Cooperative Output-Feedback Secure Control of Distributed Linear Cyber-Physical Systems Resist Intermittent DoS Attacks

Xin Wang, *Member, IEEE*, Ju H. Park, *Senior Member, IEEE*, Heng Liu, and Xian Zhang, *Senior Member, IEEE*

***Abstract*—This article studies a cooperative output-feedback secure control problem for distributed cyber-physical systems over an unreliable communication interaction, which is to achieve coordination tracking in the presence of intermittent denial-of-service (DoS) attacks. Under the switching communication network environment, first, a distributed secure control method for each subsystem is proposed via neighborhood information, which includes the local state estimator and cooperative resilient controller. Second, based on the topology-dependent Lyapunov function approach, the design conditions of secure control protocol are derived such that cooperative tracking errors are uniformly ultimately bounded. Interestingly, by exploiting the topology-allocation-dependent average dwell-time (TADADT) technique, the stability analysis of closed-loop error dynamics is presented, and the proposed coordination design conditions can relax time constraints on interaction topology switching. Finally, two numerical examples are presented to demonstrate the effectiveness of the theoretical results.**

***Index Terms*—Cooperative secure control, distributed cyber-physical systems (CPSs), intermittent denial-of-service (DoS) attacks, observer-based output-feedback control, unreliable switching topology.**

I. Introduction

THE NOTATION of cyber-physical systems (CPSs) is a new generation of networked intelligent control systems that integrate physical processes, computational resources, communication, and control implementation [1]–[3]. As the wide application of the wireless sensor technology and the intelligent computation method [4]–[6] over a communication network in the industrial engineering field, the complex distributed CPSs (DCPSs) connect the physical devices through the communication/sensor network (such as multiagent systems [7]–[10], multivehicle platoon systems [11], distributed power systems [12], multiple underactuated ships formation [13], cooperative mobile manipulators [14], and so on), which enable these physical devices to manipulate physical entities in a remote, reliable, real time, secure, and collaborative manner through network space to achieve desired goals. Note that the coordination control objective of the above CPSs in a practical scenario may usually be transformed into the consensus/synchronization issues of distributed CPSs or MASs [15]–[19]. For example, the aim of platoon control is to track the leader's speed, and keep a safe distance between two consecutive follower vehicles The synchronization of the voltage magnitudes for distributed generators (DGs) in power systems is equivalent to synchronizing the direct term of reference voltages [20], [21].

As is well known, the unreliable information interactions or fragile network connections usually have to face the malicious cyber-attacks [22], [23]. For example, the denial-of-service (DoS) attacks, as a typical kind of cyber-attack, attempt to block the transmission of information, in communication channels [24]–[26]. Therefore, the information-flow security issue and reliable secure control problems of DCPSs have been paid considerable attention in engineering practice [27]–[32]. In recent years, under the assumption of cyber-attacks whose model is described by a random Markov process, the distributed secure tracking control problem of DCPSs is studied in [33], and then the cooperative resilient control protocol is designed to guarantee exponential cooperative tracking in a mean-square sense. Later on, Xu *et al.* [34] and Feng and Hu [35] investigated the secure coordination control issue of MASs against network DoS attacks by using event-triggered and self-triggered schemes, in which the consensus objective can be ensured if the frequency and duration of DoS attacks satisfy certain conditions. In [36], the decentralized adaptive output-feedback control issue of interconnected nonlinear systems is investigated in the presence of intermittent

Manuscript received April 23, 2020; revised September 2, 2020 and October 23, 2020; accepted October 25, 2020. Date of publication December 1, 2020; date of current version October 12, 2021. This work was supported by the National Research Foundation of Korea grant funded by the Korea Government (Ministry of Science and ICT) under Grant 2019R1A5A8080290. The work of Xin Wang was supported in part by the National Natural Science Foundation of China under Grant 61703148 and Grant 61873306, in part by the Natural Science Foundation of Heilongjiang Province under Grant LH2019F030, and in part by the Outstanding Youth Fund of Heilongjiang University under Grant JCL201903. This article was recommended by Associate Editor Y.-J. Liu. *(Corresponding author: Ju H. Park.)*

Xin Wang is with the School of Mathematical Science, Heilongjiang University, Harbin 150080, China, and also with the Department of Electrical Engineering, Yeungnam University, Gyeongsan 38541, South Korea (e-mail: xinwang@hlju.edu.cn).

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

Heng Liu and Xian Zhang are with the School of Mathematical Science, Heilongjiang University, Harbin 150080, China, and also with the Heilongjiang Provincial Key Laboratory of the Theory and Computation of Complex Systems, Heilongjiang University, Harbin 150080, China (e-mail: hengliu0404@163.com; xianzhang@ieee.org).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCYB.2020.3034374.

Digital Object Identifier 10.1109/TCYB.2020.3034374

DoS attacks. As the DoS attacks occur on different interaction channels, the distributed state-feedback and observer-based secure consensus control law is developed in [37]. By means of the switched stochastic time-delay system model approach, an output consensus secure control protocol for heterogeneous agent networks is designed under aperiodic sampling and random DoS attacks [38]. It is noted that the aforementioned secure coordination control design developments for DCPSs dealt mainly with the case of the underlying communication network for all subsystems persist in a time-invariant topology structure.

However, this constraint cannot hold in many practical network environments. For example, due to the communication failures or sensor range limitations that may often occur in the underwater environment, the agent subsystem in a team of autonomous underwater vehicles, who works together to fulfill a coordination task, need to cut off or connect with its neighbors in different time intervals. Therefore, it is also natural to study the cooperative secure control resist DoS attacks under switching communication network. But in general, the problem of designing a secure control protocol is more difficult for a switching agent network than for a fixed one. This is because, when the connection network among all subsystems is changing, it is a challenge to analyze and prove the global convergence caused by the complex interaction among the subsystem tracking performance, switching topology constraints, and the DoS attacks in communication channels. Consequently, how to establish a cooperative output-feedback-based secure control methodology for DCPSs with intermittent DoS attacks under switching communication constraints motivates this study.

In this article, we propose a novel cooperative secure control approach for DCPSs under switching topology in the presence of intermittent DoS attacks, which partially resolves the above problems. Compared with the existing results, the main contributions can be summarized as follows. First, unlike the previous results in [32]–[38], where the connection network is assumed to be a fixed topology, a switching topology network, including intermittent DoS attacks, is considered, which is more reasonable in practical applications. Second, a novel output-feedback-based secure control approach is designed for linear distributed CPSs under DoS attacks, in which, a local state observer for each subsystem is introduced to estimate the unmeasurable subsystem states, and the distributed secure controller is also designed by exploiting the exchanged neighborhood state estimates. Finally, the design conditions of secure control protocol on ensuring the cooperative tracking objective are set up by exploiting the topology-dependent Lyapunov function method and topology-allocation-dependent average dwell-time (TADADT) scheme, which develops the distributed secure control technology to defend cyber-attacks in practical industrial CPSs.

The remainder of the work is summarized as follows. Distributed CPSs description and preliminaries are given in Section II. The main result is proposed in Section III. Section IV contains two illustrative examples. Finally, the conclusion of this work is drawn in Section V.

Notation: $\mathbb{R}^n$ stands for the n-dimensional Euclidean space. $\mathbf{0}$, $\mathbf{1}$, and I are zero matrix, all 1 column vector, and the identity matrix with appropriate dimension, respectively. $\|\cdot\|$ means the Euclidean norm. $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$ express the maximum and minimum eigenvalue of matrix $A \in \mathbb{R}^{n\times n}$. A^{T} is the transpose mark of A. $M \otimes N$ indicates the Kronecker product of $M \in \mathbb{R}^{m\times n}$ and $N \in \mathbb{R}^{p\times q}$. If matrix P is positive, it is noted as $P > 0$.

II. Preliminaries and Problem Statement

A. Basic Graph Theory

A communication graph can be denoted by $\mathcal{G}(\mathcal{V}, \mathcal{E}, \mathcal{A})$, where $\mathcal{V} = \{v_1, v_2, \ldots, , v_N\}$, $\mathcal{E} = \mathcal{V} \times \mathcal{V}$, and $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$ stand for the N nodes set, edges set, and the associated adjacency matrix, respectively. Here, $a_{ij} > 0$ indicates the signal can be transferred between nodes i and j. For node i, the set of its neighbors is denoted by $\mathcal{N}_i = \{v_i \in \mathcal{V} : \varepsilon_{ij} \in \mathcal{E}, j \neq i\}$. If edges $\varepsilon_{ij} = \varepsilon_{ji}$, for $\forall \varepsilon_{ij}, \varepsilon_{ji} \in \mathcal{E}$ and there exists a path between any pair of vertices, that means the communication graph is undirected and connected. A path here refers to a series of connected edges. The Laplacian matrix $\mathcal{L} = [\mathcal{L}_{ij}] \in \mathbb{R}^{N\times N}$ is depicted by $\mathcal{L}_{ii} = \sum_{j\neq i} a_{ij}$ and $\mathcal{L}_{ij} = -a_{ij}, i \neq j$.

B. DCPS Dynamics and Switching Communication Networks

Consider a DCPS consisting $N + 1$ subsystems distributed on a time-varying communication network, the dynamics of the ith subsystem of the DCPSs are modeled as

$$\begin{aligned} \dot{x}_i(t) &= \mathrm{A}x_i(t) + \mathrm{B}u_i(t) \\ y_i(t) &= \mathrm{C}x_i(t), \quad i = 1, \ldots, N \end{aligned} \tag{1}$$

where $x_i(t) \in \mathbb{R}^n$ means the ith subsystem state, $u_i(t) \in \mathbb{R}^p$ and $y_i(t) \in \mathbb{R}^q$ represent the control input and output signals, respectively, and A, B, and C are constant matrices with appropriate dimensions, and satisfy (A, B, C) is stabilizable and detectable. Here, the leader node can be indexed with 0 and its model is described by

$$\begin{aligned} \dot{x}_0(t) &= \mathrm{A}x_0(t) + \mathrm{B}u_0(t) \\ y_0(t) &= \mathrm{C}x_0(t) \end{aligned} \tag{2}$$

with $x_0(t)$ and $y_0(t)$ are the state and output vectors, respectively, $u_0(t)$ is the unknown time-varying input signal of leader satisfying $\|u_0(t)\| \leq \bar{u}$, and $\bar{u} > 0$ is an unknown constant.

Let $\mathbf{G} = \{\mathcal{G}_p : p \in \mathcal{P}\}$ be a set with an index set $\mathcal{P}$, which contains all possible undirected connected graphs. Meanwhile, define a topology switching signal $\sigma(t) : [0, +\infty) \to \mathcal{P}$. Then, the time-varying adjacency matrix and the Laplacian matrix can be rewritten as $\mathcal{A}^{\sigma(t)} = [a_{ij}^{\sigma(t)}] \in \mathbb{R}^{N\times N}$ and $\mathcal{L}^{\sigma(t)} = \begin{bmatrix} 0 & 0_{1\times N} \\ \mathcal{L}_2^{\sigma(t)} & \mathcal{L}_1^{\sigma(t)} \end{bmatrix} \in \mathbb{R}^{(N+1)\times(N+1)}$, with $\mathcal{L}_1^{\sigma(t)} = [\mathcal{L}_{ij}^{\sigma(t)}] \in \mathbb{R}^{N\times N}$ and $\mathcal{L}_2^{\sigma(t)} \in \mathbb{R}^{N\times 1}$. Denote $[t_m, t_{m+1})$, $m \in \mathbb{N}$ as an infinite time sequence of bounded nonoverlapping intervals. Here, the sequence $t_0, t_1, \ldots,$ represents topology switching time. Supposed that there is a dwell time τ_m such that $t_{m+1} - t_m \geq \tau_m$, across $[t_m, t_{m+1})$ the interactive connection graph is time invariant.

Assumption 1: The communication interaction graph $\{\mathcal{G}_p : p \in \mathcal{P}\}$ is fixed and connected on every interval $[t_m, t_{m+1})$, $m = 1, 2, \ldots, .$ Each subgraph of all follower subsystems is undirected, the leader has a directed path to one subsystem at least.

Inspired by the work presented in [31], the notion of TADADT will be introduced. First, by applying the topology allocation strategy, we define a set $S(\mathcal{G}_p)$ be all eigenvalues of the matrix $\mathcal{L}_1^p$ with all $p \in \mathcal{P}$, that is, $S(\mathcal{G}_p) = \{s_1^p, s_2^p, \ldots, s_N^p | s_i^p = \lambda_i(\mathcal{L}_1^p), i = 1, \ldots, N\}$. Then, the topology partition of all possible graphs $\mathbf{G} = \bigcup_{z\in\mathcal{Z}} Q_z$ with $Q_z = \{\mathcal{G}_{z1}, \mathcal{G}_{z2}, \ldots, \mathcal{G}_{zr} | S(\mathcal{G}_{zi}) = S(\mathcal{G}_{zj})\ \forall zi, zj \in \mathcal{P}, zi \neq zj\}$ and $\mathcal{Z}$ is an index set which includes all possible graph connection types. Thus, we can find the following set, which includes the same eigenvalues of the matrix $\mathcal{L}_1^p$, $\bar{S} = \{\bar{s}_1^z, \bar{s}_2^z, \ldots, \bar{s}_N^z | \bar{s}_i^z = \lambda_i(\mathcal{L}_1^{\bar{z}}), i = 1, \ldots, N, \bar{z} \in \{z_1, z_2, \ldots, z_{qr}\}\}$. In addition, by applying [31, Lemma 1], the TADADT is defined as follows.

Definition 1 [31]: For any $\tau_2 > \tau_1 \geq 0$, if there exists a switching signal $\sigma(t)$ over (τ_1, τ_2) such that the following inequality established:

$$\mathcal{N}_\sigma^z(\tau_1, \tau_2) \leq \mathcal{N}_0^z + \frac{T^z(\tau_1, \tau_2)}{\tau_{az}} \tag{3}$$

then τ_{az} is called TADADT for $\tau_{az} > 0$ and $\mathcal{N}_0^z \geq 0$. Moreover, $\mathcal{N}_\sigma^z(\tau_1, \tau_2)$ and $T^z(\tau_1, \tau_2)$ are the number of switching and total running time of Q_z over (τ_1, τ_2), respectively.

Remark 1: Note that the TADADT method is introduced to divide the topology graph set $\mathbf{G}$ according to the topology connectivity property. In each communication graph subset Q_z, all elements have the same network connectivity property, which means the augmented Laplacian matrix $\mathcal{L}_1^{zk}$ of topology $\mathcal{G}_{zk}$ in the same subset Q_z has the same eigenvalues. Then, the TADADT condition of $\mathcal{G}_{zk}$ can be used to design the distributed secure control algorithm resist intermittent DoS attacks under switching communication networks. It is worth noting that the proposed methods in this study can reduce the conservation of ADT and topology-dependent ADT ones [23], [39].

C. Intermittent DoS Attacks Constraints

A DoS attack is an attack means that interferes with the virtual channel of a normal wireless network communication. The information exchange of the virtual channel is blocked by transmitting other uncorrelated signals, so that the agent cannot receive timely neighborhood information. When the virtual channel ε_{ij} is attacked, it is assumed that the virtual channel ε_{ji} is also attacked.

Owing to the energy constraints and environmental factors from the interfering signals transmitted by the opponents, the arrival time of DoS attacks is usually intermittent or random. The following situation is considered one attack: 1) If the two attacks have the same arrival time and the duration is different and 2) If the arrival time of the two attacks is different, but the duration of the attack is intersecting. So assume that the attacks occur in some discontinuous time intervals. Define $\mathcal{T}_m = [\mathbf{t}_m, \mathbf{t}_m^1)$ as a time sequence in which the attacks occur. For any $\mathbf{t} \geq \mathbf{t}_0$, $\mathbf{t}_0$ is the initial time, we can define the following time intervals:

$$\Lambda(t) = \bigcup_{m\in\mathbb{N}^+} \mathcal{T}_m \bigcap [\mathbf{t}_0, \mathbf{t}), \quad \Xi(t) = [\mathbf{t}_0, \mathbf{t})/\Lambda(t) \tag{4}$$

where $[\mathbf{t}_0, \mathbf{t})$ means a time set containing the arrival and nonarrival of the all attacks. Hence, it could be rewritten as $[\mathbf{t}_0, \mathbf{t}) = \bigcup_{m\in\mathbb{N}^+} [\mathbf{t}_m, \mathbf{t}_{m+1}) \bigcup [\mathbf{t}_0, \mathbf{t}_1)$, which each interval $[\mathbf{t}_m, \mathbf{t}_{m+1})$ consists of the nonoverlapping subintervals $[\mathbf{t}_m^0, \mathbf{t}_m^1), \ldots, [\mathbf{t}_m^{l_m-1}, \mathbf{t}_m^{l_m})$, l_m represents the frequency of topology switching during the time interval between two adjacent attacks.

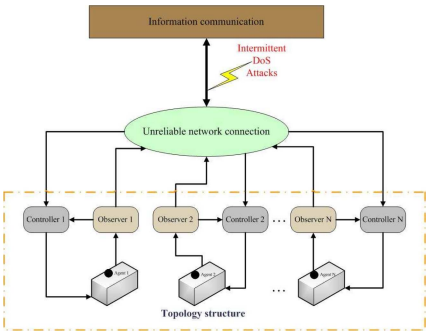


Fig. 1. Distributed CPSs under intermittent DoS attacks.

D. Cooperative Secure Control Objective

For the considered DCPSs with intermittent DoS attacks under a switching communication network, the main objective here is to design a cooperative secure control algorithm for each subsystem only using the output information, to achieve the convergence of estimation errors and the coordination tracking of DCPSs under the leader-following network structure. Fig. 1 shows the distributed CPSs under intermittent DoS attacks.

Remark 2: Compared with the traditional centralized CPSs under network attacks, the major difficulties in designing the cooperative secure control scheme for DCPSs lie in that: first, the complex structure of distributed networked systems increases the possibility of suffering network attacks; and second, malicious attacks not only cause the performance deterioration for local subsystems but also may affect the coordination synchronization of the distributed network. Therefore, it is important and challenging to solve coordination secure problems subject to network DoS attacks in CPS security.

III. Main Results

Suppose that only a group of subsystems acquires the leader's information, and each follower subsystem can use relative information from its neighbors to design a cooperative secure controller. In this section, we will present a systematic design procedure for the cooperative secure output-feedback control problem of the considered DCPSs via distributed neighborhood information.

A. Cooperative Secure Control Scheme Design

Note that in the unreliable communication environment, the relative output information of neighboring subsystems is

unavailable for designing control protocol when a DoS attack is launched. On the basis of the discontinuous neighborhood output signals, the following observer-based cooperative secure controller is designed for the ith follower subsystem:

$$\begin{aligned}
&\text{i) if } t \in \Xi(t):\\
&\quad\begin{cases}\dot{v}_i(t) = Av_i(t) + \mathrm{B}u_i(t) + L\big[Cv_i(t) - y_i(t)\big]\\ u_i(t) = \theta\omega_i(t) + \theta f_i(\omega_i(t))\\ \omega_i(t) = K\sum\limits_{j=0}^{N} a_{ij}^{\sigma(t)}\big(v_i(t) - v_j(t)\big)\end{cases}\\
&\text{ii) if } t \in \Lambda(t):\\
&\quad\begin{cases}\dot{v}_i(t) = Av_i(t) + \mathrm{B}u_i(t) + L\big[Cv_i(t) - y_i(t)\big]\\ u_i(t) = 0\end{cases}
\end{aligned} \tag{5}$$

where $v_i(t) \in \mathbb{R}^n$ is the estimate of the state $x_i(t)$, and θ, L, and K are the controller parameter, observer gain matrix, and the feedback gain matrix to be designed, respectively. The control auxiliary function $f_i(\omega_i)$ is defined as

$$f_i(\omega_i) = \begin{cases}\omega_i(t)/(\|\omega_i(t)\|), & \text{if } \theta\omega_i > \pi\\ \theta\omega_i(t)/\pi, & \text{if } \theta\omega_i \le \pi\end{cases} \tag{6}$$

where π is a positive parameter. Meanwhile, the leader's estimate state $v_0(t)$ can be obtained from its local observer, that is, $\dot{v}_0(t) = Av_0(t) + \mathrm{B}u_0 + L[Cv_0(t) - y_0(t)]$. Denote

$$\begin{aligned}
\tilde{x}_i(t) &= x_i(t) - x_0(t),\ \ \tilde{v}_i(t) = v_i(t) - v_0(t)\\
\tilde{x}(t) &= \big[\tilde{x}_1^{\mathrm{T}}(t), \ldots, \tilde{x}_N^{\mathrm{T}}(t)\big]^{\mathrm{T}},\ \ \tilde{v}(t) = \big[\tilde{v}_1^{\mathrm{T}}(t), \ldots, \tilde{v}_N^{\mathrm{T}}(t)\big]^{\mathrm{T}}\\
\omega_i(t) &= \Big(\Big[0_{1\times N}\mathcal{L}_{i1}^{\sigma(t)} \cdots \mathcal{L}_{iN}^{\sigma(t)}\Big] \otimes K\Big)e(t)\\
F(\omega(t)) &= \big[f_1^{\mathrm{T}}(\omega_1), \ldots, f_N^{\mathrm{T}}(\omega_N)\big]^{\mathrm{T}}
\end{aligned}$$

then, the dynamics of segmented closed-loop error $e(t) = [\tilde{x}^{\mathrm{T}}(t), \tilde{v}^{\mathrm{T}}(t)]^{\mathrm{T}}$ can be written as

$$\dot{e}(t) = \begin{cases}\Pi_1 e(t) + \theta\begin{bmatrix}I_N \otimes B\\ I_N \otimes B\end{bmatrix}F(\omega(t)) - \begin{bmatrix}\mathbf{1}_N \otimes B\\ \mathbf{1}_N \otimes B\end{bmatrix}u_0\\ \qquad\qquad \text{if } t \in \Xi(t)\\ \begin{bmatrix}I_N \otimes A & \mathbf{0}\\ -I_N \otimes \mathrm{LC} & I_N \otimes D_2\end{bmatrix}e(t) - \begin{bmatrix}\mathbf{1}_N \otimes B\\ \mathbf{1}_N \otimes B\end{bmatrix}u_0\\ \qquad\qquad \text{if } t \in \Lambda(t)\end{cases} \tag{7}$$

where $\Pi_1 = \begin{bmatrix}I_N \otimes A & \theta\mathcal{L}_1^{\sigma(t)} \otimes (\mathrm{BK})\\ -I_N \otimes (\mathrm{LC}) & D_1\end{bmatrix}$, and $D_1 = I_N \otimes D_2 + \theta\mathcal{L}_1^{\sigma(t)} \otimes (\mathrm{BK})$, $D_2 = A + \mathrm{LC}$. Furthermore, we define the cooperative error as

$$\delta(t) = \begin{bmatrix}\xi(t)\\ \tilde{v}(t)\end{bmatrix} = \begin{bmatrix}I_{nN} & -I_{nN}\\ \mathbf{0} & I_{nN}\end{bmatrix}e(t) \tag{8}$$

with $\xi(t) = \tilde{x}(t) - \tilde{v}(t) = [\xi_1^{\mathrm{T}}(t), \ldots, \xi_N^{\mathrm{T}}(t)]^{\mathrm{T}}$. From (7), we imply the dynamics of the closed-loop cooperative error $\delta(t)$ satisfying

$$\dot{\delta}(t) = \begin{cases}\Pi_2\delta(t) + \theta\begin{bmatrix}\mathbf{0}\\ I_N \otimes B\end{bmatrix}F(\omega(t))) - \begin{bmatrix}\mathbf{0}\\ \mathbf{1}_N \otimes B\end{bmatrix}u_0\\ \qquad\qquad \text{if } t \in \Xi(t)\\ \begin{bmatrix}I_N \otimes D_2 & \mathbf{0}\\ I_N \otimes (-\mathrm{LC}) & I_N \otimes A\end{bmatrix}\delta(t) - \begin{bmatrix}\mathbf{0}\\ \mathbf{1}_N \otimes B\end{bmatrix}u_0\\ \qquad\qquad \text{if } t \in \Lambda(t)\end{cases} \tag{9}$$

where $\Pi_2 = \begin{bmatrix}I_N \otimes (A + \mathrm{LC}) & \mathbf{0}\\ -I_N \otimes (\mathrm{LC}) & I_N \otimes A + \theta\mathcal{L}_1^{\sigma(t)} \otimes (\mathrm{BK})\end{bmatrix}$. From the above analysis, the cooperative secure control problem of DCPSs (1)-(2) with observer-based distributed controller (5) has been converted to the simultaneously stability of zero equilibrium points for the cooperative error system (9).

B. Stability Analysis

In this section, the uniform ultimate boundedness of the closed-loop cooperative error system (9) will be proved. Besides, let us denote $a_z = \lambda_{\min_{z\in\mathcal{Z}}}(Q_z)$ and $b_z = \lambda_{\max_{z\in\mathcal{Z}}}(Q_z)$, $\underline{\lambda}_a = \min_{z\in\mathcal{Z}}(a_z)$, $\bar{\lambda}_b = \max_{z\in\mathcal{Z}}(b_z)$. By the aforementioned design of the cooperative secure control protocol and analysis procedure, the following theorem can be derived.

Theorem 1: Consider the DCPSs (1)-(2) described by dynamic leader–follower networks satisfying Assumptions 1 and 2. If there exist matrices $P_1 > 0$, $P_2 > 0$, L, and a constant $\alpha^* > 0$ such that the following inequalities hold:

$$\begin{bmatrix}P_1(A + \mathrm{LC}) + (A + \mathrm{LC})^{\mathrm{T}}P_1 + \alpha^* P_1 & C^{\mathrm{T}}\\ C & -I\end{bmatrix} < 0 \tag{10a}$$

$$\begin{bmatrix}P_2A + A^{\mathrm{T}}P_2 - 2P_2\mathrm{B}\mathrm{B}^{\mathrm{T}}P_2 + \alpha^* P_2 & P_2L\\ L^{\mathrm{T}}P_2 & -I\end{bmatrix} < 0. \tag{10b}$$

In addition, we select parameters $\alpha_z^* < ([\alpha^* a_z]/b_z)$, $\kappa_z > (b_z/\underline{\lambda}_a)$, and $\beta_z^* > \beta^* > 0$ such that the following conditions hold:

$$\sum_{z\in\mathcal{Z}}\Big(\alpha_z^* - \frac{\ln\kappa_z}{\tau_{az}}\Big)T^z\Big(\mathbf{t}_J^1, \mathbf{t}_{J+1}\Big) - \sum_{z\in\mathcal{Z}}\mathcal{N}_0^z \ln\kappa_z - \ln\frac{1}{\underline{\lambda}_a} - \beta_z^*\Big(\mathbf{t}_J^1 - \mathbf{t}_J\Big) > 0 \tag{11a}$$

$$\sum_{z\in\mathcal{Z}}\Big(\alpha_z^* - \frac{\ln\kappa_z}{\tau_{az}}\Big)T^z(\mathbf{t}_0, \mathbf{t}_1) - \sum_{z\in\mathcal{Z}}\mathcal{N}_0^z \ln\kappa_z - \ln\frac{1}{\underline{\lambda}_a} > 0 \tag{11b}$$

$$P_1(A + \mathrm{LC}) + (A + \mathrm{LC})^{\mathrm{T}}P_1 + \mathrm{C}\mathrm{C}^{\mathrm{T}} - \beta^* P_1 < 0 \tag{11c}$$

$$P_2A + A^{\mathrm{T}}P_2 + P_2LL^{\mathrm{T}}P_2 - \beta^* P_2 < 0. \tag{11d}$$

Then, there exists the observer-based cooperative controller (5) such that the cooperative secure control objective is ensured, that is, all the closed-loop error signals in the cooperative error system (9) are UUB even in the cases of the intermittent DoS attacks. And the gain matrix of the designed observers is given as $K = -B^{\mathrm{T}}P_2$. Furthermore, the cooperative error signal $\delta(t)$ will eventually converge to the following compact set:

$$\delta^* = \{\delta(t) | \|\delta(t)\| < \delta_1\} \tag{12}$$

where $\delta_1 = \max\{\delta_0, \sqrt{(\bar{\lambda}_b/\underline{\lambda}_a)\delta_0^2}\}$ and $\delta_0 > 0$.

Proof: Consider the following segmented multiple topology-dependent Lyapunov functions candidate:

$$V_{\sigma(t)}(t) = \begin{cases}\delta^{\mathrm{T}}(t)\Upsilon_{\sigma(t)}\delta(t), & \text{if } t \in \Xi(t)\\ \delta^{\mathrm{T}}(t)\Omega\delta(t), & \text{if } t \in \Lambda(t)\end{cases} \tag{13}$$

where $\Upsilon_{\sigma(t)} = \mathrm{diag}\{\mathcal{L}_1^{\sigma(t)} \otimes P_1, \mathcal{L}_1^{\sigma(t)} \otimes P_2\}$ and $\Omega = \mathrm{diag}\{I_N \otimes P_1, I_N \otimes P_2\}$. This entire proof is divided into the following three parts.

Part A: First, we denote $\sigma(t) = p$, $p \in \mathcal{P}$ on the interval $t \in [\mathbf{t}_m^f, \mathbf{t}_m^{f+1}), f = 1, 2, \ldots, l_m - 1$. Then, the time derivative of $V_{\sigma(t)}(t)$ along the error system (9) on every interval satisfies

$$\dot{V}_p(t) = \delta^{\mathrm{T}}(t)\begin{bmatrix} \mathcal{L}_1^p \otimes 2P_1(A+\mathrm{LC}) & \mathbf{0} \\ \mathcal{L}_1^p \otimes (-2P_2\mathrm{LC}) & D_4 \end{bmatrix}\delta(t) + 2\delta^{\mathrm{T}}(t) \times \begin{bmatrix} \mathbf{0} \\ \theta\mathcal{L}_1^p \otimes P_2B \end{bmatrix}F(\omega) - 2\delta^{\mathrm{T}}(t)\begin{bmatrix} \mathbf{0} \\ \mathcal{L}_1^p\mathbf{1}_N \otimes P_2B \end{bmatrix}u_0 \tag{14}$$

where $D_4 = \mathcal{L}_1^p \otimes (2P_2A) + 2\theta(\mathcal{L}_1^p)^2 \otimes (P_2\mathrm{BK})$. In views of $\|u_0\| \le \bar{u}$, it follows that:

$$-2\delta^{\mathrm{T}}\begin{bmatrix} \mathbf{0} \\ \mathcal{L}_1^p\mathbf{1}_N \otimes P_2B \end{bmatrix}u_0 \le 2\bar{u}\sum_{i=1}^{N}\left\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\right\|. \tag{15}$$

Furthermore, we consider the following three cases.

Consider 1). When $\theta\omega_i > \pi$, that is, $f_i(\omega_i) = (\omega_i/\|\omega_i\|)$, we have $2\delta^{\mathrm{T}}\begin{bmatrix} \mathbf{0} \\ \theta\mathcal{L}_1^p \otimes P_2B \end{bmatrix}F(\omega) = -2\theta\sum_{i=1}^{N}\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\|$. Hence, (14) could be rewritten as

$$\dot{V}_p(t) \le \Gamma^p(t) - 2(\theta-\bar{u})\sum_{i=1}^{N}\left\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\right\| \tag{16}$$

where $\Gamma^p(t) = \delta^{\mathrm{T}}(t)\begin{bmatrix} \mathcal{L}_1^p \otimes 2P_1(A+\mathrm{LC}) & \mathbf{0} \\ \mathcal{L}_1^p \otimes (-2P_2\mathrm{LC}) & D_4 \end{bmatrix}\delta(t)$.

Consider 2). While $\theta\omega_i \le \pi$, using the inequality $-(\theta^2/\pi)\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\|^2 + \theta\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\| \le (1/4)\pi$, one obtains $\dot{V}_p(t) \le \Gamma^p(t) - 2(\theta-\bar{u})\sum_{i=1}^{N}\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\| + (1/2)N\pi$.

Consider 3). Let ι be a positive integer satisfying $2 \le \iota \le N-1$, and assume that

$$f_i(\omega_i) = \begin{cases} \frac{\omega_i}{\|\omega_i\|}0, & i = 1, \ldots, \iota \\ \frac{\theta\omega_i}{\pi}, & i = \iota+1, \ldots, N. \end{cases} \tag{17}$$

Then, one has $2\delta^{\mathrm{T}}\begin{bmatrix} \mathbf{0} \\ \theta\mathcal{L}_1^p \otimes P_2B \end{bmatrix}F(\omega) = -2\theta\sum_{i=1}^{\iota}\|\sum_{j=1}^{N}\mathcal{L}_{ij}^p B^{\mathrm{T}}P_2\tilde{\nu}_j(t)\| - 2(\theta^2/\pi)\sum_{i=\iota+1}^{N}\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\|^2$. Hance, it follows from (17) that: $\dot{V}_p(t) \le \Gamma^p(t) - 2(\theta-\bar{u})\sum_{i=1}^{N}\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\| + \bar{\iota}$, where $\bar{\iota} = (1/2)(N-\iota)\pi$. In the light of the above three cases, we can obtain the following unified result:

$$\dot{V}_p(t) \le \Gamma^p(t) - 2(\theta-\bar{u})\sum_{i=1}^{N}\left\|\sum_{j=1}^{N}\mathcal{L}_{ij}^pB^{\mathrm{T}}P_2\tilde{\nu}_j(t)\right\| + \tfrac{1}{2}N\pi. \tag{18}$$

Note that

$$\Gamma^p(t) \le \xi^{\mathrm{T}}(t)\big[\mathcal{L}_1^p \otimes \big[P_1(A+\mathrm{LC}) + (A+\mathrm{LC})^{\mathrm{T}}P_1 + C^{\mathrm{T}}C\big]\xi(t) + \tilde{\nu}^{\mathrm{T}}(t)\big[\mathcal{L}_1^p \otimes \big(P_2A + A^{\mathrm{T}}P_2 - 2\theta a_zP_2\mathrm{BB}^{\mathrm{T}}P_2 + P_2LL^{\mathrm{T}}P_2^{\mathrm{T}}\big)\big]\tilde{\nu}(t) \tag{19}$$

where we use the fact $2a^{\mathrm{T}}b \le a^{\mathrm{T}}a + b^{\mathrm{T}}b$ and $K = -B^{\mathrm{T}}P_2$. Then, substituting (19) into (18) yields

$$\dot{V}_p(t) \le \xi^{\mathrm{T}}(t)\big\{\mathcal{L}_1^p \otimes \big[P_1(A+\mathrm{LC}) + (A+\mathrm{LC})^{\mathrm{T}}P_1 + C^{\mathrm{T}}C\big]\big\}\xi(t) + \tilde{\nu}^{\mathrm{T}}(t)\big[\mathcal{L}_1^p \otimes \big(P_2A + A^{\mathrm{T}}P_2 - 2\theta a_zP_2\mathrm{BB}^{\mathrm{T}}P_2 + P_2LL^{\mathrm{T}}P_2\big)\big]\tilde{\nu}(t) + \frac{1}{2}N\pi - 2(\theta-\bar{u})\sum_{i=1}^{N}\left\|B^{\mathrm{T}}P_2\sum_{j=1}^{N}\mathcal{L}_{ij}^p\tilde{\nu}_j(t)\right\|. \tag{20}$$

Choosing θ sufficiently large such that $\theta a_z \ge 1$ and $\theta \ge \bar{u}$, as well as exploiting inequality (10) and the Schur complement lemma, that is, $\dot{V}_p(t) \le -\alpha^*V_p(t) + (1/2)N\pi$, which means $\dot{V}_p(t) < 0$ on $V_p(t) = \rho$ when $\alpha^* > (N\pi/2\rho)$. Thus, it knows that all error signals are bounded with $t \in [\mathbf{t}_m^f, \mathbf{t}_m^{f+1}), f = 1, 2, \ldots, l_m - 1$. By choosing some positive constants $\alpha_z^* < (\alpha^*a_z/b_z)$, $\kappa_{z1} > (b_{z1}/\underline{\lambda}_a)$ and define $M = (1/2)N\pi$, the following relationships are obtained for any $t \in [\mathbf{t}_m^1, \mathbf{t}_m^{l_m})$, $m \in N^+$: 1) $\dot{V}_p(t) \le -\alpha_z^*V_p(t) + M\ \forall \mathcal{G}_p \in Q_z, z \in \mathcal{Z}$ and 2) $V_{p1}(t) \le \kappa_{z1}V_{p2}(t)\ \forall \mathcal{G}_{p1} \in Q_{z1}, \mathcal{G}_{p2} \in Q_{z2}$. Furthermore, using the above inequalities for $t \in [\mathbf{t}_m^1, \mathbf{t}_m^{l_m})$, one has

$$\begin{aligned} V_{\sigma\left(\mathbf{t}_m^{l_m-1}\right)}\left(\mathbf{t}_m^{l_m-}\right) &\le \prod_{f=2}^{l_m-1}\kappa_{\sigma\left(\mathbf{t}_m^f\right)}\exp\left\{-\alpha^*_{\sigma\left(\mathbf{t}_m^{l_m-1}\right)}\mathbf{t}_m^{l_m} + \sum_{f=2}^{l_m-1}\left(\alpha^*_{\sigma\left(\mathbf{t}_m^f\right)} - \alpha^*_{\sigma\left(\mathbf{t}_m^{f-1}\right)}\right)\mathbf{t}_m^f + \alpha^*_{\sigma(\mathbf{t}_m^1)}\mathbf{t}_m^1\right\}V_{\sigma(\mathbf{t}_m^1)}\left(\mathbf{t}_m^1\right) + M\int_{t_m^{l_m-1}}^{t_m^{l_m}}\exp \\ &\quad \left\{-\alpha^*_{\sigma\left(\mathbf{t}_m^{l_m-1}\right)}\left(\mathbf{t}_m^{l_m}-\tau\right)\right\}d\tau + \cdots + M\prod_{f=2}^{l_m-1}\kappa_{\sigma\left(\mathbf{t}_m^f\right)} \\ &\quad \times \int_{\mathbf{t}_m^1}^{\mathbf{t}_m^2}\exp\left\{-\sum_{f=3}^{l_m}\alpha^*_{\sigma\left(\mathbf{t}_m^{f-1}\right)}\left(\mathbf{t}_m^f - \mathbf{t}_m^{f-1}\right) - \alpha^*_{\sigma(\mathbf{t}_m^1)}\left(\mathbf{t}_m^2-\tau\right)\right\}d\tau. \end{aligned} \tag{21}$$

Similarly, for $t \in [\mathbf{t}_0, \mathbf{t}_1)$, it follows that:

$$\begin{aligned} V_{\sigma\left(\mathbf{t}_0^{l_0-1}\right)}\left(\mathbf{t}_1^-\right) &\le \exp\left\{\sum_{f=1}^{l_0-1}\ln\kappa_{\sigma\left(\mathbf{t}_0^f\right)} - \sum_{f=1}^{l_0}\alpha^*_{\sigma\left(\mathbf{t}_0^{f-1}\right)}\left(\mathbf{t}_0^f - \mathbf{t}_0^{f-1}\right)\right\} \\ &\quad \times V_{\sigma(\mathbf{t}_0)}(\mathbf{t}_0) + M\int_{\mathbf{t}_0^{l_0-1}}^{\mathbf{t}_0^{l_0}}\exp \\ &\quad \left\{-\alpha^*_{\sigma\left(\mathbf{t}_0^{l_0-1}\right)}\left(\mathbf{t}_0^{l_0}-\tau\right)\right\}d\tau + \cdots + M\prod_{f=1}^{l_0-1}\kappa_{\sigma\left(\mathbf{t}_0^f\right)} \end{aligned}$$

$$\times \int_{\mathbf{t}_0^0}^{\mathbf{t}_0^1} \exp\left\{-\sum_{f=2}^{l_0-1}\alpha^*_{\sigma\left(\mathbf{t}_0^f\right)}\left(\mathbf{t}_0^f-\mathbf{t}_0^{f-1}\right) - \alpha^*_{\sigma(\mathbf{t}_0^1)}\left(\mathbf{t}_0^1-\tau\right)\right\}d\tau. \tag{22}$$

Part B: When the DoS attacks are launched in interval $t \in [\mathbf{t}_m, \mathbf{t}_m^1), m \in N^+$, the time derivative of $V_{\sigma(t)}(t)$ along the trajectory of (9) satisfies

$$\begin{aligned}\dot{V}_{\sigma(t)}(t) \le{}& \xi^{\mathrm{T}}(t)\left[I_N\otimes\left(P_1(A+\mathrm{LC})+(A+\mathrm{LC})^{\mathrm{T}}P_1+\mathrm{CC}^{\mathrm{T}}\right)\right]\xi(t)\\ &+\tilde{\nu}^{\mathrm{T}}(t)\left[I_N\otimes\left(P_2A+A^{\mathrm{T}}P_2+P_2LL^{\mathrm{T}}P_2\right)\right]\tilde{\nu}(t)\\ &-2\delta^{\mathrm{T}}(t)\begin{bmatrix}\mathbf{0}\\ \mathbf{1}_N\otimes P_2B\end{bmatrix}u_0.\end{aligned}$$

From (11c) and (11d), it implies $\dot{V}_{\sigma(t)}(t) \le \beta^* V_{\sigma(t)}(t) + 2\|\delta_0\|\|P_2B\|\|u_0\| \le \beta_z^* V_{\sigma(t)}(t)$, where $\beta_z^* \ge \beta^* + ([2\|P_2B\|\bar{u}]/[\delta_0\underline{c}])$, $\underline{c} = \min\{\lambda_{\min}(P_1), \lambda_{\min}(P_2)\}$ for any given parameter $\delta_0 > 0$ satisfies $\|\delta(t)\| > \delta_0$. Therefore, using $V_{\sigma(\mathbf{t}_m)}(\mathbf{t}_m) \le (1/\underline{\lambda}_a)V_{\sigma(\mathbf{t}_{m-1}^{l_m-1})}(\mathbf{t}_m^{l_m-})$, the following inequality holds:

$$\begin{aligned}V_{\sigma(\mathbf{t}_m)}\left(\mathbf{t}_m^{1-}\right) &\le \exp\left\{\beta_z^*\left(\mathbf{t}_m^1-\mathbf{t}_m\right)\right\}V_{\sigma(\mathbf{t}_m)}(\mathbf{t}_m)\\ &\le \frac{1}{\underline{\lambda}_a}\exp\left\{\beta_z^*(\mathbf{t}_m^1-\mathbf{t}_m)\right\}V_{\sigma\left(\mathbf{t}_{m-1}^{l_m-1}\right)}\left(\mathbf{t}_m^{l_m-}\right).\end{aligned} \tag{23}$$

Part C: Finally, combining (21) and (22) with (23) on the interval $t \in [\mathbf{t}_0, \mathbf{t})$, it follows that:

$$\begin{aligned}&V_{\sigma(\mathbf{t}_{m+1})}(\mathbf{t}_{m+1})\\ &\le \left(\frac{1}{\underline{\lambda}_a}\right)^{\mathcal{N}_\sigma^d(\mathbf{t}_0,\mathbf{t})}\exp\\ &\quad\left\{\sum_{k=0}^{m}\left[\beta_z^*\left(\mathbf{t}_k^1-\mathbf{t}_k\right)+\sum_{z\in\mathcal{Z}}\mathcal{N}_0^z\ln\kappa_z - \sum_{z\in\mathcal{Z}}\left(\alpha_z^*-\frac{\ln\kappa_z}{\tau_{az}}\right)T^z\left(\mathbf{t}_k^1,\mathbf{t}_{k+1}\right)\right]\right\}\\ &\quad\times V_{\sigma(\mathbf{t}_m)}(\mathbf{t}_m)+\sum_{k=0}^{m}\\ &\quad\times\left[M\int_{\mathbf{t}_k^1}^{\mathbf{t}_{k+1}}\exp\left\{\sum_{z\in\mathcal{Z}}\mathcal{N}_0^z\ln_{\kappa_z} - \sum_{z\in\mathcal{Z}}\left(\alpha_z^*-\frac{\ln\kappa_z}{\tau_{az}}\right)T^z(\tau,\mathbf{t})\right\}d\tau\right]\\ &\le \exp\left\{-\sum_{j=1}^{m}\Psi_j-\Psi_0\right\}V_{\sigma(\mathbf{t}_0)}(\mathbf{t}_0)+\sum_{j=1}^{m}\Delta_j\end{aligned} \tag{24}$$

where $\Psi_j = \sum_{z\in\mathcal{Z}}(\alpha_z^* - [\ln\kappa_z/\tau_{az}])T^z(\mathbf{t}_j^1, \mathbf{t}_{j+1}) - \sum_{z\in\mathcal{Z}}\mathcal{N}_0^z\ln\kappa_z - \ln(1/\underline{\lambda}_a) - \beta_z^*(\mathbf{t}_j^1 - \mathbf{t}_j)$, $\Delta_j = M\int_{\mathbf{t}_j^1}^{\mathbf{t}_{j+1}}\exp\{\sum_{z\in\mathcal{Z}}\mathcal{N}_0^p\ln\kappa_z - \sum_{z\in\mathcal{Z}}(\alpha_z^* - [\ln\kappa_z/\tau_{az}])T^z(\tau,\mathbf{t})\}d\tau$, and $\Psi_0 = \sum_{z\in\mathcal{Z}}(\alpha_z^* - [\ln\kappa_z/\tau_{az}])\ T^z(\mathbf{t}_0^1, \mathbf{t}_1) - \sum_{z\in\mathcal{Z}}\mathcal{N}_0^p\ln\kappa_z - \ln(1/\underline{\lambda}_a)$. In addition, we know that there exists a non-negative constant $\bar{m}$ at any $t \ge 0$ such that $\mathbf{t}_{\bar{m}} \le t \le \mathbf{t}_{\bar{m}+1}$. Denote $\varsigma^* = \max_{m\in\mathbb{N}}(\mathbf{t}_{m+1} - \mathbf{t}_m)$, $\Psi^* = \min_{j\in\mathbb{N}}(\Psi_j)$, and $\Delta^* = \max_{j\in\mathbb{N}}(\Delta_j)$, substituting (11a)-(11b) results in $V_{\sigma(\mathbf{t}_{\bar{m}})}(t) \le \mu e^{-\eta(\mathbf{t}-\mathbf{t}_0)}V_{\sigma(\mathbf{t}_0)}(\mathbf{t}_0) + \bar{m}\Delta^*$ with $\mu = \exp\{\beta_z^*\varsigma^* + \Psi^*\}$, $\eta = (\Psi^*/\varsigma^*)$. According to the definition of MLFs candidate in (13), it is shown that there exists a scalar $\bar{a} > 0$ such that $0 < \bar{a}\|\delta\| < V_{\sigma(t)}(t)$, thus, it implies

$$0 \le \|\delta(t)\| \le \frac{\mu}{\bar{a}}e^{-\eta(t-\mathbf{t}_0)}V_{\sigma(t_0)}(t_0) + \bar{m}\Delta^* \tag{25}$$

which means that all signals of the closed-loop cooperative error system (9) are UUB as $t \to \infty$. Furthermore, we know that $\|\delta(t)\|^2 \le (\bar{\lambda}_b/\underline{\lambda}_a)\mu e^{-\eta(t-\mathbf{t}_0)}\|\delta(\mathbf{t}_0)\|^2 + \bar{m}\Delta^*$. By letting $\mu^* = (\bar{\lambda}_b/\underline{\lambda}_a)\mu$, the error signals $\delta(t) = [\xi^{\mathrm{T}}(t), \tilde{\nu}^{\mathrm{T}}(t)]^{\mathrm{T}}$ enter the set $\|\delta(t)\| < \delta_0$ within the time interval $[\mathbf{t}_0, \mathbf{t}_0 + (1/\eta)\ln([\mu^*\|\delta(t_0)\|^2]/[\delta_0^2 - \bar{m}\Delta^*])]$. By letting $\delta_1 = \max\{\delta_0, \sqrt{(\bar{\lambda}_b/\underline{\lambda}_a)}\delta_0^2\}$, for all $\delta(t_0) \in \mathbb{R}^{2nN}$, it concludes the cooperative error $\delta(t)$ eventually converges to the set $\delta^* = \{\delta(t)|\|\delta(t)\| < \delta_1\}$ for all $t \ge \mathbf{t}_0 + T$ with $T = \mathbf{t}_0 + (1/\eta)\ln([\mu^*\|\delta(t_0)\|^2]/[\delta_0^2 - \bar{m}\Delta^*])$ that is, both signals $\tilde{x}_i(t) - \tilde{\nu}_i(t)$ and $\tilde{\nu}_i(t)$ converge to a compact set δ^*. The proof is completed. ■

Remark 3: Compared with the previous works [32]–[38], the main advantages of this article lie in three-fold: 1) the assumption of the intermittent DoS attacks break out switching communication network is considered, which is usually realistic in a practical scenario; 2) by constructing the local state estimators and distributed controllers for each subsystem via neighborhood information, an output-feedback-based secure control algorithm is established to achieve a cooperative secure synchronization objective; and 3) by using the topology-dependent Lyapunov function analysis method, the convergence of the closed-loop error systems is proved in the presence of intermittent DoS attacks.

Remark 4: It is worth noting that the designed parameters can be divided into three parts according to the proposed control scheme. First, α^* is chosen to guarantee the feasibility of LMI (10). Second, α^z and κ_z are selected based on the connectivity property of all possible switching topology graphs, while β^*, β_z^*, α^z and κ_z given in (11) are used to guaranteed the total communication time without DoSs is larger than a threshold quantity. Finally, θ and π are selected to improve the convergence performances of the closed-loop tracking error system.

Remark 5: Indeed, the proposed theoretical results cannot be used directly to solve the specific challenges coming from the inherent nonlinearity of distributed CPSs. However, the main idea and theoretical analysis method under this framework combining with a nonlinear control technique, such as adaptive neural network algorithms [40]–[42] and fuzzy control approaches [43]–[46], can be able to handle the nonlinear CPSs subject to unreliable communications and DoSs, that is, an interesting issue for further investigation.

IV. Simulation Example

Example 1: In the first example, we will verify the effectiveness of the proposed cooperative secure control approach for a group of multiple vehicle systems, which includes one

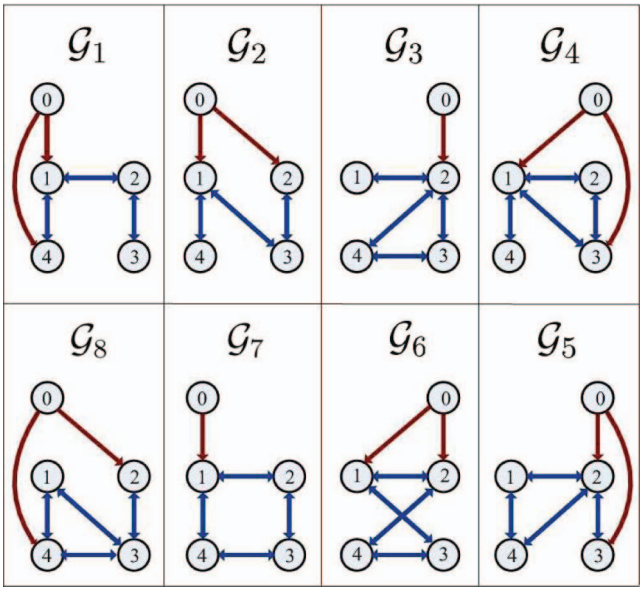


Fig. 2. Switching topology graphs.

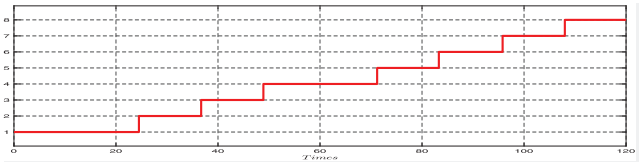


Fig. 3. Topology switching signal of Example 1.

leader and four follower vehicles. Inspired by the technical literature [11], the longitudinal dynamics of the ith vehicle subsystem can be approximated as follows:

$$\begin{aligned}\dot{\mathbf{p}}_i(t) &= \mathbf{v}_i(t)\\ \dot{\mathbf{v}}_i(t) &= \mathbf{a}_i(t)\\ \dot{\mathbf{a}}_i(t) &= -\frac{1}{\Gamma}\mathbf{a}_i(t) + \frac{1}{\Gamma}\mathbf{u}_i(t), \quad i = 0, 1, \ldots, 4 \end{aligned} \tag{26}$$

where $\mathbf{p}_i(t)$, $\mathbf{v}_i(t)$, $\mathbf{a}_i(t)$, and $\mathbf{u}_i(t)$ represent the absolute vehicle position, velocity, acceleration, and control input, respectively, and Γ is the power-train time constant. Suppose that the vehicles team are distributed on a time-varying communication network, and all possible interconnected topologies $\mathbf{G} = \{\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \mathcal{G}_4, \mathcal{G}_5, \mathcal{G}_6, \mathcal{G}_7, \mathcal{G}_8\}$ are presented in Fig. 2. In view of the topology allocation strategy introduced in the preliminaries, we can propose that

$$\begin{aligned} S(\mathcal{G}_1) = S(\mathcal{G}_3) &= S(\mathcal{G}_8) = \{0.1392, 1.7459, 3, 4.1149\}\\ S(\mathcal{G}_2) &= S(\mathcal{G}_4) = \{0.1729, 0.6617, 2.2091, 3.9563\}\\ S(\mathcal{G}_5) &= S(\mathcal{G}_7) = \{0.4094, 2.4927, 4.2075, 4.8904\}\\ S(\mathcal{G}_6) &= \{0.2598, 1.8564, 2, 0.4512\}. \end{aligned}$$

So, a topology partition set of $\mathbf{G}$ can be divided as

$$\mathbf{G} = Q_1 \bigcup Q_2 \bigcup Q_3 \bigcup Q_4$$

where $Q_1 = \{\mathcal{G}_1, \mathcal{G}_3, \mathcal{G}_8\}$, $Q_2 = \{\mathcal{G}_2, \mathcal{G}_4\}$, $Q_3 = \{\mathcal{G}_5, \mathcal{G}_7\}$, and $Q_4 = \{\mathcal{G}_6\}$. The switching rule of the network communication topology is $\mathcal{G}_1 \to \mathcal{G}_2 \to \cdots \to \mathcal{G}_8 \to \mathcal{G}_1 \to \cdots$. Also, Fig. 3 shows the topology switching signal in this simulation.

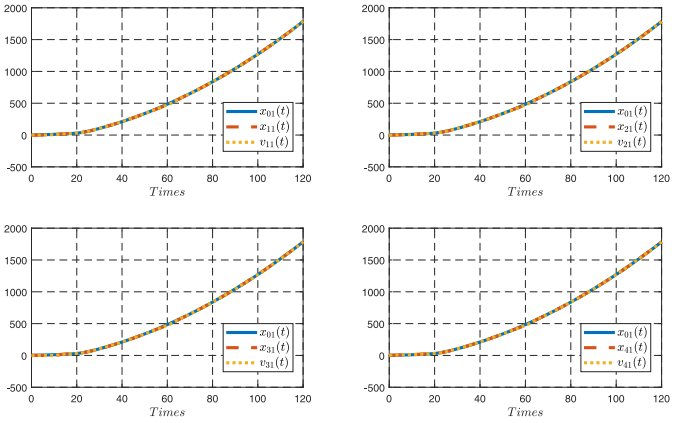


Fig. 4. Profiles of the first state and estimate trajectories for vehicle i, $i = 0, 1, \ldots, 4$.

Let $\mathbf{x}_i(t) = [\mathbf{p}_i(t)\ \mathbf{v}_i(t)\ \mathbf{a}_i(t)]^{\mathrm{T}}$, then, the state-space model for the ith vehicle dynamics can be described by (1)–(2), where the matrix parameters are described as

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\Gamma} \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\Gamma} \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}.$$

In order to demonstrate the effectiveness of the secure control design algorithm presented in this study, we assume there are three intermediate DoS attacks occurring in connected multiple vehicle network, that is, $t \in [0\ \text{s}, 10\ \text{s}) \cup [48.9\ \text{s}, 60.9\ \text{s})$. Meanwhile, let the vehicle parameter $\Gamma = 0.4$, and the input signal of leader vehicle be

$$\mathbf{u}_0(t) = \begin{cases} 0.1, & 0\ \text{s} \le t < 8\ \text{s} \\ \sin 0.1t, & 8\ \text{s} \le t < 18\ \text{s} \\ 0.2, & t \ge 18\ \text{s}. \end{cases}$$

Moreover, the initial conditions are $x_0(0) = [2, 1, -1.5]^{\mathrm{T}}$, $x_1(0) = [-5, 1.8, -2]^{\mathrm{T}}$, $x_2(0) = [-2, 0.5, 1]^{\mathrm{T}}$, $x_3(0) = [2, -1, 1.5]^{\mathrm{T}}$, $x_4(0) = [0.5, 1.5, -0.5]^{\mathrm{T}}$, $\nu_0(0) = [2, -0.7, 1.4]^{\mathrm{T}}$, $\nu_1(0) = [5, -8, 2]^{\mathrm{T}}$, $\nu_2(0) = [-4, 3, 6]^{\mathrm{T}}$, $\nu_3(0) = [-6, -3, -2]^{\mathrm{T}}$, and $\nu_4(0) = [6, 8, 4]^{\mathrm{T}}$. By selecting $\theta = 10$, $\pi = 1$, $\alpha^* = 0.9$ and $\beta^* = 47.5$, and solving LMIs (10a) and (10b) in Theorem 1, the feedback gain matrices are obtained:

$$L = \begin{bmatrix} -0.7287 \\ -0.9259 \\ -0.1944 \end{bmatrix} \text{ and } K = \begin{bmatrix} -1.9112 & -4.0803 & -1.6360 \end{bmatrix}.$$

It is easy to verify that the criteria (11) in Theorem 1 are satisfied under the above constant. In the simulations results, the time responses of states and estimates of five vehicles are shown in Figs. 4-6, from which it can be observed that the states and estimates of each follower vehicle can track leader's trajectories under intermittent DoS attacks. As a result, the simulation example illustrates the efficiency of the proposed output-feedback secure control strategy.

Example 2: Consider the model of a term of F-18 aircrafts with four follower subsystems and one reference leader (Node 0) [31]. Suppose that the underlying communication topology and switching signal are given in Figs. 2 and 7. What's more, the system parameters of each aircraft model are given as $A = \begin{bmatrix} -1.175 & 0.9871 \\ -8.458 & -0.8776 \end{bmatrix}$, $B = \begin{bmatrix} -0.194 & -0.03593 \\ -19.29 & -3.803 \end{bmatrix}$,

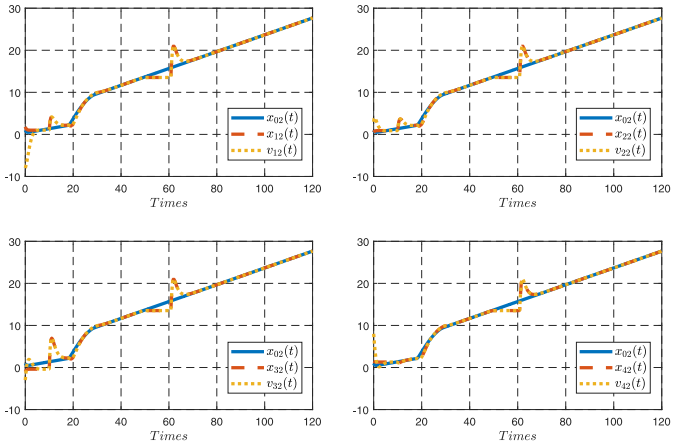


Fig. 5. Profiles of the second state and estimate trajectories for vehicle i, $i = 0, 1, \ldots, 4$.

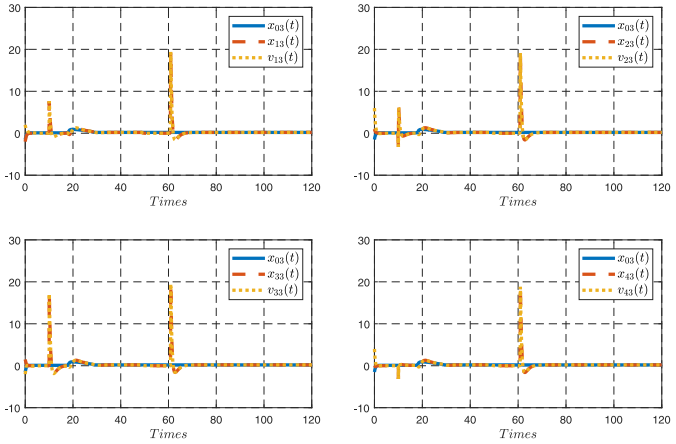


Fig. 6. Profiles of the third state and estimate trajectories for vehicle i, $i = 0, 1, \ldots, 4$.

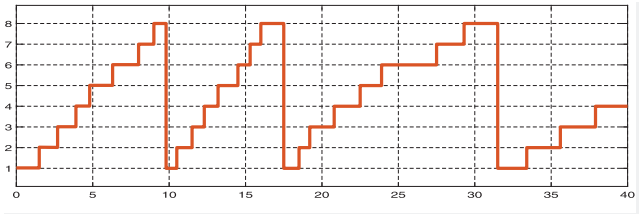


Fig. 7. Topology switching signal of Example 2.

and $C = \begin{bmatrix} 1 & 0 \end{bmatrix}$. Here, we assume that the leader's input signal is given by $u_0(t) = [1, 4]^{\mathrm{T}}$ for 0 s $< t <$ 8 s; $u_0(t) = [\sin(0.5t), \cos(0.5t)]^{\mathrm{T}}$ for 8 s $< t <$ 18 s, and $u_0(t) = [-2, -3]^{\mathrm{T}}$ for $t >$ 18 s In addition, the initial conditions are $x_0(0) = [5, -5]^{\mathrm{T}}$, $x_1(0) = [-1, -2.8]^{\mathrm{T}}$, $x_2(0) = [-4, 1.8]^{\mathrm{T}}$, $x_3(0) = [0, 0]^{\mathrm{T}}$, $x_4(0) = [5, -1.8]^{\mathrm{T}}$, $v_0(0) = [2, -0.7]^{\mathrm{T}}$, $v_1(0) = [5, -8]^{\mathrm{T}}$, $v_2(0) = [-4, 3]^{\mathrm{T}}$, $v_3(0) = [-6, -3]^{\mathrm{T}}$, $v_4(0) = [6, 8]^{\mathrm{T}}$, $\theta = 4, \pi = 1, \alpha^* = 1$ and $\beta^* = 8.2$. This example considers three intermediate DoS attacks, in other words, systems face DoS attacks when $t \in [0\text{ s}, 1.2\text{ s}) \cup [10.5\text{ s}, 11.2\text{ s}) \cup [23.9, 26.2)$. By solving the LMI (10) given in Theorem 1, we obtain the following feedback gain matrices K and L in the cooperative secure

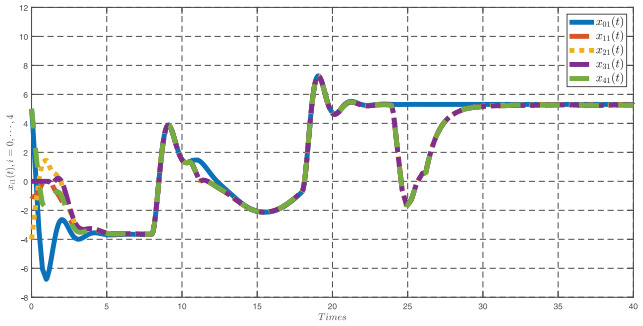


Fig. 8. Profiles of state trajectories $x_{i1}(t)$, $i = 0, 1, \ldots, 4$.

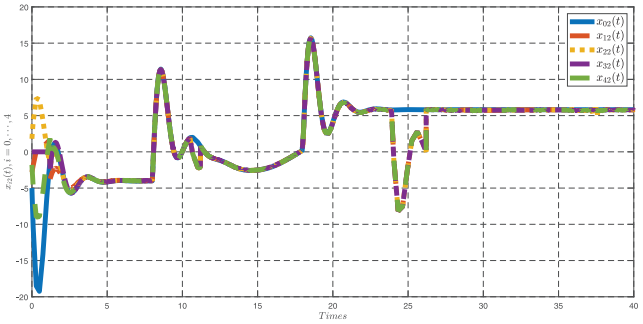


Fig. 9. Profiles of state trajectories $x_{i2}(t)$, $i = 0, 1, \ldots, 4$.

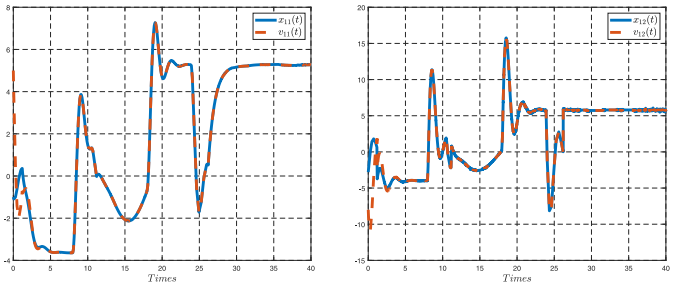


Fig. 10. Profiles of subsystem 1 states and estimates.

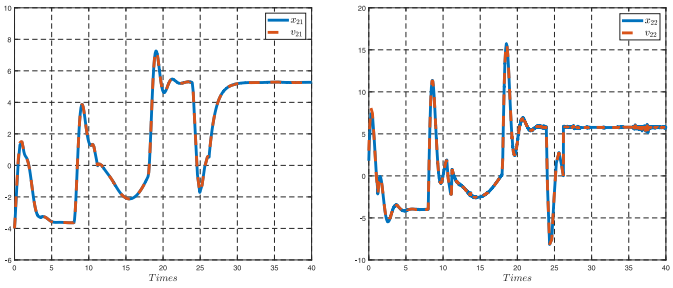


Fig. 11. Profiles of subsystem 2 states and estimates.

controller (5)

$$L = \begin{bmatrix} -0.7170 \\ 0.7890 \end{bmatrix}, \quad K = \begin{bmatrix} 0.1788 & 17.782 \\ 0.0331 & 3.5058 \end{bmatrix}.$$

Thus, based on Theorem 1 by choosing the relevant parameters ($\theta = 4, \pi = 1, \alpha^* = 1$, and $\beta^* = 8.2$), we can verify that the criteria (11) in Theorem 1 are satisfied, under which the cooperative consensus is achieved. Consequently, Figs. 8 and 9 show the trajectories of one leader and four subsystems

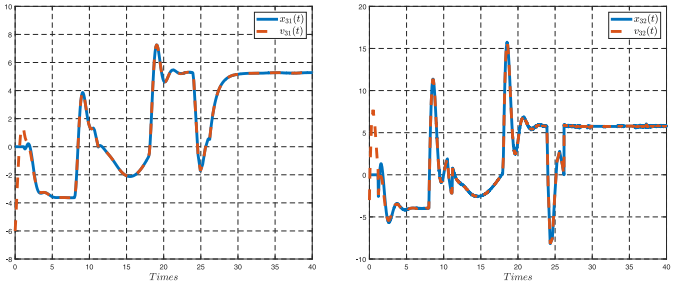


Fig. 12. Profiles of subsystem 3 states and estimates.

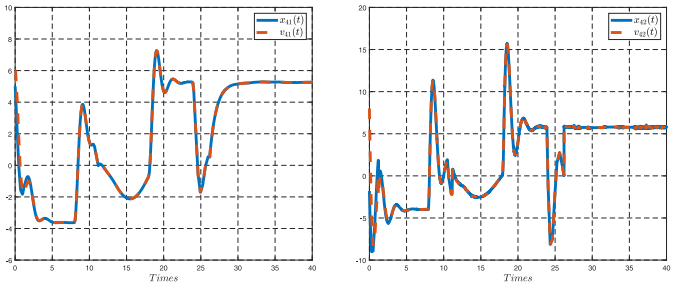


Fig. 13. Profiles of subsystem 4 states and estimates.

states, and Figs. 10– 13 show the state and estimate trajectories of subsystems. Compounded with Figs. 10– 13, all these figures validate the applicability of the proposed secure control strategy for a switching communication network, even in the presence of intermittent DoS attacks. It is obvious to conclude that the secure control problem for DCPSs could be solved by applying the control scheme (5), which also proves the feasibility of Theorem 1.

V. Conclusion

In this article, the problem of cooperative output secure tracking control for a class of CPSs is studied under switching communication network. Its main advantage is that an output-feedback-based secure control algorithm subject to unreliable communication with intermittent DoS attacks is developed. Compared with the existing works, the resulting distributed output-feedback-based secure control algorithm can guarantee that, in the presence of intermittent DoS attacks under switching communication channels, the estimator errors and cooperative errors can converge into a compact set. Note that the designed secure control approach is not able to deal with nonlinear CPSs under various cyber-attacks. Therefore, in our future work, it is to be the further consideration for secure control problem of nonlinear CPSs. Moreover, the proposed methodology will be applied to distributed reliable control for distributed microgrids, cooperative mobile manipulators, and multiple vehicular platoons.

References

[1] P. Antsaklis, "Goals and challenges in cyber-physical systems research editorial of the editor in chief," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3117–3119, Dec. 2014.

[2] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, "A survey on model-based distributed control and filtering for industrial cyber-physical systems," *IEEE Trans. Ind. Inf.*, vol. 15, no. 5, pp. 2483–2499, May 2019.

[3] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[4] C. L. P. Chen and Y.-H. Pao, "An integration of neural network and rule-based systems for design and planning of mechanical assemblies," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 23, no. 5, pp. 1359–1371, Sep./Oct. 1993.

[5] M. Gan, C. L. P. Chen, G.-Y. Chen, and L. Chen, "On some separated algorithms for separable nonlinear least squares problems," *IEEE Trans. Cybern.*, vol. 48, no. 10, pp. 2866–2874, Oct. 2018.

[6] Y. Xiao, C. L. P. Chen, and B. Wang, "Bandwidth degradation QoS provisioning for adaptive multimedia in wireless/mobile networks," *Comput. Commun.*, vol. 25, no. 13, pp. 1153–1161, 2002.

[7] J. Qin, Q. Ma, Y. Shi, and L. Wang, "Recent advances in consensus of multi-agent systems: A brief survey," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 4972–4983, Jun. 2017.

[8] H. J. Ma, G.-H. Yang, and T. W. Chen, "Event-triggered optimal dynamic formation of heterogeneous affine nonlinear multi-agent systems," *IEEE Trans. Autom. Control*, early access, Mar. 27, 2020, doi: 10.1109/TAC.2020.2983108.

[9] C. Deng, W. Che, and Z. G. Wu, "A dynamic periodic event-triggered approach to consensus of heterogeneous linear multiagent systems with time-varying communication delays," *IEEE Trans. Cybern.*, early access, Sep. 29, 2020, doi: 10.1109/TCYB.2020.3015746.

[10] X. Jin, S. Lü, C. Deng, and M. Chadli, "Distributed adaptive security consensus control for a class of multi-agent systems under network decay and intermittent attacks," *Inf. Sci.*, vol. 547, pp. 88–102, Aug. 2020.

[11] S. E. Li, X. Qin, Y. Zheng, J. Wang, K. Li, and H. Zhang, "Distributed platoon control under topologies with complex Eigenvalues: Stability analysis and controller synthesis," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 1, pp. 206–220, Jan. 2019.

[12] G. Wen, X. Yu, Z. W. Liu, and W. Yu, "Adaptive consensus-based robust strategy for economic dispatch of smart grids subject to communication uncertainties," *IEEE Trans. Ind. Inf.*, vol. 14, no. 6, pp. 2484–2496, Jun. 2018.

[13] T. Li, R. Zhao, C. L. P. Chen, L. Fang, and C. Liu, "Finite-time formation control of under-actuated ships using nonlinear sliding mode control," *IEEE Trans. Cybern.*, vol. 48, no. 11, pp. 3243–3253, Nov. 2018.

[14] A. Marino, "Distributed adaptive control of networked cooperative mobile manipulators," *IEEE Trans. Control Syst. Technol.*, vol. 26, no. 5, pp. 1646–1660, Sep. 2018.

[15] B. Wei, F. Xiao, and Y. Shi, "Fully distributed synchronization of dynamic networked systems with adaptive nonlinear couplings," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 2926–2934, Jul. 2020.

[16] J. Qin, Q. Ma, X. Yu, and L. Wang, "On synchronization of dynamical systems over directed switching topologies: An algebraic and geometric perspective," *IEEE Trans. Autom. Control*, early access, Feb. 8, 2020, doi: 10.1109/TAC.2020.2971980.

[17] B. Mu and Y. Shi, "Distributed LQR consensus control for heterogeneous multiagent systems: Theory and experiments," *IEEE/ASME Trans. Mechatron.*, vol. 23, no. 1, pp. 434–443, Feb. 2018.

[18] C. Deng, W.-W. Che, and P. Shi, "Cooperative fault-tolerant output regulation for multiagent systems by distributed learning control approach," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 11, pp. 4831–4841, Nov. 2020, doi: 10.1109/TNNLS.2019.2958151.

[19] C. X. Liu, H. P. Li, Y. Shi, and D. M. Xu, "Distributed event-triggered gradient method for constrained convex minimization," *IEEE Trans. Autom. Control*, vol. 65, no. 2, pp. 778–785, Feb. 2020.

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

[21] J.-W. Zhu, C.-Y. Gu, S. X. Ding, W.-A. Zhang, X. Wang, and L. Yu, "A new observer based cooperative fault-tolerant tracking control method with application to networked multi-axis motion control system," *IEEE Trans. Ind. Electron.*, early access, Jun. 17, 2020, doi: 10.1109/TIE.2020.3001857.

[22] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2nd Quart., 2010.

[23] X. Wang and G.-H. Yang, "Fault-tolerant consensus tracking control for linear multi-agent systems under switching directed network," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1921–1930, May 2020.

[24] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.

[25] A.-Y. Lu and G.-H. Yang, "Observer-based control for cyber-physical systems under denial-of-service with a decentralized event-triggered scheme," *IEEE Trans. Cybern.*, early access, Oct. 21, 2019, doi: 10.1109/TCYB.2019.2944956.
[26] L. Tang, D. Ma, and J. Zhao, "Adaptive neural control for switched non-linear systems with multiple tracking error constraints," *IET Signal Process.*, vol. 13, no. 3, pp. 330–337, May 2019.
[27] S. Deshmukh, B. Natarajan, and A. Pahwa, "State estimation over a lossy network in spatially distributed cyber-physical systems," *IEEE Trans. Signal Process.*, vol. 62, no. 15, pp. 3911–3923, Aug. 2014.
[28] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.
[29] G. Wen, W. Yu, X. Yu, and J. Lü, "Complex cyber-physical networks: From cybersecurity to security control," *J. Syst. Sci. Complexity*, vol. 30, no. 1, pp. 46–67, 2017.
[30] H.-J. Ma and G.-H. Yang, "Adaptive fault tolerant control of cooperative heterogeneous systems with actuator faults and unreliable interconnections," *IEEE Trans. Autom. Control*, vol. 61, no. 11, pp. 3240–3255, Nov. 2016.
[31] X. Wang and G.-H. Yang, "Adaptive reliable coordination control for linear agent networks with intermittent communication constraints," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1120–1131, Sep. 2018.
[32] T.-Y. Zhang and D. Ye, "Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 3094–3103, Jul. 2020.
[33] Z. Feng, G. Wen, and G. Hu, "Distributed secure coordinated control for multiagent systems under strategic attacks," *IEEE Trans. Cyber.*, vol. 47, no. 5, pp. 1273–1284, May 2017.
[34] W. Xu, D. W. Ho, J. Zhong, and B. Chen, "Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 10, pp. 3137–3149, Oct. 2019.
[35] Z. Feng and G. 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.
[36] 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.
[37] A.-Y. Lu and G.-H. Yang, "Distributed consensus control for multi-agent systems under denial-of-service," *Inf. Sci.*, vols. 439–440, pp. 95–107, May 2018.
[38] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.
[39] X. Wang and G. H. Yang, "Distributed reliable $\mathcal{H}_\infty$ consensus control for a class of multi-agent systems under switching networks: A topology-based average dwell time approach," *Int. J. Robust Nonlinear Control*, vol. 26, no. 13, pp. 2767–2787, 2016.
[40] T. Gao, Y. J. Liu, L. Liu, and D. Li, "Adaptive neural network-based control for a class of nonlinear pure-feedback systems with time-varying full state constraints," *IEEE/CAA J. Autom. Sinica*, vol. 5, no. 5, pp. 923–933, Sep. 2018.
[41] L.-B. Wu and J. H. Park, "Adaptive fault-tolerant control of uncertain switched nonaffine nonlinear systems with actuator faults and time delays," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 9, pp. 3470–3480, Sep. 2020.
[42] L. Liu, T. Gao, Y.-J. Liu, and S. C. Tong, "Time-varying asymmetrical BLFs based adaptive finite-time neural control of nonlinear systems with full state constraints," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1335–1343. Sep. 2020.
[43] L. Liu, Y. J. Liu, S. C. Tong, and C. L. P. Chen, "Integral barrier Lyapunov function-based adaptive control for switched nonlinear systems," *Sci. China Inf. Sci.*, vol. 63, no. 3, pp. 1–14, Mar. 2020.
[44] L. B. Wu, J. H. Park, and N.-N. Zhao, "Robust adaptive fault-tolerant tracking control for nonaffine stochastic nonlinear systems with full-state constraints," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3793–3805, Aug. 2020.
[45] W. B. Xie, B. Liu, L. Bu, Y. Wang, and J. Zhang, "A decoupling approach for observer-based controller design of T–S fuzzy system with unknown premise variables," *IEEE Trans. Fuzzy Syst.*, early access, Jul. 2, 2020, doi: 10.1109/TFUZZ.2020.3006572.
[46] L. Liu, Y.-J. Liu, D. P. Li, S. C. Tong, and Z. S. Wang, "Barrier Lyapunov function-based adaptive fuzzy FTC for switched systems and its applications to resistance–inductance–capacitance circuit system," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3491–3502, Aug. 2020.

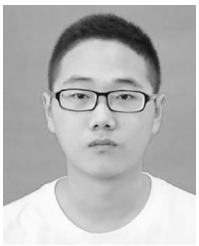
Xin Wang (Member, IEEE) received the B.S. degree in information and computing science and the M.S. degree in operational research and cybernetics from Heilongjiang University, Harbin, China, in 2008 and 2011, respectively, and the Ph.D. degree in navigation guidance and control from Northeastern University, Shenyang, China, in 2016.

He is currently an Associate Professor with the School of Mathematical Science, Heilongjiang University. From 2019 to 2020, he was a Postdoctoral Fellow with Yeungnam University, Gyeongsan, South Korea. From 2017 to 2018, he was a Visiting Professor with the Department of Mechanical Engineering, University of Victoria, Victoria, BC, Canada. His research interests include fault diagnosis, fault-tolerant control, multiagent coordination, and cyber-physical 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 (POSTECH), Pohang, South Korea, in 1997.

From 1997 to 2000, he was a Research Associate with the Engineering Research Center and Automation Research Center, POSTECH. He joined Yeungnam University, Kyongsan, South Korea, in 2000, where he is currently the Chuma Chair Professor. He has coauthored the monographs *Recent Advances in Control and Filtering of Dynamic Systems With Constrained Signals* (New York, NY, USA: Springer-Nature, 2018) and *Dynamic Systems With Time Delays: Stability and Control* (New York, NY, USA: Springer-Nature, 2019). His research interests include robust control and filtering, neural/complex networks, fuzzy systems, multiagent systems, and chaotic systems. He has published a number of articles in the above areas.

Prof. Park has been a recipient of the Highly Cited Researchers Award by Clarivate Analytics (formerly, Thomson Reuters) since 2015 and listed in three fields: Engineering, Computer Sciences, and Mathematics, in 2019. He is an Editor of an edited volume *Recent Advances in Control Problems of Dynamical Systems and Networks* (New York, NY, USA: Springer-Nature, 2020). He also serves as an Editor for the *International Journal of Control, Automation and Systems*. He is also a Subject Editor/Advisory Editor/Associate Editor/Editorial Board Member of several international journals, including *IET Control Theory and Applications*, *Applied Mathematics and Computation*, *Journal of The Franklin Institute*, *Nonlinear Dynamics*, *Engineering Reports*, *Cogent Engineering*, the IEEE TRANSACTIONS ON FUZZY SYSTEMS, the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, and the IEEE TRANSACTIONS ON CYBERNETICS. He is a Fellow of the Korean Academy of Science and Technology.



Heng Liu was born in Heilongjiang, China, in 1994. He received the B.S. degree from the School of Science, Qiqihar University, Qiqihar, China, in 2017, and the M.S. degree in mathematics from Heilongjiang University, Harbin, China, in 2020. He is currently pursuing the Ph.D. degree with the Harbin Institute of Technology, Harbin.

His research interests include adaptive control, fault-tolerant control, and multiagent coordination.

Xian Zhang (Senior Member, IEEE) received the Ph.D. degree in control theory from the Queen's University of Belfast, Belfast, U.K., in 2004.

Since 2004, he has been with Heilongjiang University, Harbin, China, where he is currently a Professor with the School of Mathematical Science. He has authored more than 100 research papers. His current research interests include neural networks, genetic regulatory networks, mathematical biology, and stability analysis of delayed dynamic systems.

Prof. Zhang has received the Second Class of Science and Technology Awards of Heilongjiang Province in 2005 and the Three Class of Science and Technology Awards of Heilongjiang Province in 2015. He is a Vice President of the Mathematical Society of Heilongjiang Province. Since 2006, he has been serving as an Editor for the *Journal of Natural Science of Heilongjiang University.*