{(N-1)\times(N-1)}$, such that

$$T(t) = \begin{bmatrix} 1_N & Y(t) \end{bmatrix}, T^{-1}(t) = \begin{bmatrix} r^{\mathrm{T}}(t) \\ W(t) \end{bmatrix}, T^{-1}(t)\mathscr{L}(t)T(t) = J(t) = \begin{bmatrix} 0 & 0 \\ 0 & \Delta(t) \end{bmatrix},$$

where diagonal entries of upper triangular matrix $\Delta(t) \in R^{(N-1)\times(N-1))}$ are nonzero eigenvalues of $\mathscr{L}(t)$. Thus, $\mathscr{L}(t)$ has the following properties

$$\mathscr{L}(t)\mathcal{M}(t) = \mathcal{M}(t)\mathscr{L}(t) = \mathscr{L}(t). \tag{10}$$

Similar to [34], Based on (8)–(10), we have

$$\dot{\delta}(t) = \begin{cases} (I_N \otimes A + c\mathscr{L}(t) \otimes BK)\delta(t) \\ +(c\mathscr{L}(t) \otimes BK)e(t), & t \in [t_k^i, t_{k+1}^i) \cap \Gamma^C[0,t) \\ (I_N \otimes A)\delta(t), & t \in [t_k^i, t_{k+1}^i) \cap \Gamma^U[0,t) \end{cases} \tag{11}$$

According to Assumption 1, similar to [35], there exists a symmetric positive definite matrix $P \in R^{n\times n}$ that makes the following inequality true.

$$PA + A^{\mathrm{T}}P - 2PBB^{\mathrm{T}}P + \rho_1 I_n < 0, \tag{12}$$

where $\rho_1 > 0$. ρ_1 can take any positive number. By using the matlab toolbox, we can find the matrix P. Then, we will prove that the fully distributed event-triggered controller (5) can ensure that MASs (3) under DoS attacks achieve consensus exponentially and the Zeno behavior can be avoided under some reasonable assumptions.

Theorem 1. *Consider the MASs (3) satisfying Assumption 1 and communication topology of the MASs (3) satisfying Assumption 2. If duration $\frac{1}{T}$ and frequency $\frac{1}{\tau_D}$ of DoS attacks satisfy following condition*

$$\frac{1}{T}+\frac{d}{\tau_D}\le\frac{\chi}{\chi+\mu}, \tag{13}$$

where $\chi=a_1\rho_1\lambda_{\max}^{-1}(P)$, $a_1\in(0,1)$, $\mu=\frac{\lambda_{\max}(A^{\mathrm{T}}P+PA)}{\lambda_{\min}(P)}$. *Then, under the secure control scheme (5) with* $K=-B^{\mathrm{T}}P$ *and* $c>\frac{1}{\lambda_{\min}(\mathrm{L}(t))}$ *and the triggered sequence determined by (6)–(7) with* $\kappa_i^2=\frac{s_i}{2\lambda_{\max}^2(L)}\le\alpha_1$, *where* $s_{\max}=max_i s_i\in(0,\frac{(1-a_1)^2\rho_1^2}{(1-a_1)^2\rho_1^2+4k_0^2c_1c^2})$, $k_0\triangleq\|PBK\|$, $c_1=\lambda_{\max}^2(L)$, α_1, α_2 *and* α *are constant with* $\alpha_1+\alpha_2=\alpha<1$, *MASs (3) can reach consensus with exponential convergence speed under DoS attacks that satisfy Assumptions 3 and 4, and there is no Zeno behavior in the event triggers of all agents.*

Proof. Step 1 (Two intervals classification) Note that the time period when there is no effective DoS attacks and the time period when there is effective DoS attacks are interleaved, so we write the above two as $t\in[h_{2n}^*,h_{2n+1}^*)$ and $t\in[h_{2n+1}^*,h_{2n+2}^*)$, $n\in N$, respectively. In actual operation scenarios, there is a time lag in the process of attack detection. We record the maximum time lag that may exist in this process as d. Thus, the maximum time interval when condition (7) does not hold for the $n+1$th time can be expressed as

$$\psi_n=[h_{2n+1}^*-d,h_{2n+2}^*). \tag{14}$$

Therefore, the time interval $[t_1,t_2)$ can also be expressed as the union of the following two sub-intervals.

$$\tilde{\Gamma}^U[t_1,t_2)=[t_1,t_2)\bigcap\bigcup_{n=1}^{\infty}\psi_n,\qquad\tilde{\Gamma}^C[t_1,t_2)=[t_1,t_2)\setminus\tilde{\Gamma}^U[t_1,t_2). \tag{15}$$

The set of effective DoS attacks that consider the maximum time lag has the following relationship with the set of effective DoS attacks in (2) that does not consider the maximum time lag.

$$|\,\tilde{\Gamma}^U[t_1,t_2)\,|\le|\,\Gamma^U[t_1,t_2)\,|+|\,n[t_1,t_2)\,|\,d. \tag{16}$$

From Assumptions 3 and 4, we can deduce that

$$|\,\tilde{\Gamma}^U[t_1,t_2)\,|\le\varsigma_*+\frac{t_2-t_1}{T_*}, \tag{17}$$

where $\varsigma_*:=\varsigma+\upsilon d$ and $T_*:=\frac{\tau_D T}{dT+\tau_D}$. **Step 2** (Stability analysis) We choose the Lyapunov function as the following form

$$V(t)=\delta^{\mathrm{T}}(t)(I_n\otimes P)\delta(t). \tag{18}$$

Case I ($t\in\tilde{\Gamma}^C[0,t)$): Along with (11), the derivative of $V(t)$ with respect to t is presented as

$$\begin{aligned}\dot{V}(t)=\;&\delta(t)^{\mathrm{T}}[I_N\otimes(A^{\mathrm{T}}P+PA)+c(\mathscr{L}(t)\otimes PBK+\mathscr{L}^{\mathrm{T}}(t)\otimes K^{\mathrm{T}}B^{\mathrm{T}}P)]\delta(t)\\&+\delta(t)^{\mathrm{T}}[c(\mathscr{L}(t)\otimes PBK+\mathscr{L}^{\mathrm{T}}(t)\otimes K^{\mathrm{T}}B^{\mathrm{T}}P)]e(t).\end{aligned} \tag{19}$$

In light of $K=-B^{\mathrm{T}}P$ and $c>\frac{1}{\lambda_{\min}(\mathscr{L})}$, introducing the state transformation $\hat{\delta}(t)\triangleq(T(t)\otimes I_n)\delta(t)$, we have

$$\begin{aligned}&\delta(t)^{\mathrm{T}}[I_N\otimes c(\mathscr{L}(t)\otimes PBK+\mathscr{L}^{\mathrm{T}}(t)\otimes K^{\mathrm{T}}B^{\mathrm{T}}P)]\delta(t)\\&\le-\hat{\delta}(t)^{\mathrm{T}}[I_N\otimes 2PBB^{\mathrm{T}}P]\hat{\delta}(t).\end{aligned} \tag{20}$$

Due to $\mathscr{L}(t)=T(t)J(t)T^{-1}(t)$, we can get $\mathscr{L}(t)\otimes PBK=(T(t)J(t)\otimes PBK)(T^{-1}(t)\otimes I_n)$. Due to $x^{\mathrm{T}}y\le(\varrho/2)x^{\mathrm{T}}x+(1/2\varrho)y^{\mathrm{T}}y$, let $x^{\mathrm{T}}=\delta(t)^{\mathrm{T}}(T(t)J(t)\otimes PBK)$, $y=(T^{-1}(t)\otimes I_n)e(t)$, we can obtain that

$$\begin{aligned}\delta(t)^{\mathrm{T}}(\mathscr{L}(t)\otimes PBK)e(t)\le\;&(\varrho/2)\delta(t)^{\mathrm{T}}(T(t)J(t)\otimes PBK)(T(t)J(t)\otimes PBK)^{\mathrm{T}}\delta(t)\\&+(1/2\varrho)e(t)^{\mathrm{T}}(T^{-1}(t)\otimes I_n)^{\mathrm{T}}(T^{-1}(t)\otimes I_n)e(t),\end{aligned}$$

where ϱ is a positive constant. Define $\hat{\delta}(t)\triangleq(T(t)^{\mathrm{T}}\otimes I_n)\delta(t)$ and $\hat{e}(t)\triangleq(T^{-1}(t)\otimes I_n)e(t)$, $k_0\triangleq\|PBK\|$, due to $\|J(t)\|^2=c_1$, we can obtain that

$$\hat{\delta}(t)^{\mathrm{T}}(J(t)\otimes PBK)(J(t)\otimes PBK)^{\mathrm{T}}\hat{\delta}(t)\le k_0^2c_1\hat{\delta}(t)^{\mathrm{T}}\hat{\delta}(t).$$

Then we can get

$$\delta(t)^{\mathrm{T}}(\mathscr{L}(t)\otimes PBK)e(t)\le(\varrho/2)k_0^2c_1\hat{\delta}(t)^{\mathrm{T}}\hat{\delta}(t)+(1/2\varrho)\hat{e}(t)^{\mathrm{T}}\hat{e}(t).$$

Similarly,

$$\delta(t)^{\mathrm{T}}(\mathscr{L}^{\mathrm{T}}(t)\otimes K^{\mathrm{T}}B^{\mathrm{T}}P)e(t)\le(\varrho/2)k_0^2c_1\hat{\delta}(t)^{\mathrm{T}}\hat{\delta}(t)+(1/2\varrho)\hat{e}(t)^{\mathrm{T}}\hat{e}(t).$$

So we can get

$$\delta(t)^{\mathrm{T}}[(\mathscr{L}(t)\otimes PBK+\mathscr{L}^{\mathrm{T}}(t)\otimes K^{\mathrm{T}}B^{\mathrm{T}}P)]e(t)\le\varrho k_0^2c_1\hat{\delta}(t)^{\mathrm{T}}\hat{\delta}(t)+\tfrac{1}{\varrho}\hat{e}(t)^{\mathrm{T}}\hat{e}(t). \tag{21}$$

Since $PA + A^{\mathrm{T}}P - 2PBB^{\mathrm{T}}P + \rho_1 I_n < 0$, substituting (20)–(21) into (19) result in

$$\dot{V}(t) \leq \quad -\rho_1\delta(t)^{\mathrm{T}}\delta(t) + c\varrho k_0^2 c_1\hat{\delta}(t)^{\mathrm{T}}\hat{\delta}(t) + \frac{c}{\varrho}\hat{e}(t)^{\mathrm{T}}\hat{e}(t), \tag{22}$$

where $\|\hat{e}(t)\| \leq \|T^{-1}(t)\otimes I_n\|\|e(t)\| \leq \|e(t)\|$ and $\|\hat{\delta}(t)\| \leq \|T^{-1}(t)\otimes I_n\|\|\delta(t)\| \leq \|\delta(t)\|$ is used with $\|T^{-1}(t)\otimes I_n\| = 1$. Let $\hat{z}(t) = [\hat{z}_1^{\mathrm{T}}(t), \ldots, \hat{z}_N^{\mathrm{T}}(t)]^{\mathrm{T}}$ with $\hat{z}_i(t) \triangleq \sum_{j=1}^N a_{ij}(t)[\hat{x}_i(t) - \hat{x}_j(t)]$ and $e_i(t) = \hat{x}_i(t) - x_i(t)$, we have

$$\begin{aligned} \|\hat{z}(t)\| \quad &= \|(\mathscr{L}(t)\otimes I_n)[x(t) + e(t)]\| = \|z(t) + (\mathscr{L}(t)\otimes I_n)e(t)\| \\ &\leq \|z(t)\| + \|(\mathscr{L}(t)\otimes I_n)e(t)\| \leq \|z(t)\| + \lambda_{max}(L)\|e(t)\|, \end{aligned} \tag{23}$$

where $z_i(t) \triangleq \sum_{j=1}^N a_{ij}(t)[x_i(t) - x_j(t)]$.

By (10), $(\mathscr{L}(t))^{\mathrm{T}}\mathscr{L}(t) \leq \lambda_{\max}^2(\mathscr{L}(t))\mathcal{M}^2(t)$ holds, which implies

$$\begin{aligned} \|z(t)\|^2 \quad &= x^{\mathrm{T}}(t)[\mathscr{L}^{\mathrm{T}}(t)\otimes I_n)(\mathscr{L}(t)\otimes I_n)]x(t) = x^{\mathrm{T}}(t)[(\mathscr{L}(t))^{\mathrm{T}}\mathscr{L}(t)\otimes I_n]x \\ &\leq \lambda_{max}^2(\mathscr{L}(t)x^{\mathrm{T}}(t)[(\mathcal{M}(t))^{\mathrm{T}}\mathcal{M}(t)\otimes I_n]x(t) \leq \lambda_{max}^2(L)\|\delta(t)\|^2. \end{aligned} \tag{24}$$

Combining (23) with (24) yields $\|\hat{z}(t)\| \leq \lambda_{\max}(L)(\|\delta(t)\| + \|e(t)\|)$. Since $\|e_i(t)\| \leq \kappa_i\|\hat{z}_i(t)\|$ (Proof in the Step 3), it follows from $\kappa_i^2 = \frac{s_i}{2\lambda_{\max}^2(L)}$ that for $s_{\max} = max_i s_i$, $\|e(t)\|^2 \leq \frac{s_{\max}\|\hat{z}(t)\|^2}{2\lambda_{\max}^2(L)} \leq s_{\max}(\|\delta(t)\|^2 + \|e(t)\|^2)$, which leads to $\|e(t)\|^2 \leq \frac{s_{\max}\|\delta(t)\|^2}{1-s_{\max}}$. Choose $s_{\max}$ in Theorem 1, then we have

$$\dot{V}(t) \leq -\rho_1\delta(t)^{\mathrm{T}}\delta(t) + c\varrho k_0^2 c_1\delta(t)^{\mathrm{T}}\delta(t) + \frac{cs_{max}}{\varrho(1-s_{max})}\delta(t)^{\mathrm{T}}\delta(t), \quad t \in \tilde{\Gamma}^C[0,t). \tag{25}$$

Choose κ_i and a_1 according to Theorem 1, $\varrho = \frac{(1-a_1)\rho_1}{2cc_1k_0^2}$, (25) becomes

$$\dot{V}(t) \leq -\chi V(t), \quad t \in \tilde{\Gamma}^C[0,t). \tag{26}$$

Case II ($t \in \tilde{\Gamma}^U[0,t)$): Along with (11), the derivative of $V(t)$ with respect to t is presented as

$$\dot{V}(t) = \delta(t)^{\mathrm{T}}[I_N\otimes(A^{\mathrm{T}}P + PA)]\delta(t). \tag{27}$$

Choose μ according to Theorem 1, (27) becomes

$$\dot{V}(t) \leq \mu V(t) \quad t \in \Gamma^U[0,t). \tag{28}$$

From the above analysis, we combine the above two cases, the following relationship exists.

$$\dot{V}(t) = \begin{cases} -\chi V(t), & t \in \Gamma^C[0,t), \\ \mu V(t), & t \in \Gamma^U[0,t). \end{cases} \tag{29}$$

It follows from (29) that

$$V(t) \leq \begin{cases} V(h_{2n}^*)e^{-\chi(t-h_{2n}^*)}, & t \in [h_{2n}^*, h_{2n+1}^*), \\ V(h_{2n+1}^*)e^{\mu(t-h_{2n+1}^*)}, & t \in [h_{2n+1}^*, h_{2n+2}^*). \end{cases} \tag{30}$$

If $t \in [h_{2n}^*, h_{2n+1}^*), n \in N$, then

$$\begin{aligned} V(t) \quad &\leq V(h_{2n}^*)e^{-\chi(t-h_{2n}^*)} = V(h_{2n}^*)^- e^{-\chi(t-h_{2n}^*)} \\ &\leq V(h_{2n-1}^*)e^{\mu(h_{2n}^*-h_{2n-1}^*)}e^{-\chi(t-h_{2n}^*)} = V(h_{2n-1}^*)^- e^{\mu(h_{2n}^*-h_{2n-1}^*)}e^{-\chi(t-h_{2n}^*)} \\ &\leq [V(h_{2n-2}^*)e^{-\chi(h_{2n-1}^*-h_{2n-2}^*)}]e^{\mu(h_{2n}^*-h_{2n-1}^*)}e^{-\chi(t-h_{2n}^*)} \leq \ldots \\ &\leq V(0)e^{-\chi\tilde{\Gamma}^C[0,t)}e^{\mu\tilde{\Gamma}^U[0,t)}. \end{aligned} \tag{31}$$

If $t \in [h_{2n+1}^*, h_{2n+2}^*), n \in N$, then

$$\begin{aligned} V(t) \quad &\leq V(h_{2n+1}^*)e^{\mu(t-h_{2n+1}^*)} \leq V(h_{2n}^*)e^{-\chi(h_{2n+1}^*-h_{2n}^*)}e^{\mu(t-h_{2n+1}^*)} \leq \ldots \\ &\leq V(0)e^{-\chi\tilde{\Gamma}^C[0,t)}e^{\mu\tilde{\Gamma}^U[0,t)}. \end{aligned} \tag{32}$$

Note that

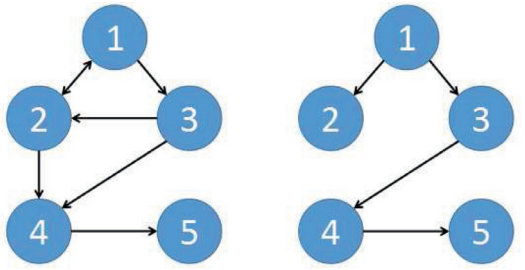
$$\tilde{\Gamma}^U[0,t)\bigcup\tilde{\Gamma}^C[0,t) = [0,t], \quad \tilde{\Gamma}^U[0,t)\bigcap\tilde{\Gamma}^C[0,t) = \emptyset.$$

Then we have

$$V(t) \leq V(0)e^{-\chi(t-\tilde{\Gamma}^U[0,t))}e^{\mu\tilde{\Gamma}^U[0,t)} \leq V(0)e^{-\chi t}e^{(\chi+\mu)\tilde{\Gamma}^U[0,t)}. \tag{33}$$

Substituting (17) into (33) result in

$$\begin{aligned} V(t) \quad &\leq V(0)e^{-\chi t}e^{(\chi+\mu)(\varsigma_\star + \frac{t}{l_\star})} \leq V(0)e^{-\chi t}e^{(\chi+\mu)\varsigma_\star}e^{(\chi+\mu)\frac{t}{l_\star}} \\ &\leq V(0)e^{-(\chi-\frac{\chi+\mu}{l_\star})t}e^{(\chi+\mu)\varsigma_\star}. \end{aligned} \tag{34}$$



(a) Laplacian matrix L (b) Laplacian matrices L1

Fig. 2. Laplacian matrices of the communication graph.

From (13),we have that $\eta = \chi - \frac{\chi+\mu}{T_\star} > 0$. Therefore

$$V(t) \le V(0)e^{-\eta t}e^{(\chi+\mu)\varsigma_\star}. \tag{35}$$

So MASs (3) can achieve consensus exponentially.

Step 3 (Excluding Zeno behavior) Inspired by Feng and Hu [6], the interevent interval of the ith event trigger in $t \in (t_k^i, t_{k+1}^i]$ is determined by ϑ_{k+1}^i or b^i. We use $Q_1(t)$ and $Q_2(t)$ to represent event triggers whose interevent interval is determined by ϑ_{k+1}^i and b^i, respectively. Then, $Q_1(t) \cup Q_2(t) = \{\nu\}$ and $Q_1(t) \cap Q_2(t) = \emptyset$. To ensure $\|e_i(t)\| \le \kappa_i\|\hat{z}_i(t)\|$ in (7), one can choose that for $\alpha_1 + \alpha_2 = \alpha < 1$

$$\sum_{i\in Q_1(t)} \|e_i(t)\|^2 \le \alpha_1 \sum_{i\in Q_1(t)} \|\hat{z}_i(t)\|^2 \le \alpha_1 \sum_{i=1}^{N} \|\hat{z}_i(t)\|^2. \tag{36}$$

$$\sum_{i\in Q_2(t)} \|e_i(t)\|^2 \le \alpha_2 \sum_{i\in Q_2(t)} \|\hat{z}_i(t)\|^2 \le \alpha_2 \sum_{i=1}^{N} \|\hat{z}_i(t)\|^2. \tag{37}$$

For event triggers in $Q_1(t)$, a sufficient condition of inequality (36) is $\|e_i(t)\| \le \kappa_i\|\hat{z}_i(t)\|$ with $\kappa_i^2 \le \alpha_1$. Next, for event triggers in $Q_2(t)$, a sufficient condition of inequality (37) is $\|e_i(t)\|^2 \le \sum_{i=1}^{N} \frac{\alpha_2}{N}\|\hat{z}_i(t)\|^2 \le \frac{2\alpha_2\lambda_{\max}^2(L)}{N(1-s_{\max})}\|\delta(t)\|^2$ for all $i \in Q_2(t)$. Let $h = \frac{2\alpha_2\lambda_{\max}^2(L)}{N(1-s_{\max})}$. Then $\|e_i(t)\|^2 \le h\|\delta(t)\|^2$. If m_i denotes a lower bound for the evolution time of $\|e_i(t)\|/\|\delta(t)\|$ from 0 to $\sqrt{h}$, for event triggers in $Q_2(t)$, We can find that $t_{k+1}^i = t_k^i + m_i$ is a sufficient condition to ensure (37). In order to prove that there is a positive interevent interval, we can estimate $\|e_i(t)\|/\|\delta(t)\|$,

$$\frac{d}{dt}\frac{\|e_i(t)\|}{\|\delta(t)\|} = \frac{e_i^{\mathrm{T}}(t)\dot{e}_i(t)}{\|e_i(t)\|\|\delta(t)\|} - \frac{\|e_i(t)\|\delta^{\mathrm{T}}(t)\dot{\delta}(t)}{\|\delta(t)\|^3} \le \frac{\|\dot{e}_i(t)\|}{\|\delta(t)\|} + \frac{\|e_i(t)\|}{\|\delta(t)\|}\frac{\|\dot{\delta}(t)\|}{\|\delta(t)\|}. \tag{38}$$

Since $\dot{e}_i(t) = Ae_i(t) + cBK\sum_{j=1}^{N} l_{ij}(t)(e_j(t) + x_j(t))$, it gets

$$\frac{\|\dot{e}_i(t)\|}{\|\delta(t)\|} \le \|A\|\frac{\|e_i(t)\|}{\|\delta(t)\|} + cN\|BK\|\left(\frac{\|e_i(t)\|}{\|\delta(t)\|} + \frac{1}{\lambda_{min}(\mathcal{M})}\right). \tag{39}$$

By using (39) and $\|e(t)\| = \sqrt{\sum_{i=1}^{N}\|e_i(t)\|^2} \le \sqrt{Nh}\|\delta(t)\|$, $(d/dt)(\|e_i(t)\|)/\$\|\delta(t)\|) \le a_2(\|e_i(t)\|)/(\|\delta(t)\|) + a_3$, where $a_2 = 2\|A\| + c\lambda_{\max}(L)\|BK\|(1+\sqrt{Nh}) + cN\|BK\|$ and $a_3 = cN\|BK\|/\lambda_{\min}(\mathcal{M})$. Thus, the evolution time of $\|e_i(t)\|/\|\delta(t)\|$ from 0 to $\sqrt{h}$ has a lower bound greater than zero. We use ϖ to represent this lower bound. For event triggers in $Q_2(t)$, we choose the interevent time $m_i \le \varpi$ to ensure that (37) holds. In summary, we can conclude that all event triggers (6) can ensure that condition (7) is established. Let $\varphi = (\lambda_{\max}(P)/\lambda_{\min}(P))e^{(\chi+\mu)\varsigma_\star}$. Hence, through (35), it has $\|\delta(t)\|^2 \le \varphi e^{-\eta t}\|\delta(0)\|^2$. Therefore, we get the conclusion that MASs can achieve secure consensus with exponential convergence speed. So we get that secure consensus is realized at the speed of exponential convergence. In addition, $\|\delta(t)\|^2 = 0$ as $t \to +\infty$. Thus, $\lim_{t\to+\infty} x_i(t) = \sum_{i=1}^{N} r_i(t)x_i(t)$. The proof of Theorem 1 is completed. □

4. Example

The purpose of this section is to verify the effectiveness of the proposed secure control mechanism through a numerical example. Consider a MASs consisting of 5 agents described by (2), where $A = [0.2, 1; 0, -2]$ and $B = [5; 5]$. (A, B) is stabilizable. The original communication topology between agents is a directed graph containing a directed spanning tree as

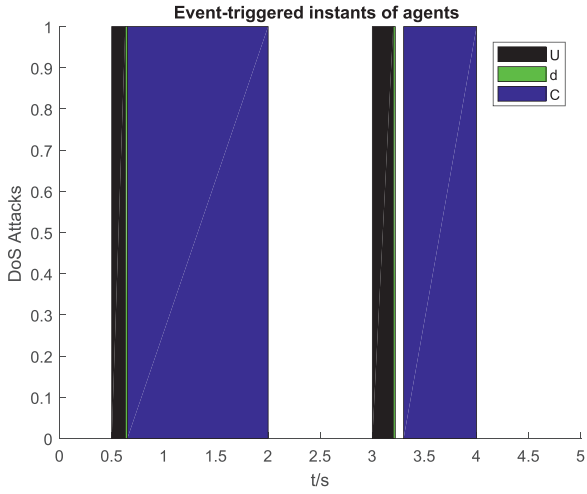
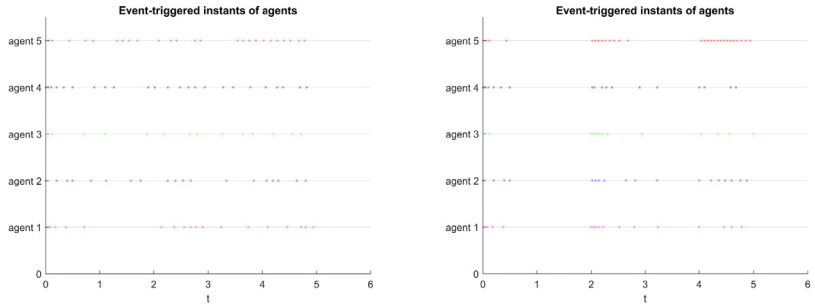


Fig. 3. Sequence of DoS attacks.



(a) Triggering times under ETC mechanism (6)-(7)

(b) Triggering times under ETC mechanism in [6]

Fig. 4. Triggering times under two ETC mechanisms.

shown in Fig. 2(a). Fig. 2(b) shows the communication topology after ineffective DoS attacks on the communication topology between agents. The Laplacian matrices L of the original communication topology $\mathscr{L}$ is:

$$L=\begin{bmatrix}1&-1&0&0&0\\-1&2&-1&0&0\\-1&0&1&0&0\\0&-1&-1&2&0\\0&0&0&-1&1\end{bmatrix}, L1=\begin{bmatrix}0&0&0&0&0\\-1&1&0&0&0\\-1&0&1&0&0\\0&0&-1&1&0\\0&0&0&-1&1\end{bmatrix}.$$

where $L1$ refers to the Laplacian matrices when MASs is under ineffective DoS attacks.

The initial states of five agents are given as follows:

$$x_1(0)=\begin{bmatrix}2\\-3\end{bmatrix}, x_2(0)=\begin{bmatrix}1\\-2\end{bmatrix}, x_3(0)=\begin{bmatrix}-1\\2\end{bmatrix}, x_4(0)=\begin{bmatrix}3\\0\end{bmatrix}, x_5(0)=\begin{bmatrix}-2\\1\end{bmatrix}.$$

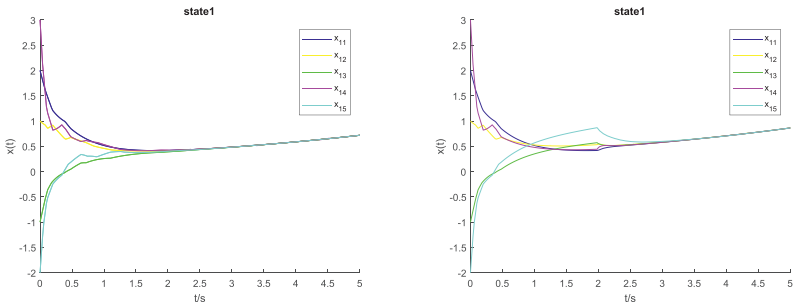
where each state is randomly chosen.

The feedback gain matrix K can be calculated as

$$P=\begin{bmatrix}0.2485&-0.1002\\-0.1002&0.1581\end{bmatrix}, K=\begin{bmatrix}-0.7414&-0.2892\end{bmatrix}.$$

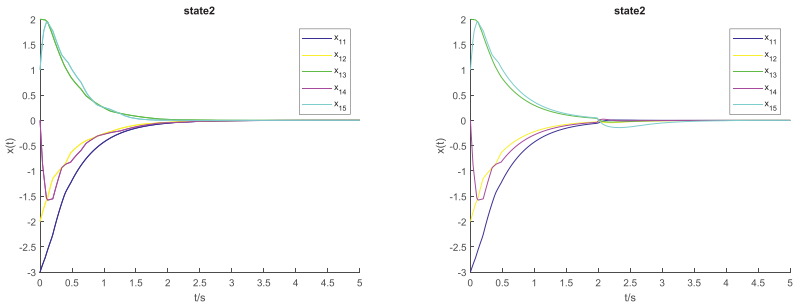
The coupling strength c can be calculated according to Theorem 1 as $c=1.0001$. Attack duration and attack frequency are $(1/T)=1/20$ and$(1/\tau_D)=2.5$ satisfying (13). The parameters κ_i are selected as $\kappa_i=0.1, i=1,2,\ldots,5$. we choose the parameter $d=0.02$.

The attack strategy of DoS attacks is shown in Fig. 3, where black bar graph represents effective DoS attacks, green bar graph represents d and blue bar graph represents ineffective DoS attacks. The width of the black bar graph represents the



(a) State trajectory under ETC mechanism (6)-(7) (b) State trajectory under ETC mechanism in [6]

Fig. 5. The first component of state trajectories for five agents.



(a) State trajectory under ETC mechanism (6)-(7) (b) State trajectory under ETC mechanism in [6]

Fig. 6. The second component of state trajectories of five agents.

duration of effective DoS attacks. The width of the green bar graph represents the duration of the maximum time lag. The width of the blue bar graph represents the duration of ineffective DoS attacks. It should be noted that Theorem 1 of this paper only limits the attack duration and attack frequency of effective DoS attacks. Therefore, compared with [6], the greater the proportion of ineffective DoS attacks, the better the control effect that can be obtained by using the event-triggered control mechanism proposed in this paper.

Fig. 4 illustrates Triggering times under ETC mechanism (6)–(7) and ETC mechanism in [6]. Fig. 5 shows the first component of state trajectories for five agents under ETC mechanism (6)–(7) and ETC mechanism in [6]. Fig. 6 shows the second component of state trajectories for five agents under ETC mechanism (6)–(7) and ETC mechanism in [6]. It can be seen from Figs. 5 to 6 that under the same initial parameters, using the event-triggered control mechanism proposed in this article can achieve better convergence results than using the event-triggered control mechanism in [6]. In addition, when the comunication topology of MASs includes a spanning tree, the condition of the theorem 3 in reference [6] is not satisfied, but the theorem 1 proposed in this paper is satisfied. Therefore, the theorem proposed in our paper has a wider application range.

5. Conclusion

In this paper, we investigated event-triggered resilient control for general linear MASs subject to asynchronous DoS attacks. Compared with the existing results of ETC for MASs under DoS attack, this paper reduces the restrictions on the communication topology of MASs and relaxes the communication topology of MASs from undirected connected graph to directed graph including a spanning tree. Secondly, this article innovatively uses the method of switching topology to deal with the ineffective DoS attacks suffered by MASs. Only by limiting the frequency and duration of effective DoS attacks, MASs can achieve consistency. Finally, this article considers the existence of asynchronous DoS attacks in MASs. The synchronous DoS attack in the previous literature is a special case of this article. In the future work, the developed method will be extended to more complicated situations, for instance, MASs with the Tagaki-Sugeno fuzzy model [36], discrete-time MASs [37], MASs with quantization [38].

Acknowledgments

This research was supported by the National Natural Science Foundation of China (NSFC) under Grant 11571322 and Grant 11971444.

References

[1] X.L. Yi, K. Liu, D.V. Dimarogonas, K.H. Johansson, Dynamic event-triggered and self-triggered control for multi-agent systems, IEEE Trans. Autom. Control 64 (8) (2019) 3300–3307.
[2] A. Hussein, M. Adel, M. Bakr, O.M. Shehata, A. Khamis, Multirobot task allocation for search and rescue missions, J. Phys. 570 (2014) 052006.
[3] J. Cheng, J.H. Park, X.-D. Zhao, H.R. Karimi, J.D. Cao, Quantized nonstationary filtering of network-based Markov switching RSNSs: a multiple hierarchical structure strategy, IEEE Trans. Autom. Control 65 (11) (2020) 4816–4823.
[4] Z.H. Zhang, D. Lin, C. Deng, Q.Y. Fan, A dynamic event-triggered resilient control approach to cyber-physical systems under asynchronous dos attacks, Inf. Sci. 519 (2020) 260–272.
[5] Y. Xu, M. Fang, Z.G. Wu, Y.J. Pan, Input-based event-triggering consensus of multiagent systems under denial-of-service attacks, IEEE Trans. Syst. Man Cybern. 50 (4) (2020) 1455–1464.
[6] Z. Feng, G.Q. Hu, Secure cooperative event-triggered control of linear multiagent systems under dos attacks, IEEE Trans. Control Syst. Technol. 28 (3) (2020) 741–752.
[7] D.-J. Wang, F. Chen, B. Meng, X.-L. Hu, J. Wang, Event-based secure H_∞ load frequency control for delayed power systems subject to deception attacks, Appl. Math. Comput. 394 (2021) 125788.
[8] M. Long, C. Wu, J. Hung, Denial of service attacks on network-based control systems: impact and mitigation, IEEE Trans. Ind. Inform. 1 (2) (2005) 85–96.
[9] Y. Wu, X. He, Secure consensus control for multiagent systems with attacks and communication delays, IEEE/CAA J. Autom. Sin. 4 (1) (2017) 136–142.
[10] Y. Wang, G.-H. Wen, X.-H. Yu, T.W. Huang, Distributed consensus tracking of networked agent systems under denial-of-service attacks, IEEE Trans. Syst. Man Cybern. (2020) 1–14, doi:10.1109/TSMC.2019.2960301.
[11] H.-J. Yang, D. Ye, Observer-based fixed-time secure tracking consensus for networked high-order multiagent systems against dos attacks, IEEE Trans. Cybern. (2020) 2168–2275, doi:10.1109/TCYB.2020.3005354.
[12] B. Cheng, Z.K. Li, Fully distributed event-triggered protocols for linear multiagent networks, IEEE Trans. Autom. Control 64 (4) (2019) 1655–1662.
[13] J. Wang, T.-T. Ru, J.-W. Xia, H. Shen, V. Sreeram, Asynchronous event-triggered sliding mode control for semi-Markov jump systems within a finite-time interval, IEEE Trans. Circuits Syst. I Regul. Pap. 68 (1) (2021) 458–468.
[14] Y.-Q. Zhang, P. Shi, R.K. Agarwal, Event-based dissipative analysis for discrete time-delay singular stochastic systems, Int. J. Robust Nonlinear Control 28 (11) (2018) 6106–6121.
[15] Y.-Q. Zhang, P. Shi, R.K. Agarwal, Y. Shi, Event-based dissipative analysis for discrete time-delay singular jump neural networks, IEEE Trans. Neural Netw. Learn. Syst. 31 (4) (2020) 1232–1241.
[16] Y.-Q. Zhang, P. Shi, R.K. Agarwal, Y. Shi, J. Control, Event-based mixed H_∞ and passive filtering for discrete singular stochastic systems, Int. J. Control, 2020b, 93, 10, 2407–2415.
[17] D.R. Ding, Z.D. Wang, W.C.H. Daniel, G.L. Wei, Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks, IEEE Trans. Cybern. 47 (8) (2017) 1936–1947.
[18] Y. Xu, Z.G. Wu, Y.J. Pan, K.A. Choon, H.C. Yan, Consensus of linear multiagent systems with input-based triggering condition, IEEE Trans. Syst. Man Cybern. 49 (11) (2019) 2308–2317.
[19] W.F. Hu, L. Liu, G. Feng, Consensus of linear multi-agent systems by distributed event-triggered strategy, IEEE Trans. Cybern. 46 (1) (2016) 148–157.
[20] L.X. Xu, H.J. Ma, L.N. Zhao, Distributed event-triggered output-feedback control for sampled-data consensus of multi-agent systems, J. Frankl. Inst. 357 (6) (2019) 3168–3192.
[21] W.F. Hu, C.H. Yang, T.W. Huang, W.H. Gui, A distributed dynamic event-triggered control approach to consensus of linear multiagent systems with directed networks, IEEE Trans. Cybern. 50 (2) (2020) 869–874.
[22] J. Wang, Y. Wang, H. Yan, et al., Hybrid event-based leader-following consensus of nonlinear multiagent systems with semi-Markov jump parameters, IEEE Syst. J. (2020) 1–12, doi:10.1109/JSYST.2020.3029156.
[23] Y. Xu, M. Fang, P. Shi, Z.G. Wu, Event-based secure consensus of mutiagent systems against dos attacks, IEEE Trans. Cybern. 50 (2019) 3468–3476.
[24] Z.-H. Cheng, D. Yue, S.-L. Hu, H. Ge, L. Chen, Distributed event-triggered consensus of multi-agent systems under periodic dos jamming attacks, Neurocomputing 400 (2020) 458–466.
[25] Z. Feng, G.Q. Hu, Distributed secure average consensus for linear multi-agent systems under dos attacks, in: Proceedings of the American Control Conference, 2017, pp. 2261–2266, doi:10.23919/ACC.2017.7963289.
[26] Y. Yang, Y.F. Li, D. Yue, Y.C. Tian, X.H. Ding, Distributed secure consensus control with event-triggering for multiagent systems under dos attacks, IEEE Trans. Cybern. (2020) 2168–2275, doi:10.1109/TCYB.2020.2979342.
[27] C. Deng, C.Y. Wen, MAS-based distributed resilient control for a class of cyber-physical systems with communication delays under dos attacks, IEEE Trans. Cybern. (2020), doi:10.1109/TCYB.2020.2972686.
[28] L.J. Zha, J.L. Liu, J.D. Cao, Resilient event-triggered consensus control for nonlinear muti-agent systems with dos attacks, J. Frankl. Inst. 356 (13) (2019) 7071–7090.
[29] W. Ren, R.W. Beard, Consensus seeking in multiagent systems under dynamically changing interaction topologies, IEEE Trans. Autom. Control 50 (5) (2005) 655–661.
[30] Z. Feng, G. Wen, G. Hu, Distributed secure coordinated control for multiagent systems under strategic attacks, IEEE Trans. Cybern. 47 (5) (2017) 1273–1284.
[31] C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Trans. Autom. Control 60 (11) (2015) 2930–2944.
[32] Y.-D. Wang, X.-H. Hu, K.-B. Shi, X.-N. Song, H. Shen, Network-based passive estimation for switched complex dynamical networks under persistent dwell-time with limited signals, J. Frankl. Inst. 357 (2020) 10921–10936.
[33] D.-P. Yang, W. Ren, X.-D. Liu, W.S. Chen, Decentralized event-triggered consensus for linear multi-agent systems under general directed graphs, Automatica 69 (2016) 242–249.
[34] R. Olfati-Saber, R.M. Murray, Consensus problems in networks of agents with switching topology and time-delays, IEEE Trans. Autom. Control 49 (9) (2004) 1520–1533.
[35] C.V. Loan, The sensitivity of the matrix exponential, SIAM J. Numer. Anal. 14 (6) (1977) 971–981.
[36] J. Cheng, Y.-N. Shan, J.-D. Cao, J.H. Park, Nonstationary control for T-S fuzzy Markovian switching systems with variable quantization density, IEEE Trans. Fuzzy Syst. (2020), doi:10.1109/TFUZZ.2020.2974440.
[37] J. Wang, J.-W. Xia, S. H, M.-P. Xing, J.H. Park, H_∞ synchronization for fuzzy Markov jump chaotic systems with piecewise-constant transition probabilities subject to PDT switching rule, IEEE Trans. Fuzzy Syst. (2020), doi:10.1109/TFUZZ.2020.3012761.
[38] J. Cheng, J.H. Park, J.-D. Cao, W.H. Qi, A hidden mode observation approach to finite-time SOFC of Markovian switching systems with quantization, Nonlinear Dyn. 100 (2020) 509–521.