

# Resiliency in Dynamic Leader-Follower Multiagent Systems <sup>★</sup>

Hamed Rezaee <sup>a</sup>, Thomas Parisini <sup>a,b,c</sup>, and Marios M. Polycarpou <sup>c,d</sup>

<sup>a</sup>Department of Electrical and Electronic Engineering, Imperial College London, London, UK

<sup>b</sup>Department of Engineering and Architecture, University of Trieste, Trieste, Italy

<sup>c</sup>KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia, Cyprus

<sup>d</sup>Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus

---

## Abstract

Resilient control of multiagent systems (MASs) in the presence of dynamic leaders is studied in this paper. We consider a network of agents consisting of a leader, a set of healthy agents, and a set of attacked malicious agents. The objective is developing a control strategy for the healthy agents to follow the trajectory of the leader, while they are in interaction with the unknown malicious agents. The main contribution of this paper is resilient leader-follower control of MASs when a dynamic leader determines a continuous time-varying trajectory for the MAS. By defining the concept of  $r$ -robust leader-follower graphs, we propose and analyze sufficient conditions on interaction among the agents such that the mentioned objective is achieved. Numerical examples verify the accuracy of the proposed control scheme.

*Key words:* Cyber-attack, leader-follower, malicious agents, multiagent systems, resilient control.

---

## 1 Introduction

Control of multiagent systems (MASs) has been a major topic of research in the control community over the past decade. Because of using open communication and computational platforms, MASs may be subject to several sources of cyber-attacks (Smith 2015, Teixeira et al. 2015, D’Innocenzo et al. 2016, Nowzari & Cortes 2016). Cyber-attacks cause malicious behaviors in some agents such that they may not follow a desired coordination strategy, and due to interaction among the agents, they may lead to erroneous behaviors in all the MAS. Thus, resiliency against cyber-attacks is an important problem in control of MASs.

### 1.1 State of the Art and Existing Problems

In general, two classical problems are considered in control of MASs, namely, *consensus* and *leader-following*. The objective of the consensus problem is agreement of agents on an *a priori* unknown common value in a leaderless scenario (Olfati-Saber & Murray 2004, Ding 2013, Rezaee & Abdollahi 2015, Boem et al. 2017), whereas in the leader-following scenario (sometimes it is called leader-follower consensus), the objective is the convergence of the agents states toward the trajectory of a leader (Ren 2007, Franco et al. 2008, Rezaee et al. 2014, Khalili et al. 2018). Most studies on resilient control of MASs are devoted to the consensus problem. This problem was first investigated in Pasqualetti et al. (2009) and Pasqualetti et al. (2012) in which achieving resilient consensus among a team of first-order agents is studied. In Zhang & Sundaram (2012) and LeBlanc et al. (2013), it is shown that to achieve resilient consensus, the network communication graph should be sufficiently  $r$ -robust with respect to the maximum number of possible malicious neighbors. The idea is that based on the knowledge of the maximum number of possible malicious neighbors, the states of the healthy agents are updated toward a convex set of their values such that by shrinking the convex set, achieving consensus in the network is realized. That idea is extended to more complex cases

---

<sup>★</sup> This paper was not presented at any IFAC meeting. Corresponding author: Hamed Rezaee. This work has been partially supported by European Union’s Horizon 2020 research and innovation program under grant agreement no. 739551 (KIOS CoE) and by the Italian Ministry for Research in the framework of the 2017 Program for Research Projects of National Interest (PRIN), Grant no. 2017YKXYXJ.

*Email addresses:* h.rezaee@imperial.ac.uk (Hamed Rezaee), t.parisini@imperial.ac.uk (Thomas Parisini), mpolycar@ucy.ac.cy (Marios M. Polycarpou).

such as asynchronous MASs (Dibaji et al. 2018), agents with double-integrator models (Dibaji & Ishii 2014), delayed networks (Wu & He 2017), high-order synchronization (LeBlanc & Koutsoukos 2018), attitude consensus (Rezaee & Abdollahi 2019), and so on.

In the presence of a leader in a MAS, since the leader does not follow other agents, the associated communication graph cannot be sufficiently  $r$ -robust (it can be at most 1-robust). Therefore, the existing strategies for resilient consensus control of MASs are not applicable for leader-follower MASs. To extend the existing results to leader-follower networks, in Usevitch & Panagou (2018), the idea of using multiple leaders is proposed. In that study, to guarantee the network resiliency, the number of the leaders is set based on the maximum number of possible malicious neighbors in the network. Accordingly, to guarantee the convergence of the healthy followers to a common value, the leaders are considered static with identical state values. In Usevitch & Panagou (2019), that idea is extended to the case of leaders with time-varying trajectories. However, under that approach, it is assumed that the states of the leaders remain constant in finite periods of time and are updated in some updating times. Therefore, those results are not applicable in problems where the agents need to follow a nonconstant/nonpiecewise constant trajectory. Moreover, under those approaches, the leaders cannot be autonomous as they should have identical state values. Specifically, since the leaders have identical states, they need a central coordinator to set their states on the same values; otherwise, their state values should be set identical in advance. Thus, such leaders cannot set their own trajectories based on local sensing. In Mustafa et al. (2020), Mustafa & Modares (2020), and Moghadam & Modares (2018), resilient control strategies for leader-follower MASs with dynamic leaders are addressed in which local strategies for compensation of the effects of cyber-attacks are proposed. However, in those studies, cyber-attacks are considered as compensable additive faults in sensors and actuators, whereas in practice, compensable additive faults may not model a wide range of cyber-attacks.

### 1.2 Objectives and Contributions

Based on the above-mentioned issues, more practical problems in resilient control of MASs require investigation. In this paper, resilient control of leader-follower MASs is addressed. Because of possible cyber-attacks, some agents are assumed to be malicious while unknown, and interaction of healthy agents with these malicious agents may lead to their divergence from a leader trajectory. The objective is to propose a resilient control strategy such that the healthy agents filter out any anomaly in interaction with neighboring agents and follow the leader trajectory. Compared with existing results in the literature, the contributions of the paper are as follows:

- 1) Compared with the resilient control strategies introduced in Pasqualetti et al. (2009, 2012), Zhang & Sundaram (2012), LeBlanc et al. (2013), Dibaji et al. (2018), Wu & He (2017), Dibaji & Ishii (2014), and LeBlanc & Koutsoukos (2018), which are limited to leaderless networks, the proposed control strategy in this paper guarantees the resilient convergence of the trajectories of the healthy followers toward a leader trajectory.
- 2) Despite the resilient leader-follower control strategies introduced in Usevitch & Panagou (2018) and Usevitch & Panagou (2019), which are applicable in the presence of multiple leaders with constant/piecewise constant trajectories, under the proposed resilient control strategy, there is a single leader that can autonomously determine the MAS trajectory. In other terms, since multiple leaders are not required, the leader trajectory is not needed to be determined in advance or via a central coordinator. Moreover, the leader trajectory is not required to be constant/piecewise constant.
- 3) Compared with the resilient leader-follower control strategies developed in Mustafa et al. (2020), Mustafa & Modares (2020), and Moghadam & Modares (2018), which are applicable in the presence of compensable additive attacks, the proposed control strategy in this paper is resilient against a wide range of malicious behaviors of the attacked followers (for instance, when a malicious follower is under the control of an attacker).

We define the concept of  $r$ -robust leader-follower graphs under which the agents exchange their state information. Based on the knowledge of the maximum number of possible malicious neighbors, we propose a criterion such that each healthy follower evaluates the state information of its neighbors, and selects and uses the safest information to update its own state. Then, we propose and analyze a control strategy such that if the network communication graph is an  $r$ -robust leader-follower graph, the states of the healthy followers converge toward the state of the leader.

It is worth mentioning that in Zhang & Sundaram (2012), based on the concept of strongly  $r$ -robust graphs, the problem of resilient “broadcasting of a message” throughout a network is studied. The main difference between broadcasting and leader-following is that in broadcasting, a message will be distributed in the network, whereas in the leader-following problem, the objective is developing a control strategy such that a group of follower agents follows the state of a leader over time. For instance, to track a sinusoidal trajectory of a leader node, broadcasting is not applicable.

The paper organization is as follows. Preliminaries are provided in Section 2. Problem statement is given in Section 3. The proposed resilient control strategy is presented in Section 4. Numerical examples are provided in Section 5, and Section 6 concludes the paper.

## 2 Preliminaries

Notations and concepts on graph theory are provided in this section.

### 2.1 Notation

Throughout the paper  $\mathbb{R}$ ,  $\mathbb{R}_{>0}$ , and  $\mathbb{R}_{\geq 0}$  denote the sets of real, positive real, and nonnegative real numbers, respectively. For a scalar  $x$ ,  $|x|$  denotes the absolute value, and for a set  $\mathcal{S}$ ,  $|\mathcal{S}|$  stands for the cardinality. For two sets  $\mathcal{S}_1$  and  $\mathcal{S}_2$ , the reduction of  $\mathcal{S}_1$  by  $\mathcal{S}_2$  is denoted by  $\mathcal{S}_1 \setminus \mathcal{S}_2$ , and for three sets  $\mathcal{S}_1$ ,  $\mathcal{S}_2$ , and  $\mathcal{S}_3$ , let  $\mathcal{S}_1 \setminus \mathcal{S}_2 \setminus \mathcal{S}_3 = (\mathcal{S}_1 \setminus \mathcal{S}_2) \setminus \mathcal{S}_3$ . Moreover,  $\sup\{\cdot\}$  denotes the supremum,  $\text{sgn}(\cdot)$  denotes the sign function, and  $\text{sat}(\cdot)$  is the saturation function which for a scalar  $x$ , it is defined as follows:

$$\text{sat}(x/\epsilon) = \begin{cases} 1 & x \geq \epsilon \\ x/\epsilon & -\epsilon \leq x \leq \epsilon \\ -1 & x \leq -\epsilon \end{cases} \quad (1)$$

where  $\epsilon \in \mathbb{R}_{>0}$ .

### 2.2 Graph Theory

The network communication topology is described by a directed graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$  where  $\mathcal{V} = \{1, 2, \dots, N\}$  is the set of nodes describing  $N$  agents,  $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$  is the set of edges describing communication links where an edge  $(j, i)$  means that the  $i$ th agent as a *child* receives information from the  $j$ th one as a *parent*, and  $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N \times N}$  is the adjacency matrix where  $a_{ij} \in \mathbb{R}_{>0}$  if  $(j, i) \in \mathcal{E}$ ,  $i \neq j$ , and it is zero, otherwise. The value of  $a_{ij}$  describes the gain of feedback from the state information of the  $j$ th agent used in the controller design in Section 4. Moreover,  $\mathcal{N}_i = \{j \in \mathcal{V} | (j, i) \in \mathcal{E}\}$  is defined as the set of the neighbors of Agent  $i$ .

Let a nonempty set  $\mathcal{S} \subset \mathcal{V}$  be *r-reachable* if  $\exists i \in \mathcal{S}$  s.t.  $|\mathcal{N}_i \setminus \mathcal{S}| \geq r$ . Let a set  $\mathcal{S} \subset \mathcal{V}$  be *f-local* if  $\forall i \in \mathcal{V} \setminus \mathcal{S}, |\mathcal{N}_i \cap \mathcal{S}| \leq f$ . According to the concept of *r-reachability*, a directed graph  $\mathcal{G}$  is said to be *r-robust* if for each two disjoint nonempty sets  $\mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{V}$ , at least one of them is *r-reachable*. Moreover, a directed graph  $\mathcal{G}$  is *strongly r-robust* if for any nonempty subset  $\mathcal{S} \subseteq \mathcal{V}$ ,  $\mathcal{S}$  is *r-reachable* or  $\exists i \in \mathcal{S}$  such that  $\mathcal{V} \setminus \mathcal{S} \subseteq \mathcal{N}_i$  (Zhang & Sundaram 2012).

## 3 Problem Statement

Consider a MAS comprising of a leader indexed as  $i = 1$  and  $N - 1$  followers indexed as  $i = 2, 3, \dots, N$  where the  $i$ th agent is described as follows:

$$\dot{x}_i(t) = u_i(t) + d_i(t) \quad (2)$$

where  $x_i(t) \in \mathbb{R}$  is the state,  $u_i(t) \in \mathbb{R}$  is the control input, and  $d_i(t) \in \mathbb{R}$  is the bounded external disturbance with known bound. Because of possible cyber-attacks, some followers are assumed to be malicious each of which has at least one of the following anomalies:

- It updates its own state in a way other than what is desired/prescribed. More specifically, if  $u_{id}(t)$  is the designed control law for the input  $u_i(t)$  (when there is no attack), under the control of the attacker,  $u_i(t) \neq u_{id}(t)$  at some time instants.
- It transmits fake/invalid state information to other agents, that is, if  $x_i(t)$  is the true state of Agent  $i$ , under the control of the attacker, Agent  $i$  communicates  $x_{ji}(t)$  to Agent  $j$  instead of  $x_i(t)$ , where  $x_{ji}(t) \neq x_i(t)$  at some time instants.

It is worth noting that this definition of attacks covers a wide range of cyber-attacks that have been considered in previous studies, including the attacks listed below:

- *Data injection attacks*: Data injection attacks may lead to wrong updates of the agents states and fake information exchange among the agents. For instance, under a data injection attack in the control input of the  $i$ th agent, we have (An & Yang 2018)

$$u_i(t) = u_{id}(t) + \beta_i(t)\phi_i(t)$$

where  $\beta_i(t) \in \{0, 1\}$  is the attack activation function and  $\phi_i(t)$  is an unknown injected data.

- *Replay attacks*: A replay attack happens if an attacker records transmitted information via a channel and replays it instead of the real information with delays. Thus, it can lead to wrong updates of the agents states and also fake information exchange among the agents. For instance, if  $x_{ji}(t)$  is the replayed information of the  $i$ th agent received by the  $j$ th agent, it can be modeled as (Gallo et al. 2018)

$$x_{ji}(t) = x_i(t) + \beta_{ji}(t)(-x_i(t) + x_i(t - T_{ji}(t)))$$

where  $\beta_{ji}(t) \in \{0, 1\}$  is the attack activation function and  $T_{ji}(t) \in \mathbb{R}_{\geq 0}$  is a time-delay.

- *Denial of service attacks*: A denial of service attack happens when the attacker prevents information flow between two components. For instance, such attacks on the control input of an agent can affect the update of the agent state.

Therefore, the MAS contains a leader,  $N_h$  healthy followers belonging to a set defined as  $\mathcal{V}_h$  (which are under our control), and  $N_m$  malicious followers belonging to a set defined as  $\mathcal{V}_m$  (which are under cyber-attacks) where  $1 + N_h + N_m = N$  and  $\{1\} \cup \mathcal{V}_h \cup \mathcal{V}_m = \mathcal{V}$ . Each healthy follower receives the state information of its neighbors, and since the malicious neighbors are unknown, the interaction of the healthy followers with their malicious

neighbors can lead to their divergence from the leader trajectory. Under this condition, the objective is designing a resilient control strategy such that the healthy followers track the trajectory of the leader.

**Assumption 1** *While the malicious followers are considered unknown to the healthy ones, we assume that  $\mathcal{V}_m$  is  $f$ -local, and  $f$  is a known parameter of the MAS.*

According to Assumption 1, the availability of the parameter  $f$  of the MAS allows to use it in designing the control algorithm of the healthy followers. Indeed, while each healthy follower does not know which neighbors are malicious, the worst case of the number of malicious neighbors is assumed to be known to the healthy followers. It should be noted that the control strategy is presented for the case of fixed  $\mathcal{V}_m$  when Assumption 1 holds. However, since a malicious follower may be under attacks only in finite time, under some conditions, the results are extendable to cases when  $\mathcal{V}_m$  varies just in finite time. The extension of the proposed control strategy to such cases is presented later.

**Assumption 2** *While  $u_1(t)$  can be a function of  $x_1(t)$  and  $t$ ,  $\dot{x}_1(t)$  is considered bounded and the bound is known to all the healthy followers.*

A necessary condition for leader-following is that the leader should transmit correct state information to the healthy followers. Therefore, the leader must be trustworthy in communication with the healthy followers (see Abbas et al. (2018) and Mitra et al. (2018) for the concept of trustworthy nodes). Moreover, we assume that healthy followers which receive information from the leader know the leader. In other words, we assume that the healthy followers are able to identify the information received from the leader  $\forall t \geq 0$  (among various information they receive from their neighbors); otherwise, leader-following may not be feasible. To explain this issue with a counterexample, consider a case when a malicious follower sends state information to other followers, but does not update its own state. This follower may play a role the same as the leader and may not be distinguishable from the leader.

**Remark 1** *It is worth noting that the main difference between a malicious agent and a faulty agent is that a malicious agent may be under the control of the attacker, and its malicious behavior may not be tolerated by designing a proper controller. Therefore, in contrast to fault-tolerant control, the main objective of resilient control is to filter out and ignore agents with malicious behaviors (while they are unknown) such that a global objective for healthy agents is achieved. However, since a faulty agent is a special form of a malicious agent, the obtained results for resilient control of MASs are useful to ignore the malicious behaviors of faulty agents as well, such that the healthy agents do not consider them in the interaction control law to update their own states.*

The main results are presented in the following section. We should note that in the rest of the paper, any control strategy is designed for the healthy followers as the malicious followers are not under our control.

## 4 Resilient Leader-Follower Control Strategy

Considering multiple leaders with identical and constant/piecewise constant states (Usevitch & Panagou 2018, 2019) or modeling of attacks by additive compensable faults in actuators and sensors (Mustafa et al. 2020, Mustafa & Modares 2020, Moghadam & Modares 2018) are the main limitations of the existing approaches for resilient control of leader-follower MASs. Accordingly, the objective of this section is developing a resilient control scheme to lead healthy followers states toward the time-varying trajectory of a leader, when the possible malicious followers may be under a wide range of cyber-attacks.

The main idea in resilient control of MASs is that each healthy agent receives and evaluates the state information of its neighbors, and updates its own state based on state information which does not lead to its divergence from the trajectories of other healthy agents. Based on this general idea, a resilient control strategy for a leader-follower MAS is proposed. Before presenting the main results, we extend the concept of graphs  $r$ -robustness for leader-follower MASs as follows.

**Definition 1** *Consider a directed graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$  with a root/leader indexed as Node 1 which has no neighbors, and let  $\mathcal{V}_c = \{i \in \mathcal{V} | 1 \in \mathcal{N}_i\}$ . Now, the directed graph  $\mathcal{G}$  is an  $r$ -robust leader-follower graph, if  $|\mathcal{V}_c| \geq r$  and any nonempty set  $\mathcal{S} \subseteq \mathcal{V} \setminus \{1\} \setminus \mathcal{V}_c$  is  $r$ -reachable.*

Examples of 3-robust leader-follower graphs are depicted in Fig. 1. For instance, in Fig. 1(a) and Fig. 1(b), Node 1 has no neighbors,  $\mathcal{V}_c = \{2, 3, 4\}$ , implying that  $|\mathcal{V}_c| = 3$ , and any nonempty subset of  $\mathcal{V} \setminus \{1\} \setminus \mathcal{V}_c = \{5, 6\}$  in Fig. 1(a) and of  $\mathcal{V} \setminus \{1\} \setminus \mathcal{V}_c = \{5, 6, 7\}$  in Fig. 1(b) is 3-reachable.

It is worth mentioning that the concept of strongly  $r$ -robust graphs given in Zhang & Sundaram (2012) for message broadcasting is different from the concept of  $r$ -robust leader-follower graphs. For instance, in a strongly  $r$ -robust graph, it is necessary for all the nodes to have at least one neighbor, whereas in an  $r$ -robust leader-follower graph, the root/leader node does not have any neighbor. Thus, a strongly  $r$ -robust graph cannot be an  $r$ -robust leader-follower graph.

By defining  $e_i(t) = x_i(t) - x_1(t)$  as the leader-following error of Follower  $i$ , we develop a resilient control strategy such that  $e_i(t), i \in \mathcal{V}_h$ , converge toward zero (with ultimately bounded errors). If there are no malicious followers in the MAS, leader-follower control strategies existing in the literature can guarantee this. However, in

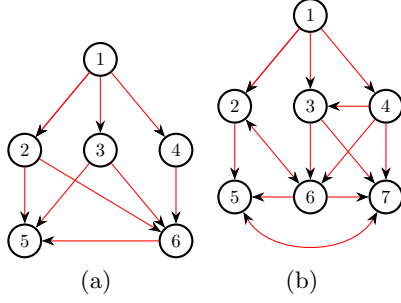


Fig. 1. Examples of 3-robust leader-follower graphs.

the presence of malicious followers, the convergence of some  $e_i(t), i \in \mathcal{V}_h$ , toward zero may be prevented by the malicious followers. To explain this issue more clearly, consider the following simple first-order interaction law:

$$\dot{x}_i = \sum_{j=1}^N a_{ij}[x_i(t) - x_j(t)] = \sum_{j=1}^N a_{ij}[e_i(t) - e_j(t)].$$

Assume that there exists a malicious follower  $k$  in the neighborhood of the healthy follower  $i$  such that at some time instants,

$$|e_k(t)| > |e_j(t)|, \forall j \in \mathcal{V}_h \cup \{1\}. \quad (3)$$

Such malicious follower may attract the state of the  $i$ th healthy follower (which is the healthy follower with index  $i \in \mathcal{V}_h$ ) toward its own trajectory, and since  $e_k(t)$  is outside the range of  $e_j(t), j \in \mathcal{V}_h \cup \{1\}$ , it can lead to the divergence of the leader-following errors of healthy followers from zero. However, according to Assumption 1, it is possible for the  $i$ th healthy follower to ignore up to  $f$  neighbors with largest  $e_j(t), j \in \mathcal{N}_i$ , and up to  $f$  neighbors with smallest  $e_j(t), j \in \mathcal{N}_i$ , such that all the possible malicious neighbors satisfying (3) are ignored. Since the  $i$ th healthy follower may have no access to  $x_1(t)$ , it may have no access to  $e_j(t), j \in \mathcal{N}_i$  (it only has access to  $x_j(t), j \in \mathcal{N}_i$ ). However, since  $x_1(t)$  is identical for all the agents, to ignore up to  $f$  neighbors with largest  $e_j(t), j \in \mathcal{N}_i$ , and up to  $f$  neighbors with smallest  $e_j(t), j \in \mathcal{N}_i$ , up to  $f$  neighbors with largest  $x_j(t), j \in \mathcal{N}_i$ , and up to  $f$  neighbors with smallest  $x_j(t), j \in \mathcal{N}_i$ , can be ignored.

By considering the above-mentioned issue, we consider variables  $k_{ij}(t), i \in \mathcal{V}_h, j \in \mathcal{N}_i$ , describing that the  $i$ th healthy follower selects Agent  $j$  or not. In other words, we consider an *effective adjacency matrix* for the network in the form  $\tilde{\mathcal{A}}(t) = [\tilde{a}_{ij}(t)]$  such that

$$\tilde{a}_{ij}(t) = k_{ij}(t)a_{ij}$$

where  $k_{ij}(t) = 1$  implies the selection of Agent  $j$  for interaction; otherwise, the  $i$ th healthy follower sets  $k_{ij}(t) = 0$ . In a similar way, the *effective neigh-*

*boring set* of each healthy follower is defined as  $\tilde{\mathcal{N}}_i(t) = \{j \in \mathcal{N}_i | k_{ij}(t) = 1\}$ . Note that since the malicious followers are under attacks and the resilient control strategy is developed for the healthy followers, the entries of the effective adjacency matrix when  $i \in \mathcal{V}_m$  are not important for us. Now, the resilient control strategy for the leader-follower MAS is proposed in **two parts** as follows:

- (a) At each time instant:
  - 1) The  $i$ th healthy follower receives the state information  $x_j(t), j \in \mathcal{N}_i$ , and sorts them from the largest state to the smallest one, and sets  $k_{ij}(t) = 1, j \in \mathcal{N}_i$ .
  - 2) If  $|\mathcal{N}_i| \geq f$ , it considers  $f$  neighbors with largest state values described by  $x_j(t)$ , and if  $j \neq 1$  and  $x_j(t) > x_i(t)$ , it sets  $k_{ij}(t) = 0$ . If  $|\mathcal{N}_i| < f$ , it considers all the  $|\mathcal{N}_i|$  neighbors described by  $x_j(t)$ , and if  $j \neq 1$  and  $x_j(t) > x_i(t)$ , it sets  $k_{ij}(t) = 0$ .
  - 3) In a similar way, if  $|\mathcal{N}_i| \geq f$ , it considers  $f$  neighbors with smallest state values described by  $x_j(t)$ . Then, if  $j \neq 1$  and  $x_j(t) < x_i(t)$ , it sets  $k_{ij}(t) = 0$ . Moreover, if  $|\mathcal{N}_i| < f$ , it considers all the  $|\mathcal{N}_i|$  neighbors described by  $x_j(t)$ , and if  $j \neq 1$  and  $x_j(t) < x_i(t)$ , it sets  $k_{ij}(t) = 0$ .
- (b) Based on  $k_{ij}(t), i \in \mathcal{V}_h, j \in \mathcal{N}_i$ , obtained in Part (a) and by considering  $\tilde{a}_{ij}(t) = k_{ij}(t)a_{ij}$ , the  $i$ th healthy follower employs the following interaction law:

$$u_i(t) = -\gamma_i(t)\xi_i(t) - \chi_i \text{sat}(\xi_i(t)/\epsilon), i \in \mathcal{V}_h, \quad (4)$$

where  $\gamma_i(t) = \alpha_i / (\sum_{j=1}^N \tilde{a}_{ij}(t))$ ,  $\alpha_i, \chi_i, \epsilon \in \mathbb{R}_{>0}$ , and

$$\xi_i(t) = \sum_{j=1}^N \tilde{a}_{ij}(t)[x_i(t) - x_j(t)]. \quad (5)$$

Note that by considering a  $(2f+1)$ -robust leader-follower graph, according to Part (a), we have  $\sum_{j=1}^N \tilde{a}_{ij}(t) \neq 0$ .

**Theorem 1** Consider the MAS described in (2) with a dynamic leader,  $N_h$  healthy followers, and  $N_m$  malicious followers, and when Assumptions 1 and 2 hold. Let the  $i$ th healthy follower be under the interaction law (4) where the gains  $k_{ij}(t), i \in \mathcal{V}_h, j \in \mathcal{N}_i$ , are obtained via the selection criterion given in Part (a). Under these conditions, if  $\mathcal{G}$  is a  $(2f+1)$ -robust leader-follower graph and

$$\chi_i > \sup_{t \geq 0} \{|\dot{x}_1(t)| + |d_i(t)|\}, \quad (6)$$

the leader-following errors  $e_i(t), i \in \mathcal{V}_h$ , are uniformly ultimately bounded such that in a finite time,

$$|x_i(t) - x_1(t)| \leq \sum_{k=1}^{N_h} \epsilon_k, i \in \mathcal{V}_h, \quad (7)$$

where  $\epsilon_1 = \epsilon$  and  $\epsilon_k = \epsilon + \sum_{q=1}^{k-1} q\epsilon_q$ ,  $k \in \{2, \dots, N_h\}$ .

**Proof.** By defining  $\dot{\mathcal{V}}_h = \mathcal{V}_h \cup \{1\}$ , at each time instant, we consider three sets  $\mathcal{S}_{1,k}(t)$ ,  $\mathcal{S}_{2,k}(t)$ , and  $\mathcal{S}_{3,k}(t)$ ,  $k \in \{1, 2, \dots, N_h + 1\}$ , as

$$\begin{aligned}\mathcal{S}_{1,k}(t) &= \{i \in \dot{\mathcal{V}}_h | e_i(t) \in e_{M,k}(t)\}, \\ \mathcal{S}_{2,k}(t) &= \{i \in \dot{\mathcal{V}}_h | e_i(t) \in e_{m,k}(t)\}, \\ \mathcal{S}_{3,k}(t) &= \dot{\mathcal{V}}_h \setminus (\mathcal{S}_{1,k}(t) \cup \mathcal{S}_{2,k}(t))\end{aligned}\quad (8)$$

where by sorting  $e_i(t)$ ,  $i \in \dot{\mathcal{V}}_h$ , from the smallest to the largest values (respectively described by  $\delta_1(t), \delta_2(t), \dots, \delta_{N_h+1}(t)$ ) as

$$\delta_1(t) \leq \delta_2(t) \leq \dots \leq \delta_{N_h+1}(t),$$

the sets  $e_{M,k}(t)$  and  $e_{m,k}(t)$  are defined as follows:

$$\begin{aligned}e_{M,k}(t) &= \{\delta_{N_h+2-k}(t), \dots, \delta_{N_h}(t), \delta_{N_h+1}(t)\}, \\ e_{m,k}(t) &= \{\delta_1(t), \delta_2(t), \dots, \delta_k(t)\}.\end{aligned}$$

Since  $e_i(t) = x_i(t) - x_1(t)$  and  $e_1(t) = 0$ , one gets  $\delta_1(t) \leq 0$  and  $\delta_{N_h+1}(t) \geq 0$ . Thus, if  $\delta_{N_h+1}(t) = \delta_1(t)$ , we have  $\delta_{N_h+1}(t) = \delta_1(t) = 0$  which implies that all the healthy followers follow the leader. Now, in three steps we analyze the behaviors of the healthy followers when  $\delta_{N_h+1}(t) \neq \delta_1(t)$ . First, we derive differential equations describing the leader-following errors evolution. Accordingly, in Step 2, we show that  $\delta_{N_h+1}(t) - \delta_{N_h}(t)$  and/or  $\delta_2(t) - \delta_1(t)$  are/is uniformly ultimately bounded, and then in Step 3, in a hierarchical analysis, we show that  $\delta_{N_h+1}(t)$  and  $\delta_1(t)$  are uniformly ultimately bounded.

### Step 1:

By substituting (4) into (2), one gets

$$\dot{x}_i(t) = -\gamma_i(t)\xi_i(t) - \chi_i \text{sat}(\xi_i(t)/\epsilon) + d_i(t), i \in \mathcal{V}_h. \quad (9)$$

From (9), it follows that

$$\dot{e}_i(t) = -\gamma_i(t)\xi_i(t) - \chi_i \text{sat}(\xi_i(t)/\epsilon) + d_i(t) - \dot{x}_1(t) \quad (10)$$

where by considering (5),  $\xi_i(t)$  can be rewritten as

$$\xi_i(t) = \sum_{j=1}^N \tilde{a}_{ij}(t)[e_i(t) - e_j(t)]. \quad (11)$$

According to (1), it can be said that for  $|\xi_i(t)| > \epsilon$ , we have  $\text{sat}(\xi_i(t)/\epsilon) = \text{sgn}(\xi_i(t))$ . In this condition, since  $d_i(t)$  and  $\dot{x}_1(t)$  are bounded, there exists a bounded real number  $\eta_i(t)$  such that (10) can be written in the following form:

$$\dot{e}_i(t) = -\gamma_i(t)\xi_i(t) - \eta_i(t)\text{sat}(\xi_i(t)/\epsilon). \quad (12)$$

Since  $\text{sat}(\xi_i(t)/\epsilon) = \text{sgn}(\xi_i(t))$ , when both  $d_i(t)$  and  $-\dot{x}_1(t)$  in (10) have the same sign as  $-\xi_i(t)$ , we have  $\eta_i(t) = \chi_i + |\dot{x}_1(t)| + |d_i(t)|$ , and when the signs of both  $d_i(t)$  and  $-\dot{x}_1(t)$  are the inverse of the sign of  $-\xi_i(t)$ , one gets  $\eta_i(t) = \chi_i - |\dot{x}_1(t)| - |d_i(t)|$  which according to (6),  $\chi_i - |\dot{x}_1(t)| - |d_i(t)| > 0$ . Therefore, at each time instant,  $\chi_i + |\dot{x}_1(t)| + |d_i(t)|$  and  $\chi_i - |\dot{x}_1(t)| - |d_i(t)|$  are the possible maximum and minimum values of  $\eta_i(t)$ . Thus, according to (6),  $\eta_i(t)$  satisfies

$$\begin{aligned}0 < \chi_i - \sup_{t \geq 0} \{|\dot{x}_1(t)| + |d_i(t)|\} &\leq \eta_i(t) \\ &\leq \chi_i + \sup_{t \geq 0} \{|\dot{x}_1(t)| + |d_i(t)|\}.\end{aligned}\quad (13)$$

### Step 2:

As  $\delta_{N_h+1}(t) \neq \delta_1(t)$ , at least one healthy follower  $i \in \mathcal{V}_h$  where  $e_i(t) \neq 0$  belongs to  $\mathcal{S}_{1,1}(t)$  or  $\mathcal{S}_{2,1}(t)$  as follows:

$$\begin{aligned}i \in \mathcal{S}_{1,1}(t) & \quad 1 \notin \mathcal{S}_{1,1}(t) \\ i \in \mathcal{S}_{2,1}(t) & \quad 1 \notin \mathcal{S}_{2,1}(t).\end{aligned}\quad (14)$$

Two cases can be considered for such healthy followers. The first case is when  $\exists i \in \mathcal{V}_c$  satisfying (14) where  $\mathcal{V}_c = \{i \in \mathcal{V} | 1 \in \mathcal{N}_i\}$ , and the second case is when  $\nexists i \in \mathcal{V}_c$  satisfying (14), each of which is analyzed below:

- i) If  $\exists i \in \mathcal{V}_c$  satisfying (14): According to the definition of  $\mathcal{V}_c$ , for  $i \in \mathcal{V}_c$ , we have  $1 \in \mathcal{N}_i$ . On the other hand, according to the selection criterion given in Part (a),  $k_{i1}(t) = 1$  if  $1 \in \mathcal{N}_i$ . Therefore, if  $i \in \mathcal{V}_c$ , we have  $1 \in \tilde{\mathcal{N}}_i(t)$ , and if (14) is satisfied, one gets

$$\begin{aligned}|\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{1,1}(t) \setminus \mathcal{V}_m| &\geq 1 \quad i \in \mathcal{S}_{1,1}(t) \\ |\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{2,1}(t) \setminus \mathcal{V}_m| &\geq 1 \quad i \in \mathcal{S}_{2,1}(t).\end{aligned}\quad (15)$$

- ii) If  $\nexists i \in \mathcal{V}_c$  satisfying (14): In this condition, since  $\mathcal{G}$  is a  $(2f+1)$ -robust leader-follower graph, by considering (14),  $\mathcal{S}_{1,1}(t)$  is  $(2f+1)$ -reachable if  $i \in \mathcal{S}_{1,1}(t)$ , and  $\mathcal{S}_{2,1}(t)$  is  $(2f+1)$ -reachable if  $i \in \mathcal{S}_{2,1}(t)$ . Thus, for some  $i \notin \mathcal{V}_c$ ,

$$\begin{aligned}|\mathcal{N}_i \setminus \mathcal{S}_{1,1}(t)| &\geq 2f + 1 \quad i \in \mathcal{S}_{1,1}(t) \\ |\mathcal{N}_i \setminus \mathcal{S}_{2,1}(t)| &\geq 2f + 1 \quad i \in \mathcal{S}_{2,1}(t),\end{aligned}\quad (16)$$

and as  $\mathcal{V}_m$  is  $f$ -local, it implies that

$$\begin{aligned}|\mathcal{N}_i \setminus \mathcal{S}_{1,1}(t) \setminus \mathcal{V}_m| &\geq f + 1 \quad i \in \mathcal{S}_{1,1}(t) \\ |\mathcal{N}_i \setminus \mathcal{S}_{2,1}(t) \setminus \mathcal{V}_m| &\geq f + 1 \quad i \in \mathcal{S}_{2,1}(t).\end{aligned}\quad (17)$$

From (16) and (17), it follows that the healthy follower  $i$  has at least  $2f+1$  neighbors outside its set which at least  $f+1$  of them are healthy. Moreover, since  $i \in \mathcal{S}_{1,1}(t)$  or  $i \in \mathcal{S}_{2,1}(t)$ , according to the selection criterion given in Part (a), the healthy follower  $i$  uses the information of at least one of these  $f+1$

healthy neighbors to update its own state. Therefore,

$$\begin{aligned} |\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{1,1}(t) \setminus \mathcal{V}_m| &\geq 1 & i \in \mathcal{S}_{1,1}(t) \\ |\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{2,1}(t) \setminus \mathcal{V}_m| &\geq 1 & i \in \mathcal{S}_{2,1}(t). \end{aligned} \quad (18)$$

As a result, from (15) and (18), it follows that for some  $i \in \mathcal{S}_{1,1}(t)$  or  $i \in \mathcal{S}_{2,1}(t)$ ,

$$\begin{aligned} |\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{1,1}(t) \setminus \mathcal{V}_m| &\geq 1 & i \in \mathcal{S}_{1,1}(t) \\ |\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{2,1}(t) \setminus \mathcal{V}_m| &\geq 1 & i \in \mathcal{S}_{2,1}(t). \end{aligned} \quad (19)$$

According to the definition of  $\mathcal{S}_{1,1}(t)$  and  $\mathcal{S}_{2,1}(t)$  in (8), if  $i \in \mathcal{S}_{1,1}(t)$  or  $i \in \mathcal{S}_{2,1}(t)$ , it implies that  $e_i(t) = \delta_{N_h+1}(t)$  or  $e_i(t) = \delta_1(t)$ , respectively. In this condition, if (this can happen when  $|\mathcal{S}_{1,1}(t)| = 1$  if  $i \in \mathcal{S}_{1,1}(t)$  and when  $|\mathcal{S}_{2,1}(t)| = 1$  if  $i \in \mathcal{S}_{2,1}(t)$ )

$$\begin{aligned} \delta_{N_h+1}(t) - \delta_{N_h}(t) &> \epsilon_1 & i \in \mathcal{S}_{1,1}(t) \\ \delta_2(t) - \delta_1(t) &> \epsilon_1 & i \in \mathcal{S}_{2,1}(t), \end{aligned} \quad (20)$$

from (19), one concludes that the distance of  $e_i(t)$  from the closest  $e_j(t)$ ,  $j \in \tilde{\mathcal{N}}_i(t) \setminus \mathcal{V}_m$ , is larger than  $\epsilon_1$ . Moreover, since  $\mathcal{V}_m$  is  $f$ -local, by considering the selection criterion given in Part (a), any malicious neighbor with leader-following error outside the range  $[\delta_1(t), \delta_{N_h+1}(t)]$  will be ignored. Therefore, according to (11), (19), and (20), for all switching  $\tilde{a}_{ij}(t) \geq 0$ , one gets (note that  $\epsilon_1 = \epsilon$ )

$$\begin{aligned} \xi_i(t) &> \epsilon & i \in \mathcal{S}_{1,1}(t) \\ \xi_i(t) &< -\epsilon & i \in \mathcal{S}_{2,1}(t). \end{aligned} \quad (21)$$

Since  $|\xi_i(t)| > \epsilon$ , we have  $\text{sat}(\xi_i(t)/\epsilon) = \text{sgn}(\xi_i(t))$ . Then, from (8), (14), and (21), it follows that

$$\text{sat}(\xi_i(t)/\epsilon) = \text{sgn}(\xi_i(t)) = \text{sgn}(e_i(t)). \quad (22)$$

Now, for  $|\xi_i(t)| > \epsilon$ , we consider the following Lyapunov candidate:

$$V_i(t) = \frac{1}{2} e_i(t)^2 \quad (23)$$

which is differentiable along (12) as follows:

$$\dot{V}_i(t) = -\gamma_i(t)\xi_i(t)e_i(t) - \eta_i(t)\text{sat}(\xi_i(t)/\epsilon)e_i(t). \quad (24)$$

Therefore, by considering (13), (22), and (24), and since  $\gamma_i(t) > 0$ , one gets for  $|\xi_i(t)| > \epsilon$ ,

$$\dot{V}_i(t) < -\eta_i(t)|e_i(t)| < 0$$

which according to the definition of  $V_i(t)$  in (23), it can be restated as follows:

$$\dot{V}_i(t) < -2^{\frac{1}{2}}\eta_i(t)V_i(t)^{\frac{1}{2}}.$$

Note that the agents belonging to  $\mathcal{S}_{1,1}(t)$ ,  $\mathcal{S}_{2,1}(t)$ , and  $\mathcal{S}_{3,1}(t)$  are not fixed, and  $\mathcal{S}_{1,1}(t)$ ,  $\mathcal{S}_{2,1}(t)$ , and  $\mathcal{S}_{3,1}(t)$  are switching sets over time. However, considering the above-mentioned issues, for all the switching sets, at each time instant if  $\delta_{N_h+1}(t) \neq \delta_1(t)$ ,

- always  $\exists i \in \mathcal{S}_{1,1}(t)$  or  $\mathcal{S}_{2,1}(t)$  such that  $e_i(t) \neq 0$  and if (20) is satisfied,  $\dot{V}_i(t) < -2^{1/2}\eta_i(t)V_i(t)^{1/2}$ .
- $\forall i \in \mathcal{S}_{3,1}(t)$ , if Agent  $i$  leaves the set  $\mathcal{S}_{3,1}(t)$ , it will join  $\mathcal{S}_{1,1}(t)$  or  $\mathcal{S}_{2,1}(t)$ .

Therefore, while  $|\xi_i(t)| > \epsilon$ ,  $V_i(t)$  is decreasing and by invoking the Lyapunov criterion for finite-time convergence (Yu et al. 2017),  $\dot{V}_i(t) < -2^{1/2}\eta_i(t)V_i(t)^{1/2}$  implies that the convergence of  $V_i(t)$  is in finite time. Now, according to (8), since  $i \in \mathcal{S}_{1,1}(t)$  or  $i \in \mathcal{S}_{2,1}(t)$ , in a finite time, we have

$$\begin{aligned} \delta_{N_h+1}(t) - \delta_{N_h}(t) &\leq \epsilon_1 & i \in \mathcal{S}_{1,1}(t) \\ \delta_2(t) - \delta_1(t) &\leq \epsilon_1 & i \in \mathcal{S}_{2,1}(t). \end{aligned} \quad (25)$$

### Step 3:

For  $\delta_{N_h+1}(t) \neq \delta_1(t)$ , since at least one of the healthy followers with nonzero leader-following error belongs to  $\mathcal{S}_{1,1}(t)$  or  $\mathcal{S}_{2,1}(t)$  and

$$\begin{aligned} \mathcal{S}_{1,1}(t) &\subseteq \mathcal{S}_{1,k}(t), \\ \mathcal{S}_{2,1}(t) &\subseteq \mathcal{S}_{2,k}(t), k \in \{2, 3, \dots, N_h + 1\}, \end{aligned}$$

at least one healthy follower  $i \in \mathcal{V}_h$  where  $e_i(t) \neq 0$  belongs to  $\mathcal{S}_{1,k}(t)$  or  $\mathcal{S}_{2,k}(t)$ . In this condition, if  $1 \notin \mathcal{S}_{1,k}(t) \cap \mathcal{S}_{2,k}(t)$ , we consider healthy followers  $i$  where

$$\begin{aligned} i \in \mathcal{S}_{1,k}(t) & \quad 1 \notin \mathcal{S}_{1,k}(t) \\ i \in \mathcal{S}_{2,k}(t) & \quad 1 \notin \mathcal{S}_{2,k}(t). \end{aligned} \quad (26)$$

As  $\mathcal{G}$  is a  $(2f+1)$ -robust leader-follower graph, similar to (19), it can be said that for some  $i \in \mathcal{S}_{1,k}(t)$  or  $i \in \mathcal{S}_{2,k}(t)$  satisfying (26),

$$\begin{aligned} |\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{1,k}(t) \setminus \mathcal{V}_m| &\geq 1 & i \in \mathcal{S}_{1,k}(t) \\ |\tilde{\mathcal{N}}_i(t) \setminus \mathcal{S}_{2,k}(t) \setminus \mathcal{V}_m| &\geq 1 & i \in \mathcal{S}_{2,k}(t). \end{aligned} \quad (27)$$

In this condition, if (this can happen when  $|\mathcal{S}_{1,k}(t)| = k$  if  $i \in \mathcal{S}_{1,k}(t)$  and when  $|\mathcal{S}_{2,k}(t)| = k$  if  $i \in \mathcal{S}_{2,k}(t)$ )

$$\begin{aligned} \delta_{N_h+2-k}(t) - \delta_{N_h+1-k}(t) &> \epsilon_k & i \in \mathcal{S}_{1,k}(t) \\ \delta_{k+1}(t) - \delta_k(t) &> \epsilon_k & i \in \mathcal{S}_{2,k}(t), \end{aligned}$$

by considering the errors ultimate bounds obtained in Steps 1 to  $k-1$  (that are  $\epsilon_1, \epsilon_2, \dots, \epsilon_{k-1}$ ) and according

to the definition of  $\epsilon_k$ , in a finite time for Step  $k$  we have

$$\begin{aligned} & \delta_{N_h+2-k}(t) - \delta_{N_h+1-k}(t) > \\ & \sum_{j=1}^{k-1} \left( \delta_{N_h+2-j}(t) - \delta_{N_h+2-k}(t) \right) + \epsilon \quad i \in \mathcal{S}_{1,k}(t) \\ \delta_{k+1}(t) - \delta_k(t) & > \sum_{j=1}^{k-1} \left( \delta_k(t) - \delta_j(t) \right) + \epsilon \quad i \in \mathcal{S}_{2,k}(t) \end{aligned}$$

implying that

- if  $1 \notin \mathcal{S}_{1,k}(t)$ , the distance of the leader-following error  $\delta_{N_h+2-k}(t)$  from the leader-following error  $\delta_{N_h+1-k}(t)$  is larger than the summation of its distances from all the possible larger leader-following errors inside  $e_{M,k}(t)$  plus  $\epsilon$ .
- if  $1 \notin \mathcal{S}_{2,k}(t)$ , the distance of the leader-following error  $\delta_k(t)$  from the leader-following error  $\delta_{k+1}(t)$  is larger than the summation of its distances from all the possible smaller leader-following errors inside  $e_{m,k}(t)$  plus  $\epsilon$ .

Moreover, based on the selection criterion given in Part (a), up to  $f$  neighbors with largest leader-following errors and up to  $f$  neighbors with smallest leader-following errors (including any malicious neighbor with leader-following error outside the range  $[\delta_1(t), \delta_{N_h+1}(t)]$ ) will be ignored by each healthy follower. As a result, from (11) and (27), for all switching  $\tilde{a}_{ij}(t) \geq 0$ , we have

$$\begin{aligned} \xi_i(t) &> \epsilon & i \in \mathcal{S}_{1,k}(t) \\ \xi_i(t) &< -\epsilon & i \in \mathcal{S}_{2,k}(t). \end{aligned} \quad (28)$$

Then, from (8), (26), and (28), it follows that

$$\text{sat}(\xi_i(t)/\epsilon) = \text{sgn}(\xi_i(t)) = \text{sgn}(e_i(t)).$$

By considering a Lyapunov candidate  $V_i(t)$  the same as (23), the time derivative of  $V_i(t)$  along (12) can be obtained as (24), and then based on similar arguments the same as Step 2, it follows that while  $|\xi_i(t)| > \epsilon$ ,  $V_i(t)$  is decreasing and the convergence is in a finite time. By considering the errors ultimate bounds obtained in Steps 1 to  $k-1$ , for Step  $k$ , in a finite time we should have

$$\begin{aligned} \delta_{N_h+2-k}(t) - \delta_{N_h+1-k}(t) &\leq \epsilon_k & i \in \mathcal{S}_{1,k}(t) \\ \delta_{k+1}(t) - \delta_k(t) &\leq \epsilon_k & i \in \mathcal{S}_{2,k}(t). \end{aligned} \quad (29)$$

Now, if for a  $1 < k \leq N_h + 1$ ,  $1 \in \mathcal{S}_{1,k}(t) \cap \mathcal{S}_{2,k}(t)$ ; then, by considering (25) and (29), it can be said that

$$|x_i(t) - x_1(t)| \leq \sum_{q=1}^{k-1} \epsilon_q, \quad i \in \mathcal{V}_h.$$

Since the maximum of  $k$  such that  $1 \in \mathcal{S}_{1,k}(t) \cap \mathcal{S}_{2,k}(t)$

is  $N_h + 1$ , (7) is satisfied, and the proof is completed. ■

**Remark 2** The main idea of using  $\text{sat}(\cdot)$  instead of  $\text{sgn}(\cdot)$  in (4) is to avoid the chattering phenomenon in the agents control inputs. However, as the leader velocity cannot be fully compensated by a  $\text{sat}(\cdot)$  function, according to Theorem 1, the error will be accumulated in leader-to-follower or follower-to-follower interaction links (simulations regarding this issue can be found in Ren (2007)). However, by choosing  $\epsilon$  small enough, the leader-following errors can be small especially for MASs with no large  $N_h$ . It should be noted that according to the proof of Theorem 1, the ultimate bound mentioned in (7) is a supremum such that out of this bound, the states of the agents converge toward the leader state.

**Remark 3** It is worth noting that the selection criterion given in Part (a) does not imply that at each time instant all the ignored neighbors are malicious or all the malicious neighbors are ignored. Indeed, according to the proposed strategy, each healthy follower evaluates the state information of its neighbors and uses the information of neighbors which do not lead to divergence in the network. In this condition, if a malicious neighbor shows safe behavior at some time instants, it may not be ignored by the healthy follower. This case may happen if according to the transmitted state value by the malicious follower, its leader-following error lies inside a range such that it is not ignored by the healthy follower.

The condition of employing a  $(2f+1)$ -robust leader-follower graph in  $\mathcal{G}$  is a sufficient condition of Theorem 1 such that the states of the healthy followers converge to the bound described in (7). However, there exist cases when if  $\mathcal{G}$  is not a  $(2f+1)$ -robust leader-follower graph, Theorem 1 cannot lead to leader-following.

**Corollary 1** If  $\mathcal{G}$  is not a  $(2f+1)$ -robust leader-follower graph, under the proposed control strategy in Theorem 1, (7) may not be satisfied.

**Proof.** If  $\mathcal{G}$  is not a  $(2f+1)$ -robust leader-follower graph, according to Definition 1, at least one of the following cases should happen:

- i) If  $|\mathcal{V}_c| < 2f + 1$ : Let us decompose  $\mathcal{V}_c$  to two subsets as follows:

$$\begin{aligned} \mathcal{V}_{ch} &= \mathcal{V}_c \cap \mathcal{V}_h, \\ \mathcal{V}_{cm} &= \mathcal{V}_c \cap \mathcal{V}_m. \end{aligned}$$

Consider a scenario when  $d_i(t) = 0, i \in \mathcal{V}, \mathcal{V}_h \setminus \mathcal{V}_{ch} \neq \emptyset$ , and  $|\mathcal{V}_{cm}| = f$  if  $|\mathcal{V}_c| \geq f$  or  $|\mathcal{V}_{cm}| = |\mathcal{V}_c|$  if  $|\mathcal{V}_c| < f$ . Now, since  $|\mathcal{V}_c| < 2f + 1$ , one gets  $|\mathcal{V}_{ch}| \leq f$ . Moreover, let  $\forall j \in \mathcal{V}_{ch}, \mathcal{N}_j \cap \{\mathcal{V} \setminus \{1\} \setminus \mathcal{V}_{ch}\} = \emptyset$ . In this condition,

$$\forall j \in \mathcal{V}_{ch} \cup \{1\}, \forall i \in \mathcal{V}_h \setminus \mathcal{V}_{ch}, \forall \ell \in \mathcal{V}_m,$$



if  $x_j(t) + \sum_{k=1}^{N_h} \epsilon_k < x_i(t) < x_\ell(t)$  or  $x_\ell(t) < x_i(t) < x_j(t) - \sum_{k=1}^{N_h} \epsilon_k$ , according to the selection criterion in Part (a) and since  $|\mathcal{V}_{ch}| \leq f$ , the healthy followers  $i \in \mathcal{V}_h \setminus \mathcal{V}_{ch}$  do not use the state information of any agent belonging to  $\mathcal{V}_{ch} \cup \{1\}$ . In other words,  $\tilde{\mathcal{N}}_i(t) \cap \{\mathcal{V}_{ch} \cup \{1\}\} = \emptyset$ , and as a result (7) cannot be satisfied.

ii) If a nonempty set  $\mathcal{S} \subseteq \mathcal{V} \setminus \{1\} \setminus \mathcal{V}_c$  is not  $(2f+1)$ -reachable: Consider a scenario when  $d_i(t) = 0, i \in \mathcal{V}, \mathcal{S} \subseteq \mathcal{V}_h, |\mathcal{V}_m| = f$ , and  $\forall i \in \mathcal{S}, \mathcal{V}_m \subseteq \mathcal{N}_i$ . Thus, as  $\mathcal{S}$  is at most  $2f$ -reachable,  $\forall i \in \mathcal{S}, |\mathcal{N}_i \setminus \mathcal{S} \setminus \mathcal{V}_m| \leq f$ . Furthermore, let  $\forall j \in \mathcal{V}_h \setminus \mathcal{S}, \mathcal{N}_j \cap \{\mathcal{S} \cup \mathcal{V}_m\} = \emptyset$ . In this condition,

$$\forall j \in \{\mathcal{V}_h \setminus \mathcal{S}\} \cup \{1\}, \forall i \in \mathcal{S}, \forall \ell \in \mathcal{V}_m,$$

if  $x_j(t) + \sum_{k=1}^{N_h} \epsilon_k < x_i(t) < x_\ell(t)$  or  $x_\ell(t) < x_i(t) < x_j(t) - \sum_{k=1}^{N_h} \epsilon_k$ , based on the selection criterion in Part (a) and since  $\forall i \in \mathcal{S}, |\mathcal{N}_i \setminus \mathcal{S} \setminus \mathcal{V}_m| \leq f$ , the healthy followers  $i \in \mathcal{S}$  do not use the state information of any agent belonging to  $\{\mathcal{V}_h \setminus \mathcal{S}\} \cup \{1\}$ . In other words,  $\tilde{\mathcal{N}}_i(t) \cap \{\{\mathcal{V}_h \setminus \mathcal{S}\} \cup \{1\}\} = \emptyset$ , and as a result (7) cannot be satisfied.

Therefore, if  $\mathcal{G}$  is not a  $(2f+1)$ -robust leader-follower graph, there exist cases where some healthy followers  $i \in \mathcal{V}_h$  cannot satisfy (7). ■

Based on the results of Theorem 1, if the number of malicious neighbors is not more than  $f$  and the set of the healthy followers is fixed, (7) will be satisfied. Moreover, while the number of malicious neighbors is not more than  $f$ , if some agents have malicious behaviors only in finite time  $t < t_f, t_f \in \mathbb{R}_+$ , and are healthy for  $t \geq t_f$ , if their states are bounded for  $t = t_f$ , they behave the same as healthy followers for  $t \geq t_f$ . Then, the new fixed set of healthy followers satisfies the conditions of Theorem 1 such that (7) will be satisfied. However, in some cases, the number of malicious neighbors may be more than  $f$  in finite time  $t < t_f$ , but for  $t \geq t_f$ , the set of the healthy followers is fixed and the number of malicious neighbors is not more than  $f$ . To extend Theorem 1 to such cases, we present the following theorem.

**Theorem 2** Consider the MAS described in (2) with a dynamic leader,  $N_h$  healthy followers, and  $N_m$  malicious followers, and when Assumption 2 holds. Let the  $i$ th healthy follower be under the interaction law (4) where the gains  $k_{ij}(t), i \in \mathcal{V}_h, j \in \mathcal{N}_i$ , are obtained via the selection criterion given in Part (a). Under this condition, if the transmitted states  $x_i(t), i \in \mathcal{V}_m$ , are bounded in a finite time period  $[t_0, t_0 + \tau), t_0 \in \mathbb{R}_{\geq 0}, \tau \in \mathbb{R}_{> 0}$ , and if  $x_i(t_0), i \in \mathcal{V}_h$ , are bounded; then,  $x_i(t), i \in \mathcal{V}_h$ , remain bounded in the finite time period  $[t_0, t_0 + \tau)$ .

**Proof.** Let us define the vector  $x_h(t) \in \mathbb{R}^{N_h}$  with entries  $x_i(t), i \in \mathcal{V}_h$ . By substituting (4) into (2), according to (9), there exists a bounded switching matrix  $A_h(t) \in$

$\mathbb{R}^{N_h \times N_h}$  such that for  $t_0 \leq t < t_0 + \tau$ ,

$$\dot{x}_h(t) = A_h(t)x_h(t) + \nu_h(t) \quad (30)$$

where  $\nu_h(t)$  is a function of  $x_1(t)$ , the transmitted states  $x_i(t), i \in \mathcal{V}_m$ , and  $-\chi_i \text{sat}(\xi_i(t)/\epsilon) + d_i(t), i \in \mathcal{V}_h$ . Since  $x_1(t)$  and the transmitted states  $x_i(t), i \in \mathcal{V}_m$ , remain bounded in the finite time period  $[t_0, t_0 + \tau)$  and  $-\chi_i \text{sat}(\xi_i(t)/\epsilon)$  and  $d_i(t), i \in \mathcal{V}_h$ , are bounded, we can consider  $\nu_h(t)$  as a bounded input vector (note that according to Assumption 2,  $x_1(t)$  remain bounded in finite time). Therefore, by considering (30), we deal with a linear switching system with bounded input, and according to the solution of linear switching systems (Sun & Ge 2005), the boundedness of the entries of  $x_h(t)$  in the finite time period  $[t_0, t_0 + \tau)$  can be concluded. ■

According to Theorem 2, under the aforementioned conditions, malicious followers with bounded transmitted states cannot lead to unboundedness of the states of the healthy followers in finite time. Hence, if the transmitted states by the malicious followers are bounded for  $t < t_f$ , if the number of the malicious neighbors is not more than  $f$  for  $t \geq t_f$ , and if new added healthy followers have bounded states at  $t = t_f$ , we will have a leader-follower MAS satisfying the conditions of Theorem 1. Thus, for the new fixed set of healthy followers, (7) will be satisfied.

**Remark 4** It should be noted that for checking that a graph is an  $r$ -robust leader-follower graph, all the subsets of the nodes  $\mathcal{V} \setminus \mathcal{V}_c \setminus \{1\}$  may be needed to be investigated. However, it is possible to propose approaches based on which an  $r$ -robust leader-follower graph can be constructed. One possible way is following a hierarchical algorithm as given in Algorithm 1. According to the first and second steps of the algorithm, the constructed graph contains a node with no neighbors and with at least  $r$  children, and according to the third step of the algorithm, any nonempty subset  $\mathcal{S} \subseteq \mathcal{V} \setminus \mathcal{V}_c \setminus \{1\}$  is  $r$ -reachable. Hence, all the features of an  $r$ -robust leader-follower graph given in Definition 1 are satisfied. By employing the mentioned algorithm, a 5-robust leader-follower graph of 13 nodes is depicted in Fig. 2.

**Algorithm 1** Construction of an  $r$ -robust leader-follower graph

- 1: Consider  $N \geq r+1$  nodes labeled as  $i = 1, 2, \dots, N$ . Set  $i = 1$  as the root/leader node, and set  $\mathcal{V}_c$  as  $\mathcal{V}_c = \{2, 3, \dots, r+1\}, r \leq r \leq N-1$ .
- 2: Add the edges  $(1, i), i \in \mathcal{V}_c$ .
- 3: If  $N \geq r+2$ , for  $i \in \{r+2, \dots, N\}$ , add  $r$  arbitrary different edges  $(j, i), j < i$ .
- 4: For  $i \in \mathcal{V} \setminus \{1\}$  add optional edges  $(j, i), j \in \mathcal{V} \setminus \{i\}$ .

**Theorem 3** The minimum number of the edges of an  $r$ -robust leader-follower graph with minimum  $|\mathcal{V}_c|$  associated with  $N$  nodes is  $(N-r)r$ .

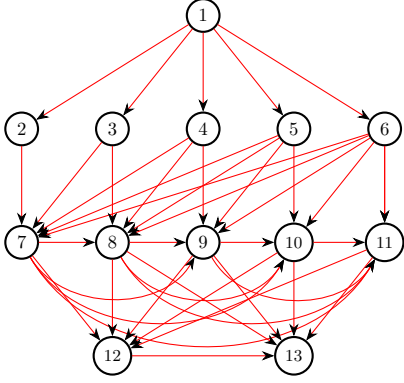


Fig. 2. A 5-robust leader-follower graph of 13 nodes.

**Proof.** According to the second and third steps of Algorithm 1, since the minimum  $|\mathcal{V}_c|$  is  $r$ ,  $r + (N - 1 - r)r = (N - r)r$  edges are sufficient to build an  $r$ -robust leader-follower graph. Now, we assume that the number of the edges is less than  $(N - r)r$ . In this condition, the number of the edges from the root/leader to its children should be less than  $r$  or at least one of the other  $N - 1 - r$  nodes of the graph should have less than  $r$  neighbors. In each of these two cases, the graph cannot be an  $r$ -robust leader-follower graph. ■

**Remark 5** To address resiliency in leader-follower MASs, we have used the concept of  $r$ -robust leader-follower graphs. Moreover, since leader-following is a tracking problem, the existing interaction protocols for resilient control of MASs are not applicable for resilient leader-following (Pasqualetti et al. 2009, 2012, Zhang & Sundaram 2012, LeBlanc et al. 2013, Dibaji et al. 2018, Dibaji & Ishii 2014, Wu & He 2017, LeBlanc & Koutsoukos 2018). Thus, based on properties of the sat( $\cdot$ ) function, we have proposed a nonlinear interaction protocol which guarantees leader-following under  $r$ -robust leader-follower graphs.

## 5 Numerical Examples

The proposed control strategy is evaluated in two scenarios. In the first scenario, a leader-follower network of 100 agents is investigated, and in the second one, a leader-follower formation of seven mobile agents on a two-dimensional plane is considered.

*Scenario 1:* Consider a leader-follower MAS containing 100 agents with initial states randomly chosen between  $[0, 20]$ . Let  $f = 20$  while the number of the malicious followers is assumed to be 15. Accordingly, a  $(2f + 1)$ -robust leader-follower communication graph generated based on Algorithm 1 is considered. The malicious followers are selected randomly, and they are assumed to be under data injection attacks in communicated information and denial of service attacks or data injection attacks in control inputs (we have used various sinusoidal

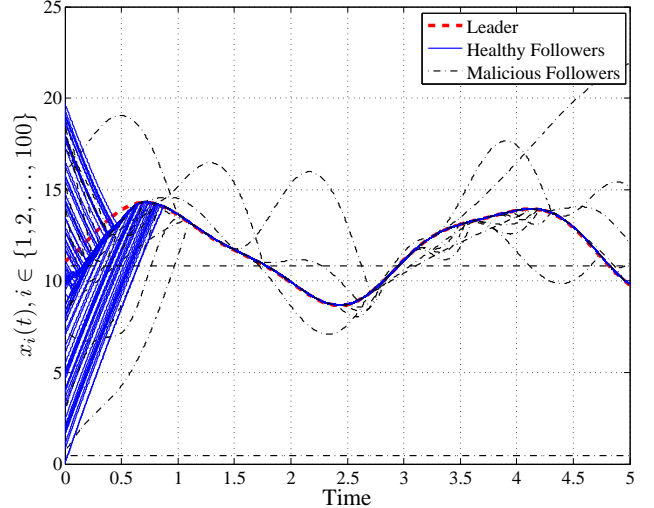


Fig. 3. State trajectories of the agents in Scenario 1: when the proposed resilient control strategy is employed.

and bias signals for data injection, and we have modeled the denial of service by setting  $u_i(t) = 0$ ).

The leader control command is considered to be  $u_1(t) = 5 \cos(2t) + 2 \sin(5t)$  and the external disturbances are supposed to be bounded as  $|d_i(t)| \leq 2$  (we have used random signals to model disturbances). The objective is following Agent 1 based on the leader-following control strategy proposed in Theorem 1. Accordingly, let  $\alpha_i = 1$ ,  $\epsilon = 0.1$ ,  $a_{ij} = 1$  if  $j \in \mathcal{N}_i$ , and  $\chi_i = 12$ . By employing the proposed resilient leader-follower control strategy, as depicted in Fig. 3, the states of the healthy followers converge to the leader state with ultimately bounded errors. According to Fig. 3, while some agents have malicious behaviors and are unknown to the healthy followers, the healthy followers follow the trajectory of the leader. To show the effect of the malicious followers in leading to divergence in the network, let us repeat the scenario when the control law is not resilient. In this condition, as demonstrated in Fig. 4, because of the healthy followers interaction with the malicious followers, the states of the healthy followers diverge from the leader trajectory.

*Scenario 2:* Consider a two dimensional leader-follower MAS under a 3-robust communication topology demonstrated in Fig. 1(b) which each dimension is described by (2) as follows:

$$\begin{aligned} \dot{x}_i(t) &= u_{x_i}(t) + d_{x_i}(t), \\ \dot{y}_i(t) &= u_{y_i}(t) + d_{y_i}(t) \end{aligned}$$

where  $x_i(t)$ ,  $u_{x_i}(t)$ , and  $d_{x_i}(t)$  respectively denote the position, control input, and external disturbance of the  $i$ th agent on the  $x$ -axis, and  $y_i(t)$ ,  $u_{y_i}(t)$ , and  $d_{y_i}(t)$  respectively denote the position, control input, and external disturbance of the  $i$ th agent on the  $y$ -axis. It should be noted that the basis for the proposed resilient control

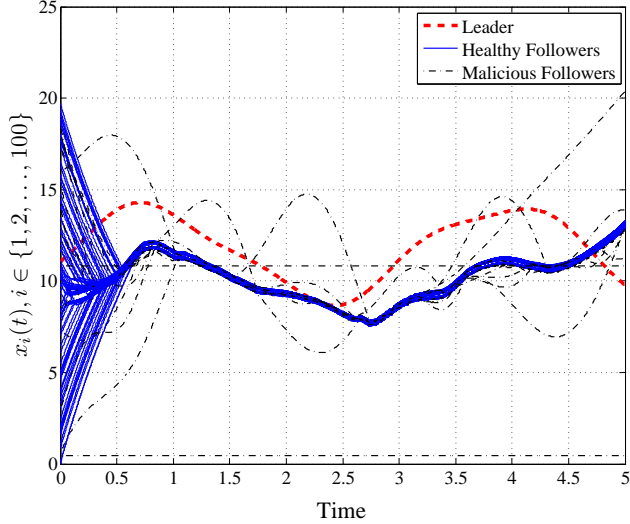


Fig. 4. State trajectories of the agents in Scenario 1: when the interaction law is not resilient.

strategy is sorting the state information of the neighboring agents by each healthy follower, and evaluating them to select the safest ones. According to this idea, the proposed control strategy is well suited to a scenario with scalar agents. The methodology can be extended to decoupled multidimensional dynamics of the agents. Therefore, we employ the proposed resilient control strategy in Theorem 1 for each axis separately (as two decoupled MASs). The agents initial states respectively are set arbitrary as 1, 3, 4, 2, 1, 1, and 2 on the  $x$ -axis, and 1, 2, 1, 3, 3, 2, and 2 on the  $y$ -axis. The leader control commands are considered to be  $u_{x1}(t) = 1$  and  $u_{y1}(t) = 1 + \sin(2t)$ , and the external disturbances are supposed to be bounded as  $|d_{xi}(t)| \leq 1$  and  $|d_{yi}(t)| \leq 1$  (we have used various sinusoidal signals to model the disturbances). Accordingly, let  $\alpha_i = 1$ ,  $\epsilon = 0.1$ ,  $a_{ij} = 1$  if  $j \in \mathcal{N}_i$ , and  $\chi_i = 5$ . We assume that Follower 3 is under a data injection attack such that for  $t > 3$ ,  $u_{x3}(t) = u_{x3d}(t)$  and  $u_{y3}(t) = u_{y3d}(t) + 5 \cos(4t) + 10 \sin(3t) - 9$ , where  $u_{x3d}(t)$  and  $u_{y3d}(t)$  are the desired control commands of Follower 3. The objective is following  $x_1(t)$  and  $y_1(t)$ , considering proper biases such that a hexagon formation around the leader with the radius of 1 is achieved. Accordingly, by considering the desired formation demonstrated in Fig. 5, the states of the followers can be considered as  $\tilde{x}_i(t) = x_i(t) - \cos((i-1)\pi/3)$  and  $\tilde{y}_i(t) = y_i(t) - \sin((i-1)\pi/3)$ ,  $i \in \{2, 3, \dots, 7\}$ . Note that the points described by  $x_1(t) + \cos((i-1)\pi/3)$  and  $y_1(t) + \sin((i-1)\pi/3)$ ,  $i \in \{2, 3, \dots, 7\}$ , imply the hexagonal formation of Fig. 5 about the leader. By employing the proposed resilient control strategy in Theorem 1, as depicted in Fig. 6, while Follower 3 has a malicious behavior, the healthy followers achieve a desired formation around the leader with ultimately bounded errors. To show the effect of the attack without employing the resilient control strategy, we have repeated the scenario when the interaction law is not resilient. In this condi-

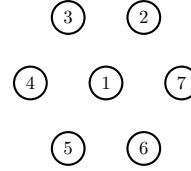


Fig. 5. Desired formation of the agents in Scenario 2.

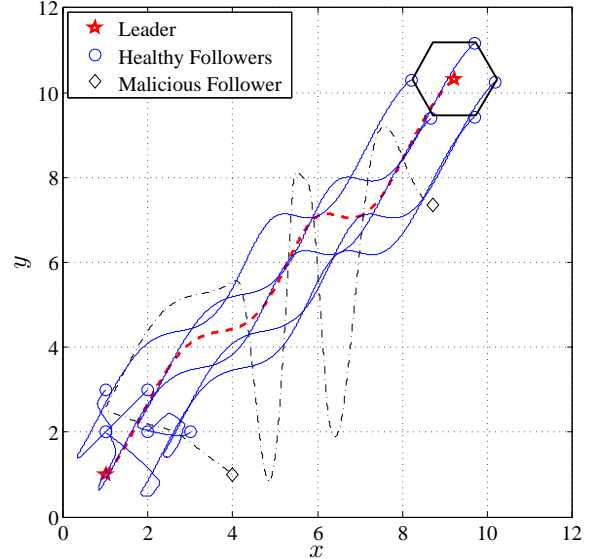


Fig. 6. State trajectories of the agents in Scenario 2: when the proposed resilient control strategy is employed (the initial and final positions of the agents during the simulation are marked).

tion, the state trajectories of the agents are depicted in Fig. 7. According to this figure, because of the healthy followers interaction with the malicious follower, some healthy followers do not follow the leader trajectory.

## 6 Conclusions and Future Work

This study was devoted to leader-follower control of MASs in the presence of cyber-attacks. The resiliency of most existing schemes for control of MASs relied on the  $r$ -robust properties of networks communication graphs, whereas such properties were not realizable when the agents followed a desired trajectory determined by a leader. Although some research also has been done on resilient leader-follower control of MASs, the base of those results was restrictive assumptions such as considering multiple identical leaders with constant/piecewise constant states or modeling of cyber-attacks by additive faults. Under the proposed control strategy in this paper, it was shown that in the presence of an  $r$ -robust leader-follower graph, the healthy followers could filter out any malicious behavior in their neighborhood, and simultaneously they could follow a time-varying trajectory determined by a leader. This study was a primary effort in this area and many problems still are worth

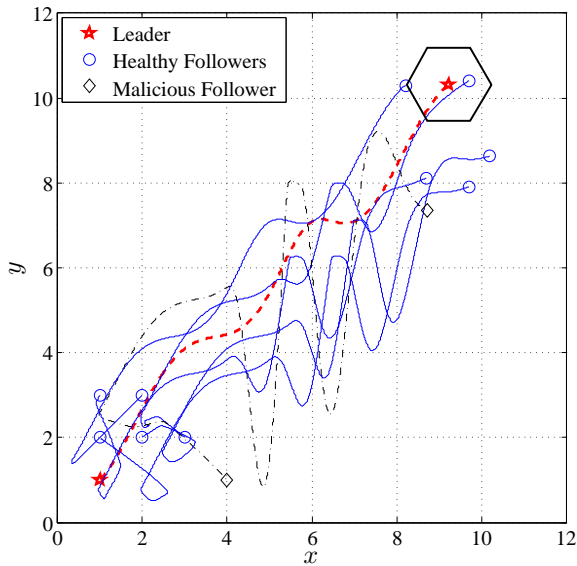


Fig. 7. State trajectories of the agents in Scenario 2: when the interaction law is not resilient (the initial and final positions of the agents during the simulation are marked).

investigation. Resilient leader-following in the presence of a moving leader with unknown speed bound and resilient leader-following considering communication problems (such as time delays, links failure, and noises (Zhan et al. 2019, 2015, Zhang & Zhang 2012)) are few problems in this area which can be considered as future work.

## References

- Abbas, W., Laszka, A. & Koutsoukos, X. (2018), ‘Improving network connectivity and robustness using trusted nodes with application to resilient consensus’, *IEEE Transactions on Control of Network Systems* **5**(4), 2036–2048.
- An, L. & Yang, G. (2018), ‘Improved adaptive resilient control against sensor and actuator attacks’, *Information Sciences* **423**, 145–156.
- Boem, F., Gallo, A. J., Ferrari-Trecate, G. & Parisini, T. (2017), A distributed attack detection method for multi-agent systems governed by consensus-based control, in ‘Proceedings of the 56th IEEE Annual Conference on Decision and Control’, Melbourne, VIC, Australia, pp. 5961–5966.
- Dibaji, S. M. & Ishii, H. (2014), Resilient consensus of double-integrator multi-agent systems, in ‘Proceedings of the American Control Conference’, Portland, OR, USA, pp. 5139–5144.
- Dibaji, S. M., Ishii, H. & Tempo, R. (2018), ‘Resilient randomized quantized consensus’, *IEEE Transactions on Automatic Control* **63**(8), 2508–2522.
- Ding, Z. (2013), ‘Consensus output regulation of a class of heterogeneous nonlinear systems’, *IEEE Transactions on Automatic Control* **58**(10), 2648–2653.
- D’Innocenzo, A., Smarra, F. & Di Benedetto, M. D. (2016), ‘Resilient stabilization of multi-hop control networks subject to malicious attacks’, *Automatica* **71**, 1–9.
- Franco, E., Magni, L., Parisini, T., Polycarpou, M. M. & Raimondo, D. M. (2008), ‘Cooperative constrained control of distributed agents with nonlinear dynamics and delayed information exchange: A stabilizing receding-horizon approach’, *IEEE Transactions on Automatic Control* **53**(1), 324–338.
- Gallo, A. J., Turan, M. S., Boem, F., Ferrari-Trecate, G. & Parisini, T. (2018), Distributed watermarking for secure control of microgrids under replay attacks, in ‘Proceedings of the 7th IFAC Workshop on Distributed Estimation and Control in Networked Systems’, Groningen, The Netherlands, pp. 182–187.
- Khalili, M., Zhang, X., Cao, Y., Polycarpou, M. M. & Parisini, T. (2018), ‘Distributed adaptive fault-tolerant leader-following formation control of nonlinear uncertain second-order multi-agent systems’, *International Journal of Robust and Nonlinear Control* **28**(15), 4287–4308.
- LeBlanc, H. J. & Koutsoukos, X. (2018), ‘Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multi-agent systems’, *IEEE Transactions on Control of Network Systems* **5**(3), 1219–1231.
- LeBlanc, H. J., Zhang, H., Koutsoukos, X. & Sundaram, S. (2013), ‘Resilient asymptotic consensus in robust networks’, *IEEE Journal on Selected Areas in Communications* **31**(4), 766–781.
- Mitra, A., Abbas, W. & Sundaram, S. (2018), On the impact of trusted nodes in resilient distributed state estimation of LTI systems, in ‘Proceedings of the 57th IEEE Conference on Decision and Control’, Miami Beach, FL, USA, pp. 4547–4552.
- Moghadam, R. & Modares, H. (2018), ‘Resilient adaptive optimal control of distributed multi-agent systems using reinforcement learning’, *IET Control Theory & Applications* **12**(16), 2165–2174.
- Mustafa, A. & Modares, H. (2020), ‘Attack analysis and resilient control design for discrete-time distributed multi-agent systems’, *IEEE Robotics and Automation Letters* **5**(2), 369–376.
- Mustafa, A., Modares, H. & Moghadam, R. (2020), ‘Resilient synchronization of distributed multi-agent systems under attacks’, *Automatica* **115**, 108869.
- Nowzari, C. & Cortes, J. (2016), ‘Team-triggered coordination for real-time control of networked cyber-physical systems’, *IEEE Transactions on Automatic Control* **61**(1), 34–47.
- Olfati-Saber, R. & Murray, R. M. (2004), ‘Consensus problems in networks of agents with switching topology and time-delays’, *IEEE Transactions on Automatic Control* **49**(9), 1520–1533.
- Pasqualetti, F., Bicchi, A. & Bullo, F. (2009), On the security of linear consensus networks, in ‘Proceedings of the 48th IEEE Conference on Decision and Control held jointly with the 28th Chinese Control Con-

- ference', Shanghai, China, pp. 4894–4901.
- Pasqualetti, F., Bicchi, A. & Bullo, F. (2012), 'Consensus computation in unreliable networks: A system theoretic approach', *IEEE Transactions on Automatic Control* **57**(1), 90–104.
- Ren, W. (2007), 'Multi-vehicle consensus with a time-varying reference state', *Systems & Control Letters* **56**(7-8), 474–483.
- Rezaee, H. & Abdollahi, F. (2015), 'Average consensus over high-order multiagent systems', *IEEE Transactions on Automatic Control* **60**(11), 3047–3052.
- Rezaee, H. & Abdollahi, F. (2019), 'Resilient attitude alignment in multispacecraft systems', *IEEE Transactions on Aerospace and Electronic Systems* **55**(6), 3651–3657.
- Rezaee, H., Abdollahi, F. & Talebi, H. A. (2014), ' $\mathcal{H}_\infty$  based motion synchronization in formation flight with delayed communications', *IEEE Transactions on Industrial Electronics* **61**(11), 6175–6182.
- Smith, R. S. (2015), 'Covert misappropriation of networked control systems: Presenting a feedback structure', *IEEE Control Systems Magazine* **35**(1), 82–92.
- Sun, Z. & Ge, S. S. (2005), *Switched Linear Systems: Control and Design*, Springer-Verlag London, London, UK.
- Teixeira, A., Shames, I., Sandberg, H. & Johansson, K. H. (2015), 'A secure control framework for resource-limited adversaries', *Automatica* **51**, 135–148.
- Usevitch, J. & Panagou, D. (2018), Resilient leader-follower consensus to arbitrary reference values, in 'Proceedings of the American Control Conference', Milwaukee, WI, USA, pp. 1292–1298.
- Usevitch, J. & Panagou, D. (2019), Resilient leader-follower consensus with time-varying leaders in discrete-time systems, in 'Proceedings of the 58th IEEE Conference on Decision and Control', Nice, France, pp. 5432–5437.
- Wu, Y. & He, X. (2017), 'Secure consensus control for multiagent systems with attacks and communication delays', *IEEE/CAA Journal of Automatica Sinica* **4**(1), 136–142.
- Yu, L., Zheng, G. & Barbot, J. (2017), 'Dynamical sparse recovery with finite-time convergence', *IEEE Transactions on Signal Processing* **65**(23), 6146–6157.
- Zhan, X.-S., Cheng, L.-L., Wu, J. & Yan, H.-C. (2019), 'Modified tracking performance limitation of networked time-delay systems with two-channel constraints', *Journal of the Franklin Institute* **356**(12), 6401–6418.
- Zhan, X.-S., Wu, J., Jiang, T. & Jiang, X.-W. (2015), 'Optimal performance of networked control systems under the packet dropouts and channel noise', *ISA Transactions* **58**, 214–221.
- Zhang, H. & Sundaram, S. (2012), Robustness of information diffusion algorithms to locally bounded adversaries, in 'Proceedings of the American Control Conference', Montreal, QC, Canada, pp. 5855–5861.
- Zhang, Q. & Zhang, J. (2012), 'Distributed parameter estimation over unreliable networks with Markovian switching topologies', *IEEE Transactions on Automatic Control* **57**(10), 2545–2560.