Neural Processing Letters (2024) 56:171
https://doi.org/10.1007/s11063-024-11630-z

Pinning Group Consensus of Multi-agent Systems Under DoS Attacks

Qian Lang[1] · Jing Xu[1] · Huiwen Zhang[1] · Zhengxin Wang[1]

Accepted: 23 April 2024

Abstract
In this paper, group consensus is investigated for a class of nonlinear multi-agent systems suffered from the DoS attacks. Firstly, a first-order nonlinear multi-agent system is constructed, which is divided into M subsystems and each subsystem has an unique leader. Then a protocol is proposed and a Lyapunov function candidate is chosen. By means of the stability theory, a sufficient criterion, which involves the duration of DoS attacks, coupling strength and control gain, is obtained for achieving group consensus in first-order system. That is, the nodes in each subsystem can track the leader of that group. Furthermore, the result is extended to nonlinear second-order multi-agent systems and the controller is also improved to obtain sufficient conditions for group consensus. Additionally, the lower bounds of the coupling strength and average interval of DoS attacks can be determined from the obtained sufficient conditions. Finally, several numerical simulations are presented to explain the effectiveness of the proposed controllers and the derived theoretical results.

Keywords Multi-agent system · Group consensus · DoS attack · Lyapunov function

1 Introduction

With the rapid development of information technology and network science, multi-agent systems (MASs) are gradually applied in numerous aspects, such as autonomous unmanned vehicles [1], unmanned aerial vehicle formation [2], factory automation management [3], etc. Due to the large scale of the MASs, however, it is more difficult for such systems to return to normal state timely when they suffer from network attacks. At this time, each node

Qian Lang, Jing Xu, Huiwen Zhang have contributed equally to this work.

✉ Zhengxin Wang
zwang@njupt.edu.cn

Qian Lang
b20070409@njupt.edu.cn

Jing Xu
b20070404@njupt.edu.cn

Huiwen Zhang
b20070406@njupt.edu.cn

[1] College of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Published online: 10 May 2024

of a networked system urgently needs to deal with the impact of the attacks to guarantee synchronization or consensus. Synchronization focuses on whether the nodes in the coupled network can achieve the same state, while consensus focuses on designing distributed control protocols for MASs to make the states of agents in the systems tend to be identical. In most cases, consensus is little different to synchronization. They are just for different networked systems. In [4] and [5], synchronization is studied for two kinds of neural networks. Specially, the sufficient conditions for ensuring secure synchronization are derived for the Markov jump neural networks in [4], where the mixed cyber-attack forms of deception attack and denial of service attack are considered.

Common network attacks include denial of service (DoS) attacks [6], distributed denial of service (DDoS) attacks [7], false data injection (FDI) attacks [8], etc. Among them, DoS attacks are relatively destructive. The working principle of DoS attacks is to compel the networked system too busy to process necessary instructions and occupy the key communication resources. DoS attacks will use packets to overwhelm the local system to disturb or intensely stop the corresponding local services answering the reasonable external demand, and sometimes will crumble the local system so that it doesn't work properly. For example, In [9] and [10], security controls of signed MASs and switching MASs under DoS attacks are studied. In [11], based on the distributed control, group consensus of first-order MAS is achieved under DoS attacks and switching topologies. It can be seen that it is of great significance to further explore the impact of DoS attacks on achieving consensus of a MAS. In particular, the different characteristics of DoS attacks need to be further discussed.

Usually, DoS attacks include periodic DoS attacks, intermittent DoS attacks and random DoS attacks. The attack intervals of periodic DoS attacks are fixed, so it is easy to be implemented. However, long-term periodic DoS attacks are easy to be monitored and defended. In contrast, short-term and uncertain DoS attacks are more covert and not easy to be detected, such as intermittent DoS attacks [12]. In addition, the attack time and other characteristics of random DoS attacks have certain randomness, which will lead to random packet loss. The existing results usually regard random DoS attacks as Markov attacks [13], and apply this perspective to establish a model. This paper adopts the aperiodic DoS attack model, where the duration of DoS attack only needs to satisfy an assumption.

To deal with such attacks, the system needs to have the ability to recover within a limited time after being attacked to ensure that the system achieves the required collective dynamics. Consensus is a typical collective dynamics and a basic research topic in the distributed cooperative coordination of MASs. This means that all agents exchange information based on the local information interaction, therefore, an appropriate distributed consensus protocol (such as event-triggered control [14]) needs to be designed so that all states of agents eventually converge to a common value. Various studies are conducted on coordination of MASs without or with DoS attacks. Specifically, in [15], the finite-horizon robust event-triggered control is studied for nonlinear MASs with state delay, and consensus of nonlinear MASs is further discussed. In [16], due to the different network environment, the states of agents are different, and the consensus convergence state is also different from [15], that is, the finite mean square consensus criterion of second-order nonlinear MAS is established. In some cases, due to the different control strategies, the conditions for reaching consensus are also different. For example, in [17], consensus of MASs is realized via the proposed event-triggered control strategy without collecting global information. For example, in [18], a second-order MAS in directed networks is studied, and practical consensus is reached in a fixed time. Nowadays, the research on the convergence problem of second-order MASs is not rich, so we also choose such systems as the research direction.

When there is a cooperative relationship among agents in a MAS, the MAS is able to achieve consensus. In [19], the event-triggered communication (ETC), self-triggered communication (STC) scheme and the corresponding resilient control protocol are designed, and the sufficient conditions for the system to achieve consensus under DoS attacks are obtained. Both references [19] and [20] apply the event-triggered scheme, however, the MAS in [20] has both cooperative relationship and competitive relationship, so that the system tends to achieve bipartite consensus. In [21], the time factor on the basis of event-triggered control is considered and the leader selection scheme is given, and the sufficient conditions for achieving bipartite consensus are finally obtained. In [22], bipartite consensus of MASs is addressed by dealing with the influence of noise. By designing a time-varying stochastic bipartite consensus protocol to reduce the harmful effects of noise, the necessary and sufficient conditions for the proposed protocol are derived to guarantee mean square bipartite consensus.

With the expansion of the scale of MASs, achieving consensus in the whole system becomes more and more restrictive. Therefore, it is necessary to study group consensus, that is, the system is divided into several subgroups, and consensus can be reached for the agents in the same subgroup. In [23], group consensus of heterogeneous MASs under Markov transformation is considered. Similarly, in [24] and [25], heterogeneous MASs are also studied, and sufficient conditions for achieving group consensus are given. The difference is that [24] considers a system with input time delay and [25] considers a heterogeneous MAS with unknown parameters. In [26], a distributed dynamic event-triggered scheme is designed for MASs with input saturation. At the same time, an algorithm for estimating initial conditions is introduced. Based on the stability theory, the conditions of mean square local group consensus are derived.

Up to now, studies on group consensus of MASs suffered from DoS attacks are relatively rare. Especially under DoS attacks, the problem of group consensus of the MASs with multiple isolated leaders deserves further study.

Enlightened by the above discussions, this article mainly focuses on group consensus of the MAS with multiple isolated leaders. Main contribution of this article are highlighted below.

(1) For a class of nonlinear MASs with multiple isolated leaders, group consensus of the nonlinear MASs is analyzed, and sufficient criteria for ensuring group consensus are derived.
(2) DoS attacks, which can be conducted aperiodically or randomly, are considered in information interaction among agents. The effect of attack durations on consensus is clearly given.
(3) The group consensus problem for a first-order nonlinear MAS is first studied under DoS attacks, and then the theoretical results are further generalized to the second-order nonlinear MAS.
(4) Distributed cooperative controllers are designed for both first-order and second-order MASs. In addition, both the information interaction within the group and the information interaction between groups are considered in the controllers.

2 Preliminaries

We suppose that the MASs have M leader agents and N follower agents. These followers can be divided into M groups, and each group has an unique leader, $N = \sum_{j=1}^{M} N_j$, where N_j denotes the total number of follower nodes in group j, $j = 1, 2, \ldots, M$.

Define the set $I_0 = \{N+1, \ldots, N+M\}$, $I_1 = \{1, 2, \ldots, N_1\}$, $I_k = \left\{\sum_{j=1}^{k-1} N_j + 1, \sum_{j=1}^{k-1} N_j + 2, \ldots, \sum_{j=1}^{k-1} N_j + N_1\right\}$, $k = 2, 3, \ldots, M$, and $I = I_1 \cup I_2 \cup \ldots \cup I_M$. The node set is $V_j = \{n_i \mid i \in I_j\}$, $j = 0, 1, 2, \ldots, M$, where V_0 is the node set of the leaders, and the rest sets are the follower nodes.

The triple $G = (V, E, A)$ represents a weighted directed graph and also indicates the relationship among those followers. The set of followers is V, which has a partition $V = V_1 \cup V_2 \cup \ldots \cup V_M$. The edge set is $E \subseteq V \times V$. In addition, the adjacency matrix is $A = [a_{ij}]_{N\times N}$, where $a_{ij} \neq 0$ if there is a directed edge from node j to node i, otherwise $a_{ij} = 0$.

The set of neighbours for node n_i is defined as:

$$N_{k,i} = \{n_j \in V_k \mid (n_i, n_j) \in E\}, \ k = 1, 2, \ldots, M.$$

Observing the information interaction between two agents in the same subsystem and also between two agents in the different subsystems, this paper divides the agents as follows [27]: $V_k^{in} = \left\{n_i \in V_k \mid \bigcup_{l\neq k} N_{l,i} = \emptyset \text{ and } n_i \notin \bigcup_{m\in I\setminus I_k} N_{k,m}\right\}$ is the k-th node set that does not exchange information with the nodes in other subsystems, and $V_k^{out} = \left\{n_i \in V_k \mid \bigcup_{l\neq k} N_{l,i} \neq \emptyset \text{ or } n_i \in \bigcup_{m\in I\setminus I_k} N_{k,m}\right\}$ is the k-th node set that exchanges information with the nodes in the k-th subsystem and other subsystems. According to the above definition, we can obtain $V_k = V_k^{in} \cup V_k^{out}$ and $V_k^{in} \cap V_k^{out} = \emptyset$. Define $V^{in} = \bigcup_{k=1}^{M} V_k^{in}$ and $V^{out} = \bigcup_{k=1}^{M} V_k^{out}$.

Furthermore, let $L = [l_{ij}]_{N\times N}$ be the Laplacian matrix of G with $l_{ii} = \sum_j^N a_{ij}$ and $l_{ij} = -a_{ij}$ for $i \neq j$.

Assumption 1 The subgraph of each group exists a spanning tree with one leader agent as its root.

DoS attack is one of the most common ways of the network attack, which compels the MASs too busy to process necessary instructions and occupies the key communication resources. Therefore, when the MASs are subjected to the DoS attack, the MASs cannot execute the designed control instructions, in other words, the control fails during the attack period. In this paper, an aperiodic DoS attack model is established. For the sake of storing energy for the next attack, the DoS attack needs to retain in a dormant state for a while after each attack. The specific description of the DoS attack of this paper is introduced below.

Let the DoS attack sequence be $\{t_\theta\}, \theta \in N^*, \ N^* = \{0, 1, 2, \ldots\}$. Then the DoS attack interval can be expressed as $S_\theta = [t_\theta, t_\theta + \tau_\theta)$, where τ_θ is the duration of the DoS attack. The intersection of all intervals where DoS attacks occur is an empty set, that is, there is no overlap, which can be expressed as $t_\theta + \tau_\theta < t_{\theta+1}, \ \theta \in N^*$. For all given bounded time interval $[t_0, t], \ t_0 < t$, it is impossible to transmit information during the DoS attack time. These time intervals that cannot transmit information can be expressed as $T_D = \bigcup S_\theta \bigcap [t_0, t]$. In that case, the corresponding time interval for information transmission can be expressed as $T_s = [t_0, t] \setminus \bigcup S_\theta$.

Definition 1 [28] The DoS attack frequency is defined as $F_s(t_0, t) = \frac{N_s(t_0,t)}{t-t_0}$, where $N_s(t_0, t)$ is the number of attacks during the interval $[t_0, t]$.

Assumption 2 With regard to the duration of DoS attack, there exist $T > 1$ and $\varphi > 0$ such that $|T_D| < \varphi + \frac{t-t_0}{T}$, where T and φ are both constants, and $|T_D|$ represents the time length of T_D.

Remark 1 In the DoS attack interval, the communications between two adjacent agents will fail properly. This paper aims to study group consensus of the MASs suffered from DoS attacks and design a suitable controller so that followers in each subgroup can still approach the state information of the corresponding leader in that subgroup.

3 Main Results on Group Consensus

In this section, group consensus of first-order MASs is first analyzed, and then the result is further extended to the second-order MASs. Several sufficient conditions are obtained.

3.1 Group Consensus of First-Order MASs Under DoS Attacks

The leaders are modeled as

$$\dot{x}_k^*(t) = f\left(x_k^*(t), t\right), \ k \in I_0, \tag{1}$$

and the follower agents are represented as

$$\dot{x}_i(t) = f\left(x_i(t), t\right) + \mu_i(t), \ i \in I, \tag{2}$$

where $x_k^*(t) \in R^n$ are the position states of leaders, $x_i(t) \in R^n$ are the position states of follower agents, $f\left(x_k^*(t), t\right)$, $f\left(x_i(t), t\right) \in R^n$ are nonlinear functions satisfying Lipschitz condition, and $\mu_i(t) \in R^n$ are external controllers to be designed.

Definition 2 If first-order nonlinear MASs (1)-(2) are in accord with $\lim_{t\to\infty} \left\|x_i(t) - x_k^*(t)\right\| = 0, \ i \in I_k$ under any initial conditions, then the group consensus of MASs (1)-(2) under DoS attacks is said to be realized.

Assumption 3 For arbitrary variables $w_1, \ w_2 \in R^n$, there is a non-negative real number ρ such that the nonlinear function satisfies

$$\|f(w_1, t) - f(w_2, t)\| \le \rho \|w_1 - w_2\|.$$

The following rules are made for information interaction.

(i) When $n_i \in V^{in} (i \in I)$ are the nodes whose leader's state of the subsystem is known, and the information interaction in this subsystem is transmitted by the position state $x_i(t)$, and the error state is expressed as $e_i(t) = x_i(t) - x_i^*(t)$, where $x_i^*(t) = x_k^*(t)$ for $i \in I_k, \ k = 1, 2, \ldots, M$.

(ii) When $n_i \in V^{out} (i \in I)$ are the nodes whose leader's state of the subsystem is known, the states of the out-group neighbors are known and the leader's state of those out-group neighbors is unknown, the information interaction in this subsystem is transmitted by the position state $x_i(t)$ and the out-group information exchange is transmitted by the error of the position state $e_i(t) = x_i(t) - x_i^*(t)$, where $x_i^*(t) = x_k^*(t)$ for $i \in I_k, \ k = 1, 2, \ldots, M$.

Next, based on the information interaction of the above two rules, that is, the information interaction within the group and the information interaction between groups, we design the external controller for first-order MASs as

$$\begin{aligned} \mu_i(t) = \alpha c \Bigg[& \sum_{j \in V_k} a_{ij} \left(x_j(t) - x_i(t)\right) + b_i \left(x_k^*(t) - x_i(t)\right) \\ & + \sum_{j \in (V \setminus V_k)} a_{ij} \left(e_j(t) - e_i(t)\right) \Bigg], \ i \in V_k, \end{aligned} \tag{3}$$

where $c \geq 0$ represents the controller gain and $\alpha > 0$ indicates the coupling strength. When the MASs suffer from DoS attacks, $c = 0$. Accordingly, when there is no attack, $c > 0$. a_{ij} refers to the weight for the edge between the ith node and the jth node. Additionally, b_i refers to pinning coupling strength of the ith node and its leader. We define matrix $B = diag\{b_1, b_2, \ldots, b_N\}$, $H = \left[h_{ij}\right]_{N\times N}$, $H = L + B$, $H^{'} = \frac{H+H^T}{2}$.

Based on the properties of the Laplacian matrix, the external controller (3) can also be transformed to

$$\begin{aligned}
\mu_i(t) &= \alpha c \left[\sum_{j\in V_k} a_{ij} \left(x_j(t) - x_k^*(t)\right) - \left(\sum_{j\in V_k} a_{ij} + b_i \right) \left(x_i(t) - x_k^*(t)\right) \right. \\
&\quad \left. + \sum_{j\in V\setminus V_k} a_{ij} e_j(t) - \sum_{j\in V\setminus V_k} a_{ij} e_i(t) \right] \\
&= \alpha c \left[\sum_{j\in V_k} a_{ij} e_j(t) - \left(\sum_{j\in V_k} a_{ij} + \sum_{j\in V\setminus V_k} a_{ij} + b_i \right) e_i(t) + \sum_{j\in V\setminus V_k} a_{ij} e_j(t) \right] \\
&= \alpha c \left[\sum_{j\in V_k, i\neq j} -l_{ij} e_j(t) - (l_{ii} + b_i) e_i(t) - \sum_{j\in V/V_k} l_{ij} e_j(t) \right] \\
&= -\alpha c \left[\sum_{j\in V} l_{ij} e_j(t) + b_i e_i(t) \right] \\
&= -\alpha c \sum_{j\in V} h_{ij} e_j(t),
\end{aligned}$$

therefore, for $t \in \left[t_\theta + \tau_\theta, t_{\theta+1}\right)$, $\theta \in N^*$, DoS attack is dormant and the error system of the MASs can be expressed as

$$\begin{aligned}
\dot{e}_i(t) &= \dot{x}_i(t) - \dot{x}_k^*(t) \\
&= -\alpha c \sum_{j\in V} h_{ij} e_j(t) + \left[f\left(x_i(t), t\right) - f\left(x_k^*(t), t\right) \right],
\end{aligned} \tag{4}$$

where $e_i(t) = x_i(t) - x_i^*(t)$. Reformulate the error systems (4) into a compact form

$$\dot{e}(t) = -\alpha c \left(L + B\right) \otimes I_n e(t) + F\left(x, t\right) = -\alpha c H \otimes I_n e(t) + F(t), \tag{5}$$

where $e(t) = \left[e_1^T(t), e_2^T(t), \ldots, e_N^T(t)\right]^T$ and $F\left(t\right) = \left[F_1^T(t), F_2^T(t), \ldots, F_N^T(t)\right]^T$ with $F_i(t) = f\left(x_i(t), t\right) - f\left(x_k^*(t), t\right)$, $i = 1, 2, \ldots, N$.

When $t \in [t_\theta, t_\theta + \tau_\theta)$, $\theta \in N^*$, DoS attack is active and the external control is failing, that is $c = 0$. Then, the error system of the MASs can be expressed as

$$\dot{e}(t) = F(t). \tag{6}$$

In fact, system (6) can be written uniformly to system (5), which becomes system (6) if $c = 0$. Next, we present the theoretical result on guaranteeing group consensus of the first-order MASs (1) and (2) suffered from the DoS attacks via the distributed cooperative controller (3).

Theorem 1 *When the assumptions 1 and 3 are true, the first-order MASs (1) and (2) under the DoS attacks can achieve group consensus via the distributed cooperative controller (3) if the following conditions hold:*

(a_1) $c > \frac{\rho^2+1}{2\alpha\lambda_{\min}(H')}$;

(b_1) $T > \frac{2\alpha c\lambda_{\min}(H')}{2\alpha c\lambda_{\min}(H')-\rho^2-1}$.

Proof Lyapunov function is designed as

$$V(t) = \frac{1}{2} e^T(t) e(t).$$

Then, computing the derivative of $V(t)$ derives

$$\begin{aligned}
\dot{V}(t) &= e^T(t)\dot{e}(t) \\
&= e^T(t)\left(-\alpha c H \otimes I_n e(t)\right) + e^T(t)F(t) \\
&\le e^T(t)\left(-\alpha c H' \otimes I_n e(t)\right) + \tfrac{1}{2} e^T(t)e(t) + \tfrac{1}{2} F^T(t)F(t) \\
&\le e^T(t)\left(-\alpha c \lambda_{\min}\left(H'\right) e(t)\right) + \tfrac{1}{2} e^T(t)e(t) + \tfrac{1}{2}\rho^2 e^T(t)e(t) \\
&= e^T(t)\left(-\alpha c \lambda_{\min}\left(H'\right) + \tfrac{1}{2} + \tfrac{1}{2}\rho^2\right) e(t) \\
&= 2\left(-\alpha c \lambda_{\min}\left(H'\right) + \tfrac{1}{2} + \tfrac{1}{2}\rho^2\right) V(t) \\
&= \left(-2\alpha c \lambda_{\min}\left(H'\right) + 1 + \rho^2\right) V(t).
\end{aligned}$$

When $t \in [t_\theta, t_\theta + \tau_\theta)$, DoS attacks occur, that is, $c = 0$, therefore,

$$\dot{V}(t) \le \left(1 + \rho^2\right) V(t), t \in [t_\theta, t_\theta + \tau_\theta).$$

When $t \in \left[t_\theta + \tau_\theta, t_{\theta+1}\right)$, $c > 0$, hence,

$$\dot{V}(t) \le \left(-2\alpha c \lambda_{\min}\left(H'\right) + 1 + \rho^2\right) V(t), t \in \left[t_\theta + \tau_\theta, t_{\theta+1}\right).$$

Therefore,

$$\begin{aligned}
\dot{V}(t) &\le V(t_0)\, e^{(-2\alpha c \lambda_{\min}(H') + 1 + \rho^2)(t - t_0) + (2\alpha c \lambda_{\min}(H'))(\varphi + \frac{t - t_0}{T})} \\
&= e^{2\alpha c \lambda_{\min}(H')\varphi} e^{(-2\alpha c \lambda_{\min}(H') + 1 + \rho^2 + \frac{2\alpha c \lambda_{\min}(H')}{T})(t - t_0)}.
\end{aligned}$$

According to conditions (a_1) and (b_1),

$$-2\alpha c \lambda_{\min}\left(H'\right) + 1 + \rho^2 + \frac{2\alpha c \lambda_{\min}\left(H'\right)}{T} < 0,$$

consequently, it follows from Lyapunov stability theory that $\lim_{t\to\infty} V(t) = 0$, that is $\lim_{t\to 0} \|e(t)\| = 0$.

In a word, group consensus of the MASs (1) and (2) is reached, and the theorem is proved. □

Remark 2 According to Theorem 1, one knows that group consensus has a requirement on the duration of the DoS attacks. In addition, when the controller gain and the attack duration satisfy the conditions (a_1) and (b_1) respectively, group consensus of the MASs (1) and (2) can still be reached based on distributed protocol (3).

3.2 Grouping Consensus of Second-Order MASs Under DoS Attacks

The leaders dynamics are given as

$$\begin{cases} \dot{x}_k^*(t) = v_k^*(t), \\ \dot{v}_k^*(t) = f\left(x_k^*, v_k^*, t\right), \end{cases} \quad k \in I_0, \tag{7}$$

and the followers dynamics are modeled as

$$\begin{cases} \dot{x}_i(t) = v_i(t), \\ \dot{v}_i(t) = f\left(x_i(t), v_i(t), t\right) + \mu_i(t), \end{cases} \quad i \in I, \tag{8}$$

where $x_k^*(t) \in R^n$ are the position states of leaders, $x_i(t)$ are the position states of follower agents, $v_k^*(t) \in R^n$ are the velocity states of the leaders, $v_i(t)$ are the velocity states of follower agents, $f\left(x_k^*(t), v_k^*(t), t\right), f\left(x_i(t), v_i(t), t\right) \in R^n$ are nonlinear functions satisfying Lipschitz condition, and $\mu_i(t) \in R^n$ are external controllers to be designed.

Definition 3 If second-order nonlinear MASs (7) and (8) are in accord with the formulation $\lim_{t\to\infty} \left\|x_i(t) - x_k^*(t)\right\| = 0$ and $\lim_{t\to\infty} \left\|v_i(t) - v_k^*(t)\right\| = 0$ under any initial conditions for any $i \in I_k$, then group consensus of MASs (7) and (8) under DoS attacks is said to be realized.

Assumption 4 For any variables $z_1, z_2, w_1, w_2 \in R^n$, there are real numbers $\rho_1 \geq 0$ and $\rho_2 \geq 0$ such that

$$\|f(z_1, z_2, t) - f(w_1, w_2, t)\| \leq \rho_1 \|z_1 - w_1\| + \rho_2 \|z_2 - w_2\|.$$

The following rules are made for information interaction.

(i) When $n_i \in V^{in}(i \in I)$ are the nodes whose leader's state of the subsystem is known, and the information interaction in this subsystem is transmitted by the position state $x_i(t)$ and the velocity state $v_i(t)$. Additionally, the error states are expressed as $e_i^{(1)}(t) = x_i(t) - x_i^*(t)$ and $e_i^{(2)}(t) = v_i(t) - v_i^*(t)$, where $x_i^*(t) = x_k^*(t)$ and $v_i^*(t) = v_k^*(t), i \in I_k, k = 1, 2, \ldots, M$.

(ii) When $n_i \in V^{out}(i \in I)$ are the nodes whose leader's state of the subsystem is known, the states of the out-group neighbors are known and the leader's state of those out-group neighbors is unknown, the information interaction in this subsystem is transmitted by the position state $x_i(t)$ and the velocity state $v_i(t)$ and the out-group information exchange is transmitted by the errors of the position state $e_i^{(1)}(t) = x_i(t) - x_i^*(t)$ and the velocity state $e_i^{(2)}(t) = v_i(t) - v_i^*(t)$, where $x_i^*(t) = x_k^*(t)$ and $v_i^*(t) = v_k^*(t), i \in I_k, k = 1, 2, \ldots, M$.

Based on the information interaction of the above two rules, which consider the information interaction within the group and the information interaction between groups, the second-order cooperative controller is proposed as

$$\begin{aligned}\mu_i(t) = \alpha c \Big[& \textstyle\sum_{j\in V_k} a_{ij}\left(x_j(t) - x_i(t)\right) + b_i\left(x_k^*(t) - x_i(t)\right) + \\ & \textstyle\sum_{j\in(V\setminus V_k)} a_{ij}\left(e_j^{(1)}(t) - e_i^{(1)}(t)\right)\Big] \\ & + \beta c \Big[\textstyle\sum_{j\in V_k} a_{ij}\left(v_j(t) - v_i(t)\right) + b_i\left(v_k^*(t) - v_i(t)\right) + \\ & \textstyle\sum_{j\in(V\setminus V_k)} a_{ij}\left(e_j^{(2)}(t) - e_i^{(2)}(t)\right)\Big],\end{aligned} \tag{9}$$

where c refers to the control gain, and α and β signify the positive coupling strengths. $c = 0$ when the MASs are under DoS attack, and $c > 0$ when no attack occurs. a_{ij} means the weight for the edge of the ith node and the jth node. Furthermore, b_i denotes the pinning coupling strength of the ith node and its leader.

Represent the cooperative controller as follows:

$$\mu_i(t) = -\alpha c \sum_{j\in V} h_{ij} e_j^{(1)}(t) - \beta c \sum_{j\in V} h_{ij} e_j^{(2)}(t).$$

Let

$$e^{(1)}(t)^T = \left[e_1^{(1)}(t)^T, e_2^{(1)}(t)^T, \ldots, e_N^{(1)}(t)^T\right]^T,$$

$$e^{(2)}(t)^T = \left[e_1^{(2)}(t)^T, e_2^{(2)}(t)^T, \ldots, e_N^{(2)}(t)^T\right]^T,$$

and

$$\bar{e}(t) = \begin{bmatrix} e^{(1)}(t) \\ e^{(2)}(t) \end{bmatrix}. \tag{10}$$

Then error systems of systems (7) and (8) can further be reexpressed as the following matrix equation

$$\dot{\bar{e}}(t) = \begin{bmatrix} 0_N & I_N \\ -\alpha c H & -\beta c H \end{bmatrix} \otimes I_n \bar{e}(t) + \begin{bmatrix} 0_{nN\times 1} \\ \left[f\left(x_i(t), t\right) - f\left(x_k^*(t), t\right) \right]_{N\times 1} \end{bmatrix}. \tag{11}$$

Let $M = \begin{bmatrix} 0_N & I_N \\ -\alpha c H & -\beta c H \end{bmatrix} \otimes I_n$, and $\bar{F}(t) = \begin{bmatrix} 0_{nN\times 1} \\ F(t) \end{bmatrix}$, the system is transformed into

$$\dot{\bar{e}}(t) = M\bar{e}(t) + \bar{F}(t). \tag{12}$$

Similar to Subsect. 3.1, system (12) can represent both an error system that is not affected by the DoS attacks and an error system that is affected by the DoS attacks. In other words, if $c = 0$ in matrix M, then system (12) represents error system that is not affected by the DoS attacks; if $c \neq 0$ in matrix M, then system (12) represents error system that is affected by the DoS attacks.

Theorem 2 *Under assumptions 2 and 4, and DoS attacks in the communication, the second-order MASs composed of (7) and (8) can reach group consensus, with the distributed cooperative controller (9) if:*

(a_2) $c > \max\left\{ \frac{\alpha}{2\beta^2\lambda_{\min}(H')}, \frac{\alpha+2\alpha\rho_1^2+\beta\rho_1^2}{2\alpha^2\lambda_{\min}(H')}, \frac{2\alpha+\beta+2\alpha\rho_2^2+2\beta\rho_2^2}{2\beta^2\lambda_{\min}(H')} \right\}$;

(b_2) $T > \frac{r_S - r_D}{r_S}$.

Proof Define $\Omega = \begin{bmatrix} 2cH' & \frac{1}{\beta} I_N \\ \frac{1}{\beta} I_N & \frac{1}{\alpha} I_N \end{bmatrix} \otimes I_n$. From $\frac{1}{\alpha} I_N > 0$ and Schur Complement Lemma that $\Omega > 0$ is equivalent to $2cH' - \frac{\alpha}{\beta^2} I_N > 0$. From condition$(a_2)$, we have $c > \frac{\alpha}{2\beta^2\lambda_{\min}(H')}$. That is, $2c\lambda_{\min}\left(H'\right) > \frac{\alpha}{\beta^2}$. Hence, $2cH' - \frac{\alpha}{\beta^2} I_N > 0$. Furthermore, Ω is positive definite. Select following Lyapunov function

$$V = \frac{1}{2}\bar{e}^T \Omega \bar{e}. \tag{13}$$

Taking the derivative of V gets

$$
\begin{aligned}
\dot{V} &= \bar{e}^T \Omega \dot{\bar{e}} \\
&= \bar{e}^T(t)\Omega(M\bar{e}(t) + \bar{F}(x,t)) \\
&= \bar{e}^T(t)\left(\tfrac{1}{2}\Omega M + \tfrac{1}{2}M^T\Omega^T\right)\bar{e}(t) + \bar{e}^T(t)\Omega\bar{F}(t) \\
&= \left[e^{(1)^T}(t),\ e^{(2)}(t)\right]\begin{bmatrix} \frac{-\alpha c}{\beta}H' & 0_N \\ 0_N & \frac{1}{\beta}I_N - \frac{\beta c}{\alpha}H' \end{bmatrix} \otimes I_n \begin{bmatrix} e^{(1)}(t) \\ e^{(2)}(t) \end{bmatrix} \\
&\quad - \tfrac{1}{\beta}e^{(1)^T}(t)F(t) - \tfrac{1}{\alpha}e^{(2)^T}(t)F(t) \\
&\le -\tfrac{\alpha c}{\beta}\lambda_{\min}\left(H'\right)e^{(1)^T}(t)e^{(1)}(t) + \left(\tfrac{1}{\beta}I_N - \tfrac{\beta c}{\alpha}\lambda_{\min}\left(H'\right)\right)e^{(2)^T}(t)e^{(2)}(t) \\
&\quad + \tfrac{1}{2\beta}e^{(1)^T}(t)e^{(1)}(t) + \tfrac{1}{2\alpha}e^{(2)^T}(t)e^{(2)}(t) + \left(\tfrac{1}{2\beta} + \tfrac{1}{2\alpha}\right)F(t)^T F(t) \\
&\le -\tfrac{\alpha c}{\beta}\lambda_{\min}\left(H'\right)e^{(1)^T}(t)e^{(1)}(t) + \left(\tfrac{1}{\beta}I_N - \tfrac{\beta c}{\alpha}\lambda_{\min}\left(H'\right)\right)e^{(2)^T}(t)e^{(2)}(t) \\
&\quad + \tfrac{1}{2\beta}e^{(1)^T}(t)e^{(1)}(t) + \tfrac{1}{2\alpha}e^{(2)^T}(t)e^{(2)}(t) \\
&\quad + \left(\tfrac{1}{\beta} + \tfrac{1}{\alpha}\right)\left(\rho_1^2 e^{(1)^T}(t)e^{(1)}(t) + \rho_2^2 e^{(2)^T}(t)e^{(2)}(t)\right) \\
&= \left(-\tfrac{\alpha c}{\beta}\lambda_{\min}\left(H'\right) + \tfrac{1}{2\beta} + \tfrac{1}{\beta}\rho_1^2 + \tfrac{1}{\alpha}\rho_1^2\right)e^{(1)^T}(t)e^{(1)}(t) \\
&\quad + \left(-\tfrac{\beta c}{\alpha}\lambda_{\min}\left(H'\right) + \tfrac{1}{\beta} + \tfrac{1}{2\alpha} + \tfrac{1}{\beta}\rho_2^2 + \tfrac{1}{\alpha}\rho_2^2\right)e^{(2)^T}(t)e^{(2)}(t) \\
&= -\bar{e}^T(t)\begin{bmatrix} m_1 I_N & 0_N \\ 0_N & m_2 I_N \end{bmatrix} \otimes I_n \bar{e}(t) \le -rV(t),
\end{aligned}
\tag{14}
$$

where $m_1 = \frac{\alpha c}{\beta}\lambda_{\min}\left(H'\right) - \frac{1}{2\beta} - \frac{1}{\beta}\rho_1^2 - \frac{1}{\alpha}\rho_1^2$, $m_2 = \frac{\beta c}{\alpha}\lambda_{\min}\left(H'\right) - \frac{1}{\beta} - \frac{1}{2\alpha} - \frac{1}{\beta}\rho_2^2 - \frac{1}{\alpha}\rho_2^2$, and $r = \frac{2\min\{m_1, m_2\}}{\lambda_{\max}(\Omega)}$.

When DoS attack occurs, $c = 0$ for $t \in [t_\theta, t_\theta + \tau_\theta)$, then $m_1 = -\frac{1}{2\beta} - \frac{1}{\beta}\rho_1^2 - \frac{1}{\alpha}\rho_1^2$, $m_2 = -\frac{1}{\beta} - \frac{1}{2\alpha} - \frac{1}{\beta}\rho_2^2 - \frac{1}{\alpha}\rho_2^2$ and $r < 0$, set $r_D = \frac{2}{\lambda_{\max}(\Omega)}\min\left\{-\frac{1}{2\beta} - \frac{1}{\beta}\rho_1^2 - \frac{1}{\alpha}\rho_1^2, -\frac{1}{\beta} - \frac{1}{2\alpha} - \frac{1}{\beta}\rho_2^2 - \frac{1}{\alpha}\rho_2^2\right\}$.

When the DoS attack stops, $c > 0$ for $t \in \left[t_\theta + \tau_\theta, t_{\theta+1}\right)$, then $m_1 = \frac{\alpha c}{\beta}\lambda_{\min}\left(H'\right) - \frac{1}{2\beta} - \frac{1}{\beta}\rho_1^2 - \frac{1}{\alpha}\rho_1^2$, $m_2 = \frac{\beta c}{\alpha}\lambda_{\min}\left(H'\right) - \frac{1}{\beta} - \frac{1}{2\alpha} - \frac{1}{\beta}\rho_2^2 - \frac{1}{\alpha}\rho_2^2$ and $r > 0$, set $r_S = \frac{2}{\lambda_{\max}(\Omega)}\min\left\{\frac{\alpha c}{\beta}\lambda_{\min}\left(H'\right) - \frac{1}{2\beta} - \frac{1}{\beta}\rho_1^2 - \frac{1}{\alpha}\rho_1^2, \frac{\beta c}{\alpha}\lambda_{\min}\left(H'\right) - \frac{1}{\beta} - \frac{1}{2\alpha} - \frac{1}{\beta}\rho_2^2 - \frac{1}{\alpha}\rho_2^2\right\}$.

Therefore,

$$
\begin{aligned}
\dot{V} &\le -r_D V, \text{ when } t \in [t_\theta, t_\theta + \tau_\theta), \\
\dot{V} &\le -r_S V, \text{ when } t \in \left[t_\theta + \tau_\theta, t_{\theta+1}\right).
\end{aligned}
$$

Thus,

$$
\begin{aligned}
V(t) &\le e^{-r_S(t - t_\theta - \tau_\theta)}V\left(t_\theta + \tau_\theta\right) \\
&\le e^{-r_D\tau_\theta - r_S(t - t_\theta - \tau_\theta)}V\left(t_k\right) \\
&\le V\left(t_0\right)e^{(r_S - r_D)(t - t_0)\frac{1}{T} - r_D\varphi - r_S(t - t_0 - \varphi)}.
\end{aligned}
$$

According to conditions (a_2) and (b_2)

$$(r_S - r_D)\frac{1}{T} - r_S < 0.$$

In summary, if conditions (a_2) and (b_2) in Theorem 2 are satisfied, the system can achieve group consensus, so Theorem 2 is proved. □

Remark 3 According to Definition 3, we know that the implementation of group consensus has a requirement on the duration of DoS attack. When the controller gain and the attack duration satisfy (a_2) and (b_2), respectively, group consensus of systems (7) and (8) can be reached with the distributed controller (9).

Remark 4 According to the conditions (a_1) and (a_2) of theorems 1 and 2 respectively, both first-order and second-order MASs subjected to DoS attacks need a certain amount of coupling strength to achieve group consensus. Meanwhile, $c > 0$ also implies that it is crucial for the external controls to achieve group consensus for the MASs subjected to DoS attacks. Base on the conditions (b_1) and (b_2) of theorems 1 and 2 respectively, T should be greater than a certain value when the first-order or second-order MASs subjected to DoS attacks achieve group consensus. In other words, in order to achieve group consensus for the MASs subjected to DoS attacks, the average interval of DoS attacks should be greater than one value. Additionally, the lower bounds of both coupling strength and constant T can be derived from theorems 1 and 2, respectively.

Remark 5 The existence of four assumptions is necessary. Assumption 1 ensures that the entire network has the basis for information interaction; Assumption 2 limits the duration of the DoS attack interval and ensures that the duration of the attack interval is less than an average; Assumptions 3 and 4 give the corresponding Lipschitz conditions. According to theorems 1 and 2, satisfying these assumptions can ensure group consensus of nonlinear MASs.

4 Simulation Results

In this section, numerical examples are presented to explain the effectiveness of the designed controllers and the obtained theoretical results. Simulations for both first-order MASs and second-order MASs are given.

4.1 Simulations for First-Order MASs

A MAS consisting of three leaders and three groups of ten followers is considered, and their dynamics are described by systems (1) and (2). The adjacency matrix of follower agents is

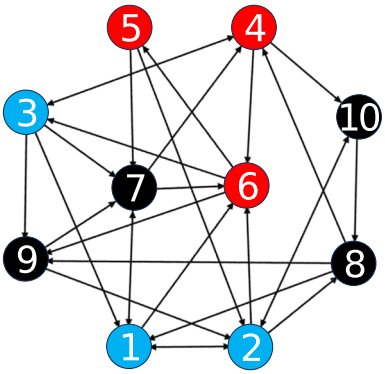

Fig. 1 The topology graph of followers

as follows:

$$A = \begin{pmatrix} 0&1&0&0&0&1&1&0&0&0 \\ 1&0&0&0&0&1&0&1&0&1 \\ 1&0&0&1&0&0&1&0&1&0 \\ 0&0&1&0&0&1&0&0&0&1 \\ 0&1&0&0&0&0&1&0&0&0 \\ 0&0&1&0&1&0&0&0&1&0 \\ 1&0&0&1&0&1&0&0&0&0 \\ 1&0&0&1&0&0&0&0&1&0 \\ 0&1&0&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0&1&0&0 \end{pmatrix}.$$

Based on the adjacency matrix, the topology of MASs, where the followers in the same group are represented by the same color, is shown in Fig. 1. Ten follower agents are divided into three subgroups. Especially, agents 1, 2 and 3 are chosen as the followers of the first subgroup, agents 4, 5 and 6 are chosen as the followers of the second subgroup, and agents 7, 8, 9 and 10 are chosen as the followers of the third subgroup.

The nonlinear function is $f(x) = \frac{1}{5}\sqrt{x^2+5}$. Obviously, function $f(x)$ is in accord with Assumption 3 with $\rho = 1/5$. In addition, set $B = \left[1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 2\right]$, implying that the first follower, fifth follower and tenth follower are pinned by the first leader, second leader and third leader, respectively. Only one agent is pinned in each subgroup.

The initial value of all followers is set in the following vector $x_0 = \left[100,\ 200,\ 300,\ 400,\ 500,\ 600,\ 700,\ 800,\ 900,\ 1000\right]$, and the initial value of three leaders x^* is set as $x_0^* = \left[20,\ 30,\ 10\right]$. By calculating, $\lambda_{\min}(H') = 0.2049$. Set $\alpha = 1$, $c = 3$ and $T = 7$. Therefore, conditions of Theorem 1 are satisfied. The trajectories of position states of both ten followers and three leaders are depicted in Fig. 2, where three thick lines in red, black and blue indicate the trajectories of three leaders. Figure 2 shows that group consensus is reached. All the followers in each subgroup track the corresponding leader of that subgroup.

In addition, the trajectories of controllers are drawn in Fig. 3, where the MASs are affected by a series of DoS attacks. As can be seen from Fig. 3, when the MASs are affected by the DoS attack, the external control fails and the corresponding external control becomes zero; When a period of DoS attack ends, the communication of the MASs is restored and the external control continues to be effective. Furthermore, the controllers of ten followers gradually tend to 0 as group consensus is asymptotically realized.

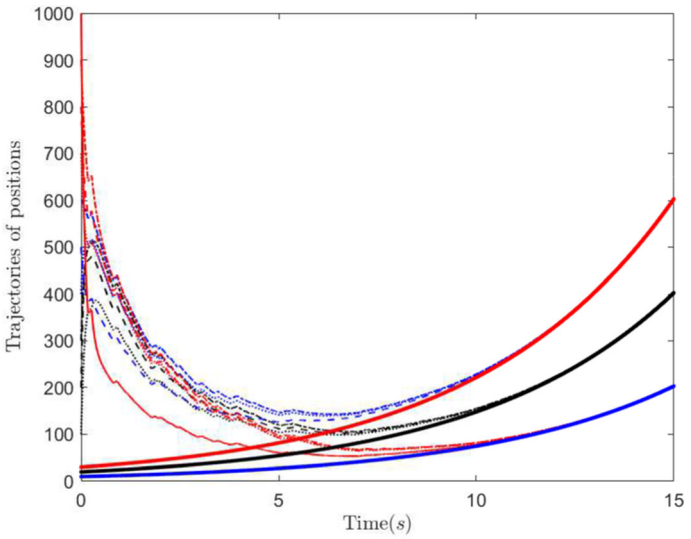

Fig. 2 The evolutions of position states of agents

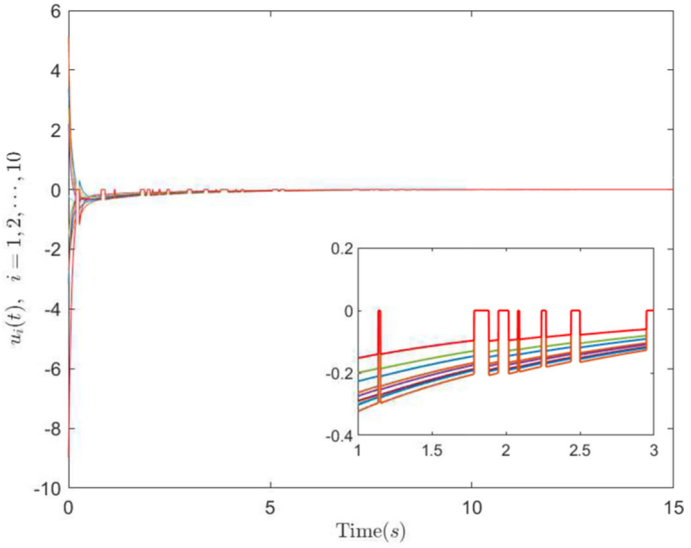

Fig. 3 The evolutions of $u_i(t), i = 1, 2, \cdots, 10$

Remark 6 Simulation results of first-order MASs show that when three groups of followers of the MASs are controlled via the controller (3), all the follower agents can asymptotically track the corresponding leaders. This also shows that the controller (3) designed in Subsect. 3.1 is effective for the first-order MASs (1)-(2).

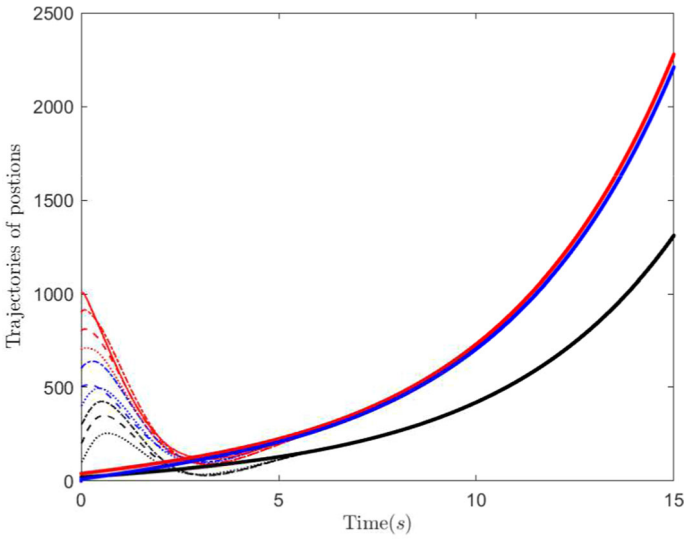

Fig. 4 The evolutions of position states of all agents

4.2 Simulations for Second-Order MASs

In this subsection, a MAS consisting of three leaders and three groups of followers is considered, and their dynamics are described by systems (7) and (8), where $f(x) = \frac{1}{20}\sqrt{x^2 + v^2 + 5}$ with $\rho_1 = 1/20$ and $\rho_2 = 1/20$. The topology of second-order MASs is the same as Fig. 1.

Select $B = [1, 0, 0, 0, 1, 0, 0, 0, 0, 2]$. The initial values of positions and velocities of followers are selected as $x_0 = [100, 200, 300, 400, 500, 600, 700, 800, 900, 1000]$, and $v_0 = [50, 100, 150, 200, 250, 300, 350, 400, 450, 500]$, respectively. The initial values of positions and velocities of leaders are set as $x_0^* = [20, 40, 10]$, and $v_0^* = [15, 25, 30]$, respectively.

Nodes 1, 2 and 3 are chosen as the first group of followers; Nodes 4, 5 and 6 are chosen as the second group of followers; Nodes 7, 8, 9 and 10 are chosen as the third group of followers. By calculating, $r_S = 0.0029$, $r_D = -0.0327$. Set $\alpha = 1$, $\beta = 1$, $c = 8$ and $T = 15$. Therefore, conditions of Theorem 2 are satisfied. The evolutions of position states and velocity states of all agents are depicted in Figs. 4 and 5, respectively.

Furthermore, the trajectories of controllers are drawn in Fig. 6. where the MASs are affected by a series of DoS attacks.

Remark 7 Simulation results of the second-order MASs show that when three groups of followers of the MASs are controlled via the controller (9), all the follower agents can asymptotically track the corresponding leaders. Therefore, the controller (9) is effective for the second-order MASs (7)–(8).

5 Conclusions

In this article, group consensus of both first-order MASs and second-order MASs under DoS attacks was investigated. According to the method of grouping, the controllers for both

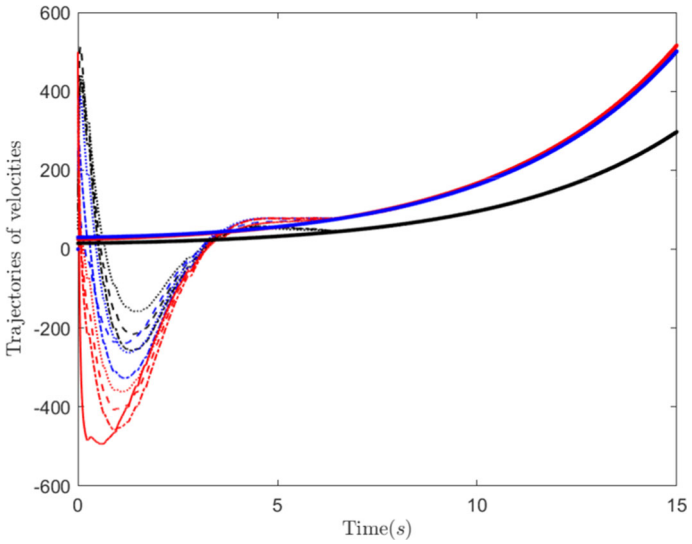

Fig. 5 The evolutions of velocity states of all agents

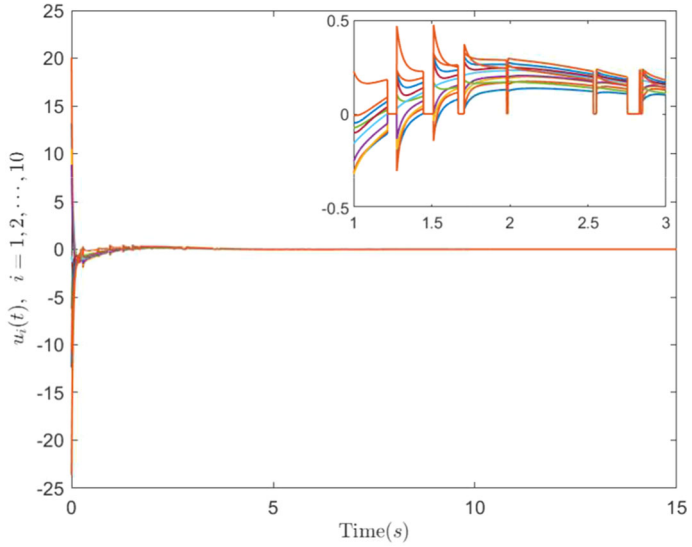

Fig. 6 The evolutions of $u_i(t), i = 1, 2, \cdots, 10$

first-order nonlinear MASs and second-order nonlinear MASs were designed. By means of the Lyapunov function method, group consensus could be achieved when control gain and durations of DoS attacks satisfied the derived conditions. The designed controller and theoretical results were explained by simulation results. In the future, group consensus of the heterogeneous MASs with switching topology and DoS attacks will be further investigated.

Acknowledgements This work was supported by the Qing Lan Project of Jiangsu Province of China and the National Natural Science Foundation of China under Grant no. 42375016.

Funding Qing Lan Project of Jiangsu Province of China, National Natural Science Foundation of China (42375016).

Data Availibility The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Zhou M, Wang P, Ding Z, Liu Z, Niu J, Shen J, He L (2023) Cooperative autonomous driving for urban intersections assisted by vehicular sensor networks. J Circuits Syst Comput 32(1):2350005
2. Jia J, Chen X, Zhang M, Li Z (2022) A distributed control for ground target tracking of nonlinear unmanned aerial vehicles formation. J Phys Conf Ser 2216(1):012062
3. Fouad B, Dirk R (2022) A review of the applications of multi-agent reinforcement learning in smart factories. Front Robot AI 9:1027340
4. Zhang Z, Chen Z, Zhang S, Li D, Wang J (2022) Static output feedback secure synchronization control for Markov jump neural networks under hybrid cyber-attacks. Appl Math Comput 430:127274
5. Wang X, Li F, Hu X, Wang J (2023) Mixed H_∞/passive synchronization for persistent dwell-time switched neural networks via an activation function dividing methodz. Appl Math Comput 442:127718
6. Xu X, Sun J, Wang C, Zou B (2022) A novel hybrid CNN-LSTM compensation model against DoS attacks in power system state estimation. Neural Process Lett 54:1597–1621
7. Mahadik S, Pawar P, Muthalagu R (2023) Edge-HetIoT defense against DDoS attack using learning techniques. Comput Secur 132:103347
8. Wang Z, Shi S, He W, Xiao M, Cao J, Gorbachev S (2023) Observer-based asynchronous event-triggered bipartite consensus of multi-agent systems under false data injection attacks. IEEE Trans Control Netw Syst 10(3):1603–1615
9. Narayanan G, Syed Ali M, Alsulami H, Stamov G, Stamova I, Ahmad B (2022) Impulsive security control for fractional-order delayed multi-agent systems with uncertain parameters and switching topology under DoS attack. Inf Sci 618:169–190
10. Bhowmick S, Halo B, Panja S (2022) Bipartite consensus control of multi-agent systems under multiple denial-of-service cyber attacks. IFAC-PapersOnLine 55(1):697–702
11. Xu B, Yang Y (2022) Group consensus of nonlinear multiagent system with switching topology under DoS attacks. Phys A 605:127969
12. Ge H, Yue D, Xie X, Dou C, Wang S (2020) Security control of cyber-physical system based on switching approach for intermittent denial-of-service jamming attack. ISA Trans 104:53–61
13. Hu W, Wang K, Hu D, Wang Y (2021) Mode-dependent switching control of bilateral teleoperation against random denial-of-service attacks. IET Cyber Phys Syst Theory Appl 7(1):16–29
14. Shi X, Li Y, Liu Q, Lin K, Chen S (2023) A fully distributed adaptive event-triggered control for output regulation of multi-agent systems with directed network. Inf Sci 626:60–74
15. Liu C, Liu L (2023) Finite-horizon robust event-triggered control for nonlinear multi-agent systems with state delay. Neural Process Lett 55:5167–5191
16. Tian Y, Li H, Han Q (2023) Finite-time average consensus of directed second-order multi-agent systems with Markovian switching topology and impulsive disturbance. Neural Comput Appl 35(11):8575–8588
17. Li Y, Wang X, Sun J, Wang G, Chen J (2023) Data-driven consensus control of fully distributed event-triggered multi-agent systems. Sci China Inf Sci 66(5):152202

18. Ni J, Zhao Y, Cao J, Li W (2022) Fixed-time practical consensus tracking of multi-agent systems with communication delay. IEEE Trans Netw Sci Eng 9(3):1319–1334
19. Zhang Y, Wu Z, Shi P (2023) Resilient event-/self-triggering leader-following consensus control of multiagent systems against DoS attacks. IEEE Trans Ind Inform 19(4):5925–5934
20. Duan Z, Wei A, Zhang X, Mu R (2023) Event-triggered bipartite consensus for nonlinear multi-agent systems under switching topologies: a time-varying gain method. J Frankl Inst 360(7):4880–4895
21. Zhou Z, Zhang W, Xiu R (2023) Bipartite leader-follower consensus for nonlinear signed networks with impulsive control. Neural Comput Appl 35:4133–4143
22. Ma C, Zhao W, Zhao Y (2018) Bipartite consensus of discrete-time double-integrator multi-agent systems with measurement noise. J Syst Sci Complex 31:1525–1540
23. Pu X, Zhang L (2023) The couple-group consensus of heterogeneous multi-agent systems with different leaders under Markov switching in cooperative-competitive networks. Neural Process Lett 55:1799–1831
24. Wen G, Yu Y, Peng Z, Wang H (2016) Dynamical group consensus of heterogenous multi-agent systems with input time delays. Neurocomputing 175:278–286
25. Li X, Yu Z, Li Z, Wu N (2021) Group consensus via pinning control for a class of heterogeneous multi-agent systems with input constraints. Inf Sci 542:247–262
26. Li H, Cao J (2023) Event-triggered group consensus for one-sided Lipschitz multi-agent systems with input saturation. Commun Nonlinear Sci Numer Simul 121:107234
27. Song H, Yu L, Hu H (2012) Group consensus in multi-agent systems via pinning control. Control Theory Appl 29(6):765–772
28. You X, Xu J, Jia X (2022) Distributed cooperative control for cyber-physical system under denial-of-service attack. Control Eng China 29(6):971–976