Secure Cooperative Event-Triggered Control of Linear Multiagent Systems Under DoS Attacks

Zhi Feng and Guoqiang Hu

***Abstract*— This paper studies secure cooperative event-triggered control of linear multiagent systems under denial-of-service (DoS) attacks. The DoS attacks refer to interruptions of communication channels carried out by an intelligent adversary. We consider a class of time-sequence-based DoS attacks allowed to occur aperiodically. Then, an explicit analysis of the frequency and duration of DoS attacks is investigated for both secure leaderless and leader-following consensus problems. A resilient cooperative event-triggered control scheme is developed and scheduling of controller updating times is determined in the presence of DoS attacks. It is shown that based on the proposed distributed algorithms, all the agents can achieve secure consensus exponentially. The effectiveness of the developed methods is illustrated through three case studies: 1) multiple robot coordination; 2) distributed voltage regulation of power networks; and 3) distributed cooperative control of unstable dynamic systems.**

***Index Terms*— Directed topology, DoS attack, event-triggered control, networked multiagent system, secure coordination.**

I. Introduction

A FUNDAMENTAL problem on cooperative control of networked multiagent systems is to develop distributed controllers by using only relative measurements such that all the agents of the whole agent group can eventually achieve the state consensus [1]–[6]. Distributed secure control of networked multiagent systems in the presence of cyberattacks is an interesting and important problem. Few efforts have been made to achieve secure consensus against malicious cyberattacks.

Typically, there are two different attack scenarios in a multiagent system: attacks on the dynamic behaviors of agents and attacks on their communication. The works in [7] and [8] show that an attack on a specific agent is identical to agent removal on a network graph. In reality, it is more general to study attacks on communication, classified as either DoS or deception attacks [9]–[21]. The former refers to interruptions of communication on control and/or measurement channels carried out by an intelligent adversary to violate availability. The latter refers to the data trustworthiness where the adversary manipulates data transmitted over communication networks to violate integrity. Gupta *et al.* [9], Zhang *et al.* [13], Teixeira *et al.* [14], Shisheh *et al.* [16], Cetinkaya *et al.* [17], De. Persis and Tesi [18], Chen *et al.* [19] studied the secure control against DoS attacks in a centralized setting. To the best of our knowledge, there are few works addressing distributed secure coordination of multiagent systems under DoS attacks. The presence of DoS attacks may lead to the loss of consensus of multiagent systems. A problem of interest is to investigate coordination from the perspective of resilience to achieve secure consensus [30]–[32].

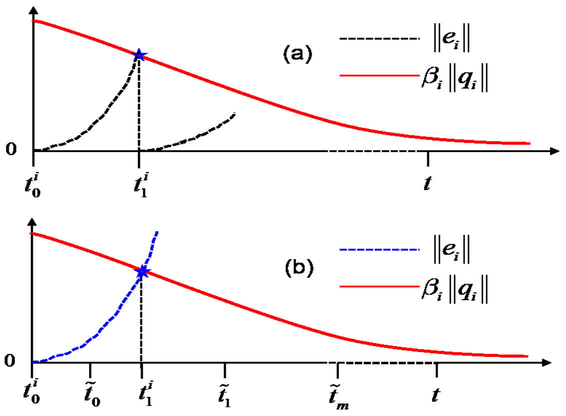


Fig. 1. Diagram for the event condition in (1) (motivated by De. Persis and Tesi [18] and Feng and Hu [34]). (a) In the absence of DoS attacks. (b) In the presence of DoS attacks. $\{\tilde{t}_m\} = \{\tilde{t}_0, \tilde{t}_1, \ldots\}$ denotes the DoS attack time sequence.

Unlike periodical samplings that may waste much energy, an event-based sampling scheme was developed in [22]–[26] to overcome the existing limitations of resource, computation, and communication. The original idea of event-based control is to trigger an event and then close the feedback loop whenever the system state deviates from the equilibrium and crosses a threshold [22]. The following widely used event-triggered condition, as illustrated in Fig. 1(a), is given to guarantee state consensus of multiagent systems [23]–[26]

$$\|e_i(t)\| = \left\|x_i\left(t^i_{k_i}\right) - x_i(t)\right\| \le \beta_i\|q_i(t)\|, \quad i = 1, 2, \ldots, N \tag{1}$$

Manuscript received March 21, 2018; revised August 24, 2018; accepted December 25, 2018. Manuscript received in final form January 6, 2019. This work was in part supported by the Singapore Economic Development Board through EIRP under Grant S14-1172-NRF EIRP-IHL, and in part by the Singapore Ministry of Education Academic Research Fund Tier 1 RG180/17(2017-T1-002-158). This paper was presented in part at the American Control Conference, 2017 and in part at the 14th IEEE International Conference on Information and Automation, 2017. Recommended by Associate Editor A. Speranzon. *(Corresponding author: Guoqiang Hu.)*

The authors are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: zhifeng@ntu.edu.sg; gqhu@ntu.edu.sg).

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

Digital Object Identifier 10.1109/TCST.2019.2892032

where $q_i(t) = \sum_{j=1}^{N} a_{ij}(x_j(t) - x_i(t))$, $t_{k_i}^i$ denotes the triggered event time, and $\beta_i \in (0,1)$ is a positive constant. Verifying this condition requires neighboring information via continuous communication. Recently, different event-triggered consensus strategies were studied in [23]–[25] and [27]–[29], respectively, for multiagent systems to avoid this requirement. Note that the aforementioned results in [22]–[29] considered consensus in ideal network environment. However, for unreliable network environment with DoS attacks, it can be seen from Fig. 1(b) that the event-triggered condition (1) might be violated in the presence of DoS attacks, which leads to the loss of consensus. Therefore, it is important to study coordination from the perspective of resilience to achieve secure consensus.

A. Related Works

Shisheh *et al.* [16] first proposed a centralized event-triggered controller to address energy-constrained DoS attacks by assuming that the known attacks occur periodically. In [18], this centralized event-triggered strategy was considered for a single agent system, and stability was achieved if attack duration was upper bounded. This design was further extended in [21] to handle DoS attacks and unavailable measurements. Unlike [16]–[21] to investigate a single agent system, a networked multiagent system in the presence of two types of attacks was first considered in [30], and the results were further extended in [31] and [32]. A hybrid secure control framework was developed to achieve secure consensus, provided that the frequency and duration of attacks satisfy certain conditions. However, Feng and Hu [30], Feng *et al.* [31], [32] assumed that the system has a complete or partial access to the attacker's movement. Based on these results, a signum function-based ternary controller was proposed in [33] for self-triggered coordination of first-order agent systems with practical consensus under an undirected graph. Recently, Feng and Hu [34] proposed the event-triggered designs to solve secure leaderless consensus under an undirected graph. Motivated by the works in [30]–[35], exponential consensus of general linear multiagent systems will be studied under a directed topology and DoS attacks with aperiodic strategies.

B. Main Contributions

Compared with consensus of networked multiagent systems in [1]–[6], and its applications in [41]–[45], this paper investigates secure consensus for general linear multiagent systems under the unreliable network environment with DoS attacks. Unlike developing control strategies against different attacks for a single agent system in [9]–[17], a time-sequence-based attack model is considered where the attacks are allowed to occur aperiodically. Different from [16]–[18] using centralized controllers and [30]–[32] using periodic samplings, a hybrid coordination framework built on the event-based samplings with an open-loop estimation scheme is proposed. The event condition is developed to determine when to update the controller for each agent, and broadcast its measurements to its neighbors. Although a similar open-loop estimation scheme was employed, this paper significantly extends the existing results in [27]–[29]. Specifically, consensus can be achieved exponentially for agents connected by a directed graph, while the uniformly ultimately bounded consensus was obtained in [27]–[29] under an undirected graph. This bidirectional case is nontrivial and brings theoretical challenges. Moreover, in contrast to [27]–[29] studying consensus in ideal network environment, the existing event conditions are not sufficient to guarantee consensus. Additional requirements are needed to eliminate the adverse effects of attacks. By the proposed designs, both secure leaderless and leader-following consensus results are achieved to provide resilience against DoS attacks, provided that the frequency and duration of attacks satisfy certain conditions.

Organization: In Section II, the relevant concepts on the graph theory, agent model, and attack model are presented, respectively. In Section III, the distributed event-triggered controller design and stability analysis for secure leaderless consensus are presented. Then, the secure leader-following consensus is further considered in Section IV. Section V provides the examples and numerical simulations on multirobot coordination, distributed voltage regulation of power networks, and distributed cooperative control of unstable dynamic systems to illustrate the effectiveness of the proposed methods. Finally, the conclusion is presented in Section VI.

Notation: $\mathbb{R}$ ($\mathbb{R}_{\geq 0}$) and $\mathbb{R}^{N\times N}$ denote the sets of reals (greater than or equal to 0) and $N \times N$ matrices, respectively. Let $\mathbb{N}$ be the set of positive natural numbers. 0_N (or 1_N) are the $N \times 1$ vector with all zeros (or ones). Let $\text{col}(x_1, \ldots, x_N)$ and $\text{diag}\{a_1, \ldots, a_N\}$ be a column vector with entries x_i and a diagonal matrix with a_i, $i = 1, \ldots, N$, respectively. $\otimes$ and $\|\cdot\|$ denote, respectively, the Kronecker product and Euclidean norm. For a real symmetric matrix M, $\lambda_{\min}(M)$ and $\lambda_{\max}(M)$ represent its smallest and maximum eigenvalues, respectively, and $M > 0$ represents that M is positive definite. $\sigma_{\min}(\cdot)$ and $\sigma_{\max}(\cdot)$ are the minimum and maximum singular values of a matrix, respectively.

II. Problem Formulation

A. Graph Theory

Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ represent a graph. $\mathcal{V} \in \{1, 2, \ldots, N\}$ denotes the set of nodes. Every agent is represented by a node. $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the set of edges. An edge is an ordered pair $(i, j) \in \mathcal{E}$ if node j can be directly supplied with information from node i. We assume that there is no self loops in the graph, that is, $(i, i) \notin \mathcal{E}$. Let $\mathcal{N}_i(\mathcal{G}) = \{j \in \mathcal{V} \,|(j, i) \in \mathcal{E}\}$ represent the neighborhood set of node i. Graph $\mathcal{G}$ is said to be undirected if for any edge $(i, j) \in \mathcal{E}$, edge $(j, i) \in \mathcal{E}$. An undirected graph is connected if there exists an undirected path between any two distinct nodes in the graph. A digraph $\mathcal{G}$ contains a directed spanning tree if there is a node which can reach all other nodes through a directed path [36]. The weighted adjacency matrix of $\mathcal{G}$ is defined as $\mathbb{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$, where $a_{ij} > 0$ if and only if $(j, i) \in \mathcal{E}$, otherwise $a_{ij} = 0$. The Laplacian matrix of $\mathcal{G}$ is defined as $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{N\times N}$ where $l_{ii} = \sum_{j=1}^{N} a_{ij}$ and $l_{ij} = -a_{ij}$ if $i \neq j$.

B. Multiagent Network Model

Consider a multiagent network consisting of N agents with identical general linear dynamics described by

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad t \in \mathbb{R}_{\geq 0} \tag{2}$$

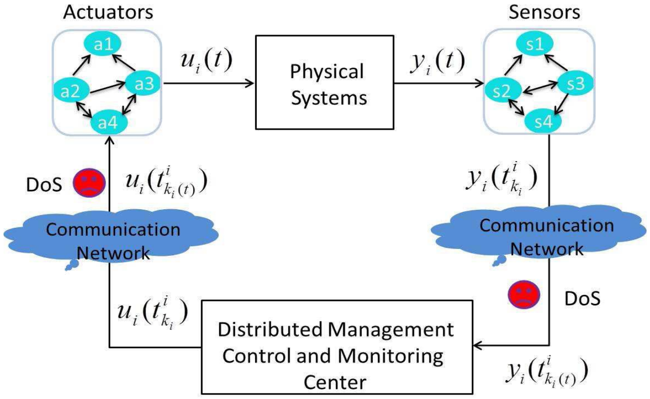


Fig. 2. Networked multiagent system under DoS attacks [34].

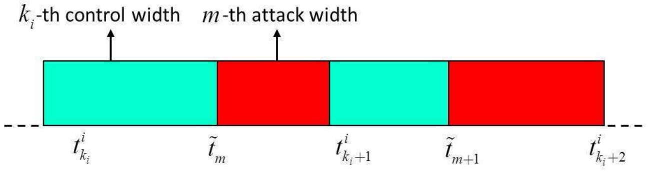


Fig. 3. Schematics of time sequences $\{\tilde{t}_m\}_{m\in\mathbb{N}}$ and $\{t^i_{k_i}\}_{k_i\in\mathbb{N}}$.

where $x_i(t) \in \mathbb{R}^n$ and $u_i(t) \in \mathbb{R}^l$, $i = 1, 2, \ldots, N$ are the state and control input, respectively, and $A \in \mathbb{R}^{n\times n}$, and $B \in \mathbb{R}^{n\times l}$ are the system and input matrices of (2), respectively. In this paper, A is assumed to be not necessarily Hurwitz, while a standard assumption is that (A, B) is stabilizable [5], [6].

As investigated in [1]–[6], the goal of distributed coordination is to design the following distributed controller such that all the agents can reach consensus of the states

$$u_i(t) = K\xi_i(t), \quad \xi_i(t) = \sum_{j=1}^{N} a_{ij}(x_j(t) - x_i(t)) \tag{3}$$

where $i = 1, 2, \ldots, N$, a_{ij} is the adjacency element, $K > 0$ is the constant gain matrix with appropriate dimension, and $\xi_i(t) \in \mathbb{R}^n$ is the consensus error.

C. DoS Attack Model

DoS attack [9]–[21]: refer to a class of attacks where an adversary renders certain or all components of an inaccessible control system. The DoS attacks can be launched by the adversary in the form of jamming the communication channels, compromising the devices, preventing them from sending data, and attacking the routing protocols. The DoS attacks can simultaneously affect both the measurement and control channels, which leads to the loss of data availability. This case can be illustrated in Fig. 2.

In the presence of DoS attacks, although the agents have the communication ability, data availability is violated. Suppose that the attacker in Fig. 2 can attack the communication network in a varying active period. Next, it needs to terminate attack activities and shift to a sleep period to supply its energy for next attacks. Assume that there exists an $m \in \mathbb{N}$ and denote $\{\tilde{t}_m\}_{m\in\mathbb{N}}$ as an attack sequence when a DoS attack is lunched at $\tilde{t}_m$. For a length $\tilde{\Delta}_m > 0$, the mth DoS time-interval is $\mathcal{A}_m = [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m)$ with $\tilde{t}_{m+1} > \tilde{t}_m + \tilde{\Delta}_m$ for all $m \in \mathbb{N}$. Thus, for given $t \geq \tau \in \mathbb{R}$, the sets of time instants where communication is denied are described in the following form [18]

$$\Xi_a(\tau, t) = \cup \mathcal{A}_m \cap [\tau, t], \quad m \in \mathbb{N} \tag{4}$$

which implies that on the interval $[\tau, t]$, the sets of time instants where communication is allowed are $\Xi_s(\tau, t) = [\tau, t] \setminus \Xi_a(\tau, t)$. In words, $|\Xi_a(\tau, t)|$ and $|\Xi_s(\tau, t)|$ represent the total lengths of the attacker being active and sleeping over $[\tau, t]$, respectively.

Suppose that there exists a $k_i \in \mathbb{N}$, and let $\{t^i_{k_i}\}_{k_i\in\mathbb{N}}$ be an update sequence to be determined, which has a finite sampling rate. To illustrate this two aperiodic time sequences $\{t^i_{k_i}\}_{k_i\in\mathbb{N}}$ and $\{\tilde{t}_m\}_{m\in\mathbb{N}}$, a sketch map is presented in Fig. 3.

D. Control Objective

In this section, two secure consensus problems are defined.

Problem 1 (Secure Leaderless Consensus Problem): Given the system (2) and a graph $\mathcal{G}$, a distributed event-triggered secure controller $u_i(t)$ is said to solve a secure leaderless consensus problem for multiagent systems (2) under DoS attacks described in Section II-C, if there exist a scalar $\kappa > 0$ and a decay rate $\rho > 0$ such that for $\forall i, j \in \mathcal{V}$

$$\|x_i(t) - x_j(t)\|^2 \leq \kappa e^{-\rho(t-t_0)}, \quad \forall t > t_0. \tag{5}$$

There is another consensus problem named leader-following consensus where the solution of each subsystem is required to approach some signal, i.e., the leader state $x_0(t)$ generated by

$$\dot{x}_0(t) = Ax_0(t). \tag{6}$$

Associated with systems (2) and (6), we define another graph $\tilde{\mathcal{G}} = (\tilde{\mathcal{V}}, \tilde{\mathcal{E}})$, where $\tilde{\mathcal{V}} = \{0, 1, \ldots, N\}$ and $(i, j) \in \tilde{\mathcal{E}}$. Clearly, $\mathcal{G}$ is a subgraph of $\tilde{\mathcal{G}}$ and can be obtained by removing the node 0 from $\tilde{\mathcal{V}}$ and all the edges on the node 0 from $\tilde{\mathcal{E}}$. $\mathcal{N}_i(\tilde{\mathcal{G}})$ denotes the new neighborhood set of node $i \in \tilde{\mathcal{V}}$.

Problem 2 (Secure Leader-Following Consensus Problem): Given the follower system (2) and leader system (6), and a graph $\tilde{\mathcal{G}}$, a distributed event-triggered secure controller $u_i(t)$ is said to solve a secure leader-following consensus problem for multiagent systems (2) and (6) under DoS attacks, if there exist a scalar $\tilde{\kappa} > 0$ and a decay rate $\tilde{\rho} > 0$ such that for $\forall i \in \mathcal{V}, t > t_0$

$$\|x_i(t) - x_0(t)\|^2 \leq \tilde{\kappa} e^{-\tilde{\rho}(t-t_0)} \|x_i(t_0) - x_0(t_0)\|^2. \tag{7}$$

III. Event-Triggered Secure Leaderless Consensus Under DoS Attacks

A. Distributed Event-Triggered Controller Design

Define $t_0 = t^i_0, t^i_1, \ldots, t^i_{k_i}, \ldots$ as the sequence of event time for each agent i. For $t \in [t^i_{k_i}, t^i_{k_i+1})$, a distributed control law for systems (2) under the DoS attacks can be designed as

$$u_i(t) = K\hat{\xi}_i(t), \quad \hat{\xi}_i(t) = \sum_{j\in\mathcal{N}_i(\mathcal{G})} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t)) \tag{8}$$

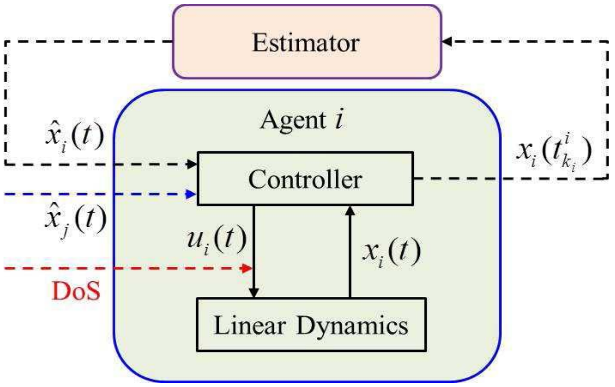


Fig. 4. Event-based secure control setup with an estimator.

where $\hat{x}_i(t) = x_i(t^i_{k_i(t)})$ is the latest broadcast state of agent i and $\hat{\xi}_i(t)$ only requires the estimates of agent i, e.g., $\hat{x}_i(t)$ and $\hat{x}_j(t)$ rather than using the true state $x_j(t)$ as required in [25] and [26]. The subscript $k_i(t)$ as described in [34] denotes the last successful update: $k_i(t) = -1$, if $\Xi_s(0,t) = \emptyset$, otherwise $k_i(t) = \sup\{k_i \in \mathbb{N} | t^i_{k_i} \in \Xi_s(0,t)\}$, where $\{t^i_{k_i}\}$ is the control sequence in Fig. 3, and we assume $k_i(0) = -1$ and when $\tilde{t}_0 = 0$, $u_i(0) = 0$ with $\hat{\xi}_i(t^i_{-1}) = 0$ for notational consistency.

In the distributed controller (8), the estimate $\hat{x}_j(t)$ is obtained by the following state estimator:

$$\dot{\hat{x}}_j(t) = A\hat{x}_j(t), \quad t^j_{k_j} \le t < t^j_{k_j+1} \tag{9}$$

$$\hat{x}_j\left(t^j_{k_j}\right) = x_j\left(t^j_{k_j}\right), \quad j \in \mathcal{N}_i(\mathcal{G}), \quad k_j \in \mathbb{N} \tag{10}$$

where $\hat{x}_j(t)$ evolves along its dynamics during $[t^j_{k_j}, t^j_{k_j+1})$ and is updated by x_j communicated from the neighboring agent j at $t^j_{k_j}$. For agent i, the state estimate $\hat{x}_i(t)$ is updated continuously in terms of (9) and discretely at $t^j_{k_j}$. It can be seen that $x_i(t^i_{k_i})$ is, thus, converted into the continuous-time signal $\hat{x}_i(t)$ until the next event occurs. Fig. 4 shows this event-based secure control setup with an estimator under DoS attacks.

Each agent needs to obtain $\hat{\xi}_i(t)$ for generating the control input in (8). To specify the event time instants, the following denotes a measurement error variable:

$$e_i(t) = \hat{x}_i(t) - x_i(t). \tag{11}$$

It is desired to employ the distributed control law that can make $e_i(t)$ in the following expression:

$$\|e_i(t)\| \le \beta_i \|\hat{\xi}_i(t)\|, \quad 0 < \beta_i < 1, \ i = 1, \ldots, N \tag{12}$$

which implies that the update rule is triggered by measuring the state $\hat{\xi}_i(t)$ and triggering a control when $\|e_i(t)\| = \beta_i \|\hat{\xi}_i(t)\|$.

Remark 1: Note that the control update relies on the successful information transmission over the network. When the network is not subject to DoS attacks, the control law is updated along (8)–(10) with the event condition in (12). When the network suffers from DoS attacks, unlike [24]–[29], the controller design and analysis fail since certain control update attempts are not successful. Thus, failing to reset $e_i(t)$ may cause (12) to be violated and consensus may be lost. In such a case, the information transmission is unsuccessful and then, all the agents do not update their protocols. That is, when an agent attempts to communicate and communication is denied by the DoS attack, the control signal is set to zero until the next successful transmission.

Remark 2: In (9) and (10), an open-loop estimation scheme is provided to ensure secure leaderless consensus. Advantages of this scheme are twofold: a) continuous communication is not required to verify the event-triggering condition; b) the system matrix A is allowed to be unstable due to the use of model-based estimates. Furthermore, if the linear agent dynamics degenerate to the single and/or double integrators, those particular cases using the zero-order-hold event-triggered scheme in [22]–[26] can be covered by the proposed framework.

Inspired by Fan *et al.* [25], [26], to guarantee that no agents in the group will exhibit Zeno behavior, a hybrid triggering approach is proposed to determine the event time instants for agent i

$$t^i_{k_i+1} = \begin{cases} t^i_{k_i} + \vartheta_i, & \text{if } k_i \in \mathcal{F} \\ t^i_{k_i} + \Delta^i_{k_i}, & \text{otherwise} \end{cases} \tag{13}$$

where ϑ_i is a positive constant,[1] and $\mathcal{F}$ denotes the set of integers related to a control update attempt occurring in the presence of the DoS attacks for any $\mathcal{A}_m$ defined in (4)

$$\mathcal{F} := \left\{(i, k_i) \in \mathcal{V} \times \mathbb{N} \,\middle|\, t^i_{k_i} \in \cup_{m\in\mathbb{N}} \mathcal{A}_m\right\} \tag{14}$$

and $\Delta^i_{k_i} = \max\{\tau^i_{k_i}, \ b_i\}$ is the interexecution interval, b_i is a positive scalar to be determined, and $\tau^i_{k_i}$ is denoted as

$$\tau^i_{k_i} = \inf_{t > t^i_{k_i}} \left\{t - t^i_{k_i} | \|e_i(t)\| = \beta_i \|\hat{\xi}_i(t)\|\right\}. \tag{15}$$

Remark 3: β_i is a weighting parameter that has a tradeoff between the convergence rate and the size of interevent interval. According to practical needs, an appropriate design parameter β_i can be selected to achieve the tradeoff. For example, if the parameter is smaller, the convergence is faster while frequent communication is required. Otherwise, the convergence is slower but less frequent communication is needed. Regarding this tradeoff, how to select an optimal β_i would be an interesting problem. We will consider this in the future work, and an optimization algorithm will be proposed to guide the selection of β_i.

B. DoS Attack Frequency and Attack Duration

Definition 1 (Attack Frequency): For any $T_2 > T_1 \ge t_0$, let $N_a(T_1, T_2)$ denote the number of DoS attacks occurring over $[T_1, T_2)$. Thus, $F_a(T_1, T_2) = (N_a(T_1, T_2))/(T_2 - T_1)$ is defined as the attack frequency over $[T_1, T_2)$ for all $T_2 > T_1 \ge t_0$.

Definition 2 (Attack Duration): For any $T_2 > T_1 \ge t_0$, denote $T_a(T_1, T_2)$ as the total time interval for systems under

[1] From (13), the best choice of ϑ_i relies on the exact information of DoS attacks. To facilitate the subsequent analysis, *a priori* positive constant ϑ_i is firstly selected.

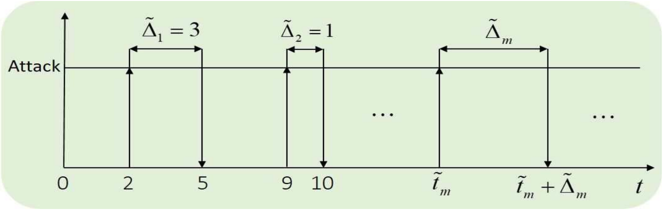


Fig. 5. Illustration of DoS attack signal. The attack occurs at 2, 9, and t_m s with the durations being 3, 1, and $\tilde{\Delta}_m$ s, respectively.

DoS attacks during $[T_1, T_2)$. The attack duration over $[T_1, T_2)$ is defined as: there exists scalars $T_0 \geq 0$ and $\tau_a > 1$ such that $T_a(T_1, T_2) \leq T_0 + (T_2 - T_1)/\tau_a$.

Remark 4: As mentioned in [30]–[34] for multiagent systems under DoS attacks, Definitions 1 and 2 are first given in [30] to specify a class of DoS attack signals in terms of their frequency and duration. Similar definitions are also used in [33]. As illustrated in Fig. 5, the DoS attack can occur at the random instant $\tilde{t}_m$ with the DoS duration $\tilde{\Delta}_m$ being the length of intervals over which communication is interrupted. The malicious DoS attack is allowed to occur aperiodically, sporadically, or intermittently. In Definition 2, $\tau_a > 1$ provides a measure of the fraction of time under the DoS attacks. The quantity $T_0 \geq 0$ is required to render $T_a(T_1, T_2) \leq T_0 + (T_2 - T_1)/\tau_a$ self-consistent. Thus, Definition 2 can provide the quantity of attacks.

Remark 5: In this paper, all the communication channels can be covered by malicious DoS attacks. In particular, the attacker can launch the attacks to interrupt several or all the communication transmissions in each time interval. In the future work, the multiple DoS attacks will be studied, one for each communication channel.

C. Stability Analysis of Secure Leaderless Consensus

Assumption 1: The undirected graph $\mathcal{G}$ is connected.

Denote the collective vectors $e(t) = \text{col}(e_1(t), \ldots, e_N(t))$, $x(t) = \text{col}(x_1(t), \ldots, x_N(t))$, and $\hat{x}(t) = \text{col}(\hat{x}_1(t), \ldots, \hat{x}_N(t)) \in \mathbb{R}^{nN}$. From the definitions of $u_i(t)$ and $e_i(t)$, it has

$$\dot{x}(t) = [I_N \otimes A - (\mathcal{L} \otimes BK)]x(t) - (\mathcal{L} \otimes BK)e(t). \quad (16)$$

Denote the state average of agents as: $\bar{x}(t) = \frac{1}{N}\sum_{i=1}^{N} x_i(t)$. Defining a disagreement vector $\delta_i(t) = x_i(t) - \bar{x}(t)$ gives

$$\delta(t) = \left[\left(I_N - \frac{1_N 1_N^T}{N}\right) \otimes I_n\right] x(t) = (\mathcal{M} \otimes I_n)x(t). \quad (17)$$

Under Assumption 1, $\mathcal{L}$ is symmetric and positive semidefinite [1]. By the definition of $\delta(t)$, it is easy to see that $(1_N^T \otimes I_n)\delta(t) = 0$. Thus, there always exists an orthogonal matrix $\Psi = [1_N/\sqrt{N}, \Phi] \in \mathbb{R}^{N\times N}$, where $\Phi = (\phi_2, \ldots, \phi_N) \in \mathbb{R}^{N\times(N-1)}$ and $\phi_i \in \mathbb{R}^N$, $i = 2, \ldots, N$, is an orthogonal eigenvector of $\mathcal{L}$ associated with eigenvalue $\lambda_i(\mathcal{L})$, i.e., $\phi_i^T \mathcal{L} = \lambda_i(\mathcal{L})\phi_i^T$. Thus, it has the following properties [36]:

$$\Psi^T\Psi = I_N, \quad \Phi\Phi^T = \mathcal{M} = I_N - (1_N 1_N^T)/N$$
$$\mathcal{L}\mathcal{M} = \mathcal{M}\mathcal{L} = \mathcal{L}, \quad \Psi^T\mathcal{L}\Psi = \text{diag}\{0, \lambda_i(\mathcal{L})\}. \quad (18)$$

Based on (16) and (18), the time derivative of δ is given by

$$\dot{\delta}(t) = [I_N \otimes A - (\mathcal{L} \otimes BK)]\delta(t) - (\mathcal{L} \otimes BK)e(t). \quad (19)$$

For clarity in the subsequent stability analysis, define $\mathfrak{B} = (1/c_1)\ln((c_1/c_2)\sqrt{c}+1)$ where $c = 2\gamma_2\lambda_N^2(\mathcal{L})/(N(1-s_{\max}))$, $\gamma_2 > 0$, $s_{\max} = \max_{i\in\mathcal{V}} s_i < \lambda_{\min}^2(Q)/(4k_0^2\lambda_N^2(\mathcal{L}) + \lambda_{\min}^2(Q))$, $k_0 = \|PBK\|$, and $c_1 = 2\|A\| + c_2$, $c_2 = \lambda_N(\mathcal{L})\|BK\|(1 + \sqrt{Nc})$. Here, $P > 0$ is the solution to algebraic Riccati equation (ARE): $PA + A^TP - PBR^{-1}B^TP + Q = 0$ where $Q > 0$ and $R > 0$ are two design positive definite matrices [37].

Next, the main result is presented as follows.

Theorem 3: Consider a group of N agents in (2), and suppose that Assumption 1 holds. Let γ_1, $\gamma_2 > 0$ satisfy $\gamma_1 + \gamma_2 = \gamma < 1$. If $\beta_i^2 = (s_i/(2\lambda_N^2(\mathcal{L}))) \leq \gamma_1$, $s_i \in (0, 1)$, and b_i in (13) is strictly positive with $b_i \leq \mathfrak{B}$, then under the proposed distributed controller (8) with $K = \tau R^{-1}B^TP$ and $\tau \geq (2\lambda_2(\mathcal{L}))^{-1}$, the agent group will achieve secure leaderless consensus, provided that

1) There exists a constant $\eta_1^* \in (0, \alpha_1)$ such that the *attack frequency* $F_a(t_0, t)$ in Definition 1 satisfies

$$F_a(t_0, t) = \frac{N_a(t_0, t)}{t - t_0} \leq \frac{\eta_1^*}{\ln(\mu) + (\alpha_1 + \alpha_2)\Delta_*}. \quad (20)$$

2) There exists a positive constant τ_a in the *attack duration Definition 2* for an arbitrary constant $T_0 \geq 0$ so that

$$\tau_a > (\alpha_1 + \alpha_2)/(\alpha_1 + \eta_1^*) \quad (21)$$

where $\alpha_1 = (\lambda_{\min}(Q)/2 - (2k_0^2\lambda_N^2(\mathcal{L})s_{\max})/(\lambda_{\min}(Q)(1 - s_{\max})))/\lambda_{\max}(P) > 0$, $\alpha_2 > \alpha_1 > 0$ such that for a matrix $S > 0, SA + A^TS - \alpha_2 S < 0$, $\mu = \max\{\lambda_{\max}(P)/\lambda_{\min}(S), \lambda_{\max}(S)/\lambda_{\min}(P)\}$, and the parameter Δ_* satisfies: $\sup_{(i,k_i)\in\mathcal{F}} \Delta_{tk_i}^i \leq \Delta_*$, where $\Delta_{tk_i}^i = t_{k_i+1}^i - t_{k_i}^i$ and $\mathcal{F}$ is given in (14).

The event detection time instants are determined by (13), and no agent will exhibit Zeno behavior.

Proof: See Appendix A. ■

Remark 6: In Theorem 3, sufficient conditions on parameters γ_1, γ_2, s_i, b_i, and β_i are provided to ensure the stability of the system and avoid Zeno behavior. As stated in Remark 3, there exists a tradeoff between the convergence speed and the size of interevent interval for selecting these interlinked parameters. Similarly, an optimization algorithm will be considered in the future work to guide the selection of these parameters. In addition, the effect of P (i.e., the solution to ARE) to the attack frequency and attack duration is summarized as follows. From (20), if $\lambda_{\max}(P)$ decreases or $\lambda_{\min}(P)$ increases, then the upper bound of the attack frequency $F_a(t_0, t)$ increases; if $\lambda_{\max}(P)$ increases or $\lambda_{\min}(P)$ decreases, then this upper bound decreases. Furthermore, by (21) and Definition 2, if $\lambda_{\max}(P)$ decreases, then the upper bound of the attack duration $T_a(t_0, t)$ increases; if $\lambda_{\max}(P)$ increases, then this upper bound decreases.

IV. Event-Triggered Secure Leader-Following Consensus Under DoS Attacks

For the defined leader-following graph $\tilde{\mathcal{G}}$, its Laplacian matrix is $\tilde{\mathcal{L}} = \begin{pmatrix} 0_{1\times 1} & 0_{1\times N} \\ -\mathcal{B}1_N & \mathcal{L}+\mathcal{B} \end{pmatrix}$, where $\mathcal{B}$ is a nonnegative diagonal matrix whose ith diagonal element is a_{i0}, where $a_{i0} > 0$ if $(0, i) \in \tilde{\mathcal{E}}$ and $a_{i0} = 0$ if otherwise. Define an information exchange matrix $\mathcal{H} = \mathcal{L} + \mathcal{B}$. Then, $\mathcal{H}$ is not necessarily symmetric and positive definite for a directed graph. In such a case, if we choose a Lyapunov function $\delta^T \mathcal{H} \delta$, the term $-\delta^T \mathcal{H} \delta$ will appear in its derivative. Therefore, a distributed event-triggered control scheme is required to solve the secure leader-following consensus problem under a directed communication topology.

Assumption 2: The digraph $\tilde{\mathcal{G}}$ contains a directed spanning tree with the leader as the root node.

Lemma 1 [3]: Under Assumption 2, $\mathcal{H}$ is nonsingular and all the eigenvalues of $\mathcal{H}$ have positive real parts.

Lemma 2 [6]: Under Assumption 2 and Lemma 1, there exists a positive diagonal matrix Ω such that $\Omega = \Theta\mathcal{H} + \mathcal{H}^T\Theta > 0$. One such Θ is given by $\mathrm{diag}\{\theta_1^{-1}, \theta_2^{-1}, \ldots, \theta_N^{-1}\}$ where $\theta = [\theta_1^{-1}, \theta_2^{-1}, \ldots, \theta_N^{-1}]^T = (\mathcal{H}^T)^{-1}1_N$ is a positive vector.

A. Distributed Event-Triggered Controller Design

Like Section III, a distributed event-triggered controller for the leader-following multiagent systems (2) and (6) is designed as

$$u_i(t) = \tilde{K}\Big(\sum_{j=1}^{N} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t)) + a_{i0}(x_0(t) - \hat{x}_i(t))\Big) \quad (22)$$

where $\tilde{K}$ is the control gain matrix, $x_0(t)$ is the leader's state in (6), and $\hat{x}_i(t)$, $\hat{x}_j(t)$ are designed by (9) and (10).

Remark 7: In (22), the true state $x_0(t)$ is available to only a small group of followers as widely used in the existing literature (see [28], [29] for just an example). This is due to the leader without having any control inputs. The leader moves freely and does not receive any information from the followers. Therefore, the communication failures induced by DoS attacks do not affect the leader's behavior. This is also why the leader does not have its control protocol under DoS attacks.

By $e_i(t)$ in (11) and for $0 < \tilde{\beta}_i < 1$, it is desired to employ the control update rule that can make $e_i(t)$ satisfy

$$\|e_i(t)\| \le \tilde{\beta}_i \|\hat{z}_i(t)\|, \quad \hat{z}_i(t) = \sum_{j\in\mathcal{N}_i(\tilde{\mathcal{G}})} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t)). \quad (23)$$

The following scheme is proposed to avoid Zeno behavior and determine the event time instants for each agent i:

$$t_{k_i+1}^i = \begin{cases} t_{k_i}^i + \tilde{\vartheta}_i, & \text{if } k_i \in \mathcal{F} \\ t_{k_i}^i + \tilde{\Delta}_{k_i}^i, & \text{otherwise} \end{cases} \quad (24)$$

where $\tilde{\vartheta}_i > 0$, $\tilde{\Delta}_{k_i}^i = \max\{\tilde{\tau}_{k_i}^i, \tilde{b}_i\}$ is the interexecution interval, $\tilde{b}_i$ is a strictly positive real number to be subsequently determined, and $\tilde{\tau}_{k_i}^i$ is determined as

$$\tilde{\tau}_{k_i}^i = \inf_{t > t_{k_i}^i} \{t - t_{k_i}^i \,|\, \|e_i(t)\| = \tilde{\beta}_i \|\hat{z}_i(t)\|\}. \quad (25)$$

B. Stability Analysis of Secure Leader-Following Consensus

Define the state tracking error between the followers and the leader as $\eta_i(t) = x_i(t) - x_0(t)$. Let $\eta(t) = \mathrm{col}(\eta_1, \ldots, \eta_N)$. From the definitions of $u_i(t)$ and $\eta_i(t)$, the dynamics of the agent group can be written in a compact form

$$\dot{\eta}(t) = [I_N \otimes A - (\mathcal{H} \otimes B\tilde{K})]\eta(t) - (\mathcal{H} \otimes B\tilde{K})e(t). \quad (26)$$

For clarity in the subsequent stability analysis, define $\tilde{\mathfrak{B}} = \frac{1}{\tilde{c}_1}\ln((\tilde{c}_1\sqrt{\tilde{\gamma}_2/N})/\tilde{c}_2 + 1)$ where $\tilde{c}_1 = 2\|A\|$ and $\tilde{c}_2 = 2\sqrt{\tilde{\gamma}_2}\|\mathcal{H} \otimes BK\| + \|BK\|$, $\tilde{\gamma}_2 > 0$. Let $\tilde{k}_2 = k_{\min}^2 \sigma_{\min}(\tilde{\mathcal{H}}^T\tilde{\mathcal{H}})$, $\tilde{k}_3 = \sigma_{\max}(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K}) - k_{\min}^2$, $\tilde{k}_4 = \sigma_{\max}(\tilde{\mathcal{H}}^T\Theta\mathcal{H} \otimes \tilde{P}B\tilde{K} - k_{\min}^2\tilde{\mathcal{H}}^T)$, $\tilde{\mathcal{H}} = \mathcal{H}^{-1} \otimes I_n$, and $k_{\min} = \lambda_{\min}(\Theta \otimes \tilde{Q}) = k_{\min}^1 + k_{\min}^2$ where $k_{\min}^1 > 0$ and $0 < k_{\min}^2 < \lambda_{\min}(\Omega/2)$. Here, $\tilde{P} > 0$ is the solution to the ARE: $\tilde{P}A + A^T\tilde{P} - \tilde{P}B\tilde{R}^{-1}B^T\tilde{P} + \tilde{Q} = 0$ for two design matrices $\tilde{Q} > 0$ and $\tilde{R} > 0$ [37].

Theorem 4: Consider a group of N agents in (2) and (6), and suppose that Assumption 2 holds. Let $\tilde{\gamma}_1$, $\tilde{\gamma}_2 > 0$ satisfy $\tilde{\gamma}_1 + \tilde{\gamma}_2 = \tilde{\gamma} < 1$. If $\tilde{\beta}_i^2 = \tilde{s}_i(\tilde{k}_2 - \frac{\tilde{k}_4}{\tilde{\varrho}})/(\tilde{k}_3 + \tilde{k}_4\tilde{\varrho}) \le \tilde{\gamma}_1$, $\tilde{s}_i \in (0, 1)$, $\tilde{\varrho} > \tilde{k}_4/\tilde{k}_2 > 0$, and $\tilde{b}_i$ in (24) is strictly positive with $b_i \le \tilde{\mathfrak{B}}$, then under the proposed controller (22) with $\tilde{K} = \tilde{\tau}\tilde{R}^{-1}B^T\tilde{P}$, $\tilde{\tau} \ge \lambda_{\min}^{-1}(\Omega)\theta_{\min}^{-1}$, $\theta_{\min} = \min \theta_i^{-1}, i \in \mathcal{V}$, secure leader-following consensus can be achieved, provided that

1) There exists a constant $\tilde{\eta}_1^* \in (0, \tilde{\alpha}_1)$ such that the *attack frequency* $F_a(t_0, t)$ in Definition 1 satisfies

$$F_a(t_0, t) = \frac{N_a(t_0, t)}{t - t_0} \le \frac{\tilde{\eta}_1^*}{\ln(\tilde{\mu}) + (\tilde{\alpha}_1 + \tilde{\alpha}_2)\tilde{\Delta}_*}. \quad (27)$$

2) There exists a positive constant τ_a in the *attack duration* Definition 2 so that

$$\tau_a > (\tilde{\alpha}_1 + \tilde{\alpha}_2)/(\tilde{\alpha}_1 + \tilde{\eta}_1^*) \quad (28)$$

where $\tilde{\alpha}_1 = k_{\min}^1 \lambda_{\max}^{-1}(\Theta \otimes \tilde{P}) > 0$, $\tilde{\alpha}_2 > \tilde{\alpha}_1 > 0$ such that for $\tilde{S} > 0$, $\tilde{S}A + A^T\tilde{S} - \tilde{\alpha}_2\tilde{S} < 0$, $\tilde{\mu} = \max\{\lambda_{\max}(\tilde{P})/\lambda_{\min}(\tilde{S}),\ \lambda_{\max}(\tilde{S})/\lambda_{\min}(\tilde{P})\}$, and $\sup_{(i,k_i)\in\mathcal{F}} \Delta_{tk_i}^i \le \tilde{\Delta}_*$.

The event detection time instants are determined by (24), and no agent will exhibit Zeno behavior.

Proof: See Appendix B. ■

Remark 8: Theorems 3 and 4 showed that secure leaderless and leader-following consensus can be achieved exponentially under Assumptions 1 and 2, respectively. Note that if the digraph $\tilde{\mathcal{G}}$ in Assumption 2 is reduced to $\mathcal{G}$ containing a directed spanning tree for the leaderless case, the design can be extended by constructing a nonnegative left eigenvector $\xi = [\xi_1, \ldots, \xi_N]^T$ satisfying $\sum_{i=1}^N \xi_i = 1$ [36]. Due to the space limit, the digraph case for leaderless consensus is not included in this paper.

When the leader-following multiagent system is not subject to any DoS attacks, then we have the following result.

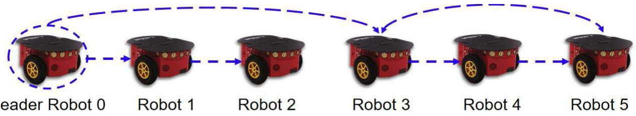


Fig. 6. Communication graph of the multirobot system.

Corollary 1: Consider a group of N agents with dynamics in (2) and (6). Suppose that Assumption 2 holds, and the parameters $\tilde{\gamma}_1$, $\tilde{\gamma}_2$, $\tilde{\varrho}$, $\tilde{\beta}_i$, $\tilde{s}_i$, $\tilde{b}_i$, $\tilde{k}_j$, $i = 1, 2, \ldots, N$, $j = 1, 2, 3, 4$, and $\tilde{R} > 0$, $\tilde{Q} > 0$ are given in Theorem 4. Then, the proposed controller (22) with the following event times for $\tilde{\Delta}^i_{k_i} = \max\{\tilde{\tau}^i_{k_i}, \tilde{b}_i\}$:

$$t^i_{k_i+1} = t^i_{k_i} + \tilde{\Delta}^i_{k_i}, \tilde{\tau}^i_{k_i} = \inf_{t>t^i_{k_i}} \{t - t^i_{k_i} | \|e_i(t)\| = \tilde{\beta}_i \|\hat{z}_i(t)\|\} \tag{29}$$

enables the agent group to achieve leader-following consensus.

Proof: It is similar to the proof of Theorem 4 by removing Steps 1 and 3. ∎

Remark 9: Corollary 1 covers the results in [27]–[29] for the general linear multiagent systems in the absence of DoS attacks. Furthermore, if the system considered in this paper degenerates to a special case with $A = 0$ or $A = [0, 1; 0, 0]$, the control scheme will be similar to those in [23]–[26]. Thus, the proposed control scheme can potentially have a wide range of applications.

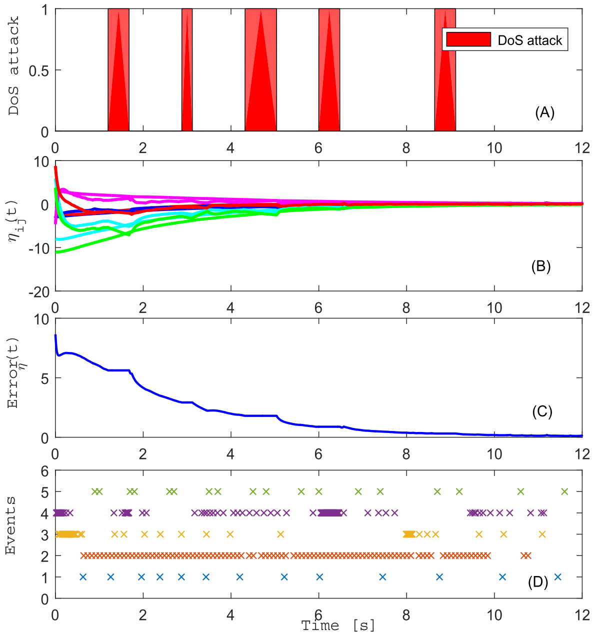


Fig. 7. Simulation results for secure leader-following consensus in the presence of DoS attacks. (A) Sustained DoS attack with varying period and duty cycle, generated randomly. Vertical red stripes: time intervals over which a DoS attack is active and it has an average duty cycle of 20%. (B) Consensus tracking states $\eta_{ij}(t)$, $i = 0, 1, \ldots, 5$, $j = 1, 2$. (C) Tracking errors $\text{Error}_\eta(t)$. (D) Occurrences of the events for all the robots.

V. Numerical Simulation

A. Distributed Multirobot Coordination

1) Multirobot Simulation Setup and Conditions: In this example, a multirobot system simulation program is developed to validate the effectiveness of the proposed event-based distributed control designs. The following control task is tested in the simulation: keep all the six robots in a line and achieve the consensus on their position and velocity, respectively. The dynamics of a group of six robots are given by (2) with $A = [0, -0.5; 0.5, 0]$ and $B = [0; 1]$. The eigenvalues of the matrix A are: $0 \pm 0.5i$ ($i = \sqrt{-1}$). One can easily verify that the matrix pair (A, B) is controllable.

2) Secure Leader-Following Consensus: The directed communication topology is shown in Fig. 6. By Theorem 4, we can obtain $\tilde{K} = [-3.9957, 6.9208]$, $\tilde{\alpha}_1 = 0.48$, and $\tilde{\alpha}_2 = 1.02$. Choose $\tilde{\beta}_i = 0.2$. The simulation results are provided in Fig. 7 by the controller (8) with (9) and (10). The DoS attack signal is simulated in Fig. 7(A) with $\tau_a = 3s$. Based on (27) and (28), the two conditions are satisfied with $F_a(t_0, t) = (N_a(t_0, t))/(t - t_0) \leq 0.01$ and $\tau_a > (\tilde{\alpha}_1 + \tilde{\alpha}_2)/(\tilde{\alpha}_1 + \eta^*_1) = 2$. That is, the attack cannot occur more than 0.01 times during a unit of time. Fig. 7(B) shows the consensus tracking states $\eta_{ij}(t), i = 0, 1, \ldots, 5$, $j = 1, 2$, and Fig. 7(C) shows the consensus tracking errors: $\text{Error}_\eta(t) = 0.2(\sum_{i=1}^{5} \|x_i(t) - x_0(t)\|^2)^{1/2}$. Fig. 7(D) shows the events for each robot.

B. Distributed Voltage Regulation of Power Networks

A microgrid example is studied and the dynamics of distributed generators (DGs) are given in [39] where the voltage regulation is formulated as a leader-following consensus problem, i.e., all the DGs need to synchronize their voltage values to a common reference with: $\dot{y}_i(t) = Ay_i(t) + Bu_i(t)$, $\dot{y}_0(t) = Ay_0(t)$, where $y_i(t) = [v_{o,\text{magi}}, \dot{v}_{o,\text{magi}}]^T$, $y_0(t) = [v_{ref}, 0]^T$, $A = [0, 1; 0, 0]$ and $B = [0; 1]$. However, the cyberlayer of distributed secondary control in Fig. 8 is vulnerable to DoS attacks. The DoS attack model is described in Section II-C. The goal is to design distributed controller $u_i(t) = \tilde{K} \sum_{j \in \mathcal{N}_i(\tilde{\mathcal{G}})} a_{ij}(\hat{y}_j(t) - \hat{y}_i(t))$ with $\hat{y}_j(t)$ similarly defined in (9) and (10), so that $y_i(t) \rightarrow y_0(t)$.

1) Microgrid Simulation Setup and Conditions: The proposed distributed secondary controller is tested with a 220-V (per phase rms) 50-Hz islanded microgrid system. The single-line diagram is illustrated in Fig. 9 where the islanded microgrid is consisted of 4 DGs and the transmission lines between the buses are also shown. The parameters of the microgrid test system are given in [39], and the reference voltage is 1.05 p.u. Fig. 9 also shows the communication topology for distributed secondary voltage control and the reference voltage is available to DG 1 only, i.e., $a_{10} = 1$ and $a_{i0} = 0$, $i = 2, 3, 4$.

2) Secure Voltage Regulation: By Theorem 4, $\tilde{K} = [5.0, 8.6603]$, $\tilde{\alpha}_1 = 0.6$, and $\tilde{\alpha}_2 = 1.4$. As considered in [39], the microgrid is islanded from the main grid at $t = 0$s, while the distributed secondary control scheme is applied at $t = 2.5$s. Choose $\tilde{\beta}_i = 0.5$. Based on the design, the simulation results are provided in Fig. 10. The DoS attack signal is simulated in Fig. 10(A) with $\tau_a = 3.75$ s. Thus, (27) and (28) are satisfied with $F_a(t_0, t) \leq 0.02$ and $\tau_a > 2$. As seen from Fig. 10(B), the distributed secondary control can return the voltage values to the reference after 2.5s.

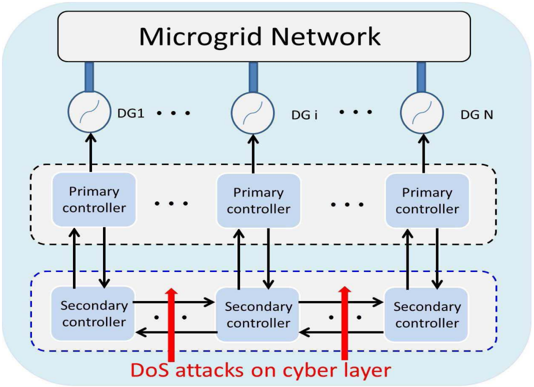


Fig. 8. Cooperative control of an islanded microgrid under DoS attacks.

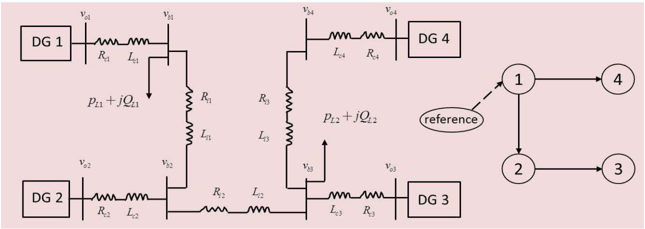


Fig. 9. Single-line diagram of a microgrid test system.

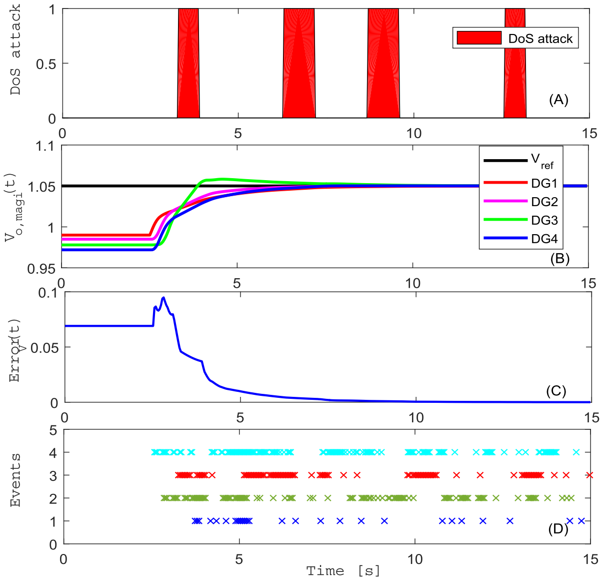


Fig. 10. Simulation results for distributed voltage regulation of microgrid in the presence of DoS attacks. (A) Sustained DoS attack with an average duty cycle of 20%. (B) State trajectory $V_{o,\mathrm{mag}i}(t)$, $i = 1, \ldots, 4$. (C) Voltage regulation error $\mathrm{Error}_V(t)$. (D) Occurrences of the events for all the DGs.

Fig. 10(C) shows the voltage regulation error $\mathrm{Error}_V(t) = 0.25(\sum_{i=1}^{4} \|y_i(t) - y_0(t)\|^2)^{1/2}$. Fig. 10(D) shows the events for each DG.

C. Distributed Cooperative Control of Unstable Dynamic Systems

Consider a group of agents with unstable linear dynamics [27]

$$A = \begin{bmatrix} 0.48 & 0.29 & -0.3 \\ 0.13 & 0.23 & 0 \\ 0 & -1.2 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 2 & 0 \\ -1.5 & 1 \\ 0 & 1 \end{bmatrix} \quad (30)$$

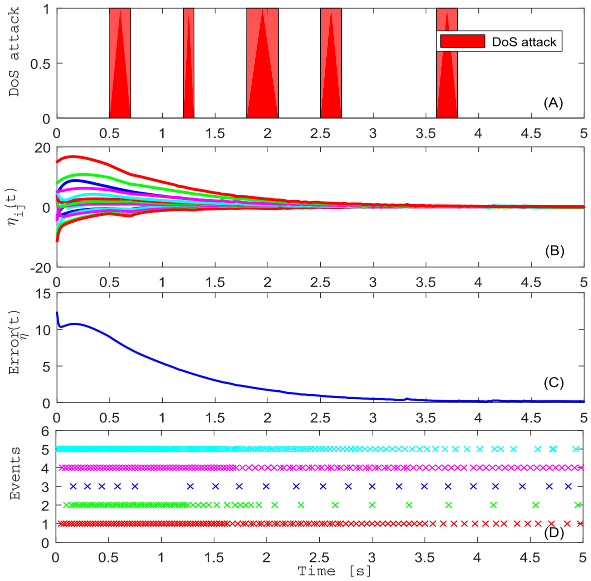


Fig. 11. Simulation results for secure leader-following consensus in the presence of DoS attacks. (A) Sustained DoS attack with varying period and duty cycle. (B) Consensus tracking states $\eta_{ij}(t), i = 0, 1, \ldots, 5, j = 1, 2, 3$. (C) Tracking errors $\mathrm{Error}_\eta(t)$. (D) Occurrences of the events for all the agents.

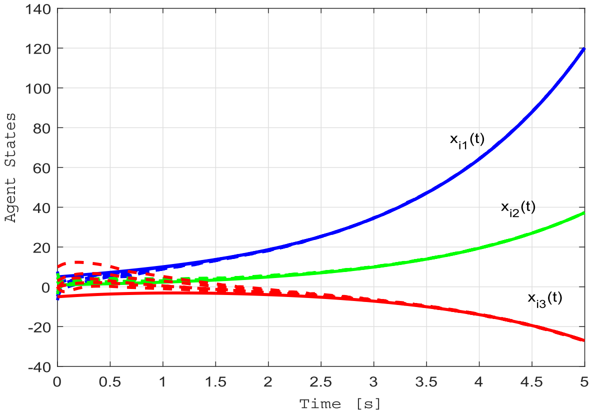


Fig. 12. State trajectories of all the followers and the leader.

where the eigenvalues of A are 0.6344, 0.048, and −0.9727. The directed communication topology is described in Fig. 6. According to Theorem 4, we have

$$\tilde{K} = \begin{bmatrix} 6.6252 & -3.9169 & 1.1142 \\ 9.8942 & 15.0607 & -2.0782 \end{bmatrix}. \quad (31)$$

The simulation results are presented in Figs. 11 and 12. Fig. 11 shows the simulated DoS attack signal, consensus tracking states, tracking errors, and triggered events, respectively. The state trajectories of all the six agents are shown in Fig. 12. It shows that each one of the three dimensions of the agents (in dashed lines) converge to a different time-varying trajectory (leader's state).

VI. Conclusion

In this paper, we investigated the distributed event-based secure coordination of general linear multiagent systems subject to DoS attacks. Distributed control schemes with event-based samplings are developed to achieve secure leaderless and leader-following consensus. It is proven that the agent team can achieve secure consensus exponentially, provided that the frequency and duration of DoS attacks satisfy certain conditions. Several case studies are provided to illustrate the effectiveness of the developed methods.

Appendix A
Proof of Theorem 1

A. Resilience Analysis

Step 1 (Two Intervals Classification): In this step, the intervals of time where (12) holds and does not hold are characterized. Consider the sequences $\{t^i_{k_i}\}_{k_i\in\mathbb{N}}$ and $\{\tilde{t}_m\}_{m\in\mathbb{N}}$. Due to the finite sampling rate, a time interval will necessarily elapse from the time $\tilde{t}_m+\tilde{\Delta}_m$, to the time at which the agents successfully sample and transmit. It can be upper bounded as: $\sup_{(i,k_i)\in\mathcal{F}}\Delta^i_{tk_i}\le\Delta_*$, where $\Delta^i_{tk_i}=t^i_{k_i+1}-t^i_{k_i}$ and $\mathcal{F}$ is given in (14). Hence, a DoS free interval of a length greater than Δ_* guarantees that the agents are able to sample and transmit. The mth time interval where (12) needs not to hold is

$$\mathfrak{A}_m=[\tilde{t}_m,\tilde{t}_m+\tilde{\Delta}_m+\Delta_*). \tag{32}$$

Thus, the time interval $[\tau,t)$ consists of the following two union of subintervals: $[\tau,t)=\tilde{\Xi}_s(\tau,t)\cup\tilde{\Xi}_a(\tau,t)$ with

$$\tilde{\Xi}_a(\tau,t):=\cup\,\mathfrak{A}_m\cap[\tau,t],\quad \tilde{\Xi}_s(\tau,t):=[\tau,t]\backslash\;\tilde{\Xi}_a(\tau,t). \tag{33}$$

Step 2 (Lyapunov Stability Analysis):

1) Consider the time interval $\tilde{\Xi}_s(\tau,t)$ over which (12) holds. Choose a Lyapunov function candidate as

$$V(t)=\delta^T(t)(I_N\otimes P)\delta(t). \tag{34}$$

Computing the time derivative of (34) yields

$$\dot{V}(t)=\delta^T(I_N\otimes(PA+A^TP))\delta-2\delta^T(\mathcal{L}\otimes PBK)(\delta+e).$$

Based on (18), defining $\tilde{\delta}=(\Psi^T\otimes I_n)\delta$ yields that $\tilde{\delta}_1=((1^T_N/N)\mathcal{M}\otimes I_n)x=0$. Since $\tau\ge(2\lambda_2(\mathcal{L}))^{-1}$, we obtain

$$\begin{aligned}&\delta^T[I_N\otimes(PA+A^TP)-2\tau(\mathcal{L}\otimes PBR^{-1}B^TP)]\delta\\&\qquad\le\sum_{i=2}^N\tilde{\delta}_i^T(PA+A^TP-PBR^{-1}B^TP)\tilde{\delta}_i.\end{aligned} \tag{35}$$

By using Young's inequality: $x^Ty\le(\varrho/2)x^Tx+(1/2\varrho)y^Ty$ for any $\varrho>0$ and any $x,y\in\mathbb{R}^{nN}$

$$-2\tau\delta^T(\mathcal{L}\otimes PBR^{-1}B^TP)e\le k_0\sum_{i=2}^N\left(\omega\varrho\tilde{\delta}_i^T\tilde{\delta}_i+\varrho^{-1}\tilde{e}_i^T\tilde{e}_i\right)$$

where $k_0=\|PBK\|$, $\omega=\lambda^2_N(\mathcal{L})$, and $\tilde{e}=(\Phi^T\otimes I_n)e$.

Since $PA+A^TP-PBR^{-1}B^TP+Q=0$, we have

$$\begin{aligned}\dot{V}(t)&\le-\lambda_{\min}(Q)\sum_{i=1}^N\delta_i^T\delta_i+k_0\sum_{i=2}^N\left(\omega\varrho\tilde{\delta}_i^T\tilde{\delta}_i+\frac{1}{\varrho}\tilde{e}_i^T\tilde{e}_i\right)\\&\le-\frac{\lambda_{\min}(Q)}{2}\sum_{i=1}^N\delta_i^T\delta_i+\frac{2k_0^2\lambda_N^2(\mathcal{L})}{\lambda_{\min}(Q)}\sum_{i=1}^Ne_i^Te_i\end{aligned} \tag{36}$$

where $\|\tilde{e}\|\le\|\Phi^T\otimes I_n\|\|e\|\le\|e\|$ is used with $\|\Phi^T\otimes I_n\|=1$.

Let $\hat{\xi}(t)=\mathrm{col}(\hat{\xi}_1,\ldots,\hat{\xi}_N)$ with $\hat{\xi}_i(t)=\sum_{j\in\mathcal{N}_i(\mathcal{G})}a_{ij}(\hat{x}_j(t)-\hat{x}_i(t))$ and $e_i(t)=\hat{x}_i(t)-x_i(t)$, we have

$$\begin{aligned}\|\hat{\xi}(t)\|&=\|-(\mathcal{L}\otimes I_n)(x+e)\|=\|\xi-(\mathcal{L}\otimes I_n)e\|\\&\le\|\xi\|+\|(\mathcal{L}\otimes I_n)e\|\le\|\xi\|+\lambda_N(\mathcal{L})\|e\|\end{aligned} \tag{37}$$

where $\xi_i(t)=\sum_{j\in\mathcal{N}_i(\mathcal{G})}a_{ij}(x_j(t)-x_i(t))$.

By (18), $\mathcal{L}^2\le\lambda^2_N(\mathcal{L})\mathcal{M}^2$ holds, which implies

$$\begin{aligned}\|\xi\|^2&=x^T(\mathcal{L}^T\otimes I_n)(\mathcal{L}\otimes I_n)x=x^T(\mathcal{L}^2\otimes I_n)x\\&\le\lambda^2_N(\mathcal{L})x^T(\mathcal{M}^2\otimes I_n)x=\lambda^2_N(\mathcal{L})\|\delta\|^2.\end{aligned} \tag{38}$$

Combining (37) with (38) yields $\|\hat{\xi}(t)\|\le\lambda_N(\mathcal{L})(\|\delta\|+\|e\|)$. Since $\|e_i(t)\|\le\beta_i\|\hat{\xi}_i\|$, it follows from $\beta_i^2=(s_i/(2\lambda^2_N(\mathcal{L})))$ that for $s_{\max}=\max_i s_i$, $\|e(t)\|^2\le s_{\max}\|\hat{\xi}\|^2/(2\lambda^2_N(\mathcal{L}))\le s_{\max}(\|\delta\|^2+\|e\|^2)$, which leads to $\|e(t)\|^2\le s_{\max}\|\delta\|^2/(1-s_{\max})$.

Choose $s_{\max}$ and α_1 in Theorem 1, then we have

$$\begin{aligned}\dot{V}(t)&\le-\left(\frac{\lambda_{\min}(Q)}{2}-\frac{2k_0^2\lambda_N^2(\mathcal{L})s_{\max}}{\lambda_{\min}(Q)(1-s_{\max})}\right)\sum_{i=1}^N\delta_i^T\delta_i\\&\le-\alpha_1\delta^T(t)(I_N\otimes P)\delta(t)=-\alpha_1V(t).\end{aligned} \tag{39}$$

2) Consider the time interval $\tilde{\Xi}_a(\tau,t)$ over which (12) does not necessarily hold. Choose a Lyapunov function candidate as

$$V(t)=\delta^T(t)(I_N\otimes S)\delta(t) \tag{40}$$

which yields that similar to [30]–[32], there exists a scale $\alpha_2>\alpha_1>0$ so that the time derivative of (40) can be described as

$$\dot{V}(t)=\delta^T[I_N\otimes(SA+A^TS)]\delta\le\alpha_2V(t) \tag{41}$$

where $SA+A^TS-\alpha_2S<0$ is used.

Denote $\sigma(t)\in\{a,b\}$ as a piecewise constant function. Thus, $V(t)=V_{\sigma(t)}(t)$, where V_a and V_b are defined in (34) and (40), respectively. Suppose that V_a is activated in $[\tilde{t}_{m-1}+\tilde{\Delta}_{m-1},\tilde{t}_m)$ and V_b is activated in $[\tilde{t}_m,\tilde{t}_m+\tilde{\Delta}_m+\Delta_*)$. Hence, by Comparison lemma [38, Lemma 3.4], it follows from (39) and (41) that

$$V(t)\le\begin{cases}e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})}V_a(\tilde{t}_{m-1}+\tilde{\Delta}_{m-1})\\e^{\alpha_2(t-\tilde{t}_m)}V_b(\tilde{t}_m).\end{cases} \tag{42}$$

Case I: If $t\in[\tilde{t}_{m-1}+\tilde{\Delta}_{m-1},\tilde{t}_m)$, it follows from (42) that

$$\begin{aligned}V(t)&\le e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})}V_a(\tilde{t}_{m-1}+\tilde{\Delta}_{m-1})\\&\le\mu e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})}V_b(\tilde{t}^-_{m-1}+\tilde{\Delta}^-_{m-1})\\&\le\mu e^{-\alpha_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})}[e^{\alpha_2(t-\tilde{t}_{m-2}-\tilde{\Delta}_{m-2})}\\&\qquad\times V_b(\tilde{t}_{m-2}+\tilde{\Delta}_{m-2})]\\&\le\cdots\\&\le\mu^me^{-\alpha_1|\tilde{\Xi}_s(t_0,t)|}e^{\alpha_2|\tilde{\Xi}_a(t_0,t)|}V_a(t_0).\end{aligned} \tag{43}$$

Case II: If $t\in[\tilde{t}_m,\tilde{t}_m+\tilde{\Delta}_m+\Delta_*)$, similarly

$$\begin{aligned}V(t)&\le e^{\alpha_2(t-\tilde{t}_m)}V_b(\tilde{t}_m)\le\mu e^{\alpha_2(t-\tilde{t}_m)}V_a(\tilde{t}^-_m)\\&\le\mu e^{\alpha_2(t-\tilde{t}_m)}[e^{-\alpha_1(\tilde{t}_m-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})}\\&\qquad\times V_a(\tilde{t}_{m-1}+\tilde{\Delta}_{m-1})]\\&\le\cdots\\&\le\mu^{m+1}e^{-\alpha_1|\tilde{\Xi}_s(t_0,t)|}e^{\alpha_2|\tilde{\Xi}_a(t_0,t)|}V_a(t_0).\end{aligned} \tag{44}$$

Step 3 (Bounds on DoS Attack Frequency and Duration): According to Definition 1, $N_a(t_0,t) = m$ for $t \in [\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}, \tilde{t}_m)$ and $N_a(t_0,t) = m+1$ for $t \in [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*)$. Thus, for $\forall t \geq t_0$, it follows from (43) and (44) that

$$V(t) \leq \mu^{N_a(t_0,t)} e^{-\alpha_1 |\tilde{\Xi}_s(t_0,t)|} e^{\alpha_2 |\tilde{\Xi}_a(t_0,t)|} V(t_0). \tag{45}$$

Note that for all $t \geq t_0$, $|\tilde{\Xi}_s(t_0,t)| = t - t_0 - |\tilde{\Xi}_a(t_0,t)|$ and $|\tilde{\Xi}_a(t_0,t)| \leq |\Xi_a(t_0,t)| + (1 + N_a(t_0,t))\Delta_*$, where $N_a(t_0,t)$ represents the number of DoS attacks. By Definition 2, it has

$$\begin{aligned} &-\alpha_1(t - t_0 - |\tilde{\Xi}_a(t_0,t)|) + \alpha_2 |\tilde{\Xi}_a(t_0,t)| \\ &\quad = -\alpha_1(t - t_0) + (\alpha_1 + \alpha_2)|\tilde{\Xi}_a(t_0,t)| \\ &\quad \leq -\alpha_1(t - t_0) + (\alpha_1 + \alpha_2)[T_0 + (t - t_0)/\tau_a \\ &\qquad + (1 + N_a(t_0,t))\Delta_*]. \end{aligned} \tag{46}$$

Substituting (46) into (45) yields

$$\begin{aligned} V(t) &\leq \mu^{N_a(t_0,t)} e^{-\alpha_1(t - t_0 - |\tilde{\Xi}_a(t_0,t)|)} e^{\alpha_2 |\tilde{\Xi}_a(t_0,t)|} V(t_0) \\ &\leq e^{(\alpha_1+\alpha_2)(T_0+\Delta_*)} e^{-\alpha_1(t-t_0)} e^{\frac{(\alpha_1+\alpha_2)}{\tau_a}(t-t_0)} \\ &\quad \times e^{[\ln(\mu) + (\alpha_1+\alpha_2)\Delta_*] N_a(t_0,t)} V(t_0). \end{aligned} \tag{47}$$

By (20) and (21), let $\eta_1 = \alpha_1 - (\alpha_1 + \alpha_2)/\tau_a - \eta_1^* > 0$ so that

$$V(t) \leq e^{(\alpha_1+\alpha_2)(T_0+\Delta_*)} e^{-\eta_1(t-t_0)} V(t_0). \tag{48}$$

B. Minimal Interevent Interval Computation

Motivated by Fan *et al.* [25], the agent interevent time at time t is specified by $\tau_{k_i}^i$ or b_i based on (13). Denote $W_1(t)$ and $W_2(t)$ as the agent sets where the latest agent interevent time is specified by $\tau_{k_i}^i$ and b_i, respectively. Then, $W_1(t) \cup W_2(t) = \{1, 2, \ldots, N\}$ and $W_1(t) \cap W_2(t) = \emptyset$. To ensure $\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|$ in (12), one can choose that for $\gamma_1 + \gamma_2 = \gamma\ < 1$

$$\sum_{i \in W_1(t)} \|e_i(t)\|^2 \leq \gamma_1 \sum_{i \in W_1(t)} \|\hat{\xi}_i(t)\|^2 \leq \gamma_1 \sum_{i=1}^{N} \|\hat{\xi}_i(t)\|^2 \tag{49}$$

$$\sum_{i \in W_2(t)} \|e_i(t)\|^2 \leq \gamma_2 \sum_{i \in W_2(t)} \|\hat{\xi}_i(t)\|^2 \leq \gamma_2 \sum_{i=1}^{N} \|\hat{\xi}_i(t)\|^2. \tag{50}$$

For the agents in $W_1(t)$, a sufficient condition for (49) is given by $\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|$ with $\beta_i^2 \leq \gamma_1$. Next, for the agents in $W_2(t)$, a sufficient condition for (50) is $\|e_i(t)\|^2 \leq \sum_{j=1}^{N} (\gamma_2/N)\beta_j^2 \|\hat{\xi}_j(t)\|^2 \leq (2\gamma_2 \lambda_N^2(\mathcal{L}))/(N(1 - s_{\max}))\|\delta(t)\|^2$. Let $c = (2\gamma_2 \lambda_N^2(\mathcal{L}))/(N(1 - s_{\max}))$. Then, $\|e_i(t)\|^2 \leq c\|\delta(t)\|^2$. If b_i denotes a lower bound for the evolution time of $\|e_i(t)\|/\|\delta(t)\|$ from 0 to $\sqrt{c}$, for the agents in $W_2(t)$, $t_{k_i+1}^i = t_{k_i}^i + b_i$ will be sufficient to ensure (50). To show the existence of a positive interexecution interval, one can estimate $\|e_i(t)\|/\|\delta(t)\|$ [24]–[26]

$$\begin{aligned} \frac{d}{dt}\frac{\|e_i(t)\|}{\|\delta(t)\|} &= \frac{e_i^T(t)\dot{e}_i(t)}{\|e_i(t)\|\|\delta(t)\|} - \frac{\|e_i(t)\|\delta^T(t)\dot{\delta}(t)}{\|\delta(t)\|^3} \\ &\leq \frac{\|\dot{e}_i(t)\|}{\|\delta(t)\|} + \frac{\|e_i(t)\|}{\|\delta(t)\|}\frac{\|\dot{\delta}(t)\|}{\|\delta(t)\|}. \end{aligned} \tag{51}$$

Since $\dot{e}_i(t) = Ae_i(t) - BK\sum_{j=1}^{N} l_{ij}(e_j(t) + x_j(t))$, it gets

$$\frac{\|\dot{e}_i(t)\|}{\|\delta(t)\|} \leq \|A\|\frac{\|e_i(t)\|}{\|\delta(t)\|} + \lambda_N(\mathcal{L})\|BK\|\left(\frac{\|e(t)\|}{\|\delta(t)\|} + 1\right). \tag{52}$$

By using (19) and $\|e(t)\| = \sum_{i=1}^{N} \|e_i(t)\| \leq \sqrt{Nc}\|\delta(t)\|$, $(d/dt)(\|e_i(t)\|)/(\|\delta(t)\|) \leq c_1(\|e_i(t)\|)/(\|\delta(t)\|) + c_2$, where c_1 and c_2 have been defined. Hence, the evolution time of $\|e_i(t)\|/\|\delta(t)\|$ from 0 to $\sqrt{c}$ is lower bounded by $\mathfrak{B}$. For the agents in $W_2(t)$, the interevent time is selected as $b_i \leq \mathfrak{B}$ to enable (50). It concludes that the controller (8) with the event trigger (13) guarantees that (48) holds for all the agents in $W_1(t) \cup W_2(t)$, which implies that $V(t)$ converges to zero. Let $\kappa_1 = (a_1/b_1)e^{(\alpha_1+\alpha_2)(T_0+\Delta_*)}$, where $a_1 = \max\{\lambda_{\max}(P), \lambda_{\max}(S)\}$ and $b_1 = \min\,\{\lambda_{\min}(P), \lambda_{\min}(S)\}$. Thus, by (48), it has $\|\delta_i(t)\|^2 \leq \kappa_1 e^{-\eta_1(t-t_0)}\|\delta_i(t_0)\|^2$, which means that secure average consensus is achieved exponentially. That is, $\|\delta_i(t)\|^2 = 0$ as $t \rightarrow +\infty$. Thus, $\lim_{t\rightarrow+\infty} x_i(t) = (1/N)\sum_{i=1}^{N} x_i(0)$.

APPENDIX B
PROOF OF THEOREM 2

A. Resilience Analysis

Step 1 (Two Intervals Classification): This section is similar to Step 1 in the proof of Theorem 1 for the update sequence $\{t_{k_i}^i\}$ determined by (24) and thus is omitted.

Step 2 (Lyapunov Stability Analysis):

1) Consider the time interval $\tilde{\Xi}_s(\tau, t)$ over which (23) holds. Choose a Lyapunov function candidate

$$V(\eta(t)) = \sum_{i=1}^{N} \theta_i^{-1} \eta_i^T(t)\tilde{P}\eta_i(t), \quad i = 1, 2, \ldots, N. \tag{53}$$

For $\Omega = \Theta\mathcal{H} + \mathcal{H}^T\Theta > 0$ defined in Lemma 2, taking the time derivative of $V(\eta(t))$ along the system (26) yields

$$\begin{aligned} \dot{V}(t) = \eta^T(t)[\Theta \otimes (\tilde{P}A + A^T\tilde{P}) - \Omega \otimes \tilde{P}B\tilde{K}]\eta(t) \\ -2\eta^T(t)(\Theta \otimes \tilde{P})(\mathcal{H} \otimes B\tilde{K})e(t). \end{aligned} \tag{54}$$

Let $\theta_{\min} = \min\theta_i^{-1}$, $i \in \mathcal{V}$ and $\tilde{\tau} \geq \lambda_{\min}^{-1}(\Omega)\theta_{\min}^{-1}$. Substituting $\tilde{K} = \tilde{\tau}\tilde{R}^{-1}B^T\tilde{P}$ into (54) gives

$$\begin{aligned} \dot{V}(t) &\leq \eta^T(t)(\Theta \otimes (\tilde{P}A + A^T\tilde{P}))\eta(t) - \tilde{\tau}\lambda_{\min}(\Omega)\theta_{\min}\eta^T(t) \\ &\qquad \times (\Theta \otimes \tilde{P}B\tilde{R}^{-1}B^T\tilde{P})\eta(t) - \eta^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t) \\ &\leq \eta^T(t)[\Theta \otimes (\tilde{P}A + A^T\tilde{P} - \tilde{P}B\tilde{R}^{-1}B^T\tilde{P})]\eta(t) \\ &\qquad - \eta^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t). \end{aligned} \tag{55}$$

By using $\tilde{P}A + A^T\tilde{P} - \tilde{P}B\tilde{R}^{-1}B^T\tilde{P} + \tilde{Q} = 0$ and denoting $k_{\min} = \lambda_{\min}(\Theta \otimes \tilde{Q})$, (55) can be expressed as

$$\begin{aligned} \dot{V}(t) &\leq -\eta^T(t)(\Theta \otimes \tilde{Q})\eta(t) - \eta^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t) \\ &\leq -k_{\min}\eta^T(t)\eta(t) - \eta^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t). \end{aligned} \tag{56}$$

Let $\hat{z}(t) = \mathrm{col}(\hat{z}_1, \ldots, \hat{z}_N)$ governed by the dynamics: $\dot{\hat{z}}(t) = (I_N \otimes A)\hat{z}(t)$ obtained from (6), (9), and (10) with $\eta_i(t) = x_i(t) - x_0(t)$ and $\hat{z}_i(t) = \sum_{j \in \mathcal{N}_i(\tilde{\mathcal{G}})} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t))$

$$\begin{aligned} \eta(t) &= \hat{x}(t) - (1_N \otimes x_0(t)) - e(t) \\ \hat{z}(t) &= (\mathcal{H} \otimes I_n)(1_N \otimes x_0(t) - \hat{x}(t)) \\ \eta(t) &= -(\mathcal{H}^{-1} \otimes I_n)\hat{z}(t) - e(t). \end{aligned} \tag{57}$$

After substituting (57) into (56) and letting $k_{\min} = k_{\min}^1 + k_{\min}^2$ and $\tilde{\mathcal{H}} = \mathcal{H}^{-1} \otimes I_n$, it is obtained that

$$\begin{aligned}\dot{V}(t) \leq &-k_{\min}^1 \eta^T(t)\eta(t) - k_{\min}^2(\hat{z}^T(t)\tilde{\mathcal{H}}^T\tilde{\mathcal{H}}\hat{z}(t) + e^T(t)e(t)) \\ &- 2k_{\min}^2 e^T(t)\tilde{\mathcal{H}}\hat{z}(t) + e^T(t)(\Theta\mathcal{H} \otimes 2\tilde{P}B\tilde{K})e(t) \\ &+ 2\hat{z}(t)^T(\tilde{\mathcal{H}}^T\Theta\mathcal{H} \otimes \tilde{P}B\tilde{K})e(t). \end{aligned} \tag{58}$$

By using Young's inequality: $x^Ty \leq (\tilde{\varrho}/2)x^Tx + (1/(2\tilde{\varrho}))y^Ty$

$$\begin{aligned}\dot{V}(t) \leq -k_{\min}^1 \eta^T(t)\eta(t) &- (\tilde{k}_2 - \tilde{k}_4/\tilde{\varrho})\hat{z}^T(t)\hat{z}(t) \\ &+ (\tilde{k}_3 + \tilde{k}_4\tilde{\varrho})e^T(t)e(t)\end{aligned} \tag{59}$$

where $\tilde{k}_i, i = 2, 3, 4$ have been defined before Theorem 4.

Let $\|e_i(t)\| \leq \tilde{\beta}_i\|\hat{z}_i(t)\|$ with $\tilde{\beta}_i^2 = \tilde{s}_i(\tilde{k}_2 - \frac{\tilde{k}_4}{\tilde{\varrho}})/(\tilde{k}_3 + \tilde{k}_4\tilde{\varrho})$, $\tilde{\varrho} > \tilde{k}_4/\tilde{k}_2$. Given $\tilde{\alpha}_1 = k_{\min}^1\lambda_{\max}^{-1}(\Theta \otimes \tilde{P})$, then (59) becomes

$$\begin{aligned}\dot{V}(t) &\leq -k_{\min}^1\sum_{i=1}^N \eta_i^T(t)\eta_i(t) - \sum_{i=1}^N(1-\tilde{s}_i)\hat{z}_i^T(t)\hat{z}_i(t) \\ &\leq -k_{\min}^1\lambda_{\max}^{-1}(\Theta \otimes \tilde{P})\eta^T(t)(\Theta \otimes \tilde{P})\eta(t) = -\tilde{\alpha}_1 V(t).\end{aligned} \tag{60}$$

2) Consider the time interval $\tilde{\Xi}_a(\tau, t)$ over which (12) does not necessarily hold. Choose a Lyapunov function

$$V(t) = \eta^T(t)(I_N \otimes \tilde{S})\eta(t) \tag{61}$$

which yields that like [30]–[32], the time derivative of (61) is

$$\dot{V}(t) = \eta^T(t)[I_N \otimes (\tilde{S}A + A^T\tilde{S})]\eta(t) \leq \tilde{\alpha}_2 V(t). \tag{62}$$

Denote $\tilde{\sigma}(t) \in \{\tilde{a}, \tilde{b}\}$ as a new piecewise constant function. Similar to that in (42), it follows from (60) and (62) that

$$V(\eta(t)) \leq \begin{cases} e^{-\tilde{\alpha}_1(t-\tilde{t}_{m-1}-\tilde{\Delta}_{m-1})}V_{\tilde{a}}(\tilde{t}_{m-1} + \tilde{\Delta}_{m-1}) \\ e^{\tilde{\alpha}_2(t-\tilde{t}_m)}V_{\tilde{b}}(\tilde{t}_m). \end{cases} \tag{63}$$

Step 3 (Bounds on DoS Attack Frequency and Duration): Similar to (43)–(48), when (27) and (28) are satisfied, there exists a constant $\tilde{\eta}_1 = \tilde{\alpha}_1 - ((\tilde{\alpha}_1 + \tilde{\alpha}_2)/\tau_a) - \tilde{\eta}_1^* > 0$ such that

$$V(\eta(t)) \leq e^{(\tilde{\alpha}_1+\tilde{\alpha}_2)(T_0+\tilde{\Delta}_*)}e^{-\tilde{\eta}_1(t-t_0)}V(\eta(t_0)). \tag{64}$$

B. Minimal Interevent Interval

Following a similar way, one can estimate the time derivative of $\|e_i(t)\|/\|\hat{z}(t)\|$ to obtain $\|\dot{e}_i(t)\|/\|\hat{z}(t)\| \leq \tilde{c}_1(\|e_i(t)\|/\|\hat{z}(t)\|) + \tilde{c}_2$ with $\tilde{c}_1 = 2\|A\|$ and $\tilde{c}_2 = 2\|\mathcal{H} \otimes BK\|\sqrt{\tilde{\gamma}_2} + \|BK\|$. The evolution time of $\|e_i(t)\|/\|\hat{z}(t)\|$ from 0 to $\sqrt{\tilde{c}}$ is, thus, lower bounded by $\tilde{\mathfrak{B}} = (1/\tilde{c}_1)\ln((\tilde{c}_1/\tilde{c}_2)\sqrt{\tilde{c}} + 1)$ with $\tilde{c} = \tilde{\gamma}_2/N$. Moreover, denote $\tilde{\kappa}_1 = (\tilde{a}_1/\tilde{b}_1)e^{(\tilde{\alpha}_1+\tilde{\alpha}_2)(T_0+\tilde{\Delta}_*)}$ with $\tilde{a}_1 = \max\{\lambda_{\max}(\Theta\otimes\tilde{P}), \lambda_{\max}(\tilde{S})\}$ and $\tilde{b}_1 = \min\,\{\lambda_{\min}(\Theta \otimes \tilde{P}), \lambda_{\min}(\tilde{S})\}$. It follows from (64) that $\|\eta_i(t)\|^2 \leq \tilde{\kappa}_1 e^{-\tilde{\eta}_1(t-t_0)}\|\eta_i(t_0)\|^2$, which implies $\|x_i(t)-x_0(t)\|^2 \leq \tilde{\kappa}_1 e^{-\tilde{\eta}_1(t-t_0)}\|x_i(t_0)-x_0(t_0)\|^2$ in (7). That is, secure leader-following consensus is achieved exponentially.

References

[1] 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.

[2] Y. Su and J. Huang, "Cooperative output regulation of linear multi-agent systems," *IEEE Trans. Autom. Control*, vol. 57, no. 4, pp. 1062–1066, Apr. 2012.

[3] Z. Feng, G. Hu, W. Ren, W. E. Dixon, and J. Mei, "Distributed coordination of multiple unknown Euler-Lagrange systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 55–66, Mar. 2018.

[4] Z. Feng, C. Sun, and G. Hu, "Robust connectivity preserving rendezvous of multirobot systems under unknown dynamics and disturbances," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 725–735, Dec. 2017.

[5] X. Dong and G. Hu, "Time-varying formation control for general linear multi-agent systems with switching directed topologies," *Automatica*, vol. 73, pp. 47–55, Nov. 2016.

[6] Z. Li, G. Wen, Z. Duan, and W. Ren, "Designing fully distributed consensus protocols for linear multi-agent systems with directed graphs," *IEEE Trans. Autom. Control*, vol. 60, no. 4, pp. 1152–1157, Apr. 2015.

[7] I. Shames, A. M. H. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757–2764, 2011.

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

[9] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Atlanta, GA, USA, Dec. 2010, pp. 1096–1101.

[10] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sep. 2012.

[11] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963–1970, Sep. 2013.

[12] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part II: Attack detection using enhanced hydrodynamic models," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1679–1693, Sep. 2013.

[13] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[14] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[15] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[16] H. S. Foroush and S. Martínez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Proc. IEEE 51st IEEE Conf. Decis. Control*, Maui, HI, USA, Dec. 2012, pp. 2551–2556.

[17] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Event-triggered control over unreliable networks subject to jamming attacks," in *Proc. 54th IEEE Conf. Decis. Control*, Osaka, Japan, Dec. 2015, pp. 4818–4823.

[18] C. De Persis and P. Tesi, "Resilient Control under denial-of-service," in *Proc. 19th IFAC Congr.*, Cape Town, South Africa, Aug. 2014, pp. 134–139.

[19] B. Chen, D. W. C. Ho, W.-A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 2, pp. 455–468, Feb. 2019.

[20] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[21] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Output-based event-triggered control systems under denial-of-service attacks," in *Proc. 54th IEEE Conf. Decis. Control*, Osaka, Japan, Dec. 2015, pp. 4824–4829.

[22] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Trans. Autom. Control*, vol. 52, no. 9, pp. 1680–1685, Sep. 2007.

[23] X. Wang and M. D. Lemmon, "Event-triggering in distributed networked control systems," *IEEE Trans. Autom. Control*, vol. 56, no. 3, pp. 586–601, Mar. 2011.

[24] D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson, “Distributed event-triggered control for multi-agent systems,” *IEEE Trans. Autom. Control*, vol. 57, no. 5, pp. 1291–1297, May 2012.

[25] Y. Fan, L. Liu, G. Feng, and Y. Wang, “Self-triggered consensus for multi-agent systems with Zeno-free triggers,” *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2779–2784, Oct. 2015.

[26] Y. Fan, G. Hu, and M. Egerstedt, “Distributed reactive power sharing control for microgrids with event-triggered communication,” *IEEE Trans. Control Syst. Technol.*, vol. 25, no. 1, pp. 118–128, Jan. 2017.

[27] E. Garcia, Y. Cao, and D. W. Casbeer, “Decentralized event-triggered consensus with general linear dynamics,” *Automatica*, vol. 50, no. 10, pp. 2633–2640, Oct. 2014.

[28] Z.-G. Wu, Y. Xu, R. Lu, Y. Wu, and T. Huang, “Event-triggered control for consensus of multiagent systems with fixed/switching topologies,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 10, pp. 1736–1746, Oct. 2018.

[29] T.-H. Cheng, Z. Kan, J. R. Klotz, J. M. Shea, and W. E. Dixon, “Event-triggered control of multiagent systems for fixed and time-varying network topologies,” *IEEE Trans. Autom. Control*, vol. 62, no. 10, pp. 5365–5371, Oct. 2017.

[30] Z. Feng and G. Hu, “Distributed tracking control for multi-agent systems under two types of attacks,” in *Proc. 19th IFAC World Congr.*, Cape Town, South Africa, Aug. 2014, pp. 1–6.

[31] 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, 2015.

[32] Z. Feng, G. Wen, and G. Hu, “Distributed secure coordinated control for multiagent systems under strategic attacks,” *IEEE Trans. Cybern.*, vol. 47, no. 5, pp. 1273–1284, May 2017.

[33] D. Senejohnny, C. De Persis, and P. Tesi, “Self-triggered coordination over a shared network under denial-of-service,” in *Proc. 54th IEEE Conf. Decis. Control*, Osaka, Japan, Dec. 2015, pp. 3469–3474.

[34] Z. Feng and G. Hu, “Distributed secure average consensus for linear multi-agent systems under DoS attacks,” in *Proc. Amer. Control Conf.*, Seattle, WA, USA, May 2017, pp. 2261–2266.

[35] Z. Feng and G. Hu, “Distributed secure leader-following consensus of multi-agent systems under DoS attacks and directed topology,” in *Proc. IEEE Int. Conf. Inf. Automat. (ICIA)*, Macau, China, Jul. 2017, pp. 73–79.

[36] W. Ren and Y. Cao, *Distributed Coordination of Multi-Agent Networks*. London, U.K.: Springer, 2011.

[37] F. L. Lewis and V. L. Syrmos, *Optimal Control*. New York, NY, USA: Wiley, 1995.

[38] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2003.

[39] A. Bidram, A. Davoudi, F. L. Lewis, and J. M. Guerrero, “Distributed cooperative secondary control of microgrids using feedback linearization,” *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3462–3470, Aug. 2013.

[40] H. Cai, G. Hu, F. L. Lewis, and A. Davoudi, “A distributed feedforward approach to cooperative control of AC microgrids,” *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 4057–4067, Sep. 2016.

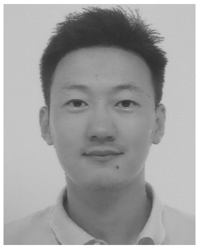
[41] T. Setter and M. Egerstedt, “Energy-constrained coordination of multi-robot teams,” *IEEE Trans. Control Syst. Technol.*, vol. 25, no. 4, pp. 1257–1263, Jul. 2017.

[42] M. Ye and G. Hu, “Distributed extremum seeking for constrained networked optimization and its application to energy consumption control in smart grid,” *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 6, pp. 2048–2058, Nov. 2016.

[43] C. Sun, G. Hu, and L. Xie, “Controllability of multiagent networks with antagonistic interactions,” *IEEE Trans. Autom. Control*, vol. 62, no. 10, pp. 5457–5462, Oct. 2017.

[44] Z. Feng and G. Hu, “Finite-time distributed optimization with quadratic objective functions under uncertain information,” in *Proc. 56th IEEE Annu. Conf. Decis. Control (CDC)*, Melbourne, VIC, Australia, Dec. 2017, pp. 208–213.

[45] Z. Feng and G. Hu, “A distributed constrained optimzation method for spatiotemporal connectivity-preserving rendezvous of multi-robot systems,” in *Proc. 57th IEEE Conf. Decis. Control*, Tallahassee, FL, USA, 2018.



Zhi Feng received the M.Sc. degree from the Dalian University of Technology, Dalian, China, in 2012, and the Ph.D. degree from Nanyang Technological University, Singapore, in 2017.

He is currently a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University. His current research interests include multiagent systems, distributed control and optimization, and security and resilience with applications to energy and robotic systems.

Dr. Feng was a recipient of the Best Paper in Automation Award in the 14th IEEE International Conference on Information and Automation in 2017.

Guoqiang Hu was with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2011. From 2008 to 2011, he was an Assistant Professor with Kansas State University, Manhattan, KS, USA. He is currently a Tenured Associate Professor and the Director of the Centre for System Intelligence and Efficiency, Nanyang Technological University, Singapore. His current research interests include distributed control, optimization and games, with applications to cooperative robotics and smart city systems.

Dr. Hu was a recipient of the Best Paper in Automation Award in the 14th IEEE International Conference on Information and Automation and the Best Paper Award (Guan Zhao-Zhi Award) in the 36th Chinese Control Conference. He serves as an Associate Editor for the IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, the Technical Editor for the IEEE/ASME TRANSACTIONS ON MECHATRONICS, an Associate Editor for the IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, and a Subject Editor for *International Journal of Robust and Nonlinear Control*.