SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •
May 2020, Vol. 63 150208:1–150208:14
https://doi.org/10.1007/s11432-019-2687-7
Special Focus on Advanced Techniques for Event-Triggered Control and Estimation

Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels

Yang YANG[1,3*], Yanfei LI[1] & Dong YUE[1,2,3]

[1]*College of Automation & College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing* 210023*, China;*
[2]*Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210023*, China;*
[3]*Jiangsu Engineering Laboratory of Big Data Analysis and Control for Active Distribution Network, Nanjing University of Posts and Telecommunications, Nanjing* 210023*, China*

Received 26 March 2019/Revised 30 June 2019/Accepted 23 September 2019/Published online 13 March 2020

Abstract This paper proposes a consensus secure control scheme in the presence of denial-of-service (DoS) attacks based on an event-trigger mechanism. In contrast to a scenario in which attacks are the same and simultaneously paralyze all channels, the DoS attack addressed in this paper occurs aperiodically and results in the independent interruption of multiple transmission channels. A sufficient condition for the attack duration is designed and a distributed event-triggered control scheme is proposed, where the updated instants are triggered aperiodically to reduce the required communication resources. It is shown that the overall system is stable with the proposed scheme according to the Lyapunov stability theory and that Zeno behavior is excluded. Finally, a numerical example is presented to verify the effectiveness of the proposed scheme.

Keywords multi-agent system, event-triggered control, consensus secure control, denial-of-service attack, multiple transmission channels

Citation Yang Y, Li Y F, Yue D. Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels. Sci China Inf Sci, 2020, 63(5): 150208, https://doi.org/10.1007/s11432-019-2687-7

1 Introduction

Over the past several years, the control issues of multi-agent systems (MASs) have attracted extensive attention owing to their wide range of applications [1–3] in unmanned aerial vehicle (UAV) formations, multi-sensor network filtering, and flocking. A fundamental problem for MASs is the design of control approaches on the basis of combined information from local and neighboring sources such that all agents achieve consensus. Remarkable results have been achieved by multiple scholars [4–7]. Accompanying the development of communication technology, it has been reported that MASs are vulnerable to malicious attacks [8–11]. Severe attacks deteriorate the control performance of the networked system [10, 12–14] and may result in undesirable instabilities. It is important and challenging to design effective secure control methods for MASs.

Many efforts have been taken into developing the secure control of networked MASs against attacks. Currently, the primary types of attacks include DoS attacks [15], replay attacks [16], and deception

* Corresponding author (email: yyang@njupt.edu.cn)

attacks [17]. These attacks act over transmission channels, control channels, sensors, and agents. For MASs, DoS attacks are one of the most common and destructive form of attacks, invalidating system resources by affecting the measurement and control channels and resulting in serious delays and packet loss problems in the system. Such attacks pose a critical problem to the secure control and stability analyses of MASs. In [18], a queue model [19] was employed to describe such attack behavior, and a system under DoS attacks was transformed into a system with time delays. A model-based resilient controller was designed for an MAS under DoS attacks in [20]. DoS attacks occur periodically in the real world, and the robust output consistency problem has been discussed for a class of heterogeneous linear MASs with aperiodic sampling [21]. Many existing secure control strategies for MASs under DoS attacks satisfying certain frequencies and durations [15, 22, 23] have also been proposed. A type of pulse controller was designed using a dynamic observer and measuring triggered state reset method in [15], which considered maximizing the frequency and duration of DoS attacks. However, in the above studies, it was assumed that the attackers simultaneously paralyzed all communication links. Only a few reports have been found for the case that multiple transmission channels are attacked independently.

Apart from time-driven strategies, another key technique related to the secure control of MASs is event-triggered mechanisms [24]. Unnecessary communication might result in the inefficient implementation of energy consumption, communication bandwidth, congestion, and computational resources. To reduce the communication requirements while guaranteeing the system performance, event-triggered control methods were widely applied to MASs [25–28]. A novel distributed periodic-resilient event-triggered communication scheme was discussed and analyzed in [29] in which it was assumed that the DoS attacks were partially identified. Event-triggered secure controls were designed in [30, 31] without Zeno behavior by observing the internal states of an agent in a linear system subjected to aperiodic DoS attacks. A flexible control framework was developed [22] to balance the performance and communication resources and obtain the input-to-state stability. A leader-following consensus issue was solved in [8, 9] using event-triggered control under DoS attacks, and a self-triggered communication scheme was proposed in [9] to further avoid continuous monitoring. Despite the fact that there exist few studies related to secure control with event-triggered mechanisms, most such studies have not taken into account the performance loss caused by DoS attacks, which is a potential issue.

Inspired by the above-mentioned studies, in this paper, a distributed secure control scheme using an event-triggered scheduling method is designed for a linear MAS to achieve consensus in the presence of DoS attacks. The main contributions of the paper can be summarized as follows.

(1) We design the secure control scheme for a linear MAS under unknown and aperiodic DoS attacks. As opposed to the scenarios in [8, 21, 30, 31], where all the communication links simultaneously suffered DoS attacks, the multiple transmission channels suffering DoS attacks from multiple adversaries are independent in this paper, and a sufficient condition of the attack duration and the decay rates for different attack modes are obtained.

(2) A novel event-triggered function is designed for the control scheme. As opposed to [11, 22, 29, 32–34], in which the authors designed secure controllers based on either time-driven or traditional event-triggered strategies, we introduce a resilient secure event-triggered mechanism considering extra errors caused by DoS attacks into an event-triggered function to update the actual state of the system only at the triggered instants and avoid unnecessary events. Moreover, compared with the event-trigger-based consensus results in [22, 29, 32], an additional term, a decaying function, is employed in the triggered function to fully guarantee Zeno-free phenomena for all agents. Accordingly, the event-triggered control scheme is feasible.

The rest of the paper is arranged as follows: Section 2 introduces the related preliminaries: algebraic graph theory, DoS attacks, and the control objective. In Section 3, a distributed trigger-based secure control scheme is proposed along with a stability analysis. A numerical example is presented in Section 4, and conclusion is given in Section 5.

Notation. $\mathbb{R}$ represents the set of real numbers. $\mathbf{1}_N$ represents an $(N \times 1)$-dimensional vector with each element set to 1. I_N is an $(N \times N)$-dimensional identity matrix. $\mathrm{diag}\{b_1, \ldots, b_N\}$ is a diagonal matrix with $b_i, i = 1, \ldots, N$. $\lambda_i(\cdot)$, $i = 1, \ldots, N$ is an eigenvalue of a matrix with $\lambda_{\min}(\cdot)$ and $\lambda_{\max}(\cdot)$ representing the minimum and maximum eigenvalue of the matrix, respectively. For two sets Y_1 and Y_2,

$Y_1 \backslash Y_2$ represents the element set belonging to Y_1 but not to Y_2, and $|Y_1|$ is the cardinality of the set Y_1. $\|\cdot\|$ and $\otimes$ are the Euclidean norm for vectors and the Kronecker product for matrices, respectively.

2 Preliminaries

2.1 Algebraic graph theory

A time-varying undirected graph is defined as $\mathcal{G}(t) = \{\mathcal{V}, \mathcal{E}(t)\}$, where $\mathcal{V} = \{1, 2, \ldots, N\}$ represents the set of nodes and $\mathcal{E}(t) \subseteq \mathcal{V} \times \mathcal{V}$ represents the set of edges. $(j, i) \in \mathcal{E}(t)$ denotes that the node i can receive the information directly from the node j. The set of agents neighboring node i is $\mathcal{N}_i = \{j \in \mathcal{V} | (j, i) \in \mathcal{E}(t)\}$, and the adjacency matrix is $\mathcal{A}(t) = [a_{ij}(t)] \in \mathbb{R}^{N\times N}$, where $a_{ij} > 0$ is the weight of the edge (j, i). If $(j, i) \in \mathcal{E}(t)$, $a_{ij} = 1$; otherwise, $a_{ij} = 0$. To simplify the notation, we set (j, i) equal to (i, j). The in-degree matrix is defined as $\mathcal{D}(t) = \mathrm{diag}\{d_1(t), \ldots, d_N(t)\} \in \mathbb{R}^{N\times N}$, where $d_i(t) = \sum_{j\in\mathcal{N}_i} a_{ij}(t)$. We define $L(t) = \mathcal{D}(t) - \mathcal{A}(t)$ as the Laplacian matrix of $\mathcal{G}(t)$, where the Laplacian matrix $L(t)$ is a symmetric matrix in this paper. The initial graph and the initial Laplacian matrix are defined as $\mathcal{G}_0 = \{\mathcal{V}, \mathcal{E}_0\}$ and L_0, respectively, where $\mathcal{E}_0$ represents the initial set of edges.

Assumption 1. The initial graph $\mathcal{G}_0$ is undirected and connected.

Assumption 1 is commonly adopted in existing studies. The authors in [30, 33] assumed that an undirected graph is connected. Following this assumption, 0 and the vector $\mathbf{1}_N$ are a simple eigenvalue and an eigenvector of L_0, respectively, and the eigenvalues of L_0 have the property $0 = \lambda_1(L_0) < \lambda_2(L_0) < \cdots < \lambda_N(L_0)$. Therefore, the eigenvalues of $L(t)$ can be expressed as $0 = \lambda_1(L(t)) \leqslant \lambda_2(L(t)) \leqslant \cdots \leqslant \lambda_N(L(t))$.

2.2 DoS attack model

The DoS attack is an immediate security threat for the MAS, and it paralyzes the system performance by invalidating the data resources over the transmission channels, control channels, or both. In this paper, it is assumed that only the transmission channels are attacked, that is, the control scheme is not able to obtain relevant information from its neighbors. As opposed to the results in [15, 22, 23, 35], where the authors reported scenarios in which all transmission channels in the MAS are simultaneously in paralysis, we consider a case that the DoS attacks over each transmission channel are independent. This means that parts of agents can successfully exchange information with their neighbors despite DoS attacks on other channels. A description of such an attack is shown in Figure 1, and it is reasonable to assume that the links $(i, j) \in \mathcal{E}_0$ and $(j, i) \in \mathcal{E}_0$ are attacked at the same time. The scenario in which DoS attacks are simultaneously posed to all the communication links as in [15, 22, 23, 35], can be viewed as one of the special cases in this paper.

Here, we define the set of all possible attack modes as Θ. The set of time intervals for the paralyzed channels over $[t_1, t_2)$ is defined as $\Pi_{ij}(t_1, t_2)$, and the set of channels launched by the adversary with time t is $\Omega(t) = \{(i, j) \in \mathcal{E}_0 \setminus \mathcal{E}(t) | t \in \Pi_{ij}(0, \infty)\}$. Then, the Laplacian matrix of the DoS attack mode is $L_{\Omega(t)}$, and from the graph theory, the Laplacian matrix of the MAS under attack is $L_0 - L_{\Omega(t)}$.

The union of two time interval sets, where one is the set of channels subjected to the DoS attack and the other is the set of channels not subjected to the DoS attack, is described as

$$\Xi_{\Omega(t)}(t_1, t_2) = (\cap_{(i,j)\in\Omega(t)} \Pi_{ij}(t_1, t_2)) \cap (\cap_{(i,j)\notin\Omega(t)} \bar{\Pi}_{ij}(t_1, t_2)), \tag{1}$$

where $\bar{\Pi}_{ij}(t_1, t_2) = [t_1, t_2] \setminus \Pi_{ij}(t_1, t_2)$ represents the set of channels that are not subjected to the DoS attack over $[t_1, t_2)$. From (1), one has $\cup_{\Omega(t)\subseteq\mathcal{E}_0} \Xi_{\Omega(t)}(t_1, t_2) = [t_1, t_2)$, $\Pi_{ij}(t_1, t_2) = \cup_{(i,j)\in\Omega(t)\subseteq\mathcal{E}_0} \Xi_{\Omega(t)}(t_1, t_2)$.

Owing to the fact that the resources and energy of the adversary are limited, the DoS attack may be interrupted, go to sleep before the next period, and launch restricted successful attacks during a finite period. As shown in Figure 2, the m-th DoS attack time interval on channel $(i, j) \in \mathcal{E}_0$ is $h_{ij}^m = [\bar{t}_{ij}^m, \bar{t}_{ij}^m + \bar{\Delta}_{ij}^m)$, where $\bar{t}_{ij}^m$ is the instant that the DoS attack occurs and $\bar{\Delta}_{ij}^m$ is the attack duration.

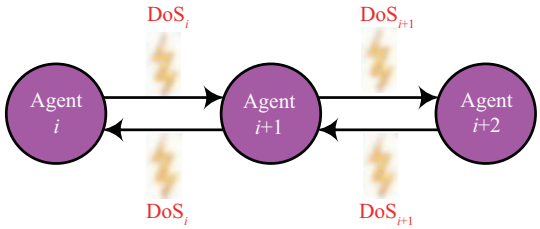

Figure 1 (Color online) A schematic of DoS attacks.

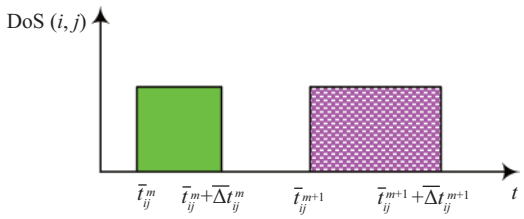

Figure 2 (Color online) Time sequences of the DoS attacks.

Assumption 2 (DoS duration)**.** For channel $(i,j)\in\mathcal{E}_0$, there exist $\Pi_{ij}^0>0$ and $0<\frac{1}{\tau_{ij}}<1$ such that

$$\mathrm{len}(\Pi_{ij}(t_1,t_2))\leqslant\Pi_{ij}^0+\frac{1}{\tau_{ij}}(t_2-t_1), \tag{2}$$

where $\mathrm{len}(\Pi_{(ij)}(t_1,t_2))$ represents the total length of time for the set of the DoS attack time intervals over $[t_1,t_2)$ and $\frac{1}{\tau_{ij}}$ denotes the magnitude of the strength of the attack.

Remark 1. Considering the fact that the number of agents in the MAS is finite and the initial communication topology is known, we can list all the DoS attack modes over the set Θ. For an MAS connected though the set of an edge $\mathcal{E}$, with the assumption that a non-DoS attack is treated as a single mode, the total number of modes is $2^{\frac{|\mathcal{E}|}{2}}$. For the set $\Omega(t)\subseteq\mathcal{E}$ at the instant t, this can also be represented by a communication topology with the adjacency matrix. Interested readers may refer to [33] for more details.

Remark 2. If the system repeatedly suffers from DoS attacks and the duration is unlimited, the control scheme will not be able to receive information from neighboring agents to achieve consensus and this may result in performance degradation for the overall system. Accordingly, an assumption concerning finite attack duration should be made, which is common in practical applications. For example, many devices have only limited resources and once the resources are exhausted, they stop working. As for $\frac{1}{\tau_{ij}}$, we discuss its influence on the control performance and present a stability analysis in Section 3, and the consensus error performance with different values of $\frac{1}{\tau_{ij}}$ is illustrated in Section 4.

2.3 Problem formulation

We consider a linear MAS composed of N identical agents, where the dynamics of the individual agent are

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

where $x_i\in\mathbb{R}^n$ is the state vector, $u_i\in\mathbb{R}^m$ is the control input, and $A\in\mathbb{R}^{n\times n}$ and $B\in\mathbb{R}^{n\times m}$ are the system matrix and the input matrix, respectively.

Assumption 3. (A,B) is stabilizable.

Remark 3. For the system (3), Assumption 3 is standard with the guarantee of the existence of a symmetric positive definite matrix that satisfies the algebraic Riccaic equation (ARE), and it can also be found in [36, 37].

The objective of this paper is to design a distributed secure control scheme using an event-triggered method, which guarantees that the MAS (3) under the DoS attack with the duration condition achieves consensus [36] such that

$$\lim_{t\to\infty}\left\|x_i(t)-\frac{1}{N}\sum_{j=1}^{N}x_j(t)\right\|=0,\quad i,j=1,2,\ldots,N,\ i\neq j, \tag{4}$$

and non-Zeno behavior is included.

3 Event-triggered secure control scheme

3.1 Secure control scheme design

For the MAS (3) under the DoS attack, the distributed event-trigger-based scheme is designed such that

$$u_i(t) = K\hat{\xi}_i(t), \tag{5}$$

where $K \in \mathbb{R}^{m\times n}$ is the feedback gain matrix, $\hat{\xi}_i(t) = \sum_{j\in\mathcal{N}_i(\mathcal{G}_0),(j,i)\notin\Omega(t)} a_{ij}(t)(\hat{x}_j(t) - \hat{x}_i(t))$, $\hat{x}_i(t) = x_i(t^i_{k_i})$, $\hat{x}_j(t) = x_j(t^j_{k_j})$, and $t^i_{k_i}$ and $t^j_{k_j}$ are the triggered instants of Agents i and j, respectively.

Remark 4. If $t^i_{k_i}$ occurs within a DoS attack interval, the real-time information of Agent i's neighbors will not be sampled. The worst part is that if all communication channels of Agent i are paralyzed, Agent i neither receives its neighbors' information nor sends its own information to nearby neighbors, and it can be viewed as $u_i(t) = 0$. This topic is addressed in [8, 30, 31], where all transmission channels in the MAS are simultaneously attacked.

The measurement error is defined as $e_i(t) = \hat{x}_i(t) - x_i(t)$. The fact that the MAS attack might cause unexpected errors results in loss of performance, and the traditional triggered design and analysis might also fail. In this paper, it is assumed that Agent i is able to evaluate the active instant $\bar{t}^m_{ij}$ of the attack from their ability to obtain their own neighbors' information. The extra error caused by the attack is denoted as $e^{\rm dos}_i = x_i(t) - x_i(\bar{t}^m_{ij})$, where $\bar{t}^m_{ij}$ is detected by Agents i and j.

The triggered instant is

$$t^i_{k_i+1} = \inf\{t > t^i_{k_i} | h_i(e_i(t), \hat{\xi}_i(t)) > 0\}, \tag{6}$$

where

$$h_i(e_i(t), \hat{\xi}_i(t)) = \|e_i(t)\|^2 - \beta_i^2(\|\hat{\xi}_i(t)\|^2 + \varpi_i(t)^2 + \psi_i(t)), \tag{7}$$

β_i is a positive constant, the decaying function $\varpi_i(t)$ is bounded satisfying $\varpi_i(t) > 0$ for $t > 0$, $\lim_{t\to\infty}\varpi_i(t) = 0$, and the extra error function $\psi_i(t) = \sum_{j\in\mathcal{N}_i(\mathcal{G}_0),(j,i)\in\Omega(t)} a_{ij}(t)\|e^{\rm dos}_i(t)\|^2$. Note that the extra error $e^{\rm dos}_i(t)$ only appears when DoS attacks occur, and $e^{\rm dos}_i(t)$ is zero when the system is not suffering from attacks. $e^{\rm dos}_i$ is constrained by the limited resources of the DoS attacks.

Remark 5. Because the triggered function is traditionally chosen as $\bar{h}_i(e_i(t), \hat{\xi}_i(t)) = \|e_i(t)\|^2 - \beta_i^2\|\hat{\xi}_i(t)\|^2$, Zeno behavior may exist in a finite time, or it can only be guaranteed that there exists at least one agent that is Zeno-free; however, it cannot be guaranteed that all agents are Zeno-free. Inspired by [38, 39], a decaying function $\varpi_i(t)$ is employed in (7) to avoid the occurrence of Zeno behavior. To rule out Zeno behavior, $\varpi_i(t)$ is a bounded and decreasing function whose value is larger than zero and approaches zero only when $t \to \infty$. We show the comparison of the number of triggered events, maximum inter-event time, and minimum inter-event time with and without $\varpi_i(t)$ in Section 4.

Remark 6. Owing to the presence of DoS attacks, Agent i cannot obtain information from its neighboring Agent j when the communication link between Agents i and j is attacked. With the data loss experienced by Agent i, the value of its triggered condition might change significantly, and the triggered number of Agent i might increase drastically. This would lead to unnecessary triggered instants or Zeno behavior. The authors in [8, 9, 30, 31] discussed the impact of attacks on triggered functions and design time-triggered schemes for the system under DoS attacks. However, the triggered instant is not determined according to the state of the system, and it may also result in unnecessary triggered events. Therefore, an extra error function $\psi_i(t)$ in the event-triggered function is introduced to indicate the impact of the DoS attacks, and the triggered instants are determined by the states of the system and the extra errors. The comparison results of the triggered function with and without $\psi_i(t)$ are shown in Section 4. Additionally, because the duration of each attack is bounded and the energy of the attack is limited, the extra error is also constrained.

3.2 Stability analysis

Define $x(t) = [x_1(t), x_2(t), \ldots, x_N(t)]^{\mathrm{T}}$, $\hat{x}(t) = [\hat{x}_1(t), \hat{x}_2(t), \ldots, \hat{x}_N(t)]^{\mathrm{T}}$. It follows from (3) and (5) that

$$\dot{x}(t) = \left[I_N \otimes A - \left((L_0 - L_{\Omega(t)}) \otimes BK\right)\right] x(t) - \left((L_0 - L_{\Omega(t)}) \otimes BK\right) e(t). \tag{8}$$

Define an error vector

$$\delta_i(t) = x_i(t) - \bar{x}(t), \tag{9}$$

where $\bar{x}(t) = \frac{1}{N}\sum_{i=1}^{N} x_i(t)$ is the average state of the MAS. In addition,

$$\delta(t) = (M \otimes I_n)x(t), \tag{10}$$

where $M = I_N - \frac{\mathbf{1}_N \mathbf{1}_N^{\mathrm{T}}}{N}$, and $\delta(t) = [\delta_1(t), \delta_2(t), \ldots, \delta_N(t)]^{\mathrm{T}}$. From the definition of $\delta(t)$, it is easy to obtain $(\mathbf{1}_N \otimes I_n)\delta(t) = 0$. Defining $\Psi = [\frac{\mathbf{1}_N}{\sqrt{N}}, \nu(t)] \in \mathbb{R}^{N\times N}$, and $\nu(t) = [v_2(t), v_3(t), \ldots, v_N(t)]$ and letting $v_i(t)$ denote the corresponding eigenvector of $\lambda_i(t)$, $i = 2, 3, \ldots, N$, the following properties hold in the Laplacian matrix of the initial communication topology:

$$\Psi\Psi^{\mathrm{T}} = \Psi^{\mathrm{T}}\Psi = I_N, \quad \Psi^{\mathrm{T}} L(t) \Psi = \mathrm{diag}\{0, \lambda_2(t), \ldots, \lambda_N(t)\},$$

$$\Psi^{\mathrm{T}} L_{\Omega(t)} \Psi = \mathrm{diag}\{0, \nu^{\mathrm{T}} L_{\Omega(t)} \nu\}, \quad L_0 - L_{\Omega(t)} \geqslant 0,$$

and

$$ML(t) = L(t)M = L(t), \quad ML_{\Omega(t)} = L_{\Omega(t)}M = L_{\Omega(t)}. \tag{11}$$

Then, combining (8) with (10) and (11) yields $\dot{\delta}(t) = [I_N \otimes A - ((L_0 - L_{\Omega(t)}) \otimes BK)]\delta(t) - ((L_0 - L_{\Omega(t)}) \otimes BK)e(t)$.

In this paper, the following symmetric and positive definite matrices R, Q and P are involved in our main result and their relationship is described by the following ARE:

$$A^{\mathrm{T}}P + PA - PBR^{-1}B^{\mathrm{T}}P + Q = 0. \tag{12}$$

Let $k_0 = \|PBK\|$, $\bar{\lambda} = \max\{\lambda_{\max}(L_0 - L_\theta), \theta \subseteq \Theta\}$, $\underline{\lambda} = \min\{\lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_\theta}) | \lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_\theta}) > 0, \theta \subseteq \Theta\}$, $w = \bar{\lambda}^2$, and $\underline{\lambda} = \min\{\lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_\theta}) | \lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_\theta}) > 0, \theta \subseteq \Theta\}$, where

$$\Lambda_{L_0} = \begin{bmatrix} \lambda_2(L_0) & 0 & \cdots & 0 \\ 0 & \lambda_3(L_0) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_N(L_0) \end{bmatrix} \quad \text{and} \quad \Lambda_{L_\theta} = \begin{bmatrix} \lambda_2(L_\theta) & 0 & \cdots & 0 \\ 0 & \lambda_3(L_\theta) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_N(L_\theta) \end{bmatrix}.$$

The main result of this paper is presented below.

Theorem 1. Consider an MAS (3) with Assumptions 1 and 3 and bounded initial conditions. There exist scalars θ_1^{ij} and θ_2^{ij} satisfying

$$\alpha_{\Omega(t)} - \left(\sum_{(i,j)\in\Omega(t)} \theta_1^{ij} + \sum_{(i,j)\in\mathcal{E}_0\setminus\Omega(t)} \theta_2^{ij} \right) \leqslant 0, \tag{13}$$

$$\bar{\tau} = \sum_{(i,j)\in\mathcal{E}_0} \left[\frac{\theta_1^{ij}}{\tau_{ij}} + \left(1 - \frac{1}{\tau_{ij}}\right) \theta_2^{ij} \right] < 0, \tag{14}$$

and

$$\theta_1^{ij} - \theta_2^{ij} \geqslant 0. \tag{15}$$

Then, under the control scheme (5) and triggered instant scheduling (6) with $K = \mu R^{-1}B^{\mathrm{T}}P$, $\mu \geqslant \frac{1}{2\underline{\lambda}}$, $\beta_{\max}^2 \leqslant \frac{\frac{3}{4}\lambda_{\min}^2(Q)}{\frac{3}{2}\lambda_{\min}^2(Q)\lambda^2+8k_0^2\lambda^4}$, and $\beta_{\max}^2 < \frac{1}{2\lambda^2}$, the MAS (3) suffering a DoS attack satisfying Assumption 2 can reach a consensus (4).

Proof. Consider the following Lyapunov function:

$$V = \delta^{\mathrm{T}}(t)\left(I_N \otimes P\right)\delta(t), \tag{16}$$

and the derivative of (16) yields

$$\begin{aligned}\dot{V} &= \dot{\delta}^{\mathrm{T}}(t)(I_N \otimes P)\delta(t) + \delta^{\mathrm{T}}(t)(I_N \otimes P)\dot{\delta}(t)\\ &= \dot{V}_1(t) + \dot{V}_2(t),\end{aligned} \tag{17}$$

where $\dot{V}_1(t) = \delta^{\mathrm{T}}(t)[I_N \otimes (A^{\mathrm{T}}P + PA) - 2(L_0 - L_{\Omega(t)}) \otimes PBK]\delta(t)$ and $\dot{V}_2(t) = -2\delta(t)[(L_0 - L_{\Omega(t)}) \otimes PBK]e(t)$. Defining $\widetilde{\delta} = \left(\Psi^{\mathrm{T}} \otimes I_n\right)\delta$, we can obtain $\widetilde{\delta}_1(\frac{\mathbf{1}_N^{\mathrm{T}}}{\sqrt{N}} \otimes I_n) = 0$ from $(\mathbf{1}_N \otimes I_n) = 0$.

For the stability analysis, the following three cases are discussed according to different attack modes. The first and second cases are scenarios in which the transmission channels remain connected or partly disconnected under the DoS attack. In the third case, we assume that all transmission channels are paralyzed.

(1) When $\lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_{\Omega(t)}}) \neq 0$, the communication topology under the DoS attack remains connected. Note that it involves the situation where the system without attacks recovers to the initial topology. From Assumption 1, we have

$$\begin{aligned}\dot{V}_1(t) &= \widetilde{\delta}^{\mathrm{T}}(t)(I_N \otimes (A^{\mathrm{T}}P + PA))\widetilde{\delta}(t) - 2\widetilde{\delta}^{\mathrm{T}}(t)(\Psi^{\mathrm{T}}(L_0 - L_{\Omega(t)})\Psi \otimes PBK)\widetilde{\delta}(t)\\ &\leqslant \widetilde{\delta}_{2:N}^{\mathrm{T}}(t)(I_{N-1} \otimes (A^{\mathrm{T}}P + PA))\widetilde{\delta}_{2:N}(t) - 2\widetilde{\delta}_{2:N}^{\mathrm{T}}(t)\underline{\lambda} \cdot (I_{N-1} \otimes PBK)\widetilde{\delta}_{2:N}(t),\end{aligned} \tag{18}$$

where $\widetilde{\delta}_{2:N} = [\widetilde{\delta}_2, \widetilde{\delta}_3, \ldots, \widetilde{\delta}_N]^{\mathrm{T}}$.

Using Assumption 3, we can obtain P from (12). Then, taking $K = \mu R^{-1}B^{\mathrm{T}}P$ with $\mu \geqslant \frac{1}{2\underline{\lambda}}$ into account, as well as (18), we have

$$\begin{aligned}\dot{V}_1(t) &\leqslant \widetilde{\delta}_i^{\mathrm{T}}(t)\left(I_{N-1} \otimes (A^{\mathrm{T}}P + PA - PBR^{-1}B^{\mathrm{T}}P)\right)\widetilde{\delta}_i(t)\\ &= \sum_{i=2}^{N}\widetilde{\delta}_i^{\mathrm{T}}(t)\left(A^{\mathrm{T}}P + PA - PBR^{-1}B^{\mathrm{T}}P\right)\widetilde{\delta}_i(t).\end{aligned} \tag{19}$$

According to the definition of $\widetilde{\delta}$, it yields $\dot{V}_2(t) = -2\widetilde{\delta}^{\mathrm{T}}[\Psi^{\mathrm{T}}(L_0 - L_{\Omega(t)})\Psi \otimes PBK](\Psi^{\mathrm{T}} \otimes I_n)e(t)$. Because of $\widetilde{\delta}_1(t) = 0$ and letting $\widetilde{e}_{2:N}(t) = (\nu^{\mathrm{T}} \otimes I_n)e_{2:N}(t)$, one finds that

$$\dot{V}_2(t) \leqslant 2\|[\nu^{\mathrm{T}}(L_0 - L_{\Omega(t)})\nu \otimes PBK]\|\|\widetilde{\delta}_{2:N}^{\mathrm{T}}\|\|\widetilde{e}_{2:N}\|.$$

With the inequality $xy \leqslant \frac{\rho}{2}x^2 + \frac{1}{2\rho}y^2$ with $0 < \rho < \frac{\lambda_{\min}(Q)}{k_0 w}$, we have

$$\begin{aligned}\dot{V}_2(t) &\leqslant 2\|PBK\|\sum_{i=2}^{N}\left(\lambda_N^2(L_0 - L_{\Omega(t)})\frac{1}{2\rho}\widetilde{\delta}_i^{\mathrm{T}}\widetilde{\delta}_i + \frac{1}{2\rho}\widetilde{e}_i^{\mathrm{T}}\widetilde{e}_i\right)\\ &\leqslant k_0\sum_{i=2}^{N}\left(w\rho\widetilde{\delta}_i^{\mathrm{T}}\widetilde{\delta}_i + \frac{1}{\rho}\widetilde{e}_i^{\mathrm{T}}\widetilde{e}_i\right).\end{aligned} \tag{20}$$

Using (12), (19) and (20), Eq. (17) can be written as

$$\dot{V} \leqslant -\sum_{i=2}^{N}\widetilde{\delta}_i^{\mathrm{T}}Q\widetilde{\delta}_i + k_0\sum_{i=2}^{N}\left(w\rho\widetilde{\delta}_i^{\mathrm{T}}\widetilde{\delta}_i + \frac{1}{\rho}\widetilde{e}_i^{\mathrm{T}}\widetilde{e}_i\right)$$

$$\leqslant (k_0 w\rho - \lambda_{\min}(Q)) \sum_{i=1}^{N} \delta_i^{\mathrm{T}} \delta_i + \frac{k_0}{\rho} \sum_{i=1}^{N} e_i^{\mathrm{T}} e_i. \tag{21}$$

Define $\xi_i(t) = \sum_{j\in\mathcal{N}_i(\mathcal{G}_0),(j,i)\notin\Omega(t)} a_{ij}(t)(x_j(t) - x_i(t))$, $t \in [t^i_{k_i}, t^i_{k_i+1}]$, and in stack forms this results in $\xi(t) = -((L_0 - L_{\Omega(t)}) \otimes I_n)x$ and $\hat{\xi}(t) = -((L_0 - L_{\Omega(t)}) \otimes I_n)(x + e)$. Then, it follows from (9) that

$$\begin{aligned} \|\hat{\xi}(t)\| &= \| - ((L_0 - L_{\Omega(t)}) \otimes I_n)(x + e)\| \\ &\leqslant \|\xi\| + \|((L_0 - L_{\Omega(t)}) \otimes I_n)e\| \leqslant \|\xi\| + \bar{\lambda}\|e\|. \end{aligned} \tag{22}$$

According to $(L_0 - L_{\Omega(t)})(L_0 - L_{\Omega(t)}) = (L_0 - L_{\Omega(t)})MM(L_0 - L_{\Omega(t)})$, one has

$$\|\xi\|^2 = x^{\mathrm{T}}((L_0 - L_{\Omega(t)}) \otimes I_n)((L_0 - L_{\Omega(t)}) \otimes I_n)x \leqslant \bar{\lambda}^2\|\delta\|^2. \tag{23}$$

Then, Eqs. (22) and (23) yield

$$\|\hat{\xi}(t)\| \leqslant \bar{\lambda}\|\delta\| + \bar{\lambda}\|e\|. \tag{24}$$

According to the triggered condition (6), during the triggered interval, one has

$$\|e(t)\|^2 \leqslant \beta_{\max}^2\|\hat{\xi}(t)\| + \|\bar{w}(t)\|^2 + \sum_{i=1}^{N} \psi_i(t), \tag{25}$$

where $\beta_{\max} = \max\{\beta_i, i = 1, \ldots, N\}$, $\hat{\xi}(t) = [\xi_1(t), \xi_2(t), \ldots, \xi_N(t)]^{\mathrm{T}}$, and $\varpi(t) = [\varpi_1(t), \varpi_2(t), \ldots, \varpi_N(t)]^{\mathrm{T}}$. Combining (24) with (25) yields

$$\|e\|^2 \leqslant \frac{1 - \sigma_{\max}}{\sigma_{\max}}\|\delta\|^2 + \frac{\beta_{\max}^2}{\sigma_{\max}} \left(\|\bar{w}(t)\|^2 + \sum_{i=1}^{N} \psi_i(t) \right), \tag{26}$$

where $0 < \sigma_{\max} = 1 - 2\beta_{\max}^2\bar{\lambda}^2 < 1$. Incorporating (26) into (21), we have

$$\dot{V}(t) \leqslant \alpha_1 V(t) + \varphi(t) + \phi(t), \tag{27}$$

where $\alpha_1 = -(\frac{3}{4}\lambda_{\min}(Q) - \varrho(1 - \sigma_{\max}))/\lambda_{\max}(P)$ and $\varphi(t) = \varrho\beta_{\max}^2 \sum_{i=1}^{N} \varpi_i^2(t)$, $\phi(t) = \varrho\beta_{\max}^2 \sum_{i=1}^{N} \psi_i(t)$, and $\varrho = \frac{4k_0^2\bar{\lambda}^2}{\lambda_{\min}(Q)\sigma_{\max}}$.

(2) When $\lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_{\Omega(t)}}) = 0$, the communication topology under the DoS attack is not connected. From (18), we know that $\dot{V}_1(t) \leqslant \widetilde{\delta}_{2:N}^{\mathrm{T}}(t)(I_{N-1} \otimes (A^{\mathrm{T}}P + PA))\widetilde{\delta}_{2:N}^{\mathrm{T}}(t)$. Further, if there exists $\widetilde{\alpha}_2 > 0$ such that $PA + A^{\mathrm{T}}P - \widetilde{\alpha}_2 P < 0$, one has

$$\dot{V}_1(t) \leqslant \widetilde{\alpha}_2\lambda_{\max}(P) \sum_{i=2}^{N} \widetilde{\delta}_i^{\mathrm{T}}\widetilde{\delta}_i. \tag{28}$$

It follows, from (20), (26) and (28), that

$$\dot{V}(t) \leqslant \alpha_2 V(t) + \varphi(t) + \phi(t), \tag{29}$$

where $\alpha_2 = [\frac{\lambda_{\min}(Q)}{4} + \widetilde{\alpha}_2\lambda_{\max}(P) + \varrho(1 - \sigma_{\max})]/\lambda_{\max}(P)$, and $\varphi(t)$ and $\phi(t)$ are defined in (27).

(3) For $L_\Omega = L$, all the communication links are attacked. From $\dot{\delta}(t) = (I_N \otimes A)\delta(t)$ and using $PA + A^{\mathrm{T}}P - \alpha_3 P < 0$, we can obtain the time derivative of (16):

$$\dot{V} = \delta^T(t) \left[I_N \otimes (PA + A^{\mathrm{T}}P) \right] \delta(t) \leqslant \alpha_3 V(t) + \varphi(t) + \phi(t), \tag{30}$$

where $\varphi(t)$ and $\phi(t)$ are presented in (27).

In summary, from the above three cases and the results of (27), (29) and (30), one has

$$\dot{V} \leqslant \alpha_{\Omega(t)} V(t) + \varphi(t) + \phi(t), \tag{31}$$

where the decay rates

$$\alpha_{\Omega(t)}=\begin{cases}\alpha_1, & \text{if } L_{\Omega(t)}\neq L_0,\ \lambda_{\min}(\Lambda_{L_0}-\Lambda_{L_\Omega})\neq 0,\\ \alpha_2, & \text{if } L_{\Omega(t)}\neq L_0,\ \lambda_{\min}(\Lambda_{L_0}-\Lambda_{L_\Omega})=0,\\ \alpha_3, & \text{if } L_{\Omega(t)}=L_0.\end{cases}$$

Define ξ_k as the instant when the DoS attack changes from one mode to another. For $t\in[\xi_k,\xi_{k+1})$ and using the iterative method, Eq. (31) yields

$$\begin{aligned}V(t)\ &\leqslant \exp(\alpha_{\Omega(\xi_k)}(t-\xi_k))V(\xi_k)+\int_{\xi_k}^{t}\exp(\alpha_{\Omega(\xi_k)}(t-s))\varphi(s)\mathrm{d}s+\int_{\xi_k}^{t}\exp(\alpha_{\Omega(\xi_k)}(t-s))\phi(s)\mathrm{d}s\\ &\leqslant \exp(D_k(t,1))V(0)+\exp\left(D_k(t,2)\right)\int_{\xi_0}^{\xi_1}\exp(\alpha_{\Omega(\xi_0)}(\xi_1-s))\varphi(s)\mathrm{d}s\\ &\quad+\cdots+\exp(D_k(t,k+1))\int_{\xi_{k-1}}^{\xi_k}\exp(\alpha_{\Omega(\xi_{k-1})}(\xi_k-s))\varphi(s)\mathrm{d}s\\ &\quad+\int_{\xi_k}^{t}\exp(\alpha_{\Omega(\xi_k)}(t-s))\varphi(s)\mathrm{d}s+\int_{\xi_k}^{t}\exp(\alpha_{\Omega(\xi_k)}(t-s))\phi(s)\mathrm{d}s\\ &\leqslant \exp(\bar{D}(0,t))V(0)+\int_{\xi_0}^{t}\exp(\bar{D}(s,t))\varphi(s)\mathrm{d}s+\int_{\xi_k}^{t}\exp(\alpha_{\Omega(\xi_k)}(t-s))\phi(s)\mathrm{d}s,\end{aligned}$$

where $D_k(t,r)=\alpha_{\Omega(\xi_k)}(t-\xi_k)+\sum_{m=r}^{k}\alpha_{\Omega(\xi_{m-1})}(\xi_m-\xi_{m-1})$ and $\bar{D}(s,t)=\sum_{\Omega(t)\subseteq\mathcal{E}_0}\alpha_{\Omega(t)}\mathrm{len}(\Xi_{\Omega(s,t)})$. From (13), we can deduce that

$$\begin{aligned}\bar{D}(s,t)\ &\leqslant \sum_{\Omega\subseteq\mathcal{E}_0}\left(\sum_{(i,j)\in\Omega(t)}\theta_1^{ij}+\sum_{(i,j)\in\mathcal{E}_0\setminus\Omega(t)}\theta_2^{ij}\right)\mathrm{len}(\Xi_{\Omega(t)}(s,t))\\ &=\sum_{(i,j)\in\mathcal{E}_0}\Big[\left(\theta_1^{ij}-\theta_2^{ij}\right)\mathrm{len}(\Pi_{ij}(s,t))+\theta_2^{ij}(t-s)\Big],\end{aligned}\tag{32}$$

where

$$\mathrm{len}(\Pi_{ij}(s,t))=\sum_{\Omega(t)\subseteq\mathcal{E}_0,(i,j)\in\Omega(t)}\mathrm{len}(\Xi_{\Omega(t)}(s,t)).$$

With Assumption 2 and according to (2), (14), and (32), Eq. (31) can be converted to

$$V(t)\leqslant\exp\left(\bar{\tau}t+\bar{\Pi}^0\right)V(0)+\int_{\xi_0}^{t}\exp(\bar{\tau}(t-s)+\bar{\Pi}^0)\varphi(s)\mathrm{d}s+\int_{\xi_k}^{t}\exp(\alpha_{\Omega(\xi_k)}(t-s))\phi(s)\mathrm{d}s,\tag{33}$$

where $\bar{\Pi}^0=\sum_{(i,j)\in\mathcal{E}_0}(\theta_1^{ij}-\theta_2^{ij})\Pi_{ij}^0$. Because the energy of the adversary is limited, $\varphi(t)$ and $\phi(t)$ are bounded. Therefore, V is bounded, which implies that $x_i(t),i=1,2,3$ are bounded.

In the following part, we analyze the Zeno behavior, which is defined in the limited time [38], under the proposed secure control scheme. A conservative triggered condition can be set such that

$$\|e_i(t)\|^2\leqslant(\omega_k^i)^2\tag{34}$$

for (7), where $\omega_k^i=\|\varpi_i'(t_{k_i}^i)\|$ and $\varpi_i'(t)$ is a bounded decreasing function with a faster decay rate than $\varpi_i(t)$. Then, during $[t_{k_i}^i,t_{k_i+1}^i)$, the derivative of $\|e_i(t)\|$ is

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\|e_i(t)\|\ &\leqslant\frac{\|e_i^{\mathrm{T}}(t)\|}{\|e_i(t)\|}\|\dot{e}_i(t)\|\\ &\leqslant\|A\|\|e_i(t)\|+\|Ax_i(t_{k_i}^i)\\ &\quad+BK\sum_{j\in\mathcal{N}_i(\mathcal{G}),(j,i)\notin\Omega(t)}a_{ij}(t)(x_j(t_{k_j}^j)-x_i(t_{k_i}^i))\|\leqslant\|A\|\|e_i(t)\|+\alpha_k^i,\end{aligned}$$

where

$$\alpha_k^i = \max_{t\in[t_{k_i}^i, t_{k_i+1}^i)} \|Ax_i(t_{k_i}^i) + BK\sum\nolimits_{j\in\mathcal{N}_i(\mathcal{G}_0),(j,i)\notin\Omega(t)} a_{ij}(t)(x_j(t_{k_j}^j) - x_i(t_{k_i}^i))\|.$$

Further, one has $\|e_i(t)\| \leqslant \frac{\alpha_k^i}{\|A\|}\left(\exp(\|A\|(t-t_{k_i}^i))-1\right)$, and, with (34), it yields $\|e_i(t_{k_i+1}^i)\| = \omega_k^i \leqslant \frac{\alpha_k^i}{\|A\|}(\exp(t_{k_i+1}^i - t_{k_i}^i) - 1)$. Then, it follows that $t_{k_i+1}^i - t_{k_i}^i \geqslant \frac{1}{\|A\|}\ln(\frac{\|A\|\omega_k^i}{\alpha_k^i}+1)$. Because $\omega_k^i > 0$ and $\alpha_k^i > 0$, we obtain $t_{k_i+1}^i - t_{k_i}^i > 0$. Therefore, it is proved that Zeno behavior can be excluded under the proposed secure control scheme.

For $t \in [0,\infty)$, we can conclude that the control scheme (5) with (6) guarantees that Eq. (33) holds for all agents. Further, owing to $\bar{\tau} < 0$ and the properties of $\varphi(t)$ and $\phi(t)$, we can obtain $V(t) \to 0$ as $t \to \infty$. Because $V = \delta^{\mathrm{T}}(t)(I_N \otimes P)\delta(t) \geqslant \delta^{\mathrm{T}}(t)\lambda_{\min}(P)\delta(t) = \lambda_{\min}(P)\|\delta\|^2$ and $\lim_{t\to\infty} V(t) \to 0$, we obtain the result $\lim_{t\to\infty}\|\delta(t)\| \to 0$ and then $\lim_{t\to\infty}\|\delta_i(t)\| \to 0$. By virtue of Assumption 1, all agents converge to $\frac{1}{N}\sum_{j=1}^N x_j(t)$ and therefore, Eq. (4) holds. This completes the proof of the theorem.

For a special case, if we choose $\varpi_i(t)$ to be an exponentially decaying function for each agent, the exponential convergence can be obtained through the following corollary.

Corollary 1. If an exponential convergence function is chosen for each agent's $\varpi_i(t)$, that is, if $\varpi_i(t) = b_i\exp(-a_i t)$, where a_i and b_i are positive constants, the convergence rate is exponential.

Proof. Choosing an exponential convergence function $\varpi_i(t) = b_i\exp(-a_i t)$ for each agent, we have $\sum_{i=1}^N \varpi_i^2(t) \leqslant \mathcal{B}\exp(-\mathcal{H}t)$, $i = 1,\ldots,N$, where $\mathcal{B}$ and $\mathcal{H}$ are positive constants. Then, the following inequalities can be obtained directly from Theorem 1:

$$\begin{aligned} V(t) \leqslant{}& \exp\left(\bar{\tau}t + \bar{\Pi}^0\right)V(0) + \varrho\beta_{\max}^2\int_{\xi_0}^t \exp(\bar{\tau}(t-s)+\bar{\Pi}^0)\mathcal{B}\exp(-\mathcal{H}s)\mathrm{d}s \\ &+\varrho\beta_{\max}^2\int_{\xi_k}^t \exp(\alpha_{\Omega(\xi_k)}(t-s))\phi(s)\mathrm{d}s. \end{aligned}$$

By integrating the above inequalities, we find

$$V(t) \leqslant \begin{cases} \exp(\bar{\tau}t+\bar{\Pi}^0)V(0) + \varrho\beta_{\max}^2\mathcal{B}\exp(\bar{\tau}t+\bar{\Pi}^0) \\ \quad +\varrho\beta_{\max}^2\int_{\xi_k}^t \exp(\alpha_{\Omega(\xi_k)}(t-s))\phi(s)\mathrm{d}s, \quad \text{when } \mathcal{H} = -\bar{\tau}, \\ \exp(\bar{\tau}t+\bar{\Pi}^0)V(0) - \frac{\varrho\beta_{\max}^2\mathcal{B}\exp(\bar{\tau}t+\bar{\Pi}^0)}{\bar{\tau}+\mathcal{H}}\exp(-\mathcal{H}t+\bar{\Pi}^0 - \exp(\bar{\tau}t+\bar{\Pi}^0-(\mathcal{H}+\bar{\tau})\xi_0)) \\ \quad +\varrho\beta_{\max}^2\int_{\xi_k}^t \exp(\alpha_{\Omega(\xi_k)}(t-s))\phi(s)\mathrm{d}s, \quad \text{when } \mathcal{H} \neq -\bar{\tau}. \end{cases} \tag{35}$$

If the performance loss caused by the DoS attacks is not taken into account, that is, if the last term disappears in (35), it is easy to find that V converges exponentially to 0 using (16) and (35). This means that $\delta \to 0$ in an exponential manner and that the convergence rate of each agent's consensus is exponential.

Remark 7. As for $\alpha_{\Omega(t)}$ in (31), it is a positive or negative constant depending on the different DoS attack modes. This poses a difficulty for the stability analysis of the system. To solve this problem, we introduce a set of equivalent parameters θ_1^{ij} and θ_2^{ij} following [33, 34], where θ_1^{ij} corresponds to the link $(i,j) \in \mathcal{E}_0$ being attacked and θ_2^{ij} corresponds to the link $(i,j) \in \mathcal{E}_0$ not being attacked. The two parameters are used to distinguish whether the channel $(i,j) \in \mathcal{E}_0$ is under the attack.

Remark 8. In this paper, the duration of the DoS attack is not arbitrary, and the distributed secure control scheme is against the specific DoS attack under certain conditions. The strength of the attack $\frac{1}{\tau_{ij}}$ in (2) should satisfy the conditions of (13) with suitable choices of the scalars θ_1^{ij} and θ_2^{ij}. More details concerning the DoS duration are shown in Section 4.

Remark 9. The decaying function $\varpi_i(t)$ in (7) is an additional term implemented to avoid the occurrence of Zeno behavior. The inter-event time will be longer than that in the traditional one. If the extra term $\varpi_i(t)$ converges slowly enough, the impact of the DoS attack on the Zeno behavior of the event-triggered scheme will be alleviated. In general, it is required that the function $\varpi_i(t)$ satisfies $\varpi_i(t) > 0$, $\mathrm{d}\varpi_i(t)/\mathrm{d}t < 0$ and $\lim_{t\to\infty}\varpi_i(t) \to 0$. For example, $\varpi_i(t) = \frac{1}{1+t}$ or $\varpi_i(t) = b_i\exp(-a_i t)$, where a_i and

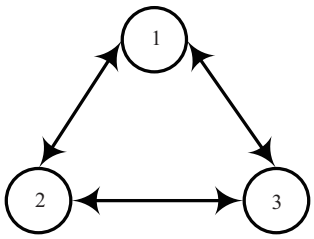

Figure 3 Communication graph.

Table 1 Decay rates α_Ω under different attack conditions

Attack condition	Algebra condition	α_Ω
$\lvert\Omega\rvert = 0, 1$	$L_\Omega \neq L$, $\lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_\Omega}) \neq 0$	-0.141
$\lvert\Omega\rvert = 2$	$L_\Omega \neq L$, $\lambda_{\min}(\Lambda_{L_0} - \Lambda_{L_\Omega}) = 0$	0.407
$\lvert\Omega\rvert = 3$	$L_\Omega = L$	0.46

b_i are positive constants. To compromise between the Zeno-free behavior and the system performance, an exponential convergence function $\varpi_i(t) = b_i \exp(-a_i t)$ can be chosen for each agent.

4 Simulation

Here, we choose an MAS consisting of three agents in $\mathbb{R}^2$. The communication topology is shown in Figure 3, and the dynamics of the agents are

$$\dot{x}_i(t) = \begin{bmatrix} 0 & -0.3 \\ 0.4 & 0 \end{bmatrix} x_i(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_i(t), \quad i = 1, 2, 3,$$

where $x_i(t) = [x_{i,1}(t), x_{i,2}(t)]^{\mathrm{T}}$ and $u_i(t)$ is the control input. The initial states are $x_1(0) = [1, 2]^{\mathrm{T}}$, $x_2(0) = [-1, -2]^{\mathrm{T}}$, and $x_3(0) = [4, 4.5]^{\mathrm{T}}$. There are eight possible attack modes in total: $\Theta = \{\emptyset, \{(1,2)\}, \{(1,3)\}, \{(2,3)\}, \{(1,2)(2,3)\}, \{(1,2)(1,3)\}, \{(1,3)(2,3)\}, \{(1,2)(1,3)(2,3)\}\}$. The strength of the DoS attack, $\frac{1}{\tau_{ij}}$, $i, j = 1, 2, 3, i \neq j$, is set to 0.2 for each communication channel in our simulation; this implies that the DoS attack duration is less than 6 s if the simulation time is set to 30 s. The set of channel-attacked instants is denoted as $\Omega \subseteq \Theta$, and $\underline{\lambda} = 1$ and $\bar{\lambda} = 3$. We choose $\mu = 0.6$ and $K = [-0.4062, 0.7115]$ with $R = 1$ and $Q = I_2$. According to a large number of simulations assessing the choice of $\varpi_i(t)$, the exponential function for all agents can have better control performance and smaller consensus error; therefore, we choose $\beta_i = \sqrt{0.02}$ and $\varpi_i(t) = \exp(-0.1t)$, $i = 1, 2, 3$ in the triggered functions. We can obtain the decay rates α_Ω, shown in Table 1, under different attack conditions according to the stability analysis. It is seen that as the number of links under the DoS attack increases the decay rates α_Ω increase gradually with fewer information interactions between agents. We choose $\theta_1^{ij} = 0.16$ and $\theta_2^{ij} = -0.045$.

The DoS attack signal is shown in Figure 4, where 1 indicates that the channel $(i, j) \in \mathcal{E}_0$ is under attack and 0 indicates that the system is not under attack. Figures 5 and 6 show the state x_i of the system and the control input u_i, respectively, for $i = 1, 2, 3$. In Figure 6, we can see that u_1, u_2, and u_3 approach zero when all the communication channels of the MAS suffer DoS attacks. Figure 7 shows the triggered instances. The performance comparison, including the triggered number, maximum inter-event time, and minimum inter-event time is recorded in Table 2 [27, 28, 35, 38–42]. Table 2 shows that the designed event-triggered function can guarantee that each agent exhibits Zeno-free behavior and works in a normal triggered manner. If $\varpi_i(t)$ is not considered in the triggered function, the minimum inter-event time equals to the accuracy of the simulation and there will be more triggered number. $\psi_i(t)$ reflects the impact of the attack on the triggered function and the number of triggers owing to the extra error, and it also avoids unnecessary triggers. Figure 8 shows the relationship between the triggered function and the measurement error of Agent 1; the threshold jitters are caused by the extra errors in the presence of the

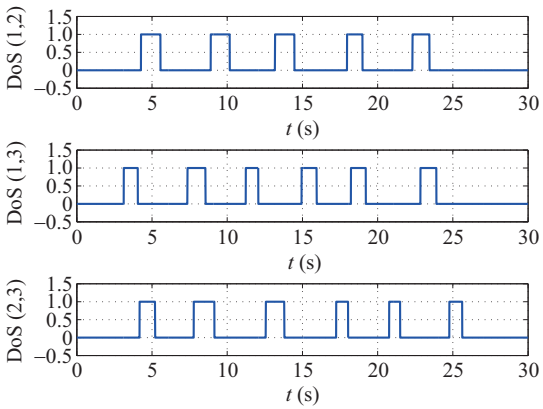

Figure 4 (Color online) DoS attacks.

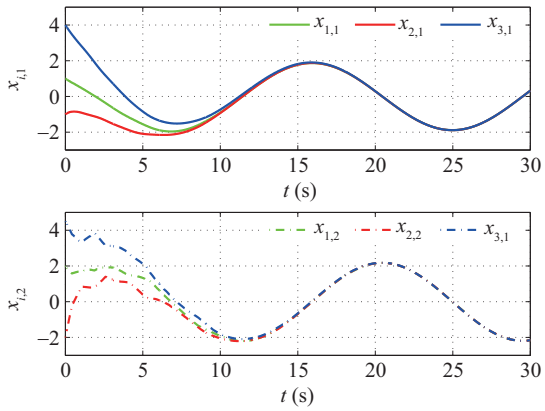

Figure 5 (Color online) Internal states $x_{i,j}$, $i = 1, 2, 3$ and $j = 1, 2$.

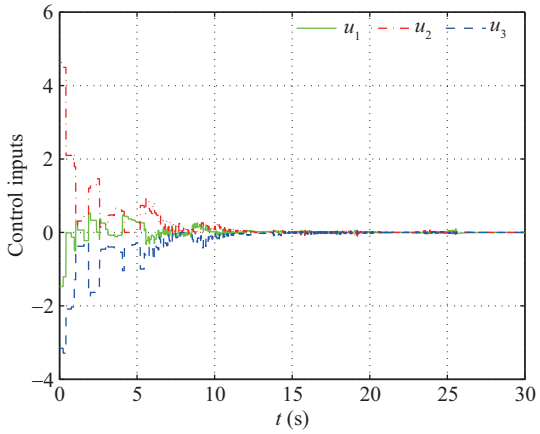

Figure 6 (Color online) Control inputs u_i, $i = 1, 2, 3$.

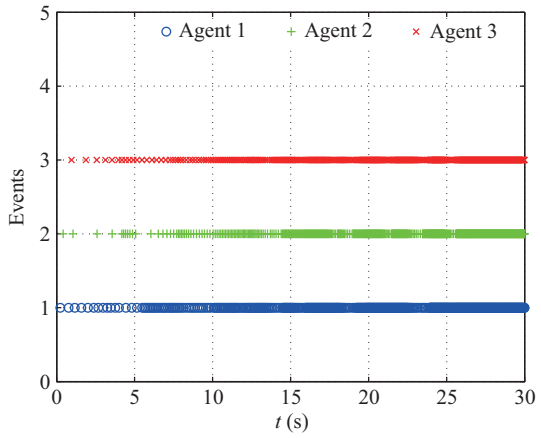

Figure 7 (Color online) Triggered events.

Table 2 Performance comparison for different triggered functions

Function	Control scheme	Updated numbers of agents			Minimum inter-event time	Maximum inter-event time
		1	2	3		
[27, 28, 40–42]	$\varpi_i(t) = 0, \psi_i(t) = 0$	1822	1899	1643	0.01	1.49
[38, 39]	$\varpi_i(t) \neq 0, \psi_i(t) = 0$	709	688	676	0.02	1.54
[35]	$\varpi_i(t) = 0, \psi_i(t) \neq 0$	1364	1271	1122	0.01	1.49
Our paper	$\varpi_i(t) \neq 0, \psi_i(t) \neq 0$	611	570	560	0.02	1.54

attacks. The consensus error is defined as $E_\delta(t) = \sqrt{\sum_{i=1}^{N} \delta_i^{\mathrm{T}}(t)\delta_i(t)}$, and a comparison of the consensus errors for different magnitudes of DoS attack strengths, such as $\frac{1}{\tau_{ij}} = 0.2$, $\frac{1}{\tau_{ij}} = 0.5$, and $\frac{1}{\tau_{ij}} = 1$, is shown in Figure 9. Greater attack strengths result in larger consensus errors. However, if the attack constantly occurs, the system will not be able to achieve consensus, resulting in an undesirable control performance.

5 Conclusion

In this paper, the event-trigger-based consensus secure control problem was discussed for linear MAS under DoS attacks. The transmission channels were paralyzed by independent aperiodic and unknown DoS attacks and the decay rates under different attack conditions were obtained. The triggered condition

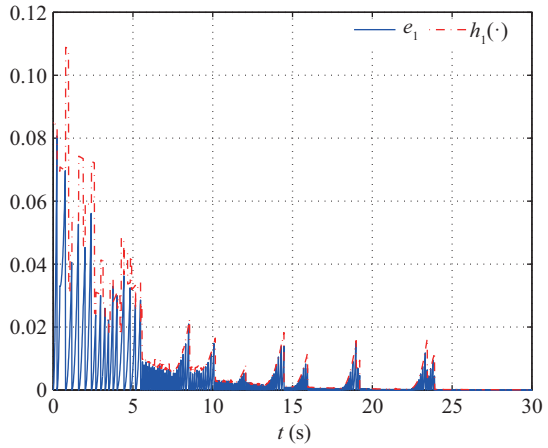

Figure 8 (Color online) The measurement error and trigger threshold of Agent 1.

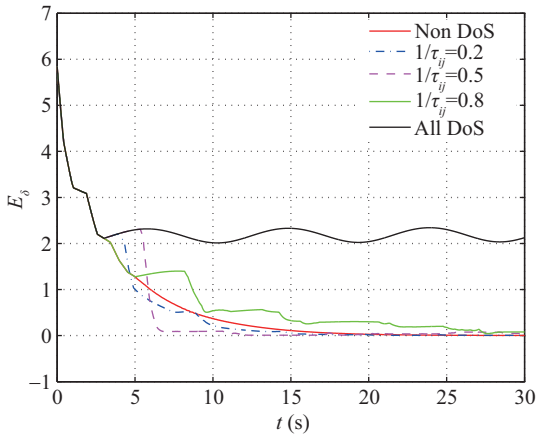

Figure 9 (Color online) Consensus performance comparison for different attack strengths.

for the DoS duration was developed, and the MAS consensus was achieved without Zeno behavior. A future line of research would include a self-triggered approach for heterogeneous MASs connected through a directed communication topology in the presence of DoS and/or other attacks.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61873130, 61833008, 61833011, 61803210), Natural Science Foundation of Jiangsu Province (Grant No. BK20191377), Jiangsu Government Scholarship for Overseas Studies (Grant No. 2017-037), and 1311 Talent Project of the Nanjing University of Posts and Telecommunications.

References

1 Ding L, Han Q L, Ge X H, et al. An overview of recent advances in event-triggered consensus of multiagent systems. IEEE Trans Cybern, 2018, 48: 1110–1123
2 Ma L F, Wang Z D, Han Q L, et al. Consensus control of stochastic multi-agent systems: a survey. Sci China Inf Sci, 2017, 60: 120201
3 Zuo Z Y, Han Q L, Ning B D, et al. An overview of recent advances in fixed-time cooperative control of multiagent systems. IEEE Trans Ind Inf, 2018, 14: 2322–2334
4 Liu J W, Huang J. Leader-following consensus of linear discrete-time multi-agent systems subject to jointly connected switching networks. Sci China Inf Sci, 2018, 61: 112208
5 Liu X Y, Lam J, Yu W W, et al. Finite-time consensus of multiagent systems with a switching protocol. IEEE Trans Neural Netw Learn Syst, 2016, 27: 853–862
6 Qiu Z R, Liu S, Xie L H. Distributed constrained optimal consensus of multi-agent systems. Automatica, 2016, 68: 209–215
7 Lin Z L. Control design in the presence of actuator saturation: from individual systems to multi-agent systems. Sci China Inf Sci, 2019, 62: 026201
8 Feng Z, Hu G Q. Secure cooperative event-triggered control of linear multiagent systems under DoS attacks. IEEE Trans Contr Syst Technol, 2019. doi: 10.1109/TCST.2019.2892032
9 Xu W Y, Ho D W C, Zhong J, et al. Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks. IEEE Trans Neural Netw Learn Syst, 2019, 30: 3137–3149
10 Zhao C C, He J P, Chen J M. Resilient consensus with mobile detectors against malicious attacks. IEEE Trans Signal Inf Process Netw, 2018, 4: 60–69
11 Zhang W B, Wang Z D, Liu Y R, et al. Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks. Int J Robust Nonlin Control, 2018, 28: 53–67
12 Zhang H, Cheng P, Shi L, et al. Optimal DoS attack scheduling in wireless networked control system. IEEE Trans Contr Syst Technol, 2016, 24: 843–852
13 Ge X, Han Q L, Zhong M, et al. Distributed Krein space-based attack detection over sensor networks under deception attacks. Automatica, 2019, 109: 108557
14 Wu Y M, Xu M, Zheng N, et al. Attack tolerant finite-time consensus for multi-agent networks. In: Proceedings of 2017 13th IEEE International Conference on Control & Automation (ICCA), 2017. 1010–1014
15 Feng S, Tesi P. Resilient control under denial-of-service: robust design. Automatica, 2017, 79: 42–51
16 Lee P, Clark A, Bushnell L, et al. A passivity framework for modeling and mitigating wormhole attacks on networked control systems. IEEE Trans Automat Contr, 2014, 59: 3224–3237

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

18 Pang Z H, Liu G P, Dong Z. Secure networked control systems under denial of service attacks. In: Proceedings of the 18th IFAC World Congress, 2011. 8908–8913

19 Long M, Wu C H, Hung J Y. Denial of service attacks on network-based control systems: impact and mitigation. IEEE Trans Ind Inf, 2005, 1: 85–96

20 Amullen E M, Shetty S, Keel L H. Model-based resilient control for a multi-agent system against denial of service attacks. In: Proceedings of 2016 World Automation Congress (WAC), 2016. 1–6

21 Zhang D, Liu L, Feng G. Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack. IEEE Trans Cybern, 2019, 49: 1501–1511

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

23 Cui T T, Yu H, Hao F. Security control for linear systems subject to denial-of-service attacks. In: Proceedings of the 36th Chinese Control Conference (CCC), 2017. 7673–7678

24 Ge X, Han Q L, Zhang X M, et al. Distributed event-triggered estimation over sensor networks: a survey. IEEE Trans Cybern, 2019. doi: 10.1109/TCYB.2019.2917179

25 Zhang X M, Han Q L, Zhang B L. An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems. IEEE Trans Ind Inf, 2017, 13: 4–16

26 Dimarogonas D V, Frazzoli E, Johansson K H. Distributed event-triggered control for multi-agent systems. IEEE Trans Automat Contr, 2012, 57: 1291–1297

27 Xie D S, Xu S Y, Li Z, et al. Event-triggered consensus control for second-order multi-agent systems. IET Control Theory Appl, 2015, 9: 667–680

28 Hu W F, Liu L, Feng G. Consensus of linear multi-agent systems by distributed event-triggered strategy. IEEE Trans Cybern, 2016, 46: 148–157

29 Hu S L, Yue D, Xie X P, et al. Resilient event-triggered controller synthesis of networked control systems under periodic dos jamming attacks. IEEE Trans Cybern, 2019, 49: 4271–4281

30 Feng Z, Hu G Q. Distributed secure average consensus for linear multi-agent systems under DoS attacks. In: Proceedings of American Control Conference (ACC), 2017. 2261–2266

31 Feng Z, Hu G Q. Distributed secure leader-following consensus of multi-agent systems under DoS attacks and directed topology. In: Proceedings of 2017 IEEE International Conference on Information and Automation (ICIA), 2017. 73–79

32 Ding D R, Wang Z D, Ho D W C, et al. Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks. IEEE Trans Cybern, 2017, 47: 1936–1947

33 Lu A Y, Yang G H. Distributed consensus control for multi-agent systems under denial-of-service. Inf Sci, 2018, 439–440: 95–107

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

35 Sun H T, Peng C, Zhang W D, et al. Security-based resilient event-triggered control of networked control systems under denial of service attacks. J Franklin Inst, 2018. doi: 10.1016/j.jfranklin.2018.04.001

36 Zhao Y, Liu Y F, Li Z K, et al. Distributed average tracking for multiple signals generated by linear dynamical systems: an edge-based framework. Automatica, 2017, 75: 158–166

37 Wen G H, Wang H, Yu X H, et al. Bipartite tracking consensus of linear multi-agent systems with a dynamic leader. IEEE Trans Circ Syst II, 2018, 65: 1204–1208

38 Sun Z Y, Huang N, Anderson B D O, et al. Event-based multiagent consensus control: zeno-free triggering via L_p signals. IEEE Trans Cybern, 2020, 50: 284–296

39 Sun Z Y, Huang N, Anderson B D O, et al. Comments on distributed event-triggered control of multi-agent systems with combinational measurements. Automatica, 2018, 92: 264–265

40 Fan Y, Feng G, Wang Y, et al. Distributed event-triggered control of multi-agent systems with combinational measurements. Automatica, 2013, 49: 671–675

41 Xie D S, Xu S Y, Chu Y M, et al. Event-triggered average consensus for multi-agent systems with nonlinear dynamics and switching topology. J Franklin Inst, 2015, 352: 1080–1098

42 Zhang Z Q, Hao F, Zhang L, et al. Consensus of linear multi-agent systems via event-triggered control. Int J Control, 2014, 87: 1243–1251