Adaptive Memory Event-Triggered Observer-Based Control for Nonlinear Multi-Agent Systems Under DoS Attacks

Xianggui Guo, Dongyu Zhang, Jianliang Wang, *Senior Member, IEEE*, and Choon Ki Ahn, *Senior Member, IEEE*

***Abstract*—This paper investigates the event-triggered security consensus problem for nonlinear multi-agent systems (MASs) under denial-of-service (DoS) attacks over an undirected graph. A novel adaptive memory observer-based anti-disturbance control scheme is presented to improve the observer accuracy by adding a buffer for the system output measurements. Meanwhile, this control scheme can also provide more reasonable control signals when DoS attacks occur. To save network resources, an adaptive memory event-triggered mechanism (AMETM) is also proposed and Zeno behavior is excluded. It is worth mentioning that the AMETM's updates do not require global information. Then, the observer and controller gains are obtained by using the linear matrix inequality (LMI) technique. Finally, simulation examples show the effectiveness of the proposed control scheme.**

***Index Terms*—Adaptive memory event-triggered mechanism (AMETM), compensation mechanism, denial-of-service (DoS) attacks, nonlinear multi-agent systems (MASs), observer-based anti-disturbance control.**

I. Introduction

NOWADAYS, multi-agent systems are widely used in various fields, such as unmanned aerial vehicles, power systems, sensor networks, etc. [1]–[4]. However, as networks evolve, the problem of network security becomes more prominent [5]–[7]. Since multi-agent systems (MASs) work in networked environments, they are vulnerable to cyber attacks, which may cause system performance degradation or even instability [8]. Hence, the security problems of MASs have attracted the research interest of many scholars in the control field [8]–[10]. In multi-agent networks, agents may be subjected to denial-of-service (DoS) attacks, stealthy deception attacks, replay attacks, false data injection attacks, etc. [11], [12]. Among these attacks, the DoS attack scenarios can be divided into two types; the first type affects the cyber-physical network (which is constituted of a physical layer with fixed physical links and a cyber layer with cyber control units) to prevent the prompt update of the control inputs, and the other type destroys the communication network within the cyber layer to affect the communication topology graph, which would hinder the information interaction among agents [13]; thus, they are more destructive than other attacks [14]. To resist DoS attacks, there are existing results on solving security problems for MASs [15]–[21]. Persis and Tesi [15] studied the input-to-state stability (ISS) of networked systems, and clearly described the frequency and duration of DoS attacks under ISS for the first time. Based on this work, in [16]–[19], the secure consensus problem of MASs under DoS attacks was analyzed, and constraint conditions on DoS attack frequency and duration were obtained under guaranteed consensus. It should be noted that most previous works only consider the security of linear MASs. However, in practice, real systems are essentially nonlinear [22]–[24], and the study of nonlinear systems is more challenging. Moreover, although some results, such as those in [20], [21], consider the security consensus of nonlinear MASs, they generally require that all system states are measurable. Nevertheless, full system states are often challenging to obtain in most practical applications [24]–[27]. Therefore, the observer-based feedback control is often used. Furthermore, in practice, it is generally believed that external disturbances in the system are the main underlying cause of performance degradation and even instability [28]. Due to the growing demand for high-accuracy performance under external disturbances, disturbance compensation control approaches have been widely applied in the control community due to their powerful ability to reject disturbances [29], [30]. The composition of the state observer

Manuscript received March 12, 2021; revised April 7, 2021; accepted May 7, 2021. This work was supported by the National Natural Science Foundation of China (61773056), the Scientific and Technological Innovation Foundation of Shunde Graduate School, University of Science and Technology Beijing (USTB) (BK19AE018), and the Fundamental Research Funds for the Central Universities of USTB (FRF-TP-20-09B, 230201606500061, FRF-DF-20-35, FRF-BD-19-002A). The work of J. L. Wang was supported by Zhejiang Natural Science Foundation (LD21F 030001). The work of C. K. Ahn was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and Information and Communications Technology) (NRF-2020R1A2C1005449). Recommended by Associate Editor Weinan Gao. *(Corresponding author: Choon Ki Ahn.)*

Citation: X. G. Guo, D. Y. Zhang, J. L. Wang, and C. K. Ahn, "Adaptive memory event-triggered observer-based control for nonlinear multi-agent systems under dos attacks," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 10, pp. 1644–1656, Oct. 2021.

X. G. Guo and D. Y. Zhang are with School of Beijing Engineering Research Center of Industrial Spectrum Imaging, School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, and also with Shunde Graduate School of University of Science and Technology Beijing, Foshan 528000, China (e-mail: guoxianggui@163.com; zhangdongyu97@126.com).

J. L. Wang is with Autonomous Intelligent Systems Department, Hangzhou Innovation Institute of Beihang University, Hangzhou 310051, China (e-mail: wjl-180@hotmail.com).

C. K. Ahn is with the School of Electrical Engineering, Korea University, Seoul 1360701, Korea (e-mail: hironaka@korea.ac.kr).

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/JAS.2021.1004132

with the disturbance compensation mechanism and the design of an observer-based anti-disturbance controller under DoS attacks make the secure consensus control problems of MASs highly complicated and challenging. Hence, how to design an observer-based anti-disturbance controller for nonlinear MASs under DoS attacks is the main motivation of this article.

Another problem in multi-agent networks is limited communication bandwidth. In contrast to the traditional time-triggered mechanism, the event-triggered mechanism (ETM) is based on pre-set conditions to determine whether the transmission and control tasks are executed, which can reduce the collection and transmission of redundant data and save network resources [31]. Therefore, the consensus problem for MASs based on ETM has been widely studied [21], [32]–[34]. In [21], an event-based consensus control scheme is proposed for MASs under cyber attacks by using fixed threshold parameters in the event triggering scheme, which may cause significant consumption of communication resources. A centralized event triggering scheme is presented in [32], in which all agents are triggered at the same time. This method reduces the design difficulty but requires global information, and will result in unnecessary usage of communication and computing resources. A distributed adaptive event triggering strategy is adopted in [33], [34], where the threshold can be adjusted dynamically with the system state, and only the information of it and its neighbors are needed to update. As a result, network resources are saved and it is a good choice for ameliorating the event triggering strategy. Certainly, reducing the communication burden will inevitably lead to the decline of system performance. Therefore, how to dynamically adjust the number of trigger points to improve system performance based on reducing the communication burden is another motivation of this article.

Considering the above discussion, the main difficulties are summarized as follows: a) how to design a more accurate state observer and a more effective controller under DoS attacks and disturbance to achieve consensus for nonlinear MASs and b) how to design an ETM based on reduced communication resources to improve system performance. To solve these problems, this paper studies the event-triggered security consensus problem for nonlinear MASs under DoS attacks, and the main contributions are as follows:

1) An Anti-Disturbance Control Scheme Based on a Novel State Observer: Compared with the observer design scheme proposed in [25], [26], by embedding a buffer in the state observer, the state of the previous moment can be stored; thus, the observer accuracy can be improved in the presence of DoS attacks. Unlike [25], [35] where the control signal is set to zero when DoS attacks occur, the proposed observer-based controller can reduce the impact of packet loss caused by DoS attacks due to the existence of the buffer, which can provide a more reasonable control signal and improve the security and reliability of MASs.

2) A Novel Adaptive Memory Event-Triggered Mechanism (AMETM): In contrast to the adaptive ETM studied in [33], [34], by storing recently received information, we can dynamically adjust the number of trigger points to improve system performance and reduce the occurrence of error triggered events caused by sudden changes due to erroneous measurements. Meanwhile, its threshold can be adjusted with state changes for the purpose of saving network resources, and the design process is considerably simpler than that of the memory ETM in [36], [37]. Moreover, a hybrid update mechanism is used to eliminate Zeno behaviors.

3) The Compensation Mechanism for the Observer and Controller: In contrast to [38] in which a disturbance observer is used based on the state feedback control technique to resist disturbances, the proposed compensation mechanism can effectively reduce the difficulty caused by unmeasurable states and resist the influence of disturbances. In addition, the consensus performance of the system can be improved.

The remaining sections of this article are organized as follows. Section II introduces the system description and some preliminaries. The main results are given in Section III. Simulation examples in Section IV illustrate the feasibility and effectiveness of the proposed method. Finally, conclusions and future work directions are presented in Section V.

The following notations are used throughout this article: $\mathbb{R}^n$, $\mathbb{R}^{N\times N}$, and $\mathbb{N}$ denote the n-dimensional space, $N\times N$ real matrices, and set of positive natural numbers, respectively; I_N represents the identity matrix of dimension N; and 1_N denotes the $N\times 1$ matrix with all ones. The superscript "T" is used to represent the transpose of a matrix. Let diag$\{\cdot\}$ be a diagonal matrix and $\text{col}\{x_1,\ldots,x_N\}=[x_1^T,\ldots,x_N^T]^T$. The Euclidean norm and union are denoted as $\|\cdot\|$ and $\cup$, respectively. For a symmetric matrix M, $M>0$ (≥ 0) or $M<0$ denotes that the matrix M is positive definite (positive semidefinite) or negative definite, respectively, and its maximum and minimum eigenvalues are denoted by $\lambda_{\max}(M)$ and $\lambda_{\min}(M)$, respectively. In addition, to facilitate the calculation, we give the definition of Kronecker product below. If $M=[m_{ij}]\in\mathbb{R}^{\alpha\times\beta}$ and $N=[n_{ij}]\in\mathbb{R}^{p\times q}$, then the Kronecker product $M\otimes N\in\mathbb{R}^{\alpha p\times\beta q}$ is the block matrix

$$M\otimes N=\begin{bmatrix} m_{11}N & \cdots & m_{1\beta}N \\ \vdots & \ddots & \vdots \\ m_{\alpha 1}N & \cdots & m_{\alpha\beta}N \end{bmatrix}.$$

II. Problem Statement and Preliminaries

Fig. 1 depicts the structure of the ith agent under DoS attacks, which mainly consists of sensor, actuator, controller, buffers, zero-order hold (ZOH), AMETM, and observer. When the AMETM picks out state variables that need to be sampled, these data are transmitted to observers and controllers over the network. If DoS attacks occur, the data transmission will be blocked, which will adversely affect the system stability and performance.

A. Graph Theory

The multi-agent system is assumed to have an undirected topology $\mathcal{G}=(\mathcal{V},\mathcal{E})$ where $\mathcal{V}=\{1,\ldots,N\}$ is the node set and $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ is the edge set. Each agent is represented by a node. In graph $\mathcal{G}$, if nodes i and j can exchange information with each other, then node j is a neighbor of node i and vice

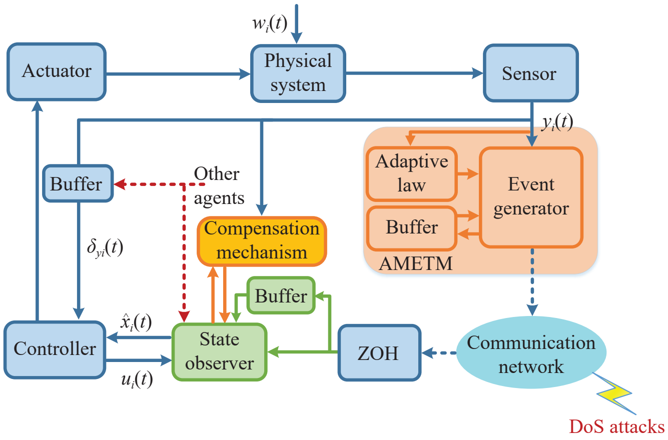


Fig. 1. Framework of the *i*th agent under DoS attacks.

versa. Let $\mathcal{N}_i=\{j\in\mathcal{V}|(j,i)\in\mathcal{E}, j\neq i\}$ represent the set of neighbor nodes of node i, and $\mathcal{A}=[a_{ij}]\in\mathbb{R}^{N\times N}$ be the adjacency matrix, where $a_{ij}=1$ if $(j,i)\in\mathcal{E}$, which means that agent i can receive information from agent j; otherwise, $a_{ij}=0$. For an undirected graph, $(j,i)\in\mathcal{E}$ implies $(i,j)\in\mathcal{E}$. Furthermore, define the degree matrix $\mathcal{D}=\text{diag}\{d_1,\ldots,d_N\}\in\mathbb{R}^{N\times N}$ with $d_i=\sum_{j\in N_i}a_{ij}$; then, the Laplacian matrix $\mathcal{L}$ is denoted by $\mathcal{L}=\mathcal{D}-\mathcal{A}$. For the fixed undirected graph $\mathcal{G}$, its Laplacian matrix $\mathcal{L}$ is a symmetric matrix with eigenvalues satisfying $0=\lambda_1(\mathcal{L})<\lambda_2(\mathcal{L})<\cdots<\lambda_N(\mathcal{L})$. For brevity, $\lambda_2(\mathcal{L})$ and $\lambda_N(\mathcal{L})$ will be denoted respectively as λ_2 and λ_N in the rest of this paper.

B. System Model

Consider a nonlinear MAS of N agents with the dynamics of the *i*th agent being given by

$$\begin{cases}\dot{x}_i(t)=(A+\Delta A)x_i(t)+Bu_i(t)+Dw_i(t)+Ff(x_i(t),t)\\ y_i(t)=Cx_i(t),\ i=1,\ldots,N\end{cases}\tag{1}$$

where $x_i(t)\in\mathbb{R}^n$, $u_i(t)\in\mathbb{R}^b$, $y_i(t)\in\mathbb{R}^q$, and $w_i(t)\in\mathbb{R}^d$ are the state, input, output and external disturbance of the *i*th agent, respectively. $f(x_i(t),t)=\text{col}\{f_1(x_i(t),t),\ldots,f_n(x_i(t),t)\}\in\mathbb{R}^n$ represents the nonlinear dynamics of the *i*th agent. Furthermore, A, B, C, D, and F are known matrices with appropriate dimensions, and ΔA is a time-varying uncertain matrix. Suppose that $\text{rank}(B)=\text{rank}(B,D)=b$.

Assumption 1: The pair (A,B) is stabilizable, the pair (A,C) is observable, and matrix C is of full row rank.

Assumption 2: There exists a positive constant ϖ and a matrix $E(t)$, such that

$$\Delta A(t)=\varpi AE(t)\tag{2}$$

where time-varying matrix $E(t)$ satisfies $E^T(t)E(t)\leq I_N$.

Assumption 3: There exists a matrix Λ such that $\forall x_1(t),x_2(t)\in\mathbb{R}^n$, the nonlinear function $f(x_i(t),t)$ satisfies

$$||f(x_2(t),t)-f(x_1(t),t)||\leq||\Lambda(x_2(t)-x_1(t))||.\tag{3}$$

Assumption 4: The disturbance signal $w_i(t)$ is bounded, i.e., $||w_i(t)||\leq\bar{w}$, where $\bar{w}$ is a known upper bound of the disturbance signal.

Remark 1: Assumption 1 is common in many existing results [10], [25], [39]. Assumption 2 is a constraint condition for the uncertainties that may be caused by mismatched parameters, inaccuracies in the model, etc. [40]. The mild Lipschitz condition in Assumption 3 describes a class of nonlinear systems, such as robot systems. In fact, all linear functions and piecewise time-invariant continuous functions also satisfy this assumption [41], [42].

C. DoS Attack Model and AMETM

In this paper, as shown in Fig. 1, we only consider DoS attacks that affect the updating of the controller, i.e., the first type of DoS attacks mentioned in the introduction section, which prevents the transmission of sensor data by destroying the communication channel from sensors to observers. It affects the updating of the observer and controller. In addition, under DoS attacks, each agent may be attacked at any time. In practice, however, it is impossible for an attacker to launch a continuous attack because it needs to gather energy for the next attack. Next, to facilitate the analysis, the relevant definitions of DoS attacks are given below.

Let $\{h_k\}_{k\geq 0}$ be a time sequence of DoS attacks, where the kth DoS time interval is $\mathcal{H}_k=[h_k,h_k+\eta_k)$ with $h_{k+1}>h_k+\eta_k$, in which h_k is the instant when the kth DoS attack starts, and $\eta_k>0$ indicates the duration of the kth attack. Over the time interval $[t_0,t)$, let $\Phi(t)$ denote the time period set, where communication is subjected to attack, and let $\Psi(t)$ denote the time period set, where communication is allowed. Then,

$$\Phi(t)=\underset{k\in\mathbb{N}}{\cup}\mathcal{H}_k\cap[t_0,t)$$
$$\Psi(t)=[t_0,t)\backslash\Phi(t).\tag{4}$$

In addition, to describe the influence of DoS attacks on trigger points, we give the following definition.

Definition 1 (Communication Failure Frequency [32]): For $\forall t>t_0$, let $n(t_0,t)$ denote the total number of trigger points under attack during $[t_0,t)$ for each agent. Then, the frequency of attack on trigger points $\ell(t_0,t)$ over $[t_0,t)$ is defined as

$$\ell(t_0,t)=\frac{n(t_0,t)}{t-t_0}.\tag{5}$$

Remark 2: In order to distinguish between a DoS attack and package dropout, the differences are summarized as follows: 1) The number of packet losses usually belongs to an integer set, and the number of continuous packet losses is usually a small number, while the DoS attack may last for a long period of time. For example, when the communication failure frequency is less than a certain value, the considered DoS attacks may include the case in which the network is blocked for a certain period of time. However, this case usually does not fall into the category of packet loss owing to the fact that the continuous packet loss is less than a small number. 2) From 1), we know that the developed method is effective when the communication failure frequency is smaller than a certain value. Thus, as long as a class of packet losses meet this condition, the developed mathematical framework is also applicable for addressing issues related to this class of packet losses. Note that such a framework for dealing with packet loss has not been used in the existing literature; therefore, it is also a new method in the area of handling packet loss.

Assume that $\{t_k^i\}$ is the event time set for the *i*th agent. For convenience of statement, define

$$\xi_i(t) = \sum_{j\in N_i}(x_i(t) - x_j(t))$$

$$e_{i,t_{k-p+1}}(t) = \xi_i(t^i_{k-p+1}) - \xi_i(t) \tag{6}$$

where $p \in \mathbb{N}$ denotes the number of data stored in a buffer. Then, in contrast to the traditional event triggering scheme, a novel AMETM is proposed as follows:

$$g_i(t) = \left(\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right)^T \Theta\left(\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right) - c_i(t)\xi_i^T(t)\Theta\xi_i(t) \tag{7}$$

where $\Theta = C^TC$, ε_p's are given positive constants with $\sum_{p=1}^{m}\varepsilon_p = 1$, and $c_i(t) \in (0,\bar{c}] \subseteq (0,1)$ is the adaptive trigger parameter and obeys the following update law:

$$\dot{c}_i(t) = \begin{cases} 0, & c_i(t) \geq \bar{c} \\ \beta_i\xi_i^T(t)\Theta\xi_i(t), & c_i(t) < \bar{c} \end{cases} \tag{8}$$

with β_i being a positive constant and $\bar{c}$ representing the upper bound of $c_i(t)$.

Remark 3: Compared with the centralized event triggered condition designed by accumulating all agent errors in [32], this paper adopts the event triggered condition (7) that requires neighboring agents only. This can effectively reduce unnecessary communication. Differently from the traditional event triggered condition [21], recently triggered packets are also used by adding a buffer of size m to (7). Note that the latest released packet is more important, so the choice of ε_1 should be larger than the other ε_p's. By adjusting the value of ε_p, we can change the number of trigger points. A smaller ε_1 and a larger m will trigger more points to ensure system performance. When $\varepsilon_1 = 1$ and $m = 1$, the event triggering scheme degenerates to a normal adaptive trigger mechanism, as in [33]. In addition, the trigger speed depends on $c_i(t)$. The smaller $c_i(t)$ is, the more triggers there are but the better the system performance is. Alternately, the larger $c_i(t)$ is, the fewer triggers there are but the worse the system performance is. Obviously, the larger the number of triggers, the heavier the communication burden. Moreover, when $c_i(t) = 0$, the event triggering scheme becomes a time triggering mechanism. Therefore, the choice of $c_i(t)$ should be a trade-off between system performance and communication burden.

To avoid Zeno behavior, similarly to [17], [32], the next triggered instant is determined as follows:

$$t^i_{k+1} = \begin{cases} \inf\{t > t^i_k | g_i(t) > 0\}, & t^i_k \in \Psi(t) \\ t^i_k + \sigma, & t^i_k \in \Phi(t) \end{cases} \tag{9}$$

where σ is a given positive constant.

In this study, undirected communication networks are considered, and the control objective is to design a control strategy based on observation information to ensure that the multi-agent system (1) can achieve consensus in the presence of DoS attacks and disturbance, i.e., $\lim_{t\to\infty}\left\| x_i(t) - \frac{1}{N}\sum_{i=1}^{N}x_i(t)\right\| = 0$, $i = 1,2,\ldots,N$.

Furthermore, to achieve the purpose of this article, the following Lemmas are necessary.

Lemma 1 [32]: For a positive definite function $V(t)$, if it satisfies:

1) $\dot{V}(t) \leq -\alpha V(t)$, for $t_k \in \Psi(t)$

2) $\dot{V}(t) \leq \rho\max\{V(t), V(t_{s+1})\}$, for $t_k \in \Phi(t)$

where α and ρ are unknown positive constants, and t_{s+1} is the next trigger instant with the latest successful trigger instant being t_s when $t \in [t_k, t_{k+1})$ and $t_k \in \Phi(t)$. Then, the following inequality holds:

$$V(t) \leq e^{[-\alpha(t-t_0-n(t_0,t)\sigma)+\rho n(t_0,t)\sigma]}V(t_0). \tag{10}$$

Lemma 2 [24]: For a matrix equality constraint, i.e., $PB = BN$, it can be transformed into a standard linear matrix inequality and be rewritten approximately as

$$\begin{bmatrix} -\nu I & PB - BN \\ * & -\nu I \end{bmatrix} < 0 \tag{11}$$

where ν is an arbitrarily small positive constant.

III. Main Results

In this section, an anti-disturbance control strategy based on a state observer is proposed, which improves the observer accuracy by storing the previous data in a buffer and compensating for the uncertainty and disturbance. The secure consensus of the multi-agent system subject to external disturbances and DoS attacks is analyzed, and the conditions for ensuring consensus are given. In addition, the problem of coupling observer and controller gains with unknown matrix variables is solved by using the linear matrix inequality (LMI) technique. Finally, Zeno behavior is excluded for all agents.

A. Design of Observer and Controller

The state observer for the ith agent is constructed as below:

$$\begin{cases} \dot{\hat{x}}_i(t) = \begin{cases} A\hat{x}_i(t) + Bu_i(t) + Ff(\hat{x}_i(t),t) + H_i(t) + DG_i(t) \\ \quad +LC\left(\sum\limits_{p=1}^{m}\varepsilon_p\xi_i(t^i_{k-p+1}) - \hat{\xi}_i(t)\right), \quad t^i_k \in \Psi(t) \\ A\hat{x}_i(t) + Bu_i(t) + Ff(\hat{x}_i(t),t) + H_i(t) + DG_i(t) \\ \quad +LC\left(\sum\limits_{p=1}^{m}\varepsilon_p\xi_i(t^i_{s-p+1}) - \hat{\xi}_i(t)\right), \quad t^i_k \in \Phi(t) \end{cases} \\ \hat{y}_i(t) = C\hat{x}_i(t), \quad i \in \mathcal{V} \end{cases} \tag{12}$$

where $\hat{x}_i(t) \in \mathbb{R}^n$ and $\hat{y}_i(t) \in \mathbb{R}^q$ denote the estimated state and output of the ith agent, respectively; L is the observer gain to be designed; t^i_s is the latest successful trigger instant while t^i_k is the instant of DoS attack; and $H_i(t)$ and $G_i(t)$ are the compensation for the uncertainty and disturbance of the ith agent, respectively, and can be designed as follows:

$$H_i(t) = \begin{cases} \chi_2\varpi^2(1+\chi_3)\dfrac{\hat{x}_i^T(t)A^TA\hat{x}_i(t)}{2e^T_{y_i}e_{y_i}}P_1^{-1}C^Te_{y_i}, & e_{y_i} \neq 0 \\ 0, & e_{y_i} = 0 \end{cases} \tag{13}$$

$$G_i(t) = \begin{cases} \bar{w}\dfrac{We_{y_i}(t)}{\left\|We_{y_i}(t)\right\| + \hbar_1}, & e_{y_i} \neq 0 \\ 0, & e_{y_i} = 0 \end{cases} \tag{14}$$

where $\chi_2 > 0$, $\chi_3 > 0$, $P_1 \in \mathbb{R}^{n\times n}$ being positive definite and $W \in \mathbb{R}^{d\times q}$ are matrix variables to be designed, $\hbar_1$ is a small positive constant, and the output estimation error $e_{y_i}(t)$ is defined as $e_{y_i}(t)=y_i(t)-\hat{y}_i(t)$.

Next, based on state observer (12), for each agent i, the observer-based controller is given by

$$u_i(t)=-K\hat{x}_i(t)-B^{+}Dz_i(t) \tag{15}$$

where matrix B^{+} satisfies $(I_N-BB^{+})D=0$ and can be calculated by Lemma 2, K is the controller gain to be designed, and $z_i(t)$ obeys

$$z_i(t)=\begin{cases}\bar{w}\dfrac{W_1\delta_{y_i}(t)}{\|W_1\delta_{y_i}(t)\|+\hbar_2}, & \delta_{y_i}(t)\neq 0\\ 0, & \delta_{y_i}(t)=0\end{cases} \tag{16}$$

with $\hbar_2$ being a small positive constant, $\bar{w}$ denoting the upper bound of the disturbance signal, $W_1\in\mathbb{R}^{d\times q}$ being the matrix parameter to be designed, and the output consensus error $\delta_{y_i}(t)$ being defined as $\delta_{y_i}(t)=y_i(t)-(1/N)\sum_{i=1}^{N}y_i(t)$.

Remark 4: It is worth mentioning that the control strategy (15) and (16) removes the assumption that the state is measurable as in [20] and only needs to use state estimation information $\hat{x}_i(t)$ and output consensus error information $\delta_{y_i}(t)$, which can be obtained in practical applications. Therefore, the control strategy is more practical. In addition, in contrast to the observer designed in [25], by introducing a buffer in observer (12), not only the current released packet $\xi_i(t_k^i)$ but also some recent packets, $\{\xi_i(t_{k-1}^i),\xi_i(t_{k-2}^i),\ldots\}$, are used. Even in the presence of DoS attacks, due to the existence of the buffer, the state can also be accurately estimated. Moreover, unlike [38] in which a disturbance observer was used based on the state-feedback control technique to reduce the influence of external disturbances, the accuracy of the state observer (12) is improved by introducing the uncertainty compensation $H_i(t)$ in (13) and the external disturbance compensation $G_i(t)$ in (14) simultaneously. Furthermore, the difficulty caused by unmeasurable states can be avoided.

B. Consensus Analysis

To simplify the notation, denote the state estimation error $e_{x_i}(t)=x_i(t)-\hat{x}_i(t)$. Then, it follows from (1) and (15) that

$$\begin{aligned}\dot{x}(t)=&\,[I_N\otimes(A-BK)+\Delta\tilde{A}]x(t)+(I_N\otimes BK)e_x(t)\\&+(I_N\otimes F)f(x(t),t)+(I_N\otimes D)w(t)-(I_N\otimes BB^{+}D)z(t)\end{aligned} \tag{17}$$

where

$$\begin{aligned}&x(t)=\operatorname{col}\{x_1(t),\ldots,x_N(t)\},z(t)=\operatorname{col}\{z_1(t),\ldots,z_N(t)\}\\&\Delta\tilde{A}=\operatorname{diag}\{\Delta A,\ldots,\Delta A\},w(t)=\operatorname{col}\{w_1(t),\ldots,w_N(t)\}\\&e_x(t)=\operatorname{col}\{e_{x_1}(t),\ldots,e_{x_N}(t)\}\\&f(x(t),t)=\operatorname{col}\{f(x_1(t),t),\ldots,f(x_N(t),t)\}.\end{aligned}$$

By defining the average state $\bar{x}(t)=(1/N)\sum_{i=1}^{N}x_i(t)$ and consensus error $\delta_i(t)=x_i(t)-\bar{x}(t)$, we have $\delta(t)=(M\otimes I_n)x(t)$, where $\delta(t)=\operatorname{col}\{\delta_1(t),\cdots,\delta_N(t)\}$ and $M=I_N-(1/N)1_N1_N^T$. Moreover, it is not difficult to see that $\mathcal{L}M=M\mathcal{L}=\mathcal{L}$, and we can obtain that $\xi(t)=(\mathcal{L}\otimes I_n)\delta(t)$ with $\xi(t)=\operatorname{col}\{\xi_1(t),\ldots,\xi_N(t)\}$.

Then, based on the above definitions and (17), the dynamic of the consensus error δ is given by

$$\begin{aligned}\dot{\delta}(t)=&\,[I_N\otimes(A-BK)+\Delta\tilde{A}]\delta(t)+(M\otimes BK)e_x(t)\\&+(I_N\otimes F)\tilde{f}(x(t),t)+(M\otimes D)w(t)-(M\otimes BB^{+}D)z(t)\end{aligned} \tag{18}$$

where

$$\begin{aligned}\tilde{f}(x(t),t)=\operatorname{col}\Big\{&(f(x_1(t),t)-\frac{1}{N}\sum_{i=1}^{N}f(x_i(t),t)),\ldots,\\&(f(x_N(t),t)-\frac{1}{N}\sum_{i=1}^{N}f(x_i(t),t))\Big\}.\end{aligned}$$

Next, the main results of this article are presented in the following theorem.

Theorem 1: Suppose that Assumptions 1–4 hold. Under the observer-based anti-disturbance controller (15) and the triggering function (7) with the triggering sequence (9), MAS (1) can achieve consensus and the designed observer (12) can give accurate estimate of the state in the presence of DoS attacks and external disturbances, if there exist symmetric positive definite matrices P_1, P_2 and matrices L, K, W, and W_1 satisfying

$$\begin{bmatrix}\Pi_{11} & *\\ \lambda_{\max}(M)P_2BK & \Pi_{22}\end{bmatrix}<0 \tag{19}$$

$$P_1D=C^TW^T \tag{20}$$

$$P_2D=C^TW_1^T \tag{21}$$

$$\begin{bmatrix}\bar{\Pi}_{11} & *\\ \lambda_{\max}(M)P_2BK & \bar{\Pi}_{22}\end{bmatrix}\leq\frac{\rho}{2}\bar{P} \tag{22}$$

$$\begin{bmatrix}0 & 0\\ * & \tilde{\Pi}_{22}\end{bmatrix}\leq\frac{\rho}{2}\bar{P} \tag{23}$$

$$\ell(t_0,t)\leq\frac{\alpha-\varsigma}{(\alpha+\rho)\sigma} \tag{24}$$

where

$$\begin{aligned}\Pi_{11}=&\,A^TP_1+P_1A+\frac{1}{\gamma}P_1FF^TP_1+\gamma\Lambda^T\Lambda+\frac{1}{\chi_1}P_1LL^TP_1\\&+\frac{1}{\chi_2}P_1P_1+\chi_2\varpi^2\left(1+\frac{1}{\chi_3}\right)A^TA-\lambda_2(P_1LC\\&+C^TL^TP_1)+\alpha P_1\\ \Pi_{22}=&\,A^TP_2+P_2A-P_2BK-K^TB^TP_2+\varpi P_2AA^TP_2\\&+\varpi I+\frac{1}{\gamma}P_2FF^TP_2+\gamma\Lambda^T\Lambda+\chi_1\bar{c}\lambda_N^2\Theta+\alpha P_2\\ \bar{\Pi}_{11}=&\,A^TP_1+P_1A+\frac{1}{\gamma}P_1FF^TP_1+\gamma\Lambda^T\Lambda+\theta_1P_1LL^TP_1\\&+\frac{1}{\chi_2}P_1P_1+\chi_2\varpi^2\left(1+\frac{1}{\chi_3}\right)A^TA-\lambda_2(P_1LC\\&+C^TL^TP_1)\\ \bar{\Pi}_{22}=&\,A^TP_2+P_2A-P_2BK-K^TB^TP_2+\varpi P_2AA^TP_2\\&+\varpi I+\frac{1}{\gamma}P_2FF^TP_2+\gamma\Lambda^T\Lambda+2\bar{\theta}_2\lambda_N^2\Theta\\ \tilde{\Pi}_{22}=&\,(\bar{\theta}_1\bar{c}+2\bar{\theta}_2)\lambda_N^2\Theta\end{aligned}$$

with $\bar{\theta}_1 = (1+1/\theta_2)/\theta_1$, $\bar{\theta}_2 = (1+\theta_2)/\theta_1$, and $\Theta = C^T C$. Besides, α, χ_1, χ_2, χ_3, θ_1, θ_2, γ, and ρ are positive constants, ς satisfies $0 < \varsigma < \alpha$, and matrix $\bar{P} = \mathrm{diag}\{P_1, P_2\}$.

Proof: The proof of Theorem 1 is given in Appendix. ■

Remark 5: In order to solve LMIs (19)–(23) more easily, we can pre-set the parameters of the same type, such as χ_1, χ_2, and χ_3, to the same value, and then adjust them by trial-and-error method. Besides, for conditions (22) and (23) in Theorem 1, since (19)–(21) have solved for P_1, P_2, L, and K, we only need to find a suitable ρ to satisfy these conditions instead of solving for L and K with (19)–(23). This can simplify the solution process.

Remark 6: In many existing results (such as [16], [17], [19]) on the secure consensus of multi-agent systems under DoS attacks, time is divided into two parts according to whether t is during the interval of DoS attacks, so the duration and frequency of DoS attacks are restricted. However, in this paper, we discuss whether the trigger time is during DoS attacks, so there is no need to limit the frequency and duration of DoS attacks separately. Instead, we just limit the frequency of communication failures, which will also indirectly limit DoS attacks. Moreover, the constraints need to be met for all agents.

Remark 7: In previous works [16]–[19], [32], [43], algebraic Riccati equation (ARE) and algebraic Riccati inequality (ARI) are used to solve for the control gain. It should be pointed out that these methods are very conservative when the matrix dimension is large or there are many parameters. In this paper, the observer and the controller are simultaneously designed based on the LMI technique without adjusting the parameters and the symmetric positive definite matrices in advance. In addition, the obtained conditions without involving the Kronecker product will be convenient to solve.

C. Joint Design of Observer and Controller

The conditions of Theorem 1 ensure that the MAS achieves consensus and observers observe the system state under external disturbances and DoS attacks. However, since L and K in (19) are coupled with unknown matrices, and (20), (21) are equality constraints, they cannot be solved directly using the LMI toolbox in MATLAB. To facilitate finding a solution, the following theorem presents a design method for observer and controller gains.

Theorem 2: For given positive scalars α, γ, χ_1, χ_2, χ_3, ν and ϖ, if there exist symmetric positive definite matrices P_1 and P_2, and matrices Q_1, N, $\bar{K}$, W and W_1 satisfying the following conditions:

$$\begin{bmatrix} \Pi'_{11} & Q_1 & P_1 & P_1F & \Pi'_{15} & 0 & 0 \\ * & -\chi_1 & 0 & 0 & 0 & 0 & 0 \\ * & * & -\chi_2 & 0 & 0 & 0 & 0 \\ * & * & * & -\gamma & 0 & 0 & 0 \\ * & * & * & * & \Pi'_{55} & \sqrt{\varpi}P_2A & P_2F \\ * & * & * & * & * & -I & 0 \\ * & * & * & * & * & * & -\gamma \end{bmatrix} < 0 \tag{25}$$

$$\begin{bmatrix} -\nu I & P_2B - BN \\ * & -\nu I \end{bmatrix} < 0 \tag{26}$$

$$\begin{bmatrix} -\nu I & P_1D - C^T W^T \\ * & -\nu I \end{bmatrix} < 0 \tag{27}$$

$$\begin{bmatrix} -\nu I & P_2D - C^T W_1^T \\ * & -\nu I \end{bmatrix} < 0 \tag{28}$$

where

$$\begin{aligned} \Pi'_{11} &= A^T P_1 + P_1 A + \gamma \Lambda^T \Lambda + \chi_2 \varpi^2 \left(1 + \frac{1}{\chi_3}\right) A^T A \\ &\quad - \lambda_2 (Q_1 C + C^T Q_1^T) + \alpha P_1 \\ \Pi'_{15} &= \lambda_{\max}(M) \bar{K}^T B^T \\ \Pi'_{55} &= A^T P_2 + P_2 A - B\bar{K} - \bar{K}^T B^T + \varpi I + \gamma \Lambda^T \Lambda \\ &\quad + \chi_1 \bar{c} \lambda_N^2 \Theta + \alpha P_2. \end{aligned}$$

Then, the observer and the controller gains are given by $L = P_1^{-1} Q_1$ and $K = N^{-1} \bar{K}$, respectively.

Proof: Let $Q_1 = P_1 L$, $P_2 B = BN$, and $NK = \bar{K}$. Then, (19) can be written as

$$\begin{bmatrix} \Pi_{11} & * \\ \lambda_{\max}(M) B\bar{K} & \Pi_{22} \end{bmatrix} < 0$$

where

$$\begin{aligned} \Pi_{11} &= A^T P_1 + P_1 A + \frac{1}{\gamma} P_1 F F^T P_1 + \gamma \Lambda^T \Lambda + \frac{1}{\chi_1} Q_1 Q_1^T \\ &\quad + \frac{1}{\chi_2} P_1 P_1 + \chi_2 \varpi^2 \left(1 + \frac{1}{\chi_3}\right) A^T A - \lambda_2 (Q_1 C \\ &\quad + C^T Q_1^T) + \alpha P_1 \\ \Pi_{22} &= A^T P_2 + P_2 A - B\bar{K} - \bar{K}^T B^T + \varpi P_2 A A^T P_2 + \varpi I \\ &\quad + \frac{1}{\gamma} P_2 F F^T P_2 + \gamma \Lambda^T \Lambda + \chi_1 \bar{c} \lambda_N^2 \Theta + \alpha P_2. \end{aligned}$$

Next, using the Schur complement lemma and Lemma 2, we can obtain (25)–(28). ■

D. Zeno Behavior Analysis

Zeno behavior is a very important issue in the event-triggering strategy. Zeno behavior will result in unlimited triggers in finite time, which is physically unrealizable and obviously violates the original intention of the event-triggering strategy to reduce the number of triggers. Therefore, we should endeavor to avoid it.

In this paper, a mixed event-triggering method is adopted to determine the triggered time instants. If DoS attacks occur, a fixed time σ is used to determine the next triggered instant, so Zeno behavior will not occur during this period. If DoS attacks do not occur, the trigger function $g_i(t)$ in (7) will determine the next trigger moment. Next, the following theorem shows that a positive lower bound exists between two arbitrary consecutive event instants in communication areas, which proves that Zeno behavior does not occur.

Theorem 3: Under the event triggering strategy (9), Zeno behavior will not be exhibited in MAS (1) and the minimum time interval between any inter-event instants is strictly positive when DoS attacks do not occur. That is

$$t_{k+1}^i - t_k^i \geq \frac{\Omega_i^2}{\|C\|\left[2\left\|\bar{A}\right\|\Xi_i^2 + 2\Xi_i\Gamma_i(t_k^i)\right]} > 0 \tag{29}$$

where

$$\Omega_i^2 = \left\|C\sum\nolimits_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|^2$$

$$\|\bar{A}\| = \|A\| + \|\varpi A\| + \|F\Lambda\|$$

$$\Xi_i^2 = \left\|\sum\nolimits_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|^2$$

$$\Gamma_i(t_k^i) = \left\|\bar{A}\right\|\left\|\sum_{p=1}^{m}\varepsilon_p\xi_i(t_{k-p+1}^i)\right\| + 2|\mathcal{N}_i|\,\|D\|\,\|\bar{w}\| + \|B\| \times \left\|\sum_{j\in\mathcal{N}_i}(u_i(t)-u_j(t))\right\|$$

and $|\mathcal{N}_i|$ represents the number of neighbors of the ith agent.

Proof: For any $t \in [t_k^i, t_{k+1}^i)$, we have

$$\begin{aligned}
&\frac{d}{dt}\left\|\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|^2\\
&\leq 2\left\|\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|\left\|\sum_{j\in\mathcal{N}_i}(\dot{x}_i(t)-\dot{x}_j(t))\right\|\\
&\leq 2\left\|\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|\left(\left\|\bar{A}\right\|\left\|\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|\right.\\
&\quad+\left\|\bar{A}\right\|\left\|\sum_{p=1}^{m}\varepsilon_p\xi_i(t_{k-p+1}^i)\right\| + \left\|\sum_{j\in\mathcal{N}_i}(Bu_i(t)-Bu_j(t))\right.\\
&\quad\left.\left.+\sum_{j\in\mathcal{N}_i}(Dw_i(t)-Dw_j(t))\right\|\right)\\
&\leq 2\left\|\bar{A}\right\|\left\|\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|^2 + 2\left\|\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|\\
&\quad\times\left(\left\|\bar{A}\right\|\left\|\sum_{p=1}^{m}\varepsilon_p\xi_i(t_{k-p+1}^i)\right\| + 2|\mathcal{N}_i|\left\|D\right\|\left\|\bar{w}\right\|\right.\\
&\quad\left.+\left\|B\right\|\left\|\sum_{j\in\mathcal{N}_i}(u_i(t)-u_j(t))\right\|\right).
\end{aligned}\tag{30}$$

Since $\Omega_i^2 = \left\|C\sum_{p=1}^{m}\varepsilon_p e_{i,t_{k-p+1}}(t)\right\|^2$, the inequality (30) can be rewritten as

$$\frac{d}{dt}\left(\Omega_i^2\right) \leq \|C\|[2\left\|\bar{A}\right\|\Xi_i^2 + 2\Xi_i\Gamma_i(t_k^i)] \tag{31}$$

where $\|\bar{A}\|$ and $\Gamma_i(t_k^i)$ are defined in (29). At the event-triggering instants $t_1^i, t_2^i, \ldots, t_k^i, \ldots$, it can be seen from (7) that the following inequality holds:

$$\Omega_i^2 > c_i(t)\left\|C\xi_i(t_k^i)\right\|^2 \geq 0. \tag{32}$$

Then, by combining (31) with (32), we obtain

$$t_{k+1}^i - t_k^i \geq \epsilon_i > \frac{\Omega_i^2}{\|C\|[2\left\|\bar{A}\right\|\Xi_i^2 + 2\Xi_i\Gamma_i(t_k^i)]} \tag{33}$$

and can conclude that $\Xi_i > 0$ and $\Gamma_i(t_k^i) > 0$, which implies that $\epsilon_i > 0$. Hence, we have $t_{k+1}^i - t_k^i \geq \min\{\epsilon_i, \sigma\} > 0$. ■

Remark 8: It should be pointed out that the proof process of Theorem 3 is enlightened by [43]. Note that the interval ϵ_i between two events is related to $c_i(t)$, so it is very important to select an appropriate $c_i(t)$ to achieve a balance between the performance and communication burden. In addition, the existence of a hybrid update mechanism means that a lower bound always exists when DoS attacks occur; thus, this mechanism prevents continuous triggering.

IV. Simulation Examples

In this section, we demonstrate the validity of our method by using the communication topology shown in Fig. 2. Consider each agent with the dynamic as (1) and system matrices as follows:

$$A = \begin{bmatrix} -2.9 & 0.3 & 0.4 & 1.2\\ -0.1 & -0.2 & 0.6 & 1.5\\ 1.2 & 2.1 & -2.8 & 3.4\\ 1 & -2 & -2.5 & -2.5 \end{bmatrix},\ B = \begin{bmatrix} 0 & 0\\ 0 & 0\\ -1 & 0.5\\ -0.1 & 0.2 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 1 \end{bmatrix},\ D = \begin{bmatrix} 0\\ 0\\ -0.1\\ -0.1 \end{bmatrix},\ E(t) = \sin(t)I_4$$

$$F = 0.01I_4.$$

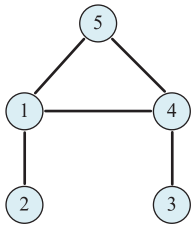


Fig. 2. Communication topology.

In addition, the nonlinear function $f(x_i(t),t)$ is denoted as $f(x_i(t),t) = [0,0,0,0.01\sin(x_{i1}(t))]^T$. Then, according to Assumption 3, one has $\Lambda = \mathrm{diag}\{0.01,\ldots,0.01\}$. Moreover, from Fig. 2, it is easy to obtain the Laplacian matrix $\mathcal{L}$ whose minimum non-zero eigenvalue and maximum eigenvalue are 0.6972 and 4.3028, respectively.

It is worth noting that in the following simulation part, we consider the following two different types of disturbances acting on the first agent to show the validity of the proposed method

$$w_1^1(t) = 0.7\cos(t), \qquad t \geq 0s$$

$$w_1^2(t) = \begin{cases} 0.5\cos(2t+1), & 0s \leq t < 9s\\ 0.4, & t \geq 9s \end{cases}$$

and there are no disturbances to other agents.

Then, based on Theorems 1 and 2, we choose parameters

$\varpi = 0.0001$, $\gamma = 1$, $\chi_1 = 0.01$, $\chi_2 = 4.5$, $\chi_3 = 0.01$, $\nu = 0.001$, $\alpha = 0.25$, $\rho = 4$, $\varsigma = 0.001$ and $\sigma = 0.04$. By solving LMIs (25)–(28), the observer gain L, the controller gain K and matrices P_1, W, and W_1 are obtained as follows:

$$L = \begin{bmatrix} 0.0006 & 0.0000 & 0.0007 \\ 0.0000 & 0.0023 & -0.0010 \\ 0.0005 & 0.0005 & 0.0014 \\ 0.0002 & -0.0015 & 0.0020 \end{bmatrix}$$

$$K = \begin{bmatrix} 0.1435 & -2.5926 & 0.2402 & -1.9829 \\ 0.5258 & -2.2773 & -0.1509 & -1.5060 \end{bmatrix}$$

$$P_1 = \begin{bmatrix} 15.4884 & -0.1750 & -5.4519 & -1.6695 \\ -0.1750 & 7.5176 & -3.1816 & 6.2076 \\ -5.4519 & -3.1816 & 8.9619 & -2.4892 \\ -1.6695 & 6.2076 & -2.4892 & 8.9626 \end{bmatrix}$$

$$W = \begin{bmatrix} 0.7121 & -0.3026 & -0.6473 \end{bmatrix}$$

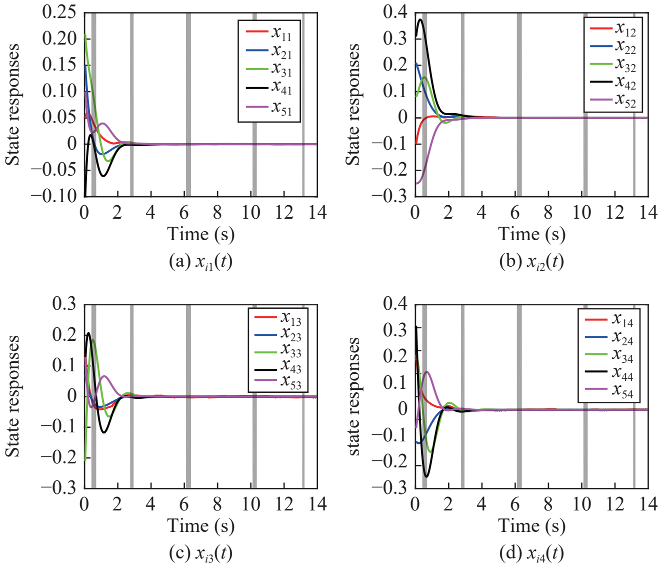
$$W_1 = \begin{bmatrix} 0.0001 & 0.0004 & -5.3476 \end{bmatrix}.$$

To achieve a trade-off between the system performance and communication burden, the parameters and initial coupling gains in the trigger function (7) and the adaptive law (8) are selected as $m = 3$, $\varepsilon_1 = 0.8$, $\varepsilon_2 = 0.15$, $\varepsilon_3 = 0.05$, $\beta_i = 0.1$, $\bar{c} = 0.3$, $c_1(0) = 0.27$, $c_2(0) = 0.28$, $c_3(0) = 0.28$, $c_4(0) = 0.1$ and $c_5(0) = 0.2$. Furthermore, the initial states of each agent are given in Table I.

TABLE I
INITIAL STATES OF EACH AGENT

Initial states	Agent 1	Agent 2	Agent 3	Agent 4	Agent 5
$x_{i1}/\hat{x}_{i1}$	0.05/–0.15	0.15/–0.05	0.21/0.11	–0.1/0.18	0.1/0.1
$x_{i2}/\hat{x}_{i2}$	–0.1/0.24	0.21/0.16	0.08/0.02	0.31/0.15	–0.25/0.1
$x_{i3}/\hat{x}_{i3}$	0.14/–0.2	0.07/0.21	–0.21/0.23	0.11/–0.24	0.13/0.14
$x_{i4}/\hat{x}_{i4}$	0.21/0.17	–0.12/0.1	0.19/–0.1	0.32/0.02	–0.07/–0.08

It is assumed that the disturbance signal $w_1^1(t)$ occurs for the first agent. Define the consensus error of the whole system as $J(t) = (1/N)\sqrt{\sum_{i=1}^{N} \|x_i(t) - \bar{x}(t)\|^2}$. The simulation results are shown in Figs. 3–7. Fig. 3 displays the state trajectories of the five agents, with gray bars indicating DoS attacks that act on all agents when the attacks occur. Note that our proposed control scheme can achieve better consensus even in the presence of external disturbances and DoS attacks. The adaptive coupling gains $c_i(t)$ and triggering instants of each agent are depicted in Figs. 4 and 5, respectively. From Fig. 5 and through calculation, we can find that the communication failure frequency of each agent satisfies (24) and prevents Zeno behavior. In addition, we find that the dense period of trigger points corresponds to the time when the disturbance signal changes most violently, i.e., when its first derivative is the largest. To achieve the ideal performance in the presence of disturbances, more packets are needed to adapt to the disturbances. This requires the event-triggered mechanism to generate more trigger points during the disturbance, which is consistent with the theoretical analysis. The observer errors for the first agent with or without disturbance compensation $G_i(t)$ in observer (12) under $w_1^1(t)$ are shown in Figs. 6. From this, we can see that the observer errors gradually tend toward 0 with $G_i(t)$. The consensus errors of the five agents with and without disturbance compensation $z_i(t)$ in control scheme (15) are shown in Fig. 7. It can be found from Figs. 6 and 7 that



(a) $x_{i1}(t)$
(b) $x_{i2}(t)$
(c) $x_{i3}(t)$
(d) $x_{i4}(t)$

Fig. 3. State trajectories of five agents under DoS attacks and $w_1^1(t)$.

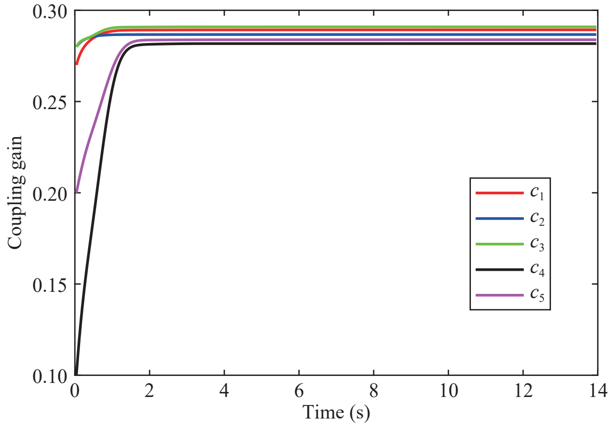


Fig. 4. Adaptive coupling gains $c_i(t)$ under $w_1^1(t)$.

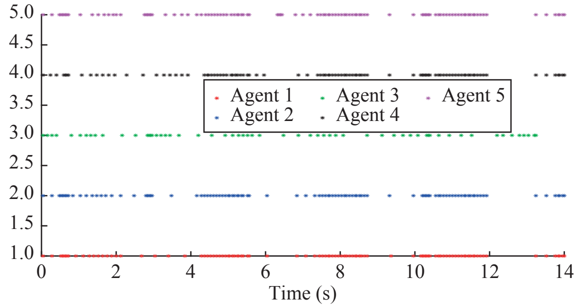
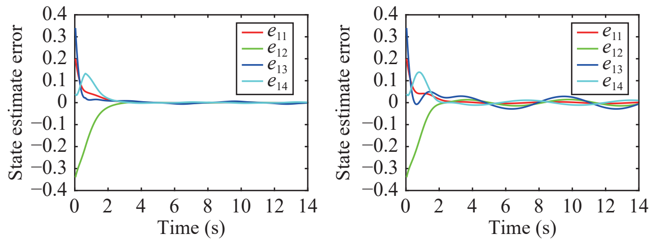


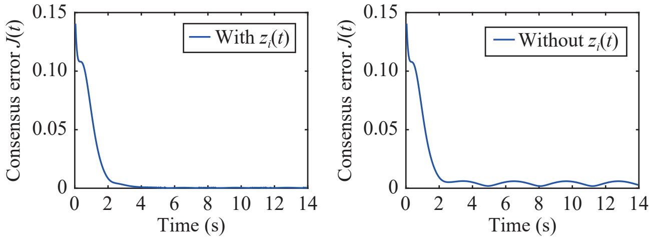
Fig. 5. Triggering instants of each agent under $w_1^1(t)$.



(a) With $G_i(t)$ in observer (b) Without $G_i(t)$ in observer

Fig. 6. Observer errors for the first agent with (a) and without (b) disturbance compensation $G_i(t)$ in observer (12) under $w_1^1(t)$.

better state estimation performance and consensus performance are achieved by introducing disturbance compensation $G_i(t)$ and $z_i(t)$, which illustrates the validity of the proposed method.



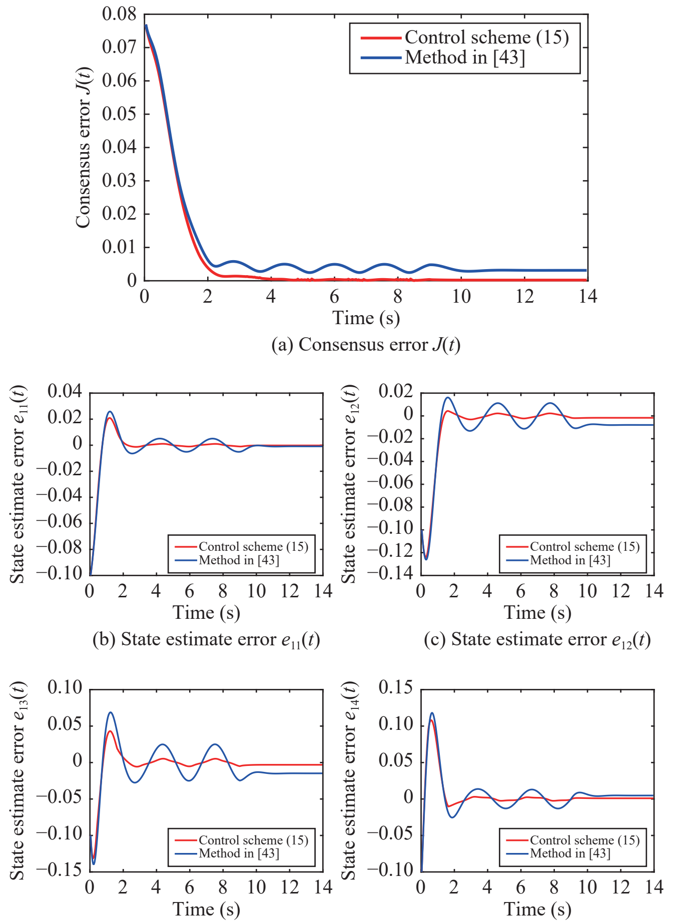
(a) With $z_i(t)$ in controller (b) Without $z_i(t)$ in controller

Fig. 7. The consensus error of five agents with (a) and without (b) disturbance compensation $z_i(t)$ in control scheme (15) under $w_1^1(t)$.

To further highlight the advantages of our design method, comparisons with existing methods are made in the following. To make the comparisons more obvious, suppose that the disturbance signal $w_1^2(t)$ occurs for the first agent, and the initial states are reset as $x_1(0) = [-0.05\ -0.05\ -0.05-0.05]^T$, $x_2(0) = [0.05\ 0.05\ 0.05\ 0.05]^T$, $x_3(0) = [0.1\ 0.1\ 0.1\ 0.1]^T$, $x_4(0) = [0.15\ 0.15\ 0.15\ 0.15]^T$, $x_5(0) = [0.2\ 0.2\ 0.2\ 0.2]^T$. Fig. 8 displays the comparison between two different methods, one of which uses the AMETM (7) and the observer-based controller (15) proposed in this paper. The other uses the method of [44]. From Fig. 8, we can see that the control strategy of [44] can not achieve consensus due to the existence of external disturbances, and the designed observer can not track the states accurately. Nevertheless, our method introduces a compensation mechanism for the observer and controller, which can achieve better performance. Moreover, Table II shows the number of releases under these two different control schemes. By comparison, we can conclude that better consensus performance and state estimation performance are obtained by using the method of this paper. Furthermore, the communication burden is also reduced.

V. Conclusions

In this paper, the consensus problem of nonlinear MASs subject to DoS attacks is studied. More practically, external disturbances and uncertainties have also been considered in this work. An observer-based controller design method is proposed to ensure the consensus of MAS under DoS attacks and disturbance signals. The controller gain and observer gain are obtained through a joint design method. Moreover, to reduce the communication burden, an AMETM for MAS is designed, whose updates not only depend on the current state but also previously stored information, and Zeno behavior is eliminated. Finally, simulation results show the advantages of our method. Note that in this paper, only undirected network communication is considered in the cyber layer. Thus, how to extend this result to directed network communication is an interesting future research direction. In addition, extending these results to fault-tolerant problems will also be a future research topic.



(a) Consensus error $J(t)$

(b) State estimate error $e_{11}(t)$ (c) State estimate error $e_{12}(t)$

(d) State estimate error $e_{13}(t)$ (e) State estimate error $e_{14}(t)$

Fig. 8. Comparison between proposed observer-based control scheme (15) in Theorem 1 and the method in [44] under $w_1^2(t)$.

TABLE II
Trigger Numbers of Each Agent Under Different Control Schemes

Control scheme	Agent 1	Agent 2	Agent 3	Agent 4	Agent 5
Control scheme (15)	69	74	68	71	75
Method in [44]	72	104	104	98	96

Appendix

Proof of Theorem 1: Choose the Lyapunov function candidate as follows

$$V(t) = \sum_{i=1}^{N} V_i(t) = \sum_{i=1}^{N} \zeta_i^T(t)\bar{P}\zeta_i(t) \tag{34}$$

where $\zeta_i(t) = \text{col}\{e_{x_i}(t), \delta_i(t)\}$. Then, according to whether t_k^i is under attack instant, we divide the proof process into two parts. First, consider $t \in [t_k^i, t_{k+1}^i)$.

1) If $t_k^i \in \Psi(t)$ with $\Psi(t)$ as in (4), this means that the latest sampling information can be collected.

Recalling that $e_{x_i}(t) = x_i(t) - \hat{x}_i(t)$, one can deduce that

$$\begin{aligned}\dot{e}_x(t) = {} & (I_N \otimes A - \mathcal{L} \otimes LC)e_x(t) + (I_N \otimes \Delta A)x(t) + (I_N \\ & \otimes D)w(t) + (I_N \otimes F)\hat{f}(x(t),t) - (I_N \otimes I)H(t) \\ & - (I_N \otimes D)G(t) - (I_N \otimes LC)\sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t) \qquad (35)\end{aligned}$$

where

$$\begin{aligned}\hat{f}(x(t),t) = {} & \mathrm{col}\{f(x_1(t),t) - f(\hat{x}_1(t),t), \ldots, \\ & f(x_N(t),t) - f(\hat{x}_N(t),t)\} \\ \sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t) = {} & \mathrm{col}\left\{ \sum_{p=1}^{m} \varepsilon_p e_{1,t_{k-p+1}}(t), \ldots, \right. \\ & \left. \sum_{p=1}^{m} \varepsilon_p e_{N,t_{k-p+1}}(t) \right\}.\end{aligned}$$

Based on (18) and (35), the time derivative of $V(t)$ is

$$\begin{aligned}\dot{V}(t) = {} & e_x^T(t)[I_N \otimes (A^T P_1 + P_1 A) - \mathcal{L} \otimes (P_1 LC + C^T L^T \\ & \times P_1)]e_x(t) + 2e_x^T(t)(I_N \otimes P_1 \Delta A)x(t) + 2e_x^T(t)(I_N \\ & \otimes P_1 D)w(t) + 2e_x^T(t)(I_N \otimes P_1 F)\hat{f}(x(t),t) \\ & - 2e_x^T(t)(I_N \otimes P_1)H(t) - 2e_x^T(t)(I_N \otimes P_1 D)G(t) \\ & - 2e_x^T(t)(I_N \otimes P_1 LC)\sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t) + \delta^T(t)[I_N \\ & \otimes (A^T P_2 + P_2 A - P_2 BK - K^T B^T P_2) + \Delta\tilde{A}^T(I_N \\ & \otimes P_2) + (I_N \otimes P_2)\Delta\tilde{A}]\delta(t) + 2\delta^T(t)(M \otimes P_2 BK) \\ & \times e_x(t) + 2\delta^T(t)(I_N \otimes P_2 F)\tilde{f}(x(t),t) + 2\delta^T(t)(M \\ & \otimes P_2 D)w(t) - 2\delta^T(t)(M \otimes P_2 BB^+ D)z(t). \qquad (36)\end{aligned}$$

From Assumption 3, it is not difficult to derive that

$$\begin{aligned}& 2e_x^T(t)(I_N \otimes P_1 F)\hat{f}(x(t),t) \\ & \quad \le e_x^T(t)\left[I_N \otimes \left(\frac{1}{\gamma}P_1 F F^T P_1 + \gamma \Lambda^T \Lambda\right)\right]e_x(t). \qquad (37)\end{aligned}$$

Note that $\sum_{i=1}^{N} \delta_i = 0$, so we have $\sum_{i=1}^{N} {\delta_i}^T P_2 F[f(\bar{x}(t),t) - (1/N)\sum_{i=1}^{N} f(x_i(t),t)] = 0$. Then, one can obtain

$$\begin{aligned}2\delta^T(t)(I_N \otimes P_2 F)\tilde{f}(x(t),t) = {} & 2\sum_{i=1}^{N} {\delta_i}^T P_2 F \tilde{f}(x_i(t),t) \\ = {} & 2\sum_{i=1}^{N} {\delta_i}^T P_2 F \Bigg[f(x_i(t),t) - f(\bar{x}(t),t) + f(\bar{x}(t),t) \\ & - \frac{1}{N}\sum_{i=1}^{N} f(x_i(t),t) \Bigg] \\ \le {} & \delta^T(t)\left[I_N \otimes \left(\frac{1}{\gamma}P_2 F F^T P_2 + \gamma \Lambda^T \Lambda\right)\right]\delta(t). \qquad (38)\end{aligned}$$

By letting $\tilde{E}(t) = \mathrm{diag}\{E(t), \ldots, E(t)\}$, we obtain $\Delta\tilde{A} = \varpi(I_N \otimes A)\tilde{E}(t)$, $\Delta\tilde{A}^T = \varpi\tilde{E}^T(I_N \otimes A^T)$. Thus,

$$\begin{aligned}& \delta^T(t)[\Delta\tilde{A}^T(I_N \otimes P_2) + (I_N \otimes P_2)\Delta\tilde{A}]\delta(t) \\ & \quad \le \delta^T(t)[\varpi I_N \otimes (P_2 A A^T P_2 + I)]\delta(t). \qquad (39)\end{aligned}$$

Furthermore, it follows from the Young's inequality that

$$\begin{aligned}& -2e_x^T(t)(I_N \otimes P_1 LC)\sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t) \\ & \quad \le \frac{1}{\chi_1} e_x^T(t)(I_N \otimes P_1 L L^T P_1)e_x(t) + \chi_1 \left(\sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t)\right)^T \\ & \qquad \times (I_N \otimes C^T C)\left(\sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t)\right) \qquad (40)\end{aligned}$$

$$\begin{aligned}& 2e_x^T(t)(I_N \otimes P_1 \Delta A)x(t) \\ & \quad \le \frac{1}{\chi_2} e_x^T(t)(I_N \otimes P_1 P_1)e_x(t) + \chi_2 \varpi^2 x^T(t)(I_N \otimes A^T A)x(t) \\ & \quad \le \frac{1}{\chi_2} e_x^T(t)(I_N \otimes P_1 P_1)e_x(t) + \chi_2 \varpi^2 \left(1 + \frac{1}{\chi_3}\right)e_x^T(t)(I_N \\ & \qquad \otimes A^T A)e_x(t) + \chi_2 \varpi^2 (1 + \chi_3)\hat{x}^T(t)(I_N \otimes A^T A)\hat{x}(t) \qquad (41)\end{aligned}$$

and according to (7), we have

$$\begin{aligned}& \left(\sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t)\right)^T (I_N \otimes C^T C)\left(\sum_{p=1}^{m} \varepsilon_p e_{t_{k-p+1}}(t)\right) \\ & \quad \le c(t)\xi^T(t)(I_N \otimes C^T C)\xi(t) = c(t)\delta^T(t)(\mathcal{L}^2 \otimes C^T C)\delta(t)\end{aligned}$$

where $c(t) = \mathrm{diag}\{c_1(t), \ldots, c_N(t)\}$.

Since $P_1 D = C^T W^T$ and $P_2 D = C^T W_1^T$ hold in (20) and (21), respectively, we can easily deduce that

$$\begin{aligned}& 2e_x^T(t)(I_N \otimes P_1 D)w(t) - 2e_x^T(t)(I_N \otimes P_1 D)G(t) \le 0 \\ & 2\delta^T(t)(M \otimes P_2 D)w(t) - 2\delta^T(t)(M \otimes P_2 BB^+ D)z(t) \le 0. \qquad (42)\end{aligned}$$

Then, substituting (37)–(42) into (36) yields

$$\begin{aligned}\dot{V}(t) \le {} & e_x^T(t)\Bigg[I_N \otimes \Bigg(A^T P_1 + P_1 A + \frac{1}{\gamma}P_1 F F^T P_1 + \gamma \Lambda^T \Lambda \\ & + \frac{1}{\chi_2}P_1 P_1\Bigg) - \mathcal{L} \otimes (P_1 LC + C^T L^T P_1) + \chi_2 \varpi^2 \Bigg(1 \\ & + \frac{1}{\chi_3}\Bigg)(I_N \otimes A^T A) + \frac{1}{\chi_1} I_N \otimes P_1 L L^T P_1 \Bigg]e_x(t) \\ & + \delta^T(t)\Bigg[I_N \otimes \Bigg(A^T P_2 + P_2 A - P_2 BK - K^T B^T P_2 \\ & + \frac{1}{\gamma}P_2 F F^T P_2 + \gamma \Lambda^T \Lambda + \varpi P_2 A A^T P_2 + \varpi I\Bigg) + \chi_1 \\ & \times c(t)(\mathcal{L}^2 \otimes \Theta)\Bigg]\delta(t) + 2\delta^T(t)(M \otimes P_2 BK)e_x(t). \qquad (43)\end{aligned}$$

By using condition (19), the following inequality can be determined

$$\dot{V}_i(t) \le \zeta_i^T(t)(-\alpha\bar{P})\zeta_i(t) = -\alpha V_i(t) \qquad (44)$$

where α is a positive constant.

2) If $t_k^i \in \Phi(t)$ with $\Phi(t)$ as in (4), this means that the latest sampling information cannot be collected. Moreover, it is assumed that DoS attacks block the network channel from t_{s+1}^i, so one obtains

$$\begin{aligned}\dot{e}_x(t) = {} & (I_N \otimes A - \mathcal{L} \otimes LC)e_x(t) + (I_N \otimes \Delta A)x(t) + (I_N \\ & \otimes D)w(t) + (I_N \otimes F)\hat{f}(x(t),t) - (I_N \otimes I)H(t) \\ & - (I_N \otimes D)G(t) - (I_N \otimes LC)\left(\sum_{p=1}^{m} \varepsilon_p \xi(t_{s-p+1}) \right. \\ & \left. - \xi(t_{s+1})\right) - (I_N \otimes LC)(\xi(t_{s+1}) - \xi(t)) \end{aligned} \tag{45}$$

where $\xi(t_{s+1}) - \xi(t) = \mathrm{col}\{\xi_1(t_{s+1}^1) - \xi_1(t), \ldots, \xi_N(t_{s+1}^N) - \xi_N(t)\}$. Then, we have

$$\begin{aligned}\dot{V}(t) = {} & e_x^T(t)[I_N \otimes (A^T P_1 + P_1 A) - \mathcal{L} \otimes (P_1 LC + C^T L^T \\ & \times P_1)]e_x(t) + 2e_x^T(t)(I_N \otimes P_1 \Delta A)x(t) + 2e_x^T(t)(I_N \\ & \otimes P_1 D)w(t) + 2e_x^T(t)(I_N \otimes P_1 F)\hat{f}(x(t),t) \\ & - 2e_x^T(t)(I_N \otimes P_1)H(t) - 2e_x^T(t)(I_N \otimes P_1 D)G(t) \\ & - 2e_x^T(t)(I_N \otimes P_1 LC)\left(\sum_{p=1}^{m} \varepsilon_p \xi(t_{s-p+1}) - \xi(t_{s+1})\right) \\ & - 2e_x^T(t)(I_N \otimes P_1 LC)(\xi(t_{s+1}) - \xi(t)) + \delta^T(t)[I_N \\ & \otimes (A^T P_2 + P_2 A - P_2 BK - K^T B^T P_2) + \Delta\tilde{A}^T(I_N \\ & \otimes P_2) + (I_N \otimes P_2)\Delta\tilde{A}]\delta(t) + 2\delta^T(t)(M \otimes P_2 BK) \\ & \times e_x(t) + 2\delta^T(t)(I_N \otimes P_2 F)\tilde{f}(x(t),t) + 2\delta^T(t)(M \\ & \otimes P_2 D)w(t) - 2\delta^T(t)(M \otimes P_2 BB^+ D)z(t). \end{aligned} \tag{46}$$

According to the Young's inequality, we can obtain

$$\begin{aligned} & -2e_x^T(t)(I_N \otimes P_1 LC)\left(\sum_{p=1}^{m} \varepsilon_p \xi(t_{s-p+1}) - \xi(t_{s+1})\right) \\ & \quad \le \frac{1}{\bar{\theta}_1} e_x^T(t)(I_N \otimes P_1 LL^T P_1)e_x(t) + \bar{\theta}_1 \left(\sum_{p=1}^{m} \varepsilon_p \xi(t_{s-p+1}) \right. \\ & \quad \left. - \xi(t_{s+1})\right)^T (I_N \otimes C^T C)\left(\sum_{p=1}^{m} \varepsilon_p \xi(t_{s-p+1}) - \xi(t_{s+1})\right) \\ & -2e_x^T(t)(I_N \otimes P_1 LC)(\xi(t_{s+1}) - \xi(t)) \\ & \quad \le \frac{1}{\bar{\theta}_2} e_x^T(t)(I_N \otimes P_1 LL^T P_1)e_x(t) + \bar{\theta}_2(\xi(t_{s+1}) - \xi(t))^T \\ & \quad \times (I_N \otimes C^T C)(\xi(t_{s+1}) - \xi(t)). \end{aligned} \tag{47}$$

From the event-triggered condition (7), we have

$$\begin{aligned} & \left(\sum_{p=1}^{m} \varepsilon_p \xi(t_{s-p+1}) - \xi(t_{s+1})\right)^T (I_N \otimes C^T C) \\ & \quad \times \left(\sum_{p=1}^{m} \varepsilon_p \xi(t_{s-p+1}) - \xi(t_{s+1})\right) \\ & \quad \le c(t_{s+1})\xi^T(t_{s+1})(I_N \otimes C^T C)\xi(t_{s+1}). \end{aligned} \tag{48}$$

Additionally, it is easy to conclude that

$$\begin{aligned} & (\xi(t_{s+1}) - \xi(t))^T (I_N \otimes C^T C)(\xi(t_{s+1}) - \xi(t)) \\ & \quad \le 2\xi^T(t_{s+1})(I_N \otimes C^T C)\xi(t_{s+1}) + 2\xi^T(t)(I_N \otimes C^T C)\xi(t). \end{aligned} \tag{49}$$

Next, using the analysis methods in Part 1), combining (47) and (48) with (49), and according to LMIs (22) and (23), we can deduce from (46) that

$$\begin{aligned}\dot{V}_i(t) & \le \zeta_i^T(t)\left(\frac{\rho\bar{P}}{2}\right)\zeta_i(t) + \zeta_i^T(t_{s+1}^i)\left(\frac{\rho\bar{P}}{2}\right)\zeta_i(t_{s+1}^i) \\ & \le \rho \max\{V_i(t), V_i(t_{s+1}^i)\}. \end{aligned} \tag{50}$$

Then, it follows from (44), (50) and Lemma 1 that

$$V_i(t) \le e^{[-\alpha(t-t_0-n(t_0,t)\sigma)+\rho n(t_0,t)\sigma]} V_i(t_0). \tag{51}$$

which, according to (24), is equivalent to

$$V_i(t) \le e^{-\varsigma(t-t_0)} V_i(t_0). \tag{52}$$

Thus,

$$V(t) \le e^{-\varsigma(t-t_0)} V(t_0) \tag{53}$$

which means that $V(t)$ is bounded. Therefore, the secure average consensus of MASs (1) is guaranteed. ■

References

[1] J. J. Cui, Y. W. Liu, and A. Nallanathan, "Multi-agent reinforcement learning-based resource allocation for UAV networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 729–743, Feb. 2020.

[2] D. Chowdhury and H. K. Khalil, "Practical synchronization in networks of nonlinear heterogeneous agents with application to power systems," *IEEE Trans. Autom. Control*, vol. 66, no. 1, pp. 184–198, Jan. 2021.

[3] Y. Kikuya, S. M. Dibaji, and H. Ishii, "Fault-tolerant clock synchronization over unreliable channels in wireless sensor networks," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1551–1562, Dec. 2018.

[4] M. B. Khalkhali, A. Vahedian, and H. S. Yazdi, "Multi-target state estimation using interactive kalman filter for multi-vehicle tracking," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1131–1144, Mar. 2020.

[5] L. W. An and G. H. Yang, "Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks," *IEEE Trans. Cybern.*, vol. 49, no. 3, pp. 827–838, Mar. 2019.

[6] C. Deng and C. Y. Wen, "Distributed resilient observer-based faulttolerant control for heterogeneous multiagent systems under actuator faults and DoS attacks," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 3, pp. 1308–1318, Sep. 2020.

[7] Y. M. Wu and X. X. He, "Secure consensus control for multiagent systems with attacks and communication delays," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 136–142, Jan. 2017.

[8] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: a survey of recent advances," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 2, pp. 319–333, Feb. 2021.

[9] W. L. He, Z. K. Mo, Q. -L. Han, and F. Qian, "Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1326–1334, Sep. 2020.

[10] X. Huang and J. X. Dong, "Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 89–99, Jan. 2020.

[11] G. Franze, F. Tedesco, and D. Famularo, "Resilience against replay attacks: A distributed model predictive control scheme for networked multi-agent systems," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 3, pp. 628–640, Mar. 2021.

[12] C. J. Zhou, B. W. Hu, Y. Shi, Y. C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proc. IEEE*, vol. 109, no. 4, pp. 517–541, Apr. 2021.

[13] Y. Wan, G. H. Wen, X. H. Yu, and T. W. Huang, "Distributed consensus tracking of networked agent systems under Denial-of-Service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, Jan. 2020. DOI: 10.1109/TSMC.2019.2960301.

[14] E. Mousavinejad, F. W. Yang, Q. L. Han, X. H. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, Sep. 2020.

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

[16] T. Y. Zhang and D. Ye, "Distributed event-triggered control for multiagent systems under intermittently random denial-of-service attacks," *Inf. Sci.*, vol. 542, pp. 380–390, Jan. 2021.

[17] Z. Feng and G. Q. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 741–752, May 2020.

[18] Y. Xu, M. Fang, Z. G. Wu, Y. J. Pan, M. Chadli, and T. W. Huang, "Input-based event-triggering consensus of multiagent systems under denial-of-service attacks," *IEEE Trans. Syst.*, *Man*, *Cybern.*, *Syst.*, vol. 50, no. 4, pp. 1455–1464, Apr. 2020.

[19] Y. Yang, Y. F. Li, D. Yue, Y. C. Tian, and X. H. Ding, "Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks," *IEEE Trans. Cybern.*, vol. 51, no. 6, pp. 2916–2928, Jun. 2021.

[20] L. Zhao and G. H. Yang, "Adaptive fault-tolerant control for nonlinear multi-agent systems with DoS attacks," *Inf. Sci.*, vol. 526, pp. 39–53, Jul. 2020.

[21] J. L. Liu, T. T. Yin, D. Yue, H. R. Karimi, and J. D. Cao, "Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 162–173, Jan. 2021.

[22] X. G. Guo, X. Fan, J. L. Wang, and J. H. Park, "Event-triggered switching-type fault detection and isolation for fuzzy control systems under DoS attacks," *IEEE Trans. Fuzzy Syst.*, to be published, Sep. 2020. DOI: 10.1109/TFUZZ.2020.3021734.

[23] W. C. Zou, C. K. Ahn, and Z. R. Xiang, "Fuzzy-approximation-based distributed fault-tolerant consensus for heterogeneous switched nonlinear multiagent systems," *IEEE Trans. Fuzzy Syst.*, to be published, Jul. 2020. DOI: 10.1109/TFUZZ.2020.3009730.

[24] X. G. Guo, J. L. Wang, and F. Liao, "Adaptive quantised H_∞ observer-based output feedback control for non-linear systems with input and output quantisation," *IET Control Theory Appl.*, vol. 11, no. 2, pp. 263–272, Jan. 2017.

[25] S. L. Hu, D. Yue, Q. L. Han, X. P. Xie, X. L. Chen, and C. X. Dou, "Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1952–1964, May 2020.

[26] Z. Y. Wu, H. D. Mo, J. L. Xiong, and M. Xie, "Adaptive event-triggered observer-based output feedback $\mathcal{L}_\infty$ load frequency control for networked power systems" *IEEE Trans. Ind. Inf.*, vol. 16, no. 6, pp. 3952–3962, Jun. 2020.

[27] Y. Wu, H. Liang, Y. Zhang, and C. K. Ahn, "Cooperative adaptive dynamic surface control for a class of high-order stochastic nonlinear multi-agent systems," *IEEE Trans. Cybern.* to be published, May 2020. DOI: 10.1109/TCYB.2020.2986332.

[28] X. G. Guo, J. L. Wang, F. Liao, and R. S. H. Teo, "Distributed adaptive sliding mode control strategy for vehicle-following systems with nonlinear acceleration uncertainties," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 981–991, Feb. 2017.

[29] I. Furtat, E. Fridman, and A. Fradkov, "Disturbance compensation with finite spectrum assignment for plants with input delay," *IEEE Trans. Autom. Control*, vol. 63, no. 1, pp. 298–305, Jan. 2018.

[30] Y. Yuan, Z. D. Wang, and L. Guo, "Event-triggered strategy design for discrete-time nonlinear quadratic games with disturbance compensations: the noncooperative case," *IEEE Trans. Syst.*, *Man*, *Cybern.*, *Syst.*, vol. 48, no. 11, pp. 1885–1896, Nov. 2018.

[31] X. G. Guo, X. Fan, and C. K. Ahn, "Adaptive event-triggered fault detection for interval type-2 T-S fuzzy systems with sensor saturation," *IEEE Trans. Fuzzy Syst.*, to be published, May 2020. DOI: 10.1109/TFUZZ.2020.2997515.

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

[33] D. Ye, M. M. Chen, and H. J. Yang, "Distributed adaptive eventtriggered fault-tolerant consensus of multiagent systems with general linear dynamics," *IEEE Trans. Cybern.*, vol. 49, no. 3, pp. 757–767, Mar. 2019.

[34] B. Cheng and Z. K. Li, "Fully distributed event-triggered protocols for linear multiagent networks," *IEEE Trans. Autom. Control*, vol. 64, no. 4, pp. 1655–1662, Apr. 2019.

[35] S. L. Hu, D. Yue, X. P. Xie, X. L. Chen, and X. X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 12, pp. 4271–4281, Dec. 2019.

[36] E. G. Tian, K. Y. Wang, X. Zhao, S. B. Shen, and J. L. Liu, "An improved memory-event-triggered control for networked control systems," *J. Franklin Inst.*, vol. 356, no. 13, pp. 7210–7223, Sep. 2019.

[37] K. Y. Wang, E. G. Tian, S. B. Shen, L. N. Wei, and J. L. Zhang, "Input-output finite-time stability for networked control systems with memory event-triggered scheme," *J. Franklin Inst.*, vol. 356, no. 15, pp. 8507–8520, Oct. 2019.

[38] C. L. Liu, L. Shan, Y. Y. Chen, and Y. Zhang, "Average-consensus filter of first-order multi-agent systems with disturbances," *IEEE Trans. Circuits Syst.*, *II*, *Exp. Briefs*, vol. 65, no. 11, pp. 1763–1767, Nov. 2018.

[39] X. D. Wang, Z. Y. Fei, T. Wang, and L. Yang, "Dynamic event-triggered actuator fault estimation and accommodation for dynamical systems," *Inf. Sci.*, vol. 525, pp. 119–133, Jul. 2020.

[40] B. H. Wang, W. S. Chen, J. C. Wang, B. Zhang, Z. Q. Zhang, and X. G. Qiu, "Accurate cooperative control for multiple leaders multiagent uncertain systems: a two-layer node-to-node communication framework," *IEEE Trans. Ind. Inf.*, vol. 14, no. 6, pp. 2395–2405, Jun. 2018.

[41] Y. B. Gao, J. X. Liu, G. H. Sun, M. Liu, and L. G. Wu, "Fault deviation estimation and integral sliding mode control design for Lipschitz nonlinear systems," *Syst. Control Lett.*, vol. 123, pp. 8–15, Jan. 2019.

[42] A. ur Rehman, M. Rehan, N. Iqbal, and C. K. Ahn, "LPV scheme for robust adaptive output feedback consensus of lipschitz multiagents using lipschitz nonlinear protocol," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, Jan. 2020. DOI: 10.1109/TSMC.2020.2964567.

[43] Y. Xu, M. Fang, P. Shi, and Z. G. Wu, "Event-based secure consensus of mutiagent systems against DoS attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3468–3476, Aug. 2020.

[44] R. N. Yang and W. X. Zheng, "Output-based event-triggered predictive control for networked control systems," *IEEE Trans. Ind. Electron.*, vol. 67, no. 12, pp. 10631–10640, Dec. 2020.

Xianggui Guo received the B.S. degree from College of Electrical Engineering, Northwest University for Nationalities, China, in 2005, and the M.S. degree from College of Electrical Engineering and Automation, Fuzhou University, China in 2008, the Ph.D. degree in control science and engineering from Northeastern University, China in 2012. From 2014 to 2016, he was a Postdoctoral Fellow at School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. From July 2018 to August 2018, he was a Visiting Scholar with the Department of Mechanical Engineering, University of Victoria, Victoria, BC, Canada. Since 2019, he has been a Professor with the School of Automation and Electrical Engineering, University of Science and Technology Beijing, China. His research interests include multi-agent systems, fuzzy systems, vehicular platoon control, and fault-tolerant Control.

Dongyu Zhang received the B.S. degree from School of Instrument and Electronics, North University of China, Taiyuan, China in 2019. He is currently a master student at the School of Automation and Electrical Engineering, University of Science and Technology Beijing, China. His research interest is multi-agent systems.

Jianliang Wang (SM'00) received the B.E. degree in electrical engineering from Beijing Institute of Technology, China in 1982, the M.S. and Ph.D. degrees in electrical engineering from The Johns Hopkins University, USA in 1985 and 1988, respectively, specializing in nonlinear systems and control theory. From 1988 to 1990, he was a Lecturer with Beijing University of Aeronautics and Astronautics, China. From 1990 to 2019, he was an Associate Professor with the School of Electrical and Electronic Engineering at Nanyang Technological University, Singapore. Since 2020, he has been a Professor with Hangzhou Innovation Institute of Beihang University, Hangzhou, China. His research interests include multi-agent systems, fault tolerant control, fault detection and identification, flight control systems, and vehicular platoon control.

Choon Ki Ahn (M'06-SM'12) received the B.S. and M.S. degrees from the School of Electrical Engineering, Korea University, Seoul, Korea, in 2000 and 2002, respectively, the Ph.D. degree from the School of Electrical Engineering and Computer Science, Seoul National University, Seoul, Korea, in 2006. He is currently a Crimson Professor of Excellence with the College of engineering and a Full Professor with the School of electrical engineering, Korea University, Seoul, Korea. His current research interests include control, estimation, fuzzy systems, neural networks, and nonlinear dynamics.

He was the recipient of the Early Career Research Award and Excellent Research Achievement Award of Korea University in 2015 and 2016, respectively. He was awarded the Medal for "Top 100 Engineers" 2010 by IBC, Cambridge, UK. In 2016, he was ranked #1 in Electrical/Electronic Engineering and #2 in entire areas of engineering among Korean young professors based on paper quality. In 2017, he received the Presidential Young Scientist Award from the President of South Korea. In 2019–2021, he received the Research Excellence Award from Korea University (Top 3% Professor of Korea University in Research). He is a member of the IEEE Technical Committee on Cyber-Physical Systems; IEEE Systems, Man, and Cybernetics Society Technical Committee on Intelligent Learning in Control Systems; and IEEE SMCS Technical Committee on Soft Computing. He has been on the editorial board of leading international journals, including the *IEEE Systems, Man, and Cybernetics Magazine; IEEE Transactions on Neural Networks and Learning Systems; IEEE Transactions on Fuzzy Systems; IEEE Transactions on Systems, Man, and Cybernetics: Systems; IEEE Transactions on Automation Science and Engineering; IEEE Transactions on Intelligent Transportation Systems; IEEE Transactions on Circuits and Systems I: Regular Papers; IEEE Systems Journal; Nonlinear Dynamics; Aerospace Science and Technology; Artificial Intelligence Review;* and other flagship journals. He was the recipient of the Highly Cited Researcher Award in Engineering by Clarivate Analytics (formerly, Thomson Reuters).