Hindawi
Journal of Control Science and Engineering
Volume 2022, Article ID 9799958, 18 pages
https://doi.org/10.1155/2022/9799958

Research Article

Intermittent Control for Synchronization of Discrete-Delayed Complex Cyber-Physical Networks under Mixed Attacks

Chaoqun Zhu, Xuan Jia, and Pan Zhang

College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China

Correspondence should be addressed to Chaoqun Zhu; chaoqunzhu@yeah.net

Received 30 October 2022; Revised 4 December 2022; Accepted 9 December 2022; Published 21 December 2022

Academic Editor: Sundarapandian Vaidyanathan

This paper is concerned with the synchronization control problem for discrete-delayed complex cyber-physical networks under mixed attacks. To handle input delays and mixed attacks, the intermittent control mechanism is employed, which is distinctly different from the traditional control method. By utilizing the Lyapunov stability theorem, a novel synchronization control method is developed for the synchronization control of complex cyber-physical networks with mixed attacks. Then, sufficient conditions are derived to guarantee that the synchronization error dynamics are ultimately bounded. Moreover, the conditions for a special case where the absence of input delays. Subsequently, certain optimization problems are formulated with the aim to minimize the synchronization error. Finally, two numerical examples are given to verify the effectiveness and superiority of the proposed synchronization control strategy.

1. Introduction

As typical massively interconnected complex systems, complex networks are composed of a large number of interacting individuals or nodes, whose dynamics can be described by a single nonlinear vector field, such as multiagent systems, transportation networks, neural networks, and electric power grids. [1–5]. Over several decades, the synchronization control of complex networks has generally been recognized as one of the most fascinating issues of research, and scholars have carried out increasing research on emergency behaviour and coordinated movement of complex networks [6]. On the one hand, due to the simultaneous transmission signal between a tremendous number of nodes in complex networks and the complex coupling of communication networks, it is inevitable to encounter the problem of time delay, which may lead to the damage of the system performance. Therefore, the synchronization problem of complex networks with time delays has received considerable attention (see, e.g., [7–9]). On the other hand, as a result of the complicated network structure, it is always difficult to achieve spontaneous synchronization. To date, various control techniques have been presented to investigate the synchronization problem of complex networks [10–15]. Among them, intermittent control methods are widely investigated due to the fact that they are easy implementation and more economic than continuous-time ones. For instance, in [14], the authors propose aperiodically intermittent pinning control methods for dynamical networks, and in [11], an intermittent control strategy is proposed to ensure exponential synchronization of neural networks under actuator saturations. It is worth mentioning that in [11], the control actions are clock-dependent, which means that the controller only works at the prescribed times. To reduce the limits of the preset clock, the authors of [12] design an event-dependent intermittent controller for quasi-synchronization control of delayed discrete-time neural networks. In [15], the authors propose intermittent control methods for competitive neural networks.

In practice, due to open network connections between individual nodes, complex networks are often vulnerable to direct or indirect damage from cyber-attacks and resulting in degraded or even missing synchronous performance of complex networks. Specifically, the availability and integrity performance of the modern system information is at serious risk, as testified by several example incidents. For instance,

the Iran nuclear program has been attacked by the Stuxnet virus in 2010, and the Ukrainian power grid has been attacked by the Black-Energy 3 virus in 2015 [16]. Generally speaking, according to the type of physical implementation, cyber-attacks can be broadly classified into false data injection (FDI) attacks [4, 17, 18], replay attacks [19, 20], and denial of service (DoS) attacks [21–24]. To date, a large number of interesting findings have been reported, which reveal the impact of cyber-attacks on system performance and provide a number of detection and identification schemes (see, e.g., [25–30]). For example, the adaptive event-triggered nonfragile state estimation problem is discussed for fractional-order complex networked systems subject to cyber-attacks [30]. Most existing results mainly report on the detection and estimation of attacks under a predesigned controller. However, there are still few explorers on the security synchronization control of complex networks. Compared with replay attacks and DoS attacks, FDI attacks can maliciously tamper with the critical operational data of complex cyber-physical networks and are more concealed and destructive than the other two types of cyber-attacks. To name a few, in [17], the resilient consensus problem is discussed for discrete-time complex cyber-physical networks subject to FDI attacks. The authors in [18] establish a defense framework for cyber-physical systems under FDI attacks. From the perspective of cyber-attacks' implementation methods, the DoS attacks are most easily put into effect and can block the communication channels or interrupt the communication of the target system. In [21], the pinning-observer-based secure synchronization control problem is investigated for complex dynamical networks under DoS attacks. In [24], the authors propose distributed cooperative control methods for linear multiagent systems subject to DoS attacks. Unfortunately, the above results only focus on cyber-attacks, and few works are involved with physical attacks. As a kind of adversarial disturbance, physical attacks may cause the system components to operate incorrectly by maliciously modifying system inputs and thus lead to system instability [31, 32]. In [31], the machine learning method is utilized to detect physical attacks on Internet of Things applications. In response to the problem of multiple stochastic physical attacks, the robust secure controller is developed to ensure the stability of cyber-physical systems [32]. Up to now, most of the existing results are concerning single malicious attacks in complex cyber-physical networks for the simplicity of analysis and design. However, in control practice, complex cyber-physical systems are often simultaneously attacked by mixed attacks (e.g., FDI attacks, DoS attacks, and physical attacks). Due to the inherent coupling between network node dynamics and the threat of mixed attacks, the issue of synchronization control for cyber-physical networks with mixed attacks remains a technical challenge that needs to be addressed urgently, which is the primary motivation of the current investigation.

Motivated by the aforementioned discussions, this paper is devoted to the investigation of the synchronization control problem for discrete-time complex cyber-physical networks with input delays and mixed attacks. The main contributions of this paper are summarized as follows:

(1) A unified model with both cyber-attacks and physical attacks is proposed to characterize the pattern feature of mixed attacks, and then the intermittent synchronization controller is proposed for discrete-time complex cyber-physical networks with input delays.

(2) Different from the periodic intermittent control mechanism in [33, 34], in which the time interval must be preset in advance, this paper adopts an event-dependent nonperiodic intermittent control mechanism. In other words, the control input is state dependent. Therefore, the control cost will be reduced fundamentally.

(3) An analytical expression of the synchronization error dynamics is developed within the energy-constrained mixed attacks, and sufficient conditions are derived to guarantee the ultimate boundedness of the synchronization control performance.

2. Problem Formulation and Preliminaries

We will model discrete-delayed complex cyber-physical networks under mixed attacks. To improve readability, the notations used in this paper are standard and expressed as Table 1.

We consider discrete-delayed complex cyber-physical networks consisting of N identically coupled nodes as follows:

$$\begin{aligned} x_i(k+1) &= Ax_i(k) + f\left(x_i(k)\right) + \sum_{j=1}^{N} \widetilde{l}_{ij}\Gamma x_j(k) + u_i\left(k-\tau_k\right) + h\left(x_i(k)\right) + E\omega_i(k), \\ x_i(\theta) &= \phi_i(\theta), \theta \in (-\infty, 0], \end{aligned} \tag{1}$$

where $x_i(k) \in \mathbb{R}^n$, $u_i(k) \in \mathbb{R}^m$, $\omega_i(k) \in \mathbb{R}^n$, and $\phi_i(\theta) \in \mathbb{R}^n$, $(i \in \{1, 2, \ldots, N\})$ denote the state vector, the control input, the disturbance input, and the initial conditions, respectively. $f(x_i(k)) \in \mathbb{R}^n$ is the nonlinear vector-valued function. $h(x_i(k)) \in \mathbb{R}^n$ is the physical attacks signal injected by the anomalies [35]. $A \in \mathbb{R}^n$ and $E \in \mathbb{R}^n$ are known constant matrices with appropriate dimensions. τ_k is the time-varying delay, which satisfies $\tau_m \le \tau_k \le \tau_M$, where τ_m and τ_M are the lower and upper bounds of the time delay, respectively. $\Gamma \in \mathbb{R}^{n\times n}$ denotes the inner-coupling matrix,

Table 1: Notations.

Notations	Expression
$\mathbb{R}^n$	n-dimensional Euclidean space
$\mathbb{R}^{n\times n}$	$n \times n$ real matrices
$\mathcal{N}$	The sets of non-negative integers
$\mathcal{N}[a,b]$	The set of integers between a and b
$\mathcal{R}_+$	The non-negative real region
G^T	The transpose of the matrix G
$P>0$	Matrix P is positive definite
$P\geq 0$	Matrix P is positive semidefinite
$\|x\|$	The Euclidean vector norm
Δ	The differential operator
$\otimes$	The Kronecker product
$*$	Symmetric entry
$\lambda_{\min}(T)$	The smallest eigenvalues of matrix T
diag$\{\cdot\}$	The diagonal matrix
$I/0$	Identity matrix/zero matrix
I_N	The $N \times N$ identity matrix

and $L = (\widetilde{l}_{ij})_{N\times N}$ is a matrix representing the outer-coupling configuration with $\widetilde{l}_{ij} \geq 0$, $(i \neq j)$ and $\widetilde{l}_{ij} = -\sum_{j=1, j\neq i}^{N} \widetilde{l}_{ij}$. The structure of control for networks node i is shown in Figure 1.

In the following, the model of cyber-attacks will be constructed for discrete-time delayed complex cyber-physical networks, which is shown in Figure 2. Firstly, the FDI attacks in the communication network aim to contaminate the control input with false data and thus threaten system security. For the FDI attacks, a Bernoulli variable $\pi(k)$ is used to indicate whether the FDI attacks occur. The data revamped by the FDI attacks can be denoted as follows [36]:

$$\overline{u}_i(k) = \pi(k)g\left(u_i(k-\tau(k))\right) + (1-\pi(k))u_i(k-\tau(k)), \quad (2)$$

where $g(u_i(k-\tau(k))) \in \mathbb{R}^n$ is the vector of FDI attacks. The Bernoulli variable $\pi(k) \in \{0,1\}$ satisfies $E\{\pi(k)\} = \overline{\pi}$, and $E\{\pi(k) - \overline{\pi}\} = \pi^2$. $\pi(k) = 1$ indicates that the FDI attacks have contaminated the control data, and $\pi(k) = 0$ denotes that the FDI attacks have failed to affect the transmitted data.

In addition, random DoS attacks in the control channel [37]. Similar to the FDI attacks, another variable $\lambda(k)$ with the Bernoulli distribution is utilized to describe the DoS attacks signal, which can be expressed as follows:

$$\lambda(k) = \begin{cases} 0, & \text{others}, \\ 1, & \text{occurs}, \end{cases} \quad (3)$$

where the Bernoulli variable $\lambda(k) \in \{0,1\}$ satisfies $E\{\lambda(k)\} = \overline{\lambda}$ and $E\left\{\lambda(k) - \overline{\lambda}\right\} = \lambda^2$. $\lambda(k) = 0$ represents that the DoS attacks are not occurring, while $\lambda(k) = 1$ denotes that the network suffers from the DoS attacks.

Based on the above description, the control signal suffering from the DoS attacks and FDI attacks can be derived as follows:

$$\widetilde{u}_i(k) = (1-\lambda(k))\overline{u}_i(k). \quad (4)$$

Comminating (2) and (4), the control input after networks transmission is obtained as follows:

$$\widetilde{u}_i(k-\tau(k)) = (1-\lambda(k))\left(\pi(k)g\left(u_i(k-\tau(k))\right) + (1-\pi(k))u_i(k-\tau(k))\right). \quad (5)$$

Then, the model of delayed complex cyber-physical networks (1) under mixed attacks can be expressed as follows:

$$\begin{aligned} x_i(k+1) &= Ax_i(k) + f\left(x_i(k)\right) + \sum_{j=1}^{N} \widetilde{l}_{ij}\Gamma x_j(k) + h\left(x_i(k)\right) + E\omega(k) \\ &\quad + (1-\lambda(k))\left(\pi(k)g\left(u_i(k-\tau(k))\right) + (1-\pi(k))u_i(k-\tau(k))\right), \\ x_i(\theta) &= \phi_i(\theta), \theta \in (-\infty, 0]. \end{aligned} \quad (6)$$

In this paper, the following form of the isolated node is considered:

$$\begin{aligned} s(k+1) &= As(k) + f(s(k)) + h(s(k)) + E\omega(k), \\ s(\theta) &= \phi(\theta), \theta \in (-\infty, 0], \end{aligned} \quad (7)$$

where $s(k) \in \mathbb{R}^n$ is the state vector of the isolated node.

For the established model of complex cyber-physical networks under mixed attacks (6), the following assumptions are given.

Assumption 1. The disturbance $\widetilde{\omega}(k)$ is energy bounded and satisfies the following conditions:

$$\sum_{k}^{+\infty} \widetilde{\omega}^T(k)\widetilde{\omega}(k) \leq \delta, \quad (8)$$

where δ is a given positive scalar.

Assumption 2. For any $v_1(k) \in \mathbb{R}^n$ and $v_2(k) \in \mathbb{R}^n$, the nonlinear functions $f(x_i(k)) \in \mathbb{R}^n$, $g(x_i(k)) \in \mathbb{R}^n$, and $h(x_i(k)) \in \mathbb{R}^n$ satisfy the following conditions:

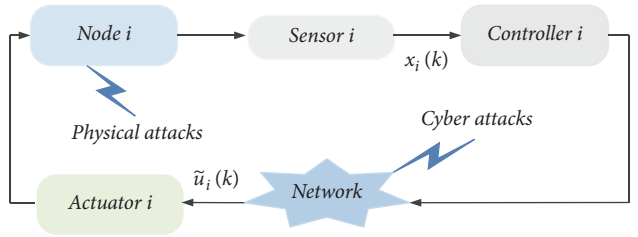

Figure 1: The structure of control for the network node i.

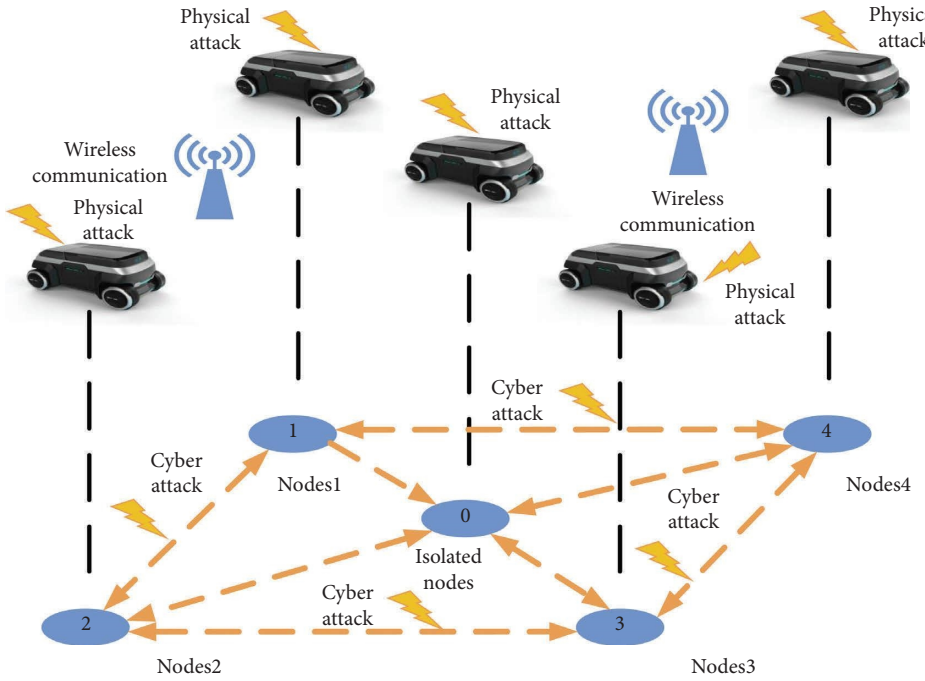

Figure 2: Illustration of complex cyber-physical networks under mixed attacks.

$$\begin{cases} \left[f(v_1(k)) - f(v_2(k)) - \mathscr{H}_{1f}(v_1(k) - v_2(k))\right]^T \times \left[f(v_1(k)) - f(v_2(k)) - \mathscr{H}_{2f}(v_1(k) - v_2(k))\right] \le 0, \\ \left[g(v_1(k)) - g(v_2(k)) - \mathscr{H}_{1g}(v_1(k) - v_2(k))\right]^T \times \left[g(v_1(k)) - g(v_2(k)) - \mathscr{H}_{2g}(v_1(k) - v_2(k))\right] \le 0, \\ \left[h(v_1(k)) - h(v_2(k)) - \mathscr{H}_{1h}(v_1(k) - v_2(k))\right]^T \times \left[h(v_1(k)) - h(v_2(k)) - \mathscr{H}_{2h}(v_1(k) - v_2(k))\right] \le 0, \end{cases} \tag{9}$$

where $\mathscr{H}_{1f}$, $\mathscr{H}_{2f}$, $\mathscr{H}_{1g}$, $\mathscr{H}_{2g}$, $\mathscr{H}_{1h}$, and $\mathscr{H}_{2h} \in \mathbb{R}^{n\times n}$ are known constant matrices.

Remark 1. Based on the above presentations, a mixed attacks model is proposed following the FDI attacks, DoS attacks, and physical attacks strategies. According to Assumption 1, the FDI attacks and physical attacks are always constrained by the limited energy. In the cyber layer, when FDI attacks and DoS attacks occur simultaneously, the DoS attacks will lead to the loss of data injected by the FDI attacks.

Define the synchronization error and the initial error as follows:

$$\begin{aligned} e_i(k) &= x_i(k) - s(k), \\ \tilde{\phi}_i(\theta) &= \phi_i(\theta) - \phi(\theta). \end{aligned} \tag{10}$$

Then, the following matrices and notations are introduced:

$$\begin{aligned}
\widetilde{A} &= I_N \otimes A, \widetilde{E} = I_N \otimes E, \widetilde{L} = L \otimes \Gamma, \widetilde{\mathscr{H}}_{1f} = I_N \otimes \mathscr{H}_{1f}, \widetilde{\mathscr{H}}_{2f} = I_N \otimes \mathscr{H}_{2f},\\
\widetilde{\mathscr{H}}_{1g} &= I_N \otimes \mathscr{H}_{1g}, \widetilde{\mathscr{H}}_{2g} = I_N \otimes \mathscr{H}_{2g}, \widetilde{\mathscr{H}}_{1h} = I_N \otimes \mathscr{H}_{1h}, \widetilde{\mathscr{H}}_{2h} = I_N \otimes \mathscr{H}_{2h},\\
e(k) &= \left[\, e_1^T(k) \;\; e_2^T(k) \;\; \cdots \;\; e_N^T(k) \,\right]^T,\\
\widetilde{\phi}(k) &= \left[\, \widetilde{\phi}_1^T(k) \;\; \widetilde{\phi}_2^T(k) \;\; \cdots \;\; \widetilde{\phi}_N^T(k) \,\right]^T,\\
\widetilde{f}(e(k)) &= \left[\, \widetilde{f}^T(e_1(k)) \;\; \cdots \;\; \widetilde{f}^T(e_N(k)) \,\right],\\
\widetilde{g}(e(k)) &= \left[\, \widetilde{g}^T(e_1(k)) \;\; \cdots \;\; \widetilde{g}^T(e_N(k)) \,\right],\\
\widetilde{h}(e(k)) &= \left[\, \widetilde{h}^T(e_1(k)) \;\; \cdots \;\; \widetilde{h}^T(e_N(k)) \,\right],\\
\widetilde{\omega}(k) &= \left[\, \widetilde{\omega}_1^T(k) \;\; \widetilde{\omega}_2^T(k) \;\; \cdots \;\; \widetilde{\omega}_N^T(k) \,\right]^T,\\
\widetilde{f}(e_i(k)) &= f(x_i(k)) - f(s(k)) - \mathscr{H}_{1f} e(k),\\
\widetilde{g}(e_i(k)) &= g(x_i(k)) - g(s(k)) - \mathscr{H}_{1g} e(k),\\
\widetilde{h}(e_i(k)) &= h(x_i(k)) - h(s(k)).
\end{aligned} \tag{11}$$

According to the above definition and (6), (7), and (9), the synchronization error dynamics can be obtained as follows:

$$\begin{aligned}
e(k+1) = {} & \left(\widetilde{A} + \widetilde{L} + \widetilde{\mathscr{H}}_{1f}\right) e(k) + \widetilde{f}(e(k)) + \widetilde{h}(e_i(k)) + \widetilde{E}\widetilde{\omega}(k)\\
& + (1 - \lambda(k))\pi(k)\widetilde{g}(u(k - \tau(k))) + (1 - \lambda(k))(1 - \pi(k))u(k - \tau(k)),\\
e(\theta) = {} & \widetilde{\phi}(\theta), \theta \in (-\infty, 0].
\end{aligned} \tag{12}$$

It is from (9) that

$$\begin{cases}
\widetilde{f}^T(e(k))\left[\widetilde{f}(e(k)) - \left(\widetilde{\mathscr{H}}_{2f} - \widetilde{\mathscr{H}}_{1f}\right) e(k)\right] \le 0,\\
\widetilde{g}^T(e(k))\left[\widetilde{g}(e(k)) - \left(\widetilde{\mathscr{H}}_{2g} - \widetilde{\mathscr{H}}_{1g}\right) e(k)\right] \le 0,\\
\left[\widetilde{h}(e(k)) - \widetilde{\mathscr{H}}_{1h} e(k)\right]^T \left[\widetilde{h}(e(k)) - \widetilde{\mathscr{H}}_{2h} e(k)\right] \le 0.
\end{cases} \tag{13}$$

In this paper, to achieve synchronization control of the complex cyber-physical networks (6), an intermittent synchronization controller is employed as follows:

$$u(k) = \begin{cases}
K_1 e(k) + K_2 e(k - \tau_k), \mathscr{V}(k) \in \mathscr{R}_1(k),\\
0, \mathscr{V}(k) \in \mathscr{R}_2(k),\\
u(k-1), \mathscr{V}(k) \in \mathscr{R}_3(k),
\end{cases} \tag{14}$$

where $K_i (i = 1, 2)$ are parametric intermittent synchronization controller gain matrices. $\mathscr{V}(k)$ is Lyapunov-like functions. $\mathscr{R}_i(k) (i = 1, 2, 3)$ are three subregions of the nonnegative real region $\mathscr{R}_+$, satisfying $\cup_{i=1}^{3} \mathscr{R}_i = \mathscr{R}_+$, $\mathscr{R}_i(k) \cap \mathscr{R}_j(k) = \varnothing$, $(i, j \in \{1, 2, 3\}, i \ne j)$.

Remark 2. The delayed control term $K_2 e(k - \tau_k)$ widens the feasible region of the synchronization control strategy, and we define the synchronization controller (14) running and sleeping states as the work region $\mathscr{R}_1(k)$ and the rest region $\mathscr{R}_2(k)$, respectively. In addition, we establish the holding region $\mathscr{R}_3(k)$ between the work region $\mathscr{R}_1(k)$ and the rest region $\mathscr{R}_2(k)$ in order to avoid the controller indefinitely cycling between $u(k) = 0$ and $u(k) = K_1 e(k) + K_2 e(k - \tau_k)$.

We substitute (14) into (10), which yields the model of the synchronization error dynamics as follows:

$$\begin{aligned}
e(k+1) = {} & \left(\widetilde{A} + \widetilde{L} + \widetilde{\mathscr{H}}_{1f} + K_1\right) e(k) + \widetilde{f}(e(k)) + K_2 \widetilde{\mathscr{H}}_{1g} (1 - \lambda(k))\pi(k) e(k - \tau(k))\\
& + K_2 (1 - \lambda(k))(1 - \pi(k)) e(k - \tau(k)) + K_2 (1 - \lambda(k))\pi(k)\widetilde{g}(e(k - \tau(k)))\\
& + \widetilde{h}(e(k)) + \widetilde{E}\widetilde{\omega}(k), \mathscr{V}(k) \in \mathscr{R}_1(k),
\end{aligned} \tag{15a}$$

$$e(k+1) = \left(\widetilde{A} + \widetilde{L} + \widetilde{\mathscr{H}}_{1f}\right) e(k) + \widetilde{f}(e(k)) + \widetilde{h}(e(k)) + \widetilde{E}\widetilde{\omega}(k), \mathscr{V}(k) \in \mathscr{R}_2(k), \tag{15b}$$

$$e(k+1) = \left(\widetilde{A} + \widetilde{L} + \widetilde{\mathscr{H}}_{1f}\right) e(k) + \widetilde{f}(e(k)) + \widetilde{h}(e(k)) + \widetilde{E}\widetilde{\omega}(k) + u(k-1), \mathscr{V}(k) \in \mathscr{R}_3(k). \tag{15c}$$

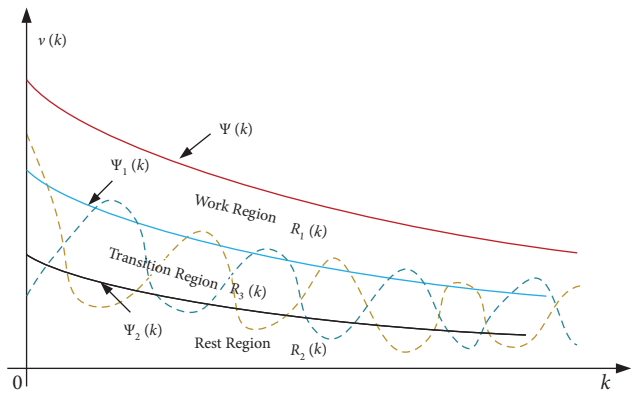

FIGURE 3: Illustration of the relations of Lyapunov-like function $\mathscr{V}(k)$ and regions $\mathscr{R}_i(k)\,(i=1,2,3)$.

In this paper, the relations of Lyapunov-like function $\mathscr{V}(k)$ and regions $\mathscr{R}_i(k)$ will be constructed for the intermittent synchronization controller, which is shown in Figure 3 where the earthy yellow line represents case $\mathscr{V}(k) \in \mathscr{R}_1(k)$ and the deep green line represents case $\mathscr{V}(k) \in \mathscr{R}_2(k) \cup \mathscr{R}_3(k)$, respectively.

According to the intermittent synchronization controller (14) and the synchronization error dynamics (15a)–(15c), the intermittent synchronization control strategy in this paper is given as follows:

(1) When Lyapunov-like function $\mathscr{V}(k) \in \mathscr{R}_1(k)$, then the intermittent synchronization controller (14) is activated, which means that the synchronization error dynamics (15a) work.

(2) When Lyapunov-like function $\mathscr{V}(k) \in \mathscr{R}_2(k)$, then the intermittent synchronization controller (14) is not activated, which means that the synchronization error dynamics (15b) do not work.

(3) When $k = k-1$, if Lyapunov-like function $\mathscr{V}(k) \in \mathscr{R}_3(k)$ and the synchronization error dynamics (15a) work, it means that the intermittent synchronization controller is activated.

(4) When $k = k-1$, if Lyapunov-like function $\mathscr{V}(k) \in \mathscr{R}_3(k)$ and the synchronization error dynamics (15b) work, it means that the intermittent synchronization controller is not activated.

In this paper, we consider the following forms of $\mathscr{R}_i(k)\,(i=1,2,3)$:

$$\begin{aligned}
\mathscr{R}_1(k) &= \left\{r \in \mathscr{R}_+ : r \geq \alpha_1 \mathscr{V}(0)\left(1-\gamma_1\right)^k + \beta_1\right\},\\
\mathscr{R}_2(k) &= \left\{r \in \mathscr{R}_+ : r < \alpha_2 \mathscr{V}(0)\left(1-\gamma_2\right)^k + \beta_2\right\},\\
\mathscr{R}_3(k) &= \frac{\mathscr{R}_+}{\left(\mathscr{R}_1(k) \cap \mathscr{R}_2(k)\right)},
\end{aligned} \tag{16}$$

where $\alpha_{1,2} > 0$, $\beta_{1,2} > 0$, and $0 < \gamma_{1,2} < 1$ are given positive scalars.

Next, we define the boundary of $\mathscr{R}_1(k)$ and $\mathscr{R}_3(k)$ as $\Psi_1(k)$ and the boundary of $\mathscr{R}_2(k)$ and $\mathscr{R}_3(k)$ as $\Psi_2(k)$, respectively. Then, it is obtained from (16) that

$$\begin{aligned}
\Psi_1(k) &= \left\{r \in \mathscr{R}_+ : r = \alpha_1 \mathscr{V}(0)\left(1-\gamma_1\right)^k + \beta_1\right\},\\
\Psi_2(k) &= \left\{r \in \mathscr{R}_+ : r = \alpha_2 \mathscr{V}(0)\left(1-\gamma_2\right)^k + \beta_2\right\},
\end{aligned} \tag{17}$$

where $\mathscr{R}_3(k) \neq \varnothing$ and $\mathscr{R}_i(k) \cap \mathscr{R}_j(k) = \varnothing\,(i,j \in \{1,2,3\}, i \neq j)$. It is assumed that the following conditions hold in this paper:

$$\alpha_1 \mathscr{V}(0)\left(1-\gamma_1\right)^k + \beta_1 > \alpha_2 \mathscr{V}(0)\left(1-\gamma_2\right)^k + \beta_2. \tag{18}$$

To satisfy condition (15a), we can assume that (1) $\alpha_1 > \alpha_2$, $\beta_1 > \beta_2$, $\gamma_1 \leq \gamma_2$; or (2) $\beta_1 > \alpha_2 + \beta_2$; or (3) $\alpha_1 = \alpha_2$, $\beta_1 > \beta_2$, $\gamma_1 < \gamma_2$.

Then, the definition of synchronization is introduced as follows.

Definition 1 (see [12]). For the given scalars $\sigma < 0$ and $\varsigma > 0$, if there exists a scalar $\delta > 0$, the following inequality holds:

$$\|e(k)\|^2 \leq \frac{((1-\sigma)\varsigma + \delta)}{\lambda_{\min}(P)}. \tag{19}$$

Then, the synchronization error dynamics (15a)–(15c) is ultimately bounded.

3. Main Results

Firstly, we define the piecewise Lyapunov-like function as follows:

$$\mathscr{V}(k) = \mathscr{V}_1(k) + \mathscr{V}_2(k) + \mathscr{V}_3(k), \tag{20}$$

where

$$\begin{aligned}
\mathscr{V}_1(k) &= e^T(k) P e(k),\\
\mathscr{V}_2(k) &= \sum_{i=k-\tau(k)}^{k-1} (1-\rho)^{k-i-1} e^T(i) Q e(i),
\end{aligned} \tag{21}$$

and

$$\mathscr{V}_3(k) = \sum_{j=k-\tau_m+1}^{k-\tau_m} \sum_{i=j}^{k-1} (1-\rho)^{k-i-1} e^T(i) Q e(i), \tag{22}$$

and $0 < \rho < 1$, $0 < P \in \mathbb{R}^{n\times n}$, and $0 < Q \in \mathbb{R}^{n\times n}$.

Theorem 1. *Let the FDI attacks probability $0 < \pi < 1$, the DoS attacks probability $0 < \lambda < 1$, the scalars $\delta > 0$, $\sigma < 0$, $0 < \gamma_1 < \rho < 1$, $0 < \gamma_2 < \rho < 1$, and $\beta_2 > (\delta/\rho)$, and the synchronization control gain matrices K_i, $(i = 1,2)$ be given. If there exist the definite matrices $0 < P \in \mathbb{R}^{n\times n}$ and $0 < Q \in \mathbb{R}^{n\times n}$ and the positive scalars $\mu_1 > 0$, $\mu_2 > 0$, and $\mu_3 > 0$, the following matrices inequalities hold:*

$$\Xi_1 = \begin{bmatrix} \Omega & \Pi_1^T \\ * & -P^{-1} \end{bmatrix} < 0, \tag{23}$$

$$\Xi_2 = \begin{bmatrix} \Omega & \Pi_2^T \\ * & -P^{-1} \end{bmatrix} < 0, \tag{24}$$

where

$$\Pi_1 = \left[P\left(\tilde{A} + \tilde{L} + \tilde{\mathscr{H}}_{1f} + K_1\right) \;\; P\left(K_2\tilde{\mathscr{H}}_{1g}(1-\lambda)\pi + K_2(1-\lambda)(1-\pi)\right)P \;\; PK_2(1-\lambda)\pi \;\; P \;\; P\tilde{E} \right],$$
$$\Pi_2 = \left[P\left(\tilde{A} + \tilde{L} + \tilde{\mathscr{H}}_{1f}\right) \;\; 0 \;\; P \;\; 0 \;\; P \;\; P\tilde{E} \right],$$
$$\Omega = \begin{bmatrix} \Omega_{11} & 0 & \Omega_{13} & 0 & 0 & 0 \\ * & -(1-\rho)^{\tau_M}Q & 0 & \Omega_{24} & 0 & 0 \\ * & * & -2\mu_1 I & 0 & 0 & 0 \\ * & * & * & -2\mu_2 I & 0 & 0 \\ * & * & * & * & -2\mu_3 I & 0 \\ * & * & * & * & * & -I \end{bmatrix}, \tag{25}$$

and $\Omega_{11} = -\rho P + (1 + \tau_M - \tau_m)Q + \mu_3(\tilde{\mathscr{H}}_{1g}^T\tilde{\mathscr{H}}_{2g} + \tilde{\mathscr{H}}_{2g}^T\tilde{\mathscr{H}}_{1g})$, $\Omega_{13} = \mu_1(\tilde{\mathscr{H}}_{2f} - \tilde{\mathscr{H}}_{1f})^T$, *and* $\Omega_{24} = \mu_2\ (\tilde{\mathscr{H}}_{2g} - \tilde{\mathscr{H}}_{1g})^T$.

Then, the synchronization error converges to $\|e(k)\|^2 \le ((1-\sigma)\beta_1 + \delta)/\lambda_{\min}(P)$ under the intermittent synchronization control mechanism (12), which means that the synchronization error dynamics are ultimately bounded.

Proof of Theorem 1. Let $\Delta\mathscr{V}(k) = \mathscr{V}(k+1) - \mathscr{V}(k)$, and the forward difference along the trajectory of synchronization error dynamics (15a) can be calculated as

$$\begin{aligned} \Delta\mathscr{V}(k) &= e^T(k+1)Pe(k+1) - e^T(k)Pe(k) + (\tau_M - \tau_m + 1)e^T(k)Qe(k) \\ &\quad - (1-\rho)^{\tau(k)}e^T(k-\tau_k)Pe(k-\tau_k) + \rho e^T(k)Qe(k) - \rho\mathscr{V}(k) \\ &\le e^T(k+1)Pe(k+1) - e^T(k)Pe(k) + (\tau_M - \tau_m + 1)e^T(k)Qe(k) \\ &\quad - (1-\rho)^{\tau_M}e^T(k-\tau_k)Pe(k-\tau_k) + \rho e^T(k)Qe(k) - \rho\mathscr{V}(k). \end{aligned} \tag{26}$$

For any scalar $\mu_i > 0$, $(i = \{1,2,3\})$, it follows from (11) that

$$-2\mu_1\tilde{f}(e(k))^T\left[\tilde{f}(e(k)) - \left(\tilde{\mathscr{H}}_{2f} - \tilde{\mathscr{H}}_{1f}\right)e(k)\right] \ge 0, \tag{27}$$

$$-2\mu_2\tilde{g}(e(k-\tau_k))^T\left[\tilde{g}(e(k-\tau_k)) - \left(\tilde{\mathscr{H}}_{2g} - \tilde{\mathscr{H}}_{1g}\right)e(k-\tau_k)\right] \ge 0, \tag{28}$$

$$-2\mu_3\left[\tilde{h}(e(k)) - \tilde{\mathscr{H}}_{1h}e(k)\right]^T\left[\tilde{h}(e(k)) - \tilde{\mathscr{H}}_{2h}e(k)\right] \ge 0. \tag{29}$$

Substituting (27)–(29) into (17), one eventually obtains

$$\begin{aligned} \Delta\mathscr{V}(k) + \rho\mathscr{V}(k) &\le e^T(k+1)Pe(k+1) - e^T(k)Pe(k) + (\tau_M - \tau_m + 1)e^T(k)Qe(k) \\ &\quad - (1-\rho)^{\tau_M}e^T(k-\tau_k)Pe(k-\tau_k) + \rho e^T(k)Qe(k) - 2\mu_1\tilde{f}(e(k))^T\left[\tilde{f}(e(k)) - \left(\tilde{\mathscr{H}}_{2f} - \tilde{\mathscr{H}}_{1f}\right)e(k)\right] \\ &\quad - 2\mu_2\tilde{g}(e(k-\tau_k))^T\left[\tilde{g}(e(k-\tau_k)) - \left(\tilde{\mathscr{H}}_{2g} - \tilde{\mathscr{H}}_{1g}\right)e(k-\tau_k)\right] \\ &\quad - 2\mu_3\left[\tilde{h}(e(k)) - \tilde{\mathscr{H}}_{1h}e(k)\right]^T\left[\tilde{h}(e(k)) - \tilde{\mathscr{H}}_{2h}e(k)\right] \\ &\le \zeta^T(k)\left(\Omega + \Pi_1^T P\Pi_1\right)\zeta(k) + \tilde{\omega}^T(k)\tilde{\omega}(k), \end{aligned} \tag{30}$$

where $\zeta(k) = \left[e^T(k) \;\; e^T(k-\tau_k) \;\; \tilde{f}^T(e(k)) \;\; \tilde{g}^T(e(k-\tau_k)) \;\; \tilde{h}^T(e(k)) \;\; \tilde{\omega}^T(k) \right]$.

Applying Schur complement lemma to (15c), it is clear that $\Omega + \Pi_1^T P\Pi_1 < 0$. We substitute $\Omega + \Pi_1^T P\Pi_1 < 0$ and (8) into (23), which yields

$$\Delta\mathscr{V}(k)+\rho\mathscr{V}(k)\le\delta. \tag{31}$$

By using the similar method, the forward difference $\Delta\mathscr{V}(k)=\mathscr{V}(k+1)-\rho\mathscr{V}(k)$ is determined along with the trajectory of synchronization error dynamics (15b).

$$\begin{aligned}\Delta\mathscr{V}(k)&=e^T(k+1)Pe(k+1)-e^T(k)Pe(k)+(\tau_M-\tau_m+1)e^T(k)Qe(k)\\&\quad-(1-\rho)^{\tau(k)}e^T(k-\tau_k)Pe(k-\tau_k)+\rho e^T(k)Qe(k)-\rho(\mathscr{V}_1(k)+\mathscr{V}_2(k))\\&\le e^T(k+1)Pe(k+1)-e^T(k)Pe(k)+(\tau_M-\tau_m+1)e^T(k)Qe(k)\\&\quad-(1-\rho)^{\tau_M}e^T(k-\tau_k)Pe(k-\tau_k)+\rho e^T(k)Qe(k)-\rho(\mathscr{V}_1(k)+\mathscr{V}_2(k)).\end{aligned} \tag{32}$$

Substituting (18)–(20) into (23), one eventually obtains

$$\begin{aligned}\Delta\mathscr{V}(k)+\rho(\mathscr{V}_1(k)+\mathscr{V}_2(k))&\le e^T(k+1)Pe(k+1)-e^T(k)Pe(k)\\&\quad+(\tau_M-\tau_m+1)e^T(k)Qe(k)-(1-\rho)^{\tau_M}e^T(k-\tau_k)Pe(k-\tau_k)\\&\quad+\rho e^T(k)Qe(k)-2\mu_1\tilde{f}(e(k))^T\left[\tilde{f}(e(k))-\left(\tilde{\mathscr{H}}_{2f}-\tilde{\mathscr{H}}_{1f}\right)e(k)\right]\\&\quad-2\mu_2\tilde{g}(e(k-\tau_k))^T\left[\tilde{g}(e(k-\tau_k))-\left(\tilde{\mathscr{H}}_{2g}-\tilde{\mathscr{H}}_{1g}\right)e(k-\tau_k)\right]\\&\quad-2\mu_3\left[\tilde{h}(e(k))-\tilde{\mathscr{H}}_{1h}e(k)\right]^T\left[\tilde{h}(e(k))-\tilde{\mathscr{H}}_{2h}e(k)\right]\\&\le\zeta^T(k)\left(\Omega+\Pi_2^TP\Pi_2\right)\zeta(k)+\tilde{\omega}^T(k)\tilde{\omega}(k).\end{aligned} \tag{33}$$

Applying Schur complement lemma to (16), it is clear that $\Omega+\Pi_2^TP\Pi_2<0$. Substituting $\Omega+\Pi_2^TP\Pi_2<0$ and (8) into (24), one has

$$\Delta\mathscr{V}(k)+\rho(\mathscr{V}_1(k)+\mathscr{V}_2(k))\le\delta. \tag{34}$$

According to (22), it is obtained that

$$\begin{aligned}\mathscr{V}(k)&\le(1-\rho)\mathscr{V}(k-1)+\delta\le(1-\rho)^2\mathscr{V}(k-2)+(1-\rho)\delta\\&\quad+\delta\le\cdots\le(1-\rho)^{k-i}\mathscr{V}(i)+\frac{\left(1-(1-\rho)^{k-i}\right)\delta}{\rho},\end{aligned} \tag{35}$$

which means that

$$\mathscr{V}(k)\le\left[\mathscr{V}(i)-\frac{\delta}{\rho}\right](1-\rho)^{k-i}+\frac{\delta}{\rho}. \tag{36}$$

From (25), it is directly obtained that

$$\Delta\mathscr{V}(k)+\sigma\mathscr{V}(k)\le\delta-\rho(\mathscr{V}_1(k)+\mathscr{V}_2(k))+\sigma(\mathscr{V}_1(k)+\mathscr{V}_2(k)+\mathscr{V}_3(k)). \tag{37}$$

Noting that $\sigma<0$ and $0<\rho<1$, we can obtain from (28) that

$$\Delta\mathscr{V}(k)+\sigma\mathscr{V}(k)\le\delta+(\sigma-\rho)(\mathscr{V}_1(k)+\mathscr{V}_2(k))\le\delta. \tag{38}$$

Similarly, from (29), it is directly obtained that

$$\mathscr{V}(k)\le\left[\mathscr{V}(i)-\frac{\delta}{\sigma}\right](1-\sigma)^{k-i}+\frac{\delta}{\sigma}. \tag{39}$$

In this paper, for $\forall k\in\mathcal{N}[0,+\infty)$, we assume that there exist switchings between the synchronization error dynamics (15a) and (15b) according to the following procedure:

(1) When Lyapunov-like function $\mathscr{V}(k)\in\mathscr{R}_1(k)$, the intermittent synchronization controller $u(k)=K_1e(k)+K_2e(k-\tau_k)$ is activated, which means that the synchronization error dynamics (15a) work at the initial time $k=0$. At the same time, because of the scalars $\rho>\gamma_1$, $\rho>\gamma_2$, and $\beta_1>\beta_2>\delta/\rho$, there must exist a time k_1 ($k_1\ge1$) that guarantees the trajectory of Lyapunov-like function $\mathscr{V}(k)$ evolution to the rest region $\mathscr{R}_2(k)$.

(2) When Lyapunov-like function $\mathscr{V}(k) \in \mathscr{R}_2(k)$, then the intermittent synchronization controller $u(k) = 0$ is activated, which means that the synchronization error dynamics (15b) work at the time $k_1 (k_1 \geq 1)$. Simultaneously, in order to avoid the trajectory of Lyapunov-like function $\mathscr{V}(k)$ stay in $\mathscr{R}_2(k)$ or $\mathscr{R}_3(k)$ for all $k > k_1$, there must exist a time $k_2 (k_2 > k_1)$ that guarantees the trajectory of Lyapunov-like function $\mathscr{V}(k)$ evolution to the rest region $\mathscr{R}_1(k)$.

According to the above procedure, we assume that all work time and rest time of the intermittent synchronization controller are $\mathscr{K}_1 = \mathscr{N}[0, k-1] \cup (\cup_{i=0}^{+\infty} \mathscr{N}[k_{2i+1}, k_{2(i+1)} - 1])$ and $\mathscr{K}_2 = \cup_{i=0}^{+\infty} \mathscr{N}[k_{2i+1}, k_{2(i+1)} - 1]$, respectively.

For $\forall k \in \mathscr{K}_1$, the synchronization error dynamics (15a) are active. According to (27), one has

$$\mathscr{V}(k) \leq \left[\mathscr{V}(0) - \frac{\delta}{\rho}\right](1-\rho)^k + \frac{\delta}{\rho}, \forall k \in \mathscr{N}[0, k_1 - 1], \tag{40}$$

and

$$\mathscr{V}(k) \leq \left[\mathscr{V}\left(k_{2(i+1)}\right) - \frac{\delta}{\rho}\right](1-\rho)^{k-k_{2(i+1)}} + \frac{\delta}{\rho}, \forall k \in \mathscr{N}\left[k_{2(i+1)}, k_{2i+3} - 1\right]. \tag{41}$$

Note that $\mathscr{V}(k) = \mathscr{R}_2(k) \cup \mathscr{R}_3(k)$ at $k = k_{2(i+1)} - 1$, which yields $\mathscr{V}(k_{2(i+1)} - 1) < \alpha_1 \mathscr{V}(0)(1-\gamma_1)^{k_{2(i+1)}-1} + \beta_1$. Then, it is obtained from (30) that

$$\begin{aligned} \mathscr{V}\left(k_{2(i+1)} - 1\right) &\leq \left[\mathscr{V}\left(k_{2(i+1)} - 1\right) - \frac{\delta}{\sigma}\right](1-\sigma) + \frac{\delta}{\sigma} \leq \left[\alpha_1 \mathscr{V}(0)(1-\gamma_1)^{k_{2(i+1)}-1} + \beta_1 - \frac{\delta}{\sigma}\right] \\ &(1-\sigma) + \frac{\delta}{\sigma} = \alpha_1 \mathscr{V}(0)\left(\frac{1-\sigma}{1-\gamma_1}\right)(1-\gamma_1)^{k_{2(i+1)}-1} + \beta_1(1-\sigma) + \delta. \end{aligned} \tag{42}$$

Substituting (33) into (32), for $\forall k \in \cup_{i=0}^{+\infty} \mathscr{N}[k_{2(i+1)}, k_{2i+3} - 1]$, it is obtained that

$$\begin{aligned} \mathscr{V}(k) &\leq \left[\alpha_1 \mathscr{V}(0)\left(\frac{1-\sigma}{1-\gamma_1}\right)(1-\gamma_1)^{k_{2(i+1)}-1} + \beta_1(1-\sigma) + \delta - \frac{\delta}{\rho}\right](1-\rho)^{k-k_{2(i+1)}} + \frac{\delta}{\rho} \\ &= \alpha_1 \mathscr{V}(0)\left(\frac{1-\sigma}{1-\gamma_1}\right)(1-\gamma_1)^{k_{2(i+1)}-1}(1-\rho)^{k-k_{2(i+1)}} + \left[(1-\sigma)\beta_1 - \frac{\delta(1-\rho)}{\rho}\right](1-\rho)^{k-k_{2(i+1)}} + \frac{\delta}{\rho}. \end{aligned} \tag{43}$$

Note that $\beta_2 > (\delta/\rho)$ and $0 < \gamma_1 < \rho < 1$, then $\forall k \in \mathscr{N}[k_{2(i+1)}, k_{2i+3} - 1]$. It is obtained from (33) that

$$\mathscr{V}(k) \leq \alpha_1 \mathscr{V}(0)\left(\frac{1-\sigma}{1-\gamma_1}\right)(1-\gamma_1)^k + \beta_1(1-\sigma) + \delta. \tag{44}$$

Furthermore, for $\forall k \in \mathscr{K}_2$ and $\mathscr{V}(k) = \mathscr{R}_2(k) \cup \mathscr{R}_3(k)$, $\mathscr{V}(k) \leq \alpha_1 V_1(0)(1-\gamma_1)^k + \beta_1$ holds. Then, from $\mathscr{K}_1 \cup \mathscr{K}_2 \in \mathscr{N}[0, +\infty)$, one has

$$\mathscr{V}(k) \leq \begin{cases} \left[\mathscr{V}(0) - \dfrac{\delta}{\rho}\right](1-\rho)^k + \dfrac{\delta}{\rho}, \forall k \in \mathscr{N}[0, k_1 - 1], \\ \alpha_1 \mathscr{V}(0)\left(\dfrac{1-\sigma}{1-\gamma_1}\right)(1-\gamma_1)^k + \beta_1(1-\sigma) + \delta, \forall k \in \mathscr{N}[k_1, +\infty). \end{cases} \tag{45}$$

Similarly, for $\forall k \in \mathcal{N}[0, +\infty)$, we assume that there exist switchings between the synchronization error dynamics (15a) and (15b) according to the following procedure:

(1) When Lyapunov-like function $\mathcal{V}(k) \in \mathcal{R}_2(k) \cup \mathcal{R}_3(k)$, the intermittent synchronization controller $u(k) = 0$ is activated, which means that the closed-loop synchronization error dynamics (15b) work at the initial time $k = 0$. Therefore, there must exist a time $k_1 (k_1 \geq 1)$ that guarantees the trajectory of Lyapunov-like function $\mathcal{V}(k)$ evolution to the rest region $\mathcal{R}_1(k)$.

(2) When Lyapunov-like function $\mathcal{V}(k) \in \mathcal{R}_1(k)$, then the intermittent synchronization controller $u(k) = K_1 e(k) + K_2 e(k - \tau_k)$ is activated, which means that the closed-loop synchronization error dynamics (15a) work at time $k_1 (k_1 \geq 1)$. Simultaneously, for the scalars $\rho > \gamma_1$, $\rho > \gamma_2$, and $\beta_1 \geq \beta_2 > \delta/\rho$, there must exist a time $k_2 (k_2 > k_1)$ that guarantees the trajectory of Lyapunov-like function $\mathcal{V}(k)$ evolution to the rest region $\mathcal{R}_2(k)$.

Similar to the analysis of the first case, we define $\widetilde{\mathcal{K}}_1 = \cup_{i=0}^{+\infty} \mathcal{N}[k_{2i+1}, k_{2(i+1)} - 1]$ and $\widetilde{\mathcal{K}}_2 = \mathcal{N}[0, k-1] \cup (\cup_{i=0}^{+\infty} \mathcal{N}[k_{2i+1}, k_{2(i+1)} - 1])$ as the work time and the rest time, respectively.

Then, for $\forall k \in \widetilde{\mathcal{K}}_1$ and $\widetilde{\mathcal{K}}_1 \cup \widetilde{\mathcal{K}}_2 \in \mathcal{N}[0, +\infty)$, according to (35) and noting the fact $\mathcal{V}(k) \leq \alpha_1 \mathcal{V}(0)(1-\gamma_1)^k + \beta_1$, $(\mathcal{V}(k) \in \mathcal{R}_2(k) \cup \mathcal{R}_3(k))$, one has

$$\mathcal{V}(k) \leq \alpha_1 \mathcal{V}(0) \left(\frac{1-\sigma}{1-\gamma_1}\right)(1-\gamma_1)^k + \beta_1(1-\sigma) + \delta, \forall k \in \mathcal{N}[0, +\infty). \tag{46}$$

From (36) and (37) and noting the facts $\mathcal{V}(k) \geq e^T(k) P e(k) \geq \lambda_{\min}(P) \|e(k)\|^2$, one has

$$\begin{aligned} \|e(k)\|^2 &\leq \frac{\left(\alpha_1 \mathcal{V}(0)(1-\sigma/1-\gamma_1)(1-\gamma_1)^k + \beta_1(1-\sigma) + \delta\right)}{\lambda_{\min}(P)} \\ &\leq \frac{\left((1-\sigma)\beta_1 + \delta\right)}{\lambda_{\min}(P)}. \end{aligned} \tag{47}$$

The proof is thus completed.

For the given parameterized synchronization control gains K_i $(i = 1, 2)$, Theorem 1 provides sufficient conditions for ensuring the bounded of the synchronization error dynamics (13). Considering the LMI (19), it is easy to find that there is certain relationship between the control gains K_i and the synchronization control performance, and the value of control gains K_i would affect the feasibility of the LMI (19). Now, we are in the position of designing the synchronization control gains K_i on the basis of Theorem 1. □

Theorem 2. *Let the FDI attacks probability $0 < \pi < 1$, the DoS attacks probability $0 < \lambda < 1$, and the scalars $\delta > 0$, $\sigma < 0$, $0 < \gamma_1 < \rho < 1$, $0 < \gamma_2 < \rho < 1$, and $\beta_2 > (\delta/\rho)$, and the synchronization control gain matrices K_i, $(i = 1, 2)$ be given. If there exist the matrices $0 < P \in \mathbb{R}^{n \times n}$, $0 < Q \in \mathbb{R}^{n \times n}$, and $0 < X_i \in \mathbb{R}^{n \times n}$ $(i = 1, 2)$ and the positive scalars $\mu_1 > 0$, $\mu_2 > 0$, and $\mu_3 > 0$, the following matrix inequalities hold:*

$$\widetilde{\Xi}_1 = \begin{bmatrix} \Omega & \widetilde{\Pi}_1^T \\ * & -P^{-1} \end{bmatrix} < 0, \tag{48}$$

$$\Xi_2 = \begin{bmatrix} \Omega & \Pi_2^T \\ * & -P^{-1} \end{bmatrix} < 0, \tag{49}$$

where

$$\widetilde{\Pi}_1 = \left[P\left(\widetilde{A} + \widetilde{L} + \widetilde{\mathscr{H}}_{1f}\right) + X_1 \quad X_2 \widetilde{\mathscr{H}}_{1g}(1-\lambda)\pi + X_2(1-\lambda)(1-\pi)P \quad X_2(1-\lambda)\pi \quad P \quad P\widetilde{E} \right]. \tag{50}$$

Then, the synchronization controller can be given by

$$K_i = P^{-1} X_i, (i = 1, 2), \tag{51}$$

which renders the closed-loop synchronization error dynamics (13) to be bounded, and the synchronization error converges to $\|e(k)\|^2 \leq ((1-\sigma)\beta_1 + \delta)/\lambda_{\min}(P)$.

Proof of Theorem 2. The variable substitution method is employed to prove this theorem. Let $PK_i = X_i$, $(i = 1, 2)$ and substitute it into (23)-(24), which yields (48)-(49). This completes the proof. □

Remark 3. Up to now, most of the existing results concerning complex networks are only subject to either cyber-attacks or time delays for the simplicity of analysis and design (see, e.g., [12, 21, 38]). Unfortunately, complex cyber-physical networks may be affected by the combined effects of cyber-attacks, physical attacks, and time delay in a control practice. It is worth noting that both FDI attacks and physical attacks may bring significant risks to some practical applications (e.g., electric power grids, the Internet of Things, and connected vehicles [31, 39]) due to their concealed characteristics. Furthermore, the time delay is another major constraint for the application of complex cyber-

physical networks, which will cause system performance degradation or even instability. Consequently, the proposed synchronous control method is an indispensable supplement to the existing results for complex cyber-physical networks with both time delays and mixed attacks.

Theorems 1 and 2 only provide sufficient conditions for ensuring the boundedness of the synchronization error dynamics for the simplicity of analysis. It is worth pointing out, however, that people are interested to obtain the minimized synchronization error as much as possible in the control practice. Therefore, we are providing an optimization strategy to minimize the synchronization error.

Assuming that there exists the minimized synchronization error δ_0, which enables $\|e(k)\|^2 \le \delta_0$. This means that the following inequality holds:

$$\|e(k)\|^2 \le \frac{((1-\sigma)\beta_1 + \delta)}{\lambda_{\min}(P)} \le \delta_0. \tag{52}$$

According to (41), we can obtain

$$\left(\frac{((1-\sigma)\beta_1 + \delta)}{\delta_0^2}\right) I \le \lambda_{\min}(P). \tag{53}$$

This means is that

$$\left(\frac{((1-\sigma)\beta_1 + \delta)}{\delta_0^2}\right) II^T \le P. \tag{54}$$

Applying Schur complement lemma to (43), it is clear that

$$\begin{bmatrix} P & I \\ * & \dfrac{\delta_0^2}{((1-\sigma)\beta_1 + \delta)} \end{bmatrix} \ge 0. \tag{55}$$

Therefore, we can provide an optimization problem to minimize the synchronization error δ_0 and determine positive definite matrices $P \in \mathbb{R}^{n\times n}$, $Q \in \mathbb{R}^{n\times n}$, and synchronization control gains K_i.

$$\min \delta_0, \tag{56}$$

subject to (38), (39), and (45), and the synchronization control gains can be determined by (44).

Remark 4. Subject to (38), (39), and (45), the synchronization control gains can be determined by (42). In this optimization problem, we further analyze the effects of the probability of mixed attacks on the synchronization error. Specifically, the probability of mixed attacks (the probabilities of the FDI attacks and DoS attacks are set as $\pi = 0.10$ and $\lambda = 0.20$, respectively) directly affects the upper limit of the synchronization error for discrete-delayed complex cyber-physical networks. A complex cyber-physical network that information of malicious attack usually results in a change in the synchronization error, such as the FDI attack and DoS attack (see [17, 21]). Note that the purpose of this optimization problem is interested to obtain the minimized synchronization error as much as possible.

Let us consider a special case where in the absence of input delay, the corresponding synchronization error dynamics can be written as follows:

$$\begin{aligned} e(k+1) &= \left(\widetilde{A} + \widetilde{L} + \widetilde{\mathscr{H}}_{1f}\right) e(k) + \widetilde{f}(e(k)) + \widetilde{h}(e_i(k)) + \widetilde{E}\widetilde{\omega}(k) + (1-\lambda(k))\pi(k)\widetilde{g}(u(k)), \\ e(\theta) &= \widetilde{\phi}(\theta), \theta \in (-\infty, 0]. \end{aligned} \tag{57}$$

Choose the following intermittent synchronization controller:

$$u(k) = \begin{cases} K_1 e(k) & \mathscr{V}(k) \in \mathscr{R}_1(k), \\ 0 & \mathscr{V}(k) \in \mathscr{R}_2(k), \\ u(k-1) & \mathscr{V}(k) \in \mathscr{R}_3(k), \end{cases} \tag{58}$$

and select the following Lyapunov function:

$$\mathscr{V}_1(k) = e^T(k) P e(k). \tag{59}$$

Then, it is easy to obtain the following result.

Corollary 1. *Let the FDI attacks probability $0 < \pi < 1$, the DoS attacks probability $0 < \lambda < 1$, and the scalars $\delta > 0$, $\sigma < 0$, $0 < \gamma_1 < \rho < 1$, $0 < \gamma_2 < \rho < 1$, and $\beta_2 > (\delta/\rho)$, and the synchronization control gain matrices K_i, $(i = 1, 2)$ be given. If there exist the matrices $0 < P \in \mathbb{R}^{n\times n}$, $0 < Q \in \mathbb{R}^{n\times n}$, and $0 < X \in \mathbb{R}^{n\times n}$ and the positive scalars $\mu_1 > 0$, $\mu_2 > 0$, and $\mu_3 > 0$, such that the following matrices inequalities hold:*

$$\begin{aligned} \Xi_1 &= \begin{bmatrix} \Omega & \Pi_1^T \\ * & -P^{-1} \end{bmatrix} < 0, \\ \Xi_2 &= \begin{bmatrix} \Omega & \Pi_2^T \\ * & -P^{-1} \end{bmatrix} < 0, \end{aligned} \tag{60}$$

where

$$\Pi_1 = \left[P\left(\tilde{A} + \tilde{L} + \tilde{\mathscr{H}}_{1f} + \tilde{\mathscr{H}}_{1g}(1-\lambda)\pi + (1-\lambda)(1-\pi)I\right) + X \;\; P \;\; (1-\lambda)\pi IP \;\; P\tilde{E} \right],$$
$$\Pi_2 = \left[P\left(\tilde{A} + \tilde{L} + \tilde{\mathscr{H}}_{1f} + \tilde{\mathscr{H}}_{1g}(1-\lambda)\pi + (1-\lambda)(1-\pi)I\right) \;\; P \;\; (1-\lambda)\pi IP \;\; P\tilde{E} \right],$$
$$\Omega = \begin{bmatrix} \Omega_{11} & \Omega_{12} & 0 & 0 & 0 \\ * & -2\mu_1 I & \Omega_{23} & 0 & 0 \\ * & * & -2\mu_2 I & 0 & 0 \\ * & * & * & -2\mu_3 I & 0 \\ * & * & * & * & -I \end{bmatrix}, \tag{61}$$

and $\Omega_{11} = -P + \mu_3(\tilde{\mathscr{H}}_{1g}^T \tilde{\mathscr{H}}_{2g} + \tilde{\mathscr{H}}_{2g}^T \tilde{\mathscr{H}}_{1g})$, $\Omega_{12} = \mu_1(\tilde{\mathscr{H}}_{2f} - \tilde{\mathscr{H}}_{1f})^T$, *and* $\Omega_{23} = \mu_2(\tilde{\mathscr{H}}_{2g} - \tilde{\mathscr{H}}_{1g})^T$.

Then, the synchronization controller can be given by

$$K = P^{-1}X, \tag{62}$$

which renders the closed-loop synchronization error dynamics (47) to be bounded, and the synchronization error converges to $\|e(k)\|^2 \le ((1-\sigma)\beta_1 + \delta)/\lambda_{\min}(P)$.

Proof of Corollary 1. The proof of this corollary can be obtained directly from that of Theorems 1 and 2. □

Remark 5. Till now, a systematic study has been conducted on the intermittent synchronization control problem for complex cyber-physical networks under mixed attacks. Theorems 1 and 2 provide sufficient conditions for the synchronization error to be bounded. Then, we developed an optimization problem to obtain minimize the synchronization error. In addition, for complex cyber-physical networks with constant delay and mixed attacks, the corresponding results can be readily obtained by revising the Lyapunov functional and synchronization error dynamics.

4. Numerical Simulations

In this section, two numerical examples are given to verify the effectiveness and superiority of the proposed synchronization control strategy.

Example 1. We consider a delayed complex cyber-physical network of the form (1), which is composed of three identical nodes with the following parameters:

$$A = \begin{bmatrix} -0.5 & 0.2 \\ 0 & 0.95 \end{bmatrix}, f(x) = \begin{bmatrix} \tanh(x_1) \\ \tanh(x_2) \end{bmatrix},$$
$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tau_k = 9 + \frac{\left[1 + (-1)^k\right]}{2}. \tag{63}$$

The inner-coupling matrix is set as $\Gamma = 0.3I$, and the outer-coupling matrices L is given as follows:

$$L = \begin{bmatrix} -0.1 & 0 & 0.1 \\ 0 & -0.1 & 0.1 \\ 0.1 & 0.1 & -0.2 \end{bmatrix}. \tag{64}$$

Assumption 1 is easily verified by using

$$\mathscr{H}_{1f} = \begin{bmatrix} 0 & 0 \\ 0 & -0.75 \end{bmatrix}, \mathscr{H}_{2f} = \begin{bmatrix} 0.2 & 0 \\ 0 & 0 \end{bmatrix},$$
$$\mathscr{H}_{1g} = \mathscr{H}_{1h} = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix}, \mathscr{H}_{2g} = \mathscr{H}_{2h} = \begin{bmatrix} 0.2 & 0 \\ 0 & 0.1 \end{bmatrix}. \tag{65}$$

The probabilities of the FDI attacks and DoS attacks are set as $\pi = 0.10$ and $\lambda = 0.20$, respectively, and the FDI attacks and physical attacks have the following forms:

$$g(x) = \left[\tanh\left(0.25x_1(k)\right) \;\; \tanh\left(0.15x_2(k)\right) \right]^T,$$
$$h(x) = \left[\tanh\left(0.04x_1(k)\right) \;\; \tanh\left(0.05x_2(k)\right) \right]^T. \tag{66}$$

The initial conditions of complex cyber-physical networks are set as $x_0 = \left[-1.5 \;\; 1.5 \right]$. Then, the FDI attacks and DoS attacks' times are shown in Figures 4 and 5, respectively, where "0" represents that cyber-attacks are not occurring, while "1" denotes that the network suffers from cyber-attacks. The energy evolution of physical attacks is given in Figure 6. Figures 7 and 8 plot the synchronization error trajectories of complex cyber-physical networks without control input, which show that the network node cannot be spontaneous synchronization with the unforced isolated node.

Let $\alpha_1 = 0.5$, $\alpha_2 = 0.3$, $\beta_1 = 0.12$, $\beta_2 = 0.09$, $\gamma_1 = 0.05$, $\gamma_2 = 0.06$, $\rho = 0.1$, and $\sigma = -2.4$, respectively. Then, Equation (15a) is satisfied for any $\mathscr{V}(k)$. Applying Theorem 2 and solving LMI (38), the corresponding synchronization control gains matrices can be obtained as follows:

$$K_{11} = \begin{bmatrix} 0.5198 & 0.0360 \\ -0.1736 & 0.1125 \end{bmatrix}, K_{12} = \begin{bmatrix} 1.7772 & 0.0741 \\ -0.1020 & 1.5021 \end{bmatrix},$$
$$K_{21} = \begin{bmatrix} 0.3404 & 0.0291 \\ -0.1822 & 0.3764 \end{bmatrix}, K_{22} = \begin{bmatrix} 1.8285 & 0.0974 \\ -0.0661 & 1.4433 \end{bmatrix}, \tag{67}$$
$$K_{31} = \begin{bmatrix} 0.4267 & 0.0206 \\ -0.0857 & 0.1124 \end{bmatrix}, K_{32} = \begin{bmatrix} 1.7809 & 0.0455 \\ -0.0551 & 1.4872 \end{bmatrix}.$$

According to the intermittent synchronization control mechanism (12), the intermittent synchronization controller $u(k) = K_1 e(k) + K_2 e(k - \tau_k)$ is activated when Lyapunov-

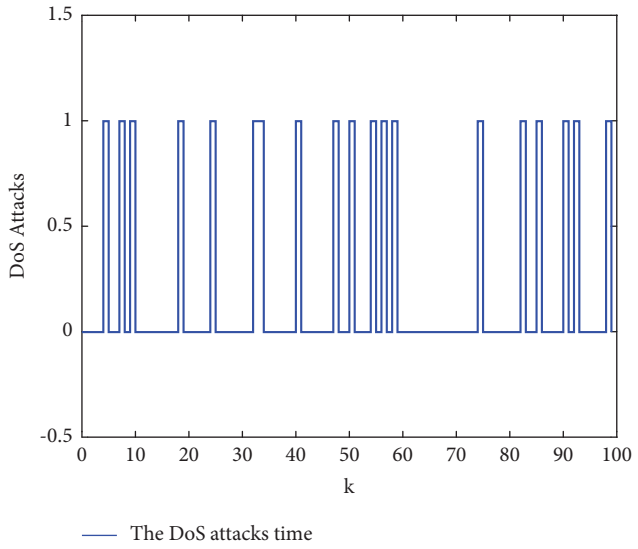

Figure 4: Attack time of the DoS attacks.

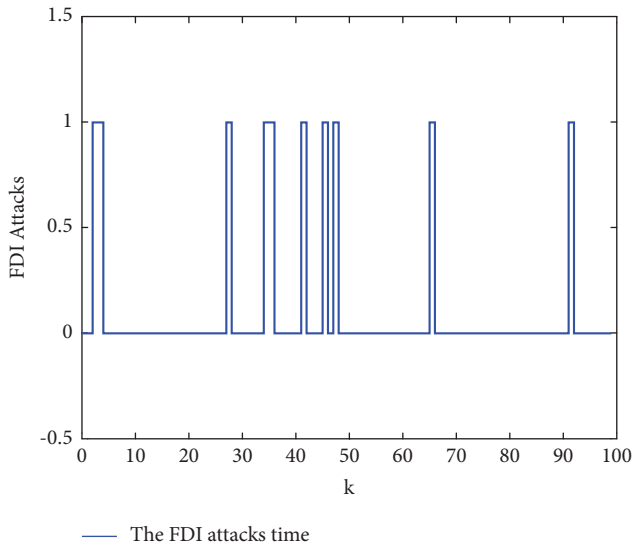

Figure 5: Attack time of the FDI attacks.

like function. The synchronization error trajectories of the network nodes under mixed attacks are given in Figures 9 and 10. It can be found from Figures 9 and 10 that synchronization errors can quickly converge within the limited sampling periods, which implies that the presented synchronization control method is effective for the discrete-time delayed complex cyber-physical networks with input delays and mixed attacks. Moreover, we choose an acceptable probability of cyber-attacks, by calculating the optimization problem (45), and then can easily obtain that the minimum upper bound $\delta_0 = 4.6026$ for the synchronization error.

In order to prove the superiority of the proposed synchronization control method, the state feedback synchronization control method [40] is utilized for complex

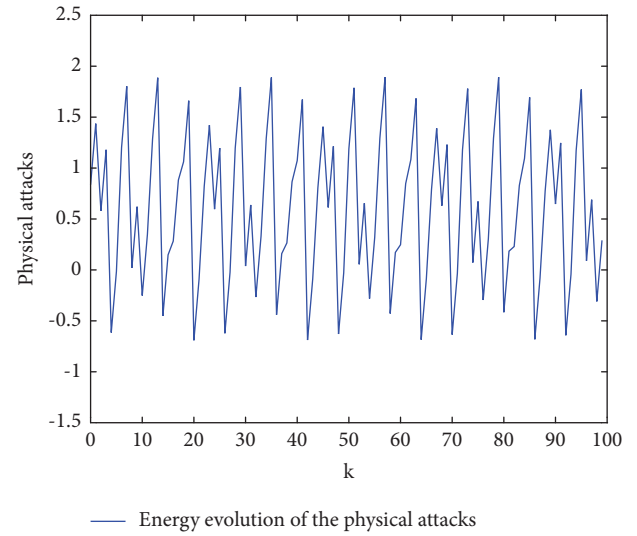

Figure 6: Energy evolution of the physical attacks.

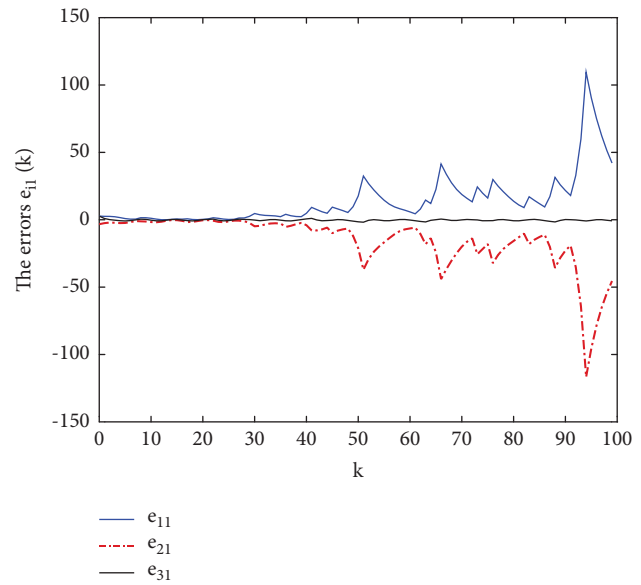

Figure 7: Synchronization error $e_{i1}(k)(i = 1, 2, 3)$ trajectories of the uncontrolled.

cyber-physical networks (1) in the same conditions. Figures 11 and 12 show the synchronization error trajectories of the network nodes under the control method of [40]. It can be seen from Figures 9–12 that the proposed synchronization control method has far lower synchronization error fluctuations than the method of [40], which shows that our control strategy can effectively reduce the negative impact of the mixed attacks and the input delays compared with the state feedback ones.

Example 2. Consider complex cyber-physical networks (1) consisting of three Chua's chaotic circuits [41] with the following parameters:

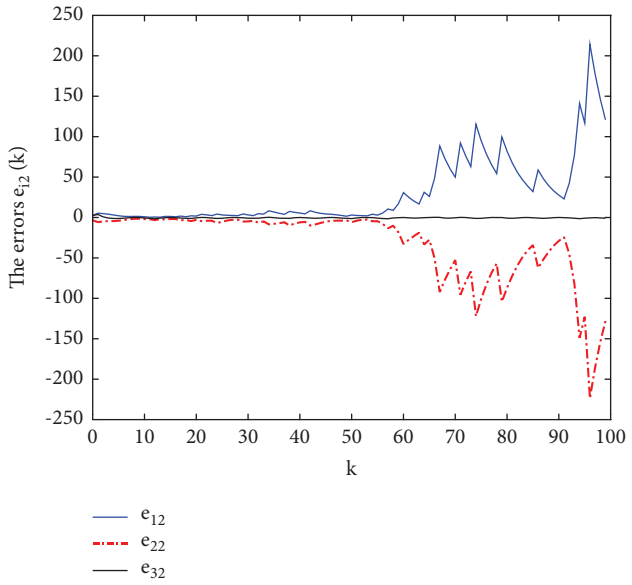

FIGURE 8: Synchronization error $e_{i2}(k)(i = 1, 2, 3)$ trajectories of the uncontrolled.

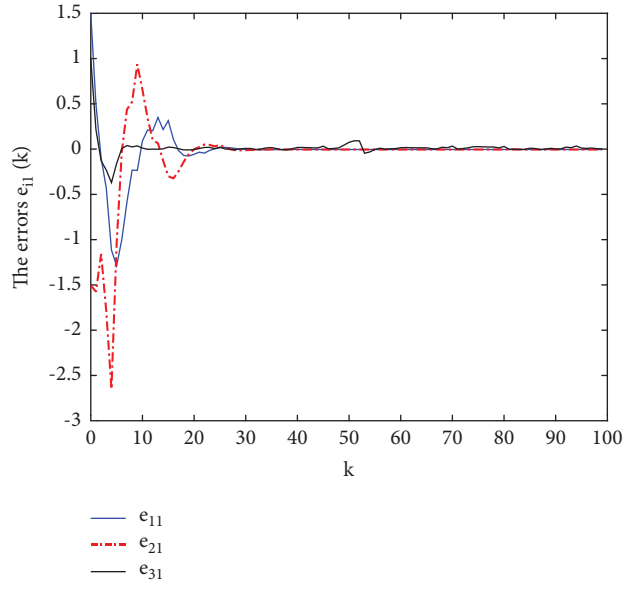

FIGURE 9: Synchronization error $e_{i1}(k)(i = 1, 2, 3)$ trajectories of the controlled.

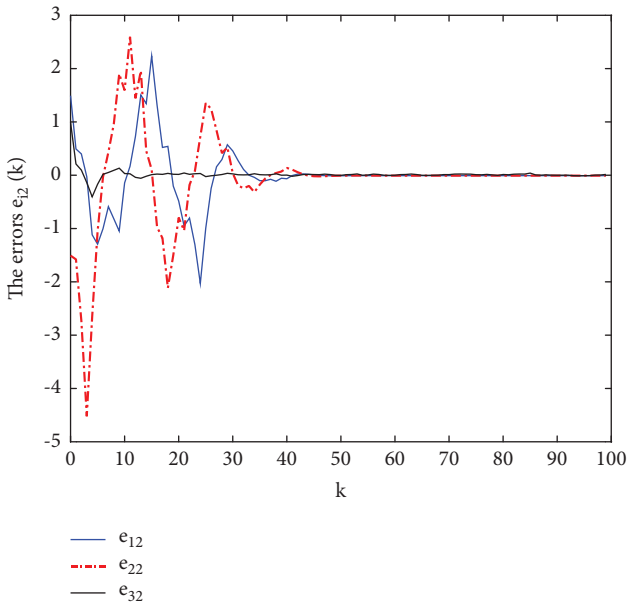

FIGURE 10: Synchronization error $e_{i2}(k)(i = 1, 2, 3)$ trajectories of the controlled.

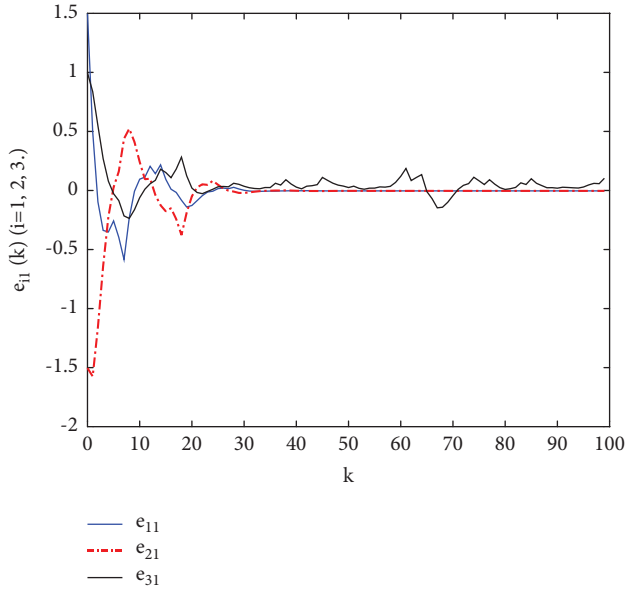

FIGURE 11: Synchronization error $e_{i1}(k)$, $(i = 1, 2, 3)$ trajectories of the control method in [40].

$$A = \begin{bmatrix} -cr & c & 0 \\ 1 & -1 & 1 \\ 0 & 14.28 & 0 \end{bmatrix}, f(x(k)) = \begin{bmatrix} 0.02\sin(x_1) & 0 & 0.01\tanh(x_1) \\ 0 & 0.02\cos(x_2) & 0 \\ 0 & 0 & 0.03\sin(x_3) \end{bmatrix}, \tag{68}$$

$$E = I, c = 9, r = \frac{2}{7}.$$

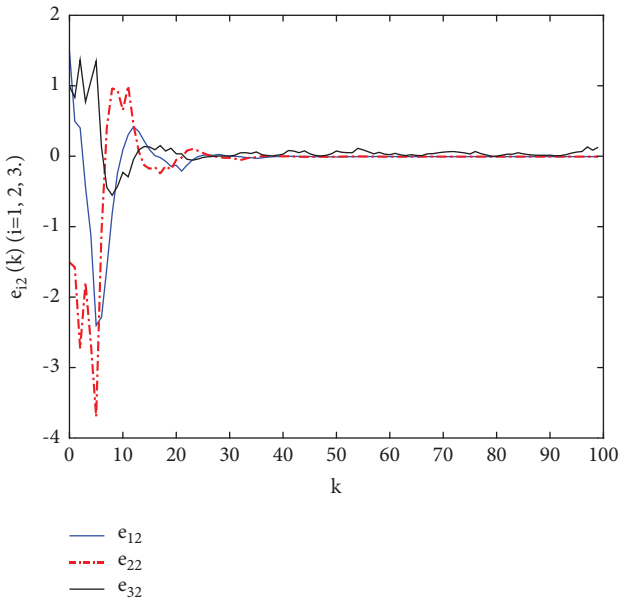

Figure 12: Synchronization error $e_{i2}(k)$, $(i = 1, 2, 3)$ trajectories of the control method in [40].

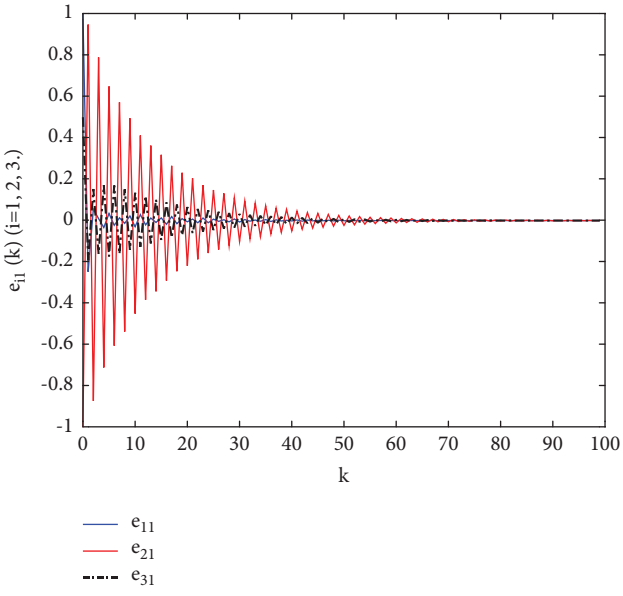

Figure 13: Synchronization error $e_{i1}(k)(i = 1, 2, 3)$ trajectories of the controlled.

The inner-coupling matrix is set as $\Gamma = 0.517I$, and the outer-coupling matrices L given as follows:

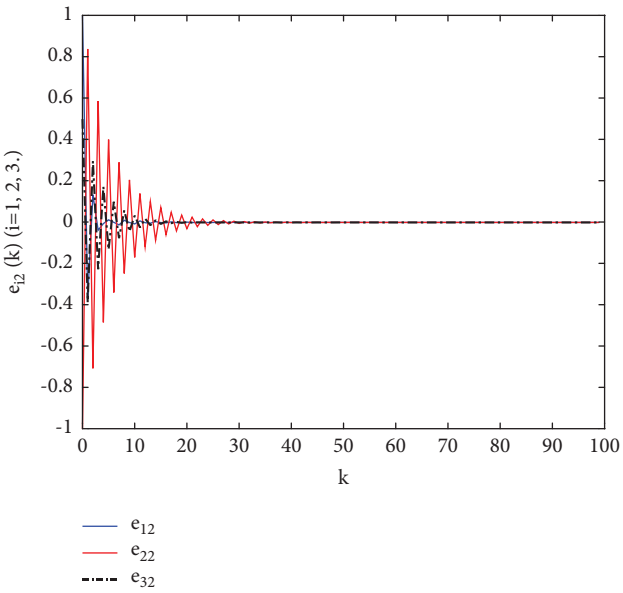

Figure 14: Synchronization error $e_{i2}(k)(i = 1, 2, 3)$ trajectories of the controlled.

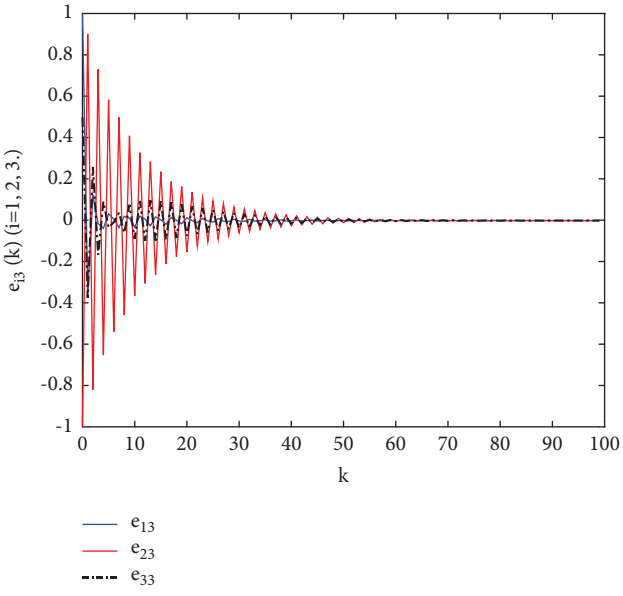

Figure 15: Synchronization error $e_{i3}(k)(i = 1, 2, 3)$ trajectories of the controlled.

$$L = \begin{bmatrix} -0.1 & 0 & 0.1 \\ 0 & -0.1 & 0.1 \\ 0.1 & 0.1 & -0.2 \end{bmatrix}, \tag{69}$$

and the time-delay boundaries are $\tau_m = 3$ and $\tau_M = 4$.

Assumption 1 is easily verified by using an improved directed crossover genetic algorithm based on multilayer mutation:

$$\begin{aligned}
\tilde{\mathscr{H}}_{1f} &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -0.75 \end{bmatrix}, \\
\tilde{\mathscr{H}}_{2f} &= \begin{bmatrix} 0.2 & 0 & 0 \\ 0 & -0.2 & 0 \\ 0 & 0 & 0.2 \end{bmatrix}, \\
\tilde{\mathscr{H}}_{1g} &= \tilde{\mathscr{H}}_{1h} = \begin{bmatrix} 0.1 & 0 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 0.1 \end{bmatrix}, \\
\tilde{\mathscr{H}}_{2g} &= \tilde{\mathscr{H}}_{2h} = \begin{bmatrix} 0.2 & 0 & 0 \\ 0 & -0.2 & 0 \\ 0 & 0 & 0.2 \end{bmatrix}.
\end{aligned} \tag{70}$$

We assume that the FDI attacks and physical attacks have the following form:

$$\begin{aligned}
g(x(k)) &= \begin{bmatrix} 0.02\sin(x_1) & 0 & 0 \\ 0 & 0.02\cos(x_2) & 0 \\ 0 & 0 & 0.03\sin(x_3) \end{bmatrix}, \\
h(x(k)) &= \begin{bmatrix} 0.02\sin(x_1) & -0.01\cos(x_1) & -0.01\tanh(x_1) \\ -0.02\sin(x_2) & 0 & 0 \\ 0 & 0 & 0.01\sin(x_3) \end{bmatrix}.
\end{aligned} \tag{71}$$

Let the other parameters be the same as in Example 1. Then, (15a) is satisfied for any $\mathscr{V}(k)$. Applying Theorem 2 and solving LMI (38), the corresponding synchronization control gains matrices can be obtained as follows:

$$\begin{aligned}
K_{11} &= \begin{bmatrix} 2.4698 & -9.0000 & -0.0000 \\ -1.0000 & 1.0000 & -1.0000 \\ -0.0000 & 14.2800 & 0.3596 \end{bmatrix}, K_{12} = \begin{bmatrix} 0.0214 & -0.0014 & 0.0136 \\ 0.0003 & 0.0006 & -0.0062 \\ -0.0290 & -0.0716 & -0.0138 \end{bmatrix}, \\
K_{21} &= \begin{bmatrix} 2.2055 & -9.0000 & 0.0000 \\ -1.0000 & 1.0786 & -1.0000 \\ -0.0000 & 14.2800 & -0.0262 \end{bmatrix}, K_{22} = \begin{bmatrix} 0.0213 & -0.0014 & 0.0135 \\ 0.0005 & 0.0011 & -0.0112 \\ -0.0216 & -0.0534 & -0.0102 \end{bmatrix}, \\
K_{31} &= \begin{bmatrix} 2.1922 & -9.0000 & -0.0000 \\ -1.0000 & 1.0811 & -1.0000 \\ -0.0000 & 14.2800 & -0.0567 \end{bmatrix}, K_{32} = \begin{bmatrix} 0.0218 & -0.0014 & 0.0138 \\ 0.0005 & 0.0011 & -0.0114 \\ -0.0221 & -0.0547 & -0.0105 \end{bmatrix}.
\end{aligned} \tag{72}$$

The initial condition of complex cyber-physical networks is set as $x_i(0) = \begin{bmatrix} 1 & -1 & 1 \end{bmatrix}^T$. In this case, the trajectories of synchronization error between the unforced isolated node and the network nodes are shown by Figures 13–15, respectively. It could be found from Figures 13–15 that the synchronization errors converge to zero within the limited sampling periods, which imply that the presented synchronization control method is effective for the discrete-time delayed complex cyber-physical networks with input delays and mixed attacks.

5. Conclusions

In this paper, the synchronization control issue has been investigated for discrete-delayed complex cyber-physical networks under mixed attacks. As a means of reducing the control costs of the complex cyber-physical networks, the intermittent mechanisms described by non-negative real regions have been introduced and applied to the design process of the synchronization control, and then an intermittent synchronization controller has been developed for the corresponding delayed complex cyber-physical networks subject to mixed attacks. By utilizing the appropriate Lyapunov function, sufficient conditions are derived for ensuring that the synchronization error dynamics are ultimately bounded, and the desired synchronization control gain matrices have been obtained by solving a group of LMIs. Subsequently, an optimization method has also been provided with the aim to minimize the synchronization error. Finally, two numerical examples are given to verify the effectiveness and superiority of the proposed synchronization control strategy.

On the other hand, it is worth pointing out that the treatment method of the nonlinear function in this article is somewhat conservative. Specifically, the sector-like descriptions of the nonlinearities do not relate to the current state of the error dynamics. Further research topics include the extension of our results to complex

cyber-physical networks with distributed input delays and mixed attacks. Also, it is more interesting to design the state-dependent treatment method for the nonlinear function.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants 61863026 and 62263019 and in part by the Major Science and Technology Special Project of Gansu Province under Grant 21ZD4GA028.

References

[1] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, "Complex networks: structure and dynamics," *Physics Reports*, vol. 424, no. 4-5, pp. 175–308, 2006.

[2] P. DeLellis, M. Di Bernardo, and F. Garofalo, "Adaptive pinning control of networks of circuits and systems in Lur'e form," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 11, pp. 3033–3042, 2013.

[3] Q. Li, B. Shen, Z. Wang, T. Huang, and J. Luo, "Synchronization control for a class of discrete time-delay complex dynamical networks: a dynamic event-triggered approach," *IEEE Transactions on Cybernetics*, vol. 49, no. 5, pp. 1979–1986, 2019.

[4] B. Shen, Z. Wang, D. Wang, and Q. Li, "State-saturated recursive filter design for stochastic time-varying nonlinear complex networks under deception attacks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 10, pp. 3788–3800, 2020.

[5] I. Qaisar, M. S. Aslam, and C. Zhou, "Event-triggered based H_∞ consensus control for multi-agent systems under time-varying delay," *Journal of Control Engineering and Applied Informatics*, vol. 22, pp. 25–32, 2020.

[6] S. Cai, J. Hao, Q. He, and Z. Liu, "Exponential synchronization of complex delayed dynamical networks via pinning periodically intermittent control," *Physics Letters A*, vol. 375, no. 19, pp. 1965–1971, 2011.

[7] S. Liu, T. Xu, and E. Tian, "Event-based pinning synchronization control for time-delayed complex dynamical networks: the finite-time boundedness," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 7, pp. 730–739, 2021.

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

[9] Q. Qi, X. Yang, Z. Xu, M. Zhang, and T. Huang, "Novel LKF method on H_∞ synchronization of switched time-delay systems," *IEEE Transactions on Cybernetics*, pp. 1–10, 2022.

[10] J. L. Wang, D. Y. Wang, H. N. Wu, and T. Huang, "Output synchronization of complex dynamical networks with multiple output or output derivative couplings," *IEEE Transactions on Cybernetics*, vol. 51, no. 2, pp. 927–937, 2021.

[11] H. Sang and J. Zhao, "Exponential synchronization and L_2 -gain analysis of delayed chaotic neural networks via intermittent control with actuator saturation," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, pp. 3722–3734, 2019.

[12] S. Ding, Z. Wang, and N. Rong, "Intermittent control for quasisynchronization of delayed discrete-time neural networks," *IEEE Transactions on Cybernetics*, vol. 51, no. 2, pp. 862–873, 2021.

[13] X. Yu and L. Li, "Trajectory tracking control with preview action for a class of continuous-time Lur'e-type nonlinear systems," *Advances in Difference Equations*, vol. 2020, pp. 293–317, 2020.

[14] C. Xu, X. Yang, J. Lu, J. Feng, F. E. Alsaadi, and T. Hayat, "Finite-time synchronization of networks via quantized intermittent pinning control," *IEEE Transactions on Cybernetics*, vol. 48, no. 10, pp. 3021–3027, 2018.

[15] Y. Zou, H. Su, R. Tang, and X. Yang, "Finite-time bipartite synchronization of switched competitive neural networks with time delay via quantized control," *ISA Transactions*, vol. 125, pp. 156–165, 2022.

[16] M. M. Hamdan, M. S. Mahmoud, and U. A. Baroudi, "Event-triggering control scheme for discrete time cyberphysical systems in the presence of simultaneous hybrid stochastic attacks," *ISA Transactions*, vol. 122, pp. 1–12, 2022.

[17] W. Fu, J. Qin, Y. Shi, W. X. Zheng, and Y. Kang, "Resilient consensus of discrete-time complex cyber-physical networks under deception attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4868–4877, 2020.

[18] Y. Zhao, Z. Chen, C. Zhou, Y. C. Tian, and Y. Qin, "Passivity-based robust control against quantified false data injection attacks in cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, pp. 1440–1450, 2021.

[19] M. Porter, P. Hespanhol, A. Aswani, M. Johnson-Roberson, and R. Vasudevan, "Detecting generalized replay attacks via time-varying dynamic watermarking," *IEEE Transactions on Automatic Control*, vol. 66, no. 8, pp. 3502–3517, 2021.

[20] K. M. Malik, A. Javed, H. Malik, and A. Irtaza, "A light-weight replay detection framework for voice controlled IoT devices," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 982–996, 2020.

[21] D. Liu and D. Ye, "Pinning-observer-based secure synchronization control for complex dynamical networks subject to DoS attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 12, pp. 5394–5404, 2020.

[22] Y. Tang, D. Zhang, P. Shi, W. Zhang, and F. Qian, "Event-based formation control for nonlinear multiagent systems under DoS attacks," *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 452–459, 2021.

[23] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Transactions on Control Systems Technology*, vol. 28, no. 3, pp. 741–752, 2020.

[24] W. Xu, G. Hu, D. W. C. Ho, and Z. Feng, "Distributed secure cooperative control under denial-of-service attacks from multiple adversaries," *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3458–3467, 2020.

[25] J. Milošević, H. Sandberg, and K. H. Johansson, "Estimating the impact of cyber-attack strategies for stochastic networked

control systems," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 2, pp. 747–757, 2020.

[26] L. Ye, N. Woodford, S. Roy, and S. Sundaram, "On the complexity and approximability of optimal sensor selection and attack for Kalman filtering," *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2146–2161, 2021.

[27] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1698–1711, 2019.

[28] H. Song, D. Ding, H. Dong, and Q. L. Han, "Distributed maximum correntropy filtering for stochastic nonlinear systems under deception attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 5, pp. 3733–3744, 2022.

[29] D. Mukherjee, "Data-driven false data injection attack: a low-rank approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2479–2482, 2022.

[30] Y. Tan, M. Xiong, B. Zhang, and S. Fei, "Adaptive event-triggered nonfragile state estimation for fractional-order complex networked systems with cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 4, pp. 2121–2133, 2022.

[31] E. Y. Güven and A. Y. Çamurcu, "Physical attack detection for smart objects," in *Proceedings of the IEEE International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1–5, IEEE, Malatya, Turkey, December, 2018.

[32] L. Dong and H. Xu, "Secure correct control for cyber-physical systems under multiple stochastic physical attacks," in *Proceedings of the IEEE 32th Chinese Control and Decision Conference, (CCDC)*, pp. 3824–3829, IEEE, Hefei, China, August, 2020.

[33] X. Yang, Y. Liu, J. Cao, and L. Rutkowski, "Synchronization of coupled time-delay neural networks with mode-dependent average dwell time switching," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 12, pp. 5483–5496, 2020.

[34] X. Yang, X. Li, J. Lu, and Z. Cheng, "Synchronization of time-delayed complex networks with switching topology via hybrid actuator fault and impulsive effects control," *IEEE Transactions on Cybernetics*, vol. 50, no. 9, pp. 4043–4052, 2020.

[35] Y. Yuan, P. Zhang, L. Guo, and H. Yang, "Towards quantifying the impact of randomly occurred attacks on a class of networked control systems," *Journal of the Franklin Institute*, vol. 354, no. 12, pp. 4966–4988, 2017.

[36] J. Liu, W. Suo, X. Xie, D. Yue, and J. Cao, "Quantized control for a class of neural networks with adaptive event-triggered scheme and complex cyber-attacks," *International Journal of Robust and Nonlinear Control*, vol. 31, no. 10, pp. 4705–4728, 2021.

[37] Z. Xu, R. Tang, Y. Sun, X. Li, and X. Yang, "Secure synchronization of coupled systems via double event-triggering mechanisms with actuator fault," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3580–3589, 2022.

[38] L. Fan and C. Wu, "Distributed finite-time consensus control of second-order multiagent systems subject to communication time delay," *Journal of Control Science and Engineering*, vol. 2021, Article ID 3786530, 12 pages, 2021.

[39] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2020.

[40] H. Divya, R. Sakthivel, Y. Liu, and R. Sakthivel, "Delay-dependent synchronization of TS fuzzy Markovian jump complex dynamical networks," *Fuzzy Sets and Systems*, vol. 416, pp. 108–124, 2021.

[41] T. H. Lee and J. H. Park, "Design of sampled-data controllers for the synchronization of complex dynamical networks under controller attacks," *Advances in Difference Equations*, vol. 2019, pp. 184–215, 2019.