IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 6, 2020, accepted April 21, 2020, date of publication April 23, 2020, date of current version May 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989743

Event-Triggered Resilient Consensus for Multi-Agent Networks Under Deception Attacks

YIMING WU[1], MING XU[1], NING ZHENG[1], AND XIONGXIONG HE[2]
[1]School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China
[2]College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China

Corresponding author: Yiming Wu (ymwu@hdu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61803135, Grant 61873239, and Grant 61702150, in part by the Cyberspace Security Major Program of the National Key Research and Development Plan of China under Grant 2016YFB0800201, in part by the State Key Program of Zhejiang Province Natural Science Foundation of China under Grant LZ15F020003, in part by the Key Research and Development Plan Project of Zhejiang Province under Grant 2017C01065, and in part by the Zhejiang Provincial Public Welfare Research Project of China under Grant LGG18F020015.

ABSTRACT In this paper, a novel distributed algorithm derived from the event-triggered strategy is proposed for achieving resilient consensus of multi-agent networks (MANs) under deception attacks. These malicious deception attacks are intended to interfere with the communication channel causing periods in time at which the sending information among nodes is modified. In particular, we develop an event-triggered update rule which can mitigate the influence of the attackers and at the same time reduce the computing and communication consumption. Each node chooses the instances to update its state information by checking whether its neighbor set meets a given cardinality-dependent function or not. With specified prerequisite on the coupling weights and the sampling period, the consensus achievement of the MANs is independent of the deception attacks, but strictly depends on the robustness of the interconnection topology. Simulation examples are finally given to illustrate the efficacy of the theoretical results.

INDEX TERMS Multi-agent networks, resilient consensus, event-triggered, deception attack.

I. INTRODUCTION

Consensus problem is widely recognized as one of the most fundamental problems in coordinated control of multi-agent networks (MANs), which means that the states of a group of agents reach an agreement based only on local information. It is the necessary prerequisite for the correctness of other collective behaviors in MANs, such as flocking, formation, and distributed optimization. For this reason, a number of papers devoted to designing consensus algorithms in various scenarios have appeared during the past decade (e.g., [1]–[5]).

Unfortunately, most of the works on consensus problem are obtained based on the assumption that the MANs are working in a secure environment and hence these consensus schemes are easily disrupted by adversarial behavior. Since there is an increasingly usage of MANs in life or mission critical applications (e.g., [6], [7]), this gives a strong motivation to design and analyze secure consensus algorithms which can be robust to cyber-attacks. However, due to the inherent limitations in the communication and computing resources available to the agents, existing computer security protection schemes (e.g., cryptographic techniques [8] and attack detection and identification techniques [9]) cannot be directly applied in MANs. Early in [10], a resilient consensus protocol was constructed for a system with fail-stop nodes. The design method therein follows from the classic probabilistic model and needs to possess a certain number of correct nodes. The work [11] explored the consensus problem for MANs with adversaries, but assumes that the network is complete. In [12], the authors analyzed the security performance of MANs under data falsification attacks, and proposed a robust distributed weighted average consensus algorithm. For systems with integrator type high-order dynamics, Feng *et al.* [13] proposed sufficient conditions to achieve secure consensus tracking control. Resilient consensus analysis for MANs of discrete- and continuous-time dynamics was addressed respectively in [14], [15]. The results have been later generalized to the case of switched MANs composed of discrete- and continuous-time subsystems [16]. In [17], random attacks on communication topology were considered when designing a distributed secure consensus controller. Combining the ideas of distributed algorithm and iterative

The associate editor coordinating the review of this manuscript and approving it for publication was Fangfei Li.

learning control, a resilient finite-time consensus protocol for MANs was obtained in [18]. More recently, a class of computationally efficient resilient consensus protocols based on the *Mean-Subsequence-Reduced* (MSR) algorithm have been proposed in [19]–[22]. In these MSR-type algorithms, each non-fault node in the network does not need to identify the faulty nodes among the system and only executes a local filtering algorithm to eliminate potential misbehavior. Since such algorithms have lightweight computation and require no information on overall network topology, they are inherently suitable for large-scale distributed networks.

Recently, there have been a growing number of research results on event-triggered control whose aim is to reduce the computation and communication burden while ensuring satisfactory system performance. Inspired by this idea, a plenty of notable results on event-triggered consensus schemes for MANs have been derived in the literature. Robust consensus analysis for event-triggered control of continuous-time first-order and second-order MANs was addressed respectively in [23], [24]. Finite-time consensus for a class of MANs with single integrator dynamics and scalar states was investigated in [25] by using a novel distributed event-triggered control approach. Specifically, in [26], the authors propose two event-triggered distributed time synchronization schemes from the viewpoint of multi-agent consensus, and show that synchronization can be achieved with less communication at guaranteed precision. Compared to static event-triggered methods, a dynamic event-triggered protocol was designed in [27], which can adaptively adjust the event-triggered function and thus may reduce the triggering times significantly. More details about event-triggered multi-agent consensus problems can be found in the recent survey paper [28].

However, most existing event-triggered schemes may also fail to work when a subset of nodes or communication links in the network is compromised by attacker. So far, only few papers address the event-triggered consensus control in MANs with cyber-attacks. Wang and Ishii [22] explored the resilient consensus of discrete-time MANs in the presence of malicious nodes in networks with directed topologies. By assuming that the maximum number of malicious nodes in the network is known, they propose two event-triggered consensus protocols for the updates of the non-faulty nodes. The authors in [29] investigated the event-triggered consensus problem of nonlinear MANs under denial-of-service (DoS) attacks, but assume the information of DoS attacks can be detected. In [30], an event-triggered strategy was adopted for distributed state estimation of nonlinear systems against DoS attacks. Besides, an event-based secure control for leader-following consensus was reported in [31], considering MANs with replay attacks and DoS attacks. The authors in [32] also studied the leader-following consensus problem in the presence of DoS attacks with event/self-triggered control schemes. In comparison with DoS attacks in [29]–[32], which interrupt information flow among the agents, deception attacks that compromise the integrity of data packets, can conduct more malicious manipulations on the whole consensus process.

A. STATEMENT OF CONTRIBUTIONS

In this paper, we first characterize the negative effect of deception attacks on the distributed multi-agent consensus process, and then quantify the resilience of the systems against such attacks using the concept of network robustness. Compared with most of the existing works which consider event-based consensus problems for continuous-time systems that need the triggering condition to be checked continuously at all times, a discrete-time system is carried out in this paper and the event condition is only required to be examined when a new neighboring message received which consumes much less computation resources.

Specifically, the main contributions of this paper can be highlighted as follows.

1) From the perspective of control theory, we characterize the effect of deception attacks on the performance of the distributed consensus algorithms for MANs. Moreover, based on the natural assumption that deception attacks are restricted in terms of attacker's capacity, we establish the corresponding mathematical attack model.
2) Under the attack model, an event-triggered control law is designed for realizing the resilient consensus of MAN, as well as an important discriminant value for each agent.
3) An explicit analysis of the attack model and network robustness is provided, as well as some sufficient conditions for the designed protocol, which guarantee that all the agents can achieve consensus in the presence of attackers.
4) Different from identifying and isolating the attacks in [17], [29], this paper studies lightweight attack-tolerant control strategy, which is suitable for large-scale distributed MANs with limited resources. Experimental results are presented to verify the effectiveness of our proposed methods.

The remainder of this paper is organized as follows. In Section II, we present preliminaries on graph theory and attack behaviors in MANs, and then formulate the problem. The design procedure of the secure event-triggered consensus scheme and the main results are shown in Section III. We give simulation results in Section IV to illustrate and verify the main results presented in this paper, and conclude in Section V.

Notations: In our development, the symbols $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{R}^+$ denote the set of natural, real, and positive real numbers, respectively. Let $\mathcal{A}$ and $\mathcal{B}$ be two sets, then $|\mathcal{A}|$ is the cardinality of set $\mathcal{A}$ and we denote by $\mathcal{A} \cup \mathcal{B}$, $\mathcal{A} \cap \mathcal{B}$ and $\mathcal{A} \backslash \mathcal{B}$ the union, intersection and difference of the sets. $a \ll b$ denotes that the number b is far larger than a.

II. PRELIMINARIES AND PROBLEM FORMULATION

In this section, first some basic concepts in the graph theory and attack models that will be used throughout the paper are reviewed, then the problem to be considered is formulated.

A. GRAPH THEORY AND NETWORK ROBUSTNESS

Here we collect some basic concepts about graphs, and one can find further details in [33].

A directed graph (digraph for short) is a triple $\mathcal{D} = (\mathcal{V}, \mathcal{E}, A)$ consisting of a set of nodes (or vertices) $\mathcal{V} = \{1, 2, \ldots, n\}$, a set of edges $\mathcal{E} = \mathcal{V} \times \mathcal{V}$, and an adjacency matrix $A = [a_{ij}] \in \mathbb{R}^{n\times n}$. A directed edge from i to j in $\mathcal{D}$ is denoted by $e_{ij} = (i, j) \in \mathcal{E}$, which means that the node j can obtain information from the node i, and node i and j are said to be neighbors. Assume $a_{ij} > 0 \Leftrightarrow e_{ji} \in \mathcal{E}$ and $a_{ij} = 0$ otherwise, and $a_{ii} = 0$ for all $i \in \{1, 2, \ldots, n\}$. The in-neighbors, or just neighbors, of node i are denoted by the sets $\mathcal{N}_i^{in} = \{j \in \mathcal{V} \,|(j, i) \in \mathcal{E}\}$. Likewise, the out-neighbors of node i are denoted by the sets $\mathcal{N}_i^{out} = \{j \in \mathcal{V} \,|(i, j) \in \mathcal{E}\}$.

Before proceeding further, we introduce a graph property known as *network robustness*, which was proposed in [34], and later studied in [19], [21], [35].

Definition 1 (r-Reachable Set [34]): For a digraph $\mathcal{D}$, the subset $\mathcal{S}$ of the node set $\mathcal{V}$ is said to be r-reachable if there exists a node that has at least r in-neighbours outside its own set $\mathcal{S}$, where $r \in \mathbb{N}$.

Definition 2 (r-Robust Graph [34]): A digraph $\mathcal{D} = \{\mathcal{V}, \mathcal{E}\}$ is said to be r-robust, with $r \in \mathbb{N}$, if for every pair of nonempty, disjoint subsets $\mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{V}$, at least one of the subsets satisfies r-reachable.

For the better description of the topology conditions for networks, we introduce two new concepts extended from the above definitions.

Definition 3 (Extra Reachable Set): For a digraph $\mathcal{D}$, the subset $\mathcal{S}$ of $\mathcal{V}$ is said to be extra reachable if there exists a node i in S such that $\left|\mathcal{N}_i^{in} \backslash S\right| > \left|\mathcal{N}_i^{in} \cap S\right|$.

Definition 4 (Extra Robust Graph): A digraph $\mathcal{D} = \{\mathcal{V}, \mathcal{E}\}$ is said to be extra robust if for every pair of nonempty, disjoint subsets $\mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{V}$, at least one of the subsets satisfies extra reachable.

In Fig. 1, we display one example graph with 4 nodes. One can check by Definitions 1-4 that the graph has enough connectivity to be 2-robust and extra robust.

B. THE ATTACK BEHAVIORS OF ADVERSARIES

Typically, there are two major types of attack behaviors that have been widely discussed in the networked control literature: disruption attacks (also known as DoS attacks [29], [36] or jamming attacks [37]) and deception attacks (or false data injection attacks [12], [38], [39]). In particular, we have to mention the deception attacks, which refer to the possibility of compromising the integrity of packets. It is shown that the deception attacks may be undetectable if the attacker launches attack sequences strategically [40]. Owing to the openness of MANs, false data can be injected into the exchanging

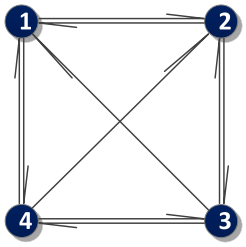

FIGURE 1. A 2-robust and extra robust graph with 4 nodes.

state information among agents by the adversaries. Under this situation, the designed consensus algorithm may not work correctly, leading to the failure of the overall system.

In this paper, we consider the case where the communication channels among neighboring nodes are suffering from deception attacks, i.e., attack spreads through links of a network. In this setting, a mathematical model for a deception attack on communication link from node j to node i at time k can be presented as

$$\tilde{x}_j(k) = x_j(k) + p_{ij}(k)x_j^a(k), \tag{1}$$

where $x_j^a(k)$ is the false information injected by a deception attack, and $p_{ij}(k)$ is the decision variable of attack acting on the directed communication channel from node j to node i, which is given by

$$p_{ij}(k) = \begin{cases} 1, & \text{if } e_{ji} \text{ is compromised by attacker} \\ 0, & \text{otherwise} \end{cases}$$

The attacker' objective is to designedly disrupt consensus process of the network via false data injection attacks. Assume $x_j^a(k)$ is arbitrary bounded real number. Then from (1) one can find that the compromised state value $\tilde{x}_j$ can be equal to any arbitrary value that the attacker wants through its carefully designed value x_j^a.

It is quite clear that no consensus among the nodes can be achieved without any constraint on the attacker's action, thus it is necessary to restrict the amount of such compromised links. For the problem of considering the range of attacks, there are two attack distribution models which have been widely used in the existing multi-agent consensus results [16], [19], [20], [34], [35]:

- *F-global* model. Under this model, the total number of compromised links in the graph is upper bounded by the number $F \in \mathbb{N}$.
- *F-local* model. Under this model, there are up to $F \in \mathbb{N}$ compromised links in the neighborhood of every node in the graph.

Considering the limited capacity of the attacker, we assume it can compromise up to F in-neighboring links of each node at one time. This is a commonplace assumption in the literature [13], [41], [42]. Therefore, we can properly adopt the *F-local* attack distribution model in this work. Based on this assumption, we obtain the following constraint condition

for parameter $p_{ij}(k)$,

$$\sum_{j\in\mathcal{N}_i^{in}} p_{ij}(k) \le F, \tag{2}$$

where F is a known finite positive number, which relates to the network topology as well as the attack model.

Remark 5: Notice that *F-global* attack model is in fact a special case of *F-local* model, and thus any resilience guarantees that hold for the latter model will also apply to the former model.

C. SYSTEM MODEL

Consider a distributed discrete-time MAN consisting of n agents, whose dynamics are described by

$$x_i((k+1)T) = x_i(kT) + u_i(kT)T, \quad i \in \mathcal{V}, \tag{3}$$

where $T \in \mathbb{R}^+$ is the sample period, $x_i(kT) \in \mathbb{R}$ is the state value of agent i and $u_i(kT)$ is the control input to be designed later. To simplify the notations, we replace all "(kT)" with "(k)" whenever no confusion would arise.

Concerning the cyber-attacks in MANs, the concept of resilient consensus has been extensively studied in the recent years [16], [19], [21], [22]. A major feature of resilient consensus is that it can effectively mitigate the influence of malicious attacks and guarantees the system achieves consensus to a value that lies in a so-called safety interval.

To be convenient, let us define

$$x_{\min}(k) = \min_{i\in\mathcal{V}} x_i(k), \quad x_{\max}(k) = \max_{i\in\mathcal{V}} x_i(k). \tag{4}$$

Note that by the above definitions, $x_{\min}(k)$ and $x_{\max}(k)$ represent the smallest and largest states among the nodes at time step k, respectively. Then, we define the resilient consensus problem for the system (3) under attacks as follow.

Definition 6 (Resilient Consensus): Given any initial conditions, we say the nodes of a MAN in the presence of malicious attacks have reached a resilient consensus if for any initial conditions, we have

$$x_i(k) \in [x_{\min}(0), x_{\max}(0)], \quad i \in \mathcal{V}, \tag{5}$$

and

$$\lim_{k\to+\infty} \left|x_j(k) - x_i(k)\right| = 0, \quad \forall i, j \in \mathcal{V}. \tag{6}$$

The purpose of this paper is to design an effective event-triggered consensus control strategy such that the system (3) can achieve resilient consensus defined by Definition 6 in the presence of deception attacks.

III. EVENT-TRIGGERED RESILIENT CONSENSUS UNDER DECEPTION ATTACKS

A. ALGORITHM DESIGN

Before giving our event-triggered control algorithm, we make the following assumptions.

Assumption 7: The communication digraph $\mathcal{D}$ is $(2F+1)$-robust.

Assumption 8: Nodes in the network transmit their state information over the channel with a communication delay Δi, where $0 < \Delta i \ll T$, $i \in \mathcal{V}$, and for all $i \neq j$, $\Delta i \neq \Delta j$, i.e., the messages received by node i from all its in-neighbors in the sampling interval $[kT, kT+T)$ are asynchronous.

In our scheme, each node $i \in \mathcal{V}$ needs to construct a detector to determine its own update moments. More specifically, node i receives a state value $x_j(kT+\Delta j)$ from one of its neighbors, and instantaneously records this value in the memory. The triggering condition is

$$\left|\mathcal{N}_{i,k}^{in}(t)\right| \ge 2F+1, \quad t \in [k, k+1), \tag{7}$$

where $\mathcal{N}_{i,k}^{in}(t)$ is the in-neighboring set of i at time step k, and F is the upper limit of number of compromised links among i' adjacent nodes. Note that the threshold depends on the upper limit number F. An event for node i is triggered as soon as the condition in (7) is satisfied, resulting in node i updating its state for the next time step. This triggering condition is easy to determine, and each node in the network is only required to be aware of the number of its neighbors.

Specifically, suppose that the deception attacks are restricted to form an F-local set, where $F \in \mathbb{N}$. The nodes do not need to know which (if any) of their incoming communication links are compromised which makes this suitable for saving distributed computational resources. At each time-step k, node $i \in \mathcal{V}$ performs the following actions in parallel with the other nodes:

1) Node i collects the state values $\{x_j(k), j \in \mathcal{N}_i^{in}(k)\}$ of its in-neighbors.
2) Once the triggering condition (7) is satisfied, node i simply stops collecting new values and starts to re-label the nodes in $\mathcal{N}_{i,k}^{in}(t)$ as $j_1, j_2, \ldots, j_{2F+1}$ according to their states from largest to smallest, that is,
$$\mathcal{N}_{i,k}^{in}(t) = \{j_1, \ldots, j_{2F+1} \left| x_{j_1} \ge x_{j_2} \ge \ldots \ge x_{j_{2F+1}} \right.\}.$$
3) Let $\check{x}_j(k)$ denote the $(F+1)$-th node' value in $\mathcal{N}_{i,k}^{in}(t)$, i.e., $\check{x}_j(k) = x_{j_{F+1}}$. Then node i applies the following control law
$$u_i(k) = \phi_{ij} a_{ij} (\check{x}_j(k) - x_i(k)), \tag{8}$$
where $\phi_{ij} > 0$ denotes the coupling weight chosen from any finite set.

With (8), the closed form of the system (3) is

$$x_i(k+1) = (1 - T\phi_{ij}a_{ij})x_i(k) + T\phi_{ij}a_{ij}\check{x}_j(k). \tag{9}$$

It should be noted that the identities of the neighboring nodes need not be known to the nodes in this paper and are used only for the analysis.

From the above description of our algorithm, we can observe that node i only uses $2F+1$ values received from its neighbouring nodes in each time step k. The computational complexity of (7)-(9) is clearly $O(|\mathcal{N}_{i,k}^{in}|)$ for each node i. We reduce the computational complexity of previous resilient consensus algorithms [11], [14], [15], [19], [21] by adopting an event-triggered function.

The attackers do not want the system to reach a consensus or intend to let the system agree on an critical value which beyond the safety interval $[x_{\min}(0), x_{\max}(0)]$, thus they will inject some false information that one can imagine into compromised links to achieve their purpose during the whole consensus process.

Our proposed algorithm mitigates the misbehavior of deception attacks by just choosing only one neighbor's information for each node to update its own state. With a sufficient number of neighboring nodes, our algorithm can adaptively eliminate the extreme values so that the false information is eventually isolated from the network.

Remark 9: With the help of the event-triggered update mechanism, we can find that there are fewer neighbor nodes that exchange information in each sampling period. Therefore, the resilience of our algorithm comes at the expense of lower computation, communication and memory costs in comparison with the existing resilient consensus algorithms [6], [13]–[15], [19], [22]. And thus it is more suitable for large-scale interconnected MANs with limited resources.

Remark 10: In our algorithm, we have relatively few requirements for any single node, that is, each node in the network knows nothing but a priori the maximum number F of compromised incoming links in its neighborhood.

B. MAIN RESULTS

We assume that the following prerequisite about the coupling weights and the sampling period of the system are satisfied:

Prerequisite 11: $\alpha < T\phi_{ij}a_{ij} < 1, 0 < \alpha < 1, \forall j \in \mathcal{N}_i^{in}$.

Based on Definition 2, the following lemma is readily obtained.

Lemma 12: For an r-robust digraph $\mathcal{D}$, one has $|\mathcal{N}_i^{in}| \geq r,\ \forall i \in \mathcal{V}$.

Theorem 13: Consider a digraph $\mathcal{D}$ with an F-local set of compromised links. If each node updates its state value according to update rule (9), and there are at least $2F+1$ in-neighbors in each node' neighborhood, i.e., $|\mathcal{N}_i^{in}| \geq 2F+1$. Then with Prerequisite 11, we have

$$x_i(k) \in [x_{\min}(0), x_{\max}(0)], \quad i \in \mathcal{V}.$$

Proof: Since there are at least $2F+1$ in-neighbors in each node' neighborhood, so the trigger condition (7) in control law can be guaranteed, which will keep the node's update process running. By the definitions of $x_{\min}[k], x_{\max}[k]$ and F-local attack distribution model, each node in the network will receive at most F values outside the interval $[x_{\min}(k), x_{\max}(k)]$ at each time step k. And it also means that such node will receive at least $F+1$ values inside the interval $[x_{\min}(k), x_{\max}(k)]$. Then by using control protocol (8), it is clear that no nodes will adopt a value outside $[x_{\min}(k), x_{\max}(k)]$ at each time-step.

With Prerequisite 11, the update rule (9) is a convex combination of node i's own value and the $(F+1)$-th node' value in $\mathcal{N}_{i,k}^{in}(t)$, which implies that both $x_{\max}(k)$ and $x_{\min}(k)$ are monotone and bounded functions of k.

Then follow the update rule (9), we have

$$\begin{aligned} x_i(k+1) &= (1-\kappa)x_i(k) + \kappa \check{x}_j(k) \\ &\leq (1-\kappa)x_{\max}(k) + \kappa x_{\max}(k) \\ &= x_{\max}(k) \end{aligned}$$

where $\kappa = T\phi_{ij}a_{ij} \in (0,1)$ based on Prerequisite 11. As a result, we have $x_{\max}(k+1) \leq x_{\max}(k)$. Similarly, we can use the same method to prove that $x_{\min}(k+1) \geq x_{\min}(k)$, which is omitted here for brevity.

Iterating, we obtain for any k,

$$x_{\min}(0) \leq x_{\min}(k) \leq \ldots \leq x_{\max}(k) \leq x_{\max}(0),$$

which concludes the proof. ∎

Theorem 13 shows that if the nodes in the network have a sufficient number of neighbors, the states of all agents under the proposed distributed control law are guaranteed to be within a so-called safety interval determined by the initial conditions.

Now, we are in a position to present some sufficient consensus conditions for the MANs with deception attacks.

Theorem 14: Consider a network $\mathcal{D} = \{\mathcal{V}, \mathcal{E}, A\}$ with an F-local set of compromised links, and let Assumptions 7 and 8 hold. Suppose the communication graph $\mathcal{D}$ satisfies an extra robust graph, and that the system (3) evolves under the control law (8) triggered by the event condition (7). Then, the whole group of agents can achieve resilient consensus.

Proof: By Lemma 12 and Assumptions 7, we know that each node in $\mathcal{D}$ has at least $2F+1$ in-neighbors. Then according to Theorem 13, we know that $x_{\min}(k)$ and $x_{\max}(k)$ defined in (4) are monotone functions of k and thus both of these two functions have a limited value. For the ease of notation, let us denote them by $\bar{x}_{\min}$ and $\bar{x}_{\max}$, respectively. It is clear that if $\bar{x}_{\min} = \bar{x}_{\max}$, the consensus is achieved for all nodes. We prove this by contradiction. Assume this is not the case, i.e., $\bar{x}_{\min} \neq \bar{x}_{\max}$. Remember that $\bar{x}_{\min} < \bar{x}_{\max}$ as defined in (4). From this, we further define a constant $\epsilon_0 > 0$ such that $\bar{x}_{\min} + \epsilon_0 < \bar{x}_{\max} - \epsilon_0$.

At the same time, given a sequence $\{\epsilon_i\}$ of positive numbers, we define the sets,

$$\mathcal{X}_M(k, \epsilon_i) = \{i \in \mathcal{V} \mid x_i(k) > \bar{x}_{\max} - \epsilon_i\},$$

and

$$\mathcal{X}_m(k, \epsilon_i) = \{i \in \mathcal{V} \mid x_i(k) < \bar{x}_{\min} + \epsilon_i\}.$$

Now one can choose a sufficiently small quantity $\epsilon < \frac{\alpha^n}{1-\alpha^n}\epsilon_0$ and note that this is smaller than ϵ_0. Then from the definition of convergence, we know that there exists a time-step k_ϵ such that for any $k \geq k_\epsilon$, $x_{\max}(k) < \bar{x}_{\max} + \epsilon$ and $x_{\min}(k) > \bar{x}_{\min} - \epsilon$. Now we consider the sets $\mathcal{X}_M(k_\epsilon, \epsilon_0)$ and $\mathcal{X}_m(k_\epsilon, \epsilon_0)$. It follows from the definition of ϵ_0 that the sets $\mathcal{X}_M(k_\epsilon, \epsilon_0)$ and $\mathcal{X}_m(k_\epsilon, \epsilon_0)$ are disjoint.

Since the communication topology of the network is extra robust, we know that there is at least one node in either $\mathcal{X}_M(k_\epsilon, \epsilon_0)$ or $\mathcal{X}_m(k_\epsilon, \epsilon_0)$ (or both) is extra reachable, i.e., the number of its neighbors from outside are more than the

number of its neighbors from inside. For definiteness, let us say, for example, that node $i \in \mathcal{X}_M(k_\epsilon, \epsilon_0)$ is extra reachable.

By Lemma 12, we know that node i has at least $2F+1$ in-neighbors, which ensures the triggering of its status update by the detector (7). Then by update rule (9), $\check{x}_j(k_\epsilon)$ from (8) will choose a value of its neighbor from outside $\mathcal{X}_M(k_\epsilon, \epsilon_0)$. By definition, an upper bound on the value of this neighbor from outside $\mathcal{X}_M(k_\epsilon, \epsilon_0)$ is $\bar{x}_{\max} - \epsilon_0$.

From (9), we see that the value of i at the next time-step is a convex combination of its own value and $\check{x}_j(k_\epsilon)$, and each coefficient in the combination is lower bounded by α. Since the largest possible state value that i may have at time-step k_ϵ is $x_{\max}(k_\epsilon)$, placing the largest possible weight $1-\alpha$ on $x_{\max}(k_\epsilon)$ in (9), we have

$$\begin{aligned} x_i(k_\epsilon+1) &\le (1-\alpha)x_{\max}(k_\epsilon) + \alpha\check{x}_j(k_\epsilon) \\ &< (1-\alpha)(\bar{x}_{\max}+\epsilon) + \alpha(\bar{x}_{\max}-\epsilon_0) \\ &= \bar{x}_{\max} - \alpha\epsilon_0 + (1-\alpha)\epsilon \\ &= \bar{x}_{\max} - \epsilon_1. \end{aligned}$$

Here $\epsilon_1 = \alpha\epsilon_0 - (1-\alpha)\epsilon$, which satisfies $0 < \epsilon < \epsilon_1 < \epsilon_0$. Similarly, let us consider the case that node i in set $\mathcal{X}_m(k_\epsilon, \epsilon_0)$ is extra reachable. By applying the same analysis as in case $i \in \mathcal{X}_M(k_\epsilon, \epsilon_0)$, we get that

$$\begin{aligned} x_i(k_\epsilon+1) &\ge (1-\alpha)x_{\min}(k_\epsilon) + \alpha\check{x}_j(k_\epsilon) \\ &> (1-\alpha)(\bar{x}_{\min}-\epsilon) + \alpha(\bar{x}_{\min}+\epsilon_0) \\ &= \bar{x}_{\min} + \alpha\epsilon_0 - (1-\alpha)\epsilon \\ &= \bar{x}_{\min} + \epsilon_1. \end{aligned}$$

Then let us further consider the sets $\mathcal{X}_M(k_\epsilon+1, \epsilon_1)$ and $\mathcal{X}_m(k_\epsilon+1, \epsilon_1)$. According to the previous analysis, we know that there either exists at least one node in $\mathcal{X}_M(k_\epsilon, \epsilon_0)$ whose value will be less than $\bar{x}_{\max} - \epsilon_1$ at time step $k_\epsilon+1$, or one node in $\mathcal{X}_m(k_\epsilon, \epsilon_0)$ whose value will be large than $\bar{x}_{\min} + \epsilon_1$ at time step $k_\epsilon+1$. Therefore, from the definition of $\mathcal{X}_M(k_\epsilon+1, \epsilon_1)$ and $\mathcal{X}_m(k_\epsilon+1, \epsilon_1)$, we have either $|\mathcal{X}_M(k_\epsilon+1, \epsilon_1)| < |\mathcal{X}_M(k_\epsilon, \epsilon_0)|$ or $|\mathcal{X}_m(k_\epsilon+1, \epsilon_1)| < |\mathcal{X}_m(k_\epsilon, \epsilon_0)|$. Note that $\epsilon_1 < \epsilon_0$, which guarantees that $\mathcal{X}_M(k_\epsilon+1, \epsilon_1)$ and $\mathcal{X}_m(k_\epsilon+1, \epsilon_1)$ are still disjoint.

We continue in this manner by defining $\epsilon_s = \alpha\epsilon_{s-1} - (1-\alpha)\epsilon$, $s \ge 1$. It is easy to verify that $\epsilon_s < \epsilon_{s-1}$. Recursively extending the previous analysis to s steps, where $s \le n$, one can find that for $\mathcal{X}_M(k_\epsilon+s, \epsilon_s)$ and $\mathcal{X}_m(k_\epsilon+s, \epsilon_s)$, at least one of them will be empty.

If $\mathcal{X}_M(k_\epsilon+s, \epsilon_s) = \emptyset$, then from the definition of $\mathcal{X}_M(k_\epsilon+s, \epsilon_s)$, we have

$$x_i(k_\epsilon+s) \le \bar{x}_{\max} - \epsilon_s.$$

Similarly, when $\mathcal{X}_m(k_\epsilon+s, \epsilon_s) = \emptyset$, we have

$$x_i(k_\epsilon+s) \ge \bar{x}_{\min} + \epsilon_s.$$

Now we will arrive at a contradiction that the largest value monotonically converges to $\bar{x}_{\max}$ or that the smallest value monotonically converges to $\bar{x}_{\min}$ with the aid of the condition $\epsilon_s > 0$. We will show this must be the case. Recall that $\epsilon < \frac{\alpha^n}{1-\alpha^n}\epsilon_0$ and $0 < \alpha < 1$ by the definitions, we have

$$\begin{aligned} 0 &< \alpha^n\epsilon_0 - (1-\alpha^n)\epsilon \le \alpha^s\epsilon_0 - (1-\alpha^s)\epsilon \\ &= \alpha^s\epsilon_0 - (1-\alpha)(1+\alpha+\ldots+\alpha^{s-1})\epsilon \\ &= \alpha^2\epsilon_{s-2} - \alpha(1-\alpha)\epsilon - (1-\alpha)\epsilon \\ &= \alpha\epsilon_{s-1} - (1-\alpha)\epsilon \\ &= \epsilon_s. \end{aligned}$$

Thus, we get a contradiction. This implies that ϵ_0 must be 0, namely, $\bar{x}_{\max} = \bar{x}_{\min}$, which concludes the proof. ■

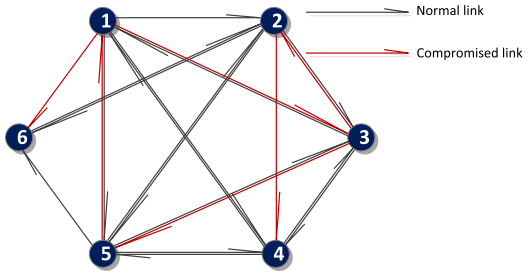

FIGURE 2. The digraph associated with the network containing 6 nodes.

IV. SIMULATION EXAMPLE

In this section, we present one simulation example to illustrate our results. Simulation experiments have been performed with MATLAB.

To illustrate the performance of the designed control law, let us consider a MAN consisting of 6 agents, whose interaction topology is modelled by a digraph with 6 nodes and 22 links (see Fig. 1). In Fig. 1, arrows indicate the direction of communication links and red solid lines indicate the compromised links which convey the false data injected by the attacker. The initial state of agents are selected randomly as $x(0) = col(15, 8, 4, -1, -7, -12)$. For simplicity, the adjacency matrix is selected as a binary matrix, whose element is either 1 or 0, and the coupling weight matrix $\Phi = [\phi_{ij}]$ is chosen as

$$\Phi = \begin{bmatrix} 0 & 0.2 & 0.1 & 0.4 & 0.2 & 0.1 \\ 0 & 0 & 0.3 & 0.2 & 0.3 & 0.2 \\ 0.2 & 0.4 & 0 & 0.1 & 0.3 & 0 \\ 0.5 & 0 & 0.3 & 0 & 0.2 & 0 \\ 0.2 & 0.2 & 0.3 & 0.1 & 0 & 0.2 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Then, by appropriately choosing sampling time $T = 0.5s$, one can check that $T\phi_{ij}a_{ij} < 1, \forall j \in \mathcal{N}_i$, which meets Prerequisite 11.

Suppose that the links (1, 3), (1, 6), (2, 4), (3, 2), (3, 5), (5, 1) are compromised by deception attacks. Let us select the following false information $x_j^a(k)$:

$$x_j^a(k) = \frac{k}{10}\pi \sin(\frac{k}{5}\pi),$$

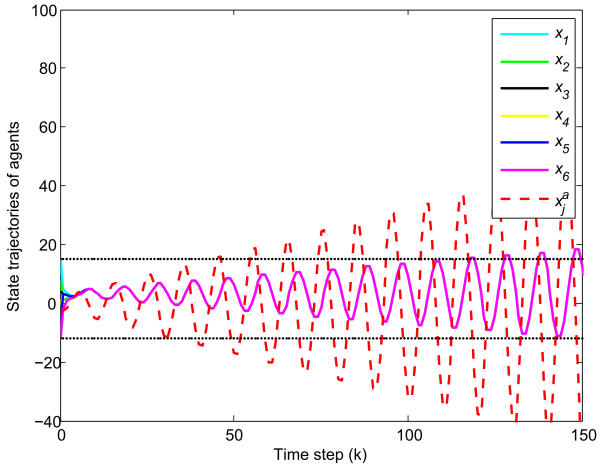

FIGURE 3. State trajectories of MAN under the LCP protocol proposed in [1].

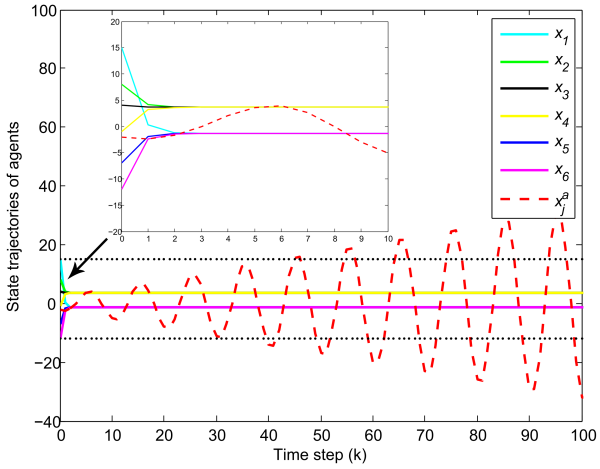

FIGURE 4. State trajectories of the agents always stay in a certain safe interval but do not reach a consensus.

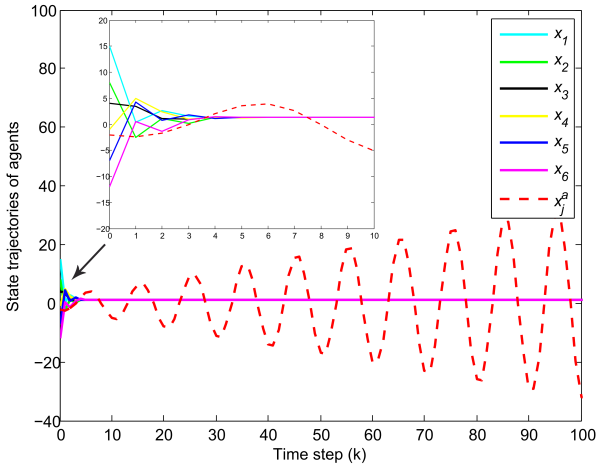

FIGURE 5. State trajectories of the agents reach a consensus under the adversarial behavior.

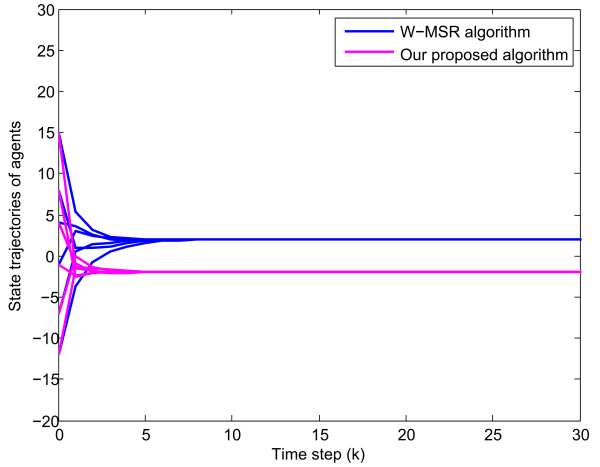

FIGURE 6. State trajectories of MAN under two different distributed consensus protocols.

where the adversary's goal is to drive the system' trajectory to a repetitive oscillation. One also notices that it satisfies the deploy requirements of 1-*local* attack model.

As stated in Definitions 2 and 4, it can be verified that the digraph in Fig. 1 satisfies both 3-robust and extra robust, indicating that up to one compromised links can be tolerated by our scheme with $F = 1$. Fig. 3 shows the state trajectories of the system equipped with a standard linear consensus protocol (LCP) [1]. Without any security strategy, the LCP algorithm is very vulnerable to attacks, and hence we can see from the figure that the adversary is able to make the state values of all agents constantly oscillate, just by intentionally injecting the above false information $x_j^a(k)$ into these compromised links. The safe boundary values (black dashed line) of initial states defined by Definition 6 is also shown in Fig. 3.

Now we show how the communication topology condition $(2F + 1)$-robustness affects the convergence performance of the proposed algorithm. For this purpose, let us temporarily remove communication link from node 1 to node 4 in Fig. 1. With this change, one can verify that the robustness of network is still 3-robust but do not satisfy the condition of extra robust. Consider the event-triggered control protocol (8) and the triggering condition (7). Set the event-triggering threshold $|\mathcal{N}_{i,k}^{in}(t)| = 3$. With these control parameters, the simulated trajectories by executing the protocol (8) is plotted in Fig. 4. As stated in Theorem 13, we can observe that, as time goes on, our algorithm ensures nodes updating their states in a certain safe state interval despite false data interferences, but cannot guarantee the convergence of the system.

Next, we reconnect the link (1, 4) to make sure that the network satisfies an extra robust graph again. We execute the protocol (8) again. Simulation results are presented in Fig. 5. From Fig. 5, one can see that consensus is achieved by getting rid of the influence of deception attacks, which is consistent with Theorem 14.

Furthermore, we compare our algorithm with the W-MSR algorithm [19]. Compared to our method, the W-MSR algorithm has no event-triggered control mechanism, and hence

needs to communicate with more neighboring nodes in the network at each sampling period. The simulation results are presented in Fig. 6. We can observe from the figure that the performances of two algorithms are similar. However, our method employs less resource, i.e., less memory, computation, and perception. Furthermore, our method has a faster convergence speed than the W-MSR algorithm, which implies that more communication does not necessarily lead to faster convergence. On the contrary, this may not only result in more communication resources consuming, but also provides more opportunities for adversaries to launch attacks.

V. CONCLUSION

In order to mitigate the impact of deception attacks and meanwhile reduce network resource consumption, a distributed resilient control scheme is developed to ensure that the consensus of MANs can be realized. The proposed scheme is event-triggered in the sense that each node selectively updates its state value in a directed network with the proper interconnection topology design. Under this scheme, the threshold condition proposed is only dependent on the number of received message coming from neighboring nodes. As a consequence, our algorithm does not rely on delicate hardware for continuous monitoring, and therefore it is more suitable for large-scale distributed MANs with limited resources for every single agent. In the end, a simulation example has been presented to illustrate the theoretical results.

In the future, we may further consider the event-triggered resilient consensus problem for the systems with second-order dynamics. Utilizing the proposed protocols in formation control of unmanned aerial vehicles, distributed filtering, and wireless sensor networks are other topics for future work.

REFERENCES

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

[2] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[3] M. Cao, A. S. Morse, and B. D. O. Anderson, "Reaching a consensus in a dynamically changing environment: A graphical approach," *SIAM J. Control Optim.*, vol. 47, no. 2, pp. 575–600, Jan. 2008.

[4] J. Xu, H. Zhang, and L. Xie, "Consensusability of multiagent systems with delay and packet dropout under predictor-like protocols," *IEEE Trans. Autom. Control*, vol. 64, no. 8, pp. 3506–3513, Aug. 2019.

[5] Y. Zheng, Q. Zhao, J. Ma, and L. Wang, "Second-order consensus of hybrid multi-agent systems," *Syst. Control Lett.*, vol. 125, pp. 51–58, Mar. 2019.

[6] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5107–5117, Jun. 2017.

[7] Z. Han, K. Guo, L. Xie, and Z. Lin, "Integrated relative localization and Leader–Follower formation control," *IEEE Trans. Autom. Control*, vol. 64, no. 1, pp. 20–34, Jan. 2019.

[8] 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.

[9] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.

[10] G. Bracha and S. Toueg, "Resilient consensus protocols," in *Proc. 2nd Annu. ACM Symp. Princ. Distrib. Comput. (PODC)*. New York, NY, USA: ACM, 1983, pp. 12–26.

[11] H. J. LeBlanc and X. D. Koutsoukos, "Consensus in networked multi-agent systems with adversaries," in *Proc. 14th Int. Conf. Hybrid Syst., Comput. Control (HSCC)*. New York, NY, USA: ACM, 2011, pp. 281–290.

[12] B. Kailkhura, S. Brahma, and P. K. Varshney, "Data falsification attacks on consensus-based detection systems," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 3, no. 1, pp. 145–158, Mar. 2017.

[13] Z. Feng, G. Hu, and G. Wen, "Distributed consensus tracking for multi-agent systems under two types of attacks," *Int. J. Robust Nonlinear Control*, vol. 26, no. 5, pp. 896–918, Mar. 2016.

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

[15] Y. Wu and X. He, "Secure consensus control for multi-agent systems with attacks and communication delays," *IEEE/CAA J. Automatica Sinica*, vol. 4, no. 1, pp. 136–142, 2017.

[16] Y. Shang, "Resilient consensus of switched multi-agent systems," *Syst. Control Lett.*, vol. 122, pp. 12–18, Dec. 2018.

[17] Y. Yang, H. Xu, and D. Yue, "Observer-based distributed secure consensus control of a class of linear multi-agent systems subject to random attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 8, pp. 3089–3099, Aug. 2019.

[18] Y. Wu, M. Xu, N. Zheng, and X. He, "Attack tolerant finite-time consensus for multi-agent networks," in *Proc. 13th IEEE Int. Conf. Control Autom. (ICCA)*, Jul. 2017, pp. 1010–1014.

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

[20] S. Sundaram and B. Gharesifard, "Distributed optimization under adversarial nodes," *IEEE Trans. Autom. Control*, vol. 64, no. 3, pp. 1063–1076, Mar. 2019.

[21] H. Zhang and S. Sundaram, "A simple median-based resilient consensus algorithm," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1734–1741.

[22] Y. Wang and H. Ishii, "Resilient consensus through asynchronous event-based communication," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2019, pp. 1842–1847.

[23] G. Shi and K. H. Johansson, "Multi-agent robust consensus-part II: Application to distributed event-triggered coordination," in *Proc. IEEE Conf. Decis. Control Eur. Control Conf.*, Dec. 2011, pp. 5738–5743.

[24] M. Cao, F. Xiao, and L. Wang, "Event-based second-order consensus control for multi-agent systems via synchronous periodic event detection," *IEEE Trans. Autom. Control*, vol. 60, no. 9, pp. 2452–2457, Sep. 2015.

[25] B. Hu, Z.-H. Guan, and M. Fu, "Distributed event-driven control for finite-time consensus," *Automatica*, vol. 103, pp. 88–95, May 2019.

[26] Y. Kadowaki and H. Ishii, "Event-based distributed clock synchronization for wireless sensor networks," *IEEE Trans. Autom. Control*, vol. 60, no. 8, pp. 2266–2271, Aug. 2015.

[27] J. Song and Y. Niu, "Dynamic event-triggered sliding mode control: Dealing with slow sampling singularly perturbed systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, early access, Jul. 4, 2019, doi: 10.1109/TCSII.2019.2926879.

[28] C. Nowzari, E. Garcia, and J. Cortés, "Event-triggered communication and control of networked systems for multi-agent consensus," *Automatica*, vol. 105, pp. 1–27, Jul. 2019.

[29] L. Zha, J. Liu, and J. Cao, "Resilient event-triggered consensus control for nonlinear muti-agent systems with DoS attacks," *J. Franklin Inst.*, vol. 356, no. 13, pp. 7071–7090, Sep. 2019.

[30] J. Liu, W. Suo, L. Zha, E. Tian, and X. Xie, "Security distributed state estimation for nonlinear networked systems against DoS attacks," *Int. J. Robust Nonlinear Control*, vol. 30, no. 3, pp. 1156–1180, Feb. 2020.

[31] J. Liu, T. Yin, D. Yue, H. R. Karimi, and J. Cao, "Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks," *IEEE Trans. Cybern.*, early access, Feb. 19, 2020, doi: 10.1109/TCYB.2020.2970556.

[32] W. Xu, D. W. C. Ho, J. Zhong, and B. Chen, "Event/Self-triggered control for leader-following consensus over unreliable network with DoS attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 10, pp. 3137–3149, Oct. 2019.

[33] M. Mesbahi and M. Egerstedt, *Graph Theoretic Methods in Multiagent Networks*. Princeton, NJ, USA: Princeton Univ. Press, 2010.

[34] H. Zhang and S. Sundaram, "Robustness of information diffusion algorithms to locally bounded adversaries," in *Proc. Amer. Control Conf. (ACC)*, Jun. 2012, pp. 5855–5861.
[35] H. Zhang, E. Fata, and S. Sundaram, "A notion of robustness in complex networks," *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 3, pp. 310–320, Sep. 2015.
[36] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Event-triggered control systems under Denial-of-Service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 93–105, Mar. 2017.
[37] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Analysis of stochastic switched systems with application to networked control under jamming attacks," *IEEE Trans. Autom. Control*, vol. 64, no. 5, pp. 2013–2028, May 2019.
[38] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Dec. 2010, pp. 5967–5972.
[39] X.-M. Li, Q. Zhou, P. Li, H. Li, and R. Lu, "Event-triggered consensus control for multi-agent systems against false data-injection attacks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1856–1866, May 2020, doi: 10.1109/TCYB.2019.2937951.
[40] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.
[41] R. Moghadam and H. Modares, "Resilient adaptive optimal control of distributed multi-agent systems using reinforcement learning," *IET Control Theory Appl.*, vol. 12, no. 16, pp. 2165–2174, Nov. 2018.
[42] H. J. LeBlanc and X. D. Koutsoukos, "Resilient synchronization in robust networked multi-agent systems," in *Proc. 16th Int. Conf. Hybrid Syst., Comput. Control (HSCC)*. New York, NY, USA: ACM, 2013, pp. 21–30.

YIMING WU received the B.E. degree in automation and the Ph.D. degree in control science and engineering from the Zhejiang University of Technology, Zhejiang, China, in 2010 and 2016, respectively. From April 2012 and April 2014, he was a Research Assistant with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Since July 2016, he has been with the School of Cyberspace, Hangzhou Dianzi University, Zhejiang, China. His main research interests include resilient consensus control, security control, iterative learning control, and applications in multiagent systems and sensor networks.

MING XU received the M.S. and Ph.D. degrees from Zhejiang University, Hangzhou, China, in 2000 and 2004, respectively. He is currently a Full Professor with Hangzhou Dianzi University, Hangzhou. His research interests include network security and digital forensics.

NING ZHENG received the M.S. degree from Zhejiang University, Hangzhou, China, in 1990. He is currently a Full Professor with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China. His current research interests include information security, information management systems, and multiagent networks.

XIONGXIONG HE received the M.S. degree from Qufu Normal University, Qufu, China, in 1994, and the Ph.D. degree from Zhejiang University, Hangzhou, China, in 1997. He held a postdoctoral position with the Harbin Institute of Technology, from 1998 to 2000. He joined the Zhejiang University of Technology Hangzhou, China, in 2001, where he has been a Professor with the College of Information Engineering. His research interests include nonlinear control, iterative learning control, intelligent control, and applications in multiagent systems and sensor networks. He was a General Chair of the 2014 IEEE Conference on Industrial Electronics and Applications and Technical Program Chair of the 2016 Conference on Data-Driven Control and Learning Systems.