Event/Self-Triggered Control for Leader-Following Consensus Over Unreliable Network With DoS Attacks

Wenying Xu, Daniel W. C. Ho, *Fellow, IEEE*, Jie Zhong, and Bo Chen, *Member, IEEE*

***Abstract*— This paper investigates the leader-following consensus issue with event/self-triggered schemes under an unreliable network environment. First, we characterize network communication and control protocol update in the presence of denial-of-service (DoS) attacks. In this situation, an event-triggered communication scheme is first proposed to effectively schedule information transmission over the network possibly subject to malicious attacks. In this communication framework, synchronous and asynchronous updated strategies of control protocols are constructed to achieve leader-following consensus in the presence of DoS attacks. Moreover, to further reduce the cost induced by event detection, a self-triggered communication scheme is proposed in which the next triggering instant can be determined by computing with the most updated information. Finally, a numerical example is provided to verify the effectiveness of the proposed communication schemes and updated strategies in the unreliable network environment.**

***Index Terms*— Denial-of-service (DoS) attack, event triggered, multiagent system, self-triggered.**

I. Introduction

THE past decade has witnessed a growing research interest on multiagent systems due to its wide applications in many real-world engineering systems including unmanned air vehicles, wireless sensor networks, distributed robot systems, and networked cyber-physical systems. Consensus is an important collective behavior of multiagent systems, and there have been abundant and excellent research results on consensus issues such as [1]–[10]. Recently, there has been literature which extends the results of consensus to more general systems and network structures such as [5], [11]–[13].

To complete a task in a collaborative fashion, the following two factors are necessary: 1) efficient communication among agents. The efficient communication ensures that sufficient information exchange among agents, and is also a precondition of the design of control protocols and 2) effective control protocol. The effective control protocol can be used to adjust the behavior of the agent such that the common task/goal can be completed in a collaborative fashion. This control protocol is generally designed with the available information via local communication. Recently, the event-triggered idea has been proposed in multiagent systems as an alternative method. This idea has been applied into the design of both communication schemes and control protocols with the advantages of mitigating energy consumption. Then, different types of event-triggered communication schemes and event-triggered control protocols have been constructed [14]–[17]. Under these kinds of communication schemes, the communication frequency is significantly reduced, and meanwhile, the event-triggered control protocol can lower the update frequency of controller.

As it is known, almost all of the existing results on event-triggered schemes have been investigated in perfect network environment [14]–[16]. As networks evolve, the transmission of a lot of important information is dependent upon network communication technology, and, hence network security issue becomes a big concern to the public. Recently, various kinds of network attacks arise for different purposes. One common type of cyberattacks is denial-of-service (DoS) attack, and its attempt is to block traffic, such that network resource is unavailable to its intended users. Obviously, the effect of DoS attack on the network communication is the packet dropout. It is well known that the issues of packet dropout have been extensively investigated for many systems in different situations. However, the packet dropout in previous works is always assumed to follow a probability distribution. Under this assumption, many excellent control methods and design technologies have been developed [7], [18]–[20]. Unfortunately, this is not always the case. In the research area of cybersecurity, it is hardly justified that the communication failures, induced by DoS attacks, follow a given class of probability

Manuscript received January 3, 2018; revised April 16, 2018 and August 2, 2018; accepted December 20, 2018. This work was supported in part by the Research Grants Council of the Hong Kong Special Administrative Region under Grant CityU 11200717 and Grant CityU7005029, 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 and Grant 61673351, in part by the Alexander von Humboldt Foundation of Germany, and in part by ZhiShan Youth Scholar Program from Southeast University. *(Corresponding author: Wenying Xu.)*

W. Xu is with the School of Mathematics, Southeast University, Nanjing 210096, China, and also with the Department of Mathematics, City University of Hong Kong, Hong Kong (e-mail: wenyingxuwinnie@gmail.com).

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

J. Zhong is with the College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China, and also with the Department of Mathematics, City University of Hong Kong, Hong Kong (e-mail: zhongjie0615@gmail.com).

B. Chen is with the Department of Automation, Zhejiang University of Technology, Hangzhou 310023, China, and also with the Institute of Cyberspace Security, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: bchen@aliyun.com).

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/TNNLS.2018.2890119

distribution [21]. In practice, it may not be feasible for the defender to assume that the packet dropouts (induced by the attacks) follow a given class of probability distribution. This is mainly due to the following two reasons: 1) *from the adversaries' perspectives*: the attack resource (energy) is unavoidably limited, and thus the adversaries need to determine when to launch the attacks by simultaneously considering the residual resource and the strategy of energy supply. Therefore, the DoS attacks launched by adversaries may not necessarily follow a given class of probability distribution and 2) *from the viewpoint of the defender*: the defenders hardly obtain the information of the adversaries. Thus, even if the attacks seem to follow a given class of probability distribution, the information is not available to the defender. Based on the above two practical reasons, in this paper, we attempt to explore new methods without using probability distribution information.

Recently, some results have been reported in the literature concerning the stability analysis, control, filtering, and attack detection problems of *networked control systems* subject to DoS attacks (see [21]–[27]). For example, a framework of the input-to-state stability is built for a closed-loop system in the presence of DoS attacks in [21]. Then, a unified game approach is proposed in [23] for the resilient control of a networked control system under DoS attacks. Nevertheless, the destructive effect of DoS attacks has not received adequate attention yet for distributed cooperation of multiagent systems [28], [29], not to mention the case where event-triggered schemes are taken into account to save resources as much as possible.

Summarizing the above-mentioned discussions, this paper is concerned with the design and implementation of both the communication scheme and control protocol in an event-triggered fashion for multiagent systems with DoS attacks. We endeavor to answer the following questions: (Q1) *how to develop a synergistic method to solve the distributed cooperation problem of multiagent system by simultaneously considering the constraints of limited communication resources and unreliable communication environment?* (Q2) *how to determine the next instant for communication when the information transmission is subject to DoS attacks?* (Q3) *how to update the control protocol when communication is interrupted?* By investigating the above-mentioned questions, some fundamental results are developed and the main contributions of this paper are summarized as follows: 1) *a novel theoretical framework of event/self-triggered scheme is developed in an unreliable network setting to mitigate energy consumption of communication and the control protocol update on the premise of achieving leader-following consensus;* 2) *two different kinds of triggered communication schemes are constructed to cope with the adverse effect of DoS attacks on the network communication; and* 3) *by applying the concepts information theory and triggered control, two efficient and robust update strategies are designed for the control protocols of agents to achieve the desired cooperative behavior in the unreliable communication environment.* Finally, we analyze the effect of attack strategy and event/self-triggered communication scheme on the information transmission over the network.

The rest of this paper is organized as follows. In Section II, the problem statement and the preliminaries of the basic graphs and matrices theory are provided. Sections III and IV discuss two kinds of updated strategies of consensus protocols, respectively, based on event-/self-triggered communication schemes. Section VI discusses the effect of some parameters on leader-following consensus. Furthermore, Section VII provides a numerical example to verify the effectiveness of the defense strategies. Then, this paper is finally concluded in Section VIII.

The following notations will be used throughout this paper. First, denote $\mathbb{R}^n$ to be a set of all n dimensional real column vectors. Let $[p_{ij}]_{n\times m}$ be a $n \times m$ matrix with an element p_{ij} in row i and column j. I_n represents n-dimension unit matrix. In addition, $\|\cdot\|$ refers to 2-norm for vectors or the induced 2-norm for matrices. For any matrix M, $\lambda_{\min}(M)$ and $\lambda_{\max}(M)$, respectively, denote its corresponding smallest and largest eigenvalues.

II. Problem Statement and Preliminaries

A. Preliminaries

A directed graph $\bar{\mathcal{G}} = \{\bar{\mathcal{V}}, \bar{\mathcal{E}}\}$ consists of a node set $\bar{\mathcal{V}} = \{0, 1, 2, \ldots, N\}$ and an edge set $\bar{\mathcal{E}} \subseteq \bar{\mathcal{V}} \times \bar{\mathcal{V}}$. Its subgraph $\mathcal{G}$ is an undirected graph consisting of a node subset $\mathcal{V} = \{1, 2, \ldots, N\}$ and an edge subset $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. Graph $\mathcal{G}$ is allowed to have several components, and all the agents in each component are connected via undirected edges in some topologies. Graph $\bar{\mathcal{G}}$ is said to be connected if at least one agent in each component of $\mathcal{G}$ is connected to the leader by a directed edge.

In graph $\mathcal{G}$, if an undirected edge exists between nodes i and j, then $(i, j) \in \mathcal{E}$, $l_{ij} = -1$, and node j is called a neighbor of node i and vice versa; if no edge exists between nodes i and j, then $(i, j) \notin \mathcal{E}$ and $l_{ij} = 0$. The set $\mathcal{N}_i$ includes all neighbors of node i. Furthermore, define the Laplacian matrix $\mathcal{L} = [l_{ij}]_{N\times N}$ with $l_{ii} = -\sum_{j\in\mathcal{N}_i} l_{ij}$. Then, define a diagonal matrix $\mathcal{D} = \text{diag}\{d_1, d_2, \ldots, d_N\}$, where $d_i = 1$ if there is a direct edge from the leader to node i; otherwise, $d_i = 0$. Moreover, define $H = \mathcal{L} + \mathcal{D}$ and its eigenvalues can be set in increasing order $0 \le \lambda_1 \le \lambda_2 \le \cdots \le \lambda_N$.

Lemma 1 [30]: The matrix H is positive semidefinite. In addition, the matrix H is positive definite if and only if the graph $\bar{\mathcal{G}}$ is connected.

B. Problem Formulation

Consider a class of multiagent systems involving a leader labeled as node 0 with dynamics

$$\dot{x}_0(t) = Ax_0(t) \tag{1}$$

and N followers ($i = 1, 2, \ldots, N$) with dynamics

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t). \tag{2}$$

Here, $x_i(t) \in \mathbb{R}^n$ denotes the state of agent i at time t, and $u_i(t) \in \mathbb{R}^m$ is its control protocol. Also, A and B are the known matrices with compatible dimensions, and the pair (A, B) is stabilizable.

The conventional control protocol for the systems (1) and (2) is generally designed in the secure network setting with the form of

$$\begin{aligned} u_i(t) &= K_c q_i(t) \\ q_i(t) &= \sum_{j\in\mathcal{N}_i}(x_j(t)-x_i(t)) + d_i(x_0(t)-x_i(t)). \end{aligned} \tag{3}$$

For agent i, its control protocol $u_i(t)$ can be designed with local information from its neighboring agents.

Owing to simultaneously considering the influence from malicious DoS attacks and constraint of limited communication resources, the tradition control (3) is hardly extended to cater for this situation. Therefore, in this paper, we endeavor to explore an efficient and robust control protocol $u_i(t)$ to reduce the frequency of communication and control protocol update on the premise of guaranteeing leader-following consensus with DoS attacks.

Let us define some notations and concepts of DoS attacks, which will be used in the following analysis. Some of the following notations and concepts can be found in [21].

Let $\{\mathcal{A}_k\}_{k\geq 0}$ denote a time sequence when the adversaries launch DoS attacks. DoS attacks are primarily intended to affect the timeliness of the information exchange, i.e., to cause packet losses [21]. To be specific, the launched attack instant $\mathcal{A}_k$, and its dwell time η_k jointly determine the time interval of attack effect, i.e., $[\mathcal{A}_k, \mathcal{A}_k+\eta_k)$. During $[\mathcal{A}_k, \mathcal{A}_k+\eta_k)$, the adversaries attack some or all channels of communication, and, thus, the information transmitted over the attacked channels during this interval will be lost and cannot be successfully transmitted to the intended agent. Moreover, if the next attack instant $\mathcal{A}_{k+1}\in[\mathcal{A}_k, \mathcal{A}_k+\eta_k]$, then such two attacks are called continual attacks. In this case, the communication network is under attack during $[\mathcal{A}_k, \mathcal{A}_{k+1}+\eta_{k+1})$.

Define $\Phi(t)=\bigcup_{\mathcal{A}_k\in[t_0,t]}[\mathcal{A}_k, \mathcal{A}_k+\eta_k)\cap[t_0,t]$, $\Psi(t)=[t_0,t]\backslash\Phi(t)$. Here, t_0 is the initial time. $\Phi(t)$ means the union of time intervals belonging to $[t_0,t]$, in which network communication is subject to successful attacks; and $\Psi(t)$ denotes the union of time intervals belonging to $[t_0,t]$, in which the network communication is free from attacks.

We now state our problem as follows.

Problem 1: Given multiagent systems (1) and (2) in the unreliable network environment with DoS attacks, for agent i, $(i=1,2,\ldots,N)$, this paper aims to design an appropriate control protocol $u_i(t)$ with an efficient communication scheme, such that, the leader-following consensus can be achieved asymptotically, i.e., $\lim_{t\to+\infty}x_i(t)-x_0(t)=0$ holds for any initial condition $x_0(t_0)$, $x_i(t_0)$, and the initial time t_0.

C. Event-Triggered Scheme

Event-triggered scheme has been proven to be suitable for multiagent system subject to limited network resources [15], [31]–[33]. This paper further investigates the event-triggered scheme in an unreliable network environment to achieve the desired behavior as well as to reduce the frequency of communication and control protocol update.

First, we introduce an event-triggered scheme in perfect network environment without attacks. Define a triggering time sequence $t_0<t_1<\cdots<t_k<\cdots$. For agent i, $x_i(t)=x_i(t_k)$, and $u_i(t)=u_i(t_k)$ when $t\in[t_k,t_{k+1})$. In this case, one finds that agents will transmit their information to their neighboring agents and update their control protocol only at triggering instant t_k. Obviously, the next task is to design an appropriate event condition to determine the triggering time sequence, and some effective event conditions have proposed in [15] and [31]–[33].

Let us return our discussion to the unreliable network environment. One finds that the information transmission at triggering instants is possibly subject to DoS attacks such that the transmitted information is lost. Hence, it is desirable to find a new way to update the control protocols and determine the next triggering instant for information transmission. These issues are not well addressed in the existing literature. In this paper, we focus on the event-triggered problems of multiagent systems in the unreliable network setting.

For the purpose of introducing the event-triggered scheme in the unreliable network environment, we first introduce two concepts, i.e., *successful attack* and *unsuccessful attack*. Assume the kth attack $\mathcal{A}_k$ and its dwell time η_k, if $[\mathcal{A}_k, \mathcal{A}_k+\eta_k)\cap\{t_p\}_{p\geq 0}\neq\varnothing$, then this attack is called as the *successful attack*; if $[\mathcal{A}_k, \mathcal{A}_k+\eta_k)\cap\{t_p\}_{p\geq 0}=\varnothing$, then this attack is called as the *unsuccessful attack*. Obviously, the successful (or unsuccessful) attack depends on whether there exists transmitted information being successfully attacked (or not).

To clearly describe the effect of DoS attack on the evolution of multiple agents' behaviors, define an edge set $\mathcal{A}^e(t)=\{\text{edge }(i,j)\in\bar{\mathcal{E}}\mid \text{The information transmission over edge}(i,j)\text{ is successfully attacked at time }t\}$, and a node set $\mathcal{A}^n(t)=\{i,j\in\bar{\mathcal{V}}\mid \text{The edge }(i,j)\in\mathcal{A}^e(t)\}\setminus\{0\}$. The edge set $\mathcal{A}^e(t)$ includes the edges subject to successful attack at time t, and the node set $\mathcal{A}^n(t)$ includes the nodes whose control protocol's update is affected by the attack at time t. In addition, let $n(t_0,t)$ denote the number of communication failures caused by successful attacks during $[t_0,t]$, in other words, $n(t_0,t)$ is the number of elements of the set $\{t_k,k\geq 0\mid t_k\in\Phi(t_0,t)\}$. In addition, $\xi(t_0,t)=n(t_0,t)/(t-t_0)$ means the frequency of communication failures caused by successful attacks during $[t_0,t]$. Moreover, denote ϑ to be maximum allowable number of successive communication failures caused by successful attacks. For example, assume that two successive communication failures over network, respectively, at instants t_p and t_{p+1}, are subject to successful attacks; meanwhile, the information is successfully transmitted at t_{p-1} and t_{p+2}. In this case, the number of successive communication failures caused by successful attacks is two.

Remark 1: In a *reliable* network environment, event-triggered schemes have been widely investigated in the literature, such as [14], [15], [32], [34], [35]. When it comes to an unreliable communication network, there are very few work on event-triggered schemes for cooperation of multiple agents. In an unreliable network environment, DoS attacks could exist, and thus the information transmission between agents could be attacked. Then, the necessary information update will be unsuccessful. In this case, the existing event-triggered communication schemes and the corresponding control update mechanisms will be invalid. This motivates us to develop new

event-triggered communication schemes and control protocols applicable to an unreliable network environment.

For convenience of analysis, define $e_i(t) = q_i(t_k) - q_i(t)$ when $t \in [t_k, t_{k+1})$, $\delta_i(t) = x_i(t) - x_0(t)$, $e(t) = [e_1^T(t), e_2^T(t), \ldots, e_N^T(t)]^T$, and $\delta(t) = [\delta_1^T(t), \delta_2^T(t), \ldots, \delta_N^T(t)]^T$.

First, an event condition is proposed with $\sigma > 0$ as

$$\sum_{i=1}^{N} e_i^T(t)e_i(t) \le \sigma \left\{ \frac{1}{2}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i}[x_i(t)-x_j(t)]^T[x_i(t)-x_j(t)] + \sum_{i=1}^{N} d_i[x_i(t)-x_0(t)]^T[x_i(t)-x_0(t)] \right\}. \tag{4}$$

Assumption 1: The communication topology $\bar{\mathcal{G}}$ is connected in the absence of DoS attack.

III. Event-Triggered Defense Strategy

In this section, we will further consider the strategies on determining the time sequence for communication and of updating the control protocols in the unreliable network environment.

First, a triggering time sequence is proposed to determine communication instants under DoS attacks

$$t_{k+1} = \begin{cases} \inf\{t > t_k \mid \text{Eq. (4) is violated}\} & t_k \notin \Phi(t) \\ t_k + \theta & t_k \in \Phi(t) \end{cases} \tag{5}$$

with a constant $\theta > 0$. The triggering scheme (5) provides a method to determine the next triggering instant of communication in the unreliable network setting.

Remark 2: The DoS attack detection techniques have been well investigated in [36], in which various methods are proposed to effectively detect DoS attacks. Therefore, in this paper, we assume that the attacks can always be detected, and focus on how to design and analyze event-triggered communication scheme and control protocols against them.

Next, we discuss two strategies of the control protocol update in communication scheme (5) for achieving leader-following consensus in unreliable network environment with DoS attacks.

A. Synchronous Update Strategy

In this section, a synchronous update strategy of the event-triggered control protocol is proposed. In this strategy, all agents take the same action once the network is subject to successful attacks.

Specifically, in the situation of involving malicious attacks, the synchronous update strategy of the event-triggered control protocol $u_i(t)$, $(i = 1, 2, \ldots, N)$, is with the following form:

$$\begin{cases} u_i(t) = K_1 q_i(t_k), & t \in [t_k, t_{k+1}) \\ u_i(t_{k+1}) = \begin{cases} K_1 q_i(t_{k+1}), & t_{k+1} \notin \Phi(t) \\ u_i(t_k), & t_{k+1} \in \Phi(t) \end{cases} \end{cases} \tag{6}$$

where $q_i(t)$ is defined in (3), and the matrix K_1 will be designed subsequently.

According to the event-triggered communication scheme (5), agents send information to their neighboring agents at triggering instants t_k, $(k = 0, 1, 2, \ldots)$. During the time interval $[t_k, t_{k+1})$, no information is transmitted over the network, and correspondingly, the agents' control protocols $u_i(t_k)$ $(i \in \mathcal{V})$ keep unchanged. At the next triggering instant t_{k+1}, agents attempt to exchange information with neighbors and update their control protocols. If the network is secured at t_{k+1} without DoS attacks, which implies that agents successfully exchange information, then their control protocols are updated with $u_i(t_{k+1}) = K_1 q_i(t_{k+1})$ for $i \in \mathcal{V}$. If the network is subject to successful attacks at instant t_{k+1}, which means some transmitted information is lost, then the protocols of all agents remain the same with those in the last instant according to (6).

An error system is obtained as

$$\dot{\delta}_i(t) = A\delta_i(t) + BK_1\sum_{j\in\mathcal{N}_i}(\delta_j(t_k) - \delta_i(t_k)) - d_i\delta_i(t_k) \tag{7}$$

for $i = 1, 2, \ldots, N$, and t_k is the latest instant of successful communication over the network before t, i.e., $t_k = \max_{s\ge 0}\{t_s < t | t_s \notin \Phi(t)\}$.

Since the pair (A, B) is stabilizable, then there exists a positive-definite matrix P_1 and $m_1 > 0$ such as

$$A^T P_1 + P_1 A - (2\lambda_1 - \gamma_1)P_1 B B^T P_1 + m_1 I_n < 0 \tag{8}$$

where $0 < \gamma_1 < 2\lambda_1$, and λ_1 is defined in Section II-A. The matrix K_1 in (6) is designed as

$$K_1 = B^T P_1. \tag{9}$$

For the matrix P_1 determined in (8), and $\mu_1 = \lambda_{\max}(P_1 B B^T P_1)$, there exists a positive number $\hat{\beta}_1$ to satisfy

$$\begin{aligned} A^T P_1 + P_1 A - \nu P_1 B B^T P_1 &\le \frac{\hat{\beta}_1}{2} I_n \\ \frac{\mu_1}{\nu_2}[\sigma(1 + 1/\nu_2)H + 2(1 + \nu_2)H^T H] &\le \frac{\hat{\beta}_1}{2} I_N \end{aligned} \tag{10}$$

where $\nu = 2\lambda_1 - \nu_1 - 2(1 + \nu_2)\lambda_N^2/\nu_1$, $\nu_i > 0$ $(i = 1, 2)$, $0 < \sigma < m_1\gamma_1/(\lambda_N\mu_1)$, λ_N, and the matrix H are defined in Section II-A.

Next, Proposition 1 will be presented to prove that the leader-following consensus of multiagent systems in an unreliable network under the event-triggered communication scheme (5) and the synchronous update strategy (6).

Proposition 1: Consider multiagent systems (1) and (2) with an event-triggered control protocol (6) and a triggering sequence (5). Suppose that Assumption 1 holds, the matrix K_1 is given in (9), the matrix P_1 and the parameter $\hat{\beta}_1$ satisfy (8) and (10), respectively. Under the DoS attacks, the leader-following consensus can be asymptotically achieved, if

$$\xi(t_0, t) \le \frac{\alpha_1 - \rho_1}{(\alpha_1 + \beta_1)\theta} \tag{11}$$

with $0 < \vartheta \le \varpi$, $\alpha_1 = (m_1 - \hat{m}_1)/\lambda_{\max}(P_1)$, $\beta_1 = \hat{\beta}_1/\lambda_{\min}(P_1)$, and $0 < \rho_1 < \alpha_1$. In addition, Zeno behavior can be excluded under the event-triggered scheme (5).

Proof: The proof is given in Appendix A. □

Remark 3: From (11), the upper bound of $\xi(t,t_0)$ is $(\alpha_1-\rho_1/(\alpha_1+\beta_1)\theta)$. Obviously, this upper bound increases if α_1 increases or β_1 decreases; and this upper bound decreases if α_1 decreases or β_1 increases. Note that $\alpha_1=(m_1-\hat{m}_1)/\lambda_{\max}(P_1)$ and $\beta_1=\hat{\beta}_1/\lambda_{\min}(P_1)$, and thus, this upper bound depends on the choice of matrix P_1. It could be concluded that if $\lambda_{\max}(P_1)$ decreases or $\lambda_{\min}(P_1)$ increases, then the upper bound of $\xi(t_0,t)$ increases; if $\lambda_{\max}(P_1)$ increases or $\lambda_{\min}(P_1)$ decreases, then this upper bound decreases.

Remark 4: Note that in this section, under the synchronous update strategy (6), all agents do not update their control protocols once the network communication suffers from successful attacks. Yet, from the perspective of energy consumption, the adversaries hardly attack all of network channels all the time. Thus, in many practical situations, there will be at least one unaffected agent successfully exchanging information with its neighbors even though the attack is successful. Next, we need to address the issue of whether this unaffected agent updates its control protocol. We shall investigate this issue in the following session.

B. Asynchronous Update Strategy

In this section, an asynchronous update strategy of the control protocol is proposed. For each successful attack, we further classify agents into two groups: 1) the affected agents and 2) the unaffected agents. In this case, although the network communication suffers from the successful attack, there may be some agents unaffected by this attacks. Here, these unaffected agents are allowed to normally update their control protocols.

Thus, an asynchronous update strategy of the event-triggered control protocol is proposed in a network environment with DoS attacks

$$\begin{cases} u_i(t)=K_2q_i(t_k), \quad t\in[t_k,t_{k+1}) \\ u_i(t_{k+1})=\begin{cases} K_2q_i(t_{k+1}), & t_{k+1}\notin\Phi(t) \\ u_i(t_k), & t_{k+1}\in\Phi(t)\ \&\ i\in\mathcal{A}^n(t) \\ K_2q_i(t_{k+1}), & t_{k+1}\in\Phi(t)\ \&\ i\notin\mathcal{A}^n(t) \end{cases} \end{cases} \tag{12}$$

where $q_i(t)$ is defined in (3), and the matrix K_2 will be designed subsequently.

Since the pair (A,B) is stabilizable, then there exists a positive-definite matrix P_2 and $m_2>0$ such as

$$A^TP_2+P_2A-(2\lambda_1-\gamma_2)P_2BB^TP_2+m_2I_n<0 \tag{13}$$

where $0<\gamma_2<2\lambda_1$, and λ_1 is defined in Section II-A. The matrix K_2 in (12) is designed as

$$K_2=B^TP_2. \tag{14}$$

For the matrix P_2 in (13) and $\mu_2=\lambda_{\max}(P_2BB^TP_2)$, there exists a positive number $\hat{\beta}_2$ to satisfy

$$\begin{aligned} A^TP_2+P_2A-\iota P_2BB^TP_2 &\le \frac{\hat{\beta}_2}{\varpi+1}I_n \\ \frac{\mu_2}{\iota_1}[(1+1/\iota_2)\sigma H+2(1+\iota_2)H^TH] &\le \frac{\hat{\beta}_2}{\varpi+1}I_n \end{aligned} \tag{15}$$

where $\iota=2\lambda_1-\iota_1-2(1+\iota_2)\lambda_N^2/\iota_1$, $\iota_i>0$ $(i=1,2)$, $\varpi>0$, $0<\sigma<m_2\gamma_2/(\lambda_N\mu_2)$, λ_N, and the matrix H are defined in Section II-A.

Theorem 1: Consider multiagent systems (1) and (2) with an event-triggerd control protocol (12) and a triggering sequence (5). Suppose that Assumption 1 holds, the matrix K_2 is designed in (9), the matrix P_2 and $\hat{\beta}_2$ satisfy (13) and (15), respectively. In the presence of DoS attacks, the leader-following consensus can be asymptotically achieved, if

$$\xi(t_0,t)\le\frac{\alpha_2-\rho_2}{(\alpha_2+\beta_2)\theta} \tag{16}$$

and $\vartheta\le\varpi$, $\alpha_2=((m_2-\hat{m}_2)/\lambda_{\max}(P_2))$, $\beta_2=\hat{\beta}_2/\lambda_{\min}(P_2)$, and $0<\rho_2<\alpha_2$. In addition, Zeno behavior can be excluded under the event-triggered scheme (5).

The proof is given in Appendix B.

Remark 5: The second equality of (10) and (15) could be rewritten in a simplified version, respectively, as

$$\begin{aligned} \frac{\mu_1}{\nu_2}[\sigma(1+1/\nu_2)\lambda_N+2(1+\nu_2)\lambda_N^2] &\le \frac{\hat{\beta}_1}{2} \\ \frac{\mu_2}{\iota_1}[(1+1/\iota_2)\sigma\lambda_N+2(1+\iota_2)\lambda_N^2] &\le \frac{\hat{\beta}_2}{\varpi+1} \end{aligned}$$

with λ_N being the largest eigenvalue of the matrix H. Under the above conditions, the results of Proposition 1 and Theorem 1 still hold.

We have to admit that both the Laplacian matrix and its eigenvalue information could belong to the global information to some degree. As we know, it is a difficult problem to realize fully distributed control for general linear multiagent systems without using any global information. Most of the existing results on distributed control of multiagent systems involve, more or less, some global information, such as the Laplacian matrix associated with the network structure [37], [38], or its eigenvalue information [14], [32], [39]. In some cases, an adaptive method proposed in [40] is a good method to avoid the utilization of eigenvalue information to realize fully distributed control. However, it is hard to extend the adaptive method to deal with the imperfect communication cases, such as event-triggered communication or insecure communication environment. Therefore, it is extremely difficult to achieve fully distributed event-triggered control over an unreliable network, which will require further investigation in our future works.

In particular, multiple time scales are used to describe the distributed event-triggered communication over different channels. Then, the involvement of DoS attacks leads to much complex modes of network communication. In this case, how to analyze and quantize the effect of DoS attacks on the whole multiagent systems by using only local information? In addition, how to choose parameters θ_i $(i=1,2,\ldots,N)$ instead of θ in (5) or (17) for different agents in a distributed fashion? How to design an effective update mechanism for the control protocol $u_i(t)$ such that the final collective behaviors can be guaranteed? These are still open problems and need further study.

Remark 6: Proposition 1 and Theorem 1, respectively, present that the leader-following consensus can be achieved

in an unreliable network setting by using the synchronous and asynchronous update strategies of event-triggered control protocols (6) and (12). These two strategies are developed under the event-triggered scheme (5). In (5), one finds that $x_i(t)$ and $x_j(t)$ are necessary to determine the next triggering instant for communication. Therefore, although the update frequency of the control protocol is reduced under the scheme (5), the continuous communication and the frequent event detection are hardly avoided to determine the next triggering instant. In order to overcome these flaws, a self-triggered scheme will be discussed in Section IV.

IV. Self-Triggered Defense Strategy

To avoid the requirement of frequent event detection involving available current states of agents [see (5)] for determining the next triggering instant of communication, a self-triggered scheme is further proposed in this section. Here, the next triggering instant can be determined with computing with the latest received information, instead of frequent event detection with continuous communication.

Differing from (5), a novel self-triggered scheme is proposed as follows:

1) when A is invertible, a self-triggering time sequence is proposed for information transmission in an insecure network setting

$$t_{k+1} = \begin{cases} \inf\{t > t_k \mid \|\Omega_1(t)\| \\ \qquad = \sqrt{\sigma}\|[\widetilde{\Xi}\Gamma_1(t)\|\}; & t_k \notin \Phi(t) \\ t_k + \theta; & t_k \in \Phi(t) \end{cases} \quad (17)$$

with $\Omega_1(t) = q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - [I_N \otimes I_n - \exp\{(I_N \otimes A)(t-t_k)\}][H \otimes (A^{-1}BK)]q(t_k)$, $\Gamma_1(t) = [H \otimes (A^{-1}BK)]q(t_k) + \exp\{(I_N \otimes A)(t-t_k)\}[I_N \otimes I_n - H \otimes (A^{-1}BK)]q(t_k)$, $\Xi^T\Xi = H$, and $\widetilde{\Xi} = (\Xi^T)^{-1} \otimes I_n$.

2) when A is not invertible, a self-triggering time sequence is proposed for information transmission in an unreliable network setting

$$t_{k+1} = \begin{cases} \inf\{t > t_k \mid \|\Omega_2(t)\| \\ \qquad = \sqrt{\sigma}\|\widetilde{\Xi}\Gamma_2(t)\|\}; & t_k \notin \Phi(t) \\ t_k + \theta; & t_k \in \Phi(t) \end{cases} \quad (18)$$

with $\Omega_2(t) = q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - [H \otimes (UA^*U^{-1}BK)]q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\}[H \otimes (U\tilde{A}U^{-1}BK)]q(t_k)$, and $\Gamma_2(t) = \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) + [H \otimes (UA^*U^{-1}BK)]q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\}[H \otimes (U\tilde{A}U^{-1}BK)]q(t_k)$.

Remark 7: In the event-triggered scheme (5), the next triggering instant is determined by event detection with frequent communication. However, in self-triggered schemes (17) and (18), the next triggering instant t_{k+1} is determined by computing with the information $q(t_k)$. Thus, the conditions on frequent event detection and communication are avoided.

Remark 8: Under the self-triggered schemes (17) and (18), at instant t_k, agents send their information to neighbors, and meantimes send it to the event detector. According to (17) and (18), the event detector is able to determine the next triggering instant t_{k+1} by using agents' information at t_k, and then to inform agents the next triggering instant t_{k+1}. At instant t_{k+1}, agents exchange information again with their neighbors. At the moment, if one agent does not receive information from its neighbors, it may realize that the network communication suffers from one successful attack, and then note the event detector. The event detector will determine $t_{k+2} = t_{k+1} + \theta$ and inform agents the next triggering instant t_{k+2}.

In this section, two main theorems will be obtained, and we will discuss the effectiveness of synchronous and asynchronous update strategies of event-triggered control protocols in the self-triggered schemes (17) and (18).

Corollary 1: Consider multiagent systems (1) and (2) with an event-based control protocol (6) and a self-triggering sequence defined in (17) and (18). Suppose that Assumption 1 holds, the matrix K_1 is designed in (9), the matrix P_1 and $\hat{\beta}_1$ satisfy (8) and (10), respectively. Under any DoS attack, the leader-following consensus can be asymptotically achieved, if $\xi(t_0, t) \leq (\alpha_1 - \rho_1/(\alpha_1 + \beta_1)\theta)$ with $\alpha_1 = ((m_1 - \hat{m}_1)/\lambda_{\max}(P_1))$, $\beta_1 = \hat{\beta}_1/\lambda_{\min}(P_1)$, and $0 < \rho_1 < \alpha_1$. In addition, Zeno behavior can be excluded under the self-triggered schemes (17) and (18).

Corollary 2: Consider multiagent systems (1) and (2) with an event-based control protocol (12) and a self-triggering sequence defined in (17) and (18). Suppose that Assumption 1 holds, the matrix K_2 is designed in (9), the matrix P_2 and $\hat{\beta}_2$ satisfy (13) and (15), respectively. Under any DoS attack, the leader-following consensus can be asymptotically achieved, if $\xi(t_0, t) \leq (\alpha_2 - \rho_2/(\alpha_2 + \beta_2)\theta)$, with $\vartheta \leq \varpi$, $\alpha_2 = ((m_2 - \hat{m}_2)/\lambda_{\max}(P_2))$, $\beta_2 = \hat{\beta}_2/\lambda_{\min}(P_2)$, and $0 < \rho_2 < \alpha_2$. In addition, Zeno behavior can be excluded under the self-triggered schemes (17) and (18).

In fact, Corollaries 1 and 2 can be obtained via the equivalent relation between event conditions (5) and (17) and (18).

Now, the equivalent relation between event conditions (5) and (17) and (18) will be proved. Note that (4) is equivalent to $e^T(t)e(t) \leq \sigma\delta^T(t)(H \otimes I_n)\delta(t)$.

First, consider $q(t) = -(H \otimes I_n)\delta(t)$, then when $t \in [t_k, t_{k+1})$, $\dot{q}(t) = -(H \otimes I_n)\dot{\delta}(t) = -(H \otimes I_n)[(I_N \otimes A)\delta(t) + [I_N \otimes (BK)]q(t_k)] = (I_N \otimes A)q(t) - [H \otimes (BK)]q(t_k)$. Then one has $q(t) = \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - \exp\{(I_N \otimes A)t\}\int_{t_k}^{t} \exp\{-(I_N \otimes A)s\}[H \otimes (BK)]q(t_k)ds$. Follow a similar procedure in [11], we divide the analysis into two cases. If A is invertible, then

$$\begin{aligned} q(t) &= \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - \exp\{(I_N \otimes A)t\} \\ &\quad \times \int_{t_k}^{t} \exp\{-(I_N \otimes A)s\}(I_N \otimes A)ds(I_N \otimes A^{-1}) \\ &\quad \times [H \otimes (BK)]q(t_k) \\ &= \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) \\ &\quad + [I_N \otimes I_n - \exp\{(I_N \otimes A)(t-t_k)\}] \\ &\quad \times [H \otimes (A^{-1}BK)]q(t_k). \end{aligned} \quad (19)$$

If A is not invertible, then there exists an invertible matrix U such that $U^{-1}AU = \bar{A} = \text{diag}\{A_1, \boldsymbol{O}\}$. Define $A^* = \text{diag}\{A_1^{-1}, \boldsymbol{O}\}$ and $\tilde{A} = \text{diag}\{A_1^{-1}, I\}$, then one has

$$\begin{aligned} q(t) &= \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - \exp\{(I_N \otimes A)t\} \\ &\quad \times (I_N \otimes U)(I_N \otimes U^{-1}) \end{aligned}$$

$$
\begin{aligned}
&\times \int_{t_k}^{t} \exp\{-(I_N \otimes A)s\}(I_N \otimes U)ds \\
&\times (I_N \otimes U^{-1})[H \otimes (BK)]q(t_k) \\
&= \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - (I_N \otimes U)(I_N \\
&\otimes \operatorname{diag}\{\exp\{A_1 t\}, I\})(I_N \otimes \operatorname{diag}\{-\exp\{-A_1 t\} \\
&+ \exp\{-A_1 t_k\}, I(t-t_k)\})(I_N \otimes \operatorname{diag}\{A_1^{-1}, I\}) \\
&(I_N \otimes U^{-1})[H \otimes (BK)]q(t_k) \\
&= \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - (I_N \otimes U) \\
&\times (I_N \otimes \operatorname{diag}\{-I, \boldsymbol{O}\})(I_N \otimes \operatorname{diag}\{A_1^{-1}, I\})(I_N \otimes U^{-1}) \\
&\times [H \otimes (BK)]q(t_k) - (I_N \otimes U) \\
&\times (I_N \otimes \operatorname{diag}\{\exp\{A_1(t-t_k)\}, I(t-t_k)\}) \\
&\times (I_N \otimes \operatorname{diag}\{A_1^{-1}, I\}) \\
&\times (I_N \otimes U^{-1})[H \otimes (BK)]q(t_k) \\
&= \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) + [H \otimes (UA^*U^{-1}BK)] \\
&\times q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\} \\
&\times [H \otimes (U\tilde{A}U^{-1}BK)]q(t_k). \qquad (20)
\end{aligned}
$$

Due to $e(t) = q(t_k) - q(t)$, then $e(t) = q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - [I_N \otimes I_n - \exp\{(I_N \otimes A)(t-t_k)\}][H \otimes (A^{-1}BK)]q(t_k)$ when A is invertible, and $e(t) = q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\}q(t_k) - [H \otimes (UA^*U^{-1}BK)]q(t_k) - \exp\{(I_N \otimes A)(t-t_k)\}[H \otimes (U\tilde{A}U^{-1}BK)]q(t_k)$ when A is not invertible.

Therefore, the event condition (5) is equivalent to the form of (17) and (18).

Remark 9: The objective of this paper is to investigate security issues of multiagent systems, and our goal is to achieve asymptotic consensus in the presence of DoS attacks. This is an extremely difficult issue, especially under event/self-triggered scheme, and, thus we investigate this issue at the expense of requiring more information of the initial stage of the matrix H. The *disadvantage* of this method is that the initial matrix H should be known. Note that the matrix H refers to the original network topology. In fact, this information could be obtained in many practical situations. Thus, this requirement is acceptable in practice. On the other hand, when the DoS attacks are taken into consideration for network communication, the network topology could be time-varying and possibly disconnected. In this situation, the corresponding matrix $H(t)$ is also time-varying. The *advantage* of our method is that it does not require to obtain the subsequent information of $H(t)$ induced by DoS attacks [see (17) and (18)]. To sum up, under the proposed self-triggered schemes with given initial matrix H, we have addressed some essential security issues on this topic.

Remark 10: For a directed communication topology as in [39], it is fairly straightforward to carry out a similar analysis by developing a Lyapunov function $V(t) = \delta^T(t)(\Omega \otimes P_1)\delta(t)$ and $V(t) = \delta^T(t)(\Omega \otimes P_2)\delta(t)$ instead of those in proofs of Proposition 1 and Theorem 1. Here, a diagonal matrix $\Omega = \operatorname{diag}\{\omega_1, \omega_2, \ldots, \omega_N\}$ with ω_i $(i = 1, 2, \ldots, N)$ satisfying $H\omega = 1_N$ with $\omega = [\omega_1, \omega_2, \ldots, \omega_N]^T$. In a directed communication topology, H becomes a nonsymmetric matrix, but $H^T\Omega + \Omega H$ is a symmetric matrix by constructing Ω. By constructing the above Lyapunov functions, the role of H could be replaced by $H^T\Omega + \Omega H$. Thus, a similar analysis could be proceeded by means of suitable coordinate transformations. In addition, in a *reliable* network, we investigate the directed network topology by developing an appropriate event-triggered scheme for a multileaders case in [35]. To avoid the unnecessary repetition, the detailed analysis is omitted in this paper, and we refer the interested reader to [35], [39] for a discussion on how the directed topology can be dealt with.

Remark 11: As we know, there are very few works on event/self-triggered schemes over an *unreliable* network for multiagent systems, not to mention distributed schemes. Therefore, the objective of this paper is to propose effective event/self-triggered schemes applicable to an unreliable communication network. It is excited that such objective has been achieved in our work. Despite the fact that the results developed are in a centralized event-triggered fashion, it contains significant break through on setting up new event-triggered model for the unreliable networks. One can see the applications and comparisons in [32] based on different topologies for centralized, clustered, and distributed event-triggered schemes. The usefulness of the centralized algorithms is dependent very much on the size and topology of the networks. The centralized event-triggered algorithm will be useful to those network structures containing many small clusters, and each cluster can use the centralized algorithms effectively. In addition, the centralized scheme developed in this paper can be utilized in medium/small size network or can be further developed for large network with clustered structure. We believe that our works lay a solid foundation for the development of a whole event-triggered control framework under an unreliable network.

V. Extension of Directed Communication Graph

VI. Discussion of the Effect of Some Parameters

In this section, the roles of parameters η_k and θ on the information transmission and the effect time of attacks will be discussed.

A. Dwell Time of Attack η_k

The parameters η_k $(k = 0, 1, \ldots)$ are the dwell time of attack $\mathcal{A}_k$, which implies that attackers intend to interrupt the information transmission over partial communication channels of the network during $[\mathcal{A}_k, \mathcal{A}_k + \eta_k)$.

The proposed event-/self-triggered communication scheme determines when to transmit information: 1) if no information is transmitted over the network during $[\mathcal{A}_k, \mathcal{A}_k + \eta_k)$, then this attack is unsuccessful and does not have any impact on agents' behaviors and 2) if the information of agents are transmitted at time instant t_p with $t_p \in [\mathcal{A}_k, \mathcal{A}_k + \eta_k)$, then this attack is successful, and the effect of this attack starts from the instant t_p instead of $\mathcal{A}_k$. Therefore, whether the network communication is affected by the attacks jointly depends on the attack strategy and communication scheme.

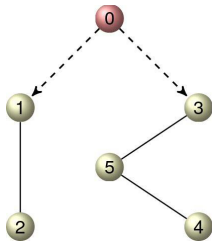

Fig. 1. Networked communication structure.

B. Parameter θ in Communications Scheme (5), (17) and (18)

The role of the parameter θ is to determine the next instant of information transmission once the current information transmission is successfully attacked. Assume the triggering instant $t_p \in [\mathcal{A}_k, \mathcal{A}_k + \eta_k)$, which implies that the communication of some channels at t_p is interrupted by this attack and partial information transmission over the network is unsuccessful. According to (5), the next triggering instant is $t_p + \theta$. Suppose that the best choice of θ (labeled as θ_b) is $\theta_b = \mathcal{A}_k + \eta_k - t_p$. If $\theta < \theta_b$, then the next communication instant t_{p+1} still belongs to $[\mathcal{A}_k, \mathcal{A}_k + \eta_k)$, which implies that this communication is attacked again and information transmission is still unsuccessful. Thus, the cost for this triggering communication is wasted. On the other hand, if $\theta > \theta_b$, then the next information transmission is possibly successful, but the attack effect time is extended from $\mathcal{A}_k + \eta_k - t_p$ to θ. Obviously, the best choice θ_b is dependent on the exact information of attacks. However, in this paper, the attacks' information is unknown, and, hence θ_b is difficult to be obtained. Note that the parameter θ_b is unavailable. Then, for the purpose of analysis, a constant θ is first chosen in the communication schemes (5), (17) and (18) to present our main idea on the communication schemes in the presence of DoS attacks.

VII. Simulation Examples

Example 1: Consider a multiagent system including one leader and five followers with

$$A = \begin{bmatrix} 0.001 & 0.001 & 0 & 0 \\ 0 & -0.01 & 0.001 & 0 \\ 0 & 0 & -0.01 & 0.001 \\ 0.001 & 0 & 0 & 0 \end{bmatrix} \tag{21}$$

and $B = 2I_4$. The networked communication structure is described in Fig. 1. Followers 1 and 3 can receive the leader's information.

Five edges exist among agents for information transmission, which are labeled as ed_1, ed_2, ed_3, ed_4, and ed_5. The attack instants and their dwell time are randomly generated [see Fig. 3]. Here, the existing five communication channels (edges) are attacked randomly [see Fig. 2], and assume that one of the existing channels (edges) is attacked by each attack. To be specific, in Fig. 2(a), the edge ed_1 is attacked, and the information transmission from the leader to agent 1 is interrupted. Thus, the protocol update of node 1 is affected by DoS attacks, but the leader is not. The reason is that the leader does not need any information from followers to update its dynamics in the leader-following network. Hence, there is no effect on leader's dynamics when the communication channels are under attacks. Similar case occurs in edge ed_2. On the other hand, the attack on edge ed_3 will lead to packet loss of communication between agents 1 and 2, and then the dynamics of nodes 1 and 2 cannot be updated unsuccessfully [see Fig. 2(c)]. Similar cases occur in edges ed_4 and ed_5.

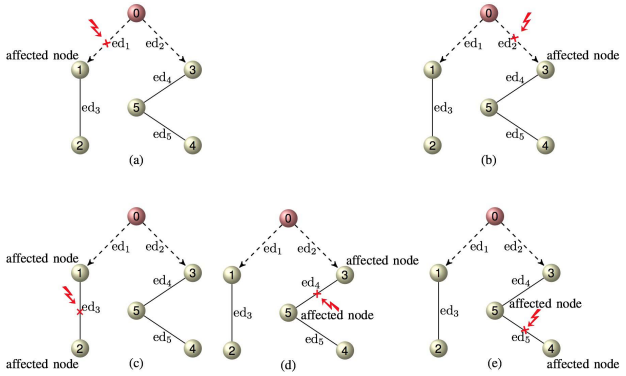

Fig. 2. Different edges are attacked by DoS attacks.

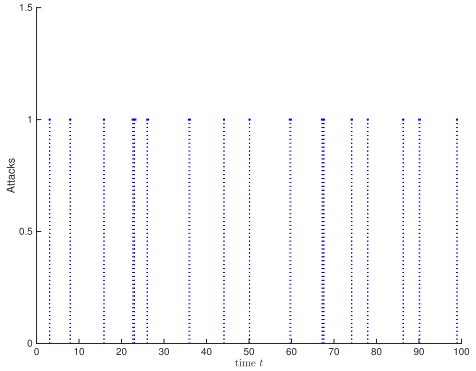

Fig. 3. Here, 17 DoS attacks are launched randomly.

It is shown in Fig. 3 that 17 times of DoS attacks are generated during [0, 100]. Then, an event-triggered communication scheme (5) is developed with $\sigma = 0.001$ and $\theta = 0.04$, and then an asynchronous control protocol is developed as (12) with

$$K_2 = \begin{bmatrix} 0.2394 & 0.0013 & 0 & 0.0013 \\ 0.0013 & 0.2127 & 0.0011 & 0 \\ 0 & 0.0011 & 0.2127 & 0.0011 \\ 0.0013 & 0 & 0.0011 & 0.2368 \end{bmatrix}. \tag{22}$$

In Fig. 2(a), only ed_1 is attacked, and then partial information of agent 1's is lost. Thus, it does not update its control protocol at this instant. However, other agents' communication is not affected by this attack, and then the control protocols of agents 2–5 are updated with the latest received information according to (12). In addition, in Fig. 2(c), ed_3 is attacked, and, hence two agents' dynamical behaviors (agents 1 and 2) are affected by this attack. In this situation, other agents (except agents 1 and 2) still update their control protocols as usual.

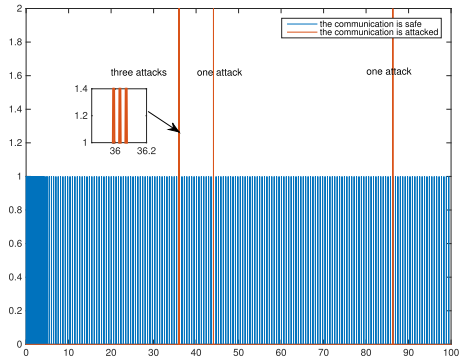

Fig. 4. The communication pattern under asynchronous update strategy (12). There are 5 out of 278 transmission suffered from DoS attacks in this simulation.

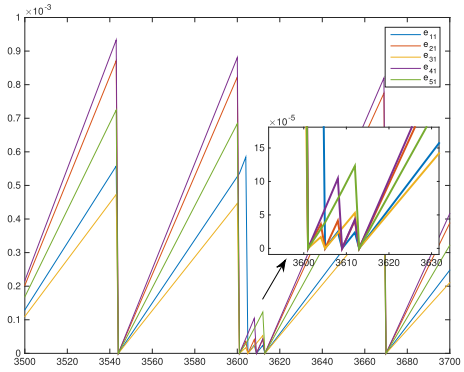

Fig. 5. Evolution of triggering condition.

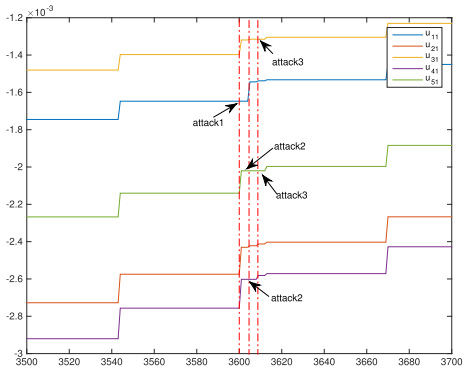

Fig. 6. Evolution of control protocol u_{i1}.

Choose the parameters $\alpha_2 = 0.0755$, $\beta_2 = 15.1292$, and $\rho_2 = 0.001$. During the time interval $[0, 100]$, the number of communication triggered by condition (5) is 278 times, and only 5 times of information transmissions suffer from successful DoS attacks (see Fig. 4). The attacked edges are ed_1, ed_5, ed_4, ed_1, and ed_3, respectively for 5 times of attacks (see Fig. 4). This implies that under the event-triggered defense strategy, most of the DoS attacks are not successful. To clearly display the effect of attacks, Figs. 5 and 6 present the evolution of triggering condition and control input. During the time interval $[36, 36.2]$, the information transmission of agents suffer from three times of attacks. The first one affects the update of agent 1, the second one affects the update of agents 4 and 5,

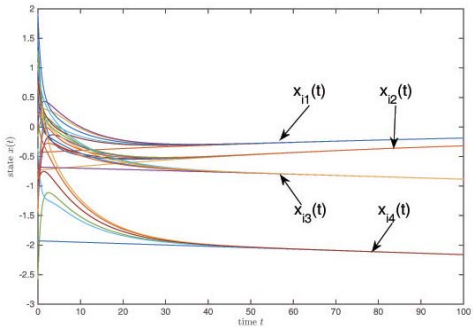

Fig. 7. State trajectory of the leader and its followers.

and the third one affects the update of agents 3–5, which is displayed in Figs. 5 and 6. Furthermore, it is found in Fig. 7 that the leader-following consensus can be achieved asymptotically under the event-triggered communication scheme (5) and the control protocol (12) in the unreliable network setting.

VIII. Conclusion

This paper has investigated a leader-following consensus problem of multiagent system by simultaneously considering communication constraints and an unreliable communication environment. Thus, two kinds of triggering communication schemes, i.e., event-triggered and self-triggered schemes, have been well designed and efficiently implemented even in the presence of DoS attacks. In each of these communication schemes, synchronous and asynchronous update strategies of control protocols have been developed, which guarantee multiple agents to asymptotically achieve the leader-following consensus in an unreliable network environment. It is worth mentioning that the self-triggered scheme has further decreased the cost of event detection, in which the next triggering instant of communication can be determined by computation. Finally, a numerical example has been provided to verify the validity of our communication strategies.

The fully distributed event/self-triggered schemes are worthy of further study, and the main difficulty is how to evaluate and quantize the effect of DoS attacks on the whole network via local information. This paper sheds some light on exploration of their design and the corresponding theoretical analysis. In addition, our future topics of research would also focus on the study of general nonlinear interconnected large-scale systems [41], [42].

Appendix A
Proof of Proposition 1

Proof: First, a Lyapunov function is built as $V(t) = \sum_{i=1}^{N} \delta_i^T(t) P_1 \delta_i(t)$. Next, the trajectory of $V(t)$ is analyzed from two aspects: 1) the latest information transmission is successful and 2) the latest information transmission suffers from successful attacks. Now, consider $t \in [t_k, t_{k+1})$: 1) if $t_k \notin \Phi(t)$, this implies that the network communication is not subject to attacks at t_k, thus one has $\dot{V}(t) = \sum_{i=1}^{N} \{\delta_i^T(t)(A^T P_1 + P_1 A)\delta_i(t) + 2\delta_i^T(t) P_1 B B^T P_1 q_i(t_k)\} =$

$\delta^T(t)[I_N \otimes (A^T P_1 + P_1 A) - 2H \otimes (P_1 B B^T P_1)]\delta(t) - 2\delta^T(t)[I_N \otimes (P_1 B B^T P_1)]e(t) \le \delta^T(t)[I_N \otimes (A^T P_1 + P_1 A - (2\lambda_1 - \gamma_1)P_1 B B^T P_1)]\delta(t) + (\mu_1/\gamma_1)e^T(t)e(t)$.

Under the event condition (5), one has $e^T(t)e(t) \le \sigma\delta^T(t)(H \otimes I_n)\delta(t)$, thus $\dot V(t) \le \sum_{i=1}^N \delta_i^T(t)[A^T P_1 + P_1 A - (2\lambda_1 - \gamma_1)P_1 B B^T P_1]\delta_i(t) + (\mu_1\sigma/\gamma_1)\delta^T(t)(H \otimes I_n)\delta(t)$, which implies $\dot V(t) \le -(m_1 - (\mu_1\sigma/\gamma_1)\lambda_N)\delta^T\delta \le -\alpha_1\delta^T(t)(I_N \otimes P_1)\delta(t) \le -\alpha_1 V(t)$ with $\alpha_1 = (m_1 - \hat m_1/\lambda_{\max}(P_1)) > 0$ and $\hat m_1 = (\mu_1\sigma\lambda_N/\gamma_1)$.

2) if $t_k \in \Phi(t)$, then the latest information transmission is unsuccessful. Assume that t_s is the latest instant when all agents successfully send information to their neighbors, and thus, the DoS attacks block the network communication from time instant t_{s+1}. Thus, when $t \in [t_k, t_{k+1})$, $\dot V(t) = \sum_{i=1}^N\{\delta_i^T(t)(A^T P_1 + P_1 A)\delta_i(t) + 2\delta_i^T(t)P_1 B B^T P_1 q_i(t) + 2\delta_i^T(t)P_1 B B^T P_1(q_i(t_s) - q_i(t))\} \le \sum_{i=1}^N \delta_i^T(t)[A^T P_1 + P_1 A - (2\lambda_1 - \nu_1)P_1 B B^T P_1]\delta_i(t) + (\mu_1(1 + 1/\nu_2)/\nu_1)\sum_{i=1}^N (q_i(t_s) - q_i(t_{s+1}))^T(q_i(t_s) - q_i(t_{s+1})) + ((1 + \nu_2)/\nu_1)\sum_{i=1}^N (q_i(t_{s+1}) - q_i(t))^T P_1 B B^T P_1(q_i(t_{s+1}) - q_i(t))$.

According to (4), one has $(q(t_s) - q(t_{s+1}))^T(q(t_s) - q(t_{s+1})) \le \sigma\delta^T(t_{s+1})(H \otimes I_n)\delta(t_{s+1})$, thus

$$\begin{aligned}\dot V(t) &\le \sum_{i=1}^N \delta_i^T(t)[A^T P_1 + P_1 A - (2\lambda_1 - \nu_1)P_1 B B^T P_1]\delta_i(t)\\ &\quad + \mu_1\sigma\bar\nu_1\delta^T(t_{s+1})(H \otimes I_n)\delta(t_{s+1}) + 2\mu_1\bar\nu_2 q^T(t_{s+1})\\ &\quad \times q(t_{s+1}) + 2\bar\nu_2 q^T(t)[I_N \otimes (P_1 B B^T P_1)]q(t)\\ &\le \sum_{i=1}^N \delta_i^T(t)[A^T P_1 + P_1 A - \nu P_1 B B^T P_1]\delta_i(t)\\ &\quad + \frac{\mu_1}{\nu_1}\delta^T(t_{s+1})[(\sigma(1 + 1/\nu_2)H\\ &\qquad + 2(1 + \nu_2)H^T H) \otimes I_n]\delta(t_{s+1})\\ &\le \beta_1 \max\{V(t), V(t_{s+1})\} \end{aligned} \tag{23}$$

with $\bar\nu_1 = (1 + 1/\nu_2)/\nu_1$, $\bar\nu_2 = (1 + \nu_2)/\nu_1$, and $\beta_1 = \hat\beta_1/\lambda_{\min}(P_1)$, thus $V(t) \le V(t_{s+1})\exp(\beta_1(t - t_{s+1}))$.

Now, let $t_{p+} = \max\{t_k \mid t_k \in \Phi(t)\}$ and $t_{q-} = \max\{t_k \mid t_k \in \Psi(t)\}$. If $t_{p+} < t_{q-}$, this implies that the latest information transmission is successful, then $\dot V(t) \le -\alpha_1 V(t)$, and $V(t) \le V(t_{q-})\exp\{-\alpha_1(t - t_{q-})\}$. Define $t_{j-} = \min\{t_k > t_{p+} \mid t_k \in \Psi(t)\}$, then $V(t_{j-}^-) \le V(t_{p+})\exp\{\beta_1(t_{j-}^- - t_{p+})\} = V(t_{p+})\exp\{\beta_1\zeta_{p+}\theta\}$, where ζ_{p+} denotes the number of successful attacks during $[t_{p+}, t_{j-})$. Due to the continuity of $V(t)$, $V(t_{j-}) = V(t_{j-}^-)$. Hence $V(t) \le V(t_{p+})\exp\{\beta_1\zeta_{p+}\theta - \alpha_1(t - t_{j-})\}$.

Similarly, if $t_{p+} > t_{q-}$, define $t_{h+} = \min\{t_k > t_{q-} \mid t_k \in \Phi(t)\}$, and ζ_{h+} is the number of information transmission being attacked during $[t_{h+}, t)$, then $V(t) \le V(t_{q-})\exp\{\beta_1\zeta_{h+}\theta - \alpha_1(t - t_{q-} - \zeta_{h+}\theta)\}$.

Therefore, one has $V(t) \le V(t_0)\exp[-\alpha_1(t - t_0 - n(t_0, t)\theta) + \beta_1 n(t_0, t)\theta] \le V(t_0)\exp(-\rho_1 t)$. This implies that $\lim_{t\to\infty} V(t) = 0$, and hence leader-following consensus can be achieved asymptotically.

Furthermore, the exclusion of Zeno behavior will be proved in Theorem 1. □

APPENDIX B
PROOF OF THEOREM 1

Proof: Construct a Lyapunov function $V(t) = \delta^T(t)(I_N \otimes P_2)\delta(t)$. The next task is to prove that $\lim_{t\to\infty} V(t) = 0$ even when the network communication suffers from DoS attacks.

First, consider the case of $t \in [t_k, t_{k+1})$. We can analyze the trajectory of $V(t)$ from two aspects: 1) the information transmission is successful at t_k, i.e., $t_k \notin \Phi(t)$ and 2) the information transmission suffers from successful attacks at t_k, i.e., $t_k \in \Phi(t)$.

For the convenience of discussion, define $\mathcal{P}_2 = P_2 B B^T P_2$, $\bar\iota_1 = (1 + (1/\iota_2))/\iota_1$, $\bar\iota_2 = (1 + \iota_2)/\iota_1$, $\mathcal{H} = (\mu_2/\iota_1)[(1 + 1/\iota_2)\sigma H + 2(1 + \iota_2)H^T H]$.

1) If $t_k \notin \Phi(t)$, this implies that information transmission over network is successful at instant t_k. Similar with the discussion in Proposition 1, it is obvious to obtain $\dot V(t) \le \delta^T(t)[I_N \otimes (A^T P_2 + P_2 A - (2\lambda_1 - \gamma_2)P_2 B B^T P_2)]\delta(t) + (\mu_2/\gamma_2)e^T(t)e(t)$. According to (13), it is easy to obtain $\dot V(t) \le -\alpha_2 V(t)$ with $\alpha_2 = (m_2 - \hat m_2/\lambda_{\max}(P_2))$ and $\hat m_2 = (\mu_2\sigma\lambda_N/\gamma_2)$.

The next step is to prove the following claim.

Claim: $V(t) \le V(t_k)\exp\{\beta_2(t - t_k)\}$ when the network communication at t_k is subject to successful attacks, i.e., $t_k \in \Phi(t)$.

2) If $t_k \in \Phi(t)$, then assume that t_s is the latest time instant of successful network communication. Next, define ϑ_1 to be the number of successive successful attacks during $[t_s, t)$ (including the attack at t_k). Obviously, $\vartheta_1 \le \vartheta$.

Next, a mathematical induction method is used for the proof of the claim.

Step 1: when $\vartheta_1 = 1$, that is, the network communication is subject to one successful attack during $[t_s, t)$. This implies that the information transmitted at t_k is lost. Obviously, $t_k = t_{s+1}$. Here, $t \in [t_k, t_{k+1})$, i.e., $t \in [t_{s+1}, t_{s+2})$. In this case, all nodes can be classified into two different groups: the affected agents $i \in \mathcal{A}^n(t_{s+1})$ and the unaffected agents $i \notin \mathcal{A}^n(t_{s+1})$. [The definition of $\mathcal{A}^n(t)$ is given in Section II-C]. Then, one has $\dot V(t) = \sum_{i\in\mathcal{A}^n(t_{s+1})}[\delta_i^T(t)(A^T P_2 + P_2 A)\delta_i(t) + 2\delta_i^T(t)\mathcal{P}_2 q_i(t_s)] + \sum_{i\notin\mathcal{A}^n(t_{s+1})}[\delta_i^T(t)(A^T P_2 + P_2 A)\delta_i(t) + 2\delta_i^T(t)\mathcal{P}_2 q_i(t_{s+1})]$. Next, by using (13) and (15), one obtains

$$\begin{aligned}\dot V(t) &\le \sum_{i=1}^N \delta_i^T(t)[A^T P_2 + P_2 A - (2\lambda_1 - \iota_1)\mathcal{P}_2]\delta_i(t)\\ &\quad + 2\bar\iota_2\sum_{i=1}^N q_i^T(t_{s+1})\mathcal{P}_2\, q_i(t_{s+1}) + 2\bar\iota_2\iota_1\sum_{i=1}^N q_i^T(t)\mathcal{P}_2 q_i(t)\\ &\quad + \sigma\,\mu_2\bar\iota_1\delta^T(t_{s+1})(H \otimes I_n)\delta(t_{s+1})\\ &\le \sum_{i=1}^N \delta_i^T(t)[A^T P_2 + P_2 A - \iota\mathcal{P}_2]\delta_i(t)\\ &\quad + \delta^T(t_{s+1})(\mathcal{H} \otimes I_n)\delta(t_{s+1}).\end{aligned}$$

By using (15), one has $\dot V(t) \le \beta_2 \max\{V(t_{s+1}), V(t)\}$ with $\beta_2 = \hat\beta_2/\lambda_{\min}(P_2)$. Thus, one obtains $V(t) \le V(t_{s+1})\exp\{\beta_2(t - t_{s+1})\}$, and it implies that $V(t_{s+2}) \le V(t_{s+1})\exp\{\beta_2(t_{s+2} - t_{s+1})\}$. Therefore, the claim of $V(t) \le V(t_k)\exp\{\beta_2(t - t_k)\}$ is proven when $\vartheta_1 = 1$.

Step 2: Assume that the claim of $V(t) \le V(t_k)\exp\{\beta_2(t-t_k)\}$ always holds when $2 \le \vartheta_1 \le r-1$, then one considers the case of $\vartheta_1 = r$. We would like to prove that this claim still holds when $\vartheta_1 = r$. In this case, obviously, $t_k = t_{s+r}$, and $t \in [t_{s+r}, t_{s+r+1})$. Successive information transmissions are attacked at instants $\{t_{s+1}, t_{s+2}, \ldots, t_{s+r}\}$. In this case, all nodes can be classified into $r+1$ different groups

$$\begin{aligned}
\mathbb{S}_1 &= \bigcap_{j=1}^{r} \mathcal{A}^n(t_{s+j}), \quad \mathbb{S}_2 = \bigcap_{j=2}^{r} \mathcal{A}^n(t_{s+j}) \cup \overline{\mathcal{A}^n(t_{s+1})}, \ldots \\
\mathbb{S}_m &= \bigcap_{j=m}^{r} \mathcal{A}^n(t_{s+j}) \cup \overline{\mathcal{A}^n(t_{m-1})}, \ldots \\
\mathbb{S}_r &= \mathcal{A}^n(t_{s+r}) \cup \overline{\mathcal{A}^n(t_{s+r-1})}, \quad \mathbb{S}_{r+1} = \overline{\mathcal{A}^n(t_{s+r})}. \qquad (24)
\end{aligned}$$

Obviously, $\bigcup_{p=1}^{r+1} \mathbb{S}_p = \{1, 2, \ldots, N\}$. Note that when node $i \in \mathbb{S}_m$, then $u_i(t) = K_2 q_i(t_{s+m})$ for $t \in [t_k, t_{k+1})$, $m = 1, 2, \ldots, r$. By denoting $\Delta q_i(t_s) = q_i(t_s) - q_i(t)$, then one obtains

$$\begin{aligned}
\dot{V}(t) &= \sum_{p=1}^{r+1} \sum_{i\in\mathbb{S}_p} \big\{\delta_i^T(t)(A^T P_2 + P_2 A)\delta_i(t) + 2\delta_i^T(t)\mathcal{P}_2\ q_i(t) \\
&\qquad + 2\delta_i^T(t)\mathcal{P}_2 \Delta q_i(t_{s+p-1})\big\} \\
&\le \sum_{i=1}^{N} \delta_i^T(t)[A^T P_2 + P_2 A - (2\lambda_1 - \iota_1)\mathcal{P}_2]\delta_i(t) \\
&\quad + \frac{1}{\iota_1} \sum_{p=2}^{r+1} \sum_{i\in\mathbb{S}_p} \Delta q_i(t_{s+p-1})^T \mathcal{P}_2 \Delta q_i(t_{s+p-1}) \\
&\quad + \bar{\iota}_1 \sum_{i\in\mathbb{S}_1} [q_i(t_s) - q_i(t_{s+1})]^T \mathcal{P}_2 [q_i(t_s) - q_i(t_{s+1})] \\
&\quad + \bar{\iota}_2 \sum_{i\in\mathbb{S}_1} \Delta q_i(t_{s+1})^T \mathcal{P}_2 \Delta q_i(t_{s+1}) \\
&\le \sum_{i=1}^{N} \delta_i^T(t)[A^T P_2 + P_2 A - (2\lambda_1 - \iota_1)\mathcal{P}_2]\delta_i(t) \\
&\quad + 2\mu_2 \bar{\iota}_2 \sum_{i\in\mathbb{S}_1\cup\mathbb{S}_2} q_i^T(t_{s+1}) q_i(t_{s+1}) \\
&\quad + 2\bar{\iota}_2 \sum_{p=1}^{r+1} \sum_{i\in\mathbb{S}_p} q_i^T(t)\mathcal{P}_2 q_i(t) + \mu_2 \bar{\iota}_1 e^T(t_{s+1}) e(t_{s+1}) \\
&\quad + \frac{2\mu_2}{\iota_1} \sum_{p=3}^{r+1} \sum_{i\in\mathbb{S}_p} q_i^T(t_{s+p-1}) q_i(t_{s+p-1}) \\
&\le \sum_{i=1}^{N} \delta_i^T(t)(A^T P_2 + P_2 A - \iota\mathcal{P}_2)\delta_i(t) \\
&\quad + \mu_2 \sigma \bar{\iota}_1 \delta^T(t_{s+1})(H \otimes I_n)\delta(t_{s+1}) \\
&\quad + 2\mu_2 \bar{\iota}_2 \delta^T(t_{s+1})(H^T H \otimes I_n)\delta(t_{s+1}) \\
&\quad + \frac{2\mu_2}{\iota_1} \sum_{p=3}^{r+1} \delta^T(t_{s+p-1})(H^T H \otimes I_n)\delta(t_{s+p-1}). \qquad (25)
\end{aligned}$$

By (15), one has $\dot{V}(t) \le (\hat{\beta}_2/\varpi + 1)\{\sum_{i=1}^{N} \delta_i^T(t)\delta_i(t) + \delta^T(t_{s+1})\delta(t_{s+1}) + \sum_{p=3}^{r+1} \delta^T(t_{s+p-1})\delta(t_{s+p-1})\}$, which implies that $\dot{V}(t) \le \beta_2 \max\{V_{s+1}, V_{s+2}, \ldots, V_{s+r}, V(t)\}$ due to $r \le \vartheta$.

Case (a): $\dot{V}(t) \le \beta_2 V(t)$, then it is easy to obtain $V(t) \le V(t_{s+r})\exp\{\beta_2(t - t_{s+r})\}$.

Case (b): $\dot{V}(t) \le \beta_2 V(t_{s+r})$, then one obtains $V(t) \le V(t_{s+r}) + \beta_2 V(t_{s+r})(t - t_{s+r}) \le V(t_{s+r})\exp\{\beta_2(t - t_{s+r})\}$ due to $\exp\{\beta_2(t - t_{s+r})\} \ge 1 + \beta_2(t - t_{s+r})$.

Case (c): $\dot{V}(t) \le \beta_2 V(t_{s+m})$, $(1 \le m \le r-1)$ then one obtains

$$\begin{aligned}
V(t) &\le V(t_{s+r}) + \beta_2 V(t_{s+m})(t - t_{s+r}) \\
&\le V(t_{s+r}) + \beta_2 V(t_{s+m})\exp\{\beta_2(t_{s+r} - t_{s+m})\} \\
&\quad \times \exp\{-\beta_2(t_{s+r} - t_{s+m})\}(t - t_{s+r}) \\
&\le V(t_{s+r}) + \beta_2 V(t_{s+r})\exp\{-\beta_2(t_{s+r} - t_{s+m})\}(t - t_{s+r}) \\
&\le V(t_{s+r})[1 + \beta_2 \exp\{-\beta_2(t_{s+r} - t_{s+m})\}(t - t_{s+r})].
\end{aligned}$$

Let $f(t) = \exp\{\beta_2(t - t_{s+r})\} - 1 - \beta_2 \exp\{-\beta_2(t_{s+r} - t_{s+m})\}(t - t_{s+r})]$, then $f'(t) = \beta_2 \exp\{\beta_2(t - t_{s+r})\} - \beta_2 \exp\{-\beta_2(t_{s+r} - t_{s+m})\} \ge 0$ for $t \ge t_{s+r}$. Thus, $f(t) \ge f(t_{s+r}) = 0$, which means $1 + \beta_2 \exp\{-\beta_2(t_{s+r} - t_{s+m})\}(t - t_{s+r}) \le \exp\{\beta_2(t - t_{s+r})\}$, and furthermore $V(t) \le V(t_{s+r})\exp\{\beta_2(t - t_{s+r})\}$.

Therefore, one concludes $V(t) \le V(t_{s+r})\exp\{\beta_2(t - t_{s+r})\}$, i.e., $V(t) \le V(t_k)\exp\{\beta_2(t - t_k)\}$ for $t \in [t_k, t_{k+1})$. This implies that the claim of $V(t) \le V(t_k)\exp\{\beta_2(t - t_k)\}$ holds when $\vartheta_1 = r$.

By using the mathematical induction method, one concludes that $V(t) \le V(t_k)\exp\{\beta_2(t - t_k)\}$ holds when $t \in [t_k, t_{k+1})$.

Similar to the discussion with Proposition 1, one has $V(t) \le V(t_0)\exp[-\alpha_2(t - t_0 - n(t_0, t)\theta) + \beta_2 n(t_0, t)\theta]$. According to (16), it is concluded that $\dot{V}(t) \le V(t_0)\exp(-\rho_2\ t)$. This implies that $\lim_{t\to\infty} V(t) = 0$ and, hence, leader-following consensus can be achieved asymptotically.

Next, we discuss the Zeno behavior. Here, consider the derivative of $\|e\|/\|(\Xi \otimes I_n)\delta\|$ with $\Xi^T \Xi = H$, then one has

$$\begin{aligned}
&\frac{d}{dt}\left(\frac{\|e(t)\|}{\|(\Xi \otimes I_n)\delta(t)\|}\right) \\
&= \frac{e^T \dot{e}}{\|e\|\|(\Xi \otimes I_n)\delta\|} - \frac{\|e\|\delta^T(H \otimes I_n)\dot{\delta}}{\|(\Xi \otimes I_n)\delta\|^3} \\
&\le \|\Xi^T \otimes I_n\|\|I_N \otimes A - (\Xi\Xi^T) \otimes (BB^T P_1)\| + (\|\Xi^T \otimes I_n\| \\
&\quad \times \|\Xi \otimes (BB^T P_1)\| + \|I_N \otimes A - (\Xi\Xi^T) \otimes (BB^T P_1)\|) \\
&\quad \times \frac{\|e\|}{\|(\Xi \otimes I_n)\delta\|} + \|\Xi \otimes (BB^T P_1)\| \frac{\|e\|^2}{\|(\Xi \otimes I_n)\delta\|^2}. \qquad (26)
\end{aligned}$$

For convenience, let $X(t) = (||e||/||(\Xi \otimes I_n)\delta||)$, and $X \le Y(t, Y_0)$ which is the solution of the following equation:

$$\frac{dY}{dt} = p_0 p_1 Y^2 + (p_0 p_2 + p_1)Y + p_2; \quad Y(0, Y_0) = Y_0 \qquad (27)$$

where $p_0 = \|\Xi^T \otimes I_n\|$, $p_1 = \|I_N \otimes A + (\Xi\Xi^T) \otimes (BB^T P_1)\|$, and $p_2 = \|\Xi \otimes (BB^T P_1)\|$. Obviously, $\Delta = (p_0 p_2 + p_1)^2 - 4p_0 p_1 p_2 = (p_0 p_2 - p_1)^2 \ge 0$. In addition, the interevent time determined by (4) is bounded by the time it takes for $Y(t)$ to evolve from 0 to $\sqrt{\sigma}$, that implies $Y(\tau, 0) = \sqrt{\sigma}$. Then, we will seek the value of τ: if $\Delta = 0$, then $\tau = (4\sqrt{\sigma}\, p_0 p_1/2\sqrt{\sigma}\, p_0 p_1(p_0 p_2 + p_1) + (p_0 p_2 + p_1)^2)$; if $\Delta > 0$, then $\tau = (1/\sqrt{\Delta})\ln|((2\sqrt{\sigma}\, p_0 p_1 + p_0 p_2 + p_1 - \sqrt{\Delta})(p_0 p_2 + p_1 + \sqrt{\Delta})/(2\sqrt{\sigma}\, p_0 p_1 + p_0 p_2 + p_1 + \sqrt{\Delta})(p_0 p_2 +$

$p_1 - \sqrt{\Delta}))|$. Hence, one can conclude that $\tau > 0$, which implies that $t_{k+1} - t_k \geq \min\{\tau, \theta\} > 0$. Therefore, Zeno behavior can be excluded. □

REFERENCES

[1] W. Ren and N. Sorensen, "Distributed coordination architecture for multi-robot formation control," *Robot. Auton. Syst.*, vol. 56, no. 4, pp. 324–333, Apr. 2008.

[2] 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, Jul. 2011.

[3] G. Wen, Y. Zhao, Z. Duan, W. Yu, and G. Chen, "Containment of higher-order multi-leader multi-agent systems: A dynamic output approach," *IEEE Trans. Autom. Control*, vol. 61, no. 4, pp. 1135–1140, Apr. 2016.

[4] Y. Wang, Z. Ma, and G. Chen, "Avoiding congestion in cluster consensus of the second-order nonlinear multiagent systems," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 8, pp. 3490–3498, Aug. 2018, doi: 10.1109/TNNLS.2017.2726354.

[5] 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.

[6] 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.

[7] W. Zhang, Y. Tang, T. Huang, and J. Kurths, "Sampled-data consensus of linear multi-agent systems with packet losses," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 11, pp. 2516–2527, Nov. 2017.

[8] S.-L. Du, X.-M. Sun, M. Cao, and W. Wang, "Pursuing an evader through cooperative relaying in multi-agent surveillance networks," *Automatica*, vol. 83, pp. 155–161, Sep. 2016.

[9] S. Yang, Q. Liu, and J. Wang, "A collaborative neurodynamic approach to multiple-objective distributed optimization," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 4, pp. 981–992, Apr. 2018.

[10] 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.

[11] L. Scardovi and R. Sepulchre, "Synchronization in networks of identical linear systems," *Automatica*, vol. 45, no. 11, pp. 2557–2562, Nov. 2009.

[12] D. Yuan, D. W. C. Ho, and Y. Hong, "On convergence rate of distributed stochastic gradient algorithm for convex optimization with inequality constraints," *J. Control Optim.*, vol. 54, no. 5, pp. 2872–2892, Oct. 2016.

[13] W. Li, G. Wei, D. W. C. Ho, and D. Ding, "A weightedly uniform detectability for sensor networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 11, pp. 5790–5796, Nov. 2018, doi: 10.1109/TNNLS.2018.2817244.

[14] H. Li, X. Liao, T. Huang, and W. Zhu, "Event-triggering sampling based leader-following consensus in second-order multi-agent systems," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1998–2003, Jul. 2015.

[15] W. Hu, L. Liu, and G. Feng, "Consensus of linear multi-agent systems by distributed event-triggered strategy," *IEEE Trans. Cybern.*, vol. 46, no. 1, pp. 148–157, Jan. 2016.

[16] W. Zhu and Z.-P. Jian, "Event-based leader-following consensus of multi-agent systems with input time delay," *IEEE Trans. Autom. Control*, vol. 60, no. 5, pp. 1362–1367, May 2015.

[17] S. Wen, Z. Zeng, M. Z. Q. Chen, and T. Huang, "Synchronization of switched neural networks with communication delays via the event-triggered control," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2334–2343, Oct. 2017.

[18] H. Dong, Z. Wang, and H. Gao, "H∞ fuzzy control for systems with repeated scalar nonlinearities and random packet losses," *IEEE Trans. Fuzzy Syst.*, vol. 17, no. 2, pp. 440–450, Apr. 2009.

[19] J. Xiong and J. Lam, "Stabilization of linear systems over networks with bounded packet loss," *Automatica*, vol. 43, no. 1, pp. 80–87, Jan. 2007.

[20] L. Zhang, Z. Ning, and P. Shi, "Input—Output approach to control for fuzzy Markov jump systems with time-varying delays and uncertain packet dropout rate," *IEEE Trans. Cybern.*, vol. 45, no. 11, pp. 2449–2460, Nov. 2015.

[21] 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.

[22] B. Chen, G. Hu, D. W. C. Ho, and L. Yu, "Distributed covariance intersection fusion estimation for cyber-physical systems with communication constraints," *IEEE Trans. Autom. Control*, vol. 61, no. 12, pp. 4020–4026, Dec. 2016, doi: 10.1109/TAC.2016.2539221.

[23] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Trans. Ind. Inform.*, vol. 12, no. 5, pp. 1786–1794, Oct. 2016.

[24] H. Zhang *et al.*, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[25] 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, doi: 10.1109/TCNS.2017.2668901.

[26] D. Ding, Z. Wang, G. Wei, and F. E. Alsaadi, "Event-based security control for discrete-time stochastic systems," *IET Control Theory Appl.*, vol. 10, no. 15, pp. 1080–1815, Oct. 2016.

[27] R. M. Jungers, W. P. M. H. Heemels, and A. Kundu. (2016). "Observability and controllability analysis of linear systems subject to data losses." [Online]. Available: https://arxiv.org/abs/1609.05840

[28] 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, doi: 10.1109/TCYB.2016.2544062.

[29] Y. Wan, J. Cao, G. Chen, and W. Huang, "Distributed observer-based cyber-security control of complex dynamical networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 11, pp. 2966–2975, Nov. 2017.

[30] W. Xu, J. Cao, W. Yu, and J. Lu, "Leader-following consensus of non-linear multi-agent systems with jointly connected topology," *IET Control Theory Appl.*, vol. 8, no. 6, pp. 432–440, Apr. 2014.

[31] L. Li, D. W. C. Ho, J. Cao, and J. Lu, "Pinning cluster synchronization in an array of coupled neural networks under event-based mechanism," *Neural Netw.*, vol. 76, pp. 1–12, Apr. 2016.

[32] W. Xu, D. W. C. Ho, L. Li, and J. Cao, "Event-triggered schemes on leader-following consensus of general linear multiagent systems under different topologies," *IEEE Trans. Cybern.*, vol. 47, no. 1, pp. 212–223, Jan. 2017.

[33] H. Li, G. Chen, T. Huang, and Z. Dong, "High-performance consensus control in networked systems with limited bandwidth communication and time-varying directed topologies," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 5, pp. 1043–1054, Sep. 2017.

[34] 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.

[35] W. Xu, G. Chen, and D. W. C. Ho, "A layered event-triggered consensus scheme," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 2334–2340, Aug. 2017.

[36] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan. 2006.

[37] Q. Liu, Z. Wang, X. He, and D. H. Zhou, "Event-based H_∞ consensus control of multi-agent systems with relative output feedback: The finite-horizon case," *IEEE Trans. Autom. Control*, vol. 60, no. 9, pp. 2553–2558, Sep. 2015.

[38] L. Ma, Z. Wang, and H.-K. Lam, "Event-triggered mean-square consensus control for time-varying stochastic multi-agent system with sensor saturations," *IEEE Trans. Autom. Control*, vol. 62, no. 7, pp. 3524–3531, Jul. 2017.

[39] G. Wen, Z. Duan, G. Chen, and W. Yu, "Consensus tracking of multi-agent systems with Lipschitz-type node dynamics and switching topologies," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 2, pp. 499–511, Feb. 2014.

[40] 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.

[41] Y. Li and S. Tong, "Adaptive neural networks decentralized FTC design for nonstrict-feedback nonlinear interconnected large-scale systems against actuator faults," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 11, pp. 2541–2554, Nov. 2017.

[42] Y. Li and S. Tong, "Adaptive neural networks prescribed performance control design for switched interconnected uncertain nonlinear systems," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 7, pp. 3059–3068, Jul. 2018, doi: 10.1109/TNNLS.2017.2712698.

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

In 2015, she was an Academic Visitor with Brunel University London, Uxbridge, U.K. From 2017 to 2018, she was a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. In 2018, she was a Senior Research Associate with the Department of Mathematics, City University of Hong Kong. Her current research interests include distributed event-triggered control, distributed cooperative control, and cyber-physical system.

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

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. In 1989, he joined the City University of Hong Kong, where he is currently a Chair Professor of applied mathematics. He has authored or co-authored 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. He was named by Clarivate Analytics as one of the "Highly Cited Researchers" in Engineering in the past five years. He has been in the editorial board of a number of journals including the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IET Control Theory and its Applications, *Journal of the Franklin Institute*, and *Asian Journal of Control*.

Jie Zhong received the B.S. degree from Zhejiang Normal University, Jinhua, China, in 2012, the M.S. degree from Southeast University, Nanjing, China, in 2015, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 2018.

In 2018, he joined the Department of Mathematics, Zhejiang Normal University. His current research interests include Boolean (control) networks, discrete event systems, and complex networks.

Bo Chen (M'17) received the B.S. degree in information and computing science from the Jiangxi University of Science and Technology, Ganzhou, China, in 2008, and the Ph.D. degree in control theory and control engineering from the Zhejiang University of Technology, Hangzhou, China, in 2014.

He is currently a Tenure-Tracked Professor with the Institute of Cyberspace Security, Zhejiang University of Technology. He was a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2014 to 2015 and from 2017 to 2018. From 2015 to 2017, he was also a Post-Doctoral Research Fellow with the Department of Mathematics, City University of Hong Kong, Hong Kong. His current research interests include information fusion estimation, distributed estimation and control, networked fusion systems, and cyber-physical systems.

Dr. Chen was a recipient of the Outstanding Thesis Award of Chinese Association of Automation in 2015. He serves as an Editor-in-Chief for Information Fusion, Control and Decision.