Resilient Control for Multiagent Systems With a Sampled-Data Model Against DoS Attacks

Fang Fang, *Senior Member, IEEE*, Jiayu Li, Yajuan Liu, and Ju H. Park, *Senior Member, IEEE*

***Abstract*—To reduce the computational burden and resist the denial-of-service (DoS) attacks, a resilient distributed sampled-data control scheme is proposed for multiagent systems. The agent states are sampled periodically by the sensors. DoS attacks disrupt the data communication from transmitters to controllers randomly or periodically with a limited duration time. Information on DoS attacks can be obtained by introducing novel logic processors embedded in corresponding controllers. Next, the problem of resilient control can be converted into one concerned with the upper and lower bound of the sampling interval of an aperiodic sampled-data control system. Some sufficient criteria for developing resilient distributed controllers are derived using the novel looped Lyapunov functional approach and the free-matrix-based inequality method. Finally, two illustrative examples, unmanned aerial vehicles and the two-mass-spring systems, are provided to demonstrate the efficiency of the proposed resilient distributed sampled-data control protocols against the DoS attacks.**

***Index Terms*—Consensus, denial-of-service (DoS) attacks, looped functional, multiagent systems (MASs), resilient control.**

I. Introduction

THE multiagent systems (MASs) are essential for a wide application in many fields, such as formation control of unmanned aerial vehicles (UAVs) [1], cooperative control of intelligent transportation systems [2] and [3], economic dispatch problem in power systems [4], and so on, which leads to further concentration of research in the academic community. Designing an effective consensus protocol for the MASs is a significant issue. A growing body of literature discuss this topic in recent decades, see [5]–[7]. For example, Li *et al.* [5] investigated the high-order scaled consensus of the MASs with external disturbances and time delays. A distributed control technique for voltage regulation in microgrids has been proposed in [6] based on the consensus algorithm.

However, most previous researches on the consensus problem for the MASs have focused on continuous-time control, which require continuous information exchanges among agents. Due to its advantages of high reliability, high accuracy, and great adaptability to the network environment, the sampled-data control has attracted academic attention with the advent of the digital age. Recently, there has been an increasing amount of literature on the sampled-based consensus protocol [8]–[12]. The aim of sampled-data control for MASs is to obtain a larger sampling interval. It is worth mentioning that larger sampling intervals can effectively reduce signal transmission and further save communication resources. In [8], based on an equivalent switched system model, an aperiodic sampled-data consensus strategy is proposed for the heterogeneous agent system. Wu *et al.* [9] dealt with the sampled-data control problem of MASs by introducing the vector extension of Wirtinger's inequality into the Lyapunov functional. In [10], an asynchronous sampled-data control law is developed for leader-following networked heterogeneous systems. However, most of the available information about the actual sampling pattern has not been fully adopted in [9] and [12], and the estimation gap on the upper bound of integral terms needs to be reduced. The existing works leave much room to improve, which is the first motivation of this article.

As is well known, the abovementioned analysis is predicated on the common assumption that the communication environment is reliable and safe. However, in the communication network, the dynamic systems may be constantly subjected to threats from possible malicious attackers, such as DoS attacks [13], [14]. A DoS attack is a typical cyber-attack that may consume excessive network resources in a short period of time, preventing the target systems receiving information. Recently, new technologies about how to counter DoS attacks for MASs are explored as well [15]–[18]. For example, the consensus of MASs subjected to periodic DoS jamming attacks has been explored with distributed event-triggered mechanism, and the allowable uniform lower bound of attack sleep intervals and event-triggering parameters are given by an algorithm [17]. It can be observed that many published works only consider deterministic attacks. Recently, there is a considerable amount of literature where the impact of DoS attacks on the system is treated as stochastic packet dropout following the given probability distribution [19], [20]. Very recently, Zhang *et al.* [21] added a logical processor to the associated controller to obtain

Manuscript received 17 October 2021; revised 20 February 2022; accepted 31 March 2022. Date of publication 7 April 2022; date of current version 8 November 2022. The work of Fang Fang was supported by the National Natural Science Foundation of China under Grant 52176005. The work of Ju H. Park was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (Ministry of Science and ICT) under Grant 2019R1A5A8080290. Paper no. TII-21-4547. (*Corresponding authors: Yajuan Liu; Ju H. Park.*)

Fang Fang, Jiayu Li, and Yajuan Liu are with the School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China (e-mail: ffang@ncepu.edu.cn; jy18708600677@163.com; yajuan.liu.12@gmail.com).

Ju H. Park is with the Department of Electrical Engineering, Yeungnam University, Kyongsan 38541, South Korea (e-mail: jessie@ynu.ac.kr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3165687.

Digital Object Identifier 10.1109/TII.2022.3165687

and handle information on the duration of each DoS attack for networked control systems. To the best of our knowledge, the resilient control for the MASs with a sampled-data model against DoS attacks by using logic processors has not been considered, which is the second motivation of this article.

To summarize the abovementioned analysis, we investigate resilient sampled-data controllers design for the MASs against DoS attacks. The main contributions of this article are listed as follows.

1) By introducing logic processors embedded in corresponding controllers, for the MASs, we construct a unified framework that can collect information on DoS attacks. To the best of our knowledge, this framework was only applied to networked control systems, but for the MASs, it is the first attempt.
2) Different from the existing work on DoS attacks for MASs, the proposed one in the work, where attacks may be random or periodic, can calculate the maximum and minimum duration time of DoS attacks. Next, the problem of resilient control can be converted into one concerned with the upper and lower bound of the sampling interval of an aperiodic sampled-data control system (ASDCS).
3) Compared with the existing results, consensus conditions with larger sampling intervals are derived for the MASs by using innovative looped-functionals with slack variables and the free-matrix-based inequality method.

Notations : $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, $\mathbb{R}^{m\times n}$ denotes the set of all $m\times n$ real matrices, $W_{N_1\times N_2}$ indicates that the matrix W is with N_1 rows and N_2 columns, W^{-1} and W^T denote the transpose and inverse of the matrix W, Sym$\{W\}$ denotes $W+W^T$, $col\{x_1,\ldots,x_n\}$ indicates $[x_1^T,\ldots,x_n^T]$, diag$\{\cdots\}$ indicates the block diagonal matrix, $W>0(W\geq 0)$ indicates that W is a symmetric and positive definite (positive semi-definite) matrix, $*$ denotes symmetric terms in a symmetric matrix, $W_1\otimes W_2$ denotes The Kronecker product of matrices W_1 and W_2, and $\|\cdot\|$ denotes 2-norm.

II. Preliminaries and Problem Formulation

A. Preliminaries

A weighted graph $\mathbb{G}=(\mathbb{V},\mathbb{E},\mathbb{A})$ is used to express communication graph of the MASs network, where $\mathbb{V}=\{v_1,v_2,\ldots,v_N\}$ is a node set, $\mathbb{E}\subseteq\mathbb{V}\times\mathbb{V}$ is an edge set, and $\mathbb{A}=[a_{ij}]_{N\times N}$ is an adjacent matrix. The edge $(v_i,v_j)\in\mathbb{V}$ represents that agent j can obtain information from agent i, then $a_{ij}>0$. If $(v_i,v_j)\notin\mathbb{V}$, $a_{ij}=0$. $\mathbb{N}_i=\{j,(v_j,v_i)\in\mathbb{V}\}$ indicates the set of all neighbors of agent i. The Laplacian Matrix of graph $\mathbb{G}$ is described with $\mathbb{L}=[l_{ij}]_{N\times N}$, where $l_{ii}=\sum_{j\in\mathbb{N}_i}a_{ij}, l_{ij}=-a_{ij}$.

B. System Description

Consider the MASs consisting of N agents with general Lipschitz nonlinearity as follows:

$$\dot{z}_l(d)=\mathcal{A}z_l(d)+v_k(z_l(d))+\mathcal{B}u_l(d), l=1,2,\ldots,N \quad (1)$$

where $z_l(d)\in\mathbb{R}^m$ and $u_l(d)\in\mathbb{R}^k$ are the state variable and the control input of the lth agent at time d, respectively, and $A\in\mathbb{R}^{m\times m}$ and $\mathcal{B}\in\mathbb{R}^{m\times k}$ are known matrices. The nonlinear

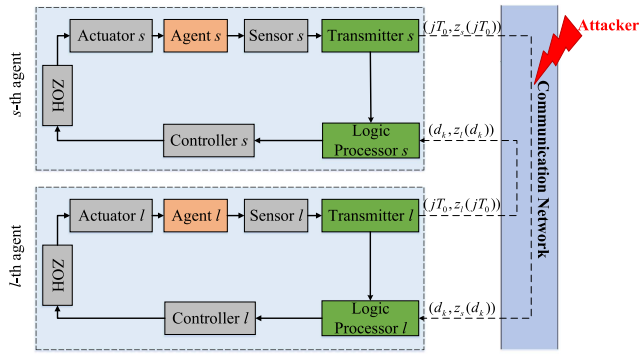


Fig. 1. Framework of the MASs under DoS attacks.

continuous vector-valued function $v_k(z_l(d))\in\mathbb{R}^m$ represents the inherent nonlinear dynamics of the lth agent and meeting the following assumption.

Assumption 1: Each nonlinear function $v_k(\cdot)$ in (1) is Lipschitz continuous and there is a positive constant $v>0$ so that

$$\|\, v_k(\delta_1)-v_k(\delta_2)\,\|\leq m_k\,\|\,\delta_1-\delta_2\,\| \quad (2)$$

for any $\delta_1,\delta_2\in\mathbb{R}^m$.

Before the signal transmission, the lth agent state needs to be sampled within a certain period $T_0>0$ by the sensor $l(l=1,2,\ldots,N)$. The sampling instants sequence is denoted as $\{k_1,k_2,\ldots,k_j,\ldots\}$ with $k_j=jT_0, j\in\mathbf{N}$. The current sampled state $z_l(k_j)$ is encapsulated with the timestamp k_j into the packet $(k_j,z_l(k_j))$ at each sampling instant and later transmitted to the processor through a communication network.

C. Signal Transmitting Process: DoS Attacks and Logic Processors

Motivated by [21], we have equipped every controller with the corresponding logic processor (controller l with logic processor l), then a unified framework that can collect information on DoS attacks is constructed for the MASs (for visualization, see Fig. 1). Subsequently, we will illustrate this signal transmitting process under DoS attacks and the mechanism of how the logic processor works through the following parts.

Every logic processor is made up of a buffer and a comparator. The current sampled-data packets received are stored in the buffer. Once the buffer is updated, all sampled-data packets are subsequently used to generate new control input. The sequence of packets received by the processors is denoted as $\{d_0,d_1,\ldots,d_k,d_{k+1},\ldots\}$ with $d_0=0$. Take the logic controller l as an example, the working mechanism of the comparator can be seen from Fig. 2. The condition $s\in\mathbb{N}_l$ is used to determine whether the agent s is a neighbor of the agent l.

By performing the manipulations shown in Fig. 2, information about DoS attacks can be obtained by the comparator. $h_m, h_M, n_0, T_m, \Delta$, and $\hat{t}$, respectively, represent the minimum attack duration time, maximum attack duration time, total times of DoS attacks, sum of attack duration time of all DoS attacks, time interval between consecutively packets received by the logical processor, and the moment when packets are received successfully in a particular period $[0,T_p]$, where T_p is a particular time instant. If $\Delta>T_0$, we can draw a conclusion that a DoS attack occurs, and n_0 is increased by one.

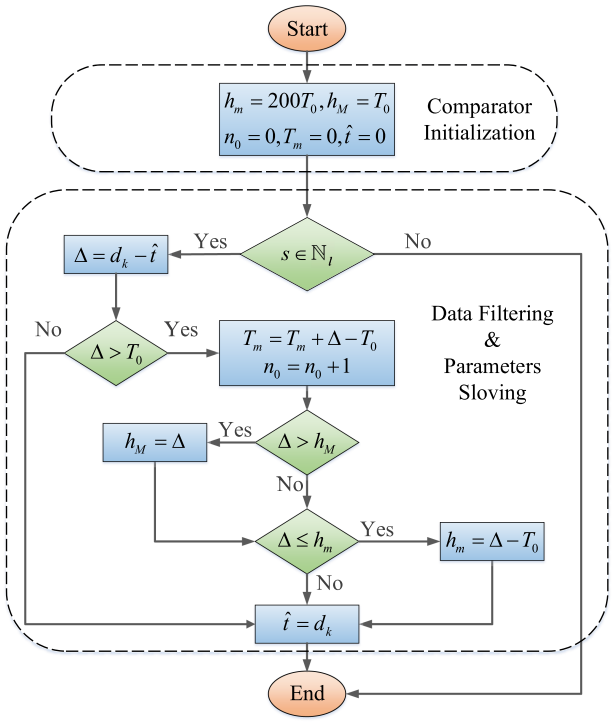


Fig. 2. Flowchart of the mechanism on how the comparator works.

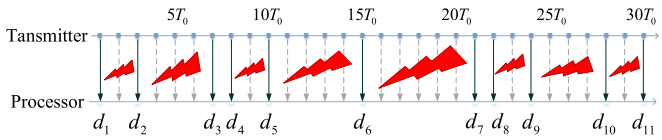


Fig. 3. Example to show the signal transmitting process under a sequence of DoS attacks.

Fig. 3 is used as an example to show the signal transmitting process under a sequence of DoS attacks. The transmitter sends data packets from 30 sampling instants to the logic processor. But due to the DoS attacks, the logic processor only received data packets from 11 sampling instants. At the first sampling instant jT_0, the packet $(d_1, z_s(d_1))$ is received by the processor as soon as the condition $s \in N_l$ is met. Since $\Delta = d_1 - \hat{t} = T_0 - 0 = T_0 \le T_0$, $\hat{t} = d_1 = T_0$ and h_M, h_m, T_m, and n_0 remain the initial values. For convenience, it is assumed that the packets received later with the sequence in Fig. 3 meet this condition: $s \in N_l$. Next, the packet $(d_2, z_s(d_2))$ is received by the processor. Since $\Delta = d_2 - \hat{t} = 3T_0 - T_0 = 2T_0 > T_0$, we can draw a conclusion that a DoS attack occurred during (d_1, d_2). According to Fig. 2, parameters about this attack sequence are calculated $h_M = 2T_0, h_m = T_0, T_m = T_0, n_0 = 1$, and $\hat{t} = d_2$. Subsequently, the same calculations are performed on the received packets in turn. As a result, we have $h_M = 6T_0, h_m = T_0$, $T_m = 19T_0$, and $n_0 = 8$, which means that the MASs has been attacked for eight times during $[0, 30T_0)$, that the minimum (maximum) attack duration time is $6T_0(T_0)$, and that $19T_0/8 \le \tilde{T}_D \le (19/8 + 1)T_0$. If the value of the sampling interval is set as $T_0 = 0.1$ s, the attack frequency during $[0, 30T_0)$ is 2.67 times per second and 0.24 s $\le \tilde{T}_D \le$ 0.34 s.

For a certain period $[0, T_p]$, the attack frequency f_D and the average duration time $\tilde{T}_D$ of each DoS attack can be estimated as

$$f_D = \frac{n_0}{T_p} \tag{3}$$

$$h_m \le \frac{T_m}{n_0} \le \tilde{T}_D < \frac{T_m}{n_0} + T_0 \le h_M. \tag{4}$$

From (3) and (4), we have

$$h_m \le \frac{T_m/T_p}{f_D} \le \tilde{T}_D < \frac{T_m/T_p}{f_D} + T_0 \le h_M \tag{5}$$

which follows:

$$\frac{T_m/T_p}{h_M} < f_D \le \frac{T_m/T_p}{h_m}. \tag{6}$$

Thus, both f_D and $\tilde{T}_D$ are heavily dependent on h_m and h_M.

Remark 1: In this article, the signal transmission process is based on the following three assumptions.

1) The network-induced delay is not considered, but only DoS attacks, such that every processor receives packets at the same sampling instant.
2) When DoS attacks happen, all sampled-data packets are not available for the MAS, all sampled-data packets from transmitters cannot be received by the processors and then become unavailable; meanwhile, the system turns to the worst attack-induced situation, zero-topology.
3) The duration time of each DoS attack is limited.

Remark 2: Based on the critical assumption that the network-induced delay is not considered in the signal transmission process, every logic processor receives sampled-data packets at the same instant so that T_m, h_m, h_M, and $\hat{t}$ calculated by the comparator are equal to the value of what calculated by other comparators. In future work, the consensus problem considering the network-induced delay and DoS attacks will be studied.

D. Control Protocol for the MASs

The operation of the controller is heavily dependent on the information provided by the logic processor. The controller works together with the logic processor. Once the logic processor receives all required data packets, the controller uses them subsequently to generate a discrete control input. Then, the property of zero-order hold (ZOH) converts the discrete signal into a continuous signal so that the agent can be actuated. The control protocol is adopted as

$$u_l(d_k) = cK \sum_{\substack{s=1 \\ l \ne s}}^{N} a_{ls}(z_s(d_k) - z_l(t_k)) \tag{7}$$

where K represents an controller gain matrix to be designed later, $c > 0$ denotes the coupling strength, and $\mathbb{I} = \{0, 1, 2, \ldots\}$ is the index set. By taking advantage of ZOH, the control law can be considered as

$$u_l(d) = cK \sum_{\substack{s=1 \\ s \ne l}}^{N} a_{ls}(z_s(d_k) - z_l(d_k)), d \in [d_k, d_{k+1}), k \in \mathbb{I}. \tag{8}$$

According to the mechanism of the comparator, one can obtain

$$\delta_k = d_{k+1} - d_k \in [h_m, h_M], k \in \mathbb{I}. \tag{9}$$

If we let

$$z(d) = [z_1^T(d), \ldots, z_{N-1}^T(d), z_N^T(d)]^T$$
$$z(d_k) = [z_1^T(d_k), \ldots, z_{N-1}^T(d_k), z_N^T(d_k)]^T$$
$$\mathbb{V}_k(z(d)) = [v_k(z_1(td))^T, \ldots, v_k(z_{N-1}(d))^T, v_k(z_N(d))^T]^T$$

the closed-loop system are described as

$$\dot{z}(d) = (I_N \otimes \mathcal{A})z(d) + \mathbb{V}(z(d)) - c(\mathbb{L} \otimes \mathcal{B}K)z(d_k) \tag{10}$$

where $d \in (d_k, d_{k+1})$.

Remark 3: By introducing novel logic processors embedded in corresponding controllers, information about DoS attacks can be obtained (See Figs. 1–3). Next, the problem of resilient control can be converted into one concerned with the upper and lower bound of the sampling interval of an ASDCS. According to the values of h_m and h_M that the logic processor provides, it is feasible to design resilient sampled-data controllers for the MASs against DoS attacks.

Definition 1 ([22]): If the following equation holds for any initial conditions:

$$\lim_{d\to\infty} = \| z_l(d) - z_s(d) \| = 0 \quad \forall l, s = 1, 2, \ldots, N$$

the consensus of MASs (1) is regarded as being reachable.

Lemma 1 ([23]): For a strongly connected graph $\mathbb{G}$, define $\epsilon = [\epsilon_1, \epsilon_2, \ldots, \epsilon_N]$ as the unique normalized left eigenvector of $\mathbb{L}$ corresponding to eigenvalue 0 with multiplicity 1 (satisfying $\sum_{i=1}^N \epsilon_i = 1$, i.e., $\epsilon \cdot \mathbb{L} = 0 \cdot \mathbb{L} = 0$). In addition, $\epsilon_i > 0$ holds for all $i = 1, 2, \ldots, N$.

Lemma 2 ([24]): For a strongly connected graph $\mathbb{G}$, define $\Xi = diag\{\epsilon_1, \epsilon_2, \ldots, \epsilon_N\} > 0$ and $W_{N\times N} = \Xi - \epsilon^T\epsilon$. If there exists matrix $P \in \mathbb{S}_+^n$, we have

$$z^T(d)(W\mathbb{L} \otimes HI_n)v_k(z(d)) = -\frac{1}{2}\sum_{q=1}^{N}\sum_{\substack{s=1\\ s\neq q}}^{N}\varepsilon_q l_{qs}$$
$$\times (z_q(d) - z_s(d))^T H[v_k(z_q(d)) - v_k(z_s(d))].$$

Lemma 3 ([25]): Let y be any continuously differentiable function $[\alpha, \beta] \to \mathbb{R}^n$. For a given matrix $H \in \mathbb{S}_+^n$ and any matrix W with an appropriate dimension, we have

$$-\int_\alpha^\beta \dot{y}^T(s)H\dot{y}(s)\mathrm{d}s \le \Phi$$

where $\Phi = \nu\theta^T(WH^{-1}W^T)\theta + \mathrm{Sym}\{\theta^T W[y(\beta) - y(\alpha)]\}$, $\nu = \beta - \alpha$, and θ can be any appropriately dimensional vector.

Lemma 4 ([26]): Let y be any continuously differentiable function $[\alpha, \beta] \to \mathbb{R}^n$. For a given matrix $Q \in \mathbb{S}_+^n$, and any matrices $S_1 \in \mathbb{R}^{3n\times n}$ and $S_2 \in \mathbb{R}^{3n\times n}$, we have

$$-\int_\alpha^\beta \dot{y}^T(s)Q\dot{y}(s)\mathrm{d}s \le \vartheta^T(\beta,\alpha)\Theta(\beta,\alpha)\vartheta(\beta,\alpha)$$

where $\vartheta(\beta,\alpha) = [y^T(\beta), y^T(\alpha), \int_\alpha^\beta y^T(s)\mathrm{d}s]^T$ and $\Theta(\beta,\alpha) = (\beta-\alpha)(S_1Q^{-1}S_1^T + [((\beta-\alpha)^2)/3]S_2Q^{-1}S_2^T - \mathrm{Sym}([S_2, S_2, 0])) + \mathrm{Sym}([S_1, -S_1, 2S_2])$.

III. Main Results

This section will give some sufficient conditions guaranteeing the secure consensus of the MASs with general Lipschitz nonlinearity. Also, sufficient conditions on how to design resilient distributed controllers are presented in this section. To simplify the descriptions of given conditions, notations of matrices and vectors are defined as follows:

$$\eta_1(d) = \left[\int_{d_k}^d \dot{z}^T(s)ds, \int_{d_k}^d z^T(s)ds\right]^T$$
$$\eta_2(d) = \left[\int_{d}^{d_{k+1}} \dot{z}^T(s)ds, \int_{d}^{d_{k+1}} z^T(s)ds\right]^T$$
$$\eta_3 = \left[z^T(d_k), z^T(d_{k+1}), \int_{d_k}^{d_{k+1}} z^T(s)ds\right]^T$$
$$\eta_4(d) = [(d_{k+1} - d)\eta_1^T(d), (d - d_k)\eta_2^T(d)]^T$$
$$\eta_5(d) = [\eta_1^T(d), \eta_2^T(d)]^T, \eta_6(d) = [\dot{z}^T(d), z^T(d)]$$
$$\eta_7(d) = [-\eta_1^T(d), \eta_2^T(d)]^T, \eta_8(d) = [0, -\eta_6^T(d)]^T$$
$$\eta_9(d) = [0, \eta_2^T(d)]^T, \eta_{10}(d) = [\eta_6^T(d), -\eta_6^T(d)]^T$$
$$\eta_{11}(d) = [\eta_6^T(d), 0]^T, \eta_{12}(d) = [\eta_1^T(d), 0]^T$$
$$\eta_{13}(d) = [z^T(d), \dot{z}^T(d), z^T(d_k)]^T$$
$$\rho(d) = \left[z^T(d), \dot{z}^T(d), z^T(d_k), \int_{d_k}^d z^T(s)\mathrm{d}s, z^T(d_{k+1})\right.$$
$$\left.\int_d^{d_{k+1}} z^T(s)\mathrm{d}s, v_k^T(z(d))\right]^T$$
$$\iota_j = [0_{m\times(j-1)m}, I_m, 0_{m\times(7-j)m}], j = 1, 2, \ldots, 7$$
$$\gamma_j = [0_{m\times(j-1)m}, I_m, 0_{m\times(6-j)m}], j = 1, 2, \ldots, 6.$$

Theorem 1: For a strongly connected graph, given two constants $h_M \ge h_m > 0$ and controller gain K, the secure consensus of MASs (1) can be reachable if there exist positive definite matrices P, Q_1, and Q_2, constant matrices $N_1, N_2, N_3, N_4, N_5, N_6, X_1, X_2, Z_1, Z_2$, and Z_3, and diagonal matrix G, so that for any $i, j = 1, 2, \ldots, N$ with $\delta_k \in \{h_m, h_M\}$, the following inequalities hold:

$$\begin{bmatrix}\Gamma_1 + \delta_k\Gamma_2 & \sqrt{\delta_k}X_1\\ * & -Q_1\end{bmatrix} < 0 \tag{11}$$

$$\begin{bmatrix}\Gamma_1 + \delta_k\Gamma_3 & \sqrt{\delta_k}X_2\\ * & -Q_2\end{bmatrix} < 0 \tag{12}$$

where

$$\Gamma_1 = \mathrm{Sym}\{\iota_1^T P\iota_2 + \Delta_3^T N_4\Delta_3 - \Delta_1^T N_4\Delta_3 + \Delta_5^T(N_5\Delta_6 + N_6\Delta_4) + X_1\Delta_{12} + X_2\Delta_{13} + \Lambda_1^T\Lambda_2\} - \Delta_1^T N_1\Delta_1 - \Delta_2^T N_2\Delta_2 + \iota_1^T D^T GD\iota_1 - \iota_7^T G\iota_7$$
$$\Gamma_2 = \mathrm{Sym}\{\Delta_2^T N_2\Delta_3 + \Delta_7^T(N_5\Delta_6 + 2N_6\Delta_4) + \Delta_8^T N_5\Delta_9\} + \iota_2^T Q_2\iota_2 - \Delta_4^T N_3\Delta_4$$

$$\Gamma_3 = \text{Sym}\{\Delta_1^T N_1 \Delta_3 + \Delta_{10}^T (N_5\Delta_6 + 2N_6\Delta_4) + \Delta_{11}^T N_5 \Delta_9\} + \iota_2^T Q_1 \iota_2 + \Delta_4^T N_3 \Delta_4$$
$$\Delta_1 = [\iota_1^T - \iota_3^T, \iota_4^T]^T, \Delta_2 = [\iota_5^T - \iota_1^T, \iota_6^T]^T, \Delta_3 = [\iota_2^T, \iota_1^T]^T$$
$$\Delta_4 = [\iota_3^T, \iota_5^T, \iota_4^T + \iota_6^T]^T, \Delta_5 = [\iota_3^T - \iota_1^T, -\iota_4^T, \iota_5^T - \iota_1^T, \iota_6^T]^T$$
$$\Delta_6 = [\iota_1^T - \iota_3^T, \iota_4^T, \iota_5^T - \iota_1^T, \iota_6^T]^T, \Delta_7 = [0, 0, -\iota_2^T, -\iota_1^T]^T$$
$$\Delta_8 = [0, 0, \iota_5^T - \iota_1^T, \iota_6^T]^T, \Delta_9 = [\iota_2^T, \iota_1^T, -\iota_2^T, -\iota_1^T]^T$$
$$\Delta_{10} = [\iota_2^T, \iota_1^T, 0, 0]^T, \Delta_{11} = [\iota_1^T - \iota_3^T, \iota_4^T, 0, 0]^T$$
$$\Delta_{12} = \iota_1 - \iota_3, \Delta_{13} = \iota_5 - \iota_1$$
$$\Lambda_1 = [Z_1, Z_2, Z_3, 0, 0, 0, 0]$$
$$\Lambda_2 = [\mathcal{A}, -I, l_{ij}/\varepsilon_j \mathcal{B}K, 0, 0, 0, I].$$

Proof: A looped-Lyapunov functional candidate is considered as follows:

$$V(d) = V_0(d) + \sum_{m=1}^{6} V_m(d), d \in (d_k, d_{k+1}) \tag{13}$$

where

$$V_0(d) = z^T(d)(W \otimes P)z(d)$$
$$V_1(d) = (d_{k+1} - d)\eta_1^T(d)(W \otimes N_1)\eta_1(d) - (d - d_k)\eta_2^T(d)(W \otimes N_2)\eta_2(d)$$
$$V_2(d) = (d - d_k)(d_{k+1} - d)\eta_3^T(W \otimes N_3)\eta_3$$
$$V_3(d) = 2\eta_1^T(d)(W \otimes N_4)\eta_2(d)$$
$$V_4(d) = 2\eta_4^T(d)[(W \otimes N_5)\eta_5(d) + (W \otimes N_6)\eta_3]$$
$$V_5(d) = (d_{k+1} - d)\int_{d_k}^{d} \dot{z}^T(s)(W \otimes Q_1)\dot{z}(s)\mathrm{d}s$$
$$V_6(d) = -(d - d_k)\int_{d}^{d_{k+1}} \dot{z}^T(s)(W \otimes Q_2)\dot{z}(s)\mathrm{d}s.$$

Taking the time derivative of (13) gives rise to

$$\dot{V}_0(d) = 2z^T(d)(W \otimes P)\dot{z}(d) \tag{14}$$
$$\dot{V}_1(d) = -\eta_1^T(d)(W \otimes N_1)\eta_1(d) - \eta_2^T(d)(W \otimes N_2)\eta_2(d) + 2(d_{k+1} - d)\eta_1^T(d)(W \otimes N_1)\eta_6(d) + 2(d - d_k)\eta_2^T(d)(W \otimes N_2)\eta_6(d) \tag{15}$$
$$\dot{V}_2(d) = (d_{k+1} - d)\eta_3^T(W \otimes N_3)\eta_3 - (d - d_k)\eta_3^T(W \otimes N_3)\eta_3 \tag{16}$$
$$\dot{V}_3(d) = 2\eta_6^T(d)(W \otimes N_4)\eta_2(d) - 2\eta_1^T(d)(W \otimes N_4)\eta_6(d) \tag{17}$$
$$\dot{V}_4(d) = 2\eta_7^T(d)[(W \otimes N_5)\eta_5(d) + (W \otimes N_6)\eta_3] + 2(d - d_k)\{\eta_8^T(d)[(W \otimes N_5)\eta_5(d) + (W \otimes N_6)\eta_3] + \eta_9^T(d)(W \otimes N_5)\eta_{10}(d)\} + 2(d_{k+1} - d)\{\eta_{11}^T(d)[(W \otimes N_5)\eta_5(d) + (W \otimes N_6)\eta_3] + \eta_{12}^T(d)(W \otimes N_5)\eta_{10}(d)\} \tag{18}$$
$$\dot{V}_5(d) = (d_{k+1} - d)\dot{z}^T(d)(W \otimes Q_1)\dot{z}(d) + \mathcal{F}_1 \tag{19}$$
$$\dot{V}_6(d) = (d - d_k)\dot{z}^T(d)(W \otimes Q_2)\dot{z}(d) + \mathcal{F}_2. \tag{20}$$

By using Lemma 3, the integral terms of (19) and (20) can be bounded as

$$\begin{aligned}\mathcal{F}_1 &= -\int_{d_k}^{d} \dot{z}^T(s)(W \otimes Q_1)\dot{z}(s)ds \\ &\le (d - d_k)\rho^T(d)(W \otimes X_1)(W \otimes Q_1)^{-1}(W \otimes X_1^T)\rho(d) \\ &\quad + \text{Sym}\{\rho^T(d)(W \otimes X_1)[z(d) - z(d_k)]\} \\ &\le \rho^T(d)[W \otimes ((d - d_k)X_1 Q_1^{-1} X_1^T + \text{Sym}(X_1\Delta_{12}))]\rho(d)\end{aligned} \tag{21}$$

$$\begin{aligned}\mathcal{F}_2 &= -\int_{d}^{d_{k+1}} \dot{z}^T(s)(W \otimes Q_2)\dot{z}(s)ds \\ &\le (d_{k+1} - d)\rho^T(d)(W \otimes X_2)(W \otimes Q_2)^{-1}(W \otimes X_2^T)\rho(d) \\ &\quad + \text{Sym}\{\rho^T(d)(W \otimes X_2)[z(d_{k+1}) - z(d)]\} \\ &\le \rho^T(d)[W \otimes ((d_{k+1} - d)X_2 Q_2^T X_2^T + \text{Sym}(X_2\Delta_{13}))]\rho(d).\end{aligned} \tag{22}$$

For any matrix $\mathcal{Z} = [Z_1, Z_2, Z_3]^T$ with an appropriate dimension, an augmented form according to system (9) is given in the following.

$$0 = 2\eta_{13}(d)(W \otimes \mathcal{Z})[(I_N \otimes \mathcal{A})z(d) + \mathbb{V}(z(d)) - \dot{z}(d) - c(\mathbb{L} \otimes \mathcal{B}K)z(d_k)]. \tag{23}$$

Moreover, from Assumption 1, the following inequality is established for a diagonal and positive matrix G.

$$(v_k(z_l(d)) - v_k(z_s(d)))^T G(v_k(z_l(d)) - v_k(z_s(d))) - (z_l(d) - z_s(d))^T D^T G D(z_l(d) - z_s(d)) \le 0. \tag{24}$$

If we let

$$\bar{z}(d) = z_l(d) - z_s(d), \dot{\bar{z}}(d) = \dot{z}_l(d) - \dot{z}_s(d)$$
$$\bar{z}(d_k) = z_l(d_k) - z_s(d_k), \bar{z}(d_{k+1}) = z_l(d_{k+1}) - z_s(d_{k+1})$$
$$\tilde{z}(s) = \int_{d_k}^{d} z_l(s)ds - \int_{d_k}^{d} z_s(s)ds$$
$$\bar{\tilde{z}}(s) = \int_{d}^{d_{k+1}} z_l(s)ds - \int_{d}^{d_{k+1}} z_s(s)ds$$
$$\bar{v_k}(z(d)) = v_k(z_l(d)) - v_k(z_s(d))$$
$$\bar{\rho}(d) = [\bar{z}^T(d), \dot{\bar{z}}^T(d), \bar{z}^T(d_k), \tilde{z}^T(s), \bar{z}^T(d_{k+1}), \bar{\tilde{z}}^T(s), \bar{v_k}(z(d))]^T.$$

According to Lemma 2, it can be obtained from (14)–(24) that

$$\dot{V}(d) \le \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1, j\ne i}^{N} \varepsilon_i\varepsilon_j \bar{\rho}^T(d)\left[\frac{d_{k+1} - d}{\delta_k}\Pi_1(\delta_k) + \frac{d - d_k}{\delta_k}\Pi_2(\delta_k)\right]\bar{\rho}(d) \tag{25}$$

where

$$\Pi_1(\delta_k) = \Gamma_1 + \delta_k\Gamma_2 + \delta_k X_1 Q_1^{-1} X_1^T$$
$$\Pi_2(\delta_k) = \Gamma_1 + \delta_k\Gamma_3 + \delta_k X_2 Q_2^{-1} X_2^T.$$

If $\Pi_1(\delta_k) < 0$ and $\Pi_2(\delta_k) < 0$ are satisfied, $\dot{V}(d) \le 0$ can be guaranteed. By the Schur complement, the abovementioned conditions are equivalent to (11) and (12). This completes the proof.

Remark 4: It is obvious that $V_0(t) > 0$, and $V_m(d_k) = V_m(d_{k+1}) = 0, m = 1, \ldots, 6$. Therefore, the function (12) is a valid Lyapunov functional for the MASs (10). The use of looped-functionals in [27] and [28] gives us easy access to choose Lyapunov functional candidates with much more slack variables. Note that $N_i (i = 1, \ldots, 6)$ in $V_2(d) - V_5(d)$ are not necessarily positive definite. Moreover, the free-weighting matrix inequality [25], helpful to reduce the conservatism in [29], is also applied to obtain some less conservative consensus conditions in this section. Later, numerical examples can demonstrate the effectiveness of our conditions.

Theorem 2: For a strongly connected graph, given constants $h_M \ge h_m > 0$ and $\sigma_i, i = 1, 2, 3$, the secure consensus of MASs (1) can be reachable by the resilient controller (8) with $K = J\bar{Z}^{-1}$ if there exist positive definite matrices $\bar{P}, \bar{Q}_1$, and $\bar{Q}_2$, constant matrices $\bar{N}_1, \bar{N}_2, \bar{N}_3, \bar{N}_4, \bar{N}_5, \bar{N}_6, \bar{X}_1, \bar{X}_2, \bar{Z}$, and J, and diagonal matrix $\bar{G}$ such that for any $i, j = 1, 2, \ldots, N$ with $\delta_k \in \{h_m, h_M\}$, the following equations hold:

$$\begin{bmatrix} \bar{\Gamma}_1 + \delta_k\bar{\Gamma}_2 & \delta_k\bar{X}_1 \\ * & -\bar{Q}_1 \end{bmatrix} < 0 \tag{26}$$

$$\begin{bmatrix} \bar{\Gamma}_1 + \delta_k\bar{\Gamma}_3 & \delta_k\bar{X}_2 \\ * & -\bar{Q}_2 \end{bmatrix} < 0 \tag{27}$$

where

$$\begin{aligned}
\bar{\Gamma}_1 &= \mathrm{Sym}\{\iota_1^T\bar{P}\iota_2 + \Delta_3^T\bar{N}_4\Delta_3 - \Delta_1^T\bar{N}_4\Delta_3 + \Delta_5^T(\bar{N}_5\Delta_6 \\
&\quad + \bar{N}_6\Delta_4) + \bar{X}_1\Delta_{12} + \bar{X}_2\Delta_{13} + \bar{\Lambda}_1^T\bar{\Lambda}_2\} - \Delta_1^T\bar{N}_1\Delta_1 \\
&\quad - \Delta_2^T\bar{N}_2\Delta_2 + \iota_1^T D^T\bar{G}D\iota_1 - \iota_7^T\bar{G}\iota_7 \\
\bar{\Gamma}_2 &= \mathrm{Sym}\{\Delta_2^T\bar{N}_2\Delta_3 + \Delta_7^T(\bar{N}_5\Delta_6 + 2\bar{N}_6\Delta_4) + \Delta_8^T\bar{N}_5\Delta_9\} \\
&\quad + \iota_2^T\bar{Q}_2\iota_2 - \Delta_4^T\bar{N}_3\Delta_4 \\
\bar{\Gamma}_3 &= \mathrm{Sym}\{\Delta_1^T\bar{N}_1\Delta_3 + \Delta_{10}^T(\bar{N}_5\Delta_6 + 2\bar{N}_6\Delta_4) + \Delta_{11}^T\bar{N}_5\Delta_9\} \\
&\quad + \iota_2^T\bar{Q}_1\iota_2 + \Delta_4^T\bar{N}_3\Delta_4 \\
\bar{\Lambda}_1 &= [\sigma_1 I, \sigma_2 I, \sigma_3 I, 0, 0, 0, 0] \\
\bar{\Lambda}_2 &= [\mathcal{A}\bar{Z}, -\bar{Z}, l_{ij}/\varepsilon_j\mathcal{B}J, 0, 0, 0, \bar{Z}].
\end{aligned}$$

Proof: Set

$$\begin{aligned}
&Z_1 = \sigma_1 Z, Z_2 = \sigma_2 Z, Z_3 = \sigma_3 Z, \bar{Z} = Z^{-1}, \bar{P} = \bar{Z}^T P\bar{Z} \\
&\bar{Q}_1 = \bar{Z}^T Q_1\bar{Z}, \bar{Q}_2 = \bar{Z}^T Q_2\bar{Z}, \bar{G} = \bar{Z}^T G\bar{Z}, \bar{N}_1 = \Phi_1^T N_1\Phi_1 \\
&\bar{N}_2 = \Phi_1^T N_2\Phi_1, \bar{N}_3 = \Phi_2^T N_3\Phi_2, \bar{N}_4 = \Phi_1^T N_4\Phi_1 \\
&\bar{N}_5 = \Phi_3^T N_4\Phi_3, \bar{N}_6 = \Phi_3^T N_4\Phi_2, \bar{X}_1 = \Delta_4^T X_1\bar{Z} \\
&\bar{X}_2 = \Delta_4^T X_2\bar{Z}, \Phi_1 = \mathrm{diag}\{\bar{Z}, \bar{Z}\}, \Phi_2 = \mathrm{diag}\{\Phi_1, \bar{Z}\} \\
&\Phi_3 = \mathrm{diag}\{\Phi_2, \bar{Z}\}, \Phi_4 = \mathrm{diag}\{\Phi_3, \bar{Z}, \bar{Z}, \bar{Z}\}.
\end{aligned}$$

Performing a congruent transformation on (11) and (12) by Φ_4^T and Φ_4, we can obtain (26) and (27). By Theorem 2, the secure consensus of MASs (1) can be reachable under the resilient control (8) with $K = J\bar{Z}^{-1}$. This completes the proof.

Remark 5: In this article, Theorem 2 is used to obtain the desired controller parameters. In the proof of Theorem 2, Lemma 2 is used to handle (13)–(23), which leads to the couplings of l_{ij} and K. With such couplings, once l_{ij} is equal to zero, K will have no solution. Therefore, the algorithm in this work is only suitable for strongly connected graphs, that is, $l_{ij} = 0$, and might not be extended to more general cases. Although there are some limitations that the algorithm in this work is only applicable to strongly connected graphs, according to [9], such limitations are accordant with the practical situation of the network of UAVs. Our future attention will focus on how to remove the abovementioned couplings on how to design algorithms for more general cases.

Remark 6: The problem of resilient sampled-data consensus of MASs is solved in Theorem 2. The feasibility of the design method for the resilient sampled-data controller can be easily verified by solving the linear matrix inequalities (LMIs) in (26) and (27). Meanwhile, these LMIs can be solved readily via the LMI toolbox in MATLAB.

By choosing the looped-Lyapunov functionals (12) and applying the same lemma utilized in [12] to deal with the integral terms of (19) and (20), we can obtain the following corollary.

Corollary 1: For a strongly connected graph, given constants $h_M \ge h_m > 0$, and $\sigma_i, i = 1, 2, 3$, the secure consensus of MASs (1) can be reachable via the resilient controller (8) with $K = J\bar{Z}^{-1}$, if there exist symmetric positive definite matrices $\bar{P}, \bar{Q}_1$, and $\bar{Q}_2$, constant matrices $\bar{N}_1, \bar{N}_2, \bar{N}_3, \bar{N}_4, \bar{N}_5, \bar{N}_6, \bar{S}_1, \bar{S}_2, \bar{S}_3, \bar{S}_4, \bar{Z}$, and J, and diagonal matrix $\bar{G}$ such that for any $i, j = 1, 2, \ldots, N$ with $\delta_k \in \{h_m, h_M\}$, the following equations hold:

$$\begin{bmatrix} \bar{\Gamma}_4 + \delta_k\bar{\Gamma}_5 & \delta_k\bar{S}_1 & \delta_k^2\bar{S}_2 \\ * & -\delta_k\bar{Q}_1 & 0 \\ * & * & -3\delta_k\bar{Q}_1 \end{bmatrix} < 0 \tag{28}$$

$$\begin{bmatrix} \bar{\Gamma}_4 + \delta_k\bar{\Gamma}_6 & \delta_k\bar{S}_3 & \delta_k^2\bar{S}_4 \\ * & -\delta_k\bar{Q}_2 & 0 \\ * & * & -3\delta_k\bar{Q}_2 \end{bmatrix} < 0 \tag{29}$$

where

$$\begin{aligned}
\bar{\Gamma}_4 &= \mathrm{Sym}\{\iota_1^T\bar{P}\iota_2 + \Delta_3^T\bar{N}_4\Delta_3 - \Delta_1^T\bar{N}_4\Delta_3 + \Delta_5^T(\bar{N}_5\Delta_6 \\
&\quad + \bar{N}_6\Delta_4) + \bar{\Sigma}_1 + \bar{\Sigma}_3 + \bar{\Lambda}_1^T\bar{\Lambda}_2\} - \Delta_1^T\bar{N}_1\Delta_1 \\
&\quad - \Delta_2^T\bar{N}_2\Delta_2 + \iota_1^T D^T\bar{G}D\iota_1 - \iota_7^T\bar{G}\iota_7 \\
\bar{\Gamma}_5 &= \mathrm{Sym}\{\Delta_2^T\bar{N}_2\Delta_3 + \Delta_7^T(\bar{N}_5\Delta_6 + 2\bar{N}_6\Delta_4) + \Delta_8^T\bar{N}_5\Delta_9 \\
&\quad - \bar{\Sigma}_2\} + \iota_2^T\bar{Q}_2\iota_2 - \Delta_4^T\bar{N}_3\Delta_4 \\
\bar{\Gamma}_6 &= \mathrm{Sym}\{\Delta_1^T\bar{N}_1\Delta_3 + \Delta_{10}^T(\bar{N}_5\Delta_6 + 2\bar{N}_6\Delta_4) + \Delta_{11}^T\bar{N}_5\Delta_9 \\
&\quad - \bar{\Sigma}_4\} + \iota_2^T\bar{Q}_1\iota_2 + \Delta_4^T\bar{N}_3\Delta_4
\end{aligned}$$

$$\bar{\Sigma}_1 = [\bar{S}_1, 0, -\bar{S}_1, 2\bar{S}_2, 0, 0, 0], \bar{\Sigma}_2 = [\bar{S}_2, 0, \bar{S}_2, 0, 0, 0, 0]$$

$$\bar{\Sigma}_3 = [-\bar{S}_3, 0, 0, 0, \bar{S}_3, 2\bar{S}_4, 0], \bar{\Sigma}_4 = [\bar{S}_4, 0, 0, 0, \bar{S}_4, 0, 0].$$

Remark 7: Choosing the different Lyapunov functionals [(12) in this article and (13) in [12]], Corollary 1 in this article and Corollary 2 in [12] are derived by using the same lemma (Lemma 4), respectively. The Lyapunov functionals we choose contain more slack variables, which can lead to less conservative consensus conditions with a larger sampling interval. Later, numerical examples can justify this conclusion.

When the nonlinear self-dynamics $v_k(z_i(d))$ is not considered, from Corollary 1, we can easily derive the following corollary.

Corollary 2: For a strongly connected graph, given constants $h_M \geq h_m > 0$ and $\sigma_i, i = 1, 2, 3$, the secure consensus of MASs (1) can be reachable via the resilient controller (8) with $K = J\bar{Z}^{-1}$, if there exist positive definite matrices $\bar{P}, \bar{Q}_1$, and $\bar{Q}_2$, constant matrices $\bar{N}_1, \bar{N}_2, \bar{N}_3, \bar{N}_4, \bar{N}_5, \bar{N}_6, \bar{S}_1, \bar{S}_2, \bar{S}_3, \bar{S}_4, \bar{Z}$, and J, such that for any $i, j = 1, 2, \ldots, N$ with $\delta_k \in \{h_m, h_M\}$, the following equations hold:

$$\begin{bmatrix} \bar{\Gamma}_7 + \delta_k \bar{\Gamma}_8 & \delta_k \bar{S}_1 & \delta_k^2 \bar{S}_2 \\ * & -\delta_k \bar{Q}_1 & 0 \\ * & * & -3\delta_k \bar{Q}_1 \end{bmatrix} < 0 \tag{30}$$

$$\begin{bmatrix} \bar{\Gamma}_7 + \delta_k \bar{\Gamma}_9 & \delta_k \bar{S}_3 & \delta_k^2 \bar{S}_4 \\ * & -\delta_k \bar{Q}_2 & 0 \\ * & * & -3\delta_k \bar{Q}_2 \end{bmatrix} < 0 \tag{31}$$

where

$$\begin{aligned}
\bar{\Gamma}_7 &= \mathrm{Sym}\{\gamma_1^T \bar{P} \gamma_2 + \tilde{\Delta}_3^T \bar{N}_4 \tilde{\Delta}_3 - \tilde{\Delta}_1^T \bar{N}_4 \tilde{\Delta}_3 + \tilde{\Delta}_5^T (\bar{N}_5 \tilde{\Delta}_6 \\
&\quad + \bar{N}_6 \tilde{\Delta}_4) + \tilde{\Sigma}_1 + \tilde{\Sigma}_3 + \bar{\Lambda}_1^T \bar{\Lambda}_2\} - \tilde{\Delta}_1^T \bar{N}_1 \tilde{\Delta}_1 \\
&\quad - \tilde{\Delta}_2^T \bar{N}_2 \tilde{\Delta}_2 \\
\bar{\Gamma}_8 &= \mathrm{Sym}\{\tilde{\Delta}_2^T \bar{N}_2 \tilde{\Delta}_3 + \tilde{\Delta}_7^T (\bar{N}_5 \tilde{\Delta}_6 + 2\bar{N}_6 \tilde{\Delta}_4) + \tilde{\Delta}_8^T \bar{N}_5 \tilde{\Delta}_9 \\
&\quad - \tilde{\Sigma}_2\} + \gamma_2^T \bar{Q}_2 \gamma_2 - \tilde{\Delta}_4^T \bar{N}_3 \tilde{\Delta}_4 \\
\bar{\Gamma}_9 &= \mathrm{Sym}\{\tilde{\Delta}_1^T \bar{N}_1 \tilde{\Delta}_3 + \tilde{\Delta}_{10}^T (\bar{N}_5 \tilde{\Delta}_6 + 2\bar{N}_6 \tilde{\Delta}_4) + \tilde{\Delta}_{11}^T \bar{N}_5 \tilde{\Delta}_9 \\
&\quad - \tilde{\Sigma}_4\} + \gamma_2^T \bar{Q}_1 \gamma_2 + \tilde{\Delta}_4^T \bar{N}_3 \tilde{\Delta}_4 \\
\tilde{\Sigma}_1 &= [\bar{S}_1, 0, -\bar{S}_1, 2\bar{S}_2, 0, 0], \tilde{\Sigma}_2 = [\bar{S}_2, 0, \bar{S}_2, 0, 0, 0] \\
\tilde{\Sigma}_3 &= [-\bar{S}_3, 0, 0, 0, \bar{S}_3, 2\bar{S}_4], \tilde{\Sigma}_4 = [\bar{S}_4, 0, 0, 0, \bar{S}_4, 0] \\
\tilde{\Delta}_1 &= [\gamma_1^T - \iota_3^T, \gamma_4^T]^T, \tilde{\Delta}_2 = [\gamma_5^T - \gamma_1^T, \gamma_6^T]^T \\
\Delta_3 &= [\gamma_2^T, \gamma_1^T]^T, \tilde{\Delta}_4 = [\gamma_3^T, \gamma_5^T, \gamma_4^T + \gamma_6^T]^T \\
\tilde{\Delta}_5 &= [\gamma_3^T - \gamma_1^T, -\gamma_4^T, \gamma_5^T - \gamma_1^T, \gamma_6^T]^T \\
\tilde{\Delta}_6 &= [\gamma_1^T - \gamma_3^T, \gamma_4^T, \gamma_5^T - \gamma_1^T, \gamma_6^T]^T, \tilde{\Delta}_7 = [0, 0, -\gamma_2^T, -\gamma_1^T]^T \\
\tilde{\Delta}_8 &= [0, 0, \gamma_5^T - \iota_1^T, \iota_6^T]^T, \tilde{\Delta}_9 = [\gamma_2^T, \gamma_1^T, -\gamma_2^T, -\gamma_1^T]^T \\
\tilde{\Delta}_{10} &= [\gamma_2^T, \gamma_1^T, 0, 0]^T, \tilde{\Delta}_{11} = [\gamma_1^T - \gamma_3^T, \gamma_4^T, 0, 0]^T \\
\bar{\Lambda}_1 &= [\sigma_1 I, \sigma_2 I, \sigma_3 I, 0, 0, 0] \\
\bar{\Lambda}_2 &= [A\bar{Z}, -\bar{Z}, l_{ij}/\varepsilon_j BJ, 0, 0, 0].
\end{aligned}$$

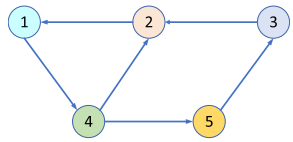


Fig. 4. Communication topology of the network UAVs.

TABLE I
MAXIMUM UPPER BOUND h_M FOR $h_m = 0.001$ OF DIFFERENT METHODS

Methods	h_M	NDV
[9](Theorem 2)	1.01	$19.5n^2 + 2.5n$
[12](Corollary 2)	1.40	$19.5n^2 + 2.5n$
Theorem 2	1.54	$58n^2 + 6n$
Corollary 2	1.62	$72n^2 + 6n$

IV. Numerical Examples

In this section, two simulation examples of the network UAVs and two-mass-spring systems (TMSSs) are illustrated to demonstrate the effectiveness of the proposed consensus conditions. Those examples can be practically used for the MASs theory.

A. Case Study on the Low-Order System

According to Wu *et al.* [9] and Ge *et al.* [12], the MAS model of the network UAVs consisting of five agents is described by

$$\dot{z}_i(d) = \mathcal{A} z_i(d) + \mathcal{B} u_i(d) + v_k(z_i(d)) \tag{32}$$

where

$$\mathcal{A} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \mathcal{B} = \begin{bmatrix} 1 & 0.5 \\ 0.5 & 1 \end{bmatrix}$$

$$v_k(z_i(d)) = [0.5\sin(z_{i1}(d)), 0.5\sin(z_{i2}(d))]^T$$

and $z_i(d) = [z_{i1}(d), z_{i2}(d)]^T (i = 1, \ldots, 5)$. According to Assumption 1, the Lipchitz constant m_k can be calculated as $m_k = 0.5$. Fig. 4 shows the communication topology the network UAV. It can be obtained that the normalized left eigenvector corresponding to eigenvalue 0 of the Laplacian matrix $\mathbb{L}$ is $\varepsilon = [1/5, 1/5, 1/5, 1/5, 1/5]$.

1) When DoS attacks are not considered, the consensus problem of this system has been investigated in [9] and [12], where h_m and h_M are treated as the upper and lower bounds, respectively, of the interval between two consecutive sampling instants. For comparison, h_M is calculated by Theorem 2 for a given $h_m = 0.001$. The comparison results of the sampling intervals and the computational complexity are shown in Table I, from which it can be concluded that Theorem 2 outperforms the ones in [9] and [12]. It is worth mentioning that the only difference between Corollary 1 and Theorem 2 in [12] is the Lyapunov functionals. Therefore, the results in Table I further illustrate the advantages of the Lyapunov functionals that we have chosen.

As we have known, the total number of decision variables (NDV) is usually used to evaluate the computational complexity. From Table I, one can see that although our method can obtain a larger sampling interval, the computational complexity of the system has increased. These LMIs can be solved readily via the LMI toolbox in MATLAB and the average calculation time for

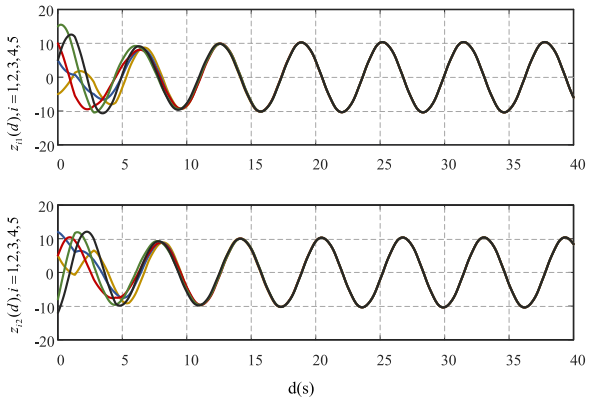


Fig. 5. State responses of the network UAVs with the sampled-data controller (33).

[9], [12], Theorem 2, and Corollary 1 is 0.21 s, 0.21 s, 0.27 s, and 0.31 s, respectively. (Related calculational processes are implemented in MATLAB environment on a desktop which has an Intel Core i7-10875 CPU 2.3 GHz and 40 GB of RAM.) Although the average calculation time increases, it is clear that our sampling period is superior to the others from Table I. The larger sampling interval of sampled-data controllers has many superiorities, such as lower computational burden, less load limitation, and fewer actuators' actions. Moreover, for the practical application, the abovementioned calculation processes which are carried out offline do not affect the real-time collaborative control of the system. Therefore, the increase in calculation time is acceptable.

Based on Corollary 1, we set the parameters $\sigma_1 = 1.2, \sigma_2 = 1.6$, and $\sigma_3 = 0.3$. Then, the maximal sampling period is obtained $h_M = 1.62$ with the given minimum one $h_m = 0.0001$ s, and the distributed control parameter is solved out as

$$K = \begin{bmatrix} 0.1792 & -0.4574 \\ 0.1311 & 0.4734 \end{bmatrix}. \tag{33}$$

Then, for the given initial conditions of the five UAVs $z_1(0) = [10; 5]$, $z_2(0) = [5; 12]$, $z_3(0) = [-5; 5]$, $z_4(0) = [15; -8]$, and $z_5(0) = [5; -12]$, the state responses of each dimension $j(j = 1, 2)$ are shown in Fig. 5 by implementing the controller gain K in (33). From the simulation results, one can verify the effectiveness of our proposed control protocol.

2) Zero-topology [17] represents the worst attack-induced situation, which means that communication among $N(N = 5$ in Fig. 4) agents is interrupted, and communication is not restored until the attacks end. Suppose the minimum attack duration time $h_m = 0.4$ s and the maximum one $h_M = 1.62$ s. Then, for the same initial conditions of the abovementioned five network UAVs, the state responses, sampled-data control input of the five network UAVs, and simulated DoS attack signal is presented in Fig. 6. From the abovementioned simulation results, it can be concluded that our proposed control protocol can counter the impact of DoS attacks to a larger extent.

B. Case Study on the High-Order System

According to Zhang *et al.* [30], [31], we consider a group of TMSSs with single force input, where each TMSS is regarded as

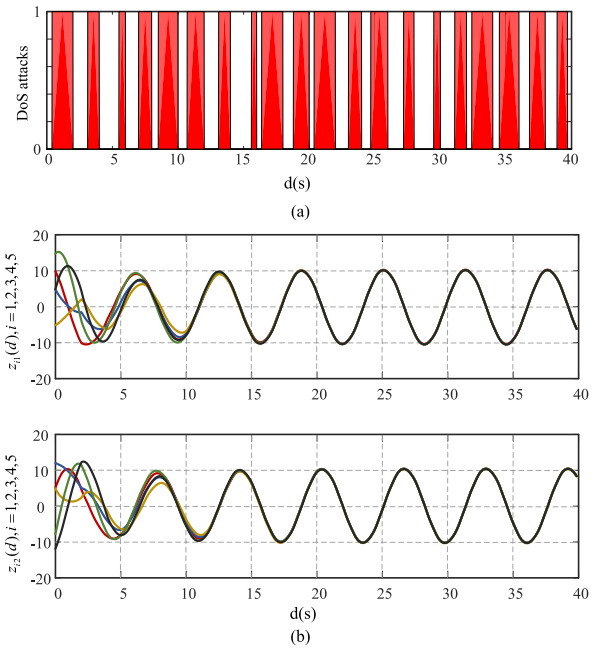


Fig. 6. Simulation results of the network UAVs under DoS attacks ($h_M = 1.62$ s, $h_m = 0.4$ s) with the controller gain (33). (a) Simulated DoS attacks signal. (b) States trajectories.

an agent. The state space equations of each agent are described by

$$\dot{z}_i(d) = \mathcal{A}z_i(d) + \mathcal{B}u_i(d)$$

where

$$\mathcal{A} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ \frac{-k_1-k_2}{m_1} & 0 & \frac{k_2}{m_1} & 0 \\ 0 & 0 & 0 & 1 \\ \frac{k_2}{m_2} & 0 & \frac{-k_2}{m_2} & 0 \end{bmatrix}, \mathcal{B} = \begin{bmatrix} 0 \\ \frac{1}{m_1} \\ 0 \\ 0 \end{bmatrix}$$

$m_1 = 1.1$ kg, $m_2 = 0.9$ kg, $k_1 = 1.5$ N/m, $k_2 = 1$ N/m, $z_i(t) = [z_{i1}(t), z_{i2}(t), z_{i3}(t), z_{i4}(t)]^T = [y_1, \dot{y}_1, y_2, \dot{y}_2]^T (i = 1, 2, 3, 4)$, m_1 and m_2 are two masses, k_1 and k_2 are spring constants, u is the force input for mass 1, and y_1 and y_2 are displacement of the two masses.

For this example, the communication topology of the TMSSs can be denoted as the following Laplacian matrix $\mathbb{L}$:

$$\mathbb{L} = \begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{bmatrix}.$$

It can be obtained that the normalized left eigenvector corresponding to eigenvalue 0 of the Laplacian matrix $\mathbb{L}$ is $\varepsilon = [1/4, 1/4, 1/4, 1/4, 1/4]^T$.

Suppose that the TMSSs are exposed to such DoS attacks with the minimum attack duration time $h_m = 0.2$ s and the maximum one $h_M = 1.6$ s. According to Corollary 2, we can design a resilient distributed sampled-data controller to counter such DoS attacks. With the paremeters $h_m = 0.2, h_M = 1.6, \sigma_1 = 0.9, \sigma_2 = 1.9$, and $\sigma_3 = 0.3$, solving the LMIs (29) and (30),

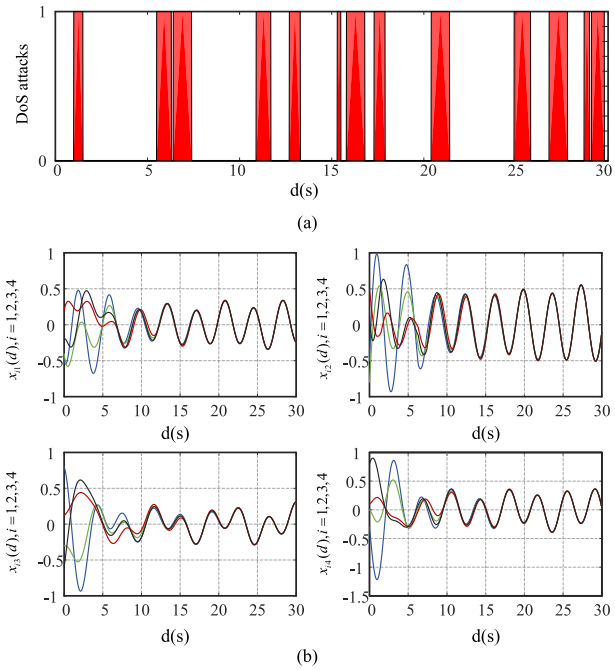


Fig. 7. Simulation results of TMSSs under DoS attacks ($h_M = 0.2\,\text{s}, h_m = 1.0\,\text{s}$) with the controller gain (34). (a) Simulated DoS attacks signal. (b) States trajectories.

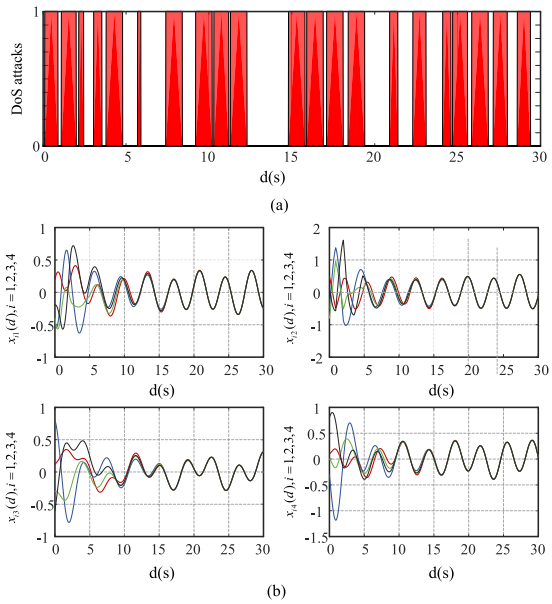


Fig. 8. Simulation results of TMSSs under DoS attacks ($h_M = 0.2\,\text{s}, h_m = 1.0\,\text{s}$) with the controller gain (34). (a) Simulated DoS attacks signal. (b) States trajectories.

the distributed control parameter is solved out as

$$K = \begin{bmatrix} -0.1626 & 0.0620 & 0.0236 & 0.0391 \end{bmatrix}. \tag{34}$$

In order to better show the effectiveness of the proposed resilient control method, we will provide simulation results under two DoS attacks with different attack frequencies and the same maximum attack duration time ($h_m = 0.2\,\text{s}$ and $h_M = 1.0\,\text{s}$).

Suppose that the TMSSs are exposed to a sequence of DoS attacks simulated by Fig. 7(a), which means that the MASs have been attacked 13 times during $[0, 30\,\text{s})$, the attack frequency is 0.433 times per second. Suppose that the TMSSs are exposed to a sequence of DoS attacks simulated by Fig. 8(a), which means that the MASs have been attacked 21 times during $[0, 30\,\text{s})$, the attack frequency is 0.7 times per second. From Figs. 7(b) and 8(b), it can be concluded that our proposed control protocol can counter the impact of DoS attacks to a larger extent.

V. Conclusion

This article has investigated a resilient sampled-data consensus problem of the MASs against DoS attacks, which may be random or periodic. The worst attack-induced situation, zero-topology, is considered. Based on the information about DoS attacks obtained by the logic processors, the issue of resilient controllers design can be converted into a problem concerned with the upper and lower bound of the sampling interval of an ASDCS. It is worth mentioning that advanced Lyapunov functionals combined with loop functionals have been utilized to decrease the results' conservativeness. From the illustrative example of UAVs, it can be concluded that the sampling interval we have obtained is better than that in [9] and [12]. Besides, the numerical simulation results of the TMSSs indicate that the designed resilient controller can counter the DoS attacks' impact. Furthermore, our future directions will consider the performance optimization problem [32] and the case of directed topology [33].

References

[1] Z. Peng, D. Wang, Y. Shi, H. Wang, and W. Wang, "Containment control of networked autonomous underwater vehicles with model uncertainty and ocean disturbance guided by multiple leaders," *Inf. Sci.*, vol. 316, pp. 163–179, Sep. 2015.

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

[3] Z. H. Ye, D. Zhang, Z. G. Wu, and H. C. Yan, "A3C-based intelligent event-triggering control of networked nonlinear unmanned marine vehicles subject to hybrid attacks," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2021.3118648.

[4] S. Yang, S. Tan, and J.-X. Xu, "Consensus based approach for economic dispatch problem in a smart grid," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4416–4426, Nov. 2013.

[5] Z. Zhang, S. M. Chen, and Y. Zheng, "Fully distributed scaled consensus tracking of high-order multi-agent systems with time delays and disturbances," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 305–314, Jan. 2022.

[6] L. Ding, Q.-L. Han, L. Y. Wang, and E. Sindi, "Distributed cooperative optimal control of DC microgrids with communication delays," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3924–3935, Sep. 2018.

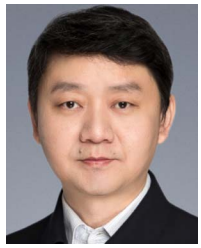
[7] H. Zhang, J. H. Park, D. Yue, and X. Xie, "Finite-horizon optimal consensus control for unknown multiagent state-delay systems," *IEEE Trans. Cybern.*, vol. 50, no. 2, pp. 402–413, Feb. 2020.

[8] D. Zhang, Z. Xu, H. R. Karimi, Q. G. Wang, and L. Yu, "Distributed H_∞ output-feedback control for consensus of heterogeneous linear multiagent systems with aperiodic sampled-data communications," *IEEE Trans. Ind. Electron.*, vol. 65, no. 5, pp. 4145–4155, May 2018.

[9] Y. Wu, H. Su, P. Shi, Z. Shu, and Z. Wu, "Consensus of multiagent systems using aperiodic sampled-data control," *IEEE Trans. Cybern.*, vol. 46, no. 9, pp. 2132–2143, Sep. 2016.

[10] Z. Wang, H. He, G. P. Jiang, and J. Cao, "Distributed tracking in heterogeneous networks with asynchronous sampled-data control," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7381–7391, Dec. 2020.

[11] H. Ren, H. R. Karimi, R. Lu, and Y. Wu, "Synchronization of network systems via aperiodic sampled-data control with constant delay and application to unmanned ground vehicles," *IEEE Trans. Ind. Electron.*, vol. 67, no. 6, pp. 4980–4990, Jun. 2020.
[12] C. Ge, J. H. Park, C. Hua, and X. Guan, "Nonfragile consensus of multiagent systems based on memory sampled-data control," *IEEE Trans. Syst. Man. Cybern., Syst.*, vol. 51, no. 1, pp. 391–399, Jan. 2021.
[13] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control systems: Impact and mitigation," *IEEE Trans. Ind. Informat.*, vol. 1, no. 2, pp. 85–96, May 2005.
[14] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, May 2017.
[15] C. Deng, D. Zhang, and G. feng, "Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks," *Automatica*, vol. 139, 2022, Art. no. 110172.
[16] J. Liu, T. Yin, D. Yue, H. R. Karimi, and J. Cao, "Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 162–173, Jan. 2021.
[17] Z. Cheng, D. Yue, S. Hu, H. Ge, and L. Chen, "Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks," *Neurocomputing*, vol. 400, pp. 458–466, Aug. 2020.
[18] Z. Zuo, X. Cao, Y. Wang, and W. Zhang, "Resilient consensus of multi-agent systems against denial-of-service attacks," *IEEE Trans. Syst. Man, Cybern.: Syst.*, vol. 52, no. 4, pp. 2664–2675, Apr. 2022.
[19] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to periodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.
[20] 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.
[21] X. Zhang, Q. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.
[22] W. Ren and R. W. Beard, "Consensus seeking in multi-agent systems under dynamically changing interaction topologies," *IEEE Trans. Autom. Control*, vol. 50, no. 5, pp. 655–661, May 2005.
[23] J. Lu, D. W. C. Ho, J. Cao, and J. Kurths, "Exponential synchronization of linearly coupled neural networks with impulsive disturbances," *IEEE Trans. Neural Netw.*, vol. 22, no. 2, pp. 329–336, Feb. 2011.
[24] J. Lu and D. W. Ho, "Globally exponential synchronization and synchronizability for general dynamical networks," *IEEE Trans. Syst., Man, Cybern. B., Cybern.*, vol. 40, no. 2, pp. 350–361, Apr. 2010.
[25] X.-M. Zhang and Q.-L. Han, "Novel delay-derivative-dependent stability criteria using new bounding techniques," *Int. J. Robust Nonlinear Control*, vol. 23, no. 13, pp. 1419–1432, Sep. 2013.
[26] T. H. Lee and J. H. Park, "Stability analysis of sampled-data systems via free-matrix-based time-dependent discontinuous Lyapunov approach," *IEEE Trans. Autom. Control*, vol. 62, no. 7, pp. 3653–3657, Jul. 2017.
[27] S. H. Lee, P. Selvaraj, M. J. Park, and O. M. Kwon, "Improved results on H_∞ stability analysis of sampled-data systems via looped-functionals and zero equalities," *Appl. Math. Comput.*, vol. 373, May 2020, Art. no. 125003.
[28] H. B. Zeng, K. L. Teo, and Y. He, "A new looped-functional for stability analysis of sampled-data systems," *Automatica*, vol. 82, pp. 328–331, Aug. 2017.
[29] H. Zeng, Z. Zhai, H. Xiao, and W. Wang, "Stability analysis of sampled-data control systems with constant communication delays," *IEEE Access*, vol. 7, pp. 111–116, 2019.
[30] H. Zhang, F. L. Lewis, and Z. Qu, "Lyapunov, adaptive, and optimal design techniques for cooperative systems on directed communication graphs," *IEEE Trans. Ind. Electron.*, vol. 59, no. 7, pp. 3026–3041, Jul. 2012.
[31] 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.
[32] Z. Zhang, W. Yan, and H. Li, "Distributed optimal control for linear multiagent systems on general digraphs," *IEEE Trans. Automat. Control*, vol. 66, no. 1, pp. 322–328, Jan. 2021.
[33] Z. Zhang, H. Li, Y. Shi, S. Zhang, and W. Yan, "Cooperative optimal control for Lipschitz nonlinear systems over generally directed topologies," *Automatica*, vol. 122, Sep. 2020, Art. no. 109279.



Fang Fang (Senior Member, IEEE) received the M.Sc. degree in control theory and engineering from North China Electric Power University (Baoding Campus), Baoding, China, in 2001, and the Ph.D. degree in thermal power engineering from North China Electric Power University, Beijing, China, in 2005.

He is currently a Professor and the Dean of the School of Control and Computer Engineering, North China Electric Power University. He has authored more than 60 high level publications and headed more than 30 research projects or industrial projects. His current research interests include cyber-physical systems, configuration and operation of integrated energy systems, and intelligent power generation technologies.

Prof. Fang is an IET Fellow, the founding Vice Chairman of the Chinese Society for Electrical Engineering Technical Committee on Offshore Wind Power, the founding Vice Chairman of China Electrotechnical Society Technical Committee on Energy Intelligence, and a Council Member of IEEE IES Technical Committee on Industrial Cyber-Physical Systems.

Jiayu Li received the B.Sc. degree in automation and the M.Sc. degree in control engineering in 2017 and 2020, respectively, from North China Electric Power University, Beijing, China, where she is currently working toward the Ph.D. degree in control science and engineering with the School of Control and Computer Engineering.

Her research interests include multiagent systems, sampled-data control, and consensus applications in power systems.

Yajuan Liu received the B.S. degree in mathematics and applied mathematics from Shanxi Normal University, Linfen, China, in 2010, the M.S. degree in applied mathematics from the University of Science and Technology Beijing, Beijing, China, in 2012, and the Ph.D. degree from the Division of Electronic Engineering, Daegu University, Daegu, South Korea, in 2015.

From 2015 to 2018, she was a Postdoctoral Research Fellow with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea. She is currently an Associate Professor with the School of Control and Computer Engineering, North China Electric Power University, Beijing, China. Her research focus is on control of dynamic systems, including neural networks and complex systems.

Ju H. Park (Senior Member, IEEE) received the Ph.D. degree in electronics and electrical engineering from the Pohang University of Science and Technology, Pohang, South Korea, in 1997.

In March 2000, he joined Yeungnam University, Kyongsan, South Korea, where he is currently the Chuma Chair Professor. His research interests include control engineering, neural/complex networks, and fuzzy systems.

Prof. Park is a Fellow of the Korean Academy of Science and Technology. He was the recipient of the Highly Cited Researchers Award by Clarivate Analytics and listed in three fields, engineering, computer sciences, and mathematics, in 2019, 2020, and 2021. He is currently an Associate Editor for the IEEE TRANSACTION ON FUZZY SYSTEMS, IEEE TRANSACTION ON NEURAL NETWORKS AND LEARNING SYSTEMS, and IEEE TRANSACTION ON CYBERNETICS.