2017 13th IEEE International Conference on Control & Automation (ICCA)
July 3-6, 2017. Ohrid, Macedonia

Attack Tolerant Finite-Time Consensus for Multi-Agent Networks*

Yiming Wu[1], Ming Xu[1], Ning Zheng[1], and Xiongxiong He[2]

Abstract— **In this paper, we study the secure consensus problem for continuous-time networked multi-agent systems under malicious attacks. Contrary to previous works, we propose a new approach based on an iterative learning control (ILC) strategy to investigate attack tolerant finite-time consensus problems in directed networks. These results are motivated by the need to secure multi-agent networks against cyber attackers that can arbitrarily corrupt and modify the communication information. By ILC approach of designing the learning gain, the sufficient conditions to achieve finite-time consensus are obtained. Simulation results are also given to demonstrate the effectiveness of theoretical results.**

I. INTRODUCTION

Over the past decade, the distributed cooperative control of multi-agent systems has drawn much research attention due to its widespread applications in formation control, distributed sensor network, flocking, distributed computation and synchronization of coupled chaotic oscillators. Among various cooperative control tasks, consensus, which requires all agents agreeing on some quantity of interest by only communicating with their neighbors, builds the foundation of others [1]–[4].

An important challenge in multi-agent networks, as in all large-scale distributed systems, is that they are vulnerable to cyber-threats through the use of open communication network environments. The analysis of security of consensus networks to attacks has received increasing attention in recent years. For achieving resilient multi-agent network behavior, [5] firstly proposes a novel intrusion detection scheme for linear consensus networks with single misbehaving node. Specifically, in [6], a new light-weight approximate Byzantine consensus in asynchronous networks is proposed. Furthermore, the algorithm is also valid when a network encounters delay over its communication paths. In [7], a secure consensus tracking problem has been studied for a class of stochastic linear multi-agent networks under two types of attacks. The authors study the attacks on the edges instead of nodes, which lead to some connected and paralyzed directed switching topologies. Departing from the existing relevant literature [5]–[8] that make specific assumptions on the graph topology, the authors in [9] develop a new distributed adaptive control architecture that utilizes a local state emulator for multi-agent networks in the presence of misbehaving agents. Moreover, secure consensus control for multi-agent networks with quantized interactions is studied in [10] and [11].

Iterative learning control (ILC) is known to be effective in handling a particular class of control processes, where the operation time in each iteration is finite and fixed, and the control task is repeated over many iterations. Since 2009, ILC has been extended to the networked control field [12]. The use of ILC for consensus problems of multi-agent networks is a relatively new field and has been reported in a few previous works in the literature [13]–[15]. In [16] and [17], the finite-time output consensus problem of multi-agent networks is considered with ILC schemes.

To the best of our knowledge, there are few applications of ILC scheme to the security of consensus networks. In this paper, to address all the important and challenging issues mentioned above, we extend our recent work in [14], [18], [19] to the directed multi-agent networks with a specific edge-bound content modification cyber attack. We show that when the information-exchange network is satisfied with the given sufficient conditions, an attack tolerant consensus control strategy combined with ILC scheme can be designed for each agent to enable him resist malicious attacks and achieve the desired agreement state over a finite-time interval $[0, T]$.

The rest of this paper is organized as follows. In Section II, the attack tolerant finite time consensus problem is formulated and the relevant notations and preliminaries are presented. Section III presents the convergence analysis while a simulation example is presented in Section IV to demonstrate the effectiveness of the results. Finally, Section V concludes the paper.

II. PROBLEM FORMULATION AND PRELIMINARIES

Consider a group of N identical agents, dynamics of the ith ($i = 1, 2, ..., N$) agent at the kth iterative is described by

$$\dot{x}_{k,i}(t) = u_{k,i},\ i = 1, 2, ..., N \tag{1}$$

where $k = 1, 2, \ldots$ is the iteration index, $t \in [0, T], T > 0$ represents the operation time in each iteration, $x_{k,i}(t) \in \mathbb{R}$ is the state of agent i, and $u_{k,i} \in \mathbb{R}$ is the control input to be designed.

The control objective is to design a distributed control algorithm so that the network can tolerant a specific number of malicious attacks and reach consensus in a finite-time.

*This work was supported in part by the cyberspace security Major Program in National Key Research and Development Plan of China under Grant 2016YFB0800201, the National Natural Science Foundation of China (NSFC) under Grant 61473262, and the State Key Program of Zhejiang Province Natural Science Foundation of China under Grant LZ15F020003.

[1]Yiming Wu, Ming Xu and Ning Zheng are with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China {ymwu, mxu, nzheng}@hdu.edu.cn

[2]Xiongxiong He is with the College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China hxx@zjut.edu.cn

The information exchange among the N agents will be represented by a weighted directed graph. The corresponding concepts and notations are recalled as below.

A weighted directed graph (or digraph) of order N is defined as $\mathcal{G} = \{\mathcal{V}_\mathcal{G}, \mathcal{E}_\mathcal{G}, A_\mathcal{G}\}$, where $\mathcal{V}_\mathcal{G} = \{1, 2, \ldots, N\}$ is a non-empty set of vertices (or nodes), $\mathcal{E}_\mathcal{G} \subset \mathcal{V} \times \mathcal{V}$ is a set of edges, and $A_\mathcal{G} = [a_{ij}] \in \mathbb{R}^{N\times N}$ is called the weighted adjacency matrix associated with $\mathcal{G}$. For an edge $(i, j) \in \mathcal{E}_\mathcal{G}$, i is called the parent node whose messages can flow to node j. It is defined by $a_{ii} = 0$, $a_{ij} > 0$ if $(j, i) \in \mathcal{E}_\mathcal{G}$ and $a_{ij} = 0$ otherwise. The neighbor set of node i is defined by $\mathcal{N}_i = \{j \in \mathcal{V}_\mathcal{G} | (j, i) \in \mathcal{E}_\mathcal{G}\}$. A directed path from node i_1 to node i_p is given by a sequence of ordered edges of the form $(i_1, i_2), (i_2, i_3), ..., (i_{p-1}, i_p)$ with $(i_{j-1}, i_j) \in \mathcal{E}_\mathcal{G}$, $\forall j \in \{2, 3, ..., p\}$. The graph $\mathcal{G}$ is said to have a spanning tree if there is a root node without any parent such that there exists a direct path from this node to the rest of nodes. The matrix $L \triangleq D - A$ is called the Laplacian matrix of $\mathcal{G}$, where $D = [d_{ii}] \in \mathbb{R}^{N\times N}$ is a diagonal matrix with $d_{ii} \triangleq \sum_{j\in\mathcal{V}_\mathcal{G}} a_{ij}$.

The use of matrix analysis is inspired by the prior work on consensus under dynamically changing interaction topologies [20]–[22]. A matrix M is said to be *nonnegative* if all its entries are nonnegative. A nonnegative matrix is said to be row stochastic if all its row sums are 1. A row-stochastic matrix is called *indecomposable and aperiodic* (SIA) if there exists a column vector such that $\lim_{k\to\infty} M^k = 1c^{\mathrm{T}}$. $\prod_{i=1}^{k} M_i M_{k-1} \cdots M_1$ denotes the left product of the matrices $M_k, M_{k-1}, \ldots, M_1$. If the graph associated with A has a spanning tree, then the graph associated with $B = A + I_n$ also has a spanning tree.

Lemma 2.1: A stochastic matrix P is called *indecomposable and aperiodic* (SIA) if $\lim_{n\to\infty} P^n = 1y^{\mathrm{T}}$.

Lemma 2.2: If the union of a set of directed graphs $\{\mathcal{G}_1, \mathcal{G}_2, ..., \mathcal{G}_m\}$ has a spanning tree, then the matrix product $D_m D_{m-1} ... D_2 D_1$ is SIA, where D_i is a stochastic matrix with positive diagonal entries corresponding to each directed graph $\mathcal{G}_i$.

Lemma 2.3: [20], [23] Let $\mathcal{S} = \{\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_k\}$ be a finite set of SIA matrices with the property that every finite product $\mathcal{S}_{i_j} \mathcal{S}_{i_{j-1}} ... \mathcal{S}_{i_1}$ is SIA. Then, for each infinite sequence $\mathcal{S}_{i_1}, \mathcal{S}_{i_2}, ...$ there exists a column vector y such that

$$\lim_{j\to\infty} \mathcal{S}_{i_j} \mathcal{S}_{i_{j-1}} \ldots \mathcal{S}_{i_1} = 1y^{\mathrm{T}}.$$

Define the maximum and minimum states of all nodes in the network at the k-th iteration as

$$M_k(t) = \max_{i\in\mathcal{V}_\mathcal{G}} x_{k,i}(t), \quad m_k(t) = \min_{i\in\mathcal{V}_\mathcal{G}} x_{k,i}(t). \tag{2}$$

Let $M_0 = \max_{i\in\mathcal{V}_\mathcal{G}} x_{i0}$ and $m_0 = \min_{i\in\mathcal{V}_\mathcal{G}} x_{i0}$ be the maximum and minimum values of all the normal nodes under initial condition, respectively.

In this paper, we are interested in the false data injection attack [24], which means the attacker has the ability of modifies the information being exchanged in the edge set $\bar{\mathcal{E}}$ at will. Suppose that link (i, j) in the network modifies the value that agent i receives from agent j at time T to be $\tilde{x}_j(T)$. The goal of the attacker is to inject false information into the connection edges such that driving the state of network to an unsafe region. However, limitations in the resources available to the attacker enable him to only manipulate at most f_a incoming edges of each agent in graph $\mathcal{G}$.

The main purpose of an attack tolerant consensus networks is to design a control law so that agents' states are within a safe region (initial state region of all agents) all the time and converge to the same state in a finite time T, i.e.,

$$x_{k,i}(t) \in [m_0, M_0], t \in [0, T], \tag{3}$$

$$\lim_{k\to\infty} [x_{k,i}(T) - x_{k,j}(T)] = 0. \tag{4}$$

To improve the consensus objective (4), a desired consensus problem is further considered for the system (1) such that

$$\lim_{k\to\infty} x_{k,i}(T) = x_T, \tag{5}$$

where x_T is the desired agreement state in finite time T.

Then, we shall recall some notions of *robustness* for a directed network. The following definitions are adopted with minor changes, from [8].

Definition 2.1: (r-reachable set): Consider a directed graph $\mathcal{G}$ and a node set $\mathcal{V}$. For any non-empty and strict subset $\mathcal{S} \subset \mathcal{V}$, we say that $\mathcal{S}$ is an r-reachable set if there exists at least a node $i \in \mathcal{S}$ such that i has no less than r neighbors inside $\mathcal{V} \setminus \mathcal{S}$, where $r \in \mathbb{Z}^+$.

Definition 2.2: (r-robust graph): Consider a directed graph $\mathcal{G}$ and a node set $\mathcal{V}$. We say that $\mathcal{G}$ is an r-robust graph if for every pair of nonempty subsets of $\mathcal{V}$ there exists at least one subset that is an r-reachable set, where $r \in \mathbb{Z}^+$.

By employing the notion of robustness, some properties of the r-robust graph are recalled below [5], [8].

Lemma 2.4: Consider an r-robust graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$. Let $\hat{\mathcal{G}}$ be the graph generated by removing up to s ($s < r$) incoming edges of each node of $\mathcal{V}$, then, we say that $\hat{\mathcal{G}}$ is an $(r - s)$-robust graph.

Lemma 2.5: Consider a directed graph $\mathcal{G}$. If $\mathcal{G}$ is a 1-robust graph, then $\mathcal{G}$ contains a spanning tree.

Lemma 2.6: For the Laplacian matrix L associated with $\mathcal{G}$, 0 is one of its eigenvalues, and 1_n is the associated eigenvector. Furthermore, the eigenvalue $\lambda = 0$ has algebraic multiplicity equal to 1 if and only if $\mathcal{G}$ has a spanning tree.

Now we present the detailed description of the proposed control scheme. For the kth iteration, agent $i \in \mathcal{V}_\mathcal{G}$ obtains its neighbors' state values, and forms a sorted list $\mathcal{L}_i$ from the largest to the smallest at time T. Then agent i removes precisely the largest f_a values the smallest f_a values in the sorted list.

Then we design the following iterative learning consensus protocol for each agent i:

$$\begin{aligned} u_{i,k+1} = u_{i,k} + \gamma_i \Big\{ & \sum_{j\in\mathcal{N}_i} a_{ij} \phi_{ij,k} [x_{k,j}(T) - x_{k,i}(T) \\ & + \omega_i [x_T - x_{k,i}(T)] \Big\}, \end{aligned} \tag{6}$$

where $a_{ij} \in \mathbb{R}$ is the weight of edge (j, i), $\gamma_i > 0$ is a learning gain to be designed, and $\phi_{ij,k}$ are filter functions

which equal one if the value of agent j is kept by agent i at the k-th iteration and zero otherwise. ω_i indicates the accessibility of x_T by agent i, if x_T is accessible by agent i, then $\omega_i > 0$, otherwise $\omega_i = 0$.

From (1), it can equivalently obtain that $x_{k,i}(t) = x_{k,i}(0) + tu_{k,i}$. Since the initial reset condition holds, i.e., $x_{k,i}(0) = x_{i0}, \forall k \in \mathbb{Z}^+$, the state of normal agent i at the terminal time T satisfies

$$\begin{aligned} x_{k+1,i}(T) &= x_{k,i}(T) + [x_{k+1,i}(T) - x_{k,i}(T)] \\ &= x_{k,i}(T) + [x_{k+1,i}(0) - x_{k,i}(0)] \\ &\quad + T(u_{k+1,i} - u_{k,i}) \\ &= x_{k,i}(T) + T(u_{k+1,i} - u_{k,i}). \end{aligned} \tag{7}$$

In view of (6), an immediate consequence of (7) is that

$$\begin{aligned} x_{k+1,i}(T) = x_{k,i}(T) + T\gamma_i \sum_{j=1}^{n} \phi_{i,j}(T) \\ \times a_{i,j}[x_{k,j}(T) - x_{k,i}(T)] \end{aligned} \tag{8}$$

which can be rewritten in a compact form of

$$x_{k+1}(T) = (I - T\Gamma L_k)x_k(T), \tag{9}$$

where $\Gamma = \mathrm{diag}\{\gamma_1, \gamma_2, ..., \gamma_n\}$.

III. Main Results

In this section, we shall present the main results. While some useful lemmas as follows are listed before giving the main results.

Lemma 3.1: [25] If the union of a set of directed graphs $\{\mathcal{G}_{i_1}, \mathcal{G}_{i_2}, ..., \mathcal{G}_{i_m}\} \subset \bar{\mathcal{G}}$ has a spanning tree, then the matrix product $D_{i_m}...D_{i_2}D_{i_1}$ is SIA, where D_{i_j} is a stochastic matrix corresponding to each directed graph $\mathcal{G}$.

Lemma 3.2: [23] Let $L_1, L_2, ..., L_k$ be a finite set of SIA matrices with the property that for each sequence $L_{i_j}, L_{i_{j-1}}, ..., L_{i_1}$ is SIA. Then, for each in-finit sequence L_{i_1}, L_{i_2},... there exists a column vector y such that

$$\lim_{j\to\infty} L_{i_j} L_{i_{j-1}} \cdots L_{i_1} = 1y^{\mathrm{T}}$$

In this paper, we make the following assumptions on the agent dynamics and the information-exchange graph.

Assumption 3.1: Root agent in a spanning tree can access the information x_T at each iteration.

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

Theorem 3.1: For multi-agent systems (1) with protocol (6), let the positive learning gain satisfy

$$T\gamma_i \left(\sum_{j\in\mathcal{N}_i} a_{ij} + \omega_i \right) < 1, \tag{10}$$

If $\mathcal{G}$ is a $(2f_a + 1)$-robust graph, then the secure finite-time consensus can be achieved as $k \to \infty$.

Proof: The proof consists of the following two steps: 1) We will first prove the safety condition (3), and 2) then prove the consensus condition (4).

Proof of 1): According to the definition of $M_k(t)$ and $m_k(t)$ in (2), it following from (8) that $\forall i \in \mathcal{V}_\mathcal{G}$:

$$\begin{aligned} x_{k+1,i}(t) &= x_{k,i}(t) + t\gamma_i \sum_{j=1}^{n} \phi_{ij,k}(t) a_{ij}[x_{k,j}(t) - x_{k,i}(t)] \\ &\le x_{k,i}(t) + t\gamma_i \sum_{j=1}^{n} \phi_{ij,k}(t) a_{ij}[M_k(t) - x_{k,i}(t)] \\ &= \alpha M_k(t) + (1-\alpha)x_{k,i}(t) \\ &\le M_k(t), \end{aligned} \tag{11}$$

which implies that $M_{k+1}(t) \le M_k(t)$. Here $\alpha = t\gamma_i \sum_{j=1}^{n} \phi_{ij,k}(t) a_{ij} < 1$. Similarly, we can get $m_{k+1}(t) \ge m_k(t)$, which guarantees the safety condition (3).

Proof of 2): Since the initial network is $(2f_a + 1)$-robust, after removing up to $2f$ incoming edges for each normal node, the network is still 1-robust from Lemma 2.4. Then by Lemma 2.5, it is easy to know that the graph $\mathcal{G}$ must contain a spanning tree. The notation A_k and L_k denotes the adjacency matrix and Laplacian matrix at kth iteration, respectively. Due to $L_k = \Delta - A_k$, we have $I - T\Gamma L_k = (I - T\Gamma\Delta) + T\Gamma A_k$. Clearly, $I - T\Gamma\Delta$ is a diagonal matrix, and its diagonal elements are $1 - T\gamma_i d_i = 1 - T\gamma_i \sum_{j=1}^{n} \phi_{ij,k}(T) a_{ij}$ which can be guaranteed to be positive under the condition (10). Hence, $I - T\Gamma\Delta \ge 0$ is a non-negative matrix. According to [26], it can be shown that $T\Gamma A_k \ge 0$ is a non-negative matrix, based on $T > 0$, $\Gamma \ge 0$ and $A \ge 0$. Consequently, we can obtain that $I - T\Gamma L_k = (I - T\Gamma\Delta) + T\Gamma A_k \ge 0$ is a non-negative matrix. From Lemma 2.6, it is obvious that the Laplacian matrix L_k satisfies $L_k 1_\mathrm{n} = 0$. This implies that $(I - T\Gamma L_k)1_\mathrm{n} = 1_\mathrm{n}$. Thus, $I - T\Gamma L_k$ is a stochastic matrix associated with the graph $\mathcal{G}$.

According to [5], we know that the eigenvalue $\lambda = 1$ of the stochastic matrix $I - T\Gamma L_k$ has algebraic multiplicity equal to 1 since $\mathcal{G}$ has a spanning tree. Thanks to $T\gamma_i a_{ii} = 0, \forall i \in \mathcal{V}_\mathcal{G}$, which implies that the diagonal elements of $I - T\Gamma L_k$ are the same as those of $I - T\Gamma\Delta$, which are guaranteed to be positive under the condition (10). According to [5], it is known that if the eigenvalue λ of the stochastic matrix $I - T\Gamma L_k$ is not equal to 1, its modulus is less than 1, i.e., $|\lambda| < 1$. From Lemma 3.1 and Lemma 3.2, it follows that $\{I - T\Gamma L_k\}$ is a SIA matrix set satisfying

$$\lim_{k\to\infty} (I - T\Gamma L_k) \cdots (I - T\Gamma L_2)(I - T\Gamma L_1) = 1y^{\mathrm{T}}. \tag{12}$$

By substituting (12) into (9), the consensus state x_C can be written in $x_C = y^{\mathrm{T}} x_0(T)$. That is, the consensus objective (4) can be derived. ■

IV. Simulation

In this section, an example is provided to validate our theoretical results. Let us consider a directed interaction graph with 6 nodes as shown in Fig. 1. The initial conditions of x_i, $i = 1, 2, ..., 6$ are selected as $x_1(0) = 15$, $x_2(0) = 9$, $x_3(0) = 10$, $x_4(0) = 7$, $x_5(0) = 5$, $x_6(0) = 8$, and the weighted adjacency vector Ω to indicate accessibility of the desired state information generating by a virtual agent labeled 0 is given by $\Omega = [1, 1, 0, 0, 0, 0]^{\mathrm{T}}$. In addition, the attacker' false information is set to be 20, which is out

of the safe initial state region. Here, the desired terminal state value of all agents is given by $x_T = 9$, while ensuring that the secure requirement (3) is not violated. We just choose the initial protocol $u_{0,i} = 0$. In view of (10), we select the nonzero learning gains such that $\Gamma = \mathrm{diag}\{0.02, 0.03, 0.02, 0.01, 0.02, 0.01\}$.

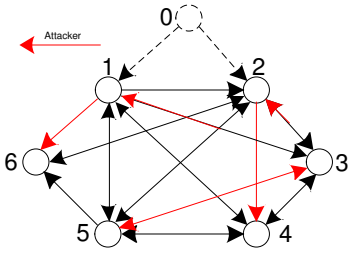

Fig. 1. Topological structure of the multi-agent network

To illustrate our Theorem, let the communication network satisfy a 3-robust graph described in Fig. 1 and the adjacency matrix be

$$A_{\mathcal{G}} = \frac{1}{10}\begin{bmatrix} 0 & 0 & 3 & 4 & 3 & 0 \\ 3 & 0 & 2 & 0 & 4 & 1 \\ 2 & 2 & 0 & 4 & 2 & 0 \\ 5 & 1 & 2 & 0 & 2 & 0 \\ 1 & 1 & 4 & 4 & 0 & 0 \\ 5 & 3 & 0 & 0 & 2 & 0 \end{bmatrix}. \tag{13}$$

Through observations, it is easy to check that the network topology in Fig. 1 satisfies a 3-robust graph. With the proper values of Γ and Ω selected above, we known that the condition (10) in Theorem 3.1 can be satisfied. From Fig. 2. we see that all agents can achieve a consensus at the desired terminal state x_T after an iterative learning process. Although the attackers try to drive the nodes to a value of 20, which is outside of their initial safe interval $[5, 15]$, the attackers are unable to achieve its goal whenever protocol (6) is applied.

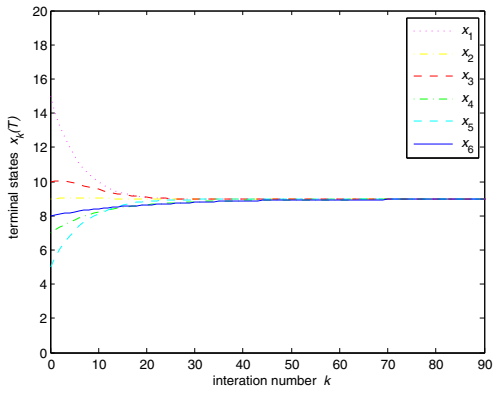

Fig. 2. State trajectories of $x_i(T), i = 1, 2, ..., 6$ under protocol (XX).

V. CONCLUSIONS

In this paper, we study the secure aspect of the consensus algorithm, which is a fundamental building block for the distributed systems. We propose a novel attack tolerance consensus algorithm in directed graph, and prove the sufficient condition for the graphs to be able to solve the finite-time consensus in the presence of edge-bound content modification attacks. One direction of the future work is to weaken the assumption on the graph topologies by exploring the use of two-hop or multi-hop neighboring information in the network.

REFERENCES

[1] J. M. Hendrickx, G. Shi, and K. H. Johansson, "Finite-time consensus using stochastic matrices with positive diagonals," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1070–1073, 2015.

[2] S. Liu, L. Xie, and D. E. Quevedo, "Event-triggered quantized communication based distributed convex optimization," *IEEE Transactions on Control of Network Systems*, 2016.

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

[4] S. Liu, D. E. Quevedo, and L. Xie, "Eventtriggered distributed constrained consensus," *International Journal of Robust and Nonlinear Control*, 2016.

[5] F. Pasqualetti, A. Bicchi, and F. Bullo, "Distributed intrusion detection for secure consensus computations," in *Proceedings of the 46th IEEE Conference on Decision and Control*, 2007, pp. 5594–5599.

[6] A. Haseltalab and M. Akar, "Approximate byzantine consensus in faulty asynchronous networks," in *Proceedings of the American Control Conference*, 2015, pp. 1591–1596.

[7] Z. Feng, G. Hu, and G. Wen, "Distributed consensus tracking for multiagent systems under two types of attacks," *International Journal of Robust & Nonlinear Control*, vol. 26, no. 5, pp. 896–918, 2016.

[8] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.

[9] G. D. L. Torre, T. Yucelen, and J. D. Peterson, "Resilient networked multiagent systems: A distributed adaptive control approachy," in *Proceedings of the 53rd IEEE Conference on Decision and Control*, 2014, pp. 5367–5372.

[10] Y. Wu, X. He, and S. Liu, "Resilient consensus for multi-agent systems with quantized communication," in *Proceedings of the American Control Conference*, 2016, pp. 5136–5140.

[11] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231–240, 2017.

[12] H.-S. Ahn and Y. Q. Chen, "Iterative learning control for multiagent formation," in *Proceedings of the ICROS-SICE International Joint Conference*, 2009, pp. 3111–3116.

[13] J. Li and J. Li, "Adaptive iterative learning control for coordination of secondorder multiagent systems," *International Journal of Robust & Nonlinear Control*, vol. 24, no. 18, pp. 3282–3299, 2014.

[14] X. Jin, "Adaptive iterative learning control for high-order nonlinear multi-agent systems consensus tracking," *Systems & Control Letters*, vol. 89, pp. 16–23, 2016.

[15] S. Yang, J.-X. Xu, and Q. Ren, "Multi-agent consensus tracking with initial state error by iterative learning control," in *Proceedings of the 11th IEEE International Conference on Control & Automation*, 2014, pp. 625–630.

[16] D. Meng and Y. Jia, "Iterative learning approaches to design finite-time consensus protocols for multi-agent systems," *Systems & Control Letters*, vol. 61, no. 1, pp. 187–194, 2012.

[17] D. Meng, Y. Jia, and J. Du, "Finite-time consensus protocols for networks of dynamic agents by terminal iterative learning," *International Journal of Systems Science*, vol. 45, no. 11, pp. 2435–2446, 2014.

[18] Y. Wu, X. He, S. Liu, and L. Xie, "Consensus of discrete-time multi-agent systems with adversaries and time delays," *International Journal of General Systems*, vol. 43, no. 3-4, pp. 402–411, 2014.

[19] Y. Wu, X. He, S. Liu, and Z. Qin, "A secure finite-time consensus scheme for multi-agent systems via terminal iterative learning," in *Proceedings of the 35th Chinese Control Conference*, 2016, pp. 8270–8274.

[20] W. Ren and R. W. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Transactions on Automatic Control*, vol. 50, no. 5, pp. 655–661, 2005.
[21] 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, 2008.
[22] C. Liu and F. Liu, "Stationary consensus of heterogeneous multi-agent systems with bounded communication delays," *Automatica*, vol. 47, no. 9, pp. 2130–2133, 2011.
[23] J. Wolfowitz, "Products of indecomposable, aperiodic, stochastic matrices," *Proceedings of the American Mathematical Society*, vol. 14, no. 5, pp. 733–737, 1963.
[24] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, p. 13, 2011.
[25] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on Automatic Control*, vol. 48, no. 6, pp. 988–1001, 2003.
[26] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge University Press, 2012.