ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理
Chinese Physics B

# Group consensus of multi-agent systems subjected to cyber-attacks

Hai-Yun Gao(高海云), Ai-Hua Hu(胡爱花), Wan-Qiang Shen(沈莞蔷), Zheng-Xian Jiang(江正仙)

**Citation:**Chin. Phys. B . 2019, 28(6): 060501. **doi:** 10.1088/1674-1056/28/6/060501
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Successive lag cluster consensus on multi-agent systems via delay-dependent impulsive control

Xiao-Fen Qiu(邱小芬), Yin-Xing Zhang(张银星), Ke-Zan Li(李科赞)
Chin. Phys. B . 2019, 28(5): 050501. **doi:** 10.1088/1674-1056/28/5/050501

## Mean-square composite-rotating consensus of second-order systems with communication noises

Li-po Mo(莫立坡), Shao-yan Guo(郭少岩), Yong-guang Yu(于永光)
Chin. Phys. B . 2018, 27(7): 070504. **doi:** 10.1088/1674-1056/27/7/070504

## Time-varying formation for general linear multi-agent systems via distributed event-triggered control under switching topologies

Jin-Huan Wang(王金环), Yu-Ling Xu(许玉玲), Jian Zhang(张建), De-Dong Yang(杨德东)
Chin. Phys. B . 2018, 27(4): 040504. **doi:** 10.1088/1674-1056/27/4/040504

## Stochastic bounded consensus of second-order multi-agent systems in noisy environment

Hong-Wei Ren(任红卫), Fei-Qi Deng(邓飞其)
Chin. Phys. B . 2017, 26(10): 100506. **doi:** 10.1088/1674-1056/26/10/100506

## Tracking consensus for nonlinear heterogeneous multi-agent systems subject to unknown disturbances via sliding mode control

Xiang Zhang(张翔), Jin-Huan Wang(王金环), De-Dong Yang(杨德东), Yong Xu(徐勇)
Chin. Phys. B . 2017, 26(7): 070501. **doi:** 10.1088/1674-1056/26/7/070501

---

# Group consensus of multi-agent systems subjected to cyber-attacks*

Hai-Yun Gao(高海云), Ai-Hua Hu(胡爱花)†, Wan-Qiang Shen(沈莞蔷), and Zheng-Xian Jiang(江正仙)

*School of Science, Jiangnan University, Wuxi* 214122, *China*

(Received 13 January 2019; revised manuscript received 3 April 2019; published online 8 May 2019)

In this paper, we investigate the group consensus for leaderless multi-agent systems. The group consensus protocol based on the position information from neighboring agents is designed. The network may be subjected to frequent cyber-attacks, which is close to an actual case. The cyber-attacks are assumed to be recoverable. By utilizing algebraic graph theory, linear matrix inequality (LMI) and Lyapunov stability theory, the multi-agent systems can achieve group consensus under the proposed control protocol. The sufficient conditions of the group consensus for the multi-agent networks subjected to cyber-attacks are given. Furthermore, the results are extended to the consensus issue of multiple subgroups with cyber-attacks. Numerical simulations are performed to demonstrate the effectiveness of the theoretical results.

**Keywords:** multi-agent systems, group consensus, cyber-attacks, multiple subgroups

**PACS:** 05.45.Xt, 07.05.Dz, 02.3.Yy **DOI:** 10.1088/1674-1056/28/6/060501

## 1. Introduction

The consensus for multi-agent systems has been intensively discussed in the past decade, due to successful applications in various areas, including formation control,[1] vehicle systems,[2] large-scale sensors,[3] obstacle avoidance,[4] *etc*. It is well-known that the foremost goal of consensus problem is to design an appropriate control protocol,[5] so that all agents can asymptotically attain a consistent quantity based on local interactions.

At present, it should be noted that most of results involve complete consensus.[6–12] However, in many real-world situations, the multi-agent systems have different cooperative tasks, and it is more general to trigger agents in the same subgroup to achieve a consistent state, while in different subgroups they behave non-identically, which can be denoted by group consensus.[13] Moreover, the phenomenon of group consensus is ubiquitous in nature and human society, such as multi-species foraging groups, the pattern formation of bacteria colonies, a school of fish and formation of opinion.[14] Obviously, group consensus is more suitable for addressing complex and flexible problems than complete consensus.

Recently, the group consensus of multi-agent systems has received much attention from researchers, and group consensus on first-order,[15,16] second-order,[13,17] or heterogeneous agents[18,19] have yielded some research results. It is found that the subgroups need to meet an in-degree balanced couple, and the Laplacian matrix $\boldsymbol{L}$ is not similar to that in complete consensus because of the introduction of competition and cooperation mechanism.[13,16] Consequently, it is much more difficult to study group consensus than complete consensus. By now, directed topology, fixed topologies, switching topologies, communication delays, nonlinear input constraints, pinning control and event-triggered control have also been introduced to study the group consensus issue; see, *e.g.*, Refs. [15]–[23]. However, many existing results of group consensus problem include the virtual leader, which may not ensure that the controllers are distributed; for further information, see Ref. [24]. In Ref. [25], distributed feedback control was used to achieve the group consensus of multi-agent systems without virtual leader. Therefore, in this paper we will further investigate the problem of leaderless group consensus.

In addition, multi-agent systems are often in an indeterminate communication environment, just like networks under cyber-attacks. Some results of the consensus problem with cyber-attack have been published; for example, in Refs. [26]–[28] Cyber-attacks may destroy the agents or the communication links between agents,[29] thus, cyber-attacks can weaken the stability of the networked systems and undermine the system performance.[30] In fact, with the development of network information technology, cyber security has become a common issue. The synchronization of complex dynamical networks under cyber-attacks has been explored in Ref. [31]. By applying new control strategies, the authors in Ref. [32] studied the stability of the network subjected to cyber-attacks, which would disrupt the communication channels existing in both controllers and observers. Distributed tracking control was proposed for multi-agent systems under two types of attacks, which are connectivity-maintained attacks and connectivity-broken attacks.[33] Inspired by this discussion, in this paper we further focus on the group consensus of multi-agent systems under cyber-attacks. Comparing with the existing papers, the main contributions of this paper include: (i) the multi-agent

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61807016 and 61772013) and the Natural Science Foundation of Jiangsu Province, China (Grant No. BK20181342).

†Corresponding author. E-mail: aihuahu@126.com

© 2019 Chinese Physical Society and IOP Publishing Ltd 

system subjected to cyber-attacks is considered for group consensus, and an effective algorithm and optimization problem for selecting parameter are designed; (ii) the results of consensus issue for multiple subgroups with cyber-attacks are given. Based on the algebraic graph theory, matrix theory, and Lyapunov stability method, some sufficient conditions are derived to ensure the group consensus with cyber-attacks.

The rest of this paper is organized as follows. In Section 2 the preliminaries about graph theory and the problem formulation are given. In Section 3 the results of consensus problem for two subgroups and multiple subgroups with cyber-attacks are obtained. In Section 4 the numerical examples are presented, and finally in Section 5 some conclusions are drawn from the present study.

The following notations are used throughout this paper: $R$ denotes the set of real numbers, $R^{(n+m)\times(n+m)}$ the set of $(n+m)\times(n+m)$ real matrices. Notation diag$\{\cdots\}$ is a diagonal matrix, $\mathbf{1}=[1\cdots 1]^{\mathrm{T}}$ has a proper dimension, $\mathbf{0}$ is the zero matrix with an appropriate dimension, and $\|\cdot\|$ is the Euclidean norm. For any real symmetric matrix $\boldsymbol{P}$, $\boldsymbol{P}>0$ indicates that $\boldsymbol{P}$ is a positive matrix.

## 2. Preliminaries and problem formulation

In this section, some essential concepts on graph theory in Ref. [34] and problem formulation are stated.

### 2.1. Preliminaries

In general, the topology of a multi-agent system is described as a weighted directed graph $G=(V,E,\boldsymbol{A})$, where $V=\{v_1,v_2,\ldots,v_{n+m}\}$ is the set of nodes representing a network containing $n+m$ nodes, $E\subseteq V\times V$ is the set of directed links, and $\boldsymbol{A}=[a_{ij}]\in R^{(n+m)\times(n+m)}$ is the weighted adjacency matrix. Define $a_{ij}\neq 0$ if and only if there is a directed link $(v_j,v_i)\in E$; otherwise, $a_{ij}=0$. Here, we assume $a_{ii}=0$ for all $v_i\in V$. The subscript set of the agents in the group $G$ is $I=\{1,2,\ldots,n,\ldots,n+m\}$. Assume $N_i=\{v_j\in V:(v_j,v_i)\in E\}$ to be the neighboring set of node $v_i$. The Laplacian matrix $\boldsymbol{L}=[l_{ij}]\in R^{(n+m)\times(n+m)}$ is denoted with $l_{ij}=-a_{ij}$ when $i\neq j$, and $l_{ii}=\sum_{k=1,k\neq i}^{n+m}a_{ik}$ for $i=j$. Moreover, the in-degree and out-degree of node $v_i$ are denoted respectively by

$$\deg_{\mathrm{in}}^{(G)}(v_i)=\sum_{j=1}^{n+m}a_{ij},\quad \deg_{\mathrm{out}}^{(G)}(v_i)=\sum_{j=1}^{n+m}a_{ji}.$$

In graph $G$, a directed path is a finite sequence of connected edges. If $G$ possesses a root node with directed paths to all other nodes, then $G$ is said to have a directed spanning tree.

### 2.2. Problem formulation

Suppose that there are $n+m$ nodes in the multi-agent system, then each agent will have the dynamics as follows:

$$\dot{x}_i(t)=u_i(t),\quad i\in I=\{1,2,\ldots,n,\ldots,n+m\},\tag{1}$$

where $x_i(t)\in R$ is the position of the agent $v_i$ at time $t$, and $u_i(t)\in R$ is the control protocol to be designed later.

First, consider that $n+m$ agents are all split into two subgroups. Suppose that $n$ agents ($V_1=\{v_1,\ldots,v_n\}$) belong to the subgroup $G_1=(V_1,E_1,\boldsymbol{A}_1)$ and the last $m$ agents ($V_2=\{v_{n+1},\ldots,v_{n+m}\}$) are in the subgroup $G_2=(V_2,E_2,\boldsymbol{A}_2)$. Let $I_1=\{1,2,\ldots,n\}$ and $I_2=\{n+1,n+2,\ldots,n+m\}$ be the subscript sets of the agents in each group, respectively.

**Remark 1** It is clear that $V=V_1\cup V_2$ and $I=I_1\cup I_2$, and the neighboring sets of node $v_i$ are correspondingly defined as $N_{1i}=\{v_j\in V_1|(v_j,v_i)\in E\}$ and $N_{2i}=\{v_j\in V_2|(v_j,v_i)\in E\}$. Thus, one has $N_i=N_{1i}\cup N_{2i}$. Furthermore, the concept of in-group links and out-group links are presented in this paper, where in-group refers to that the links exist between nodes in the same subgroup, and out-group implies that the links exist between nodes in the different subgroups.

The following group consensus protocol is presented for each agent:

$$u_i(t)=\begin{cases}\sum\limits_{v_j\in N_{1i}}a_{ij}(x_j(t)-x_i(t))+\sum\limits_{v_j\in N_{2i}}a_{ij}x_j(t), & \forall i\in I_1,\\ \sum\limits_{v_j\in N_{1i}}a_{ij}x_j(t)+\sum\limits_{v_j\in N_{2i}}a_{ij}(x_j(t)-x_i(t)), & \forall i\in I_2,\end{cases}\tag{2}$$

where $a_{ij}\geq 0$ for all $(i,j)\in\Delta=\{(i,j):i\in I_1,j\in I_1\}\cup\{(i,j):i\in I_2,j\in I_2\}$; otherwise, $a_{ij}\in R$ for all $(i,j)\in\Lambda=\{(i,j):i\in I_1,j\in I_2\}\cup\{(i,j):i\in I_2,j\in I_1\}$.

**Assumption 1** $\sum_{j=n+1}^{n+m}a_{ij}=0,\forall i\in I_1;\sum_{j=1}^{n}a_{ij}=0,\forall i\in I_2$.

**Remark 2** Obviously, both cooperation interaction and competition interaction are considered for the agents, namely, $a_{ij}>0$ indicates that the agents $v_i$ and $v_j$ are cooperative, while $a_{ij}<0$ can be regarded as the agents $v_i$ and $v_j$ being competitive, which is close to a practical system. Assumption 1 implies that an interaction in-degree balance exists between two subgroups.

**Definition 1**[16] (Group consensus) Under the group consensus protocol (2), system (1) is said to realize group consensus asymptotically, if for any initial condition, the states of agents satisfy:

(i) $\lim\limits_{t\to\infty}\|x_i(t)-x_j(t)\|=0,\forall i,j\in I_1$;

(ii) $\lim\limits_{t\to\infty}\|x_i(t)-x_j(t)\|=0,\forall i,j\in I_2$.

Define the group consensus error of system (1) as follows:

$$\begin{cases}e_i^{(1)}(t)=x_1(t)-x_{i+1}(t), & \forall i=1,2,\ldots,n-1,\\ e_i^{(2)}(t)=x_{n+1}(t)-x_{i+2}(t), & \forall i=n,\ldots,n+m-2.\end{cases}\tag{3}$$

For the sake of obtaining a compact form of the dynamics of the agents, one can denote

$$x(t)=(x_1(t),\ldots,x_n(t),x_{n+1}(t),\ldots,x_{n+m}(t))^{\mathrm{T}}.$$

Then, the multi-agent system (1) under protocol (2) can be represented as

$$\dot{x}(t)=-\boldsymbol{L}x(t),\tag{4}$$

where $\boldsymbol{L}$ is the Laplacian matrix of the graph representing communication topology.

Before putting forward the main results, a necessary lemma is stated.

**Lemma 1**[25] Under the proposed group consensus error (3), system (1) is transformed into the following reduced-order system:

$$\dot{e}(t) = \boldsymbol{H}e(t), \tag{5}$$

where

$$\begin{aligned} &e(t) = ((e^{(1)}(t))^{\mathrm{T}},\ (e^{(2)}(t))^{\mathrm{T}})^{\mathrm{T}},\\ &e^{(1)}(t) = (e_1^{(1)}(t),\ldots,\ e_{n-2}^{(1)}(t), e_{n-1}^{(1)}(t))^{\mathrm{T}},\\ &e^{(2)}(t) = (e_n^{(2)}(t),\ e_{n+1}^{(2)}(t),\ldots, e_{n+m-3}^{(2)}(t), e_{n+m-2}^{(2)}(t))^{\mathrm{T}}, \end{aligned}$$

and $\boldsymbol{H} = -\boldsymbol{BLF} \in R^{(n+m-2)\times(n+m-2)}$. Additionally, it follows from Ref. [25] that $\boldsymbol{B} = \mathrm{diag}\{\boldsymbol{B}_1, \boldsymbol{B}_2\} \in R^{(n+m-2)\times(n+m)}$ with $\boldsymbol{B}_1 = \begin{bmatrix} 1 & -\boldsymbol{I}_{n-1} \end{bmatrix}$, $\boldsymbol{B}_2 = \begin{bmatrix} 1 & -\boldsymbol{I}_{m-1} \end{bmatrix}$, and $\boldsymbol{F} = \mathrm{diag}\{\boldsymbol{F}_1, \boldsymbol{F}_2\} \in R^{(n+m)\times(n+m-2)}$ with $\boldsymbol{F}_1 = \begin{bmatrix} \boldsymbol{0} & -\boldsymbol{I}_{n-1} \end{bmatrix}^{\mathrm{T}}$, $\boldsymbol{F}_2 = \begin{bmatrix} \boldsymbol{0} & -\boldsymbol{I}_{m-1} \end{bmatrix}^{\mathrm{T}}$.

**Remark 3** Through this analysis, if the reduced-order system (5) satisfies the condition $\lim\limits_{t\to\infty} \|e(t)\| = 0$, then one can obtain that system (1) under protocol (2) will asymptotically achieve the group consensus.

### 2.3. Multi-agent systems subjected to cyber-attacks

Since the mass data transmit through the channel of communication topology, which is vulnerable to attack, cyber-attacks will be introduced into the network environment.

First, the definition of cyber-attacks is given.

**Definition 2**[29] A cyber-attack is called "a successful but recoverable attack" if the attack changes the directed network $G$ containing a spanning tree into $\widehat{G}$ that does not contain a spanning tree. However, after a short period of time, the original directed path of $G$ can be reverted. In other words, $\widehat{G}$ can be reconstructed into $G$.

Figure 1 shows the communication topology graphs under the cyber-attacks. Obviously, $t_1 > t_0$ denotes the time when the cyber-attacks occur, and $t_2$ refers to the time when the recovered system works. Specifically, from $t_1$ to $t_2$, the network $G$ becomes paralyzed. Since the influence of the cyber-attacks vanishes at $t_2$, the topology of network $G$ will be reverted to its original setting during $t_2$ to $t_3$. Then next attack occurs at time $t_3$. Without loss of generality, suppose that $t_{2k+1}(k \in N)$ is the moment of attack and the network works well during $[t_{2k}, t_{2k+1})$, therefore, the network is paralyzed during $[t_{2k+1}, t_{2k+2})$, and $t^{2k+1} = t_{2k+2} - t_{2k+1}$ is denoted as the duration of the attack.

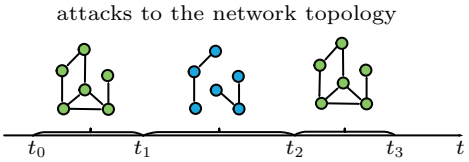



**Fig. 1.** Evolution of network topology subjected to cyber-attacks. Green network graph represents the original network graph, and blue network graph denotes the network under cyber-attacks without any directed spanning tree.

It can be seen from Fig. 1 that the cyber-attacks will affect the communication channels; therefore, an attack will destroy original links. To achieve group consensus, it is necessary to satisfy the in-degree balanced condition for subgroups. Thus, in this paper we consider that the cyber-attacks just affect the links existing between nodes in the same subgroup, in other words, cyber-attacks will attack in-group links of $G_1$ and $G_2$.

Let $x(t) = ((x^1(t))^{\mathrm{T}}, (x^2(t))^{\mathrm{T}})^{\mathrm{T}}$ represent the states of the agents, with state $x^1(t) = (x_1, x_2, \ldots, x_n)^{\mathrm{T}}$ and $x^2(t) = (x_{n+1}, x_{n+2}, \ldots, x_{n+m})^{\mathrm{T}}$, respectively. The $\boldsymbol{L}$ has a block form

$$\boldsymbol{L} = \begin{pmatrix} \boldsymbol{L}_{11} & \boldsymbol{L}_{12} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22} \end{pmatrix}, \tag{6}$$

where $\boldsymbol{L}_{12} \in R^{n\times m}$ and $\boldsymbol{L}_{21} \in R^{m\times n}$, and $\boldsymbol{L}_{11} \in R^{n\times n}$ and $\boldsymbol{L}_{22} \in R^{m\times m}$ are the Laplacian matrices of two subgroups, respectively. Thus, the multi-agent system (1) can be represented as

$$\begin{cases} \dot{x}^1(t) = -\boldsymbol{L}_{11}x^1(t) - \boldsymbol{L}_{12}x^2(t), \\ \dot{x}^2(t) = -\boldsymbol{L}_{21}x^1(t) - \boldsymbol{L}_{22}x^2(t). \end{cases} \tag{7}$$

Apparently, according to Lemma 1, the decomposition of $\boldsymbol{H}$ is

$$\boldsymbol{H} = \begin{pmatrix} -\boldsymbol{B}_1\boldsymbol{L}_{11}\boldsymbol{F}_1 & -\boldsymbol{B}_1\boldsymbol{L}_{12}\boldsymbol{F}_2 \\ -\boldsymbol{B}_2\boldsymbol{L}_{21}\boldsymbol{F}_1 & -\boldsymbol{B}_2\boldsymbol{L}_{22}\boldsymbol{F}_2 \end{pmatrix}, \tag{8}$$

where $-\boldsymbol{B}_1\boldsymbol{L}_{11}\boldsymbol{F}_1 \in R^{(n-1)\times(n-1)}$, $-\boldsymbol{B}_1\boldsymbol{L}_{12}\boldsymbol{F}_2 \in R^{(n-1)\times(m-1)}$, $-\boldsymbol{B}_2\boldsymbol{L}_{21}\boldsymbol{F}_1 \in R^{(m-1)\times(n-1)}$, and $-\boldsymbol{B}_2\boldsymbol{L}_{22}\boldsymbol{F}_2 \in R^{(m-1)\times(m-1)}$.

Then, group consensus error (5) can be rewritten equivalently as

$$\begin{cases} \dot{e}^{(1)}(t) = -\boldsymbol{B}_1\boldsymbol{L}_{11}\boldsymbol{F}_1e^{(1)}(t) - \boldsymbol{B}_1\boldsymbol{L}_{12}\boldsymbol{F}_2e^{(2)}(t), \\ \dot{e}^{(2)}(t) = -\boldsymbol{B}_2\boldsymbol{L}_{21}\boldsymbol{F}_1e^{(1)}(t) - \boldsymbol{B}_2\boldsymbol{L}_{22}\boldsymbol{F}_2e^{(2)}(t). \end{cases} \tag{9}$$

In the time intervals $[t_{2k+1}, t_{2k+2})$, suppose that in-group links of $G_1$ and $G_2$ are subjected to the $a(a > 0)$ types of cyber-attacks simultaneously. Denote the corresponding Laplacian matrix of the communication topology $G_1$ as $\boldsymbol{L}_{11}^{\sigma(t)}$ and $G_2$ as $\boldsymbol{L}_{22}^{\sigma(t)}$, $\sigma(t) \in \{1, 2, \ldots, a\}$ as a piecewise constant function. Then equation (7) can be rewritten as

$$\begin{cases} \dot{x}^1(t) = -\boldsymbol{L}_{11}^{\sigma(t)}x^1(t) - \boldsymbol{L}_{12}x^2(t), \\ \dot{x}^2(t) = -\boldsymbol{L}_{21}x^1(t) - \boldsymbol{L}_{22}^{\sigma(t)}x^2(t), \end{cases} \tag{10}$$

and the dynamics of the group consensus error (9) can also be expressed as follows:

$$\begin{cases} \dot{e}^{(1)}(t) = -\boldsymbol{B}_1\boldsymbol{L}_{11}^{\sigma(t)}\boldsymbol{F}_1e^{(1)}(t) - \boldsymbol{B}_1\boldsymbol{L}_{12}\boldsymbol{F}_2e^{(2)}(t), \\ \dot{e}^{(2)}(t) = -\boldsymbol{B}_2\boldsymbol{L}_{21}\boldsymbol{F}_1e^{(1)}(t) - \boldsymbol{B}_2\boldsymbol{L}_{22}^{\sigma(t)}\boldsymbol{F}_2e^{(2)}(t). \end{cases} \tag{11}$$

**Remark 4** Since the network is subjected to different types of cyber-attacks, the values of $t^{2k+1}$ may be non-identical.

**Assumption 2** Assume that there exist two positive constants $T_m$ and $T_M$, so that $T_m < t_{k+1} - t_k < T_M$, $k \in N$.

**Remark 5** On the one hand, in order to achieve group consensus with cyber-attacks, the stability of the attacked system should be available. Therefore, the Zeno's behavior must be excluded, which means that the dwell time $t_{k+1} - t_k$ should be positive, accordingly, suppose that the value of lower bound $T_m$ exists. On the other hand, it is impossible that the network is always paralyzed or working, then assumption of the existence of an upper bound for $t_{k+1} - t_k$ is consistent with the realistic situation.

**Assumption 3** Subgraph of each group in system (1) is assumed to contain a directed spanning tree.

**Remark 6** For system (1), assume that a directed spanning tree exists in each group. Thus, information about the root node can be diffused in each group, which guarantees the feasibility of the group consensus.

**Remark 7** Based on Definition 2, the cyber-attacks considered in this paper can be "successful" due to Assumption 3.

## 3. Main results

In this section, the main theoretical results are given and discussed.

### 3.1. Group consensus in multi-agent systems with two subgroups

To achieve group consensus in multi-agent system under cyber-attacks, we introduce the following algorithm to obtain the corresponding parameters.

**Algorithm 1**

i) Solve the following linear matrix inequality (LMI)

$$(\boldsymbol{BLF})^{\mathrm{T}}\boldsymbol{Q} + \boldsymbol{Q}(\boldsymbol{BLF}) > 0, \tag{12}$$

then a matrix $\boldsymbol{Q} > 0$ will be obtained.

ii) Search for a positive constant $\alpha$ to satisfy the following LMI:

$$(\boldsymbol{BLF})^{\mathrm{T}}\boldsymbol{Q} + \boldsymbol{Q}(\boldsymbol{BLF}) - \alpha\boldsymbol{Q} > 0. \tag{13}$$

Next, the following main theorem is established.

**Theorem 1** Consider that in-group links of $G_1$ and $G_2$ are subjected to cyber-attacks at the same time, and the cyber-attacks can be recovered. Suppose that Assumptions 1–3 hold, and LMIs (12) and (13) have feasible solutions. Furthermore, if the following condition holds:

$$-\gamma(t_{2k+2} - t_{2k+1}) + \alpha(t_{2k+1} - t_{2k}) > \varepsilon, \tag{14}$$

where $\varepsilon > 0$, and $\gamma$ is determined by converting the optimization problem into minimizing $\gamma$ subject to

$$\boldsymbol{Q}\left(\boldsymbol{B}\begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} \end{pmatrix}\boldsymbol{F}\right) + \left(\boldsymbol{B}\begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} \end{pmatrix}\boldsymbol{F}\right)^{\mathrm{T}}\boldsymbol{Q} + \gamma\boldsymbol{Q} > 0, \tag{15}$$

then the group consensus of multi-agent system (1) with cyber-attacks can be achieved.

**Proof** Construct the Lyapunov function candidate as follows:

$$V(t) = e^{\mathrm{T}}(t)\boldsymbol{Q}e(t), \tag{16}$$

where $\boldsymbol{Q} > 0$ is a solution for inequality (12) in Algorithm 1.

For $t \in [t_{2k}, t_{2k+1})$, $k \in N$, with no cyber-attack occurring, according to Eq. (13), we have

$$\begin{aligned} \dot{V}(t) &= e^{\mathrm{T}}(t)((-\boldsymbol{BLF})^{\mathrm{T}}\boldsymbol{Q} - \boldsymbol{Q}(\boldsymbol{BLF}))e(t) \\ &\le -\alpha e^{\mathrm{T}}(t)\boldsymbol{Q}e(t). \end{aligned} \tag{17}$$

When $t \in [t_{2k+1}, t_{2k+2})$, $k \in N$, cyber-attacks affect in-group links, therefore, the corresponding topology graph will change. Take the derivative of each $V(t)$ with respect to $t$ on the trajectory of error system (11) and select $\gamma$ in view of optimization problem (15), then we will have

$$\begin{aligned} \dot{V}(t) &= e^{\mathrm{T}}(t)\left(\boldsymbol{Q}(-\boldsymbol{B}\begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} \end{pmatrix}\boldsymbol{F}\right) \\ &\quad - \left(\boldsymbol{B}\begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} \end{pmatrix}\boldsymbol{F}\right)^{\mathrm{T}}\boldsymbol{Q})e(t) \\ &\le \gamma e^{\mathrm{T}}(t)\boldsymbol{Q}e(t). \end{aligned} \tag{18}$$

By combining Eqs. (17) and (18), one can obtain that

$$V(t_{2k+2}) < \mathrm{e}^{-\alpha(t_{2k+1}-t_{2k})+\gamma(t_{2k+2}-t_{2k+1})}V(t_{2k}). \tag{19}$$

Substituting condition (14) into the above inequality (19) leads to

$$V(t_{2k+2}) < \mathrm{e}^{-\varepsilon}V(t_{2k}). \tag{20}$$

According to the fact that $\varepsilon > 0$ and time intervals $[t_{2k}, t_{2k+2})$ are bounded, we can easily conclude that $\lim_{t\to\infty}\|e(t)\| = 0$. This proof demonstrates that the group consensus of multi-agent system (1) with cyber-attacks is achieved.

**Remark 8** Actually, the optimization problem (15) is a convex optimization issue, which can be directly solved by the "mincx" LMI toolbox in MATLAB. The optimization method is also applied to the control of complex dynamic networks in Ref. [32]. In this paper, we mainly use the optimization technique to solve the problem of group consensus.

**Remark 9** Under condition (14), *i.e.*, $-\gamma(t_{2k+2} - t_{2k+1}) + \alpha(t_{2k+1} - t_{2k}) > \varepsilon$, the minimum $\gamma$ can extend the range of feasible solutions for this condition.

In view of Remark 5, one can derive the following corollary.

**Corollary 1** Consider that in-group links of $G_1$ and $G_2$ are subjected to cyber-attacks at the same time, and the cyber-attacks can be recovered. Suppose that Assumptions 1–3 hold, LMIs (12) and (13) have feasible solutions, and obtain a parameter $\gamma$ by optimization problem (15). Furthermore, if the following condition holds:

$$-\gamma T_M + \alpha T_m > \varepsilon, \tag{21}$$

where $\varepsilon > 0$, then group consensus of multi-agent system (1) with cyber-attacks can be achieved.

### 3.2. Group consensus in multi-agent systems with multiple subgroups

In this subsection, we mainly extend the above results to the consensus issue of multiple subgroups with cyber-attacks.

Suppose that the agents in system (1) can be partitioned into $q$ groups, *i.e.*, there are $q$ proper subgroups $(G_r, V_r, E_r)$, $r \in \varsigma = \{1, 2, \ldots, q\}$. The weighted directed graph $(G, V, E)$ is considered to have a set of nodes $V = \{v_1, v_2, \ldots, v_N\}$. Let $0 = n_0 < n_1 < \ldots < n_r \ldots < n_q = N$, then, the $r$-th subgroup $G_r$ has the node set $V_r = \{v_{n_{r-1}+1}, \ldots, v_{n_r}\}$ and the state $x^r(t) = (x_{n_{r-1}+1}(t), \ldots, x_{n_r}(t))^{\mathrm{T}}$. Besides, the indexes of agents in $G_r$ are described as a finite set $I_r = \{n_{r-1}+1, \ldots, n_r\}$.

For multi-agent system (1), we give the following consensus protocol:

$$\begin{aligned} u_i(t) = & \sum_{v_j \in N_{\delta_i, i}} a_{ij}(x_j(t) - x_i(t)) + \sum_{v_j \in N_{r,i}, r \neq \delta_i} a_{ij} x_j(t) \\ & i \in I = \{1, 2, \ldots, N\}, \end{aligned} \tag{22}$$

where $\delta_i \in \varsigma$, $r \in \varsigma$, and $a_{ij} \geq 0$ for all $i, j \in I_r$; $a_{ij} \in R$, if nodes $v_i$ and $v_j$ are in different subgroups.

Next, the assumption, definition and lemma are given.

**Assumption 4** $\sum_{j=n_{s-1}+1}^{n_s} a_{ij} = 0, \forall i \in I_r, \forall s \in \varsigma, s \neq r$.

**Remark 10** Assumption 4 means that the in-degree balanced condition exists between any two subgroups.

**Definition 3** Multi-agent system (1) with multiple subgroups is said to achieve group consensus asymptotically under protocol (22), if for any initial condition, the states of agents satisfy

$$\lim_{t \to \infty} \left\| x_i(t) - x_j(t) \right\| = 0, \forall i, j \in I_r, r = 1, 2, \ldots, q.$$

Denote the group consensus error vector as

$$e_{j-r}^{(r)}(t) = x_{n_{r-1}+1}(t) - x_j(t) \ \ \forall j \in I_r \setminus \{n_{r-1}+1\}. \tag{23}$$

According to Lemma 1, one can obtain a lemma below.

**Lemma 2** Under the proposed consensus error (23), system (1) is transformed into the following reduced-order system

$$\dot{e}(t) = -\boldsymbol{BLF} e(t), \tag{24}$$

where $-\boldsymbol{BLF} \in R^{(N-q)\times(N-q)}$. Furthermore,

$$\boldsymbol{B} = \mathrm{diag}\{\boldsymbol{B}_1, \boldsymbol{B}_2, \ldots, \boldsymbol{B}_r, \ldots, \boldsymbol{B}_q\} \in R^{(N-q)\times N}$$

with $\boldsymbol{B}_r = \left[ \boldsymbol{1} \ -\boldsymbol{I}_{n_r - n_{r-1}-1} \right]$, and

$$\boldsymbol{F} = \mathrm{diag}\{\boldsymbol{F}_1, \boldsymbol{F}_2, \boldsymbol{F}_3, \ldots, \boldsymbol{F}_q\} \in R^{N\times(N-q)}$$

with $\boldsymbol{F}_q = \left[ \boldsymbol{0} \ -\boldsymbol{I}_{n_q - n_{q-1}-1} \right]^{\mathrm{T}}$.

Obviously, the error vector

$$e(t) = \left( (e^{(1)}(t))^{\mathrm{T}}, (e^{(2)}(t))^{\mathrm{T}}, \ldots, (e^{(q)}(t))^{\mathrm{T}} \right)^{\mathrm{T}} \in R^{N-q}$$

can describe the error between the agents in the same subgroup.

**Remark 11** Group consensus of system (1) with multiple subgroups under protocol (22) is equivalent to the asymptotical stability of error system (24), that is, $\lim_{t\to\infty} \|e(t)\| = 0$.

In the time intervals $[t_{2k+1}, t_{2k+2})$, suppose that the in-group links of $G_r$, $r \in \varsigma$ are subjected to the $a (a > 0)$ types of cyber-attacks simultaneously. Denote the Laplacian matrix of the communication topology $G_r$ as $\boldsymbol{L}_{rr}^{\sigma(t)}$, then the Laplacian matrix of graph $G$ will be expressed as

$$\begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} & \ldots & \boldsymbol{L}_{1q} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} & \ldots & \boldsymbol{L}_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{L}_{q1} & \boldsymbol{L}_{q2} & \ldots & \boldsymbol{L}_{qq}^{\sigma(t)} \end{pmatrix}.$$

Based on the above analysis, error system (24) can be represented as

$$\dot{e}(t) = -\boldsymbol{B} \begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} & \ldots & \boldsymbol{L}_{1q} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} & \ldots & \boldsymbol{L}_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{L}_{q1} & \boldsymbol{L}_{q2} & \ldots & \boldsymbol{L}_{\mathrm{qq}}^{\sigma(t)} \end{pmatrix} \boldsymbol{F} e(t), \tag{25}$$

where $\boldsymbol{B}$ and $\boldsymbol{F}$ are the same as those in Lemma 2.

Then, the main theorem is established as follows.

**Theorem 2** Consider that in-group links of $G_r$ are subjected to cyber-attacks at the same time, and the cyber-attacks can be recovered. Suppose that Assumptions 2–4 hold, the LMIs (12) and (13) have feasible solutions. Moreover, if the following condition holds:

$$-\gamma_2(t_{2k+2} - t_{2k+1}) + \alpha(t_{2k+1} - t_{2k}) > \varepsilon, \tag{26}$$

where $\varepsilon > 0$, and $\gamma_2$ is determined by the following optimization problem:

Minimize $\gamma_2$ subject to

$$\begin{aligned} & \boldsymbol{Q} \left( \boldsymbol{B} \begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} & \ldots & \boldsymbol{L}_{1q} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} & \ldots & \boldsymbol{L}_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{L}_{q1} & \boldsymbol{L}_{q2} & \ldots & \boldsymbol{L}_{\mathrm{qq}}^{\sigma(t)} \end{pmatrix} \boldsymbol{F} \right) \\ & + \left( \boldsymbol{B} \begin{pmatrix} \boldsymbol{L}_{11}^{\sigma(t)} & \boldsymbol{L}_{12} & \ldots & \boldsymbol{L}_{1q} \\ \boldsymbol{L}_{21} & \boldsymbol{L}_{22}^{\sigma(t)} & \ldots & \boldsymbol{L}_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{L}_{q1} & \boldsymbol{L}_{q2} & \ldots & \boldsymbol{L}_{\mathrm{qq}}^{\sigma(t)} \end{pmatrix} \boldsymbol{F} \right)^{\mathrm{T}} \boldsymbol{Q} + \gamma_2 \boldsymbol{Q} > 0, \end{aligned} \tag{27}$$

then the group consensus of multi-agent system (1) with multiple subgroups subjected to cyber-attacks can be achieved.

The proof of Theorem 2 is similar to that of Theorem 1, therefore, we omit it here.

## 4. Numerical simulations

In this section, three simulation examples are provided to demonstrate the main results.

**Example 1** (Two subgroups with one type of cyber-attack). Consider a multi-agent system (1) consisting of $N = 14$ agents. The communication graph is described in Fig. 2, where the blue agents belong to subgroup 1, and the green agents belong to subgroup 2. This topology is commonly existent in reality. Apparently, $G$ satisfies Assumptions 1 and 3. The $x(0) = [-1\ 8\ -4\ 0\ -5\ 3\ 6\ 0\ -2\ 9\ 1\ 5\ -3\ 4]^{\mathrm{T}}$ is taken as the initial state.

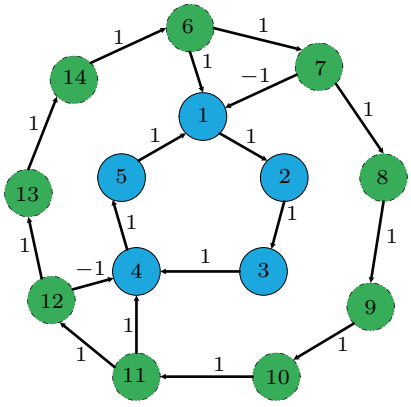



**Fig. 2.** Topology structure of agents.

For the network under cyber-attacks, the in-group links $(v_2, v_3)$, $(v_4, v_5)$, $(v_6, v_7)$, $(v_{10}, v_{11})$, $(v_{13}, v_{14})$ are assumed to be destroyed. In the simulation, let

$$(t_{2k+1} - t_{2k})/(t_{2k+2} - t_{2k+1}) = 12.5.$$

By using Algorithm 1 and Theorem 1, we can obtain $\alpha = 0.1229$ and $\gamma = 1.4931$; the condition (14) is satisfied. The state trajectories are shown in Fig. 3 and group consensus errors are shown in Fig. 4. It shows that the group consensus is reached on the proposed protocol (2).

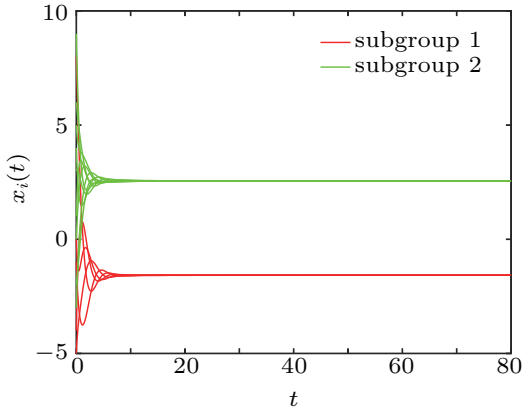



**Fig. 3.** State trajectories of agents with two subgroups

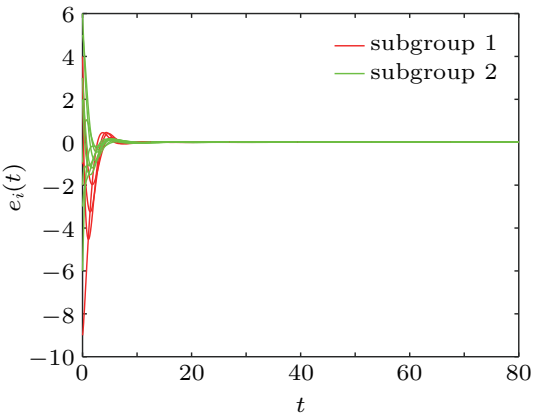



**Fig. 4.** Trajectories of $e(t)$ in system (1) with two subgroups

**Example 2** (Two subgroups with two types of cyber-attacks). Suppose that a multi-agent system contains 7 nodes with two subgroups $G_1$ and $G_2$, which is shown in Fig. 5(a), then Agents 1–3 will be in $G_1$, and agents 4–7 in the other subgroup $G_2$. Note that subgroups $G_1$ and $G_2$ satisfy in-degree balanced condition, and $G$ satisfies Assumptions 1 and 3, then the initial state is set to be $x(0) = [-7\ 2\ 4\ 1\ -2\ 6\ -5]^{\mathrm{T}}$.

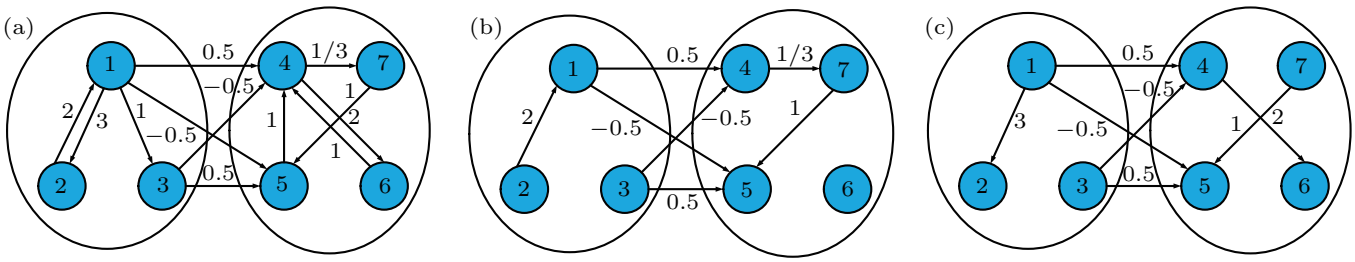



**Fig. 5.** Topology structure of agents: (a) original directed topology, (b) the first kind of topology under attack, (c) the second kind of topology under attack.

**Case 1** Without loss of generality, suppose that there are two kinds of cyber-attacks in subgroups $G_1$ and $G_2$, which are shown in Figs. 5(b) and 5(c) specifically, when the attack happens to the in-group links of $G_1$ and $G_2$. Let $(t_{2k+1} - t_{2k})/(t_{2k+2} - t_{2k+1}) = 5.5$. According to Algorithm 1 and optimization problem in Theorem 1, we can obtain $\alpha = 0.3492$ and $\gamma = 1.8631$. Obviously, condition (14) is satisfied. Under the group consensus protocol (2), one can conclude that

the group consensus under cyber-attacks is achieved. Figures 6 and 7 show the simulation results for the state variables and group consensus errors.

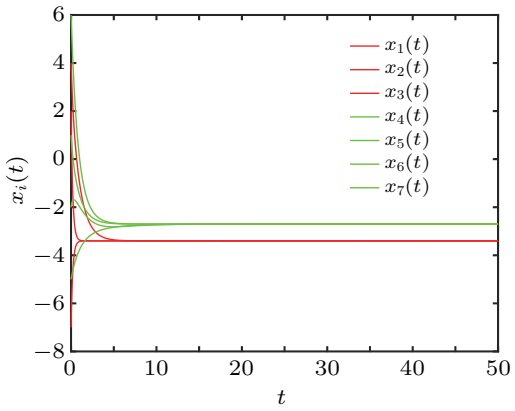



**Fig. 6.** State trajectories of agents with two subgroups.

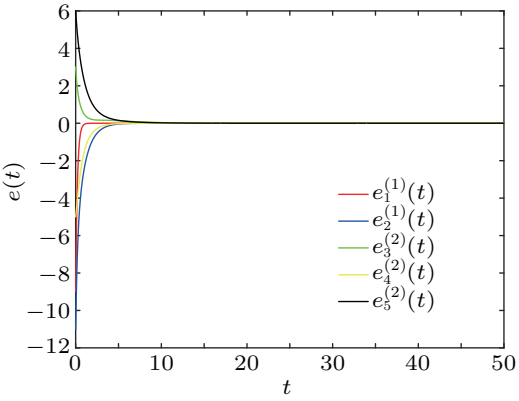



**Fig. 7.** Trajectories of $e(t)$ in system (1) with in-degree balance.

**Case 2** If we add the edges of $(v_6, v_1)$, $(v_7, v_2)$, $(v_2, v_6)$, their weights are set to be $-1$, and the edges of $(v_3, v_4)$ and $(v_1, v_5)$ are deleted, the subgroups $G_1$ and $G_2$ are not in-degree balanced, Assumption 1 is not satisfied. In addition, we still choose the two types of cyber-attacks mentioned above. Even if the calculated $\alpha = 0.3428$, $\gamma = 1.3504$ satisfy condition (14), the ultimate errors will not close to zero, which means that system (1) cannot achieve group consensus. The trajectories of the error vectors are plotted in Fig. 8.

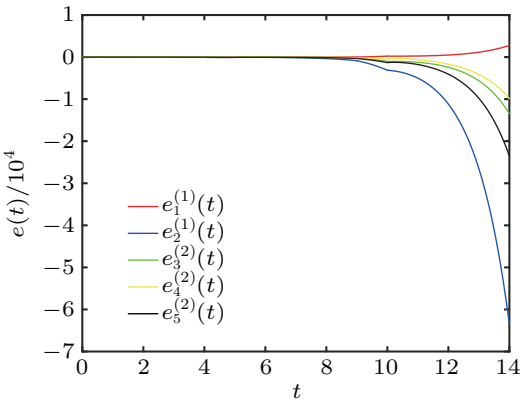



**Fig. 8.** Trajectories of $e(t)$ in system (1) without in-degree balance.

**Example 3** (Multiple subgroups). Suppose that a multi-agent system consists of 10 nodes with three subgroups, where agents 1–3 are in subgroup 1, agents 4–7 are in subgroup 2, and agents 8–10 are in subgroup 3. The original communication topology is shown in Fig. 9(a). Note that $G_1$, $G_2$, and $G_3$ are in-degree balanced, and $G$ satisfies Assumptions 3 and 4. If the cyber-attack happens to the in-group links of $G_1$, $G_2$ and $G_3$, without loss of generality, we suppose that there is one type of cyber-attack given in Fig. 9(b). When an attack occurs, according to Algorithm 1 and optimization problem (15), we can obtain $\alpha = 0.8062$ and $\gamma_2 = 4.9247$. Finally, figure 10 shows the state trajectory of the agents with initial value $x(0) = [-1\ 8\ -4\ 0\ -5\ 3\ 6\ 0\ -2\ 9]^{\mathrm{T}}$, and the trajectories of group consensus error vectors are depicted in Fig. 11.

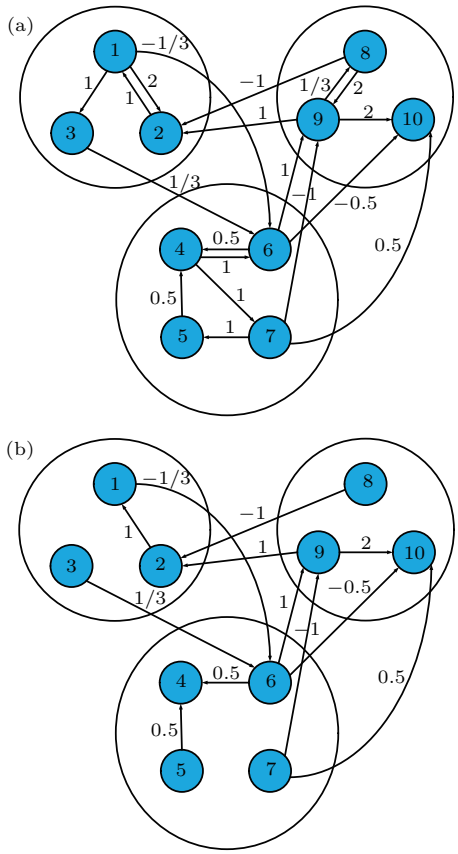



**Fig. 9.** Topology structure of agents with three subgroups: (a) original directed topology and (b) topology under attack.

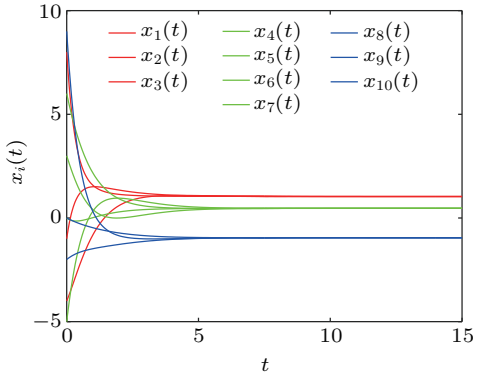



**Fig. 10.** State trajectories of agents with three subgroups.

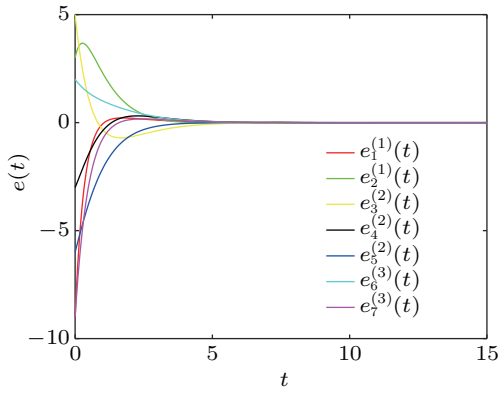



**Fig. 11.** Trajectories of $e(t)$ with three subgroups.

## 5. Conclusions

In this paper, the group consensus problem for the multi-agent systems in the presence of cyber-attack has been investigated. When attacks happen, the network topology containing a directed spanning tree can be damaged. By using algebraic graph theory, linear matrix inequality, and Lyapunov stability theory, the group consensus conditions with cyber-attacks are established. The effectiveness of the theoretical results is demonstrated by numerical simulations. However, the network needs to satisfy the condition of in-degree balanced couple. Our future work will focus on studying the group consensus for more general topology and second-order multi-agent systems with cyber-attacks.

## References


[1] Chen L M, Li C J, Sun Y C and Ma G F 2017 *Chin. Phys. B* **26** 068703

[2] Ren W, Beard R W and Atkins E M 2007 *IEEE Control Syst. Mag.* **27** 71

[3] Yu W, Chen G, Wang Z and Yang W 2009 *IEEE Trans. Syst. Man Cybern. B* **39** 1568

[4] Cao F J, Ling Z H, Yuan Y F and Gao C 2014 *Chin. Phys. B* **23** 070509

[5] Ren W and Cao Y C 2011 *Distributed Coordination of multi-agent networks* (London: Springer-Verlag) pp. 24–27

[6] Shahamatkhah E and Tabatabaei M 2018 *Chin. Phys. B* **27** 010701

[7] Wang C R and Ji H B 2014 *Syst. Control Lett.* **70** 23

[8] Wang Y J, Tu L L, Song S and Li K Y 2018 *Acta Phys. Sin.* **67** 050504 (in Chinese)

[9] Ni W and Cheng D Z 2010 *Syst. Control Lett.* **59** 209

[10] Yang W and Shi H B 2012 *Neurocomputing* **87** 132

[11] Wang J H, Xu Y L, Zhang J and Yang D D 2018 *Chin. Phys. B* **27** 040504

[12] Wang R S, Gao L X, Chen W H and Dai D M 2016 *Chin. Phys. B* **25** 100202

[13] Cui Q, Xie D M and Jiang F C 2016 *Neurocomputing* **218** 286

[14] Aeyels D and Smet F D 2011 *Automatica* **47** 2481

[15] Oyedeji M O and Mahmoud M S 2018 *Syst. Control Lett.* **117** 37

[16] Yu J Y and Wang L 2009 *Proceedings 7th Asian Control Conference,* August 27–29, 2009, Hong Kong, China, p. 105

[17] Ma Q, Wang Z and Miao G 2014 *J. Frankl. Inst.* **351** 1288

[18] Wen G G, Huang J, Peng Z X and Yu Y J 2016 *Neurocomputing* **207** 623

[19] Hu H X, Yu W W, Xuan Q, Zhuang C G and Xie G M 2014 *Neurocomputing* **142** 383

[20] Qin J H and Yu C B 2013 *Automatica* **49** 2898

[21] Hu H X, Yu W W, Wen G H, Xuan Q and Cao J D 2016 *IEEE Trans. Circuits Syst. I: Reg. Papers* **63** 2036

[22] Hu A H, Cao J D, Hu M F and Guo L X 2018 *J. Frankl. Inst.* **355** 7384

[23] Xia H, Huang T Z, Shao J L and Yu J Y 2016 *Neurocomputing* **171** 1666

[24] Ji L H, Liu Q and Liu X F 2014 *Inf. Sci.* **287** 1

[25] Yu J Y and Wang L 2010 *Syst. Control Lett.* **59** 340

[26] Zha L J, Tian E G, Xie X P, Gu Z and Cao J 2018 *Inf. Sci.* **457–458** 141

[27] Dan Y and Xiang Y 2019 *Inf. Sci.* **473** 178

[28] Pasqualetti F, Dorfler F and Bullo F 2013 *IEEE Trans. Autom. Control* **58** 2715

[29] Zhang W B, Wang Z D, Liu Y R, Ding D R and Alsaadi F E 2018 *Int. J. Robust. Nonlinear Control* **28** 53

[30] Liu S, Wei G L, Song Y and Liu Y R 2016 *Neurocomputing* **207** 708

[31] Wang Y W, Wang H O, Xiao J W and Guan Z H 2010 *Automatica* **46** 197

[32] Wan Y, Cao J D, Chen G R and Huang W 2017 *IEEE Trans. Circuits Syst. I: Reg. Papers* **64** 2966

[33] Feng Z and Hu G Q 2014 *Proceedings 19th World Congress: The International Federation of Automatic Control,* August 24–29, 2014, Cape Town, Sourth Africa, p. 5790

[34] Dai Y Q, Hu G Z and Chen W 1995 *Graph theory and algebraic structure* (Beijing: Tsinghua University Press) pp. 1–35 (in Chinese)