Consensus of discrete-time multi-agent systems with adversaries and time delays

Yiming Wu[ab], Xiongxiong He[a], Shuai Liu[b] & Lihua Xie[b]

[a] College of Information Engineering, Zhejiang University of
Technology, Hangzhou, China.

[b] School of EEE, Nanyang Technological University, Singapore,
Singapore.
Published online: 04 Mar 2014.

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis
Taylor & Francis Group

Consensus of discrete-time multi-agent systems with adversaries and time delays

Yiming Wu[a,b], Xiongxiong He[a]*, Shuai Liu[b] and Lihua Xie[b]

[a]*College of Information Engineering, Zhejiang University of Technology, Hangzhou, China;* [b]*School of EEE, Nanyang Technological University, Singapore, Singapore*

This paper studies the resilient asymptotic consensus problem for discrete-time multi-agent systems in the presence of adversaries and transmission delays. The network is assumed to have p loyal agents and $n - p$ adversarial agents, and each loyal agent in the network has no knowledge of the network topology other than an upper bound on the number of adversarial agents in its neighborhood. For the considered networked system, only locally delayed information is available for each loyal agent, and also the information flow is directed and a control protocol using only local information is designed to guarantee the realization of consensus with respect to communication graph, which satisfies a featured network robustness. Numerical examples are finally given to demonstrate the effectiveness of theoretical results.

Keywords: multi-agent systems; discrete-time; resilient consensus; adversary; delay systems

1. Introduction

Consensus control means to design a networked interaction protocol such that all the agents reach an agreement on their certain variables of common interest states asymptotically or in a finite time (Liu, Xie, and Zhang 2011). Due to potential applications of multi-agent systems in broad areas such as distributed sensor networks, congestion control,the and formation flight, algorithms for consensus of multi-agent systems becomes a field that has been studied by numerous researchers from various perspectives; see Jadbabaie, Lin, and Morse (2003), Cortés and Bullo (2005), Paganini, Doyle, and Low (2001), Ren and Beard (2005), Fax and Murray (2004), Vidal, Shakernia, and Sastry (2003) and references therein. Several results have appeared in recent literature that consider systems with different motion models and network interactions (Liu, Xie, and Zhang 2013; Liu et al. 2013).

The resilient consensus problem for multi-agent systems involves designing a control protocol such that the networks are robust to the effects of adversaries. Pasqualetti, Bicchi, and Bullo (2009) considered two cases of adversaries, namely Byzantine and non-colluding faults. By considering Byzantine agents, they proved that if the connectivity of the communication graph is $2k + 1$, then a linear consensus network can be generically resilient to k concurrent faults, and $k + 1$ when consider non-colluding agents. LeBlanc and Koutsoukos (2011) presented the adversarially robust consensus protocol (ARC-P) combining ideas from distributed computing and control consensus protocols. It shows that ARC-P solves the consensus problem in complete networks whenever

---

*Corresponding author. Email: hxx@zjut.edu.cn

there are more fault-free agents than adversarial agents. In LeBlanc et al. (2013), the authors extended the results to the discrete-time model and weakened the condition of full knowledge of the network topology. In addition to the above works, some researchers also considered linear iterative schemes in presence of adversarial agents (Sundaram and Hadjicostis 2011; Pasqualetti, Bicchi, and Bullo 2012; Vaidya, Tseng, and Liang 2012).

Another important concern with respect to networked systems is the issue of communication delays. In practical networked multi-agent systems delays are unavoidable in information acquisition and transmission, which should be taken into consideration when designing a consensus protocol. An initial study on this problem can be found in Olfati-Saber and Murray (2004) using a frequency domain method, and a necessary and sufficient condition on the upper bound of time delays is provided under the assumption that all the delays are equal and time-invariant. Lee and Spong (2006) provided a stability analysis of a linear continuous-time system and showed the robustness of delays. The authors in Wang and Slotine (2006) studied non-linear time-delayed dynamics with a linear control law and a contraction theorem was applied to show consensus. Bliman and Ferrari-Trecate (2008) studied the continuous-time systems with transmission delays and provided a systematic way for analyzing the average consensus problem. In the presence of both delay and measurement noises, Liu, Xie, and Zhang (2011) proposed a consensus protocol based on stochastic approximation theorem. Necessary and sufficient conditions are provided for mean square consensus and strong consensus. When we consider quantization effect, Liu, Li, and Xie (2011) proved that the consensus can be achieved if we carefully design the dynamic quantizer.

In our work, we consider the consensus problem for discrete-time multi-agent systems in the presence of both adversaries and transmission delays. We assume a directed delayed network in which all agents belong to two disjoint classes: loyal agents and adversarial ones; loyal agents will follow the protocol all the time while, on the contrary, adversarial agents are rational and will attempt to alter the outcome so as to increase its utility. Every agent in the network, including the adversarial ones, sends the same information to all its neighbors, which appears to be realistic for control scenarios (Pasqualetti, Bicchi, and Bullo 2012). We consider the network-wide malicious adversary as the threat model. A malicious adversary has full knowledge of the networked system and may participate with the goal of leading the consensus process to an invalid value. To deal with this problem, we design an efficient consensus protocol while using only locally delayed information. The system allows for time-dependent communication patterns which are important when we take into account link failure and link creation, reconfigurable networks, and nearest-neighbor coupling. Based on a proposed control protocol, sufficient conditions are obtained which guarantee that all loyal agents asymptotically achieve a consensus under both adversaries and delays.

The rest of the paper is organized as follows: In Section 2, some preliminaries in graph theory are given, after which the problem to be considered is formulated. The main result is presented in Section 3. A numerical example is presented for illustration in Section 4. The conclusions are drawn in Section 5.

Before closing this section, some remarks on notation are given as follows. We denote by $\mathbb{R}$ (respectively $\mathbb{R}^n$, $\mathbb{R}^{m \times n}$) the set of real numbers (respectively n-dimensional real vectors, $m \times n$ real matrices). $\mathbb{Z}$ (respectively $\mathbb{Z}^+$) denotes the set of all integers (respectively positive integers). Given $A \in \mathbb{R}^{m \times n}$, $A^{i,j}$ means the element is on i-th row and j-th column of matrix A. I denotes the identity matrix with an appropriate size. For a pair of sets $\mathcal{S}$ and $\mathcal{T}$, $\mathcal{S} \backslash \mathcal{T}$ denotes the set of elements that are in $\mathcal{S}$ but not in $\mathcal{T}$. Sets $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_n$ are said to form a partition of set $\mathcal{S}$ provided that (i) $\cup_{1 \le i \le n} \mathcal{S}_i = \mathcal{S}$, and (ii) $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$ if $i \ne j$.

2. Problem statement

In this section, we will formulate the consensus problem in the presence of adversary agents and transmission time delays. Before that, some preliminaries in graph theory and adversary model are reviewed.

2.1. Preliminaries in graph theory

A directed graph, denoted by $\mathcal{G}$, with vertex set $\mathcal{V}$ and edge set $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is often used to model communications among agents. For convenience, we define $\mathcal{V} = \{1, 2, ..., n\}$, where n is the number of vertices. We consider that $(i, j) \in \mathcal{E}$ if and only if vertex (node) i can send its information to vertex j. If $(i, i) \in \mathcal{E}$, we say that vertex i has self-loop. The set of neighbors of vertex i is denoted by $\mathcal{N}_i = \{j \,|\, (j, i) \in \mathcal{E}\}$. We denote by $a_{i,j} \geq 0$ the weighting on the edge (j, i). When $j \notin \mathcal{N}_i$, which means there is no information flow from vertex j to vertex i, $a_{i,j} = 0$, otherwise $a_{i,j} > 0$. Usually, we use the triplet $\{\mathcal{V}, \mathcal{E}, A\}$ to describe a graph $\mathcal{G}$, where $A \in \mathbb{R}^{n \times n}$ is the weighted adjacency matrix associated with $\mathcal{G}$ and $\forall i, j \in \mathcal{V}$, $A^{i,j} = a_{i,j}$. Given a graph $\mathcal{G}$, it contains a spanning tree if there exists at least one vertex i, such that for any other vertex j there is a path from i to j.

2.2. Adversary model

We now set out to define the adversary model and scope of adversary we consider in the paper. The adversary models can be classified as *crash failure* (Raynal 2010), *non-colluding* (Pasqualetti, Bicchi, and Bullo 2009; Pasqualetti, Bicchi, and Bullo 2012), and *malicious* (or *Byzantine*) (Sundaram and Hadjicostis 2011; Ichimura and Shigeno 2010; Zhang and Sundaram 2012) agents, depending on their abilities. Crash failure agents behave correctly before crashing, but once they have crashed they will stop executing prematurely and do nothing. Non-colluding agents are unaware of the structure and state of the network and ignore the presence of other adversarial agents. Instead, both malicious and Byzantine agents have a complete knowledge of the networked system and possess unlimited sensing, communication, and computation capabilities. Compared to the Byzantine agents, the malicious agents simply lack the deceitful capacity to convey different information to different neighbors in the network. However, this type of deceit is usually not possible for the agents broadcasting their information to neighbors. Therefore, we consider malicious as adversary model under the local broadcast assumption. Here, we assume that the total number of malicious agents is upper bounded by a number $f \in \mathbb{Z}^+$ in each loyal agent's neighborhood. This is called the f-local malicious model (Pelc and Peleg 2005; LeBlanc et al. 2013). We provide the following formal definition.

Definition 1 (f-local malicious model) A set $\mathcal{S} \subset \mathcal{V}$ of malicious agents is f-local malicious model if it contains at most f agents in the neighborhood of the other agents for all time instant k, i.e., $|\mathcal{N}_i \cap \mathcal{S}| \leq f, \forall i \in \mathcal{V} \backslash \mathcal{S}, f \in \mathbb{Z}^+$.

2.3. Delay-robust resilient consensus

We shall formulate the consensus problem in a network of multi-agent system. Suppose that the network system under consideration consists of n dynamic agents, labeled from 1 to n. Each agent is regarded as a node in a directed graph, denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Without loss of generality, the agent set is partitioned into the set of p loyal agents $\mathcal{V}_l = \{1, 2, ..., p\}$ and the set of $n - p$ adversarial agents $\mathcal{V}_a = \{p + 1, p + 2, ..., n\}$.

For all agent $i \in \mathcal{V}_l$ and $j \in \mathcal{N}_i$, the information flow from agent j to agent i through edge (j, i) is assumed to suffer from a time delay $d_{i,j}$, which is an unknown positive integer and may

be time-varying. The agent is assumed to be able to access its own instantaneous state value, i.e. $d_{i,i} = 0$.

We assume that each loyal agent has the following dynamics

$$\begin{cases} x_i(k+1) = x_i(k) + u_i(k), & i \in \mathcal{V}_l \\ x_i(s) = \phi_i(s), & s = -\bar{d}, -\bar{d}+1, \ldots, 0, \end{cases} \tag{1}$$

where $x_i(k) \in \mathbb{R}$ is the state value of agent i, $\phi_i(s)$ is a initial function, $\bar{d}$ is the upper delay bound to be determined, and $u_i(k) \in \mathbb{R}$ is the control protocol. We will design the control protocol by using the local information such as neighbors state values received through wireless channels such that two important conditions, safety and consensus, are satisfied. In most of the cases, transmission delay is not negligible in the control protocol design. We shall show that the proposed control protocol is robust to time delay.

Denote

$$M(k) = \max_{i \in \mathcal{V}_l, \theta=0,\ldots,\bar{d}} x_i(k-\theta), \quad m(k) = \min_{i \in \mathcal{V}_l, \theta=0,\ldots,\bar{d}} x_i(k-\theta). \tag{2}$$

where $\bar{d} = \sup_{k \geq 0} \max\{d_{j,i}(k), i \in \mathcal{N}_j, j \in \mathcal{V}\}$. Since time delays are uniformly bounded, we know that $\bar{d} < +\infty$. It is clear that $M(0)$ and $m(0)$ are the maximum and minimum values of the initial states among the loyal agents, respectively. Then, we define the problem to be studied specifically as follows.

Definition 2 (Delay-robust f-local resilient consensus)   The discrete-time multi-agent system (1) with bounded time-varying delays $\{d_{i,j}, i \in \mathcal{V}_l, j \in \mathcal{N}_i\}$ are said to achieve resilient consensus in the presence of f-local malicious agents if and only if

$$m(0) \leq \inf_{k \geq 0} \min_{i \in \mathcal{V}_l} x_i(k) \leq \sup_{k \geq 0} \max_{i \in \mathcal{V}_l} x_i(k) \leq M(0), \tag{3}$$

$$\lim_{k \to \infty} \left(x_i(k) - x_j(k) \right) = 0, \quad \forall i, j \in \mathcal{V}_l. \tag{4}$$

In Definition 2, (3) guarantees that all the loyal agents are within the safe region all the time. This condition is equivalent to that of $\forall k \geq 0$, $m(k) \geq m(0)$, and $M(k) \leq M(0)$. On the other hand, consensus is guaranteed by (4).

3. Main results

In this section, we shall introduce a delay-robust f-local resilient consensus protocol first and after which the convergence analysis is provided.

3.1. *Delay-robust f-local resilient consensus protocol*

In the proposed protocol, each agent i sorts its received (delayed) state values in a descending order. If there are less than f values strictly larger than its own value $x_i(k)$, then agent i removes all of these values by effectively setting their weights to zero. Otherwise, it removes precisely the largest f values in the sorted list. The same manipulation is applied to the smallest values in agent i's neighborhood. The similar protocols without considering transmission delay can be found in Zhang and Sundaram (2012), LeBlanc et al. (2012), Cárdenas, Amin, and Sastry (2008). Let $\mathcal{R}_i(k)$ denotes the set of agents whose values are removed by agent i at time instant k. The proposed consensus protocol is provided as follows:

$$u_i(k) = \sum_{j \in \mathcal{N}_i \setminus \mathcal{R}_i(k)} a_{i,j}(k)(x_j(k - d_{i,j}) - x_i(k)). \tag{5}$$

We assume that $\sum_{j \in \mathcal{N}_i} a_{i,j}(k) < 1$, which is very standard for discrete-time system. According to the definition of $\mathcal{R}_i(k)$, we say that protocol (5) is with parameter f. Due to the existence of the adversary agents, $\mathcal{R}_i(k)$ is possibly time-varying even if the underlying network is fixed, which implies the control topology is dynamically switching. In the following, we shall provide the stability analysis of multi-agent system (1) under protocol (5).

3.2. *Stability analysis*

In this section, we will prove that when the network topology satisfies some connectivity conditions, the safe condition (3) and consensus goal (4) can be achieved. In order to interpret the delayed value of the agents in the protocol (5), we introduce some virtual nodes $v_{i,j}$ which corresponds to node i with j steps time delay. It is clear that $v_{i,0} = i$. Denote $\mathcal{V}_{(i)} = \{v_{i,0}, \cdots, v_{i,\bar{d}}\}$. To begin with, we need to introduce the following topological properties (Cao, Morse, and Anderson 2008; LeBlanc et al. 2013).

Definition 3 (Delay graph)   Given a digraph $\mathcal{G}$ with node set $\mathcal{V}$ and edge set $\mathcal{E}$, the graph $\bar{\mathcal{G}}(k)$ is called delay graph corresponding to $\mathcal{G}$ if

(1) the node set is $\bigcup_{i \in \mathcal{V}} \mathcal{V}_{(i)}$;
(2) the edge set is $\{(v_{i,j-1}, v_{i,j}), j = 1, \ldots, \bar{d}\} \bigcup \{(v_{i,d_{j,i}}, v_{j,0}) : \forall (i,j) \in \mathcal{E}\}$.

From Definition 3, we can see that there is one and only one path from the node to the virtual nodes representing its delayed values. Due to the time-varying delays, the delay graph is essentially dynamically switching.

Definition 4 (r-reachable set)   Given a digraph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ and a nonempty subset $S \subset \mathcal{V}$, we say $\mathcal{S}$ is an r-reachable set if $\exists i \in \mathcal{S}$ such that $|\mathcal{N}_i \backslash \mathcal{S}| \geq r, r \in \mathbb{Z}^+$.

Observe that an r-reachable set $\mathcal{S}$ contains an agent that has at least r neighbors outside of $\mathcal{S}$ at time instant k, which can be intuitively understood as that there exists at least one agent in the set that can be influenced by a large number of agents from outside of the set. The following definition of r-robust graph can generalize this notion of redundancy to the entire network.

Definition 5 (r-robust graph)   A digraph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ is r-robust, with $r \in \mathbb{Z}^+$, if for every pair of nonempty, disjoint subsets of $\mathcal{V}$, at least one of the subsets is r-reachable.

Given an r-robust graph $\mathcal{G}$, let $\mathcal{G}'$ be the graph produced by removing up to t incoming edges of each agent in $\mathcal{G}$ ($t < r$). According to Definition 5, we can observe that $\mathcal{G}'$ is $(r - t)$-robust. Then, we have the following lemmas.

LEMMA 1   *Graph contains a spanning tree if and only if $\mathcal{G}$ is 1-robust.*

Proof   **Necessity**: By contradiction, we assume that $\mathcal{G}$ contains a spanning tree and it is not 1-robust. According to Definition of 5, there exist two disjoint subsets, $\mathcal{S}_1$ and $\mathcal{S}_2$, who do not have neighbors outside their own set. Then, there is no information flow between $\mathcal{S}_1$ and $\mathcal{S}_2$, which contradicts the definition of spanning tree.

Sufficiency: By contradiction, we assume that $\mathcal{G}$ does not contain a spanning tree. Denote A as the adjacency matrix of $\mathcal{G}$. According to Seneta (2006), Wolfowitz (1963), it has that A is decomposable, which means we can partition the node set into two subsets and no information exchange happens between them. This contradicts the definition of 1-robust.   □

The same result without necessity part can be found in Zhang and Sundaram (2012), LeBlanc et al. (2012). It is noted that if a graph is r-robust it implies that it is 1-robust, and therefore contains a spanning tree.
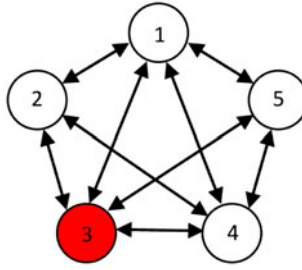
Figure 1. Directed graph with 5 agents.

LEMMA 2 (Cao, Morse, and Anderson 2008)   *For system (1) with protocol (5), if the communication graphs jointly contains a spanning tree, there is a constant x*, depending only on initial values, for which*

$$\lim_{k \to \infty} x_i(k) = x^*,$$

where the limit is approached exponentially fast.

Now we are in the position to provide the main result.

THEOREM 1   *Consider a discrete-time directed delayed network modeled by (6). Suppose each loyal agent updates its state according to consensus protocol (5) with parameter f. The delay-robust f-local resilient consensus can be achieved if the network $\mathcal{G}$ is $(2f + 1)$-robust.*

Proof   The proof is divided into two steps. The first step is to prove the safety condition (3) and the second step is to prove the consensus condition (4).

Step 1 (Safety)   The closed-loop system can be written in the following form

$$
\begin{cases}
x_i(k+1) = x_i(k) + \sum_{j \in \mathcal{N}_i \setminus \mathcal{R}_i(k)} a_{i,j}(k)(x_j(k - d_{i,j}) - x_i(k)), \\
x_i(s) = \phi_i(s), s = -\bar{d}, -\bar{d} + 1, \ldots, 0.
\end{cases}
\tag{6}
$$

According to the definition of $M(k)$ and $m(k)$ in (2), it follows from (6) that $\forall i \in \mathcal{V}_l$

$$
\begin{aligned}
x_i(k+1) &\leq x_i(k) + \sum_{j \in \mathcal{N}_i \setminus \mathcal{R}_i(k)} a_{i,j}(k)(M(k) - x_i(k)) \\
&= \alpha M(k) + (1 - \alpha) x_i(k) \\
&\leq M(k),
\end{aligned}
\tag{7}
$$

which implies that $M(k+1) \leq M(k)$. Here $\alpha = \sum_{j \in \mathcal{N}_i \setminus \mathcal{R}_i(k)} a_{i,j}(k) < 1$. Similarly, we can get $m(k+1) \geq m(k)$, which guarantees the safety condition (3).

Step 2 (Consensus)   From consensus protocol (5), we can observe that each agent can remove up to $2f$ values from the data it received at each time step. When the values of some adversary agents is not in the top and bottom f values for some nodes, the removed state value from these nodes may be less than $2f$. In this case, the state values of the unremoved adversary agents can be expressed in terms of the linear combination of all the (delayed) state values of all the loyal nodes, i.e.

$$
x_i(k) = \sum_{j \in \mathcal{V}_l} \beta_{q,j}(k) x_j(k), \quad i \in \mathcal{V}_a \cap \left(\mathcal{N}_q \setminus \mathcal{R}_q(k) \right),
$$

where $\beta_{q,j} \geq 0$ and $\sum_{j \in \mathcal{V}_l} \beta_{q,j}(k) = 1$. It is noted that the state value of adversary agent i may be included in the protocol of a different loyal agent q and there may exist different (in fact infinite many) expressions of $x_i(k)$. We just arbitrarily choose one. To slightly abuse the notation, for each loyal agent q, which does not include adversary state information in the protocol at time instant k, we set $\beta_{q,j}(k) = 0$, $j \in \mathcal{V}_l$.

We consider the following augmented system

$$\bar{X}(k+1) = \Theta(k)\bar{X}(k)$$

where

$$\bar{X}(k) = \begin{bmatrix} X(k) \\ X(k-1) \\ \vdots \\ X(k-\bar{d}) \end{bmatrix}, \quad X(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ \vdots \\ x_p(k) \end{bmatrix}, \quad \Theta(k) = \Theta_1(k) + \Theta_2(k),$$

$$\Theta_1(k) = \begin{bmatrix} A_0 & A_1 & \cdots & A_{\bar{d}} \\ I & & & \\ & \ddots & & \\ & & I & \end{bmatrix}, \quad \Theta_2(k) = \begin{bmatrix} B & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \quad B^{i,j}(k) = \beta_{i,j}(k),$$

$$A_0^{j,q}(k) = \begin{cases} 1 - \sum\limits_{q \in \mathcal{N}_j \backslash \mathcal{R}_j(k)} a_{j,q}(k), & j = q \\ a_{j,q}(k)\delta_{0,d_{j,q}}, & j \neq q \end{cases}, \quad A_i^{j,q}(k) = a_{j,q}(k)\delta_{i,d_{j,q}}, \quad i = 1, \ldots, p.$$

It can be checked that Θ, Θ_1, and Θ_2 are valid adjacency matrix corresponding to some delay graphs as defined in Definition 3. Note that $\sum_{i=1,\ldots,\bar{d}} A_i(k)$ is the adjacency matrix corresponding to $\mathcal{G}_r$, which is $\mathcal{G}$ by removing some links according to protocol (5). By Lemma 1 we know that $\mathcal{G}_r$ is 1-robust and consequently contains a spanning tree. On the other hand, according to Xiao and Wang (2006), we know that the delay graph corresponding to Θ_1, denoted by $\mathcal{G}_1$, contains a spanning tree if graph $\mathcal{G}_r$ contains a spanning tree. Meanwhile, the delay graph corresponding to Θ, denoted by $\mathcal{G}_0$ contains more edges than $\mathcal{G}_1$ which implies that $\mathcal{G}_0$ contains a spanning tree. Then, according to Lemma 2, the consensus can be achieved under protocol (5), which completes the proof. $\qquad\square$

4. Simulations

In this section, we illustrate the result derived in the above sections by numerical simulations using the MATLAB tool. We consider a digraph with $n = 5$ agents as shown in Figure 1. The initial values of the 5 agents are $x_1(0) = 1$, $x_2(0) = 2$, $x_3(0) = 3$, $x_4(0) = 4$, and $x_5(0) = 5$. Here, we assume that agent 3 is a malicious agent and designed as

$$x_3(k+1) = 0.9x_3(k) + 0.1u,$$

where the reference inputs u for the malicious agent is $u = 10$. The goal of agent 3 is to drive the loyal agent values outside of the range of their initial values. To illustrate Theorem 1, let the communication graph be 3-robust in Figure 1. By the above analysis, it can be seen that system (6) can sustain one malicious agent in the network under the 1-local malicious model. Here, we assume upper delay bound $\bar{d} = 5$, the edge weight $a_{i,j} = \frac{0.8}{|\mathcal{N}_i \backslash \mathcal{R}_i|}$, and initial condition $\phi_i(s) = i$, $s = -\bar{d}, -\bar{d}+1, \ldots, 0$.

The results for this example are shown in Figure 2. It can be seen that the malicious agent 3 attempts to drive the values of the loyal agents to a value of 10, but fails whenever the obtained
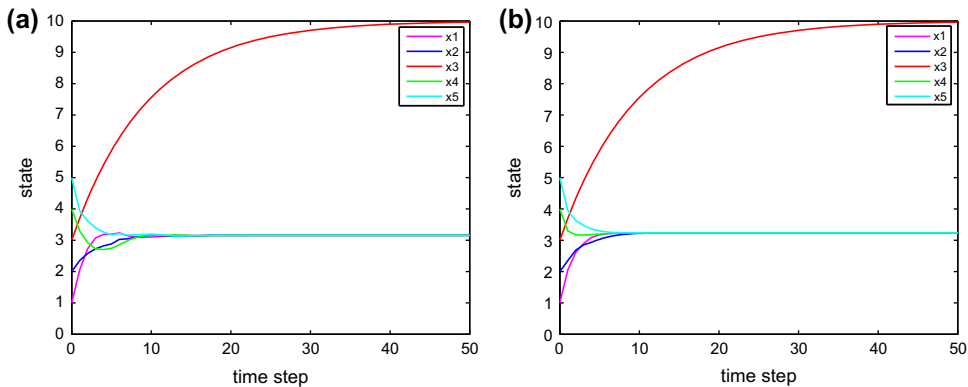
Figure 2. State trajectories of all agents with and without a transmission delay.

control protocol (5) is used in Figure 2(a). Furthermore, the result for the delay-free communication network of Figure 1 is shown in Figure 2(b).

5. Conclusions

In this paper, we have considered the resilient consensus problem of discrete-time multi-agent systems with transmission delays. An improved form of local filtering strategy for the loyal agents to resist adversaries in a directed delayed network has been provided. Under the condition that the time delays are uniformly bounded, a sufficient condition for the resilient consensus under the proposed protocol has been obtained, which is $(2f + 1)$-robust.

Funding

Notes on contributors
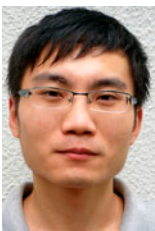
Yiming Wu received the BE degree in automation from Zhejiang University of Technology, China, in 2010. He is currently working toward the PhD degree in control science and engineering at Zhejiang University of Technology, China. Since April 2012, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, as a Research Assistant. His research interests include secure control systems, resilient consensus and multi-agent networks.

Xiongxiong He received his MS degree from the Institute of Automation, Qufu Normal University, China, in 1994, and his PhD 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 and the Director of the Institute of Intelligence System and Robotics. Dr He's research interests include robotics, intelligence systems and signal processing.

Shuai Liu received his BE and ME degrees in Control Theory and Engineering from Shandong University in 2004 and 2007, respectively, and his PhD degree in Electrical and Electronic Engineering from Nanyang Technological University, Singapore, in 2012. Since 2011, he has been a research fellow with Berkeley education alliance for research in Singapore (BEARS). His research interests include cooperative control, distributed consensus, optimal estimation and control, time-delay systems, fault detection and estimation.

Lihua Xie received the BE and ME degrees in electrical engineering from Nanjing University of Science and Technology in 1983 and 1986, respectively, and the PhD degree in electrical engineering from the University of Newcastle, Australia, in 1992. Since 1992, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, where he is currently a professor and the Head of Control and Instrumentation Division. He held teaching appointments in the Department of Automatic Control, Nanjing University of Science and Technology from 1986 to 1989 and Changjiang Visiting Professorship with South China University of Technology from 2006 to 2011. Dr Xie's research interests include robust control and estimation, networked control systems, multi-agent networks, and disk drive servo. In these areas, he has published many journal papers and co-authored two patents and four books. He has served as an editor of IET Book Series in Control and an Associate Editor of a number of journals including IEEE Transactions on Automatic Control, Automatica, IEEE Transactions on Control Systems Technology, and IEEE Transactions on Circuits and Systems-II. Dr Xie is Fellow of IEEE and Fellow of IFAC.

References

Bliman, P.-A., and G. Ferrari-Trecate. 2008. "Average Consensus Problems in Networks of Agents with Delayed Communications." *Automatica* 44 (8): 1985–1995.

Cao, M., A. S. Morse, and B. D. O. Anderson. 2008. "Reaching a Consensus in a Dynamically Changing Environment: Convergence Rates, Measurement Delays, and Asynchronous Events." *SIAM Journal on Control and Optimization* 47 (2): 601–623.

Cárdenas, A. A., S.Amin, and S. Sastry. 2008. "Research Challenges for the Security of Control Systems." In *Proceedings of the 3rd Conference on Hot Topics in Security*, 1–6. San Jose, CA, July 28-August 1.

Cortés, J., and F. Bullo. 2005. "Coordination and Geometric Optimization Via Distributed Dynamical Systems." *SIAM Journal on Control and Optimization* 44 (5): 1543–1574.

Fax, J. A., and R. M. Murray. 2004. "Information Flow and Cooperative Control of Vehicle Formations." *IEEE Transactions on Automatic Control* 49 (9): 1465–1476.

Ichimura, A., and M. Shigeno. 2010. "A New Parameter for a Broadcast Algorithm with Locally Bounded Byzantine Faults." *Information processing letters* 110 (12): 514–517.

Jadbabaie, A., J. Lin, and A. S. Morse. 2003. "Coordination of Groups of Mobile Autonomous Agents Using Nearest Neighbor Rules." *IEEE Transactions on Automatic Control* 48 (6): 988–1001.

LeBlanc, H. J., and X. D. Koutsoukos. 2011. "Consensus in Networked Multi-agent Systems with Adversaries." In *Proceedings of the 14th International Conference on Hybrid Systems: Computation and Control*, 281–290. Chicago, IL, April 12–14.

LeBlanc, H. J., H. Zhang, X. Koutsoukos, and S. Sundaram. 2013. "Resilient Asymptotic Consensus in Robust Networks." *IEEE Journal on Selected Areas in Communications* 31 (4): 766–781.

LeBlanc, H. J., H. Zhang, S. Sundaram, and X. Koutsoukos. 2012. "Consensus of Multi-agent Networks in the Presence of Adversaries Using Only Local Information." In *Proceedings of the 1st International Conference on High Confidence Networked Systems*, 1–10. Beijing, April 17–18.

Lee, D., and M. W.Spong. 2006. "Agreement with Non-uniform Information Delays." In *Proceedings of the 2006 American Control Conference*, 756–761. Minneapolis, MN, June 14–16.

Liu, S., T. Li, and L. Xie. 2011. "Distributed Consensus for Multiagent Systems with Communication Delays and Limited Data Rate." *SIAM Journal on Control and Optimization* 49 (6): 2239–2262.

Liu, S., L. Xie, and H. Zhang. 2011. "Distributed Consensus for Multi-agent Systems with Delays and Noises in Transmission Channels." *Automatica* 47 (5): 920–934.

Liu, S., T. Li, L. Xie, M. Fu, and J. Zhang. 2013. "Continuous-time and Sampled-data Based Average Consensus with Logarithmic Quantizers." *Automatica* 49 (11): 3329–3336.

Liu, S., L.Xie, and H. Zhang. Forthcoming. "Containment Control of Multi-agent Systems by Exploiting the Control Inputs of Neighbors." *International Journal of Robust and Nonlinear Control*. doi:10.1002/rnc.3026.

Olfati-Saber, R., and R. M. Murray. 2004. "Consensus Problems in Networks of Agents with Switching Topology and Time-delays." *IEEE Transactions on Automatic Control* 49 (9): 1520–1533.

Paganini, F., J. Doyle, and S. Low. 2001. "Scalable Laws for Stable Network Congestion Control." In *Proceedings of the 40th IEEE Conference on Decision and Control*, 185–190. Orlando, FL, December 4–7.

Pasqualetti, F., A. Bicchi, and F. Bullo. 2009. "On the Security of Linear Consensus Networks." In *Proceedings of the 48th IEEE Conference on Decision and Control, 2009 Held Jointly with the 2009 28th Chinese Control Conference*, 4894–4901. Shanghai, December 16–18.

Pasqualetti, F., A. Bicchi, and F. Bullo. 2012. "Consensus Computation in Unreliable Networks: A System Theoretic Approach." *IEEE Transactions on Automatic Control* 57 (1): 90–104.

Pelc, A., and D. Peleg. 2005. "Broadcasting with Locally Bounded Byzantine Faults." *Information Processing Letters* 93 (3): 109–115.

Raynal, M. 2010. "Fault-tolerant Agreement in Synchronous Message-passing Systems." *Synthesis Lectures on Distributed Computing Theory* 1 (1): 1–189.

Ren, W., and R. W. Beard. 2005. "Consensus Seeking in Multiagent Systems Under Dynamically Changing Interaction Topologies." *IEEE Transactions on Automatic Control* 50 (5): 655–661.

Seneta, E.. 2006. *Non-negative Matrices and Markov Chains*. New York: Springer.

Sundaram, S., and C. N. Hadjicostis. 2011. "Distributed Function Calculation Via Linear Iterative Strategies in the Presence of Malicious Agents." *IEEE Transactions on Automatic Control* 56 (7): 1495–1508.

Vaidya, N. H., L. Tseng, and G. Liang. 2012. "Iterative Approximate Byzantine Consensus in Arbitrary Directed Graphs." In *Proceedings of the 2012 ACM Symposium on Principles of, Distributed Computing*, 365–374.

Vidal, R., O. Shakernia, and S. Sastry. 2003. "Formation Control of Nonholonomic Mobile Robots with Omnidirectional Visual Servoing and Motion Segmentation." In *Proceedings ICRA '03. IEEE International Conference on Robotics and Automation*, 584–589. Taipei, September 14–19.

Wang, W., and J. J. Slotine. 2006. "Contraction Analysis of Time-delayed Communications and Group Cooperation." *IEEE Transactions on Automatic Control* 51 (4): 712–717.

Wolfowitz, J. 1963. "Products of Indecomposable, Aperiodic, Stochastic Matrices." In *Proceedings of the American Mathematical Society* 14 (5): 733–737.

Xiao, F., and L. Wang. 2006. "State Consensus for Multi-agent Systems with Switching Topologies and Time-varying Delays." *International Journal of Control* 79 (10): 1277–1284.

Zhang, H. , and S. Sundaram. 2012. "Robustness of Information Diffusion Algorithms to Locally Bounded Adversaries." In *Proceedings of the 2012 American Control Conference*, 5855–5861. Montréal, QC, June 27–29.