Secure Consensus Control for Multi-Agent Systems With Attacks and Communication Delays

Yiming Wu and Xiongxiong He

***Abstract*—This paper addresses the consensus problem for nonlinear multi-agent systems suffering from attacks and communication delays. The network studied in this paper consists of two types of agents, namely, loyal agents and attack agents. The loyal agents update their states based on delayed state information exchanged with their neighbors. Meanwhile, the attack agents can strategically send messages with wrong values, or collude with other attack agents to disrupt the correct operation of the system. We design a novel delay robust secure consensus (DRSC) algorithm according to the neighboring nodes' delayed information. Convergence analysis of the system under the protocol designed is provided by using Lyapunov-Krasovskii stability theory and Barbalat-like argument approach. Finally, an example and simulation results are presented to demonstrate the effectiveness of the algorithm.**

***Index Terms*—Consensus, delay systems, multi-agent systems, security.**

I. Introduction

DISTRIBUTED control over multi-agent networks is an area that has received significant attention from the systems and control community recently. In multi-agent networks, consensus control as a fundamental distributed control problem has been a hot topic in the past decade due to its wide applications such as sensor networks, traffic control, time synchronization and formation flying. A number of authors have investigated the consensus problems from various perspectives in recent works; see [1]−[10] and references therein.

Recently, the security and resilience of consensus against malicious attackers in multi-agent systems has attracted attention of researchers. A first study of the resilience of consensus to malicious attacks appears in [11], where the authors consider the task of agreeing upon a common value sent by loyal nodes, when the network graph is not completely connected. The work [12] studies the security of linear consensus networks for both non-colluding and Byzantine attacks. In [13], [14], a novel graph-theoretic property in terms of network robustness is developed, based on which a consensus protocol that is resistant to Byzantine nodes is proposed. The results have been later extended to the case of second-order multi-agent systems in the recent work [15]. In order to relax the requirement of high network connectivity and some non-local information, the authors of [16] propose an resilient consensus strategy by setting a trusted node set within the network. They prove that, when the trusted nodes make up a connected dominating set, the network under this strategy can be resilient to any number of malicious attackers. Furthermore [17] provides a reputation-based resilient control protocol for both leader-follower and leaderless consensus networks in the presence of misbehaving nodes. Besides the above works, researchers also investigate some iteration-based consensus protocols against malicious nodes [18]−[20].

Most of the works mentioned above assume an ideal communication channel among agents, i.e., each agent receives the real-time states from its neighbors. It should be noted that in real dynamical systems, delays are unavoidable in information acquisition and transmission. An initial study on consensus problems with delays can be found in [2], where a necessary and sufficient condition in terms of the upper bound of time delays is provided to guarantee the consensus. In [21], a consensus analysis of a linear continuous-time system with non-uniform delays is provided. For multi-agent systems with discrete dynamics and time-varying topologies, the authors of [22] introduce a kind of novel consensus protocols that are based on repeatedly utilizing the same data at two time-steps. In the presence of both delays and measurement noises, a stochastic approximation theory based consensus protocol is proposed in [23], and necessary and sufficient conditions are obtained for achieving consensus under non-leader-follower and leader-follower cases, respectively. By introducing dynamic encoder and decoder, a consensus protocol is designed in [24] so that an exact consensus can be achieved when both quantization and delay exist in transmission channels.

It can be seen that most of the above works deal with the consensus problem with adversarial attacks and communication delays separately. However, attacks and delays may coexist in real multi-agent networks. As indicated in [25], some adversarial nodes even have the ability to launch message-delay attacks in communication channels via specific technique. To the best of our knowledge, only a few works involved the consensus problems in delayed dynamic networks with attackers.

Manuscript received March 19, 2015; accepted October 13, 2015. This work was supported by National Natural Science Foundation of China (61473262). Recommended by Associate Editor Zhigang Zeng.

Citation: Y. M. Wu and X. X. He, "Secure consensus control for multi-agent systems with attacks and communication delays," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 136−142, Jan. 2017.

Y. M. Wu and X. X. He are with the College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: yimgwu@hotmail.com; hxx@zjut.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2016.7510010

The motivation of this work is to extend the consensus in the existing results to a nonlinear network with both attackers and delays. Specifically, in this paper we assume a directed time-delayed multi-agent network, in which two classes of agents are considered: loyal and attack agents. The loyal agents will follow a properly designed control law all the time, while the attack agents will not obey the law and can update their states arbitrarily (with a malicious goal). Most existing algorithms require agents to share some global information or know the identities of their neighbors. In our scheme, we develop a distributed coordinated control law by using local delayed neighbors' information. The system we consider allows for time dependent communication properties which are very important when our scheme take into account random link removal and creation, nearest node coupling and reconfigurable communication networks. Sufficient conditions are given based on which asymptotic consensus of all loyal agents can be guaranteed.

The rest of this paper is organized as follows. Some useful preliminary results are reviewed in Section II. The problem under investigation is formulated in Section III. The main results are presented in Section IV. A simulation example is given in Section V. Some conclusions are given in Section VI.

The following notation will be used throughout the paper: The set of real numbers (respectively, n-dimensional real Euclidean space, set of $m \times n$ real matrix) is denoted by $\mathbb{R}$ (respectively, $\mathbb{R}^n$, $\mathbb{R}^{m\times n}$). The set of all integers (respectively, positive integers) is denoted by $\mathbb{Z}$ (respectively, $\mathbb{Z}^+$). For $\tau \geq 0$, $\mathcal{C} = \mathcal{C}([-\tau, 0], \mathbb{R}^n)$ stands for the Banach space of continuous functions mapping the interval $[-\tau, 0]$ into $\mathbb{R}^n$ with the topology of uniform convergence. The norm on $\mathcal{C}$ is defined as $\|\phi\| = \sup_{-\tau<\theta<0} |\phi(\theta)|$. Moreover, let $x \in \mathcal{C}([-\tau, 0], \mathbb{R}^n)$, then, for brevity, we denote $x_t = x(t + \theta)$, $\theta \in [-\tau, 0]$.

II. Preliminaries and Assumptions

In this section, we briefly introduce some definitions and basic properties of functional differential equations, graph theory, and attack model that are needed in our later development.

A. Stability of Functional Differential Equations

Here we give a brief review of stability properties for functional differential equations. For more details, see [26], [27].

Consider an autonomous retarded functional differential equation:

$$\dot{x}(t) = f(x_t) \tag{1}$$

where $\Omega \in \mathcal{C}$ and $f : \Omega \to \mathbb{R}^n$. Given $\varphi \in \mathcal{C}$ and scalar $\rho > 0$, we say that a function $x(\varphi)$ is a solution to (1) on $[-\tau, \rho)$ with initial condition φ, if $x \in \mathcal{C}([-\tau, \rho), \mathbb{R}^n), x_t \in \Omega$, $x(t)$ satisfies (1) for $t \in [0, \rho)$ and $x(\varphi)(0) = \varphi$.

Definition 1 (ω-limit set [26]): Let $\varphi \in \Omega$. An element $\psi \in \Omega$ is said to be in the ω-limit set of φ (denoted as $\omega(\varphi)$), if $x(\varphi)(t)$ is defined on $[-\rho, \infty)$ and there is a sequence of nonnegative real numbers $t_n \to \infty$ as $n \to \infty$ such that $\|x_{t_n}(\varphi) - \psi\| \to 0$ as $n \to \infty$.

Definition 2 (positively invariant set [26]): A set $M \subset \Omega$ is said to be positively invariant for (1) if for any φ in M there is a solution $x(\varphi)(t)$ of (1) that is defined on $[-\tau, \infty)$ such that $x_t \in M$ for all $t \geq 0$ and $x_0 = \varphi$.

If $x(\varphi)(t)$ is a solution to (1) which is defined and bounded on $[-\tau, \infty)$, then 1) the orbit through φ, i.e., the set $\{x_t(\varphi) : t \geq 0\}$ is precompact, 2) $\omega(\varphi)$ is non-empty, compact, connected and invariant, and 3) $x_t(\varphi) \to \omega(\varphi)$ as $t \to \infty$.

For a given Lyapunov-Razumikhin function $V = V(x)$, $V : D \to \mathbb{R}$, $D \subseteq \mathbb{R}^n$, the upper right-hand derivative of V with respect to (1) is defined by:

$$D^+V(\phi) = \lim_{h\to 0^+} \sup \frac{1}{h}(V(\phi(0) + hf(\phi)) - V(\phi(0))).$$

Given a set $\Omega \subset \mathcal{C}$, we define:

$$\begin{aligned} E_V = \{\varphi \in \Omega : & \max_{s\in[-\tau,0]} V(x_t(\varphi)(s)) \\ & = \max_{s\in[-\tau,0]} V(\varphi(s)), \forall t \geq 0\} \end{aligned} \tag{2}$$

$$M_V = \text{Largest set in } E_V. \tag{3}$$

Note that M_V is the set of functions $\varphi \subset \Omega$ which can serve as initial conditions for (1) such that $x_t(\varphi)$ satisfies

$$\max_{s\in[-\tau,0]} V(\varphi(s)) = \max_{s\in[-\tau,0]} V(x_t(\varphi)(s))$$

for $t \in (-\infty, \infty)$. Consequently, for a Lyapunov-Razumikhin function $V(x)$ and for any $\varphi \in E_V$, we have $D^+V(x_t(\phi)) = 0$ for any time $t > 0$ such that $\max_{-\tau\leq s\leq 0} V(x_t(\varphi)(s)) = V(x_t(\varphi)(0))$. Then, we have the following result.

Lemma 1: Assume that there exists a Lyapunov-Razumikhin function $V = V(x)$ and a closed set Ω which is positively invariant with respect to (1) such that

$$\begin{aligned} & D^+V(\varphi) \leq 0, \quad \forall \varphi \in \Omega \\ & \text{s.t.} \quad V(\varphi(0)) = \max_{-\tau\leq s\leq 0} V(\varphi(s)). \end{aligned} \tag{4}$$

Then, for any $\varphi \in \Omega$ such that $x(\varphi)(\cdot)$ is defined and bounded on $[-\tau, \infty), \omega(\varphi) \subseteq M_V \subseteq E_V$, and we have

$$x_t(\varphi) \to M_V \quad \text{as} \quad t \to \infty. \tag{5}$$

Let $h : (a, b) \to \mathbb{R}$ be a continuous function on (a, b). h is non-increasing on (a, b) if and only if $D^+h(t) \leq 0$ for any $t \in (a, b)$. The following lemma will be useful in the rest of the development [28], [29].

Lemma 2: Let $\mathcal{I}_0 = \{1, 2, \ldots, n\}$. For $i \in \mathcal{I}_0$, let $V_i(t, x) : \mathbb{R} \times \mathbb{R}^m \to \mathbb{R}$ be C^1 and $V(t, x) = \max_{i=1,2,\ldots,n} V_i(t, x)$. Then we have

$$D^+V(t, x(t)) = \max_{i\in\mathcal{I}(t)} \dot{V}_i(t, x(t)) \tag{6}$$

where $\mathcal{I}(t)$ is the set of indices of the maximum of $V_i(t, x(t))$ at time t, i.e., $\mathcal{I}(t) = \{i \in \mathcal{I}_0 | V_i(t, x(t)) = V(t, x(t))\}$.

B. Graph Theory

A directed weighted graph of order N is denoted by $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\mathcal{G}}, A_{\mathcal{G}}\}$, where $\mathcal{V} = \{1, 2, \ldots, N\}$ is a finite set of nodes (representing the agents); $\mathcal{E}_{\mathcal{G}}$ is a set of edges which are represented by pairs of node indices (i, j). For an edge $(i, j) \in \mathcal{E}_{\mathcal{G}}$, we say that i is the parent node, and j is the child node. We say that node i has self-loop if $(i, i) \in \mathcal{E}_{\mathcal{G}}$. Here, we assume the graph excludes self-loop. The neighbor set of node i is defined by $\mathcal{N}(\mathcal{G}, i) = \{j \in \mathcal{V} | (j, i) \in \mathcal{E}_{\mathcal{G}}\}$. The adjacency matrix $A_{\mathcal{G}}$ is a matrix representation of $\mathcal{G}$ with $[A_{\mathcal{G}}]^{i,j} = a_{i,j}$ for $(j, i) \in \mathcal{E}_{\mathcal{G}}$ and $[A_{\mathcal{G}}]^{i,j} = 0$, otherwise. A path from node i to node j in $\mathcal{G}$ is a sequence of ordered edges of the form $(i, e_1), \ldots, (e_p, j) \in \mathcal{E}_{\mathcal{G}}$, where $i, j, e_1, \ldots, e_p$ are distinct nodes. $\mathcal{G}$ contains a directed tree if each node in the graph has exactly one parent node, except one node which is called the root. Then, we say that $\mathcal{G}$ contains a spanning tree if a subset of the edges forms a directed tree that connects every other node through paths. Given a piecewise constant function $\sigma : \mathbb{R} \geq 0 \rightarrow \mathcal{Q}$, where $\mathcal{Q}$ is a finite set which indicates the possible communication topologies, let $\mathcal{G}_{\sigma(t)} = \{\mathcal{V}, \mathcal{E}_{\sigma(t)}, A_{\sigma(t)}\}$ denote a time-varying graph.

C. Attack Model

The attack agents in the system are rational and participate with the goal of preventing other agents from achieving consensus or driving their values into an invalid value (unsafe region). According to their attack characteristics, attack agents in existing works can be classified as crash failure [30], non-colluding [20], malicious [18], [31] and Byzantine [32], [33] agents. One type of attack agent is called Byzantine agent, which usually has a complete knowledge of the whole system and possesses an unlimited capability of communication and computation. It can update its state in an arbitrary way and send different information to distinct neighbors at the same time. In most networks, Byzantine agent represents the worst-case attacker, and therefore some algorithms working correctly in networks with Byzantine attacker can be safely used under any assumptions involving attackers. In this paper, we just consider Byzantine agent as the attack agent.

It is clear that consensus cannot be achieved when attack agents become the majority of the network. So, it is necessary to restrict the number of attack agents. There are several models based on the number and location of attackers. One of these models is k-locally bounded, in which at most k permanent neighbors of each agent in the network may be attacker. We will refer to this attack model as the "k-locally bounded Byzantine model".

III. Problem Statement

The system to be considered is assumed to have N agents with n_l loyal agents and $n_a = N - n_l$ attack agents. Each agent in the network is regarded as a node which connects with each other via a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\mathcal{G}}, A_{\mathcal{G}}\}$. We denote by $\mathcal{V}_l$ and $\mathcal{V}_a$ the node set of the loyal nodes and the node set of attack nodes, respectively. It is clear that $\mathcal{V}_l \cup \mathcal{V}_a = \mathcal{V}$ and $\mathcal{V}_l \cap \mathcal{V}_a = \emptyset$.

Each loyal node i is assumed to take the following dynamics:

$$\dot{x}_i(t) = u_i(t), \quad i \in \mathcal{V}_l \tag{7}$$

where $x_i(t) \in \mathbb{R}$ and $u_i(t) \in \mathbb{R}$ represent the state value and control input of agent i, respectively. In multi-agent networked systems, the received state information from neighbors are often delayed due to transmission delay. Let $\tau_{i,j} \geq 0$ be the non-uniform constant delay from node j to node i, and assume that the delays are bounded, i.e., $\tau_{i,j} \leq \tau_{\max}, \forall i, j \in \mathcal{V}$, where $\tau_{\max}$ is a positive constant.

The objective of this paper is to design a consensus protocol $u_i(t)$ under which all loyal nodes can resist attackers and resiliently achieve an agreement as time goes to infinity.

Now we present the detailed description of the delay-robust secure consensus (DRSC) protocol: For node $i \in \mathcal{V}_l$, it senses or receives the delayed state information of its neighbors at time t, and then sorts these data in a descending order. If there are less than k neighbor nodes whose delayed state information received by i larger than $x_i(t)$, then the loyal node i removes all of these nodes' information by correspondingly cutting off the incoming edges. Otherwise, node i removes completely the largest k state information from the above sorted list. Similarly, If there are less than k neighbor nodes whose delayed state information received by i smaller than $x_i(t)$, then the loyal node i removes all of these nodes' information by correspondingly cutting off the incoming edges. Otherwise, node i removes completely the smallest k state information from the above sorted list.

It should be noted that while the previous network of the system (7) seems to be a fixed graph, the above algorithm involve manipulations of communication links can arbitrarily lead the network to a stochastically time-varying graph $\mathcal{G}_{\sigma(t)} = \{\mathcal{V}, \mathcal{E}_{\sigma(t)}, A_{\sigma(t)}\}$. Then, we denote by $\mathcal{N}(\mathcal{G}_{\sigma(t)}, i)$ the set of agents whose information are received and kept by i after the corresponding manipulations.

Then the control protocol for i is proposed as:

$$u_i(t) = \sum_{j \in \mathcal{N}(\mathcal{G}_{\sigma(t)}, i)} a_{i,j}(t) f_{i,j}(x_j(t - \tau_{i,j}), x_i(t)), \quad i \in \mathcal{V}_l \tag{8}$$

where $a_{i,j}(t)$ is the (i, j)th entry of the adjacency matrix at time t and $f_{i,j}$ is the nonlinear function. To facilitate our analysis, we impose the following assumptions:

Assumption 1: The nonlinear function $f_{i,j}$ $(\mathbb{R} \times \mathbb{R}) \rightarrow \mathbb{R}$ in (8) is assumed to hold the following properties: 1) $f_{i,j}$ is a continuous mapping and satisfies the local Lipschitz condition with a Lipschitz constant, 2) $f_{i,j}(x, y) = 0 \Leftrightarrow x = y$, and 3) $(x - y) f_{i,j}(x, y) > 0, \forall x \neq y$.

Assumption 2: There exist scalars $\bar{a}^1 \geq \bar{a}^2 > 0$, such that $\bar{a}^2 \leq a_{i,j}(t) \leq \bar{a}^1$ for all t and $(j, i) \in \mathcal{E}_{\sigma(t)}$.

Assumption 3: Denote $\{t_k\}_{k\in\mathbb{Z}^+}$ as the set of all switching time instants of $\sigma(t)$. There exists a scalar $\tau_D > 0$ for $\sigma(t)$, as a lower bound between any two instants, i.e., $t_{k+1} - t_k \geq \tau_D$.

Using protocol (8) for time-delayed multi-agent system (7), we obtain the closed-loop network dynamics as

$$\begin{cases} \dot{x}_i(t) = \sum\limits_{j\in\mathcal{N}(\mathcal{G}_{\sigma(t)},i)} a_{i,j}(t) f_{i,j}(x_j(t-\tau_{i,j}), x_i(t)) \\ \qquad\qquad\qquad\qquad\qquad\qquad i \in \mathcal{V}_l; \;\; t > 0 \\ x_i(\varphi) = \varphi_i(t), \;\; t \in [-\tau_{\max}, 0]. \end{cases} \tag{9}$$

Note that for resilient protocol (8) above, each loyal node may remove up to $2k$ values from the information it received. However, when the attack nodes' state information are not inside the range of the top and bottom k values of the sorted list. Under this case, it may possibly lead to loyal nodes adopt these attack nodes' values for updating their own states. This special attack node is summarized in the following definition.

Definition 3: A mild attack node is a attack node q, $q \in \mathcal{V}_a$ whose state information is received and kept by its loyal neighbor p, $p \in \mathcal{V}_l$ under the protocol (8). Then, its state $x_q(t)$ can be expressed as a convex combination of all the delayed state information of all loyal nodes. i.e.,

$$x_q(t) = \sum_{j\in\mathcal{V}_l} \varphi_{p,j}(t) x_j(t+\theta) \qquad q \in \mathcal{V}_a \cap \mathcal{N}(\mathcal{G}_{\sigma(t)}, i); \;\; \theta \in [-\tau_{\max}, 0] \tag{10}$$

where the scalars $\varphi_{p,j}(t) \in \mathbb{R}$ satisfy: 1) $0 \leq \varphi_{p,j}(t) \leq 1$ and 2) $\sum_{j\in\mathcal{V}_l} \varphi_{p,j}(t) = 1$.

Define

$$V_M(t) = \max_{i=1,2,\ldots,n_l} x_i(t), \quad V_m(t) = \min_{i=1,2,\ldots,n_l} x_i(t) \tag{11}$$

as the maximum and minimum values within all the loyal nodes at time t. Moreover, let $V_M(\varphi) = \gamma^+$ and $V_m(\varphi) = \gamma^-$ be the maximum and minimum within all loyal nodes under initial values, respectively.

Definition 4: We say that system (7) achieves a secure consensus if the following two conditions are satisfied:

$$V_m(\varphi) \leq \inf_{t\geq 0} \min_{i\in\mathcal{V}_l} x_i(t) \leq \sup_{t\geq 0} \max_{i\in\mathcal{V}_l} x_i(t) \leq V_M(\varphi) \tag{12}$$

$$\lim_{t\to\infty} (x_i(t) - x_j(t)) = 0 \;\; \forall\, i, j \in \mathcal{V}_l. \tag{13}$$

Remark 1: In Definition 4, condition (12) ensures that all loyal nodes are within the secure interval determined by their maximal and the minimal initial values. It is equal to that for any $t \geq 0$, $V_m(t) \geq \gamma^-$ and $V_M(t) \leq \gamma^+$. On the other hand, condition (13) ensures all loyal nodes eventually converge to the same state.

IV. Main Results

In this section, we shall first introduce some useful topological features, and then we prove the convergence property of the proposed consensus protocol (8).

Below we introduce some definitions of network robustness which are adopted with minor changes, from [13].

Definition 5 (r-reachable set): Consider a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\sigma(t)}\}$ and a nonempty subset $S \subset \mathcal{V}$. The set $\mathcal{S}$ is called an r-reachable set if there exists a node $i \in \mathcal{S}$ such that $|\mathcal{N}_i \backslash \mathcal{S}| \geq r$, $r \in \mathbb{Z}^+$.

From the above definition, we can observe that an r-reachable set $\mathcal{S}$ contains a node which has at least r neighboring nodes outside of $\mathcal{S}$ at all times $t \in \mathbb{R}$. Then we have the following definition of r-robust graph.

Definition 6 (r-robust graph): Consider a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_{\sigma(t)}\}$. The graph is called an r-robust graph if for every pair of nonempty, disjoint subsets of $\mathcal{V}$, denoted as $\mathcal{V}_1$ and $\mathcal{V}_2$, there are at least one node $i \in \mathcal{V}_\kappa$, such that $|\mathcal{N}_i \backslash \mathcal{V}_\kappa| \geq r$, $r \in \mathbb{Z}^+$, $\kappa = 1, 2$.

By employing the notion of robustness, some properties of the r-robust graph are recalled below.

Lemma 3: Given an r-robust graph $\mathcal{G}$, let $\mathcal{G}'$ be the graph generated by removing up to s $(s < r)$ incoming edges of each node in $\mathcal{G}$, then, we have that $\mathcal{G}'$ is $(r-s)$-robust.

Lemma 4: Let $\mathcal{G}$ be a directed graph. The network contains a directed spanning tree, if and only if $\mathcal{G}$ is 1-robust.

Proof: 1) Necessity. We prove this by contradiction. Assume $\mathcal{G}$ contains a directed spanning tree but it is not a 1-robust graph. By Definition 6, we know there exists two disjoint subsets $\mathcal{V}_1$ and $\mathcal{V}_2$ of $\mathcal{V}$, which do not have neighboring nodes from outside their own sets. That means there is no information flow between $\mathcal{V}_1$ and $\mathcal{V}_2$, which contradicts the assumption that $\mathcal{G}$ contains a spanning tree.

2) Sufficiency. By contradiction, we first assume $\mathcal{G}$ does not contain a directed spanning tree. Let A denote the adjacency matrix of $\mathcal{G}$. According to [34], [35], we get that A can be decomposed, which means the set of nodes $\mathcal{V}$ can be partitioned into two subsets with no information flow from one to another. ■

Lemma 5: Consider the multi-agent system (7) with bounded communication delays. Assume each loyal node in the network updates its state according to consensus protocol (8), then one can show that for any node i, $i \in \mathcal{V}_l$, $x_i(t) \in [\gamma^-, \gamma^+]$ for all $t \geq -\tau_{\max}$.

Proof: We will first prove that $x_i(t) \leq \gamma^+$. According to the bounds of initial values, we have that $x_i(\theta) \leq \gamma^+$ for $\theta \in [-\tau_{\max}, 0]$. Assume this condition is violated at time t^*. When this happens, the following must hold: $x_i(t) \leq \gamma^+$ for $t \in [-\tau_{\max}, t^*]$ for all $i \in \mathcal{V}_l$; At time t^* there exists a node $i \in \mathcal{V}_l$ such that we have $x_i(t^*) = \gamma^+$ and $\dot{x}_i(t^*) > 0$. Suppose above case holds. Recall node i' dynamics structure:

$$\dot{x}_i(t^*) = \sum_{j\in\mathcal{N}(\mathcal{G}_{\sigma(t)},i)} a_{i,j}(t) f_{i,j}(x_j(t^* - \tau_{i,j}), x_i(t^*)), \;\; i \in \mathcal{V}_l.$$

From the observations above, each term on the right hand side is non-positive as $x_i(t^*) = \gamma^+ \geq x_j(t^* - \tau_{i,j})$ and $a_{i,j}$ are positive weights; and therefore $\dot{x}_i(t^*) \leq 0$, which leads to a contradiction. The other direction $x_i(t) \geq \gamma^-$ can be easily verified by a similar analysis as above. ■

For initial condition $\varphi \in \mathcal{C}_D = \mathcal{C}([-\tau_{\max}, 0], D)$, the region of attraction D is given by

$$D = \{x \in \mathbb{R}^{n_l} : \gamma^- \leq x_i \leq \gamma^+\}. \tag{14}$$

It follows from Lemma 5 that set $\mathcal{C}_D$ of system (7) is positively invariant.

Considering system (7), a Lyapunov-Krasovskii functional is constructed as:

$$\bar{V}(x_t) = \bar{V}_M(x_t) + \bar{V}_m(x_t) \tag{15}$$

where

$$\bar{V}_M(x_t) = \max_{\theta_1 \in [0,\tau_{\max}]} V_M(x(t-\theta_1)) \tag{16}$$

and

$$\bar{V}_m(x_t) = -\min_{\theta_2 \in [0,\tau_{\max}]} V_m(x(t-\theta_2)). \tag{17}$$

Note that $\bar{V}(x_t)$ which involves the system (7) with dynamic topologies may not be continuously differentiable, however, it is continuous all the time. Based on this condition, we can analyze the Dini derivative of $\bar{V}(x_t)$ to study its convergence property. We denote I and J as the indices that satisfy $x_I(t) = \max_{i\in\mathcal{V}_l} x_i(t)$, $x_J(t) = \min_{i\in\mathcal{V}_l} x_i(t)$. There may exist several such indices, one could choose those with the maximal derivatives.

Theorem 1: Consider the nonlinear multi-agent system (7) under a $(2k+1)$-robust topology. Assume that each loyal node updates its state according to consensus protocol (8) with delayed neighbors' information, then the DRSC can be achieved under the k-locally bounded Byzantine model.

Proof: By Lemma 5, we know that the set containing all of the values of loyal nodes is positively invariant, and hence solutions $x_i(\varphi)(t)$, $i \in \mathcal{V}_l$ are bounded, which satisfies the safety requirement (12).

It remains to verify that the consensus condition (13) is also satisfied. For any graph topology $p \in \mathcal{Q}$, let $t^1 = t - \theta_1$ and $t^2 = t - \theta_2$, and based on Lemma 2, the Dini derivatives of $\bar{V}_M(x_t)$ and $\bar{V}_m(x_t)$ along the trajectory of (9) are given as

$$\begin{aligned} D^+\bar{V}_M(x_t) &= \dot{x}_I(t^1) \\ &= \sum_{j\in\mathcal{N}(\mathcal{G}_{\sigma(t^1)},I)} a_{I,j} f_{I,j}(x_j(t^1-\tau_{I,j}), x_I(t^1)), \quad I \in \mathcal{V}_l \end{aligned} \tag{18}$$

$$\begin{aligned} D^+\bar{V}_m(x_t) &= -\dot{x}_J(t^2) \\ &= -\sum_{j\in\mathcal{N}(\mathcal{G}_{\sigma(t^2)},J)} a_{J,j} f_{J,j}(x_j(t^2-\tau_{J,j}), x_J(t^2)), \ J \in \mathcal{V}_l. \end{aligned} \tag{19}$$

By combining (18) and (19), we have

$$\begin{aligned} D^+\bar{V}(x_t) &= D^+\bar{V}_M(x_t) + D^+\bar{V}_m(x_t) \\ &= \dot{x}_I(t^1) - \dot{x}_J(t^2) \\ &= \sum_{j\in\mathcal{N}(\mathcal{G}_{\sigma(t^1)},I)} a_{I,j} f_{i,j}(x_j(t^1-\tau_{I,j}), x_I(t^1)) \\ &\quad - \sum_{j\in\mathcal{N}(\mathcal{G}_{\sigma(t^2)},J)} a_{J,j} f_{i,j}(x_j(t^2-\tau_{J,j}), x_J(t^2)). \end{aligned} \tag{20}$$

From (20) above, one can find that the Dini derivatives of $\bar{V}_M(x_t)$ and $\bar{V}_m(x_t)$ are difficult to calculate directly. Fortunately, one can determine that both of them are non-positive according to a simple analysis of the following three situations. Here we first analyze the case of $D^+\bar{V}_M(x_t)$. Let a time instant $t^* \in [t-\tau_{\max}, t]$ be such that

$$x_I(t^*) = \max_{\theta\in[0,\tau_{\max}]} \max_{i\in\mathcal{V}_l} x_i(t-\theta). \tag{21}$$

Then, consider the following three situations.

1) $t^* = t - \tau_{\max}$: In this case, $D^+\bar{V}_M(x_t) < 0$, if and only if $t^* = t-\tau_{\max}$ satisfies (21) and meanwhile ensure that there is not a time instant $t^* \in (t-\tau_{\max}, t)$ satisfying (21) (see Fig. 1 (a)).

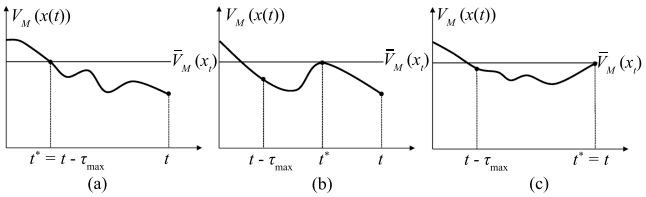


Fig. 1. Three situations of $D^+\bar{V}_M(x_t)$.

2) $t^* \in (t-\tau_{\max}, t)$: In this case, $D^+\bar{V}_M(x_t) = 0$, if and only if there is a time instant $t^* \in (t-\tau_{\max}, t)$ satisfying (21) (see Fig. 1 (b)).

3) $t^* = t$: While for this case, the value of $D^+\bar{V}_M(x_t)$ is not obvious. Since the state $x_I(t^*) = x_I(t) \geq x_j(t-\tau_{I,j})$ at this time instant, each term on the right hand of (18) is non-positive (see Fig. 1 (c)).

Thus, we can conclude that $D^+\bar{V}_M(x_t) \leq 0$. With the similar analysis, we can get that $D^+\bar{V}_m(x_t) \leq 0$, which is omitted here for brevity.

Now we will prove that under our topology conditions $D^+\bar{V}(x_t)$ tends to zero as $t \to \infty$. Suppose that $D^+\bar{V}(x_t)$ does not converge to zero as $t \to \infty$. Then, there must be a constant $\varepsilon_0 > 0$ such that $\forall T > 0$, there is a time instant $t > T$ such that $D^+\bar{V}(x_t) \leq -\varepsilon_0$ (note that $D^+\bar{V}(x_t) \leq 0$). Therefore, there must be a constant $\delta_0 > 0$ and an sequence of time $\{t_i\}_{i\in\mathbb{Z}^+}$, with t_i tends to infinity as $i \to \infty$, such that $\forall\, i$, $D^+\bar{V}(x_t) \leq -\varepsilon_0$ and $|t_{i+1} - t_i| > \delta_0$. Consider the time interval Δt on which $D^+\bar{V}(x_t)$ is continuous, i.e., $t_k \notin \Delta t$. According to Assumptions 1 and 2, we know that $\dot{x}_i(t)$ remain bounded, which guarantees that $D^+\bar{V}(x_t)$ is uniformly continuous on Δt. Therefore, there is a constant $\delta_1 > 0$ such that for any t^1 and t^2 such that $\left|t^1 - t^2\right| < \delta_1$, the inequality

$$\left|D^+\bar{V}(x_{t^1}) - D^+\bar{V}(x_{t^2})\right| < \frac{\varepsilon_0}{2}$$

holds. This implies that for any t within the δ_1-neighborhood of t_i, i.e., $t \in [t_i - \delta_1, t_i + \delta_1]$, we have

$$\begin{aligned} D^+\bar{V}(x_t) &= -\left|D^+\bar{V}(x_{t_i}) - (D^+\bar{V}(x_{t_i}) - D^+\bar{V}(x_t))\right| \\ &\le -(\left|D^+\bar{V}(x_{t_i})\right| - \left|D^+\bar{V}(x_{t_i}) - D^+\bar{V}(x_t)\right|) \\ &\le -\varepsilon_0 + \frac{\varepsilon_0}{2} = -\frac{\varepsilon_0}{2}. \end{aligned}$$

Next, we consider the situation where t_i is on the right side of a discontinuous time instant t_k. Under this case, the inequality $D^+\bar{V}(x_t) \le -\varepsilon_0/2$ might not hold if $t_k \in [t_i - \delta_1,\ t_i + \delta_1]$ as $D^+\bar{V}(x_t)$ may increase at t_k. However, according to Assumption 3, we know that there exists a dwell time τ_D until the next discontinuity. Therefore there must exist a $\delta_2 \in (0, \tau_D)$ such that $D^+\bar{V}(x_t) \le -\varepsilon_0/2$ for all $t \in [t_k, t_k + \delta_2]$. Integrating $D^+\bar{V}(x_t)$ over the time interval $(0, \infty)$, we have

$$\begin{aligned} \int_0^\infty D^+\bar{V}(x_t)dt &\le \lim_{N\to\infty} \sum_{i=1}^{N} \int_{t_i-\delta}^{t_i+\delta} D^+\bar{V}(x_t)dt \\ &\le -\lim_{N\to\infty} \sum_{i=1}^{N} \int_{t_i-\delta}^{t_i+\delta} \frac{\varepsilon_0}{2} dt \\ &= -\lim_{N\to\infty} N\varepsilon_0\delta = -\infty, \quad \delta \in \min\{\delta_1, \delta_2\}. \end{aligned}$$

This is obviously a contradiction to $\bar{V}(x_t) \ge 0$, for all time t. We have thus shown, by this contradiction, that $D^+\bar{V}(x_t) \to 0$ as t trends to infinity, which implies that $\lim_{t\to\infty}\bar{V}(x_t) = constant$, i.e., the nodes with maximum and minimum in the system eventually hold fixed values. For node I, this is equivalent to $\bar{V}_M(x_t) = x_I(t^1) = c_M$, as time t trends to infinity, where c_M is a constant value. Since the initial network is a $(2k+1)$-robust graph, after removing up to $2k$ incoming edges for each loyal node, the network is still 1-robust from Lemma 3. Then by applying Lemma 4, we know that the graph must exist a spanning tree, and consequently, all loyal nodes in the path from the root to node I possess the common state c_M. Then, let c_m be a constant and $\bar{V}_m(x_t) = x_J(t^2) = c_m$ as time t trends to infinity. With similar argument, we can get that all loyal nodes in the path from the root to node J possess the common state c_m. Since the root in the network possesses both the maximum and the minimum states, we have $c_M = c_m$. ■

V. Numerical Example

In this section, we present one numerical example to validate the effectiveness of our proposed algorithm. Suppose we have 5 agents disposed on a digraph as in Fig. 2 and suppose agent 2 is an attack agent. The initial conditions of the five agents' states are assigned as $x(\varphi) = [5, 4, 3, 2, 1]^T$ for $\varphi \in [-\tau_{\max}, 0]$. We set the upper delay bound $\tau_{\max} = 1\,\text{s}$ in the simulation. To illustrate Theorem 1, let the interaction graph be 3-robust. Note that, in order to verify the network is 3-robust, we must thoroughly check any disjoint, nonempty pair of subsets of agents to make sure that the network with one agent in either of the two subsets has at least 3 neighbors outside of its own set. Let $\tau_{1,2} = \tau_{1,4} = \tau_{1,5} = 0.4\,\text{s}$, $\tau_{3,2} = \tau_{3,4} = \tau_{3,5} = 0.5\,\text{s}$, $\tau_{4,1} = \tau_{4,2} = \tau_{4,3} = \tau_{4,5} = 0.6\,\text{s}$, $\tau_{5,1} = \tau_{5,2} = \tau_{5,3} = \tau_{5,4} = 0.7\,\text{s}$ in (9). The nonlinear function is chosen as $f_{i,j}(x, y) = \arctan(x - y)$ for each loyal agent. It is obvious that $f_{i,j}(\cdot)$ satisfies the local Lipschitz condition. The dynamics of the attacker (agent 2) is designed as

$$\dot{x}_2(t) = -0.8x_2(t) + 0.8u$$

where the attacker' malicious input $u = 8$. Let the adjacency matrix $A(t) = [a_{i,j}(t)] \in \mathbb{R}^{n\times n}$ be

$$A(t) = \begin{bmatrix} 0 & 2 & 0 & 1 & 3 \\ 1 & 0 & 2 & 2 & 1 \\ 1 & 3 & 0 & 2 & 3 \\ 0 & 1 & 3 & 0 & 1 \\ 2 & 2 & 3 & 1 & 0 \end{bmatrix}$$

when $j \in \mathcal{N}_i(\sigma(t))$ and $a_{i,j}(t) = 0$ otherwise.

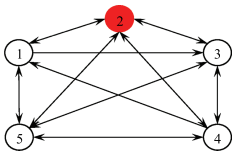


Fig. 2. Network topology.

Since the graph is the so-called 3-robust graph, Theorem 1 indicates that secure consensus can be achieved under this 1-locally bounded attack network. The agents' trajectories under the DRSC protocol (8) are shown in Fig. 3. It can be seen that the loyal agents are not affected by agent 2 and achieve resilient consensus. Furthermore, the results of DRSC in the network of Fig. 2 with and without attack are shown in Fig. 4. It can be seen that the convergence rate of consensus for multi-agent network without attack is slightly faster than with attack.

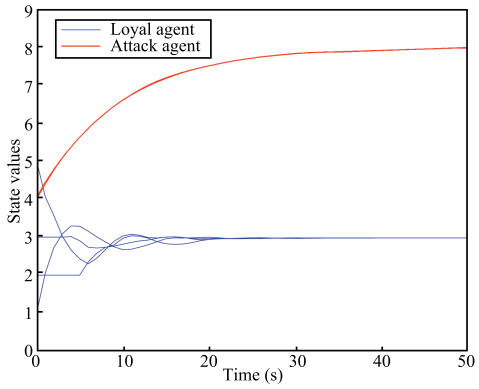


Fig. 3. State trajectories of the network with attack.

VI. Conclusion

In this paper, we have investigated the secure consensus problem of nonlinear multi-agent systems with attackers and bounded communication delays. The traditional approaches including Lyapunov analysis approach and Barbalat' lemma are not directly applicable to analyze the convergence property for the class of systems under attacks as well as delays. The results of this paper showed that if the network topology satisfies $(2k + 1)$-robust, the loyal agents under uniformly bounded communication delays can resist at most k neighboring attack agents to reach a consensus asymptotically. Finally, the effectiveness of the proposed algorithm has been validated via a numerical example.

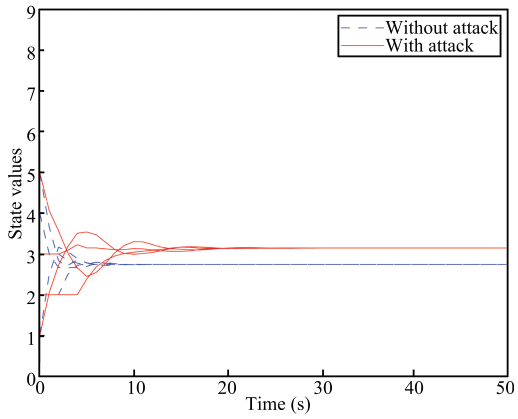


Fig. 4. Comparison of trajectories of the network with and without attack.

REFERENCES

[1] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Trans. Automat. Contr.*, vol. 48, no. 6, pp. 988−1001, Jun. 2003.

[2] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. Automat. Contr.*, vol. 49, no. 9, pp. 1520−1533, Sep. 2004.

[3] W. Ren and R. W. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Trans. Automat. Contr.*, vol. 50, no. 5, pp. 655−661, May 2005.

[4] M. Cao, A. S. Morse, and B. D. O. Anderson, "Reaching a consensus in a dynamically changing environment: a graphical approach," *SIAM J. Contr. Optimiz.*, vol. 47, no. 2, pp. 575−600, Feb. 2008.

[5] T. Li, M. Y. Fu, L. H. Xie, and J. F. Zhang, "Distributed consensus with limited communication data rate," *IEEE Trans. Automat. Contr.*, vol. 56, no. 2, pp. 279−292, Feb. 2011.

[6] S. Liu, T. Li, L. H. Xie, M. Y. Fu, and J. F. Zhang, "Continuous-time and sampled-data-based average consensus with logarithmic quantizers," *Automatica*, vol. 49, no. 11, pp. 3329−3336, Nov. 2003.

[7] N. Xiao, W. H. Wang, L. H. Xie, T. Wongpiromsarn, E. Frazzoli, and D. Rus, "Road pricing design based on game theory and multi-agent consensus," *IEEE/CAA J. Automat. Sin.*, vol. 1, no. 1, pp. 31−39, Jan. 2014.

[8] J. F. Gao, L. H. Feng, and Y. B. Zhang, "Improvement of consensus convergence speed for linear multi-agent systems based on state observer," *Neurocomputing*, vol. 158, pp. 26−31, Jan. 2015.

[9] Z. H. Wang, J. J. Xu, and H. S. Zhang, "Consensus seeking for discrete-time multi-agent systems with communication delay," *IEEE/CAA J. Automat. Sin.*, vol. 2, no. 2, pp. 151−157, Apr. 2015.

[10] Z. X. Wang, M. R. Fei, D. J. Du, and M. Zheng, "Decentralized event-triggered average consensus for multi-agent systems in CPSS with communication constraints," *IEEE/CAA J. Automat. Sin.*, vol. 2, no. 3, pp. 248−257, Jul. 2015.

[11] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382−401, Jul. 1982.

[12] F. Pasqualetti, A. Bicchi, and F. Bullo, "On the security of linear consensus networks," in *Proc. 48th IEEE Conf. Decision and Control, the 28th Chinese Control Conf.*, Shanghai, China, 2009, pp. 4894−4901.

[13] H. J. LeBlanc, H. T. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Select. Areas Commun.*, vol. 31, no. 4, pp. 766−781, Apr. 2013.

[14] H. T. Zhang and S. Sundaram, "Robustness of information diffusion algorithms to locally bounded adversaries," in *Proc. 2012 American Control Conf.*, Montreal, Canada, 2012, pp. 5855−5861.

[15] S. M. Dibaji and H. Ishii, "Consensus of second-order multi-agent systems in the presence of locally bounded faults," *Syst. Contr. Lett.*, vol. 79, pp. 23−29, May 2015.

[16] W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Resilient consensus protocol in the presence of trusted nodes," in *Proc. 7th Int. Symp. Resilient Control Systems*, Denver, CO, USA, 2014, pp. 1−7.

[17] W. T. Zeng and M. Y. Chow, "Resilient distributed control in the presence of misbehaving agents in networked control systems," *IEEE Trans. Cybernet.*, vol. 44, no. 11, pp. 2038−2049, Nov. 2014.

[18] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Automat. Contr.*, vol. 56, no. 7, pp. 1495−1508, Jul. 2011.

[19] N. H. Vaidya, L. Tseng, and G. F. Liang, "Iterative approximate byzantine consensus in arbitrary directed graphs," in *Proc. 2012 ACM Symposium on Principles of Distributed Computing*, Madeira, Portugal, 2012, pp. 365−374.

[20] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: a system theoretic approach," *IEEE Trans. Automat. Contr.*, vol. 57, no. 1, pp. 90−104, Jan. 2012.

[21] D. Lee and M. W. Spong, "Agreement with non-uniform information delays," in *Proc. 2006 American Control Conf.*, Minneapolis, MN, USA, 2006. pp. 756−761.

[22] F. Xiao and L. Wang, "Consensus protocols for discrete-time multi-agent systems with time-varying delays," *Automatica*, vol. 44, no. 10, pp. 2577−2582, Oct. 2008.

[23] S. Liu, L. H. Xie, and H. S. Zhang, "Distributed consensus for multi-agent systems with delays and noises in transmission channels," *Automatica*, vol. 47, no. 5, pp. 920−934, May 2011.

[24] S. Liu, T. Li, and L. H. Xie, "Distributed consensus for multiagent systems with communication delays and limited data rate," *SIAM J. Contr. Optimiz.*, vol. 49, no. 6, pp. 2239−2262, Nov. 2011.

[25] X. Hu, T. Park, and K. G. Shin, "Attack-tolerant time-synchronization in wireless sensor networks," in *Proc. 27th Conf. Computer Communications*, Phoenix, AZ, USA, 2008. pp. 448−456.

[26] J. R. Haddock and J. Terjéki, "Liapunov-razumikhin functions and an invariance principle for functional differential equations," *J. Differ. Equat.*, vol. 48, no. 1, pp. 95−122, Apr. 1983.

[27] A. Papachristodoulou, A. Jadbabaie, and U. Münz, "Effects of delay in multi-agent consensus and oscillator synchronization," *IEEE Trans. Automat. Contr.*, vol. 55, no. 6, pp. 1471−1477, Jun. 2010.

[28] J. M. Danskin, "The theory of max-min, with applications," *SIAM J. Appl. Math.*, vol. 14, no. 4, pp. 641−664, Aug. 1966.

[29] G. D. Shi, K. H. Johansson, and Y. G. Hong, "Reaching an optimal consensus: dynamical systems that compute intersections of convex sets," *IEEE Trans. Automat. Contr.*, vol. 58, no. 3, pp. 610−622, Mar. 2013.

[30] M. Raynal, "Fault-tolerant agreement in synchronous message-passing systems," *Synthesis Lectures on Distributed Computing Theory*. San Rafael, CA: Morgan & Claypool, 2010, pp. 1−189.

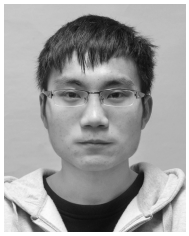
[31] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automat. Contr.*, vol. 58, no. 11, pp. 2715−2729, Nov. 2013.

[32] A. Ichimura and M. Shigeno, "A new parameter for a broadcast algorithm with locally bounded byzantine faults," *Inf. Process. Lett.*, vol. 110, no. 12−13, pp. 514−517, Jun. 2010.

[33] H. Moniz, N. F. Neves, and M. Correia, "Byzantine fault-tolerant consensus in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 12, pp. 2441−2454, Dec. 2013.

[34] E. Seneta, *Non-Negative Matrices and Markov Chains*. New York: Springer-Verlag, 2006.

[35] J. Wolfowitz, "Products of indecomposable, aperiodic, stochastic matrices," *Proc. Amer. Math. Soc.*, vol. 14, no. 5, pp. 733−737, Oct. 1963.



Yiming Wu received his B.E. degree in automation from Zhejiang University of Technology, China, in 2010. From 2012 to 2014, he worked as a research assistant at Nanyang Technological University, Singapore. Currently, he is working toward his Ph.D. degree in control science and engineering at Zhejiang University of Technology, China. His research interests include multi-agent systems, resilient consensus, and secure control systems.

Xiongxiong He received his M.S. degree from the Institute of Automation, Qufu Normal University, China, in 1994, and his Ph. D. degree from the Institute of Industrial Control Technology, Zhejiang University, China, in 1997. From 1998 to 2000, he was a postdoctor in Harbin Institute of Technology, China. Since 2000, he has been with the College of Information Engineering, Zhejiang University of Technology, where he is currently a professor. His current research interests include robotics, multi-agent systems, networked control systems, intelligent systems, and signal processing. Corresponding author of this paper.