Secure Synchronization Control for a Class of Cyber-Physical Systems With Unknown Dynamics

Ning Wang and Xiaojian Li, *Member, IEEE*

***Abstract*—This paper investigates the secure synchronization control problem for a class of cyber-physical systems (CPSs) with unknown system matrices and intermittent denial-of-service (DoS) attacks. For the attack free case, an optimal control law consisting of a feedback control and a compensated feedforward control is proposed to achieve the synchronization, and the feedback control gain matrix is learned by iteratively solving an algebraic Riccati equation (ARE). For considering the attack cases, it is difficult to perform the stability analysis of the synchronization errors by using the existing Lyapunov function method due to the presence of unknown system matrices. In order to overcome this difficulty, a matrix polynomial replacement method is given and it is shown that, the proposed optimal control law can still guarantee the asymptotical convergence of synchronization errors if two inequality conditions related with the DoS attacks hold. Finally, two examples are given to illustrate the effectiveness of the proposed approaches.**

***Index Terms*—Algebraic Riccati equation (ARE), complex dynamical networks (CDNs), denial-of-service (DoS), secure control.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) combine physical processes, computational resources, with communication capability [1], which have been studied intensively for their various fields of applications, such as power grid systems in [2], multi-agent systems in [3]–[6] and smart networked systems in [7], [8]. However, CPSs embedded networked control technique are more vulnerable on account of cyber attacks. Therefore, the security of CPSs has recently attracted extensive concern in control field, such as secure state estimation under sparse attacks in [9], [10], secure control and distributed filtering under deception attacks in [11], [12], the resilient control for systems under replay attacks in [13] and the effects of denial-of-service (DoS) attacks on systems in [14]–[19].

DoS attacks, a kind of common attacks in CPSs, attempt to render some or all components of a control system inaccessible by preventing the information transmission. Some existing studies referred to DoS attacks have been published. For example, the stability analysis for a networked system in the presence of DoS attacks, which is on assumptions about the limited DoS attacks frequency and duration, is given in [14]. In [15]–[19], some resilient control methods for CPSs under DoS attacks, which is used to maximize frequency and duration of DoS attacks under the condition that the close-loop stability is not destroyed [15], are introduced. In order to improve the resilience ability of a system under DoS attacks, the state estimation problem is proposed in [20]–[22]. While, the above results are all for a single system.

Recently, based on the studies for a single system, the secure synchronization problem of complex networked systems, which results from that the synchronization behavior relying on the information of other nodes will be affected when DoS attacks successfully break down the information transmission channels, has triggered considerable attentions [23]–[26]. For example, for complex dynamical networks (CDNs) under recoverable attacks destroying the network topology, the authors in [24] introduced the attack frequency and the average recovering time to study the secure synchronization problem. In the presence of DoS attacks interrupting the communication channels of each agent in [25], [26], some sufficient conditions about achieving secure consensus of multi-agent systems are derived by using the Lyapunov function approach. However, it should be pointed that the exact system dynamic matrices are required to be known to analyze the stability of a networked system in [14]–[22] or to solve the secure synchronization control problem in [23]–[26].

In fact, in the absence of DoS attacks, the synchronization problem for the complex networked systems with unknown dynamics has been investigated. To solve optimal synchronization problems of multi-agent systems, a Q-learning method and a model-free off-policy reinforcement learning approach are developed in [27], [28], respectively.

Manuscript received January 6, 2020; accepted February 21, 2020. This work was supported in part by the National Natural Science Foundation of China (61873050), the Fundamental Research Funds for the Central Universities (N180405022, N2004010), the Research Fund of State Key Laboratory of Synthetical Automation for Process Industries (2018ZCX14), and Liaoning Revitalization Talents Program (XLYC1907088). Recommended by Associate Editor Giuseppe Franzè. *(Corresponding author: Xiaojian Li.)*

Citation: N. Wang and X. J. Li, "Secure synchronization control for a class of cyber-physical systems with unknown dynamics," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1215–1224, Sept. 2020.

N. Wang is with the College of Information Science and Engineering, Northeastern University, Shenyang 110819, China (e-mail: 1910320@stu.neu.edu.cn).

X. J. Li is with the State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, and with the Key Laboratory of Vibration and Control of Aero-Propulsion System, Ministry of Education, Northeastern University, and also with the College of Information Science and Engineering, Northeastern University, Shenyang 110819, China (e-mail: lixiaojian@ise.neu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2020.1003192

Besides, for CDNs of which the couplings are involved in node dynamic equations, the optimal synchronization control problem has been explored in our previous works [29], [30]. Nevertheless, the above results [27]–[30] about the complex networked systems with unknown dynamics were all based on the assumption that the networks were attack free. For the case that the CDNs are with unknown dynamics, how to design the secure synchronization control strategy and further to characterize the frequency and duration of DoS attacks under which the stability of synchronization errors is not destroyed, are challenging. Therefore, it is highly desired to study those problems, which motivates the current research.

In this paper, the secure synchronization control problem is considered for a class of CDNs with unknown dynamics in the presence of intermittent DoS attacks. The main contributions of this paper are summarized as follows.

1) For the attack cases, the stability analysis of synchronization errors cannot be directly carried out by using the existing Lyapunov function approach due to the presence of unknown system matrices. To overcome this difficulty, a matrix polynomial replacement method is proposed in the paper. More specifically, the unknown system matrices involved in the Lyapunov function are replaced with the known control gain matrices derived by iteratively solving an algebraic Riccati equation (ARE). And based on the replacement method, the decay rates about sleeping and active intervals of DoS attacks are further computed by solving a set of linear matrix inequalities.

2) According to the obtained decay rates and using the switching technique, the upper bounds of the frequency and duration of DoS attacks, under which the CDNs with unknown dynamics achieve secure synchronization, are given in terms of inequalities.

This paper is organized as follows. In Section II, some necessary concepts about the graph theory and the attack model are presented. An optimal synchronization control protocol is proposed in Section III. Stability analysis of secure synchronization is given in Section IV. In Section V, two examples of the CDNs are provided. Conclusion is given in Section VI.

Notations: In this paper, $\|\cdot\|$ is used to represent the Euclidean norm for vectors or matrices. For a matrix P, define P^T as its transpose and $He(P)=P+P^T$. For a symmetric matrix P, $P>0$ means that P is a positive definite matrix. Besides, given a real symmetric matrix P, $\lambda_{\min}(P)$ and $\lambda_{\max}(P)$ denote the smallest eigenvalue and the largest eigenvalue of P, respectively. $P=[p_{ij}]_{n\times n}$ denotes a matrix $P\in\mathbb{R}^{n\times n}$ with the ith row and jth column being p_{ij}. Define $vec(A)$ as an mn-vector for $A\in\mathbb{R}^{m\times n}$, i.e., $vec(A)=[\alpha_1^T,\alpha_2^T,\ldots,\alpha_n^T]$, where $\alpha_i\in\mathbb{R}^n$ is the ith column of A. Assume two sets W and N and $W\backslash N$ means that the elements belong to W, but not to N. Finally, let $\otimes$ represent the Kronecker product.

II. Preliminaries and Problem Formulation

A. Graph Theory

A directed graph (digraph) $\mathcal{G}=(V,E)$ contains a set $V=1,2,\ldots,N$ of vertices and a set $E=1,2,\ldots,M$ of arcs (i,j) leading from the initial vertex i to the terminal vertex j. Each arc $(i,j)\in E$ is associated with a real-valued weight with $l_{ij}>0$, while the ith node and the jth node have no connection with $l_{ij}=0$. Assumed that there is no self loop in the graph. Furthermore, define the Laplacian matrix of a digraph as

$$L=\begin{bmatrix} \sum\limits_{m\neq 1} l_{1m} & -l_{12} & \cdots & -l_{1N} \\ -l_{21} & \sum\limits_{m\neq 2} l_{2m} & \cdots & -l_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ -l_{N1} & -l_{N2} & \cdots & \sum\limits_{m\neq N} l_{Nm} \end{bmatrix}.$$

More detailed concepts on the digraph were shown in [31].

B. System Description

Consider the CDNs model with N linear nodes given as

$$\dot{x}_i(t)=Ax_i(t)+B_iu_i(t)+\sum_{j=1,j\neq i}^{N} l_{ij}\Gamma_i(x_j(t)-x_i(t)) \tag{1}$$

where $x_i\in\mathbb{R}^n$ and $u_i\in\mathbb{R}^m$ are the state and the controlled input, respectively. $A\in\mathbb{R}^{n\times n}$ is an unknown matrix and $B_i\in\mathbb{R}^{n\times n}$ is the constant invertible matrix. l_{ij} are known coupling weights, and $\Gamma_i\in\mathbb{R}^m$ is the known inner connecting matrix of the ith node.

Assume the dynamic equation of the leader has the following form

$$\dot{z}_0=Sz_0 \tag{2}$$

where $z_0\in\mathbb{R}^n$ is the leader's state. The leader can be regarded as a command generator, which generates the desired target trajectory.

Assumption 1: (A,B_i) is controllable.

C. Denial-of-Service Attack

In practice, the state information x_i measured by using sensors is sent to controllers via networked channels. As a kind of common attacks in CPSs, DoS attacks compromise certain or all transmission channels of a control system (see Fig. 1), which leads to the unavailability of transmitted information.

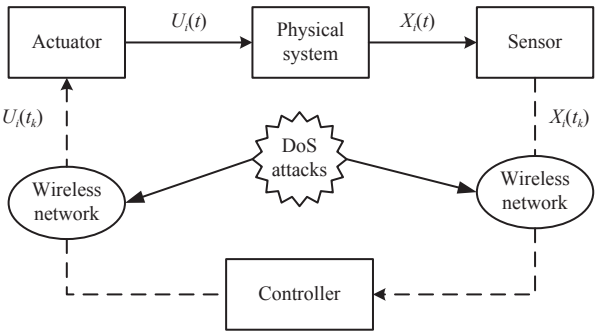

Fig. 1. Framework of the CDNs under DoS attacks.

Due to the energy constraint of adversaries [32], [33], DoS attacks need to terminate attack activities and shift to a sleep period to supply its energy for next attack. That is to say, one adversary launches DoS attacks discontinuously. As mentioned in [14] and [19], $\{z_s\}_{s\in\mathbb{N}^+}$ represents the time instant when the sth DoS attack is active. Then

$$T_s = [z_s, z_s + d_s) \tag{3}$$

means the time interval of the sth DoS attack with a length $d_s \in \mathbb{R}^+$. Thus, for given $t > \tau$, define that

$$\Xi(\tau, t) = \bigcup_{j \in \mathbb{N}} T_s \bigcap [\tau, t] \tag{4}$$

$$\Lambda(\tau, t) = [\tau, t] \backslash \Xi(\tau, t) \tag{5}$$

which denote, during each interval $[\tau, t]$, the sets of time instants when the communication is denied or allowed, respectively. Moreover, $|\Xi(\tau, t)|$ and $|\Lambda(\tau, t)|$ represent the total lengths of DoS attacks being active and sleeping during the interval $[\tau, t]$.

Further, let $\{t_k\}_{k \in \mathbb{R}_0}$ with $t_0 = 0$ represent the sequence of time instants at which communication is attempted. Define the finite sampling rate as

$$\Delta_k = t_{k+1} - t_k \tag{6}$$

for $k \in \mathbb{N}$. Thus, the state information received by controllers is considered as

$$x_i(t_k) = \begin{cases} 0, & t \in \Xi(0, +\infty) \\ x_i(t_k), & t \in \Lambda(0, +\infty) \end{cases}$$

with $i = 0, 1, 2, \ldots, N$. And the information received by actuators is given as

$$u_i(t_k) = \begin{cases} 0, & t \in \Xi(0, +\infty) \\ u_i(t_k), & t \in \Lambda(0, +\infty). \end{cases}$$

Similar to [14], there are two assumptions for DoS attacks.

Assumption 2 (DoS frequency): There exist constants $\eta \geq 0$ and $\tau_D > 0$ such that for all $t, \tau \in \mathbb{R}^+$

$$n(\tau, t) \leq \eta + \frac{t - \tau}{\tau_D}. \tag{7}$$

Assumption 3 (DoS Duration): There exists constant $T \geq 1$ such that for all $t, \tau \in \mathbb{R}^+$

$$|\Xi(\tau, t)| \leq \frac{t - \tau}{T}. \tag{8}$$

Assumption 2 is inspired by the concept of average dwell time [14] to specify the number of DoS attacks occurring on the interval $[\tau, t]$ and Assumption 3 is used to describe the length of the interval over which communication is interrupted. From [14] and [16], it is known that those two assumptions are common for reflecting the constraint energy of DoS attacks.

Now, the considered problem in this paper is presented as follows.

Problem 1: The main objective of this paper is to design a secure synchronization control law for the system (1) with unknown system matrices, such that the synchronization errors are asymptotically convergent for both attack-free and attack cases.

III. The Optimal Synchronization Controller Design Without Attacks

A. The Optimal Synchronization Control Law

By using (1) and (2), define the synchronization error e_i for the ith node as

$$e_i = x_i - z_0, \quad i = 1, 2, \ldots, N. \tag{9}$$

Then the synchronization problem is described as

$$\lim_{t \to \infty} (x_i - z_0) = 0, \quad i = 1, 2, \ldots, N. \tag{10}$$

The dynamic equation of the synchronization error e_i has the following form

$$\begin{aligned} \dot{e}_i &= A e_i + B_i u_i + \sum_{j=1, j \neq i}^{N} l_{ij} \Gamma_i (e_j - e_i) \\ &= \bar{A}_i e_i + B_i (u_i + F_i \omega_i) \end{aligned} \tag{11}$$

where $\bar{A}_i = A - \sum_{j=1, j \neq i}^{N} l_{ij} \Gamma_i$, $\omega_i = \sum_{j=1, j \neq i}^{N} l_{ij} \Gamma_i e_j$ and F_i satisfies $B_i F_i = I$.

Besides, similar to [30], define the performance function for the ith node (11), which involves the couplings information

$$\begin{aligned} J_i = \frac{1}{2} \int_t^{\infty} (& e_i^T Q_i e_i + u_i^T R_i u_i + 2 u_i^T R_i M_i \omega_i \\ & + \omega_i^T F_i^T R_i F_i \omega_i) d\tau \end{aligned} \tag{12}$$

where $Q_i \in \mathbb{R}^{n \times n}$ and $R_i \in \mathbb{R}^{n \times n}$ are symmetric positive weight matrices.

Theorem 1: For the error dynamics of CDNs (11) with the quadratic performance index (12), a control protocol is an optimal one if and only if it has the following form

$$u_i = -F_i \sum_{j=1, j \neq i}^{N} l_{ij} \Gamma_i e_j - R_i^{-1} B_i^T P_i e_i \tag{13}$$

where P_i is a symmetric positive matrix and satisfies the following ARE

$$\bar{A}_i^T P_i + P_i \bar{A}_i + Q_i - P_i B_i R_i^{-1} B_i^T P_i = 0. \tag{14}$$

Proof: First, one gives the necessity proof of Theorem 1.

Based on (12), define the Hamiltonian function for (11) as

$$\begin{aligned} H_i = \frac{1}{2} (& e_i^T Q_i e_i + u_i^T R_i u_i + 2 u_i^T R_i M_i \omega_i + \omega_i^T F_i^T R_i F_i \omega_i) \\ & + \lambda_i^T (t) (\bar{A}_i e_i + B_i (u_i + F_i \omega_i)) \end{aligned} \tag{15}$$

where $\lambda_i(t)$ is a multiplier to be determined. The necessary condition $\frac{\partial H_i}{\partial u_i} = 0$ on which a control protocol of system (11) is an optimal one results in

$$u_i = -F_i \sum_{j=1, j \neq i}^{N} l_{ij} \Gamma_i e_j - R_i^{-1} B_i^T \lambda_i. \tag{16}$$

Since $\frac{\partial^2 H_i}{\partial u_i^2} = R_i > 0$, the optimal control has the form of (16). Assume that e_i and λ_i satisfy the following linear equation [34]

$$\lambda_i(t) = P_i e_i \tag{17}$$

where P_i is obtained by solving the ARE (14). According to (17) and the canonical equation shown in [29], one gets the ARE

$$\bar{A}_i^T P_i + P_i \bar{A}_i + Q_i - P_i B_i R_i^{-1} B_i^T P_i = 0.$$

Using (16) and (17), it yields the control law (13). Therefore, the necessity is proven.

The proof process of sufficiency for Theorem 1, which is divided into two steps, is given as follows.

Step 1: It is necessary to prove that the control law (13) ensures the asymptotical stability of the synchronization errors. That is to say

$$\lim_{t\to\infty} e_i^T(t)P_ie_i(t)=0. \tag{18}$$

Define the Lyapunov function of system (11) as $V(t)=e_i^TP_ie_i$, and its derivative is

$$\begin{aligned}\dot V_i(t)&=\dot e_i^TP_ie_i+e_i^TP_i\dot e_i^T\\&=(\bar A_ie_i+B_i(u_i+F_i\omega_i))^TP_ie_i\\&\quad+e_iP_i(\bar A_ie_i+B_i(u_i+F_i\omega_i))\\&=e_i^T(P_i\bar A_i+\bar A_i^TP_i-2P_iB_iR_i^{-1}B_i^TP_i)e_i\\&=-e_i^T(Q_i+P_iB_iR_i^{-1}B_i^TP_i)e_i.\end{aligned} \tag{19}$$

According to ARE (14), (19) is rewritten as

$$\dot V_i(t)=-e_i^T(Q_i+P_iB_iR_i^{-1}B_i^TP_i)e_i. \tag{20}$$

Since $Q_i\ge 0$, $R_i>0$, and $Q_i+P_iB_iR_i^{-1}B_i^TP_i>0$ for all states e_i, $\dot V_i(t)<0$, and the control law (13) ensures that the synchronization errors (9) asymptotically converge to zero.

Step 2: Consider the following equation:

$$\begin{aligned}&\lim_{t\to\infty}e_i^T(t)P_ie_i(t)-e_i^T(t_0)P_ie_i(t_0)\\&=\int_{t_0}^{\infty}\frac{d(e_i^TP_ie_i)}{d\tau}d\tau=\int_{t_0}^{\infty}(e_i^TP_i\dot e_i+\dot e_i^TP_ie_i)d\tau\\&=\int_{t_0}^{\infty}(e_i^T(\bar A_i^TP_i+P_i\bar A_i)e_i+(u_i+F_i\omega_i)^TB_i^TP_ie_i\\&\quad+e_i^TP_iB_i(u_i+F_i\omega_i))d\tau.\end{aligned} \tag{21}$$

Based on the ARE (14) and the condition (18), the performance index J_i is rewritten as

$$J_i=\frac{1}{2}\left(e_i^T(t_0)P_ie_i(t_0)+\int_{t_0}^{\infty}(u_i-u_i^*)^TR_i(u_i-u_i^*)d\tau\right) \tag{22}$$

with $u_i^*=-F_i\sum_{j=1,j\ne i}^N l_{ij}\Gamma_ie_j-R_i^{-1}B_i^TP_ie_i$. Due to $R_i>0$ and $X_i^T(t_0)P_iX_i(t_0)$ being a constant, the minimum value $J_i^*=\frac{1}{2}e_i^T(t_0)P_ie_i(t_0)$ of the performance function (22) can be obtained if and only if $u_i=u_i^*$. ■

The optimal control law (13) is composed of the feedback control $-R_i^{-1}B_i^TP_ie_i$ and feedforward control $-F_i\sum_{j=1,j\ne i}^N l_{ij}\Gamma_ie_j$ compensating the couplings in system dynamics. The details are also shown in [30].

B. The Optimal Synchronization Controller Design With Unknown Dynamics

Consider the optimal controller with the following form

$$u_i=-K_ie_i-F_i\sum_{j=1,j\ne i}^{N}l_{ij}\Gamma_ie_j \tag{23}$$

where

$$K_i=R_i^{-1}B_i^TP_i. \tag{24}$$

When all system dynamics are accurately known, the feedback gain K_i is determined by solving the ARE (14). Since (14) is nonlinear in P_i, the solution P_i cannot be obtained from (14) directly. To overcome this difficulty, an algorithm has been developed in [35] by solving (25) iteratively

$$\begin{aligned}&(\bar A_i-B_iK_i^k)^TP_i^k+P_i^k(\bar A_i-B_iK_i^k)+Q_i\\&\quad+(K_i^{k+1})^TR_iK_i^{k+1}=0\end{aligned} \tag{25}$$

with $K_i^{k+1}=R_i^{-1}B_i^TP_i^k$, where K_i^0 is a given feedback gain matrix stabilizing system (11) and k represents the number of iterations.

However, when the system matrix A is unavailable which means that the system matrices $\bar A_i$ are unknown, the above method is invalid. To obtain the feedback gain K_i, according to [29] and [30], an online iterative policy relying on the information of state, input and couplings is given as follows.

First, for a given stabilizing controller gain matrix K_i^0, the input signal for learning is chosen as $u_i=-K_i^0-F_i\omega_i+e$ with e being the exploration noise. Based on (25) and $K_i^{k+1}=R_i^{-1}B_i^TP_i^k$, one has

$$\begin{aligned}&e_i^T(t+\delta t)P_i^ke_i(t+\delta t)-e_i^T(t)P_i^ke_i(t)\\&\quad=\int_t^{t+\delta t}e_i^T((\bar A_i^k)^TP_i^k+P_i^k\bar A_i^k)e_i\\&\qquad+2(u_i+K_i^ke+F_i\omega_i)^TB_i^TP_i^ke_id\tau\\&\quad=-\int_t^{t+\delta t}e_i^TQ_i^ke_id\tau\\&\qquad+2\int_t^{t+\delta t}(u_i+K_i^ke_i+F_i\omega_i)^TR_iK_i^{k+1}e_id\tau\end{aligned} \tag{26}$$

with $\bar A_i^k=\bar A_i-B_iK_i^k$ and $Q_i^k=Q_i+(K_i^k)^TR_iK_i^k$. Note that, relying on (26), the requirement of the system matrix in (25) is replaced by the information of states x_i, inputs u_i and couplings $F_i\omega_i$ measured online.

Further, for all $t=t_j$, $j=1,2,\dots,l$, satisfying $0\le t_0\le t_1\le\cdots\le t_l$ and $\delta t=t_l-t_0=t_2-t_1=\cdots=t_l-t_{l-1}$, (26) holds. Define matrices $\delta_{ixx}\in\mathbb{R}^{l\times\frac{1}{2}n(n+1)}$, $I_{ixx}\in\mathbb{R}^{l\times n^2}$, $I_{ixu}\in\mathbb{R}^{l\times n^2}$ and $I_{ixw}\in\mathbb{R}^{l\times n^2}$, so that

$$\begin{aligned}\delta_{ixx}&=[\hat e_i(t_1)-\hat e_i(t_0),\hat e_i(t_2)-\hat e_i(t_1),\dots,\hat e_i(t_l)-\hat e_i(t_{l-1})]^T\\I_{iee}&=\left[\int_{t_0}^{t_1}e_i\otimes e_id\tau,\int_{t_1}^{t_2}e_i\otimes e_id\tau,\dots,\int_{t_{l-1}}^{t_l}e_i\otimes e_id\tau\right]^T\\I_{ieu}&=\left[\int_{t_0}^{t_1}e_i\otimes u_id\tau,\int_{t_1}^{t_2}e_i\otimes u_id\tau,\dots,\int_{t_{l-1}}^{t_l}e_i\otimes u_id\tau\right]^T\\I_{iew}&=\left[\int_{t_0}^{t_1}(e_i\otimes F_i\omega_i)d\tau,\int_{t_1}^{t_2}(e_i\otimes F_i\omega_i)d\tau,\dots,\right.\\&\quad\left.\int_{t_{l-1}}^{t_l}(e_i\otimes F_i\omega_i)d\tau\right]^T\end{aligned} \tag{27}$$

where $\hat e_i$ has been defined in [29]. For a matrix $P=[p_{ij}]_{n\times n}$, an operator is defined as

$$\hat P=\left[\ p_{11},2p_{12},\dots,p_{22},2p_{23},\dots,2p_{n-1,n},p_{nn}\ \right]^T. \tag{28}$$

According to (26)–(28), one has the following equation:

$$\Theta_i^k\begin{bmatrix}\hat P_i^k\\vec(K_i^{k+1})\end{bmatrix}=\Xi_i^k \tag{29}$$

where $\Theta_i^k\in\mathbb{R}^{l\times[\frac{1}{2}n(n+1)+n^2]}$ and $\Xi_i^k\in\mathbb{R}^l$ are given as

$$\Theta_i^k = \Big[\delta_{ixx}, -2I_{ixx}(I_{nq}\otimes(K_i^k)^T R_i) - 2I_{ixu}(I_{nq}\otimes R_i) \\ -2I_{ixw}(I_{nq}\otimes R_i)\Big]$$
$$\Xi_i^k = -I_{ixx}vec(Q_i^k).$$

Furthermore, if Θ_i^k has full column rank ([36], Lemma 1), the unknown matrices P_i^k and K_i^{k+1} can be solved together by the least squares method as follows:

$$\begin{bmatrix} \hat{P}_i^k \\ vec(K_i^{k+1}) \end{bmatrix} = (\Theta_i^{kT}\Theta_i^k)^{-1}(\Theta_i^k)^T\Xi_i^k. \tag{30}$$

And the sequences of P_i^k and K_i^{k+1} have been proven to be convergent (that is, $\lim_{k\to\infty}K_i^k = K_i^*$, $\lim_{k\to\infty}P_i^{k-1} = P_i^*$) in [29].

Remark 1: The feedback gain K_i is obtained under the attack free case, and the proposed iterative policy method requires that all the information of states x_i, control inputs u_i and couplings ω_i are available.

IV. Synchronization Errors of Stability Analysis With Intermittent DoS Attacks

As shown in [14], there may be a time interval elapsing from the time $z_s + d_s$ to the time $z_s + d_s + v_s$ at which the state information is successfully sampled and transmitted. And the time interval v_s (shown in Fig. 2) satisfies

$$v_s \le \Delta_k \le \Delta_* \tag{31}$$

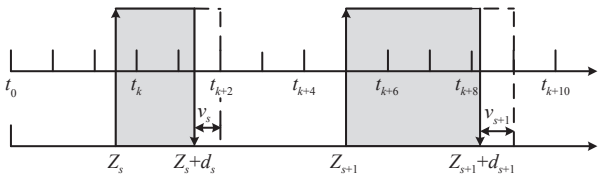

Fig. 2. An example of DoS attacks.

with Δ_* representing the upper bound on the inter-sampling rate in [14]. Thus the time interval $[\tau, t)$ is composed of the following two sub-intervals:

$$\tilde{\Xi}(\tau,t) = \bigcup_{s\in\mathbb{N}^+} V_s \bigcap [\tau,t] \tag{32}$$

$$\tilde{\Lambda}(\tau,t) = [\tau,t)\backslash\tilde{\Xi}(\tau,t) \tag{33}$$

where $V_s = [z_s, z_s + d_s + v_s)$. Specially, for all $\tau, t \in \mathbb{R}_{\ge 0}$,

$$|\tilde{\Xi}(\tau,t)| \le |\Xi(\tau,t)| + (1 + n(\tau,t))\Delta_* \tag{34}$$

$$|\tilde{\Lambda}(\tau,t)| = t - \tau - |\tilde{\Xi}(\tau,t)| \\ \ge t - \tau - |\Xi(\tau,t)| - (1 + n(\tau,t))\Delta_*. \tag{35}$$

Next, by using the Lyapunov function method and switching technique, the stability of the error systems (11) under DoS attacks will be discussed.

Note that, to analyze the stability of synchronization errors, the system dynamic matrices are required to be known in [23]–[26]. However, such a requirement cannot be satisfied in this paper, and then these existing methods are no longer applicable. To overcome this difficulty, a matrix polynomial replacement method is proposed based on the ARE (37) and the iterative learning results P_{ia} and K_i. The details are shown as follows.

Divide the process of stability analysis into two steps.

Step 1: Consider the time interval $\tilde{\Lambda}(\tau,t)$ and define the Lyapunov function of the ith node

$$V_{ia}(t) = e_i^T P_{ia} e_i. \tag{36}$$

According to the ARE (14) and the condition $K_i = R_i^{-1}B_i^T \times P_{ia}$, one gets

$$(\bar{A}_i - B_iK_i)^T P_{ia} + P_{ia}(\bar{A}_i - B_iK_i) = -(Q_i + K_i^T R_i K_i). \tag{37}$$

Define $\varphi(\bar{A}_i, P_{ia}) = P_{ia}\bar{A}_i + \bar{A}_i^T P_{ia} - 2P_{ia}B_iR_i^{-1}B_i^T P_{ia}$ and $\psi(K_i) = -(Q_i + K_i^T R_i K_i)$. Then the derivative of the Lyapunov function (36) is

$$\dot{V}_{ia}(t) = e_i^T\varphi(\bar{A}_i, P_{ia})e_i \\ = -e_i^T(Q_i + P_{ia}B_iR_i^{-1}B_i^T P_{ia})e_i. \tag{38}$$

By resorting to ARE (37) and the iterative learning results P_{ia} and K_i in (37), one has

$$\dot{V}_{ia}(t) = -e_i^T\psi(K_i)e_i. \tag{39}$$

As clarified in Theorem 1, the error systems (11) are asymptotically stable during the time interval $\tilde{\Lambda}(\tau,t)$. Thus suppose

$$\dot{V}_{ia}(t) \le -\alpha_i V_{ia} \tag{40}$$

with $\alpha_i > 0$. That is to say,

$$\psi(K_i) \ge \alpha_i P_{ia}. \tag{41}$$

Therefore, the convergence rate α_i of the system (11) can be computed by (41). Before applying the optimal control gain K_i to system (1), the matrix P_{ia} and the feedback gain matrix K_i in ARE (37) have been obtained by iteratively solving (30).

Step 2: Consider the time interval $\tilde{\Xi}(\tau,t)$. The state information received by controllers is $x_i = 0$, i.e. $e_i = 0$. Thus controllers are out of action, i.e., $u_i = 0$. Define the Lyapunov function as

$$V_{ib}(t) = e_i^T P_{ib} e_i \tag{42}$$

where its derivative satisfies

$$\dot{V}_{ib}(t) = \dot{e}_i^T P_{ib} e_i + e_i^T P_{ib}\dot{e}_i^T \\ = e_i^T(\bar{A}_i^T P_{ib} + P_{ib}\bar{A}_i)e_i \le \beta V_{ib} \tag{43}$$

with the exponential divergence rates $\beta_i > 0$. That is

$$\bar{A}_i^T P_{ib} + P_{ib}\bar{A}_i \le \beta_i P_{ib}. \tag{44}$$

Choose $P_{ib} = I_n$, and (44) becomes $\bar{A}_i^T + \bar{A}_i < \beta_i I_{nN}$. From (11), it is known that

$$\bar{A}_i^T + \bar{A}_i = A^T + A - \left(\sum_{j=1, j\ne i}^{N} l_{ij}\Gamma_i\right)^T - \sum_{j=1, j\ne i}^{N} l_{ij}\Gamma_i. \tag{45}$$

Assumption 4: Assume $\lambda_{\max}(He(\bar{A}_i))$ is available.

Based on Assumption 4, one has

$$He(\bar{A}_i)-He\left(\sum_{j=1,j\neq i}^{N} l_{ij}\Gamma_i\right)$$
$$\leq \lambda_{\max}(He(\bar{A}_i))I_n-\lambda_{\min}\left(He\left(\sum_{j=1,j\neq i}^{N} l_{ij}\Gamma_i\right)\right)I_n<\beta_i I_n \quad (46)$$

which yields the following inequality

$$\beta_i>\lambda_{\max}(He(A))-\lambda_{\min}\left(He\left(\sum_{j=1,j\neq i}^{N} l_{ij}\Gamma_i\right)\right). \quad (47)$$

Combining the above analysis results (41) and (47) of the piecewise Lyapunov functions (36) and (42), respectively, the stability of closed-loop system, which switches between stable and unstable subsystems, is established by using the switching technique. The conditions on the frequency and duration of DoS attacks, under which the secure synchronization can be guaranteed, are shown in Theorem 2.

Theorem 2: For system (11), suppose Assumptions 1–4 hold. Given any positive definite symmetric matrices R_i and Q_i with $i=1,2,\ldots,N$, if there exist positive constants θ_i such that the following two inequalities hold

$$\frac{1}{T}<\min_i\left\{\frac{\alpha_i-\theta_i}{\alpha_i+\beta_i}\right\} \quad (48)$$

$$\frac{1}{\tau_D}<\min_i\left\{\frac{\theta_i}{2\ln\mu_i+(\alpha_i+\beta_i)\Delta_*}\right\} \quad (49)$$

where α_i and β_i satisfy (41) and (47), respectively, and $\mu_i=\max\{\lambda_{\max}(P_{ia})/\lambda_{\min}(P_{ib}),\lambda_{\max}(P_{ib})/\lambda_{\min}(P_{ia})\}$. Then, the optimal control laws (13) ensure that the synchronization errors are convergent under DoS attacks.

Proof: Consider any time interval $[z_s,z_{s+1})$ that V_{ib} is activated in $[z_s,z_s+d_s+v_s)$ and V_{ia} is activated in $[z_s+d_s+v_s,z_{s+1})$. By comparison lemma in [37], one gives

$$V_i(t)\leq\begin{cases}e^{\beta_i(t-z_s)}V_{ib}(z_s), & t\in[z_s,z_s+d_s+v_s)\\ e^{-\alpha_i(t-z_s-d_s-v_s)}V_{ia}(z_s+d_s+v_s), & t\in[z_s+d_s+v_s,z_s+1)\end{cases} \quad (50)$$

Similar to [26], there are the following two cases:

Case 1: If $t\in[z_s,z_s+d_s)$, $n(t_0,t)=s$,

$$\begin{aligned}V_i(t)&\leq e^{\beta_i(t-z_s)}V_{ib}(z_s)\leq\mu_i e^{\beta_i(t-z_s)}V_{ia}(z_s^-)\\&\leq\mu_i e^{\beta_i(t-z_s)}e^{-\alpha_i(z_s-z_{s-1}-d_{s-1}-v_{s-1})}\\&\quad\times V_{ia}(z_{s-1}+d_{s-1}+v_{s-1})\\&\leq\mu_i^2 e^{\beta_i(t-z_s)}e^{-\alpha_i(z_s-z_{s-1}-d_{s-1}-v_{s-1})}\\&\quad\times V_{ib}(z_{s-1}^-+d_s^-+v_s^-)\\&\leq\mu_i^2 e^{\beta_i(t-z_s+z_{s-1}+d_{s-1}+v_{s-1}-z_{s-1})}\\&\quad\times e^{-\alpha_i(z_s-z_{s-1}-d_{s-1}-v_{s-1})}V_{ib}(z_{s-1})\\&\quad\vdots\\&\leq\mu_i^{2s-1}e^{\beta_i|\tilde{\Xi}(t_0,t)|}e^{-\alpha|\tilde{\Lambda}(t_0,t)|}V_i(t_0)\\&=\mu_i^{2n(t_0,t)-1}e^{\beta_i|\tilde{\Xi}(t_0,t)|}e^{-\alpha|\tilde{\Lambda}(t_0,t)|}V_i(t_0).\end{aligned} \quad (51)$$

Case 2: If $t\in[z_s+d_s+v_s,z_{s+1})$, $n(t_0,t)=s$,

$$\begin{aligned}V_i(t)&\leq e^{-\alpha_i(t-z_s-d_s-v_s)}V_{ia}(z_s+d_s+v_s)\\&\leq\mu_i e^{-\alpha_i(t-z_s-d_s-v_s)}V_{ib}(z_s^-+d_s^-+v_s^-)\\&\leq\mu_i e^{-\alpha_i(t-z_s-d_s-v_s)}e^{\beta_i(z_s+d_s+v_s-z_s)}V_{ib}(z_s)\\&\leq\mu_i^2 e^{-\alpha_i(t-z_s-d_s-v_s)}e^{\beta_i(z_s+d_s+v_s-z_s)}V_{ia}(z_s^-)\\&\quad\vdots\\&\leq\mu_i^{2s}e^{\beta_i|\tilde{\Xi}(t_0,t)|}e^{-\alpha_i|\tilde{\Lambda}_i(t_0,t)|}V(t_0)\\&=\mu_i^{2n(t_0,t)}e^{\beta_i|\tilde{\Xi}(t_0,t)|}e^{-\alpha_i|\tilde{\Lambda}(t_0,t)|}V_i(t_0).\end{aligned} \quad (52)$$

Thus, for $\forall t\geq t_0$,

$$V_i(t)\leq\mu_i^{2n(t_0,t)}e^{\beta_i|\tilde{\Xi}(t_0,t)|}e^{-\alpha_i|\tilde{\Lambda}(t_0,t)|}V_i(t_0). \quad (53)$$

According to Assumptions 2 and 3, and inequalities (34) and (35), it yields that

$$\begin{aligned}V_i(t)&\leq\mu_i^{2\eta_i}e^{(\alpha_i+\beta_i)(1+\eta_i)\Delta_*}\\&\quad\times e^{-(\alpha_i-\frac{2\ln\mu_i+(\alpha_i+\beta_i)\Delta_*}{\tau_D}-\frac{\alpha_i+\beta_i}{T})(t-t_0)}V_i(t_0).\end{aligned} \quad (54)$$

Let $\xi_i=\mu_i^{2\eta_i}e^{(\alpha_i+\beta_i)(1+\eta_i)\Delta_*}$ and $\delta_i=\alpha_i-\frac{2\ln\mu_i+(\alpha_i+\beta_i)\Delta_*}{\tau_D}-\frac{\alpha_i+\beta_i}{T}$. Then, one has

$$V_i(t)\leq\xi_i e^{-\delta_i(t-t_0)}. \quad (55)$$

From (48) and (49), it is known that $\delta_i>0$. Thus the synchronization errors e_i, $i=1,2,\ldots,N$, are convergent exponentially, which implies that $\lim_{t\to\infty}e_i(t)=0$. ■

Remark 2: DoS attacks compromise certain or all transmission channels, which is also introduced in [15], [16], [19] and [26]. The case that all transmission channels are interrupted when DoS attacks occur is considered in Theorem 2. This case can also be found in [23] and [26].

Remark 3: The stability analysis of synchronization errors under DoS attacks in [23]–[26] is based on the Lyapunov function approach and the exact system dynamic matrices are required to be known. While, the system matrices are not available in this paper. To overcome this difficulty, the matrix polynomial $\varphi(\bar{A}_i,P_{ia})$ including the unknown matrices $\bar{A}_i$ and P_{ia} is replaced by $\psi(K_i)$, which includes the known matrices Q_i, R_i and the control gain matrix K_i obtained by the iterative learning method.

V. Simulation Example

In this section, two complex dynamical network examples are taken to verify the effectiveness of above methods.

Example 1: Similar to [7], consider a spring-connected multi-vehicle system (shown in Fig. 3) composed of an isolated leader and four slave vehicles. The springs are regarded as the interconnection between two vehicles. In fact, the *i*th vehicle is modeled as

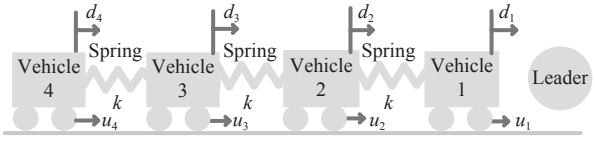

Fig. 3. Spring-connected multi-vehicle system with four slave vehicles.

$$m_i\ddot{d}_i = \sum_{j=1,j\neq i}^{N} l_{ij}k(d_j - d_i) + u_i \tag{56}$$

where d_i is the position of ith vehicle from its equilibrium position ($i = 1,2,3,4$), m_i represents the weight of ith vehicle and k means the stiffness coefficient of spring. The information of d_i and the velocity $\dot{d}_i$ is transmitted to controllers through communication channels. From (56), the slave vehicle dynamics can be governed as

$$\dot{x}_i = Ax_i + \sum_{j=1,j\neq i}^{N} l_{ij}\Gamma_i(x_j - x_i) + u_i \tag{57}$$

where $x_i = [d_i, \dot{d}_i]^T$,

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \ \Gamma_i = \begin{bmatrix} 0 & 0 \\ \dfrac{k}{m_i} & 0 \end{bmatrix}.$$

Here, assume $m_1 = 1$, $m_2 = 2.5$, $m_3 = 1.5$, $m_4 = 0.5$ and $k = 1$. Moreover, the dynamic equation of leader is described as

$$\dot{z}_0 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} z_0.$$

The simulation process is divided into two steps:

Step 1: Solving process of the solutions K_i and P_{ia} satisfying (37).

Suppose the initial values $e_1 = [-9,-9]^T$, $e_2 = [-8,-8]^T$, $e_3 = [-7,-7]^T$ and $e_4 = [-6,-6]^T$. Then choose the weighting matrices $Q_1 = 10I_2$, $Q_2 = 20I_2$, $Q_3 = 15I_2$, $Q_4 = 18I_2$ and $R_i = I_2$ for $i = 1,2,3,4$. The initial feedback gain is assumed as

$$K_{i0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

with $i = 1,2,3,4$. The exploration noise e, introduced in [36], is the sum of sinusoidal signals with different frequencies from $t = 0$ s to $t = 4$ s and it has the following form:

$$e = 5\sum_{l=1}^{50} \sin(\omega_l t) \tag{58}$$

where ω_l, with $l = 1,\ldots,50$, is randomly selected from $[-50,50]$. Besides, the internal $\sigma_k = 0.01$s is used to solve the optimal control gain K_i based on policy iteration with the information of states x_i, inputs u_i and couplings ω_i. The matrices P_{ia} and K_i, with $i = 1,2,3,4$, converge to their optimal values after 5 iterations, 4 iterations, 4 iterations, 4 iterations, respectively. Similar to [29], P_{ia}^k and K_i^k respectively converge to the corresponding optimal values in (59) and (60) when the stopping criterion $\| P_a^k - P_a^{k-1} \| \leq 0.005$ is met.

$$P_{1a} = \begin{bmatrix} 3.1623 & 0 \\ 0 & 3.1623 \end{bmatrix}, \quad P_{2a} = \begin{bmatrix} 4.4539 & 0.0961 \\ 0.0961 & 4.4925 \end{bmatrix}$$

$$P_{3a} = \begin{bmatrix} 3.9223 & -0.1528 \\ -0.1528 & 3.8303 \end{bmatrix}, \ P_{4a} = \begin{bmatrix} 4.4252 & -0.445 \\ -0.445 & 4.1124 \end{bmatrix} \tag{59}$$

$$K_1 = \begin{bmatrix} 3.1623 & 0 \\ 0 & 3.1623 \end{bmatrix}, \quad K_2 = \begin{bmatrix} 4.4539 & 0.0961 \\ 0.0961 & 4.4925 \end{bmatrix}$$

$$K_3 = \begin{bmatrix} 3.9223 & -0.1528 \\ -0.1528 & 3.8303 \end{bmatrix}, \ K_4 = \begin{bmatrix} 4.4252 & -0.445 \\ -0.445 & 4.1124 \end{bmatrix}. \tag{60}$$

After applying the optimal control law (23) with obtained gains K_i to this spring-connected multi-vehicle system (56), the state synchronization errors without any attacks are shown in Fig. 4. Clearly, the state synchronization errors of vehicles 1 – 4 are asymptotically convergent.

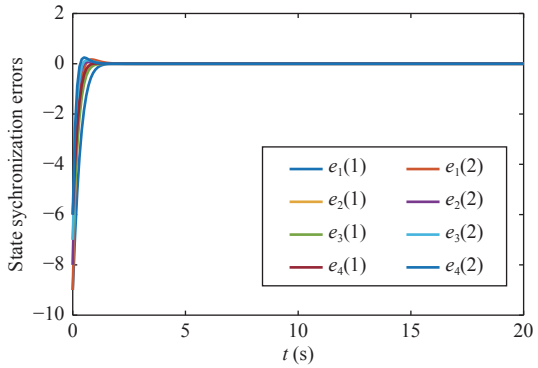

Fig. 4. Synchronization errors of vehicles 1–4 for the attack free case.

Step 2: Stability analysis of secure synchronization.

Based on the analysis results (41) and (47), one gets

$$\begin{aligned} &\alpha_1 = 20.0000,\ \alpha_2 = 39.1422,\ \alpha_3 = 28.8137,\ \alpha_4 = 32.4177 \\ &\beta_1 = 2.0000,\ \ \beta_2 = 1.8000,\ \ \beta_3 = 2.3333,\ \ \beta_4 = 3.0000 \\ &\mu_1 = 3.1623,\ \ \mu_2 = 4.5712,\ \ \mu_3 = 4.0359,\ \ \mu_4 = 4.7405. \end{aligned} \tag{61}$$

Assume the adversary launches DoS attacks with $\tau_D = 2$ and $T = 1.24$. Here $\Delta_* \geq \Delta_k = 0.001$. By computing (48) and (49), it is obtained that

$$\begin{aligned} \theta_1 &> \frac{2\ln\mu_1 + (\alpha_1+\beta_1)\Delta_*}{\tau_D} = 2.2513 \\ \theta_1 &< \alpha_1 - \frac{\alpha_1+\beta_1}{T} = 2.2581 \\ \theta_2 &> \frac{2\ln\mu_2 + (\alpha_2+\beta_2)\Delta_*}{\tau_D} = 3.5669 \\ \theta_2 &< \alpha_2 - \frac{\alpha_2+\beta_2}{T} = 6.1243 \\ \theta_3 &> \frac{2\ln\mu_3 + (\alpha_3+\beta_3)\Delta_*}{\tau_D} = 2.9526 \\ \theta_3 &< \alpha_3 - \frac{\alpha_3+\beta_3}{T} = 3.6951 \\ \theta_4 &> \frac{2\ln\mu_4 + (\alpha_4+\beta_4)\Delta_*}{\tau_D} = 3.3270 \\ \theta_4 &< \alpha_4 - \frac{\alpha_4+\beta_4}{T} = 3.8550. \end{aligned} \tag{62}$$

From (62), it is known that the conditions in (48) and (49) of Theorem 2 are satisfied. Further, the synchronization errors with DoS attacks are plotted in Fig. 5 and it is known that the states of the spring-connected multi-vehicle system with

unknown dynamics can track the leader's if the DoS frequency and DoS duration satisfy $n(0,20) \le \eta + 10$ and $|\tilde{\Xi}(0,20)| \le 16.1$, respectively. While, the system performance shown in Fig. 5 degrades due to the effects of the DoS attacks. Besides, the control laws u_i, which are larger after each DoS attack ends, are plotted in Fig. 6.

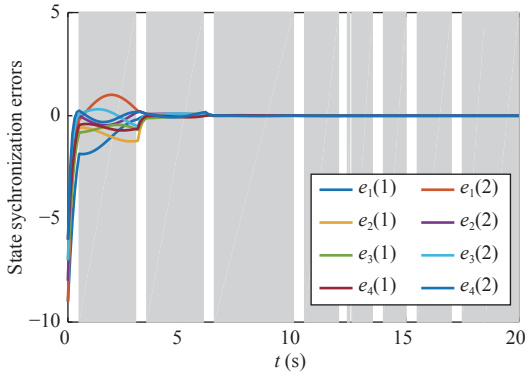

Fig. 5. Synchronization errors of vehicles 1–4 with unknown system matrix A for the DoS attacks case.

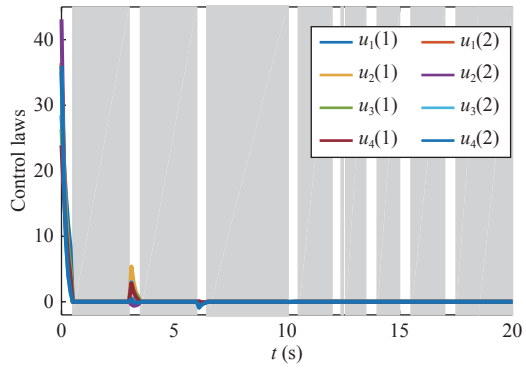

Fig. 6. Control laws of vehicles 1–4 with unknown system matrix A for the DoS attacks case.

Moreover, under the assumption of availability on the system matrices $\bar{A}_i$, the solutions P_{ia}^* of ARE (37) and the optimal controller gains K_i^* are directly computed by (37) and (24). In particular, they are the same as the optimal values P_{ia} and K_i in (59) and (60), respectively ($i = 1,2,3,4$). Then, one gets the exponential convergence rates $\alpha_i^* = \alpha_i$ by solving (41) directly. Due to (44) is nonlinear in P_{ib} and β_i, we search for solutions of (44) with $\beta_i^k = \beta_i^{k-1} + 0.001$ ($\beta_i^0 = 0$) where k represents the number of searches. Finally, the exponential divergence rates $\beta_i^* = 0.001$ and the following matrices P_{ib}^* are obtained

$$P_{1b}^* = \begin{bmatrix} 15.8850 & 0 \\ 0 & 15.8850 \end{bmatrix}, \quad P_{2b}^* = \begin{bmatrix} 14.6136 & -0.0001 \\ -0.0001 & 18.2673 \end{bmatrix}$$

$$P_{3b}^* = \begin{bmatrix} 114.4736 & -0.0005 \\ -0.0005 & 85.8552 \end{bmatrix}, \quad P_{4b}^* = \begin{bmatrix} 114.4736 & -0.0005 \\ -0.0005 & 85.8552 \end{bmatrix}.$$

According to P_{ia} and P_{ib}, one has $\mu_i = 5.0233$ for $i = 1,2,3,4$. Assume the adversary launches DoS attacks with $\tau_D = 2$ and $T = 1.156$. By computing (48) and (49), it is obtained that

$$2.6141 < \theta_1 < 2.6990, \ \ 3.5712 < \theta_2 < 5.2821$$
$$3.0548 < \theta_3 < 3.8883, \ \ 3.2350 < \theta_4 < 4.3746.$$

Obviously, the conditions in (48) and (49) of Theorem 2 are satisfied. The synchronization errors under DoS attacks with frequency satisfying $n(0,20) \le \eta + 10$ and the duration satisfying $|\tilde{\Xi}(0,20)| \le 17.3$ are plotted in Fig. 7. Besides, the corresponding control laws u_i are plotted in Fig. 8. As shown in Figs. 7 and 8, the system performance degrades due to the effects of the DoS attacks. Further, after each DoS attack ends, much control effort is needed to drive the synchronization errors to be convergent.

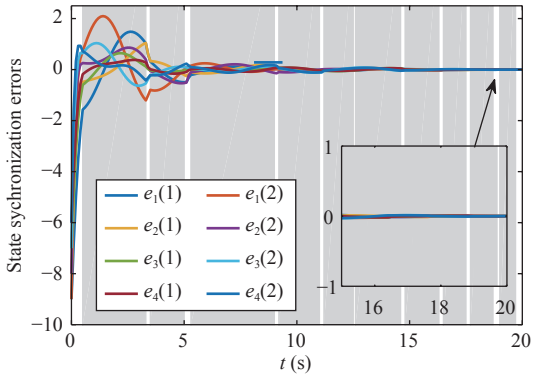

Fig. 7. Synchronization errors of vehicles 1–4 with known system matrix A for DoS attacks case.

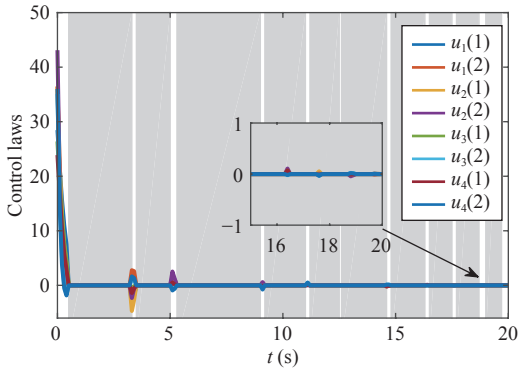

Fig. 8. Control laws of vehicles 1–4 with known system matrix A for DoS attacks case.

As shown above, the upper bounds of the DoS attack frequency and the DoS duration which are solved by the proposed method in this paper are slightly smaller than those obtained by the model based method.

To further prove the effectiveness of the proposed approaches in this paper, Example 2 with more complex graph structure is given as follows.

Example 2: Consider CDNs are with five nodes, and the correlative graph is shown in Fig. 9. The leader node's dynamic is described as

$$\dot{x}_0(t) = \begin{bmatrix} 0.4 & 1 \\ -1 & 0 \end{bmatrix} x_0$$

and the system dynamics of five nodes are shown as

$$A = \begin{bmatrix} 0.4 & 1 \\ -1 & 0 \end{bmatrix}$$

with $B = I_2$, $\Gamma_1 = 0.9I_2$, $\Gamma_2 = 0.7I_2$, $\Gamma_3 = 0.9I_2$, $\Gamma_4 = I_2$, $\Gamma_5 = 2I_2$. Suppose the initial values $e_1 = [-6,-6]^T$, $e_2 = [-5,-5]^T$, $e_3 = [-4,-4]^T$, $e_4 = [-2,-6]^T$ and $e_5 = [-5,-3]^T$. Then choose the weighting matrices $Q_5 = 12I_2$.

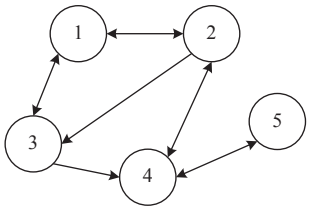

Fig. 9. Graph structure for the CDNs.

Similar to Example 1, the simulation process is divided into two steps.

Step 1: Use the policy iteration method to obtain the solutions P_{ia} and K_i. The initial controller gain is chosen as

$$K_{i0} = \begin{bmatrix} 1 & 0 \\ 0 & 0.1 \end{bmatrix}.$$

Besides, the other parameters are assumed to be the same as those in Example 1. By utilizing the PI method, the optimal solutions P_{ia} and K_i with $i = 1,2,3,4,5$ are obtained after 4 iterations. They are given as

$$K_{1a} = \begin{bmatrix} 2.0499 & 0.0287 \\ 0.0287 & 1.8464 \end{bmatrix}, \quad K_{2a} = \begin{bmatrix} 3.5758 & 0.0306 \\ 0.0306 & 3.2926 \end{bmatrix}$$
$$K_{3a} = \begin{bmatrix} 2.7114 & 0.0279 \\ 0.0279 & 2.4773 \end{bmatrix}, \quad K_{4a} = \begin{bmatrix} 2.3725 & 0.0170 \\ 0.0170 & 2.1994 \end{bmatrix}$$
$$K_{5a} = \begin{bmatrix} 2.3725 & 0.0170 \\ 0.0170 & 2.1994 \end{bmatrix} \tag{63}$$

$$P_{1a} = \begin{bmatrix} 2.0499 & 0.0287 \\ 0.0287 & 1.8464 \end{bmatrix}, \quad P_{2a} = \begin{bmatrix} 3.5758 & 0.0306 \\ 0.0306 & 3.2926 \end{bmatrix}$$
$$P_{3a} = \begin{bmatrix} 2.7114 & 0.0279 \\ 0.0279 & 2.4773 \end{bmatrix}, \quad P_{4a} = \begin{bmatrix} 2.3725 & 0.0170 \\ 0.0170 & 2.1994 \end{bmatrix}$$
$$P_{5a} = \begin{bmatrix} 2.3725 & 0.0170 \\ 0.0170 & 2.1994 \end{bmatrix}. \tag{64}$$

Step 2: Stability analysis of secure synchronization

According to the analysis results (41) and (47), suppose that the DoS attacks with $\tau_D = 2$ and $T = 1.2$ occur during time interval $(0,20)$, which satisfying the conditions in (48) and (49) in Theorem 2.

The synchronization errors under the DoS attacks are given in Fig. 10. Besides, the corresponding control laws u_i are plotted in Fig. 11. As shown in Fig. 10, the synchronization errors become large when the system is under DoS attacks. Finally, the system with unknown dynamics can track the leader, if the DoS frequency satisfies $n(0,20) \le \eta + 10$ and the DoS duration satisfies $|\Xi(0,20)| \le 16.6$.

VI. Conclusion

This paper investigates the secure synchronization control problem for CPSs subject to intermittent DoS attacks. The considered CPSs are modeled as a class of CDNs with unknown dynamics. First, to deal with the state couplings, a distributed optimal controller is proposed based on our previous works [29]. And the optimal feedback gain matrix is learned by iteratively solving the ARE. Especially, based on the ARE and the iteratively learning results, the decay rates for each node about sleeping and active intervals of DoS attacks, are determined by solving a set of linear matrix inequalities. Moreover, by using the switching technique and the obtained decay rates, the upper bounds of the DoS attacks frequency and duration, under which the synchronization for all nodes is still achieved, have been proposed. Finally, the simulations of two examples verify the effectiveness of the proposed methods.

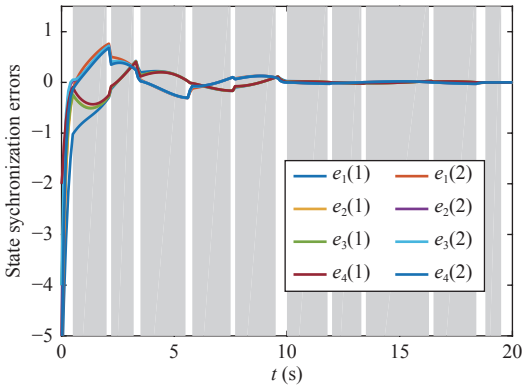

Fig. 10. Synchronization errors of nodes 1–5 with unknown system matrix A for the DoS attacks case.

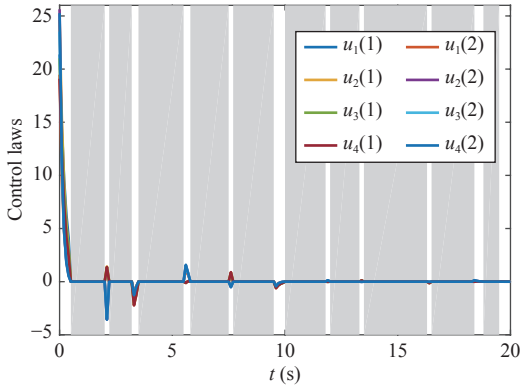

Fig. 11. Control laws of nodes 1–5 with unknown system matrix A for the DoS attacks case.

References

[1] V. Reppa, M. M. Polycarpou, and C. G. Panayiotou, "Distributed sensor fault diagnosis for a network of interconnected cyberphysical systems," *IEEE Trans. Control of Network Systems*, vol. 2, no. 1, pp. 11–23, 2015.

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

[3] A. Isidori, L. Marconi, and G. Casadei, "Robust output synchronization of a network of heterogeneous nonlinear agents via nonlinear regulation theory," *IEEE Trans. Autom. Control*, vol. 59, no. 10, pp. 2680–2691, 2014.

[4] M. H. Zhu and S. Martinez, "On the performance analysis of resilient

networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, 2014.

[5] H. Liu, X. H. Cao, J. P. He, P. Cheng, C. G. Li, J. M. Chen, and Y. X. Sun, "Distributed identification of the most critical node for average consensus," *IEEE Trans. Signal Processing*, vol. 63, no. 16, pp. 4315–4328, 2015.

[6] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Trans. Industrial Informatics*, vol. 13, no. 2, pp. 436–447, 2017.

[7] X. Z. Jin, G. H. Yang, and W. W. Che, "Adaptive synchronization of master-slave large-scale systems against bias actuators and network attenuations," *Int. J. Control, Autom. and Systems*, vol. 10, no. 6, pp. 1102–1110, 2012.

[8] Y. Wang, J. L. Xiong, and D. W. C. Ho, "Decentralized control scheme for large-scale systems defined over a graph in presence of communication delays and random missing measurements," *Automatica*, vol. 98, pp. 190–200, 2018.

[9] A. Y. Lu and G. H. Yang, "Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer," *Information Sciences*, vol. 417, pp. 454–464, 2017.

[10] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 8, pp. 2079–2091, 2016.

[11] D. R. Ding, Z. D. Wang, D. W. C. Ho, and G. L. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231–240, 2017.

[12] X. Huang and J. X. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Trans. Cybernetics*, vol. 48, no. 12, pp. 3432–3439, 2018.

[13] G. Franzè, F. Tedesco, and W. Lucia, "Resilient control for cyberPhysical systems subject to replay attacks," *IEEE Control Systems Letters*, vol. 3, no. 4, pp. 984–989, 2019.

[14] C. D. Persis and P. Tesi, "Input-to-state stabilizing control under denial-ofservice," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[15] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

[16] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Eventtriggered control systems under denial-of-service attacks," *IEEE Trans. Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2017.

[17] A. Y. Lu and G. H. Yang, "Input-to-state stabilizing control for cyberphysical systems with multiple transmission channels under denial of service," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1813–1820, 2018.

[18] S. L. Hu, D. Yue, X. L. Chen, Z. H. Cheng, and X. P. Xie, "Resilient H_∞ filtering for event-triggered networked systems under nonperiodic DoS jamming attacks," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, Mar. 2019. DOI: 10.1109/TSMC.2019.2896249.

[19] L. W. An and G. H. Yang, "Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks," *IEEE Trans. Cybernetics*, vol. 49, no. 3, pp. 827–838, 2017.

[20] L. H. Peng, L. Shi, X. H. Cao, and C. Y. Sun, "Optimal attack energy allocation against remote state estimation," *IEEE Trans. Autom. Control*, vol. 63, no. 7, pp. 2199–2205, 2017.

[21] K. M. Ding, Y. Z. Li, D. E. Quevedo, S. Dey, and L. Shi, "A multi-channel transmission schedule for remote state estimation under DoS attacks," *Automatica*, vol. 78, pp. 194–201, 2017.

[22] B. Chen, D. W. C. Ho, W. A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 49, no. 2, pp. 455–468, 2017.

[23] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybernetics*, vol. 49, no. 4, pp. 1501–1511, 2018.

[24] Y. W. Wang, H. O. Wang, J. W. Xiao, and Z. H. Guan, "Synchronization of complex dynamical networks under recoverable attacks," *Automatica*, vol. 46, no. 1, pp. 197–203, 2010.

[25] Y. Xu, M. Fang, P. Shi, and Z. G. Wu, "Event-based secure consensus of mutiagent systems against DoS attacks," *IEEE Trans. Cybernetics*, Jun. 2019. DOI: 10.1109/TCYB.2019.2918402.

[26] Z. Feng and G. Q. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Systems Technology*, 2019. DOI: 10.1109/TCST.2019.2892032.

[27] B. Kiumarsi and F. L. Lewis, "Output synchronization of heterogeneous discrete-time systems: A model-free optimal approach," *Automatica*, vol. 84, pp. 86–94, 2017.

[28] H. Modares, S. P. Nageshrao, G. A. D. Lopes, R. Babuška, and F. L. Lewis, "Optimal model-free output synchronization of heterogeneous systems using off-policy reinforcement learning," *Automatica*, vol. 71, pp. 334–341, 2016.

[29] N. Wang and X. J. Li, "Optimal output synchronization control of a class of complex dynamical networks with partially unknown system dynamics," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, 2018. DOI: 10.1109/TSMC.2018.2882827.

[30] Y. W. Cao, G. H. Yang, and X. J. Li, "Optimal synchronization controller design for complex dynamical networks with unknown system dynamics," *J. Franklin Institute*, vol. 356, no. 12, pp. 6071–6086, 2019.

[31] M. Y. Li and Z. S. Shuai, "Global-stability problem for coupled systems of differential equations on networks," *J. Differential Equations*, vol. 248, no. 1, pp. 1–20, 2010.

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

[33] H. Zhang, P. Cheng, L. Shi, and J. M. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Systems Technology*, vol. 24, no. 3, pp. 834–852, 2016.

[34] F. L. Lewis, D. Vrabie, and V. Syrmos, *Optimal Control*, 3rd edition, New York: Wiley, 2012.

[35] D. Kleinman, "On an iterative technique for Riccati equation computations," *IEEE Trans. Autom. Control*, vol. 13, no. 1, pp. 114–115, 1968.

[36] Y. Jiang and Z. P. Jiang, "Computational adaptive optimal control for continuous-time linear systems with completely unknown dynamics," *Automatica*, vol. 48, pp. 2699–2704, 2012.

[37] H. K. Khalil, *Nonlinear Systems*, 3rd edition, Prentice Hall, Englewood Cliffs, NJ, 2003.

Ning Wang received the B.S. degree in measuring and control instrument from Northeastern University at Qinhuangdao, in 2017, and the M.S. degree in control theory and control engineering from Northeastern University, in 2019, where she is currently pursuing the Ph.D. degree. Her research interests include fault diagnosis, adaptive dynamics program, and the security of cyber-physical systems.

Xiao-Jian Li (M'16) received the B.S. and M.S. degrees in mathematics from Northeast Normal University, in 2003 and 2006, respectively, and the Ph.D. degree in control theory and engineering from Northeastern University, in 2011. He is currently a Professor at the College of Information Science and Engineering, Northeastern University. His research interests include fault diagnosis, distributed optimization, and the security of cyber-physical systems.