Distributed Secure Cooperative Control Under Denial-of-Service Attacks From Multiple Adversaries

Wenying Xu, Guoqiang Hu, *Member, IEEE*, Daniel W. C. Ho, *Fellow, IEEE*, and Zhi Feng

***Abstract*—This paper develops a fully distributed framework to investigate the cooperative behavior of multiagent systems in the presence of distributed denial-of-service (DoS) attacks launched by multiple adversaries. In such an insecure network environment, two kinds of communication schemes, that is, sample-data and event-triggered communication schemes, are discussed. Then, a fully distributed control protocol with strong robustness and high scalability is well designed. This protocol guarantees asymptotic consensus against distributed DoS attacks. In this paper, "fully" emphasizes that the eigenvalue information of the Laplacian matrix is not required in the design of both the control protocol and event conditions. For the event-triggered case, two effective dynamical event-triggered schemes are proposed, which are independent of any global information. Such event-triggered schemes do not exhibit Zeno behavior even in the insecure environment. Finally, a simulation example is provided to verify the effectiveness of theoretical analysis.**

***Index Terms*—Asymptotic consensus, distributed denial-of-service (DoS) attack, distributed secure control, event-triggered, sample data.**

I. Introduction

DISTRIBUTED control plays a crucial role in completing a group task of multiple agents in a cooperative fashion, which has been widely applied to sensor networks, unmanned autonomous vehicles (UAVs), moving robot/vehicle teams, power systems, etc. In general, cooperation exists among neighboring agents with a close relationship, and refers to information sharing among neighboring agents [1]–[5]. The design of a distributed control protocol is dependent on local information sharing, and its main objective is to achieve a cooperative global task. The distributed property of the multiagent system leads to many advantages, such as strong robustness, high scalability, and low operational costs [2], [3], [6].

Network security plays a fundamental role in successful information transmission. As is known, the perfectly secure network environment is hardly guaranteed in the real world, as many types of attacks increasingly emerge, such as denial-of-service (DoS) attacks, replay attacks, and false data injection (FDI) attacks. *DoS attacks* refer to destroying the information availability [7], [8], *replay attacks* mean that the transmitted data are maliciously repeated [9], and *FDI attacks* denote that false information is injected and is then transmitted instead of true information [10]. Various types of attacks could generate different adverse impacts on system performance. Therefore, in the insecure network environment, it is of prominent importance to achieve the control objective and to maintain system performance against malicious attacks. So far, there have been some results reported on network security problems of networked control systems [8], [9], [11]–[15].

The security threat is of primary importance in multiagent systems, since distributed control is deeply dependent on the information sharing among neighboring agents. The malicious attacks will interrupt, delay, or even tamper transmitting information such that the efficiency of the distributed control protocol will be degraded significantly. Therefore, in an insecure communication environment, it is highly desirable to design an effective distributed control protocol against malicious attacks to maintain cooperative behavior among multiple agents. In the literature, a few attempts on secure control of multiagent systems have been reported. In [16], the consensus problem of multiagent systems is addressed in the presence of *malicious agents*. The effect of malicious attacks on network communication has been discussed in [10], [17], and [18]. In this paper, we mainly investigate a class of a DoS attack strategy launched from multiple adversaries, which is called a distributed DoS attack strategy. Compared with traditional DoS attacks [7], [12], [18], it is much harder for a multiagent system to withstand distributed

Manuscript received December 17, 2018; accepted January 21, 2019. This work was supported in part by the Singapore Economic Development Board through EIRP under Grant S14-1172-NRF EIRP-IHL, in part by the Singapore Ministry of Education Academic Research Fund Tier 1 under Grant RG180/17 (2017-T1-002-158), in part by the Research Grants Council of the Hong Kong under Grant CityU 11200717 and Grant CityU 7005029, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20180367, in part by the National Natural Science Foundation of China under Grant 61803082, in part by the Fundamental Research Funds for the Central Universities, in part by the Alexander von Humboldt Foundation of Germany, and in part by the ZhiShan Youth Scholar Program from Southeast University. This paper was recommended by Associate Editor J. Chen. *(Corresponding author: Guoqiang Hu.)*

W. Xu is with the School of Mathematics, Southeast University, Nanjing 210096, China, and also with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: wenyingxuwinnie@gmail.com).

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

D. W. C. Ho is with the Department of Mathematics, City University of Hong Kong, Hong Kong (e-mail: madaniel@cityu.edu.hk).

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/TCYB.2019.2896160

DoS attacks, since the joint impact of distributed DoS attacks on the entire communication network is more complex and diverse.

In most previous works on distributed control of multiagent systems, some eigenvalue information (especially the smallest nonzero eigenvalue) of the Laplacian matrix associated with the communication graph is required for the design of consensus protocols [19]. The eigenvalue information is global, since it implies that the entire communication graph is available to all agents. In a communication network, each agent has limited information on other agents and adversaries and, hence, the mentioned eigenvalue information can hardly be obtained in many situations. An adaptive method is proposed in [3] to avoid the utilization of eigenvalue information in some cases. However, it is hard to extend the adaptive method to deal with the imperfect communication cases, such as event-triggered communication or an insecure communication environment. Therefore, the objective of this paper is to develop a *fully* distributed control framework for imperfect network communication. Here, "fully" emphasizes that the eigenvalue information of the Laplacian matrix is not required [3] for the design of both the control protocol and event conditions. In this control framework, it is desirable to design a fully distributed control protocol to guarantee the satisfactory cooperative behavior of multiple agents. This protocol is expected to be robust to adverse impact from multiple adversaries, and to be independent of the eigenvalue information of the Laplacian matrix associated with the communication graph.

The contributions of this paper can be summarized as follows. This paper investigates one class of distributed DoS attacks, in which each adversary attacks one communication channel, and follows one attacking strategy. Under joint attacks of multiple adversaries, two kinds of communication scenarios are discussed, that is, time-triggered (sample-data) and event-triggered communication schemes. In these scenarios, a fully distributed control protocol is developed, which is independent of the eigenvalue information of the Laplacian matrix. The proposed protocol can guarantee asymptotic consensus from any initial values against the adverse impact from distributed DoS attacks. Moreover, two types of distributed event-triggered communication schemes are proposed with the following obvious advantages: 1) they are designed in a *fully distributed* way; 2) they guarantee *asymptotic* consensus even in the presence of distributed DoS attacks; and 3) they do not exhibit Zeno behavior. Finally, a simulation example is provided to verify the effectiveness of the proposed method.

The following notations will be used throughout this paper. First, denote $\mathbb{R}$ and $\mathbb{R}^n$ to be sets of reals and n-dimensional real column vectors, respectively. $\mathbf{1}$ means a column vector with all elements being 1. $\mathbb{N}^+$ denotes a set of positive integers. Let S_i $(i = 1, 2, \ldots, n)$ be n sets; then, $\bigcup_{i=1}^n S_i$ $(\bigcap_{i=1}^n S_i)$ denotes the union (intersection) of sets $S_1, \ldots, S_n$. The matrix $[d_{ij}]_{n\times m}$ is $n \times m$-dimensional, and its element d_{ij} is in row i and column j. For a real number a, $[a]$ means the largest integral number which is less than or equal to a.

II. Problem Statement and Preliminaries

A. Mathematical Modeling and Preliminaries

Consider a multiagent dynamical system with N agents, and the dynamics of each agent can be described as

$$\dot{x}_i(t) = u_i(t) \quad i = 1, 2, \ldots N \tag{1}$$

where $x_i(t) \in \mathbb{R}$ is the state of agent i at instant t and $u_i(t) \in \mathbb{R}$ is its control protocol at instant t.

To simplify the notation, choose $x_i(t) \in \mathbb{R}$, and all of the results in this paper hold when $x_i(t) \in \mathbb{R}^n$ by introducing the symbol $\otimes$.

Consider an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ consisting of a node set $\mathcal{V} = \{1, 2, \ldots, N\}$ and a set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. Let m be the total number of edges in $\mathcal{E}$. If node i connects node j by an edge, then denote $(i, j) \in \mathcal{E}$, and nodes i and j are called *neighbors*. Define $\mathcal{N}_i$ to be a set including all neighbors of node i, and denote d_i to be the total number of nodes in $\mathcal{N}_i$. In addition, for $1 \le i, j \le N$, define

$$a_{ij} = \begin{cases} 1, & i \neq j \ \& \ (i, j) \in \mathcal{E} \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

Now, we assign an orientation to the undirected edge by choosing one of two nodes as the head of this edge and the other one as its tail. Note that the choice of the orientation does not change the results. Then define the incidence matrix $D = [d_{ik}]_{N\times m} \in \mathbb{R}^{N\times m}$ with

$$d_{ik} = \begin{cases} 1, & \text{if node } i \text{ is the head of the } k\text{-th oriented edge} \\ -1, & \text{if node } i \text{ is the tail of the } k\text{-th oriented edge} \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

Furthermore, if agents i and j are connected by edge k, then

$$y_k = \begin{cases} x_i - x_j & \text{if node } i \text{ is the head} \\ x_j - x_i & \text{if node } j \text{ is the head.} \end{cases} \tag{4}$$

Meanwhile, define the Laplace matrix $L = [l_{ij}]_{N\times N} \in \mathbb{R}^{N\times N}$ with $l_{ij} = -a_{ij}$ when $i \neq j$ and $l_{ij} = \sum_{k\in\mathcal{N}_i} a_{ik}$ when $i = j$. Obviously, $L = DD^T$.

B. Distributed DoS Attack Strategies

In this section, we introduce the distributed DoS attack strategies launched by multiple adversaries. Each adversary aims at one communication channel, and its task is to corrupt and interrupt information transmission over its targeted channel. In this distributed DoS attack strategy, each adversary follows an attacking strategy independently with those of other adversaries. In this situation, these multiple attack strategies have a joint effect on the entire network communication.

To be specific, for channel (edge) (i, j) between agents i and j, let $\mathcal{A}_n^{ij}$ be the nth launch attack signal, and denote the duration of this attack signal $\mathcal{A}_n^{ij}$ as τ_n^{ij}. Note that when $\tau_n^{ij} = 0$, this attack signal is similar to a form of one impulse. Then, a DoS attack strategy $\{\mathcal{I}_n^{ij}\}_{n\in\mathbb{N}^+}$ is generated for channel $(i, j) \in \mathcal{E}$ with $\mathcal{I}_n^{ij} = \{\mathcal{A}_n^{ij}\} \cup [\mathcal{A}_n^{ij}, \mathcal{A}_n^{ij} + \tau_n^{ij})$, and its objective is to interrupt information transmission over channel (i, j). This implies that the transmission attempt t' $(t' \in \mathcal{I}_n^{ij})$ over channel (i, j) is

always attacked and unsuccessful. Moreover, define $n^{ij}(t_0, t)$ to be the sum of $\mathcal{A}_n^{ij}$ belonging to the interval $[t_0, t)$.

Under the distributed DoS attack, given a time instant $t_0 \in \mathbb{R}$ and $t \geq t_0 \in \mathbb{R}$, define

$$\Psi^{ij}(t_0, t) = \bigcup_{n \in \mathbb{N}^+} \mathcal{I}_n^{ij} \cap [t_0, t]; \;\; \Phi^{ij}(t_0, t) = [t_0, t] \backslash \Psi^{ij}(t_0, t) \tag{5}$$

for channel $(i, j) \in \mathcal{E}$. In other words, $\Psi^{ij}(t_0, t)$ and $\Phi^{ij}(t_0, t)$ denote the sets of time instants when the information transmission is unsuccessful or successful, respectively.

Assumption 1 (DoS Frequency): For channel $(i, j) \in \mathcal{E}$, there exist $T_d^{ij} > 0$ and $\mu_1^{ij} > 0$ satisfying

$$n^{ij}(t_0, t) \leq \mu_1^{ij} + \frac{t - t_0}{T_d^{ij}} \tag{6}$$

for any t_0, $t \geq t_0$.

Assumption 2 (DoS Duration): For channel $(i, j) \in \mathcal{E}$, there exist $T_f^{ij} > 0$ and $\mu_2^{ij} > 0$ satisfying

$$\left|\Psi^{ij}(t_0, t)\right| \leq \mu_2^{ij} + \frac{t - t_0}{T_f^{ij}} \tag{7}$$

for any t_0, $t \geq t_0$.

Remark 1: Assumptions 1 and 2 are commonly used for DoS attacks [7], [17], [18]. Similarly, two assumptions on the frequency and duration of distributed DoS attacks are presented in this paper. As we know, there are very few works on the investigation of distributed DoS attacks in multiagent systems. Senejohnny *et al.* [17] discussed the impact of distributed DoS attacks, and their goal is to achieve the bounded consensus. However, in this paper, the proposed objective is to achieve asymptotic consensus under Assumptions 1 and 2. Thus, it requires designing a new communication scheme and providing a novel theoretical analysis method.

C. Distributed Communication and Control Protocol

To achieve distributed cooperation of multiple agents, information transmission between agents is necessary. When the network environment is perfectly secure, the information transmission is always successful. However, in this paper, the information is transmitted over an insecure network, which implies that the transmission attempts could be attacked and, hence, unsuccessful.

Let t_k^{ij} be the kth transmission attempt over the channel (i, j) between agents i and j. If $t_k^{ij} \in \Psi^{ij}(t_0, t)$ with $t \geq t_k^{ij}$, which implies that this transmission attempt is subject to malicious attacks and, thus, this attempt is unsuccessful. On the other hand, if $t_k^{ij} \in \Phi^{ij}(t_0, t)$, then this information is successfully transmitted over channel (i, j), that is, this transmission attempt is successful.

Our objective is to design a fully distributed control protocol $u_i(t)$ to guarantee asymptotic consensus against distributed DoS attacks in an insecure network.

Definition 1 (Asymptotic Consensus): The multiagent system (1) is said to achieve asymptotic consensus if, for any initial conditions, the following equation holds:

$$\lim_{t \to \infty} x_i(t) - x_j(t) = 0, \quad \forall i, j = 1, 2, \ldots, N. \tag{8}$$

A distributed control protocol $u_i(t)$ for system (1) is designed with the following form:

$$u_i(t) = -\sum_{(i,j) \in \mathcal{E}} y_{ij}(t) \tag{9}$$

with

$$y_{ij}(t) = \begin{cases} x_i\left(t_k^{ij}\right) - x_j\left(t_k^{ij}\right) & t = t_k^{ij} \in \Phi^{ij}(t_0, t) \\ 0 & t = t_k^{ij} \in \Psi^{ij}(t_0, t) \\ y_{ij}\left(t_k^{ij}\right) & t \in \left[t_k^{ij}, t_{k+1}^{ij}\right) \end{cases} \tag{10}$$

where $\{t_k^{ij}\}_{k \in \mathbb{N}^+}$ is the time sequence of transmission attempts over channel (i, j), $(i, j) \in \mathcal{E}$.

Remark 2: Distributed control has wide applications in the real world, such as moving robots, vehicle teams, sensor networks, UAVs, power systems, etc. Note that the distributed control is deeply dependent on the information sharing among neighboring agents. The malicious attacks could interrupt, delay, or even tamper transmitting information, such that the efficiency of the distributed control protocol is degraded significantly. Therefore, in an insecure communication environment, it is highly desirable to design an effective distributed control protocol against malicious attacks to maintain cooperative behavior among multiple agents. These schemes could make the distributed control applicable for a more complex network environment.

III. Main Results

In this section, we present our main results on the design and implementation of a fully distributed control protocol against the adverse impact from distributed DoS attacks. Under this protocol, the asymptotic consensus can be guaranteed. In this section, two kinds of communication schemes are discussed, that is, sample-data (time-triggered) and event-triggered communication schemes. For the event-triggered cases, two different event conditions are proposed, and there is no involvement of global information in the event conditions.

A. Time-Triggered Communication Scheme

First, we investigate a time-triggered (sample-data) communication scheme, under which the transmission attempts are periodic over each channel, that is

$$t_{k+1}^{ij} - t_k^{ij} = h \tag{11}$$

with $h > 0$, $t_0^{ij} = t_0$, $k \in \mathbb{N}^+$, and $(i, j) \in \mathcal{E}$.

In the sample-data scheme (11), information is periodically transmitted. However, a distributed attack strategy will lead to the transmission attempts of each channel that could be asynchronously attacked. Under this attack strategy, the communication of the entire network is possibly always affected by malicious attacks, even though the attacks for one channel are intermittent.

Next, the following theorem presents the main result under the time-triggered communication scheme.

Theorem 1: Consider a multiagent system (1) with an undirected connected network topology. Suppose that distributed DoS attack strategies satisfy Assumptions 1 and 2.

The information transmission attempts $\{t_k^{ij}\}_{k\in\mathbb{N}^+}$ over channel (i,j) follow a given periodic sampling (11) with $0 < h < (1/[2(N-1)])$, and the distributed control protocol is designed in (9). Then, the asymptotic consensus can be guaranteed even in an insecure network, if

$$\frac{1}{T_f^{ij}} + \frac{h}{T_d^{ij}} < 1. \tag{12}$$

The proof of Theorem 1 will be shown in Appendix A.

Remark 3: Theorem 1 illustrates the effectiveness of the distributed control protocol (9) when the frequency and duration of distributed DoS attacks satisfy the condition (12). This condition implies that each communication channel is not always under attack. Despite this, the joint effect of distributed DoS attacks under condition (12) on the entire network communication is complex and diverse. Therefore, the proof of Theorem 1 brings many challenges to the theoretical analysis. In communication scheme (11), the design and implementation of the control protocol (9) are executed in a distributed way. The condition for the sampling period h involves the information N, that is, the number of agents. This information will no longer be involved in event-triggered schemes in the following sections.

B. Dynamical Event-Triggered Communication Scheme

In this section, we further consider the event-triggered communication scheme, under which the impact of distributed DoS attacks on cooperation behavior of multiple agents will be thoroughly discussed and analyzed. In this situation, the transmission attempts of each channel are generated by some well-defined events, which could be aperiodic and asynchronous.

For the requirement of fully distributed behavior, the challenges of this section are given as follows: 1) how to design a fully distributed event condition without Zeno behavior and 2) how to prove the validity of the distributed control protocol (9) on guaranteeing asymptotic consensus in the presence of distributed DoS attacks. These two questions will be addressed in this section.

Let $\{t_k^{ij}\}_{k\in\mathbb{N}^+}$ be the time sequence of the transmission attempts over channel (i,j). Different from periodic transmission attempts, in this section, these attempts are generated by event conditions and, thus, they could be aperiodic and asynchronous.

First, for channel $(i,j)\in\mathcal{E}$, let $z_{ij}(t) = x_i(t) - x_j(t)$ be the information of channel (i,j), and $e_{ij}(t) = z_{ij}(t_{k_s}^{ij}) - z_{ij}(t)$ is an error function of channel (i,j) with $t_{k_s}^{ij} = \max_l\{t_l^{ij} \le t : t_l^{ij} \in \Phi^{ij}(t_0,t)\}$. Obviously, at successful transmission attempts $t_{k_s}^{ij}$, $e_{ij}(t)$ is always reset to zero, that is, $e_{ij}(t_{k_s}^{ij}) = 0$.

Now, we proceed to address challenge 1).

In this section, a dynamical event-triggered scheme is introduced as

$$t_{k+1}^{ij} = \begin{cases} \max_{t\ge t_k^{ij}}\left\{t : \beta_{ij}\left(\frac{1}{4\tilde{a}_{ij}}e_{ij}^2(t) - \tilde{\theta}_{ij}\frac{2-\tilde{a}_{ij}}{4}y_{ij}^2\left(t_k^{ij}\right)\right) \le \eta_{ij}(t)\right\} \\ \qquad\qquad t_k^{ij} \in \Phi^{ij}(t_0,t) \\ t_k^{ij} + \theta^{ij} \qquad t_k^{ij} \in \Psi^{ij}(t_0,t) \end{cases} \tag{13}$$

with a dwell time $\theta^{ij} > 0$ and for $t \in [t_k^{ij}, t_{k+1}^{ij})$

$$\dot{\eta}_{ij}(t) = \begin{cases} -\alpha_{ij}\eta_{ij}(t) - \xi_{ij}\left(\frac{1}{4\tilde{a}_{ij}}e_{ij}^2(t) - \tilde{\theta}_{ij}\frac{2-\tilde{a}_{ij}}{4}y_{ij}^2\left(t_k^{ij}\right)\right) \\ \qquad\qquad t_k^{ij} \in \Phi^{ij}(t_0,t) \\ 0, \qquad t_k^{ij} \in \Psi^{ij}(t_0,t) \end{cases} \tag{14}$$

where $\alpha_{ij}, \beta_{ij}, \tilde{\theta}_{ij} > 0$, $0 < \xi_{ij} < 2$, and $\tilde{a}_{ij} > 0$, and $y_{ij}(t)$ is defined in (10) for $(i,j)\in\mathcal{E}$.

The dynamical event-triggered scheme (13) is designed to schedule the information transmission over channel (i,j), $(i,j)\in\mathcal{E}$ in an insecure network environment.

Two lemmas will be first discussed as follows.

Lemma 1: Under the dynamical event-triggered mechanism (13), the function $\eta_{ij}(t)$ in (14) is always positive with $\eta_{ij}(t_0) > 0$, that is, $\eta_{ij}(t) > 0$ for all $(i,j)\in\mathcal{E}$.

Proof: Under the event-triggered mechanism (13), the transmission attempts $\{t_k^{ij}\}_{k\in\mathbb{N}^+}$ can be generated, and then can be further classified into the successful transmission attempts denoted by $\{t_{k_s}^{ij}\}_{s\in\mathbb{N}^+}$ and the attacked (unsuccessful) transmission attempts $\{t_{k_a}^{ij}\}_{a\in\mathbb{N}^+}$. Obviously, $\{t_{k_s}^{ij}\}_{s\in\mathbb{N}^+}\bigcup\{t_{k_a}^{ij}\}_{a\in\mathbb{N}^+} = \{t_k^{ij}\}_{\in\mathbb{N}^+}$. Choose any $t_{k_{s_0}}^{ij} \in \Phi^{ij}(t_0,\infty)$, and then denote $a_1 = \min\{a\in\mathbb{N}^+ : t_{k_a}^{ij} > t_{k_{s_0}}^{ij}\}$. When $t \in [t_k^{ij}, t_{k+1}^{ij}) \subseteq [t_{k_{s_0}}^{ij}, t_{k_{a_1}}^{ij})$, according to (13), one has

$$\frac{1}{4\tilde{a}_{ij}}e_{ij}^2(t) - \tilde{\theta}_{ij}\frac{2-\tilde{a}_{ij}}{4}y_{ij}^2\left(t_k^{ij}\right) \le \frac{\eta_{ij}(t)}{\beta_{ij}}.$$

Then, we have $\dot{\eta}_{ij}(t) = -\alpha_{ij}\eta_{ij}(t) - \xi_{ij}([1/(4\tilde{a}_{ij})]e_{ij}^2(t) - \tilde{\theta}_{ij}[(2-\tilde{a}_{ij})/4]y_{ij}^2(t_k^{ij})) \ge -(\alpha_{ij} + [\xi_{ij}/\beta_{ij}])\eta_{ij}(t)$, which implies that $\eta_{ij}(t) \ge \eta_{ij}(t_k^{ij})\exp\{-(\alpha_{ij} + [\xi_{ij}/\beta_{ij}])(t - t_k^{ij})\}$ for $t \in [t_k^{ij}, t_{k+1}^{ij}) \subseteq [t_{k_{s_0}}^{ij}, t_{k_{a_1}}^{ij})$. Next, by mathematical induction, one has $\eta_{ij}(t) \ge \eta_{ij}(t_{k_{s_0}}^{ij})\exp\{-(\alpha_{ij} + [\xi_{ij}/\beta_{ij}])(t - t_{k_{s_0}}^{ij})\}$. On the other hand, denote $s_1 = \min_s\{s\in\mathbb{N}^+ : t_{k_s}^{ij} > t_{k_{a_1}}^{ij}\}$. When $t \in [t_{k_{a_1}}^{ij}, t_{k_{s_1}}^{ij})$, according to (14), $\dot{\eta}_{ij}(t) = 0$ and, thus, $\eta_{ij}(t) = \eta_{ij}(t_{k_{a_1}}^{ij})$. Due to $\eta_{ij}(t_0) > 0$, one concludes $\eta_{ij}(t) > 0$. ∎

Lemma 2: Consider distributed DoS attack strategies with Assumptions 1 and 2, under the dynamical distributed event-triggered communication scheme (13). For the attacked transmission attempt $t_{k_a}^{ij} \in [\mathcal{A}_k^{ij}, \mathcal{A}_k^{ij} + \tau_k^{ij})$, the following condition:

$$\frac{1}{T_f^{ij}} + \frac{\theta^{ij}}{T_d^{ij}} < 1 \tag{15}$$

guarantees that there exists at least one successful transmission during $[t_{k_a}^{ij}, \mathcal{A}_k^{ij} + \tau_k^{ij} + \widetilde{\Delta}^{ij})$ with $\widetilde{\Delta}^{ij} := [(\mu_1^{ij}\theta^{ij} + \mu_2^{ij})/(1-\widetilde{\gamma}^{ij})]$, $\widetilde{\gamma}^{ij} = (1/T_f^{ij}) + (\theta^{ij}/T_d^{ij})$, and θ^{ij} is defined in (13).

The conclusion in Lemma 2 is motivated by [7] and [17], and its proof is similar to that of Lemma 3 in Appendix A.

To address challenge 2), we present our main results in Theorem 2, in which the validity of the fully distributed control protocol (9) under the dynamical event-triggered communication scheme (13) will be proved in the presence of distributed DoS attacks.

Theorem 2: Consider a multiagent system (1) with an undirected connected network topology. Suppose that distributed

DoS attack strategies satisfy Assumptions 1 and 2. The information transmission attempts $\{t_k^{ij}\}_{k\in\mathbb{N}^+}$ over channel (i,j) are generated by the distributed dynamical event-triggered scheme (13). Under condition (15) with $0<\tilde{\theta}_{ij}<1$, $\alpha_{ij}>\tilde{\xi}_{ij}$, $\tilde{\xi}_{ij}=[(2-\xi_{ij})/\beta_{ij}]+[(2(1-\tilde{\theta}_{ij})(2-\tilde{a}_{ij})\tilde{a}_{ij})/([1+\tilde{a}_{ij}(2-\tilde{a}_{ij})\tilde{\theta}_{ij}]\beta_{ij})]$, and $0<\tilde{a}_{ij}<2$, the distributed control protocol (9) guarantees the asymptotic consensus in the presence of a distributed DoS attacks.

The proof of Theorem 2 will be shown in Appendix B.

Theorem 3: Under the event-triggered communication scheme (13), Zeno behavior can be successfully excluded.

The proof of Theorem 3 is provided in Appendix C.

The effectiveness of the dynamical event-triggered scheme (13) has been proved in Theorem 2 for an insecure network environment. Actually, the triggered scheme (13) aims at scheduling the information transmission of each channel, that is, when to activate one channel for information transmission between the corresponding two agents. The error function $e_{ij}(t)$ in (13) measures the change of the information z_{ij} of channel (i,j). However, in some situations, if the information change of channels could not always be obtained even for event detection, then, how can the next triggering instant for channels be determined? To further solve this issue, an alternative dynamical event-triggered scheme will be further proposed.

Motivated by the design of the event-triggered scheme (13), an alternative dynamical event-triggered scheme will be further proposed. First, define two error functions $e_i^j=x_i(t_k^{ij})-x_i(t)$ and $e_j^i(t)=x_j(t_k^{ij})-x_j(t)$. Then, an alternative dynamical event-triggered scheme can be proposed as

$$t_{k+1}^{ij}=\begin{cases}\min\left\{t_{k+1,i}^{ij},t_{k+1,j}^{ij}\right\} & t_k^{ij}\in\Phi^{ij}(t_0,t)\\ t_k^{ij}+\theta^{ij} & t_k^{ij}\in\Psi^{ij}(t_0,t)\end{cases}\tag{16}$$

with a dwell time $\theta^{ij}>0$

$$\begin{aligned}t_{k+1,i}^{ij}&=\max_{t\geq t_k^{ij}}\left\{t:\beta_{ij}\left(\frac{1}{2\hat{a}_{ij}}e_i^{j2}(t)-\tilde{\theta}_{ij}\frac{1-\hat{a}_{ij}}{2}y_{ij}^2\left(t_k^{ij}\right)\right)\leq\eta_i^j(t)\right\}\\ t_{k+1,j}^{ij}&=\max_{t\geq t_k^{ij}}\left\{t:\beta_{ij}\left(\frac{1}{2\hat{a}_{ij}}e_j^{i2}(t)-\tilde{\theta}_{ij}\frac{1-\hat{a}_{ij}}{2}y_{ij}^2\left(t_k^{ij}\right)\right)\leq\eta_j^i(t)\right\}\end{aligned}\tag{17}$$

and for $t\in[t_k^{ij},t_{k+1}^{ij})$

$$\begin{aligned}\dot{\eta}_i^j(t)&=\begin{cases}-\alpha_{ij}\eta_i^j(t)-\xi_{ij}\left(\frac{1}{2\hat{a}_{ij}}e_i^{j2}(t)-\tilde{\theta}_{ij}\frac{1-\hat{a}_{ij}}{2}y_{ij}^2\left(t_k^{ij}\right)\right) & t_k^{ij}\in\Phi^{ij}(t_0,t)\\ 0, & t_k^{ij}\in\Psi^{ij}(t_0,t)\end{cases}\\ \dot{\eta}_j^i(t)&=\begin{cases}-\alpha_{ij}\eta_j^i(t)-\xi_{ij}\left(\frac{1}{2\hat{a}_{ij}}e_j^{i2}(t)-\tilde{\theta}_{ij}\frac{1-\hat{a}_{ij}}{2}y_{ij}^2\left(t_k^{ij}\right)\right) & t_k^{ij}\in\Phi^{ij}(t_0,t)\\ 0, & t_k^{ij}\in\Psi^{ij}(t_0,t)\end{cases}\end{aligned}\tag{18}$$

where $\alpha_{ij},\beta_{ij},\tilde{\theta}_{ij}>0$, $0<\xi_{ij}<1$ for $(i,j)\in\mathcal{E}$, $\hat{a}_{ij}>0$, and $y_{ij}(t)$ is defined in (10).

Under the dynamical event-triggered scheme (16), agents i and j can independently determine $t_{k+1,i}^{ij}$ and $t_{k+1,j}^{ij}$, respectively. Instead of measuring the change of channel information [i.e., $e_{ij}(t)$] in (13), under the event-triggered scheme (16), agents i and j just measure the change of their own states $e_i^j(t)$ and $e_j^i(t)$, respectively. If one of two inequalities (17) is satisfied, then this channel will be activated for information transmission attempts between agents i and j. Next, the effectiveness of the dynamical event-triggered scheme (16) in the insecure network environment is illustrated in Corollary 1.

Corollary 1: Consider a multiagent system (1) with an undirected connected network topology. Suppose that distributed DoS attack strategies satisfy Assumptions 1 and 2. The information transmission attempts $\{t_k^{ij}\}_{k\in\mathbb{N}^+}$ over channel (i,j) are generated by the distributed dynamical event-triggered scheme (16). Under condition (15) with $0<\tilde{\theta}_{ij}<1$, $\alpha_{ij}>\tilde{\xi}_{ij}$, $\tilde{\xi}_{ij}=[(1-\xi_{ij})/\beta_{ij}]+[(4(1-\tilde{\theta}_{ij})(1-\hat{a}_{ij})\hat{a}_{ij})/([1+4\hat{a}_{ij}(1-\hat{a}_{ij})\tilde{\theta}_{ij}]\beta_{ij})]$, and $0<\hat{a}_{ij}<1$, the distributed control protocol (9) guarantees the asymptotic consensus in the presence of distributed DoS attack. In addition, the Zeno behavior can be successfully excluded under the event-triggered communication scheme (13).

Proof: The proof is similar to those in Theorems 2 and 3 by constructing a Lyapunov function $\hat{W}(t)=V(t)+\sum_{(i,j)\in\mathcal{E}}\eta_i^j(t)+\sum_{(i,j)\in\mathcal{E}}\eta_j^i(t)$. Here, the $V(t)$ is the same as that in Theorem 2. To avoid repetition, the detailed proof is omitted. ■

Remark 4: Dynamical event-triggered schemes have been studied in [20]–[22], which focus on the investigation of a perfectly insured network setting. However, two novel dynamical event-triggered communication schemes (13) and (16) are designed for an insecure network environment. The event-triggered communication scheme (13) generates transmission attempts along each channel in the presence of distributed DoS attacks. In addition, there exist several methods to exclude Zeno behavior based on a predefined dwell time [23], [24], or a combination with sample-data schemes [25], [26], or the introduction of a time-varying function in the control protocol [27]. In the aforementioned literature, it is unavoidable to use the global information of the Laplacian matrix [23]–[26] or to involve the global conditions [27]. However, the dynamical event-triggered communication schemes (13) and (16) avoid the involvement of global information, and more important, its efficiency has been verified in the presence of distributed DoS attacks. Hence, the application of the dynamical event-triggered scheme leads to fully distributed secure control of multiagent systems.

Remark 5: In Theorem 2 and Corollary 1, the asymptotic consensus can be guaranteed under the fully distributed control protocol (9) based on the dynamical event-triggered communication schemes, although distributed DoS attacks lead to a lot of unsuccessful transmission attempts in each communication channel. The main contributions of this section can be illustrated in a class of fully distributed behaviors. Here, "fully distributed behaviors" can be reflected in the following three aspects: 1) the control protocol (9) is designed in a distributed way; 2) there is no involvement of global information in the dynamical event-triggered communications (13) and (16); and 3) the condition (15) on distribution DoS attacks only involves local information. To summarize, fully distributed design and implementation are realized in this paper in the presence of distributed DoS attacks.

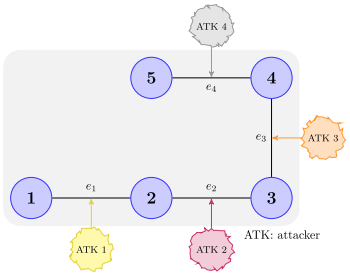


Fig. 1. Network communication is subject to distributed DoS attacks from four attackers.

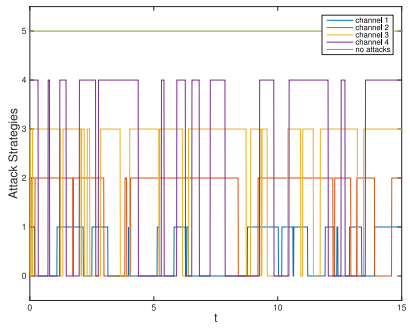


Fig. 2. Attack strategies of four attackers: lines 1–4 (in blue, orange, yellow, and purple, respectively) denote the time intervals without DoS attacks over four communication channels; line 0 denotes the time intervals under DoS attacks generated by four channels (in blue, orange, yellow, and purple, respectively). Line 5 is the reference case with no attacks.

IV. Simulations

In this section, a simulation example will be provided to verify the effectiveness of the fully distributed control protocol against distributed attacks under a dynamical event-triggered communication scheme.

Example 1: Consider a multiagent system (1) with five agents, and there are four communication channels among them, that is, e_i, $i = 1, 2, 3, 4$. Here, there exist four attackers labeled as ATK i in Fig. 1. One ATK just attacks one channel, and follows one DoS attack strategy. This implies that each ATK can determine when to launch one attack signal and the dwell time of this signal, that is, $\mathcal{A}_k^{ij}$ and τ_k^{ij}. For example, during $[\mathcal{A}_k^{12}, \mathcal{A}_k^{12}+\tau_k^{ij})$, the transmission attempt over channel e_1 will be attacked and unsuccessful. Note that $\{\mathcal{A}_k^{ij}\}\bigcup[\mathcal{A}_k^{ij}, \mathcal{A}_k^{ij}+\tau_k^{ij})$ $(i,j) \in \mathcal{E}$ are independently generated by different ATKs (attackers).

The attack signals and their dwell time for four communication channels are shown in Fig. 2. Note that any one of the channels $e_i (i = 1, 2, 3, 4)$ is subject to attacks; then, the connectivity of the network topology is destroyed. In Fig. 2, different color lines mean different channels, and lines 1–4 mean the secure time interval without DoS attacks, and line 0 denotes the insecure time intervals generated by different ATKs (displayed in different colors). From Fig. 2, each communication channel is immediately subject to DoS attacks, see lines 1–4; however, the network is always under the effect of DoS attacks, which is well displayed in line 0. This implies that the connectivity of the network topology is hardly satisfied for a long time interval under distributed DoS attacks. Despite this, the effectiveness of the fully distributed control protocol (9) is verified in Fig. 5.

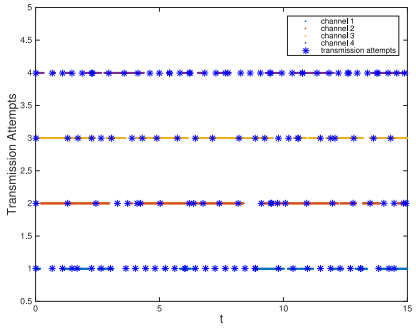


Fig. 3. Transmission attempts over four channels. Under the dynamical event-triggered scheme (16), the generated transmission attempts of four communication channels are 36, 26, 25, and 42, respectively.

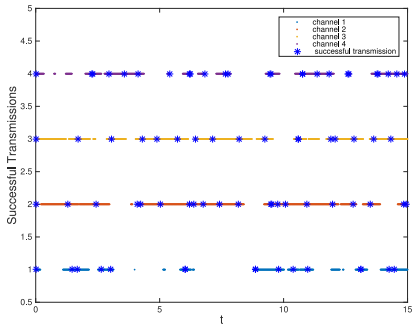


Fig. 4. Successful transmissions over four channels. Under distributed DoS attacks, the successful transmissions are 16, 21, 17, and 25 over channels 1, 2, 3, and 4, respectively.

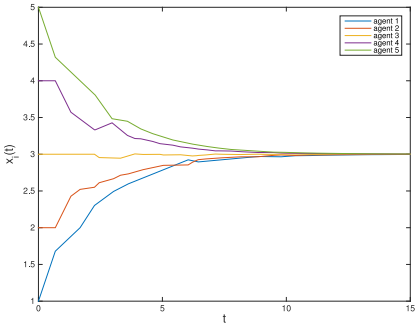


Fig. 5. Five agents achieve asymptotic consensus.

Choose $\theta^{ij} = 0.4$, $\alpha_{ij} = 2$, $\beta_{ij} = 1$, $\hat{a}_{ij} = 0.8$, and $\tilde{\theta}_{ij} = 0.4$ for $(i,j) \in \{(1,2), (2,3), (3,4), (4,5)\}$, then under the distributed dynamical event-triggered communication scheme (16), the transmission attempts over four channels are generated, respectively, which is shown in Fig. 3. The number of attempts over channels 1, 2, 3, and 4 are 31, 23, 14, and 21, respectively. However, due to the insecure communication environment, partial transmission attempts suffer from DoS attacks. Then, according to Fig. 4, only 16, 21, 17, and 25 of transmissions are successful for the corresponding channels, respectively. Under distributed event-triggered communication (16), the control protocol is well designed in a fully distributed way with the form of (9), and it indeed guarantees that all agents achieve asymptotic consensus eventually (see Fig. 5) even under the distributed DoS attacks (see Fig. 2).

V. Conclusion

This paper has investigated the distributed secure control of multiagent systems under DoS attacks. We focus on the investigation of a jointly adverse impact of distributed DoS attacks from multiple adversaries. In this scenario, two kinds of communication schemes, that is, sample-data and event-triggered communication schemes, have been discussed and, then, a fully distributed control protocol has been developed to guarantee satisfactory asymptotic consensus. Note that this protocol has strong robustness and high scalability. Its design does not involve any global information, and its efficiency has been proved. For the event-triggered case, two effective dynamical event conditions have been designed and implemented in a fully distributed way, and both of them have excluded Zeno behavior. Finally, a simulation example has been provided to verify the effectiveness of theoretical analysis. Our future research topics focus on fully distributed event/self-triggered control for linear/nonlinear multiagent systems to gain a better understanding of fully distributed control.

Appendix A
Proof of Theorem 1

Before proving Theorem 1, we present a lemma to facilitate the proof, and similar lemmas have been provided in [7] and [17].

Lemma 3: Under distributed DoS attack strategies with Assumptions 1 and 2, and the periodic information transmission scheme (11), condition (12) guarantees that the time interval between two consecutive successful information transmissions is less than $\Delta^{ij}+h$ with $\Delta^{ij}=[(\mu_1^{ij}h+\mu_2^{ij})/(1-\gamma^{ij})]$ and $\gamma^{ij}=(1/T_f^{ij})+(h/T_d^{ij})$.

Proof: Under communication scheme (11), if two consecutive transmission attempts are not subject to attacks, then both of them are successful and the interval between them is h. In this case, the conclusion of this lemma holds.

Next, assume $t_{k_s}^{ij}\in\Phi(t_0,t)$, but $t_{k_s+1}^{ij}=t_{k_s}^{ij}+h\in[\mathcal{A}_n^{ij},\mathcal{A}_n^{ij}+\tau_n^{ij})$. This implies that the next transmission attempt after the successful one suffers from attack; then, in this case, we would like to evaluate the upper bound of the next *successful* transmission attempt.

Define $\widetilde{\mathcal{I}}_n^{ij}=\{\mathcal{A}_n^{ij}\}\cup[\mathcal{A}_n^{ij},\mathcal{A}_n^{ij}+\eta_n^{ij}+h)$ for $(i,j)\in\mathcal{E}$. Then, let $\widetilde{\Psi}^{ij}(t_0,t)=\bigcup_{n\geq\mathbb{N}^+}\widetilde{\mathcal{I}}_n^{ij}\cap[t_0,t]$, and $\widetilde{\Phi}^{ij}(t_0,t)=[t_0,t]\backslash\widetilde{\Psi}^{ij}(t_0,t)$. Note that $|\widetilde{\Phi}^{ij}(\mathcal{A}_n^{ij},t)|>0$ denotes that there exists at least one successful information transmission during $[\mathcal{A}_n^{ij},t)$. If the conclusion of Lemma 3 is false, then this implies that $|\widetilde{\Phi}^{ij}(\mathcal{A}_n^{ij},\mathcal{A}_n^{ij}+\Delta^{ij})|=0$. Next, one has $|\widetilde{\Phi}^{ij}(\mathcal{A}_n^{ij},t)|\geq(t-\mathcal{A}_n^{ij})(1-\gamma^{ij})-\mu_2^{ij}-\mu_1^{ij}h$. Assume the last transmission attempt t_1^{ij} during $[\mathcal{A}_n^{ij},\mathcal{A}_n^{ij}+\Delta^{ij}]$, and obviously, $t_1^{ij}\in\mathcal{I}_{m_0}^{ij}$ for some m_0, and $|\widetilde{\Psi}^{ij}(t_1^{ij},t_1^{ij}+h)|=0$. Due to the fact that t_1^{ij} is the last transmission attempt during $[\mathcal{A}_n^{ij},\mathcal{A}_n^{ij}+\Delta^{ij}]$, one has $t_1^{ij}+h>\mathcal{A}_n^{ij}+\Delta^{ij}$. Thus, $|\widetilde{\Psi}^{ij}(\mathcal{A}_n^{ij},t_1^{ij}+h)|\geq(t_1^{ij}+h-\mathcal{A}_n^{ij})(1-\gamma^{ij})-\mu_2^{ij}-\mu_1^{ij}h>0$. However, by hypothesis, $|\widetilde{\Psi}^{ij}(\mathcal{A}_n^{ij},t_1^{ij}+h)|=|\widetilde{\Psi}^{ij}(\mathcal{A}_n^{ij},t_1^{ij})|+|\widetilde{\Psi}^{ij}(t_1^{ij},t_1^{ij}+h)|=0$. ■

We are now ready to prove Theorem 1.

Construct the following Lyapunov function $V(t)=(1/2)\sum_{i=1}^N(x_i(t)-(1/N)\sum_{j=1}^N x_j(t))^2$. Assume $t\in[t_0+kh,t_0+(k+1)h)$, then one has

$$\dot V(t)=-\sum_{i=1}^N\left(x_i(t)-\frac{1}{N}\mathbf{1}^Tx(t)\right)\left(\sum_{(i,j)\in\mathcal{E}}y_{ij}(t)-\frac{1}{N}\mathbf{1}^TD\hat y(t)\right)$$

with $\hat y(t)=[\hat y_1(t),\hat y_2(t),\ldots,\hat y_m(t)]^T=\mathrm{col}\{y_{ij}(t),(i,j)\in\mathcal{E}\}$. According to the definition in (4), if agents i and j are connected by edge k; then, $y_{ij}(t)$ is the kth element of $\hat y(t)$, that is, $\hat y_k(t)$.

In the sample-data communication scheme (11), $t_k^{ij}=t_0+kh$ for $(i,j)\in\mathcal{E}$ with $k=0,1,\ldots$, then further, one has $\dot V(t)=-\sum_{i=1}^N x_i(t)\sum_{(i,j)\in\mathcal{E}\atop t_k^{ij}\in\Phi^{ij}(t_0,t)}(x_i(t_k^{ij})-x_j(t_k^{ij}))$. For agent i, when $t\in[t_k^{ij},t_{k+1}^{ij})$, that is, $t\in[t_0+kh,t_0+(k+1)h)$, $x_i(t)=x_i(t_k^{ij})-(t-t_k^{ij})\sum_{(i,j)\in\mathcal{E}\atop t_k^{ij}\in\Phi^{ij}(t_0,t)}(x_i(t_k^{ij})-x_j(t_k^{ij}))$ and thus

$$\begin{aligned}\dot V(t)\leq&-\frac{1}{2}\sum_{i=1}^N\sum_{(i,j)\in\mathcal{E}\atop t_k^{ij}\in\Phi^{ij}(t_0,t)}\left(x_i\left(t_k^{ij}\right)-x_j\left(t_k^{ij}\right)\right)^2\\&+\sum_{i=1}^N\left(t-t_k^{ij}\right)d_i\sum_{(i,j)\in\mathcal{E}\atop t_k^{ij}\in\Phi^{ij}(t_0,t)}\left(x_i\left(t_k^{ij}\right)-x_j\left(t_k^{ij}\right)\right)^2.\end{aligned}$$

Here, $d_i\leq N-1$, $t\in[t_0+kh,t_0+(k+1)h)$, and $t_k^{ij}=t_0+kh$. Thus, $\dot V(t)\leq-[(1/2)-h(N-1)]\sum_{(i,j)\in\mathcal{E}\atop t_k^{ij}\in\Phi^{ij}(t_0,t)}(x_i(t_k^{ij})-x_j(t_k^{ij}))^2$. Due to $h\leq(1/[2(N-1)])$, $\dot V(t)\leq0$. Then, using the LaSalle's invariance principle for hybrid systems [23], [28], $x(t)$ converges to the largest invariant set contained in $\{x\in\mathbb{R}^N|\dot V(x(t))=0\}$ with $x(t)=[x_1(t),x_2(t),\ldots,x_N(t)]^T$.

Obviously, function $V(t)$ is monotonously nonincreasing and, thus, $\lim_{t\to\infty}V(t)$ exists. Define $\{t_{k_s}^{ij}\}_{s\in\mathbb{N}^+}=\{t_k^{ij}\}_{k\in\mathbb{N}^+}\bigcap\Phi^{ij}(t_0,\infty)$, $(i,j)\in\mathcal{E}$. Note that $\dot V(t)=0$ implies that each channel (i,j) satisfies one of the following two cases: Case 1) there exists a subsequence $\{t_{k_s}^{ij}\}_{s\in\mathbb{N}^+}=\{t_k^{ij}\}_{k\in\mathbb{N}^+}\bigcap\Phi^{ij}(t_0,\infty)$ such that $x_i(t_{k_s}^{ij})-x_j(t_{k_s}^{ij})\to0$ as $s\to\infty$; that is, $\forall\varepsilon>0$, $\exists k_*^{ij}>0$, $\forall k_s>k_*^{ij}$, $|x_i(t_{k_s}^{ij})-x_j(t_{k_s}^{ij})|<\varepsilon$. Case 2) there exists a $k_\star\in\mathbb{N}^+$ such that $t_k^{ij}\in\Psi(t_0,\infty)$ for all $k\geq k_\star$. Next, we will prove that Case 2) will be excluded. According to Lemma 3, for any channel (i,j), the interval between two consecutive successful transmission attempts is less than $\Delta^{ij}+h$. Thus, one concludes that there exists a subsequence $\{t_{k_s'}^{ij}\}_{s\in\mathbb{N}^+}\subseteq\{t_k^{ij}\}_{k\in\mathbb{N}^+}$ for any channel $(i,j)\in\mathcal{E}$, such that the transmission attempt at $t_{k_s'}^{ij}$ over channel (i,j) is always successful. This means $t_{k_s'}^{ij}\in\Phi(t_0,\infty)$ for all $s\in\mathbb{N}^+$ and $(i,j)\in\mathcal{E}$. Therefore, Case 2) is excluded. That is, only Case 1) always holds for all channels. Therefore, it is concluded that $x_i(t_{k_s}^{ij})-x_j(t_{k_s}^{ij})\to0$ as $s\to\infty$ for $(i,j)\in\mathcal{E}$. The next step is to prove $\lim_{t\to\infty}x_i(t)-x_j(t)=0$ for $(i,j)\in\mathcal{E}$.

Assume that $\lim_{t\to\infty}x_i(t)-x_j(t)\neq0$, then $\exists\varepsilon_0>0$, $\forall t_*\gg\max\{t_{k_*^{ij}}^{ij}:(i,j)\in\mathcal{E}\}$, $\exists t_1>t_*$ such that $|x_i(t_1)-x_j(t_1)|>\varepsilon_0$. Note that the expressions $t_{k'}^{ij}\in\{t_{k_s}^{ij}\}_{s\in\mathbb{N}^+}$ and $t_{k'}^{ij}\in\Phi^{ij}(t_0,\infty)$ are equivalent.

Obviously, $\exists m_1 \in \mathbb{N}^+$, $t_1 \in [t_0 + m_1 h, t_0 + (m_1+1)h)$. By (11), $t_{m_1}^{ij} = t_0 + m_1 h$ for $(i,j) \in \mathcal{E}$. Note that $x_i(t_1) = x_i(t_0 + m_1 h) - [t_1 - (t_0 + m_1 h)] \sum_{\substack{(i,q)\in\mathcal{E} \\ t_{m_1}^{iq} \in \Phi^{iq}(t_0,t_1)}} (x_i(t_{m_1}^{iq}) - x_q(t_{m_1}^{iq}))$, and $x_j(t_1) = x_j(t_0+m_1 h) - [t_1 - (t_0+m_1 h)] \sum_{\substack{(j,p)\in\mathcal{E} \\ t_{m_1}^{jp} \in \Phi^{jp}(t_0,t_1)}} (x_j(t_{m_1}^{jp}) - x_p(t_{m_1}^{jp}))$.

Due to the arbitrary of ε in Case 1), choose $\varepsilon < [\varepsilon_0/(1 + 2\tilde{d}hN_{\max})]$, then the existence of k_*^{ij} can be guaranteed. Here, $\tilde{d} = \max_{i\in\mathcal{V}}\{d_i\}$, $N_{\max} = \max_{(i,j)\in\mathcal{E}}\{N_{\max}^{ij}\}$, and $N_{\max}^{ij} = [(\Delta^{ij} + h)/h] + 1$.

Case a): If $t_{m_1}^{ij} \in \{t_{k_s}^{ij}\}_{s\in\mathbb{N}^+}$, then this implies that the transmission attempt $t_{m_1}^{ij}$ is successful for channel (i,j) and, thus, $|x_i(t_{m_1}^{ij}) - x_j(t_{m_1}^{ij})| = |x_i(t_0+m_1 h) - x_j(t_0+m_1 h)| < \varepsilon$. Therefore,

$$\begin{aligned}\left|x_i(t_1) - x_j(t_1)\right| \le{}& \left|x_i(t_0 + m_1 h) - x_j(t_0 + m_1 h)\right| \\ &+ [t_1 - (t_0 + m_1 h)] \\ &\times \sum_{\substack{(i,q)\in\mathcal{E} \\ t_{m_1}^{iq} \in \Phi^{iq}(t_0,t_1)}} \left|\left(x_i\left(t_{m_1}^{iq}\right) - x_q\left(t_{m_1}^{iq}\right)\right)\right| \\ &+ [t_1 - (t_0 + m_1 h)] \\ &\times \sum_{\substack{(j,p)\in\mathcal{E} \\ t_{m_1}^{jp} \in \Phi^{jp}(t_0,t_1)}} \left|\left(x_j\left(t_{m_1}^{jp}\right) - x_p\left(t_{m_1}^{jp}\right)\right)\right|. \quad (19)\end{aligned}$$

Thus, $|x_i(t_1) - x_j(t_1)| \le \varepsilon + hd_i\varepsilon + hd_j\varepsilon = [1 + (d_i + d_j)h]\varepsilon < \varepsilon_0$.

Case b): If $t_{m_1}^{ij} \notin \{t_{k_s}^{ij}\}_{s\in\mathbb{N}^+}$, then according to case a), one has $|x_i(t_1) - x_j(t_1)| \le |x_i(t_0+m_1 h) - x_j(t_0+m_1 h)| + h(d_i + d_j)\varepsilon$. By the mathematical induction method, $|x_i(t_0 + m_1 h) - x_j(t_0 + m_1 h)| \le |x_i(t_0 + sh) - x_j(t_0 + sh)| + (m_1 - s)h(d_i + d_j)\varepsilon$ with $s < m_1$ and $s \in \mathbb{N}^+$. Let t_*^{ij} with $* = \max\{k_s \in \mathbb{N}^+ : t_{k_s}^{ij} < t_1\}$ be the latest successful transmission attempt of channel (i,j) before t_1. This implies $|x_i(t_*^{ij}) - x_j(t_*^{ij})| < \varepsilon$. Note that attempt $t_{m_1}^{ij}$ is unsuccessful, and according to Lemma 3, one has $t_{m_1}^{ij} - t_*^{ij} \le h(N_{\max}^{ij} - 1)$. Thus, $|x_i(t_1) - x_j(t_1)| \le |x_i(t_*^{ij}) - x_j(t_*^{ij})| + (t_{m_1}^{ij} - t_*^{ij})(d_i + d_j)\varepsilon + h(d_i + d_j)\varepsilon \le \varepsilon + hN_{\max}^{ij}(d_i + d_j)\varepsilon < [1 + hN_{\max}^{ij}(d_i + d_j)]\varepsilon < \varepsilon_0$.

According to Case a) and Case b), one has $|x_i(t_1) - x_j(t_1)| < \varepsilon_0$, which is contradictory with $|x_i(t_1) - x_j(t_1)| > \varepsilon_0$ from the assumption of $\lim_{t\to\infty} x_i(t) - x_j(t) \neq 0$. Therefore, $\lim_{t\to\infty} x_i(t) - x_j(t) = 0$ for $\forall (i,j) \in \mathcal{E}$. Due to the connectivity of the network topology, the asymptotic consensus can be guaranteed even in the presence of distributed DoS attacks. ■

Appendix B
Proof of Theorem 2

Construct a Lyapunov function as $W(t) = V(t) + \sum_{(i,j)\in\mathcal{E}} \eta_{ij}(t) = (1/2)\sum_{i=1}^{N}[x_i(t) - (1/N)\sum_{j=1}^{N} x_j(t)]^2 + \sum_{(i,j)\in\mathcal{E}} \eta_{ij}(t)$. Define $t_k^{ij} \triangleq \max_s\{t_s^{ij} : t_s^{ij} \le t, s \in \mathbb{N}^+, (i,j) \in \mathcal{E}\}$, and according to (9) and (14), one obtains

$$\begin{aligned}\dot{W}(t) = {}& - \sum_{\substack{(i,j)\in\mathcal{E} \\ t_k^{ij} \in \Phi^{ij}(t_0,t)}} \left[x_i\left(t_k^{ij}\right) - x_j\left(t_k^{ij}\right) - e_{ij}(t)\right]^T \left(x_i\left(t_k^{ij}\right) - x_j\left(t_k^{ij}\right)\right) \\ &- \sum_{\substack{(i,j)\in\mathcal{E} \\ t_k^{ij} \in \Phi^{ij}(t_0,t)}} \left(\alpha_{ij}\eta_{ij}(t) + \xi_{ij}\left(\frac{1}{4\tilde{a}_{ij}} e_{ij}^2(t) - \tilde{\theta}_{ij}\frac{2 - \tilde{a}_{ij}}{4} y_{ij}^2\left(t_k^{ij}\right)\right)\right) \\ \le{}& - \sum_{\substack{(i,j)\in\mathcal{E} \\ t_k^{ij} \in \Phi^{ij}(t_0,t)}} \left(1 - \frac{\tilde{a}_{ij}}{2}\right)\left(x_i\left(t_k^{ij}\right) - x_j\left(t_k^{ij}\right)\right)^2 + \left(1 - \frac{\xi_{ij}}{2}\right)\frac{1}{2\tilde{a}_{ij}} e_{ij}^2 \\ &+ \sum_{\substack{(i,j)\in\mathcal{E} \\ t_k^{ij} \in \Phi^{ij}(t_0,t)}} \left(-\alpha_{ij}\eta_{ij}(t) + \xi_{ij}\tilde{\theta}_{ij}\frac{2 - \tilde{a}_{ij}}{4} y_{ij}^2\left(t_k^{ij}\right)\right)\end{aligned}$$

with $\hat{y}(t) = [\hat{y}_1(t), \hat{y}_2(t), \ldots, \hat{y}_m(t)]^T = \mathrm{col}\{y_{ij}(t), (i,j) \in \mathcal{E}\}$. According to the definition in (4), if agents i and j are connected by edge k; then, $y_{ij}(t)$ is the kth element of $\hat{y}(t)$, that is, $\hat{y}_k(t)$.

According to the dynamical event-triggered scheme (13), we can further obtain the following inequality $\dot{W}(t) \le -\sum_{\substack{(i,j)\in\mathcal{E} \\ t_k^{ij} \in \Phi^{ij}(t_0,t)}} (\alpha_{ij} - [(2 - \xi_{ij})/\beta_{ij}])\eta_{ij}(t) + (1 - \tilde{\theta}_{ij})[(2 - \tilde{a}_{ij})/2]y_{ij}^2(t_k^{ij})$. For channel $(i,j) \in \mathcal{E}$ with $t_k^{ij} \in \Phi^{ij}(t_0,t)$, note that t_k^{ij} is its latest successful transmission attempt of channel (i,j), in this case, $y_{ij}(t_k^{ij}) = z_{ij}(t_k^{ij})$, then according to (13), one has $z_{ij}^2(t) = [z_{ij}(t_k^{ij}) - e_{ij}(t)]^2 \le 2y_{ij}^2(t_k^{ij}) + 2e_{ij}^2(t) \le [2 + 2\tilde{a}_{ij}(2 - \tilde{a}_{ij})\tilde{\theta}_{ij}]y_{ij}^2(t_k^{ij}) + (8\tilde{a}_{ij}/\beta_{ij})\eta_{ij}(t)$. Then, we obtain

$$\begin{aligned}\dot{W}(t) \le{}& - \sum_{\substack{(i,j)\in\mathcal{E} \\ t_k^{ij} \in \Phi^{ij}(t_0,t)}} \left(1 - \tilde{\theta}_{ij}\right)\frac{2 - \tilde{a}_{ij}}{4\left[1 + \tilde{a}_{ij}(2 - \tilde{a}_{ij})\tilde{\theta}_{ij}\right]} z_{ij}^2(t) \\ &- \sum_{\substack{(i,j)\in\mathcal{E} \\ t_k^{ij} \in \Phi^{ij}(t_0,t)}} \left(\alpha_{ij} - \frac{2 - \xi_{ij}}{\beta_{ij}} - \frac{2\left(1 - \tilde{\theta}_{ij}\right)(2 - \tilde{a}_{ij})\tilde{a}_{ij}}{\left[1 + \tilde{a}_{ij}(2 - \tilde{a}_{ij})\tilde{\theta}_{ij}\right]\beta_{ij}}\right)\eta_{ij}(t). \quad (20)\end{aligned}$$

Obviously, $\dot{W}(t) \le 0$ due to $\alpha_{ij} > \tilde{\xi}_{ij}$, $0 < \tilde{\theta}_{ij} < 1$, and $0 < \tilde{a}_{ij} < 2$. This implies that $W(t)$ is monotonously nonincreasing and, thus, $\lim_{t\to\infty} W(t)$ exists.

For the channel (i,j), we classify the time interval $[0,\infty)$ into $\{\mathcal{S}_n^{ij}\}_{n\in\mathbb{N}^+}$ and $\{\mathcal{U}_n^{ij}\}_{n\in\mathbb{N}^+}$. Here, $\mathcal{S}_n^{ij} = [t_{n_p}^{ij}, t_{n_q}^{ij})$ and $\mathcal{U}_n^{ij} = [t_{n_q}^{ij}, t_{n_r}^{ij})$ with $t_{n_p}^{ij}, t_{n_q}^{ij}, t_{n_r}^{ij} \in \{t_k^{ij}\}_{k\in\mathbb{N}^+}$. Here, transmission attempts t_k^{ij} with $k = n_p, n_p + 1, \ldots, n_q - 1$ are successful, and the transmission attempts $t_{n_p-1}^{ij}$ and $t_{n_q}^{ij}$ are attacked and unsuccessful. And the transmission attempts t_k^{ij} with $k = n_q, n_q + 1, \ldots, n_r - 1$ are attacked and unsuccessful, and the transmission attempts $t_{n_q-1}^{ij}$ and $t_{n_r}^{ij}$ are successful.

Define $\widetilde{\eta}_{ij}$ and $\tilde{z}_{ij}(t)$ as

$$\widetilde{\eta}_{ij}(t) = \begin{cases} \eta_{ij}(t) & t \in \mathcal{S}_n^{ij}, \quad n = 1,2,\ldots \\ 0 & t \in \mathcal{U}_n^{ij}, \quad n = 1,2,\ldots \end{cases} \quad (21)$$

$$\tilde{z}_{ij}(t) = \begin{cases} z_{ij}(t) & t \in \mathcal{S}_n^{ij}, \quad n = 1,2,\ldots \\ 0 & t \in \mathcal{U}_n^{ij}, \quad n = 1,2,\ldots \end{cases} \quad (22)$$

According to (20), one obtains $\dot{W}(t) \le -\sum_{(i,j)\in\mathcal{E}}[((2 - \tilde{a}_{ij})(1 - \tilde{\theta}_{ij}))/(4[1 + \tilde{a}_{ij}(2 - \tilde{a}_{ij})\tilde{\theta}_{ij}])]\tilde{z}_{ij}^2(t) - \sum_{(i,j)\in\mathcal{E}}(\alpha_{ij} - \tilde{\xi}_{ij})\widetilde{\eta}_{ij}(t)$. It is noted that $\dot{W}(t) = 0$ if and only if $\tilde{z}_{ij}(t) = 0$ and $\widetilde{\eta}_{ij}(t) = 0$. Using LaSalle's invariance principle for hybrid systems [28], one has $\lim_{t\to\infty} \widetilde{\eta}_{ij}(t) = 0$ and $\lim_{t\to\infty} \tilde{z}_{ij}(t) = 0$ for $(i,j) \in \mathcal{E}$. Next, we further prove $\lim_{t\to\infty} \eta_{ij}(t) = 0$ and $\lim_{t\to\infty} z_{ij}(t) = 0$ for $(i,j) \in \mathcal{E}$.

The first step is to prove $\lim_{t\to\infty} \eta_{ij}(t) = 0$.

i) If $\lim_{t\to\infty} \eta_{ij}(t) \neq 0$, then $\exists \varepsilon_0 > 0$, $\forall T^{ij} (\gg \widehat{T}^{ij})$, there exists $t_3^{ij} > T^{ij}$ such that $|\eta_{ij}(t_3^{ij})| > \varepsilon_0$.

ii) From $\lim_{t\to\infty}\widetilde{\eta}_{ij}(t)=0$, choose $\varepsilon=\varepsilon_0$, $\exists\widehat{T}^{ij}>0$, $\forall t>\widehat{T}^{ij}$, and one has $|\widetilde{\eta}_{ij}(t)|<\varepsilon_0$, that is, $\forall t>\widehat{T}^{ij}$ and $t\in\mathcal{S}_n^{ij}$ for some n, the inequality $|\eta_{ij}(t)|<\varepsilon_0$ holds.

Due to $t_3^{ij}>T^{ij}\gg\widehat{T}^{ij}$ and $|\eta_{ij}(t_3^{ij})|>\varepsilon_0$; hence, $t_3^{ij}\in\mathcal{U}_p^{ij}$ for some positive integral p. According to (14), $\dot{\eta}_{ij}(t)=0$ when $t\in\mathcal{U}_n^{ij}$ with $n\in\mathbb{N}^+$. Therefore, there exists $t_{n_p}^{ij-}\in\mathcal{S}_p^{ij}$ and $t_{n_p}^{ij}\in\mathcal{U}_p^{ij}$ such that $\eta_{ij}(t_3^{ij})=\eta_{ij}(t_{n_p}^{ij})$. However, from i), $|\eta_{ij}(t_3^{ij})|>\varepsilon_0$, and from ii), $|\eta_{ij}(t_{n_p}^{ij-})|<\varepsilon_0$. Note that $\eta_{ij}(t)$ is a continuous function, then $|\eta_{ij}(t_{n_p}^{ij})|=|\eta_{ij}(t_{n_p}^{ij-})|<\varepsilon_0$. This contradiction comes from the false assumption of $\lim_{t\to\infty}\eta_{ij}(t)\neq 0$. Therefore, $\lim_{t\to\infty}\eta_{ij}(t)=0$.

The second step is to prove $\lim_{t\to\infty}z_{ij}(t)=0$.

iii) If $\lim_{t\to\infty}z_{ij}(t)\neq 0$, then $\exists\varepsilon_0>0$, $\forall T_0^{ij}$, there exists $t_4^{ij}>T_0^{ij}$ such that $|z_{ij}(t_4^{ij})|>\varepsilon_0$.

iv) Note that $\lim_{t\to\infty}\tilde{z}_{ij}(t)=0$, that is, choose $\varepsilon<\varepsilon_0/[1+2d_{\max}(\tau_{\max}+\widetilde{\Delta}_{\max})]$ with $d_{\max}=\max_{1\le i\le N}\{d_i\}$, $\tau_{\max}=\max\{\tau_k^{ij}:k\in\mathbb{N}^+,(i,j)\in\mathcal{E}\}$ and $\widetilde{\Delta}_{\max}=\max\{\widetilde{\Delta}^{ij}:(i,j)\in\mathcal{E}\}$, $\exists\widehat{T}_0^{ij}>0$, $\forall t>\widehat{T}_0^{ij}$, one has $|\tilde{z}_{ij}(t)|<\varepsilon$, that is, $\forall t>\widehat{T}_0^{ij}$ and $t\in\mathcal{S}_n^{ij}$ for some n, the inequality $|z_{ij}(t)|<\varepsilon$.

Define $T_\delta^{ij}=\min_k\{t_k^{ij}:t_k^{ij}>\widehat{T}_0^{ij},t_k^{ij}\in\bigcup_{n\in\mathbb{N}^+}\mathcal{S}_n^{ij}\}$, and $T_\delta=\max\{T_\delta^{ij}:(i,j)\in\mathcal{E}\}$. Due to the arbitrary of T_0^{ij} in iii), we choose $T_0^{ij}\gg T_\delta$, then t_4^{ij} still exists. Note that $t_4^{ij}>\widehat{T}_0^{ij}$, but $z_{ij}(t_4^{ij})>\varepsilon_0>\varepsilon$; thus, $t_4^{ij}\in\mathcal{U}_q^{ij}$ for some positive integral q.

Denote $t_{k(t)}^{ij}$ to be the latest successful transmission attempt before t. From iv), when $t>T_0^{ij}\gg\widehat{T}_0^{ij}$, according to Lemma 2, $t_{k(t)}^{ij}>\widehat{T}_0^{ij}$ and, thus, $|x_j(t_{k(t)}^{ij})-x_i(t_{k(t)}^{ij})|<\varepsilon$ for channel $(i,j)\in\mathcal{E}$. According to (9), one has $\dot{x}_i(t)=-\sum_{(i,j)\in\mathcal{E}}y_{ij}(t)$. Let $s*=\max\{k\in\mathbb{N}^+:t_k^{ij}<t_4^{ij},t_k^{ij}\in\bigcup_{n\in\mathbb{N}^+}\mathcal{S}_n^{ij}\}$. Obviously, t_{s*+1}^{ij} is the attacked transmission attempt and $[t_{s*}^{ij},t_{s*+1}^{ij})\in\mathcal{S}_{n_0}^{ij}$ for some n_0. By iv), one has $|x_i(t_{s*+1}^{ij-})-x_j(t_{s*+1}^{ij-})|<\varepsilon$. Then

$$x_i\Big(t_4^{ij}\Big)=x_i\Big(t_{s*+1}^{ij-}\Big)-\int_{t_{s*+1}^{ij-}}^{t_4^{ij}}\sum_{\substack{(i,j)\in\mathcal{E}\\ t_{k(t)}^{ij}\in\mathcal{S}_q^{ij}}}\Big(x_i^{ij}\Big(t_{k(t)}^{ij}\Big)-x_j^{ij}\Big(t_{k(t)}^{ij}\Big)\Big)dt$$

and

$$x_j\Big(t_4^{ij}\Big)=x_j\Big(t_{s*+1}^{ij-}\Big)-\int_{t_{s*+1}^{ij-}}^{t_4^{ij}}\sum_{\substack{(j,l)\in\mathcal{E}\\ t_{k(t)}^{jl}\in\mathcal{S}_q^{jl}}}\Big(x_j^{jl}\Big(t_{k(t)}^{jl}\Big)-x_l^{jl}\Big(t_{k(t)}^{jl}\Big)\Big)dt.$$

Note that $x_i(t)$ is a continuous function; therefore

$$\begin{aligned}\Big|x_i\Big(t_4^{ij}\Big)-x_j\Big(t_4^{ij}\Big)\Big|\le{}&\Big|x_i\Big(t_{s*+1}^{ij-}\Big)-x_j\Big(t_{s*+1}^{ij-}\Big)\Big|\\&+\Bigg|\int_{t_{s*+1}^{ij-}}^{t_4^{ij}}\sum_{\substack{(i,j)\in\mathcal{E}\\ t_{k(t)}^{ij}\in\mathcal{S}_q^{ij}}}\Big(x_i^{ij}\Big(t_{k(t)}^{ij}\Big)-x_j^{ij}\Big(t_{k(t)}^{ij}\Big)\Big)dt\\&-\int_{t_{s*+1}^{ij-}}^{t_4^{ij}}\sum_{\substack{(j,l)\in\mathcal{E}\\ t_{k(t)}^{jl}\in\mathcal{S}_q^{jl}}}\Big(x_j^{jl}\Big(t_{k(t)}^{jl}\Big)-x_l^{jl}\Big(t_{k(t)}^{jl}\Big)\Big)dt\Bigg|\end{aligned}$$

which implies that $|x_i(t_4^{ij})-x_j(t_4^{ij})|\le\varepsilon+(t_4^{ij}-t_{s*+1}^{ij})(d_i+d_j)\varepsilon\le[1+2d_{\max}(\tau_{\max}+\widetilde{\Delta}_{\max})]\varepsilon$ with $\tau_{\max}=\max\{\tau_k^{ij}:k\in\mathbb{N}^+,(i,j)\in\mathcal{E}\}$ and $\widetilde{\Delta}_{\max}=\max\{\widetilde{\Delta}^{ij}:(i,j)\in\mathcal{E}\}$. This implies that $|x_i(t_4^{ij})-x_j(t_4^{ij})|<\varepsilon_0$, which is contradictory to the fact of $|z_{ij}(t_4^{ij})|>\varepsilon_0$ from the assumption $\lim_{t\to\infty}z_{ij}(t)\neq 0$. Therefore, this assumption is false, and $\lim_{t\to\infty}z_{ij}(t)=0$. ■

APPENDIX C
PROOF OF THEOREM 3

For channel (i,j), if the Zeno behavior exists, then this implies that $\lim_{k\to\infty}t_k^{ij}=T_0^{ij}$. Here, $T_0^{ij}\in\bigcup\overline{\mathcal{S}_n^{ij}}$ and $\overline{\mathcal{S}_n^{ij}}$ is the closure of $\mathcal{S}_n^{ij}$. Then, choosing

$$\varepsilon<\frac{2\sqrt{\frac{\tilde{a}_{ij}\eta_{ij}(0)}{\beta_{ij}}}\exp\Big\{-\frac{1}{2}\Big(\alpha_{ij}+\frac{\xi_{ij}}{\beta_{ij}}\Big)\Big(T_0^{ij}-t_0\Big)\Big\}}{2\big(d_i+d_j\big)b_0}$$

$\exists N(\varepsilon)$ and $n_0\in\mathbb{N}^+$, $\forall k>N(\varepsilon)$, one obtains

$$t_k^{ij}\in\Big[T_0^{ij}-\varepsilon,T_0^{ij}\Big]\subseteq\mathcal{S}_{n_0}^{ij}. \tag{23}$$

From Theorem 2, $x_i(t)$ is bounded and, hence, assume $\|x_i(t)\|\le b_0$ for $i=1,2,\ldots,N$. Note that $\|z_{ij}(t)=x_i(t)-x_j(t)\|\le 2b_0$, and $\|u_i(t)=-\sum_{(i,j)\in\mathcal{E}}y_{ij}(t)\|\le 2d_ib_0$.

Next, $z_{ij}(t)-z_{ij}(t_k^{ij})=(x_i(t)-x_j(t))-(x_i(t_k^{ij})-x_j(t_k^{ij}))=\int_{t_k^{ij}}^t u_i(s)ds-\int_{t_k^{ij}}^t u_j(s)ds$ and, thus, $\|z_{ij}(t)-z_{ij}(t_k^{ij})\|\le\|\int_{t_k^{ij}}^t u_i(s)ds-\int_{t_k^{ij}}^t u_j(s)ds\|\le(t-t_k^{ij})2(d_i+d_j)b_0$.

Note that $t_k^{ij}\in\Phi^{ij}(t_0,t)$ and, thus, the next transmission attempt is determined by

$$t_{k+1}^{ij}=\max_{t\ge t_k^{ij}}\Big\{t:\beta_{ij}\Big(\frac{1}{4\tilde{a}_{ij}}e_{ij}^2(t)-\tilde{\theta}_{ij}\frac{2-\tilde{a}_{ij}}{4}y_{ij}^2\Big(t_k^{ij}\Big)\Big)\le\eta_{ij}(t)\Big\}.$$

From (14), one has $\eta_{ij}\ge\eta_{ij}(t_0)\exp\{-(\alpha_{ij}+[\xi_{ij}/\beta_{ij}])(t-t_0)\}$. One sufficient condition for the above inequality is

$$e_{ij}(t)\le 2\sqrt{\frac{\tilde{a}_{ij}\eta_{ij}(0)}{\beta_{ij}}}\exp\Big\{-\frac{1}{2}\Big(\alpha_{ij}+\frac{\xi_{ij}}{\beta_{ij}}\Big)(t-t_0)\Big\}. \tag{24}$$

Thus

$$t_{k+1}^{ij}-t_k^{ij}\ge\frac{2\sqrt{\frac{\tilde{a}_{ij}\eta_{ij}(0)}{\beta_{ij}}}\exp\Big\{-\frac{1}{2}\Big(\alpha_{ij}+\frac{\xi_{ij}}{\beta_{ij}}\Big)\Big(T_0^{ij}-t_0\Big)\Big\}}{2\big(d_i+d_j\big)b_0} \tag{25}$$

which is contradictory to (23).

Furthermore, according to (13), the case of $t_k^{ij}\in\Psi^{ij}(t_0,t)$ does not lead to Zeno behavior. This fact is due to the existence of a positive dwell time θ^{ij}. ■

REFERENCES

[1] Y. Cao, W. Yu, W. Ren, and G. Chen, "An overview of recent progress in the study of distributed multi-agent coordination," *IEEE Trans. Ind. Inf.*, vol. 9, no. 1, pp. 427–438, Feb. 2013.

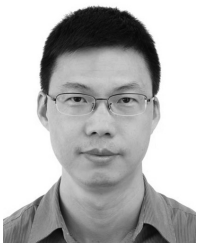
[2] S. Yang, Q. Liu, and J. Wang, "A multi-agent system with a proportional-integral protocol for distributed constrained optimization," *IEEE Trans. Autom. Control*, vol. 62, no. 7, pp. 3461–3467, Jul. 2017.

[3] 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.
[4] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Neural-network-based output-feedback control under round-Robin scheduling protocols," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/TCYB.2018.2827037.
[5] Y. Yang, D. Yue, and C. Dou, "Distributed adaptive output consensus control of a class of heterogeneous multi-agent systems under switching directed topologies," *Inf. Sci.*, vol. 345, pp. 294–312, Jun. 2016.
[6] S. Yang, J. Wang, and Q. Liu, "Cooperative-competitive multi-agent systems for distributed minimax optimization subject to bounded constraints," *IEEE Trans. Autom. Control*, to be published. doi: 10.1109/TAC.2018.2862471.
[7] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, May 2017.
[8] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal Denial-of-Service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.
[9] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *IEEE Trans. Cybern.*, vol. 48, no. 6, pp. 1862–1876, Jun. 2018.
[10] M. Zhu and S. Martínez, "On attack-resilient distributed formation control in operator-vehicle networks," *SIAM J. Control Optim.*, vol. 52, no. 5, pp. 3176–3202, 2014.
[11] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[12] C. D. 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.
[13] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.
[14] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Syst. Technol.*, to be published. doi: 10.1109/TCST.2019.2892032.
[15] W. Xu, D. W. 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.*, to be published. doi: 10.1109/TNNLS.2018.2890119.
[16] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.
[17] D. Senejohnny, P. Tesi, and C. D. Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 981–990, Sep. 2018.
[18] Z. Feng and G. Hu, "Distributed tracking control for multi-agent systems under two types of attacks," in *Proc. 19th World Congr. Int. Fed. Autom. Control*, vol. 19, 2014, pp. 5790–5795.
[19] W. Yu, W. X. Zheng, G. Chen, W. Ren, and J. Cao, "Second-order consensus in multi-agent dynamical systems with sampled position data," *Automatica*, vol. 47, no. 7, pp. 1496–1503, 2011.
[20] A. Girard, "Dynamic triggering mechanisms for event-triggered control," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1992–1997, Jul. 2015.
[21] X. Yi, K. Liu, D. V. Dimarogonas, and K. H. Johansson, "Distributed event-triggered control for multi-agent systems," *arXiv:1704.05434*.
[22] Y. Yang, D. Yue, and C. Xu, "Dynamic event-triggered leader-following consensus control of a class of linear multi-agent systems," *J. Frankl. Inst.*, vol. 355, no. 15, pp. 7706–7734, 2018.
[23] 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.
[24] W. Xu, D. W. C. Ho, J. Zhong, and B. Chen, "Distributed edge event-triggered consensus protocol of multi-agent systems with communication buffer," *Int. J. Robust Nonlin. Control*, vol. 27, no. 3, pp. 483–496, 2017.
[25] F. Xiao, X. Meng, and T. Chen, "Average sampled-data consensus driven by edge events," in *Proc. 31st Chin. Control Conf.*, Hefei, China, 2012, pp. 6239–6244.
[26] X. Meng and T. Chen, "Event based agreement protocols for multi-agent networks," *Automatica*, vol. 49, no. 7, pp. 2125–2132, 2013.
[27] C. D. Persis and P. Frasca, "Robust self-triggered coordination with ternary controllers," *IEEE Trans. Autom. Control*, vol. 58, no. 12, pp. 3024–3038, Dec. 2013.
[28] J. Lygeros, K. H. Johansson, S. N. Simic, J. Zhang, and S. S. Sastry, "Dynamical properties of hybrid automata," *IEEE Trans. Autom. Control*, vol. 48, no. 1, pp. 2–17, Jan. 2003.

Wenying Xu received the M.S. degree in applied mathematics from Southeast University, Nanjing, China, in 2014 and the Ph.D. degree in applied mathematics from the City University of Hong Kong, Hong Kong, in 2017.

From 2017 to 2018, she was a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. She was an Academic Visitor with Brunel University London, Uxbridge, U.K., in 2015, for four months, and was also a Senior Research Associate with the Department of Mathematics, City University of Hong Kong in 2018, for three months. She is currently an Assistant Professor with the School of Mathematics, Southeast University. Her current research interests include distributed event-triggered control, distributed cooperative control, and cyber-physical systems.

Dr. Xu was a recipient of the Outstanding Master Degree Thesis Award from Jiangsu Province, China, in 2015 and the Alexander von Humboldt Fellowship in 2018.



Guoqiang Hu (M'08) received the B.Eng. degree in automation from the University of Science and Technology of China, Hefei, China, in 2002, the M.Phil. degree in automation and computer-aided engineering from the Chinese University of Hong Kong, Hong Kong, in 2004, and the Ph.D. degree in mechanical engineering from the University of Florida, Gainesville, FL, USA, in 2007.

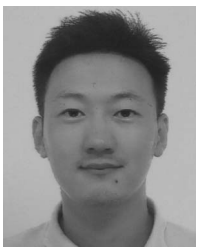
He joined the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2011, where he is currently a Tenured Associate Professor and the Director of the Centre for System Intelligence and Efficiency. He was an Assistant Professor with Kansas State University, Manhattan KS, USA, from 2008 to 2011. His current research interests include distributed control, distributed optimization, and game theory with applications to energy and robotic systems.

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

Daniel W. C. Ho (M'88–SM'05–F'17) received the B.S., M.S., and Ph.D. degrees in mathematics from the University of Salford, Greater Manchester, U.K., in 1980, 1982, and 1986, respectively.

From 1985 to 1988, he was a Research Fellow with the Industrial Control Unit, University of Strathclyde, Glasgow, U.K. He joined the City University of Hong Kong, Hong Kong, in 1989, where he is currently a Chair Professor of applied mathematics. He has over 200 publications in scientific journals. His current research interests include control and estimation theory, complex dynamical distributed networks, multiagent networks, and stochastic systems.

Dr. Ho was a recipient of the Chang Jiang Chair Professor awarded by the Ministry of Education, China, in 2012 and the Highly Cited Researchers Award in Engineering by Clarivate Analytics in the past five years. He has been on the editorial board of a number of journals, including the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, *IET Control Theory and Its Applications*, the *Journal of the Franklin Institute*, and the *Asian Journal of Control*.



Zhi Feng received the M.Sc. degree in control engineering from the Dalian University of Technology, Dalian, China, in 2012 and the Ph.D. degree in control engineering 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 at the 14th IEEE International Conference on Information and Automation in 2017.