ITC 1/52
Information Technology and Control
Vol. 52 / No. 1 / 2023
pp. 155-168
DOI 10.5755/j01.itc.52.1.31775

Event-Based Pinning Synchronization Control for Discrete-Time Delayed Complex Cyber-Physical Networks Under All-Around Attacks

Received 2022/07/05 | Accepted after revision 2023/01/30

https://doi.org/10.5755/j01.itc.52.1.31775

HOW TO CITE: Zhu, C., Jia, X. (2023). Event-Based Pinning Synchronization Control for Discrete-Time Delayed Complex Cyber-Physical Networks Under All-Around Attacks. *Information Technology and Control*, 52(1), 155-168. https://doi.org/10.5755/j01.itc.52.1.31775

Event-Based Pinning Synchronization Control for Discrete-Time Delayed Complex Cyber-Physical Networks Under All-Around Attacks

Chaqun Zhu, Xuan Jia

College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou, 730050, China; e-mails: chaoqunzhu@yeah.net, jiaxuan_cn@icloud.com

Corresponding author: chaoqunzhu@yeah.net

This paper is concerned with the problem of pinning synchronization control for a class of nonlinear discrete-time delayed complex cyber-physical networks under all-around attacks. To handle the all-around attacks, a constrained hybrid attacks model is established, which incorporates the pattern feature of false data injection attacks and physical attacks. By utilizing the Lyapunov stability theory and the linear matrix inequality technique, a novel dynamic event-triggering pinning synchronization control scheme is developed to cope with the synchronization control task. Subsequently, sufficient conditions are obtained to guarantee that the closed-loop error dynamics are ultimately exponentially bounded. Furthermore, the design procedure of the synchronization controller is presented for the considered complex cyber-physical networks subject to all-around attacks. Finally, an illustrative example is delivered to demonstrate the effectiveness of the proposed method.

KEYWORDS: Complex cyber-physical networks, all-around attacks, dynamic event-triggered mechanism, pinning control, synchronization control.

1. Introduction

As a class typical massively interconnected complex systems, complex networks are composed of interacting individuals or nodes, whose dynamics could be described by a single nonlinear vector field. For example, biological networks, social networks, Internet networks, transportation networks, neural networks, electric power grids, etc. [3, 5, 6, 13, 25].

Complex cyber-physical networks have many characteristics of a complex network, such as large node scale [28], the complexity of network dynamic behaviors [29], and continuous evolution of network topology [23] and so on. Due to the information interaction process between the nodes of complex cyber-physical networks through cyber space has become more complicated, thus complex cyber-physical networks are confronted with a larger risk of communications network-induced issues like network delay [29] and cyber attacks [28]. As an emerging field, security issues due to cyber attacks in the complex networks has attracted extensive attention and achieved a series of meaningful research results [10, 11, 12, 19, 34]. In general, there have been three cyber attacks that frequently arise in addressing the problem of secure control, i.e., false data injection (FDI) attacks [10, 12, 34], denial of service (DoS) attacks [19] and replay attacks [11]. From the perspective of security level, FDI attacks are the most dangerous attack, because the attackers can inject malicious data to worsen or destabilize the performance of the target system. In [12], considering the resource constraints of cyber attacks, the method of local attacks on sensor channels is proposed. In [10] and [34], sufficiently conditions have been derived for the state estimation issue under FDI attacks to guarantee the security of cyber-physical systems (CPS). However, the attacker needs to have complete information of the system in all of these cases. On the other hand, as a kind of adversarial disturbance, the physical attacks may cause the system components to operate incorrectly by maliciously modifying system inputs, and thus lead to system instability [7] and [9]. In [7], the machine learning method is utilizing to detect physical attacks on Internet of Things applications. In response to the problem of multiple stochastic physical attacks, the robust secure controller is proposed to ensure the stability of the systems in [9]. The above results provide the secure control strategy of control systems in the malicious attack environment, considering either FDI attacks or physical attacks. However, most of the available results only consider the impact of a single attack behaviour for the secure control of the system, and few results are obtained for the scene with all-around attacks (e.g., FDI attacks and physical attacks), which are more in line with control practice. Especially, it remains challenging now to address the synchronous control issue for discrete-time delayed complex cyber-physical networks with all-around attacks, and this provides us with motivation for shortening such a gap.

In complex networks, the synchronization of all nodes has been generally recognized as one of the most fascinating issues of research [18, 22, 24]. On the one hand, because of the simultaneous transmission of signals between a tremendous number of nodes in complex cyber-physical networks and the complex coupling of the communication networks, it is inevitable to encounter the problem of time delay, which will lead to the damage of network performance, see, e.g., [20, 29, 33]. On the other hand, as a result of the complicated network structure, it is always difficult to achieve synchronization spontaneously. So far, various control techniques have been presented to investigate the synchronization issue of complex networks, including continuous control [17], and discontinuous control [16, 32]. Among them, it is impractical to control every network node of the complex networks since only partial network nodes could be directly controlled according to their characteristics in practice. In such a situation, pinning control has been shown to be an efficient method of synchronizing complex networks. For instance, in [32], the pinning synchronization of a class of complex dynamical networks is investigated to obtain a general criterion for ensuring network synchronization, and in [16], the pinning control synchronization problem with and nonlinear coupling function is discussed for the complex network with symmetric coupling matrix. Recently, a pinning synchronization controller is proposed for ensuring the complex switching networks subject to nonzero control inputs to be stability in [27]. In [31], a pinning synchronization control method is presented to guarantee the synchronization control performance of the nonlinear multi-agent systems. In [21], the pinning synchronization control problem is discussed for the adaptive trajectory tracking of complex dynamical networks.

Due to the simultaneous transmission of signals between a tremendous number of nodes, the limited communication resources is one of the major problems that restrict the application of complex cyber-physical networks. It is worth noting that, most of the existing results on control of complex networks investigate are obtained by the time-triggered scheme for simplicity of analysis and design [1, 8]. However, under the time-triggered control strategy, the simultaneous transmission of signals between a tremendous number of network nodes will inevitably cause a waste of communication resources. To address this problem, researchers have proposed a variety of event triggering mechanisms to limit the waste of communication resources, including static event-triggered strategy [30], dynamic event-triggered strategy [26], and adaptive event-triggered strategy [14]. Among these event-based control techniques, a distributed security control technique based on a static event triggering scheme is proposed to handle second-order connected vehicle systems subject to DoS attacks and FDI attacks in [30]. By using the dynamic event-triggered strategy, the dynamic event-triggered state estimation problem is investigated for a class of discrete-time stochastic neural networks [26]. In [14], the quantized control problem of a class of neural networks subject to DoS attacks, FDI attacks and replay attacks is discussed by employing the adaptive event-triggered scheme. By now, most of the existing results focus on the synchronization control problem for the complex networks under the cyber attacks. In practice, however, the complex networks may be subject to both cyber attacks and physical attacks simultaneously. As a result, it is necessary to find a synchronization control technique that can defend cyber attacks and physical attacks, and decrease the utilization of communication resources, which constitutes second motivation of our work.

Motivated by the above-mentioned discussions, this paper is concerned with the dynamic event-triggering pinning synchronization control issue for complex cyber-physical networks under all-around attacks. For underlying issues, we have to face the following technical challenges: 1) how to model the all-around attacks arising from the combination of FDI attacks and physical attacks? 2) how to handle the synchronization control problem for the considered complex cyber-physical networks subject to all-around attacks? 3) how to determine the parameter of the synchronization controller such that the closed-loop synchronization error dynamics is ultimately exponentially bounded? Therefore, the paper aims to provide satisfactory answers to the three technical challenges mentioned above, and the following are the primary contributions of this paper:

1. For the first time, the system model is established for the discrete-time delayed complex cyber-physical networks subject to all-around attacks.
2. The pinning synchronization control strategy based on dynamic event-triggered communication is employed to deal with the time delay and the all-around attacks.
3. The design procedure of the synchronization controller is provided to ensure the ultimately exponentially bounded of the closed-loop synchronization error dynamics.

The rest of this paper is organized as follows. Section II is the problem description and preliminaries. In Section III, the design procedure of the synchronization controller is proposed for the discrete-time

Table 1
Notations

Notations	Expression
$\mathbb{R}^n$	N-dimensional Euclidean space
$\mathbb{R}^{n\times n}$	The $n \times n$ - real matrices
$\mathbb{R}^+$	Natural number
$\mathrm{h}: \mathbb{R}^n \times \mathbb{R}^+ \rightarrow \mathbb{R}^n$	The nonlinear vector-valued function
R^T	The transpose of the matrix
$P > 0$	Matrix P is positive definite
$P \geq 0$	The positive semidefinite
$\lambda_{min}(P)$	The smallest eigenvalues of Matrix P
$diag\{R\}$	The diagonal matrix
$\|\|x\|\|_2$	The 2-norm
$\otimes$	The Krorecker product
*	Symmetric entry
$I / 0$	Identity matrix/zero matrix
I_N	The $n \times n$ identity matrix
Δ	The differential operator

delayed complex cyber-physical networks with the effects of all-around attacks. An illustrative example is provided in Section IV to demonstrate the effectiveness of the proposed results. Finally, Section V concludes the paper and discusses future research directions.

The notations used in this paper are standard and expressed as Table 1.

2. Problem Formulation and Preliminaries

Considering the following discrete-time delayed complex cyber-physical networks consisting of N coupled nodes subject to FDI attacks [2] and physical attacks:

$$\begin{aligned} x_i(k+1) &= Ax_i(k) + f(x_i(k)) + g(x_i(k-\tau_k)) \\ &+ \sum_{j=1}^{N} \tilde{l}_{ij}\Gamma x_j(k) + \pi(k)m(x_i(k)) \\ &+ u_i(k) + h(x_i(k)) \\ x_i(\theta) &= \phi_i(\theta), \theta \in [-\tau_M, 0]. \end{aligned} \tag{1}$$

for $k \in \mathbb{R}^+$ and $i \in \mathcal{V} \triangleq \{1,2,...,N\}$, where $x_i(k) \in \mathbb{R}^n$, $u_i(k) \in \mathbb{R}^m$, and $\phi_i(\theta) \in \mathbb{R}^n$ are the state vector, the control input, and the initial condition, respectively. $f: \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$and $g: \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$ are nonlinear functions, respectively. $h: \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$ is physical attack signal injected by the anomalies. $A \in \mathbb{R}^{n\times n}$ is known constant matrices. τ_k is the time-varying delay satisfying $\tau_m \le \tau_k \le \tau_M$, where τ_m and τ_M are known non-negative integers. $\Gamma \in \mathbb{R}^{n\times n}$ denote the inner-coupling matrix, and $L = (\tilde{l}_{ij})_{N\times N}$ is a matrix representing the outer-coupling configuration with $\tilde{l}_{ij} \ge 0 (i \ne j)$ and $\tilde{l}_{ij} = -\sum_{j=1, j\ne i}^{N} \tilde{l}_{ij}$. $m(x_i(k)) \in \mathbb{R}^n$ is the vector of FDI attacks. The Bernoulli variable $\pi(k) \in \{0,1\}$ with satisfy $E\{\pi(k)\} = \bar{\pi}$ and $E\{\pi(k) - \bar{\pi}\} = \pi^2$. $\pi(k) = 1$ indicates that FDI attacks have contaminated the measured data with false data, and $\pi(k) = 0$ indicates that FDI attacks have failed to affect the transmitted data.

Before proceeding further, we give the following Assumptions:

Assumption 1. For any $v_1(k) \in \mathbb{R}^n$ and $v_2(k) \in \mathbb{R}^n$, the nonlinear functions $f: \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$, $g: \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$, and $h: \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$ satisfy the conditions as follows:

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

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

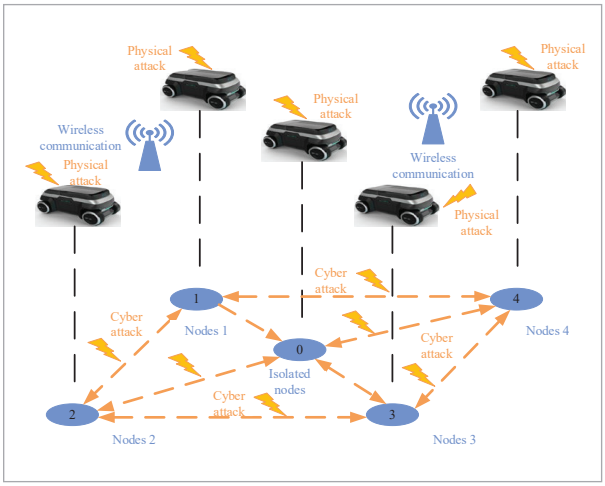
Assumption 2. For the constant matrices $C \in \mathbb{R}^{n\times n}$ and $U \in \mathbb{R}^{n\times n}$, FDI attacks behaviour $m(x_i(k))$ and physical attacks behaviour $h(x_i(k))$ satisfy the following conditions:

$$\|m(x_i(k))\|_2 \le \|Ux_i(k)\|_2,$$
$$\|h(x_i(k))\|_2 \le \|Cx_i(k)\|_2,$$

which represent the upper bound of FDI attacks and physical attacks. C and U are given matrices with appropriate dimensions.

Remark 1. Based on above analysis, an all-around attacks model is established following the above FDI

Figure 1
Illustration of complex cyber-physical networks under all-around attacks



attacks and physical attack strategies for the discrete-time delayed complex cyber-physical networks. It is assumed that the FDI attacks and physical attacks have limited resources by Assumption 2.

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

$$\begin{aligned} s(k+1) &= As(k)+f(s(k))+g(s(k-\tau_k)) \\ &\quad +\pi(k)m(s(k))+h(s(k)) \\ s(\theta) &= \phi(\theta),\theta\in[-\tau_M,0], \end{aligned} \tag{3}$$

where $s(k)\in\mathbb{R}^n$ and $\phi(\theta)\in\mathbb{R}^n$ are the state vector and initial condition of isolated nodes, respectively. $m(s(k))\in\mathbb{R}^n$ indicates the vector of FDI attacks. $\pi(k)\in\{0,1\}$ is the Bernoulli variable. $h(s(k))$ denotes the physical attack signal injected by the anomalies.

Define the initial condition error and the synchronization error as follows:

$\tilde{\phi}_i(\theta)=\phi_i(\theta)-\phi(\theta)$, $e_i(k)=x_i(k)-s(k)$.

Then, the following matrices and notations are introduced:

$$\tilde{f}(e_i(k))=f(x_i(k))-f(s(k))-\mathcal{D}_{1f}e(k),$$

$$\tilde{g}(e_i(k-\tau_k))=g(x_i(k-\tau_k))-g(s(k-\tau_k))-\mathcal{D}_{1g}e(k-\tau_k),$$

$$\tilde{h}(e_i(k))=h(x_i(k))-h(s(k)),$$

$$\tilde{m}(e_i(k))=m(x_i(k))-m(s(k)),$$

$$\tilde{A}=I_N\otimes A,\ \tilde{L}=L\otimes\Gamma,\ \tilde{\mathcal{D}}_{2h}=I_N\otimes\mathcal{D}_{2h},\ \tilde{\mathcal{D}}_{1f}=I_N\otimes\mathcal{D}_{1f},$$

$$\tilde{\mathcal{D}}_{2f}=I_N\otimes\mathcal{D}_{2f},\ \tilde{\mathcal{D}}_{1g}=I_N\otimes\mathcal{D}_{1g},\ \tilde{\mathcal{D}}_{2g}=I_N\otimes\mathcal{D}_{2g},$$

$$\tilde{\mathcal{D}}_{1h}=I_N\otimes\mathcal{D}_{1h},\ e(k)=\left[e_1^T(k)\ \cdots\ e_N^T(k)\right]^T,$$

$$\tilde{\phi}(\theta)=\left[\tilde{\phi}_1^T(\theta)\ \cdots\ \tilde{\phi}_N^T(\theta)\right]^T,$$

$$\tilde{f}(e(k))=\left[\tilde{f}^T(e_1(k))\ \cdots\ \tilde{f}^T(e_N(k))\right]^T,$$

$$\tilde{g}(e(k-\tau_k))=\left[\tilde{g}^T(e_1(k-\tau_k))\ \cdots\ \tilde{g}^T(e_N(k-\tau_k))\right]^T,$$

$$\tilde{h}(e(k))=\left[\tilde{h}^T(e_1(k))\ \cdots\ \tilde{h}^T(e_N(k))\right]^T,$$

$$\tilde{m}(e(k))=\left[m^T(e_1(k))\ \cdots\ m^T(e_N(k))\right]^T.$$

According to the above definition, the synchronization error dynamics can be obtained as follows:

$$\begin{aligned} e(k+1) &= \left(\tilde{A}+\tilde{L}+\tilde{\mathcal{D}}_{1f}\right)e(k)+\tilde{f}(e(k)) \\ &\quad +\tilde{g}(e(k-\tau_k))+\pi(k)\tilde{m}(e(k)) \\ &\quad +u(k)+\tilde{\mathcal{D}}_{1g}e(k-\tau_k)+\tilde{h}(e(k)) \\ e(\theta) &= \tilde{\phi}(\theta),\theta\in[-\tau_M,0], \end{aligned} \tag{4}$$

where $\tilde{A}$, $\tilde{L}$, $\tilde{\mathcal{D}}_{1f}$ and $\tilde{\mathcal{D}}_{1g}\in\mathbb{R}^{n\times n}$ are known constant matrices.

By using the Assumption 1, one has

$$\begin{cases} \tilde{f}^T(e(k))\left[\tilde{f}(e(k))-\left(\tilde{\mathcal{D}}_{2f}-\tilde{\mathcal{D}}_{1f}\right)e(k)\right]\le 0 \\ \tilde{g}^T(e(k))\left[\tilde{g}(e(k))-\left(\tilde{\mathcal{D}}_{2g}-\tilde{\mathcal{D}}_{1g}\right)e(k)\right]\le 0 \\ \left[\tilde{h}(e(k))-\tilde{\mathcal{D}}_{1h}e(k)\right]^T\left[\tilde{h}(e(k))-\tilde{\mathcal{D}}_{2h}e(k)\right]\le 0 \end{cases}. \tag{5}$$

In this paper, to achieve the synchronization control for the complex cyber-physical networks, a pinned synchronization controller is employed as follows:

$$u_i(k)=\begin{cases} K_ie_i(k), i\in\mathcal{V}_{Pin}, \\ 0, i\in\mathcal{V}\setminus\mathcal{V}_{Pin} \end{cases}, \tag{6}$$

where K_i is the synchronization control gain matrices, $\mathcal{V}_{Pin}=\{1,2,3,...,\kappa\}\subseteq\mathcal{V}$ is the set of nodes to be fixed by the pinned state feedback synchronization controller.

Let $\{k_r^i\}_{r\in\mathbb{R}^+}$ be the real-time sequence triggered by the event for the i-th network node, which is determined iteratively according to the following triggering rules [15]:

$$\begin{aligned} k_{r+1}^i=\min\Big\{ & k\in\mathbb{R}^+\,|\,k>k_r^i,\frac{1}{\psi_i}\chi_i(k) \\ & +\rho_i-\zeta_i^T(k)\zeta_i(k)<0\Big\}, \end{aligned} \tag{7}$$

for $r\in\mathbb{R}^+$ and $i\in\mathcal{V}_{Pin}=\{1,2,3,...,\kappa\}\subseteq\mathcal{V}$, where $k_0^i=0$, $\psi_i>0$ and $\rho_i>0$ are given positive scalars. The measurement error of the dynamic event-triggered strategy $\zeta_i(k)$ is denoted by $\zeta_i(k)=e_i(k)-e_i(k_r^i)$, and the internal dynamic variables $\chi_i(k)$ of dynamic event-triggered strategy are satisfied the following conditions:

$$\chi_i(k+1)=\varepsilon_i\chi_i(k)+\rho_i-\zeta_i^T(k)\zeta_i(k), \tag{8}$$

where $\varepsilon_i\in(0,1)$ is given positive scalars, and $\chi_i(0)=\chi_0^i\geq 0$ is the initial condition.

According to the function of zero-order holder, the sampled value at moment k is maintained until moment $k+1$. Thus, the control input of the i-th node can be expressed as follows:

$$u_i(k)=K_ie_i\left(k_r^i\right),k\in\left[k_r^i,k_{r+1}^i\right),i\in\mathcal{V}_{Pin}, \tag{9}$$

where $k\in\left[k_r^i,k_{r+1}^i\right)$ is the event-triggered instant sequence.

Based on the above analysis, substituting $\zeta_i(k)=e_i(k)-e_i\left(k_r^i\right)$ and (9) into (6), the event-based pinning controller is obtained as follows:

$$u_i(k)=\begin{cases}K_i\left(e_i(k)-\zeta_i(k)\right),i\in\mathcal{V}_{Pin}\\0,i\in\mathcal{V}\setminus\mathcal{V}_{Pin}\end{cases}. \tag{10}$$

Substituting (10) into (4), which yields the closed-loop synchronization error dynamics as follows:

$$\begin{cases}e(k+1)=\left(\tilde{A}+\tilde{L}+\tilde{\mathcal{D}}_{1f}\right)e(k)+\tilde{f}\left(e(k)\right)\\\qquad+\tilde{g}\left(e(k-\tau_k)\right)+\pi(k)\tilde{m}\left(e(k)\right)\\\qquad+Ke(k)-K\zeta(k)+\tilde{\mathcal{D}}_{1g}e(k-\tau_k)\\\qquad+\tilde{h}\left(e(k)\right),i\in\mathcal{V}_{Pin}\\e(k+1)=\left(\tilde{A}+\tilde{L}+\tilde{\mathcal{D}}_{1f}\right)e(k)+\tilde{f}\left(e(k)\right)\\\qquad+\tilde{g}\left(e(k-\tau_k)\right)+\pi(k)\tilde{m}\left(e(k)\right)\\\qquad+\tilde{\mathcal{D}}_{1g}e(k-\tau_k)+\tilde{h}\left(e(k)\right),i\in\mathcal{V}\setminus\mathcal{V}_{Pin}\end{cases}, \tag{11}$$

where $K=\mathrm{diag}\{K_1\ \cdots\ K_\kappa\ 0\ \cdots\ 0\}$, and $k\in\left[k_r^i,k_{r+1}^i\right)$ for $i\in\mathcal{V}_{Pin}$.

According to (9) and (11), the closed-loop synchronization error dynamics can be obtained as follows:

$$\begin{aligned}e(k+1)=&\left(\tilde{A}+\tilde{L}+\tilde{\mathcal{D}}_{1f}\right)e(k)+\tilde{f}\left(e(k)\right)\\&+\tilde{g}\left(e(k-\tau_k)\right)+\tilde{\mathcal{D}}_{1g}e(k-\tau_k)\\&+\pi(k)\tilde{m}\left(e(k)\right)+Ke(k)\\&-K\zeta(k)+\tilde{h}\left(e(k)\right),i\in\mathcal{V}_{Pin}.\end{aligned} \tag{12}$$

This paper aims at designing an event-triggered pinning synchronization controller, which can guarantee that the closed-loop synchronization error dynamics (12) is ultimately exponentially bounded.

3. Main Results

In this section, we will provide the design procedure of event-based pinning synchronization controller for the delayed complex cyber-physical networks subject to all-around attacks. Before proceeding further, let us introduce the following definition of boundedness and piecewise Lyapunov-like functional which will be helpful in subsequent developments.

Definition 1 [4]. For the FDI attacks probability $0<\pi<1$ be given, assume there exists scalar $\delta_0>0$, such that the following conditions hold

$$\left\|e(k)\right\|^2\leq V(0)+\delta_0. \tag{13}$$

Then, the closed-loop synchronization error dynamics (12) is exponentially bounded.

The piecewise Lyapunov-like functions is defined as follows:

$$\begin{aligned}V(k)=&e^T(k)Pe(k)+\sum_{i=k-\tau(k)}^{k-1}\gamma^{k-i-1}e^T(i)Qe(i)\\&+\sum_{j=k-\tau_M+1}^{k-\tau_m}\sum_{i=j}^{k-1}\gamma^{k-i-1}e^T(i)Qe(i)+\sum_{i=1}^{\kappa}\gamma^{-1}\frac{1}{\psi_i}\chi_i(k).\end{aligned} \tag{14}$$

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

Theorem 1. Let the FDI attacks probability $0<\pi<1$, the positive scalars δ_0, $\varepsilon_i<1$, $\gamma<1$, ψ_i and $\varepsilon_i\psi_i\geq 1$ ($i\in\mathcal{V}_{Pin}$), and the controller gains K be given. If there exist the matrices $0<P\in\mathbb{R}^{n\times n}$, $0<Q\in\mathbb{R}^{n\times n}$, and the scalars $\mu_1>0$, $\mu_2>0$, $\mu_3>0$ and $\mu_4>0$ that satisfies the following inequalities

$$\Pi=\begin{bmatrix}\Pi_{11}&\Pi_{12}\\*&-P\end{bmatrix}<0, \tag{15}$$

$$\frac{\delta}{1-\gamma}\leq\delta_0, \tag{16}$$

and

$$\begin{bmatrix}\gamma I&I\\I&P\end{bmatrix}>0, \tag{17}$$

where

$$\Pi_{11}=\begin{bmatrix}\Lambda_{11}&0&\Lambda_{13}&0&\Lambda_{15}&0&0&0\\ *&\Lambda_{22}&0&\Lambda_{24}&0&0&0&0\\ *&*&\Lambda_{33}&0&0&0&0&0\\ *&*&*&\Lambda_{44}&0&0&0&0\\ *&*&*&*&\Lambda_{55}&0&0&0\\ *&*&*&*&*&\Lambda_{66}&0&0\\ *&*&*&*&*&*&\Lambda_{77}&0\\ *&*&*&*&*&*&*&\Lambda_{88}\end{bmatrix},$$

$$\Pi_{12}=\begin{bmatrix}P\left(\tilde{A}+\tilde{L}+\tilde{\mathcal{D}}_{1f}+K\right) & P\tilde{\mathcal{D}}_{1g} & P & P\\ P & P & -K & 0\end{bmatrix}^T,$$

$$\Lambda_{11}=-\gamma P+\left(1+\tau_M-\tau_m\right)Q-\mu_3\left(\tilde{\mathcal{D}}_{1h}^T\tilde{\mathcal{D}}_{2h}+\tilde{\mathcal{D}}_{2h}^T\tilde{\mathcal{D}}_{1h}\right),$$

$$\Lambda_{13}=\mu_1\left(\tilde{\mathcal{D}}_{2f}-\tilde{\mathcal{D}}_{1f}\right)^T,\ \Lambda_{15}=\mu_3\left(\tilde{\mathcal{D}}_{2h}+\tilde{\mathcal{D}}_{1h}\right)^T,$$

$$\Lambda_{22}=-\gamma^{\tau_M}Q,\ \Lambda_{24}=\mu_2\left(\tilde{\mathcal{D}}_{2g}-\tilde{\mathcal{D}}_{1g}\right)^T,\ \ \Lambda_{33}=-2\mu_1 I,$$

$$\Lambda_{44}=-2\mu_2 I,\ \Lambda_{55}=-2\mu_3 I,\ \Lambda_{66}=-\pi I,$$

$$\Lambda_{77}=-diag\left\{\frac{1}{\psi_1}\gamma^{-1}+\mu_4,...,\frac{1}{\psi_\kappa}\gamma^{-1}+\mu_4\right\}I,$$

$$\Lambda_{88}=diag\left\{\frac{\left(\gamma^{-1}\varepsilon_1-1\right)+\mu_4}{\psi_1},...,\frac{\left(\gamma^{-1}\varepsilon_\kappa-1\right)+\mu_4}{\psi_\kappa}\right\}I,$$

$$\delta=\sum_{i=1}^{\kappa}\left(\frac{1}{\psi_i}\chi_i(k)+\mu_4\right)\rho_i.$$

Then, the closed-loop synchronization error dynamics (12) is ultimately exponentially bounded.

Proof. For $\forall i\in\mathcal{V}_{Pin}$, define the $\Delta V(k)$ as follows:

$$\Delta V(k)=V(k+1)-\gamma V(k), \tag{18}$$

where $0<\gamma<1$ is decay index. by calculations, one obtains

$$\begin{aligned}&\Delta V(k)=V(k+1)-\gamma V(k)\\ &\le\left(e(k+1)-e(k)\right)^T P\left(e(k+1)-e(k)\right)\\ &\quad+2e^T(k)Pe(k+1)-(1+\gamma)e^T(k)Pe(k)\\ &\quad+e^T(k)Qe(k)-\gamma^{\tau_M}e^T\left(k-\tau(k)\right)Qe\left(k-\tau(k)\right)\\ &\quad+\sum_{i=k+1-\tau_M}^{k-\tau_m}\gamma^{k-i}e^T(i)Qe(i)\\ &\quad+\left(\tau_M-\tau_m\right)e^T(k)Qe(k)-\sum_{i=k-\tau_M+1}^{k-\tau_m}\gamma^{k-i}e^T(i)Qe(i)\\ &\quad+\sum_{i=1}^{\kappa}\frac{1}{\psi_i}\chi_i(k)\left(\gamma^{-1}\varepsilon_i-1\right)+\sum_{i=1}^{\kappa}\gamma^{-1}\frac{1}{\psi_i}\rho_i\\ &\quad-\sum_{i=1}^{\kappa}\gamma^{-1}\frac{1}{\psi_i}\zeta_i^T(k)\zeta_i(k).\end{aligned} \tag{19}$$

For any scalars $\mu_1>0$, $\mu_2>0$ and $\mu_3>0$ it follows from (5) that:

$$-2\mu_1\tilde{f}\left(e(k)\right)^T\left[\tilde{f}\left(e(k)\right)-\left(\tilde{\mathcal{D}}_{2f}-\tilde{\mathcal{D}}_{1f}\right)e(k)\right]\ge 0, \tag{20}$$

$$\begin{aligned}&-2\mu_2\tilde{g}\left(e\left(k-\tau_k\right)\right)^T\left[\tilde{f}\left(e\left(k-\tau_k\right)\right)\right.\\ &\qquad\left.-\left(\tilde{\mathcal{D}}_{2g}-\tilde{\mathcal{D}}_{1g}\right)e\left(k-\tau_k\right)\right]\ge 0,\end{aligned} \tag{21}$$

$$-2\mu_3\left[\tilde{h}\left(e(k)\right)-\tilde{\mathcal{D}}_{1h}e(k)\right]^T\left[\tilde{h}\left(e(k)\right)-\tilde{\mathcal{D}}_{2h}e(k)\right]\ge 0. \tag{22}$$

and, for scalars $\mu_4>0$, it follows from the triggering condition (7) that

$$\mu_4\sum_{i=1}^{\kappa}\gamma^{-1}\frac{1}{\psi_i}\left[\varepsilon_i\chi_i(k)+\rho_i-\zeta_i^T(k)\zeta_i(k)\right]\ge 0. \tag{23}$$

Considering (19)-(23), one eventually obtains

$$\begin{aligned}&\Delta V(k)=V(k+1)-\gamma V(k)\\ &\le\left(e(k+1)-e(k)\right)^T P\left(e(k+1)-e(k)\right)\\ &\quad+2e^T(k)Pe(k+1)-(1+\gamma)e^T(k)Pe(k)\\ &\quad+e^T(k)Qe(k)-\gamma^{\tau_M}e^T\left(k-\tau(k)\right)Qe\left(k-\tau(k)\right)\\ &\quad+\sum_{i=k+1-\tau_M}^{k-\tau_m}\gamma^{k-i}e^T(i)Qe(i)\\ &\quad+\sum_{i=1}^{\kappa}\frac{1}{\psi_i}\chi_i(k)\left(\gamma^{-1}\varepsilon_i-1\right)+\sum_{i=1}^{\kappa}\gamma^{-1}\frac{1}{\psi_i}\rho_i\\ &\quad-\sum_{i=1}^{\kappa}\gamma^{-1}\frac{1}{\psi_i}\zeta_i^T(k)\zeta_i(k)\\ &\quad-2\mu_1\tilde{f}\left(e(k)\right)^T\left[\tilde{f}\left(e(k)\right)-\left(\tilde{\mathcal{D}}_{2f}-\tilde{\mathcal{D}}_{1f}\right)e(k)\right]\\ &\quad-2\mu_2\tilde{g}\left(e\left(k-\tau_k\right)\right)^T\left[\tilde{f}\left(e\left(k-\tau_k\right)\right)\right.\\ &\quad\left.-\left(\tilde{\mathcal{D}}_{2g}-\tilde{\mathcal{D}}_{1g}\right)e\left(k-\tau_k\right)\right]\\ &\quad-2\mu_3\left[\tilde{h}\left(e(k)\right)-\tilde{\mathcal{D}}_{1h}e(k)\right]^T\\ &\quad\times\left[\tilde{h}\left(e(k)\right)-\tilde{\mathcal{D}}_{2h}e(k)\right]\\ &\quad+\mu_4\sum_{i=1}^{N}\left(\frac{1}{\psi_i}\chi_i(k)+\sigma_i-\zeta_i^T(k)\zeta_i(k)\right)\\ &=\xi^T(k)\left(\Pi_{11}+\Pi_{12}P^{-1}\Pi_{12}^T\right)\xi(k)\\ &\quad+\sum_{i=1}^{N}\left(\frac{1}{\psi_i}\gamma^{-1}\rho_i+\mu_4\rho_i\right)\\ &=\xi^T(k)\left(\Pi_{11}+\Pi_{12}P^{-1}\Pi_{12}^T\right)\xi(k)+\delta,\end{aligned} \tag{24}$$

where

$$\xi(k)=\left[e^T(k)\quad e^T(k-\tau_k)\quad \tilde{f}^T(e(k))\right.$$
$$\tilde{g}^T(e(k-\tau_k))\quad \tilde{h}^T(e(k))\quad \tilde{m}^T(e(k))$$
$$\left.\zeta^T(k)\quad \tilde{\chi}^T(k)\right]^T,$$
$$\tilde{\chi}(k)=\left[\chi_1^{1/2}(k)\quad \chi_2^{1/2}(k)\quad \cdots\quad \chi_\kappa^{1/2}(k)\right].$$

Applying Schur's Lemma for (15), that the following inequality holds

$$\Pi_{11}+\Pi_{12}P^{-1}\Pi_{12}^T<0. \tag{25}$$

It follows from (24) and (25) that

$$V(k+1)-\gamma V(k)\le\delta, \tag{26}$$

which means that

$$\begin{aligned}V(k)&\le\gamma V(k_1)+\delta\\&\le\gamma V(k_2)+\gamma\delta+\delta\\&\le\cdots\le\gamma^k V(0)+\frac{1-\gamma^k}{1-\gamma}\delta\\&\le\gamma^k V(0)+\frac{1}{1-\gamma}\delta,\end{aligned} \tag{27}$$

where $\delta=\sum_{i=1}^{\kappa}\left(\frac{1}{\psi_i}\chi_i(k)+\mu_4\right)\rho_i>0$.

Subsequently, by considering (16) and (27), one has

$$\begin{aligned}\lambda_{\min}(P)\|e(k)\|^2&\le\gamma^k V(0)+\frac{1}{1-\gamma}\delta\\&\le\gamma^k V(0)+\delta_0.\end{aligned} \tag{28}$$

From $0<\gamma<1$ and (28), it can be obtained as follows:

$$\lambda_{\min}(P)\|e(k)\|^2\le\gamma V(0)+\delta_0. \tag{29}$$

According to (17), one has

$$P>\frac{1}{\gamma}I. \tag{30}$$

Note the facts (29) and (30), it is obtained that

$$\|e(k)\|^2\le V(0)+\delta_0. \tag{31}$$

According to the Definition 1, the closed-loop synchronization error dynamics (12) is ultimately exponentially bounded. The proof is thus completed.

Now, we are in the position of deriving the synchronization control gain K_i on the basis of Theorem 1, which provides sufficient conditions for the ultimately exponentially bounded of the closed-loop synchronization error dynamics (12).

Theorem 2. Let the FDI attacks probability $0<\pi<1$, the positive scalar δ_0, $\varepsilon_i<1$, $\gamma<1$, ψ_i and $\varepsilon_i\psi_i\ge1$ ($i\in\mathcal{V}_{Pin}$) be given. If there exist the diagonal matrices $0<P=daig\{P_1,P_2,\cdots,P_N\}\in\mathbb{R}^{n\times n}$, the real matrices $Y=daig\{Y_1,\cdots,Y_\kappa,0,\cdots,0\}\in\mathbb{R}^{n\times n}$, the matrices $0<Q\in\mathbb{R}^{n\times n}$, and the scalar $\mu_1>0$, $\mu_2>0$, $\mu_3>0$ and $\mu_4>0$ that satisfies the following inequalities

$$\tilde{\Pi}=\begin{bmatrix}\Pi_{11}&\tilde{\Pi}_{12}\\*&-P\end{bmatrix}<0, \tag{32}$$

$$\frac{\delta}{1-\gamma}\le\delta_0, \tag{33}$$

and

$$\begin{bmatrix}\gamma I&I\\I&P\end{bmatrix}>0, \tag{34}$$

where

$$\tilde{\Pi}_{12}=\left[P\left(\tilde{A}+\tilde{L}+\tilde{\mathcal{D}}_{1f}\right)+Y^T\quad P\tilde{\mathcal{D}}_{1g}\quad P\quad P\right.$$
$$\left.P\quad P\quad -Y\quad 0\right]^T.$$

Then, the synchronization controller that renders the closed-loop synchronization error dynamics (12) to be exponentially bounded can be determined by

$$K_i=P_i^{-1}Y_i, i\in\mathcal{V}_{Pin}. \tag{35}$$

Proof. The variable substitution method is employed to prove this Theorem. Let $P_iK_i=Y_i$, and substitute it into (15), which yields (32). This completes the proof.

Remark 2. In Theorem 2, the design issue of synchronization control is investigated for delayed complex cyber-physical networks under all-around attacks. From the Theorem 2, it is easy to obtain that the control gain matrices of the proposed synchronization control scheme. Compared with the results of existing work, this paper has provided the first attempts to consider the synchronization control problem for delayed complex cyber-physical networks under all-around attacks.

For comparison with the results of Theorem 2, the static event-triggering strategy is adopted in Corollary 1.

Corollary 1: Let the FDI attack probability $0<\pi<1$, the positive scalar $\varepsilon_i<1$, $\gamma<1$, ψ_i and $\varepsilon_i\psi_i\geq 1$ $(i\in\mathcal{V}_{Pin})$ be given. The static trigger condition is shown as follows.

$$k_{r+1}^i=\min\left\{k\in\mathbb{R}^+\left|k>k_r^i,\rho_i-\zeta_i^T\left(k\right)\zeta_i\left(k\right)<0\right.\right\}, \tag{36}$$

for all $i\in\mathcal{V}_{Pin}$. If there exist diagonal matrices $0<P=daig\left\{P_1,P_2,\cdots,P_N\right\}\in\mathbb{R}^{n\times n}$, the real matrices $Y=daig\left\{Y_1,\cdots,Y_\kappa,0,\cdots,0\right\}\in\mathbb{R}^{n\times n}$, the matrices $0<Q\in\mathbb{R}^{n\times n}$, and the scalar $\mu_1>0$, $\mu_2>0$, $\mu_3>0$ and $\mu_4>0$ that satisfies the following inequalities

$$\ddot{\Pi}=\begin{bmatrix}\ddot{\Pi}_{11} & \ddot{\Pi}_{12}\\ * & -P\end{bmatrix}<0, \tag{37}$$

and

$$\begin{bmatrix}\gamma I & I\\ I & P\end{bmatrix}>0, \tag{38}$$

where

$$\ddot{\Pi}_{11}=\begin{bmatrix}\Lambda_{11} & 0 & \Lambda_{13} & 0 & \Lambda_{15} & 0 & 0\\ * & \Lambda_{22} & 0 & 0 & 0 & 0 & 0\\ * & * & \Lambda_{33} & 0 & 0 & 0 & 0\\ * & * & * & \Lambda_{44} & 0 & 0 & 0\\ * & * & * & * & \Lambda_{55} & 0 & 0\\ * & * & * & * & * & -\pi I & 0\\ * & * & * & * & * & * & -\mu_4 I\end{bmatrix},$$

$$\ddot{\Pi}_{12}=\left[P\left(\tilde{A}+\tilde{L}+\tilde{\mathcal{D}}_{1f}\right)+Y_i^T \quad P\tilde{\mathcal{D}}_{1g} \quad P \quad P \quad P \quad P \quad -Y\right]^T.$$

Then, the synchronization controller that renders the closed-loop synchronization error dynamics (12) to be exponentially bounded can be obtained by

$$K_i=P_i^{-1}Y_i, i\in\mathcal{V}_{Pin}. \tag{39}$$

Proof. By letting $\psi_i\to+\infty$, $i\in\mathcal{V}_{Pin}$, the proof of Corollary 1 can follow the same way as Theorem 2. No further details here.

Remark 3. In Theorem 2 and Corollary 1, the design procedure of dynamic event-triggered and static event-triggered pinning synchronization controllers, respectively, is addressed for complex cyber-physical networks with unforced isolated node and all-around attacks. The exponential boundedness of synchronization error dynamics (12) has been proved, and the required synchronization controller gain matrices K_i is obtained by solving a group of LMIs.

4. Numerical Simulations

In this section, an illustrative example is provided for the discrete-time delayed complex cyber-physical networks to demonstrate the effectiveness of presented synchronization control scheme. In what follows, we consider a delayed complex cyber-physical network of the form (1) that is composed of three identical nodes with the inner-coupling matrix is set as $\Gamma=0.517I$ and the following parameters (e.g., coupling matrix):

$$L=\begin{bmatrix}-0.65 & 0.1 & 0.55\\ 0 & -0.05 & 0.05\\ 0.5 & 0 & -0.5\end{bmatrix}.$$

The complex cyber-physical networks (1) are with the following parameters:

$$A=\begin{bmatrix}1.21 & -0.012 & -0.01\\ -0.51 & 0.32 & 0\\ -0.2 & 0.1 & 0.5\end{bmatrix},$$

$$f\left(x\right)=\begin{bmatrix}0.02\sin\left(x_1\right) & 0 & 0.01\tanh\left(x_1\right)\\ 0 & 0.02\cos\left(x_2\right) & 0\\ 0 & 0 & 0.03\sin\left(x_3\right)\end{bmatrix},$$

$$g\left(x\right)=\begin{bmatrix}0 & -0.01\cos\left(x_1\right) & -0.01\tanh\left(x_1\right)\\ -0.02\sin\left(x_2\right) & 0 & -0.02\tanh\left(x_2\right)\\ 0 & 0.02\cos\left(x_3\right) & 0.01\sin\left(x_3\right)\end{bmatrix},$$

and the time-delay boundaries are as $\tau_m=3$, $\tau_M=4$. Assumption 1 is easily verified by using

$$\mathcal{D}_{1f}=\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & -0.75\end{bmatrix},\ \mathcal{D}_{2f}=\begin{bmatrix}0.2 & 0 & 0\\ 0 & -0.2 & 0\\ 0 & 0 & 0.2\end{bmatrix},$$

$$\mathcal{D}_{1g}=\mathcal{D}_{1h}=\begin{bmatrix}0.1 & 0 & 0\\ 0 & 0.1 & 0\\ 0 & 0 & 0.1\end{bmatrix},$$

$$\mathcal{D}_{2g} = \mathcal{D}_{2h} = \begin{bmatrix} 0.2 & 0 & 0 \\ 0 & -0.2 & 0 \\ 0 & 0 & 0.2 \end{bmatrix}.$$

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

$$m\left(x_i(k)\right) = \begin{bmatrix} 0.02\sin\left(x_1\right) & 0 & 0 \\ 0 & 0.02\cos\left(x_2\right) & 0 \\ 0 & 0 & 0.03\sin\left(x_3\right) \end{bmatrix},$$

$$h\left(x_i(k)\right) = \begin{bmatrix} 0.02\sin\left(x_1\right) & -0.01\cos\left(x_1\right) & -0.01\tanh\left(x_1\right) \\ -0.02\sin\left(x_2\right) & 0 & 0 \\ 0 & 0 & 0.01\sin\left(x_3\right) \end{bmatrix}.$$

The probabilities of FDI attack for the two selected network nodes are $\pi_1 = 0.15$ and $\pi_2 = 0.20$, respectively. $i \in \mathcal{V}_{Pin}$ denotes the i-th network nodes.

The random FDI attacks' attack times of the two network nodes are shown in Figure 2. The energy evolution trajectory of a physical attack on two network nodes is given in Figure 3. Figures 4-6 plot the state evolutions trajectory of the synchronization error of the uncontrolled, which show that the network node cannot be synchronization with the unforced isolated node.

Let the thresholds of dynamic trigger conditions (7) be $\rho_1 = 0.17$ and $\rho_2 = 0.15$, and other parameters are selected as $\varepsilon_1 = 0.45$, $\varepsilon_2 = 0.55$, $\psi_1 = 5.8$ as well as $\psi_2 = 6.8$, respectively. Applying Theorem 2 and solving LMIs (32)-(34), a set of feasible solutions and the corresponding synchronization control gains matrices can be obtained as follow:

$\mu_1 = 4.5861$, $\mu_2 = 6.0727$, $\mu_3 = 5.7304$, $\mu_4 = 6.1709$,

$$K_1 = \begin{bmatrix} -0.9210 & 0.0051 & 0.0075 \\ 0.2979 & -0.1494 & -0.0014 \\ 0.1400 & -0.0695 & -0.4595 \end{bmatrix},$$

$$K_2 = \begin{bmatrix} -0.0821 & 0.0255 & 0.0131 \\ 0.0975 & -0.1085 & -0.0010 \\ 0.1370 & -0.0668 & 1.2269 \end{bmatrix}.$$

Figure 2
Attack time of the FDI attacks

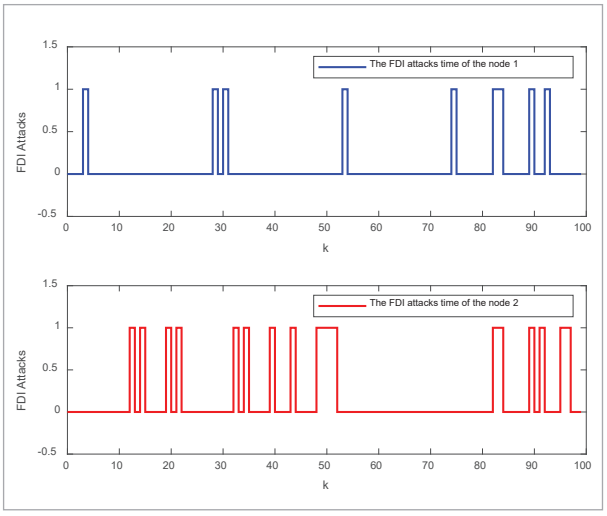


Figure 3
Energy evolution of the physical attacks

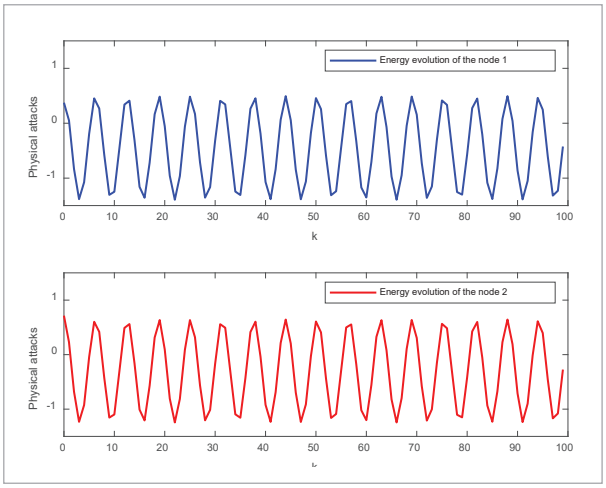


Figure 4
Synchronization error $e_i^1(k), (i = 1,2,3)$ trajectory of the uncontrolled

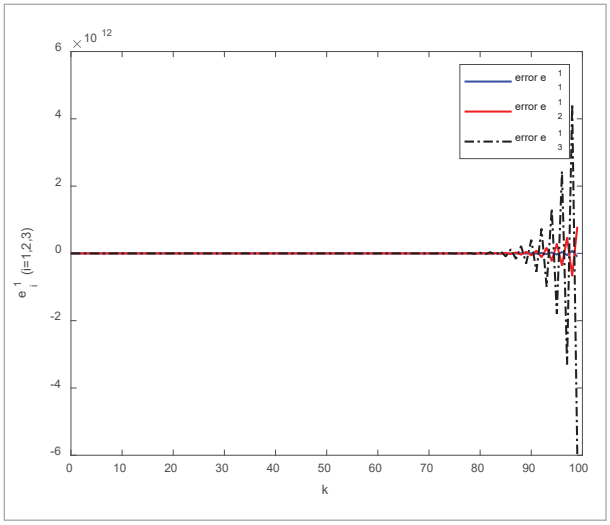


Figure 5
Synchronization error $e_i^2(k),(i=1,2,3)$ trajectory of the uncontrolled

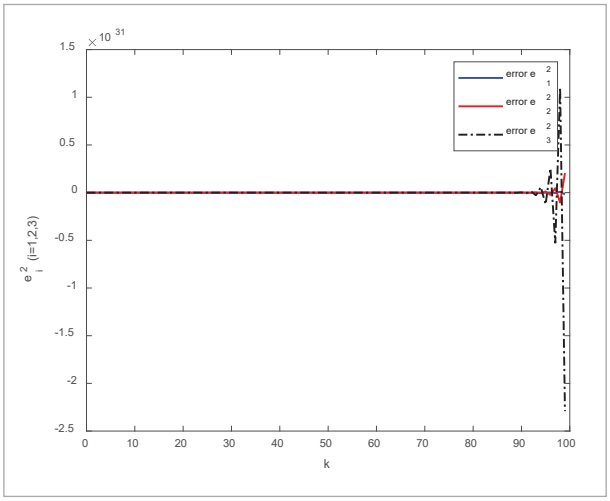
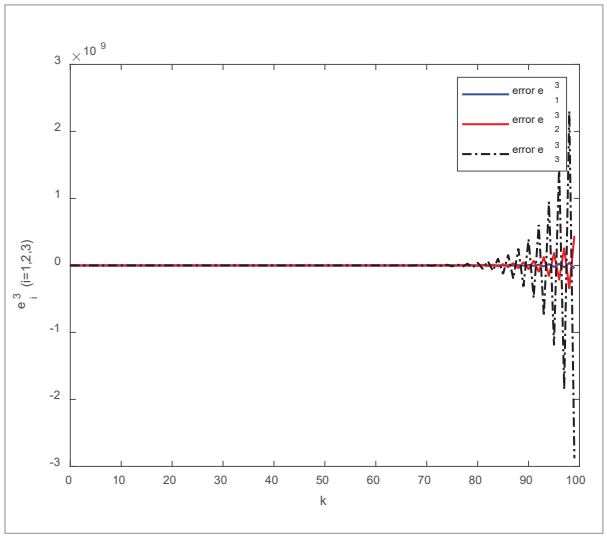


Figure 6
Synchronization error $e_i^3(k),(i=1,2,3)$ trajectory of the uncontrolled



The initial condition of complex cyber-physical networks and the unforced isolate node are set as $x_i(0)=[1 \quad -1 \quad 1]^T$ and $s(0)=[2 \quad -0.5 \quad -2]^T$, respectively. The initial value of internal dynamic variables for the dynamic event-triggering strategy is set as $\chi_0^1=8.5$ and $\chi_0^2=8.6$, respectively. In this case, the trajectories of synchronization error between the unforced isolated node and the network nodes are shown by Figures 7-9, respectively. It could be found from Figures 7-9 that the synchronization errors converge to zero within the limited sampling periods, which implies that the presented event-based pinning control method is effective for the complex cyber-physical networks subject to all-around attack. Subsequently, the results of dynamic event triggering communication are compared with those of static event triggering communication. Figures 10-11 show the triggered instants associated with nodes 1 and 2 for the dynamic and static

Figure 7
Synchronization error $e_i^1(k),(i=1,2,3)$ trajectory of the controlled

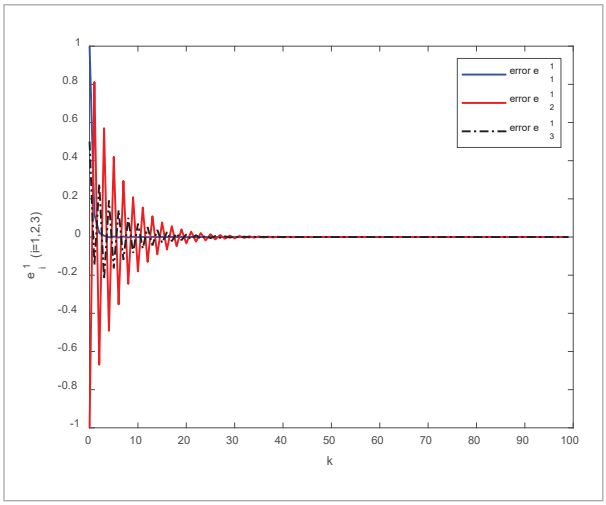
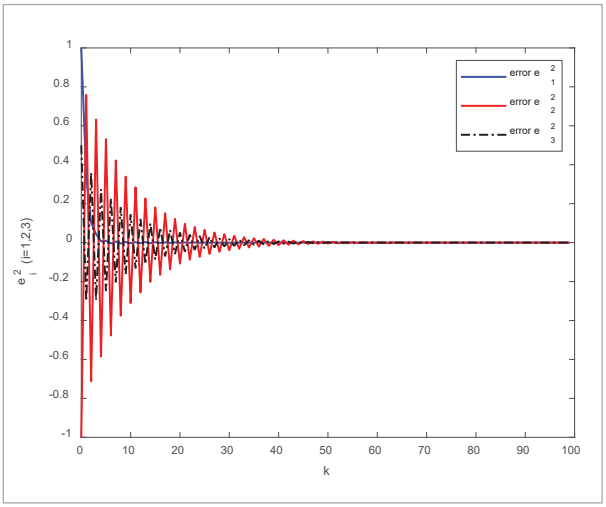


Figure 8
Synchronization error $e_i^2(k),(i=1,2,3)$ trajectory of the controlled



event-triggering schemes, respectively. It can be seen from Figures 10-11 that the dynamic event triggering communication has far fewer times than its static counterpart. Therefore, it is easy to conclude that the dynamic events triggering strategy can effectively reduce the updating frequency of the control signals compared with the static ones.

Figure 9

Synchronization error $e_i^3(k),(i=1,2,3)$ trajectory of the controlled

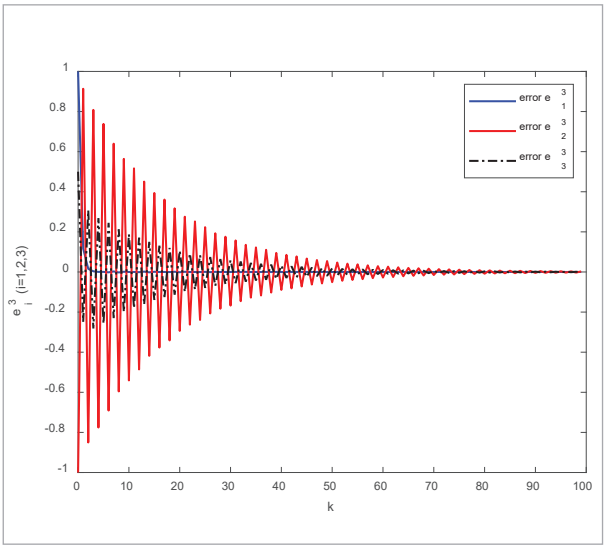


Figure 10

Triggering instants of the dynamic event trigger

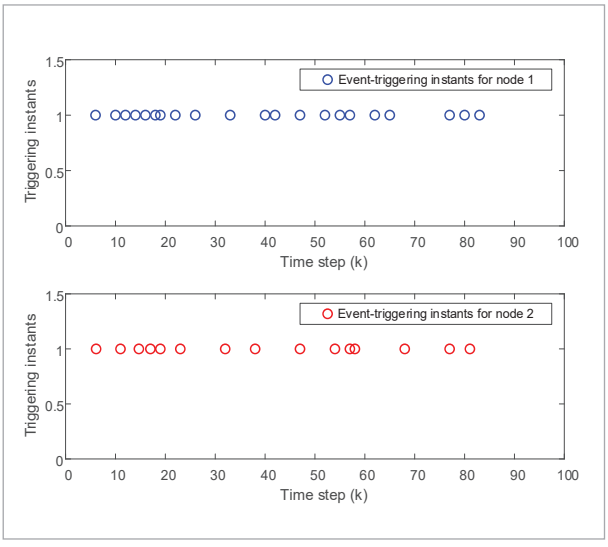
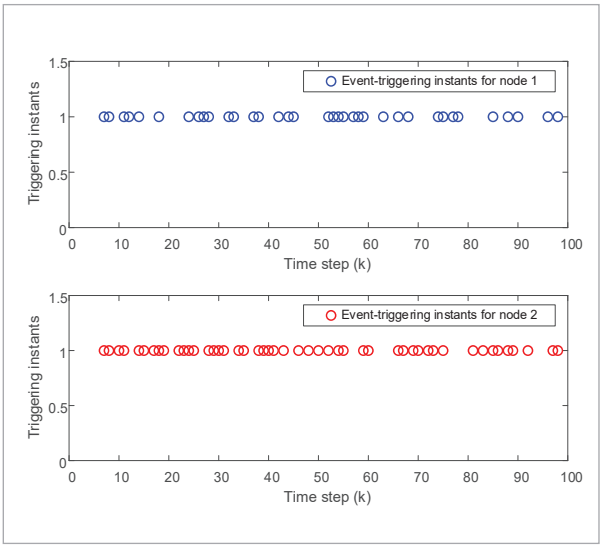


Figure 11

Triggering instants of the static event trigger



5. Conclusion

In this paper, the dynamic event-triggered pinning synchronization control issue has been investigated for the discrete-time delayed complex cyber-physical networks under all-around attacks. By using some linear matrix inequalities and the piecewise Lyapunov-like functions, an ultimately exponentially bounded condition has been derived for the closed-loop synchronization error dynamics. Furthermore, the special case of pinning synchronization control method based on static event-triggered scheme have also been addressed for the complex cyber-physical networks subject to all-around attacks. In addition, it is interesting to consider the synchronization control problem for complex cyber-physical networks with fast-varying input delays and complex cyber-physical attacks, which is our future works.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China under Grants 61863026 and 61563031, in part by the Major Science and Technology Special Project of Gansu Province under Grant 21ZD4GA028.

References

1. Ali, M. S., Yogambigai, J., Cao, J. Synchronization of Master-Slave Markovian Switching Complex Dynamical Networks with Time-Varying Delays in Nonlinear Function via Sliding Mode Control. Acta Mathematica Scientia, 2017, 37(2), 368-384. https://doi.org/10.1016/j.amc.2017.05.007
2. Babadi, N., Doustmohammadi, A. A Moving Target Defence Approach for Detecting Deception Attacks on Cyber-Physical Systems. Computers and Electrical Engineering, 2022, 100, 107931. https://doi.org/10.1016/j.compeleceng.2022.107931
3. Boccaletti, S., Latora, V., Moreno, Y., Hwang, D. U. Complex Networks: Structure and Dynamics. Physics Reports, 2006, 424(4-5), 175-308. https://doi.org/10.1016/j.physrep.2005.10.009
4. Chen, Y., Wang, Z., Hu, J., Han, Q. L. Synchronization Control for Discrete-Time-Delayed Dynamical Networks with Switching Topology Under Actuator Saturations. IEEE Transactions on Neural Networks and Learning Systems, 2020, 32(5), 2040-2053. https://doi.org/10.1109/TNNLS.2020.2996094
5. DeLellis, P., Di, B. M., Garofalo, F. Adaptive Pinning Control of Networks of Circuits and Systems in Lur'e Form. IEEE Transactions on Circuits and Systems I: Regular Papers, 2013, 60(11), 3033-3042. https://doi.org/10.1109/TCSI.2013.2252714
6. Ding, S., Wang, Z., Rong, N. Intermittent Control for Quasisynchronization of Delayed Discrete-Time Neural Networks. IEEE Transactions on Cybernetics, 2020, 51(2), 862-873. https://doi.org/10.1109/TCYB.2020.3004894
7. Dong, L., Xu, H. Secure Correct Control for Cyber-Physical Systems under Multiple Stochastic Physical Attacks. Proceedings of IEEE 32th Chinese Control and Decision Conference, (CCDC 2020), Hefei, China, August 22-24, 2020, 3824-3829. https://doi.org/10.1109/CCDC49329.2020.9164734
8. Guan, Y., Wu, Y., Wu, H., Li, Y., He, S. Synchronization of Complex Dynamical Networks with Actuator Saturation by Using Sampled-Data Control. Circuits Systems & Signal Processing, 2019, 38(12), 5508-5527. https://doi.org/10.1007/s00034-019-01154-6
9. Güven, E. Y., Çamurcu, A. Physical Attack Detection for Smart Objects. Proceedings of IEEE International Conference on Artificial Intelligence and Data Processing (IDAP 2018), Malatya, Turkey, September 28-30, 2018, 1-5. https://doi.org/10.1109/IDAP.2018.8620791
10. Hu, L., Wang, Z., Han, Q. L., Liu, X. State Estimation Under False Data Injection Attacks: Security Analysis and System Protection. Automatica, 2018, 87, 176-183. https://doi.org/10.1016/j.automatica.2017.09.028
11. Li, D., Gebraeel, N., Paynabar, K. Detection and Differentiation of Replay Attack and Equipment Faults in SCADA Systems. IEEE Transactions on Automation Science and Engineering, 2020, 99, 1-14. https://doi.org/10.1109/TASE.2020.3013760
12. Li, F., Tang, Y. False Data Injection Attack for Cyber-Physical Systems with Resource Constrain. IEEE Transactions on Cybernetics, 2018, 50(2), 729-738. https://doi.org/10.1109/TCYB.2018.2871951
13. Li, Q., Shen, B., Wang, Z., Luo, J. Synchronization Control for a Class of Discrete Time-Delay Complex Dynamical Networks: A Dynamic Event-Triggered Approach. IEEE Transactions on Cybernetics, 2018, 49(5), 1979-1986. https://doi.org/10.1109/TCYB.2018.2818941
14. Liu, J., Suo, W., Xie, X., Yue, D., Cao, J. Quantized Control for a Class of Neural Networks with Adaptive Event-Triggered Scheme and Complex Cyber Attacks. International Journal of Robust and Nonlinear Control, 2021, 31(10), 4705-4728. https://doi.org/10.1002/rnc.5500
15. Liu, S., Xu, T., Tian, E. Event-Based Pinning Synchronization Control for Time-Delayed Complex Dynamical Networks: The Finite-Time Boundedness. IEEE Transactions on Signal and Information Processing over Networks, 2021, 7, 730-739. https://doi.org/10.1109/TSIPN.2021.3125132
16. Liu, X., Chen, T. Synchronization of Nonlinear Coupled Networks via Aperiodically Intermittent Pinning Control. IEEE Transactions on Neural Networks and Learning Systems, 2014, 26(1), 113-126. https://doi.org/10.1109/TNNLS.2014.2311838
17. Lu, J., Guo, Y., Ji, Y., Fan, S. S. Finite-Time Synchronization for Different Dimensional Fractional-Order Complex Dynamical Networks. Chaos, Solitons & Fractals, 2020, 130, 109433. https://doi.org/10.1016/j.chaos.2019.109433
18. Ma, L., Wang, Z., Lam, H. K. Event-Triggered Mean-Square Consensus Control for Time-Varying Stochastic Multi-Agent System with Sensor Saturations. IEEE

Transactions on Automatic Control, 2016, 62(7), 3524-3531. https://doi.org/10.1109/TAC.2016.2614486

19. Malliga, S., Nandhini, P. S., Kogilavani, S. V. A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks. Information Technology and Control, 2022, 51(1), 180-215. https://doi.org/10.5755/j01.itc.51.1.29595
20. Qian, W., Wang, L., Chen, M. Z. Q. Local Consensus of Nonlinear Multiagent Systems with Varying Delay Coupling. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017, 48(12), 2462-2469. https://doi.org/10.1109/TSMC.2017.2684911
21. Rodriguez-Castellanos, D., Solis-Perales, G., Alanis, A. Y., Sanchez, E. N., Chen, G., Vega, C. J. Neural Pinning Control for Adaptive Trajectory Tracking of Complex Dynamical Networks. Mathematical Methods in the Applied Sciences, 2022, 1-19. https://doi.org/10.1002/mma.8389
22. Shen, B., Wang, Z., Liu, X. Sampled-Data Synchronization Control of Dynamical Networks with Stochastic Sampling. IEEE Transactions on Automatic Control, 2012, 57(10), 2644-2650. https://doi.org/10.1109/TAC.2012.2190179
23. Wang, B., Chen, W., Zhang, B. Semi-Global Robust Tracking Consensus for Multi-Agent Uncertain Systems with Input Saturation via Metamorphic Low-Gain Feedback. Automatica, 2019, 103, 363-373. https://doi.org/10.1016/j.automatica.2019.02.002
24. Wang, L., Wang, Z., Han, Q. L., Wei, G. Synchronization Control for a Class of Discrete-Time Dynamical Networks with Packet Dropouts: A Coding-Decoding-Based Approach. IEEE Transactions on Cybernetics, 2017, 48(8), 2437-2448. https://doi.org/10.1109/TCYB.2017.2740309
25. Wang, L., Wang, Z., Huang, T., Wei, G. An Event-Triggered Approach to State Estimation for a Class of Complex Networks with Mixed Time Delays and Nonlinearities. IEEE Transactions on Cybernetics, 2015, 46(11), 2497-2508. https://doi.org/10.1109/TCYB.2015.2478860
26. Wang, L., Wang, Z., Wei, G., Alsaadi, F. E. Finite-Time State Estimation for Recurrent Delayed Neural Networks with Component-Based Event-Triggering Protocol. IEEE Transactions on Neural Networks and Learning Systems, 2017, 29(4), 1046-1057. https://doi.org/10.1109/TNNLS.2016.2635080
27. Wen, G., Wang, P., Yu, X., Yu, W., Cao, J. Pinning Synchronization of Complex Switching Networks with a Leader of Nonzero Control Inputs. IEEE Transactions on Circuits and Systems I: Regular Papers, 2019, 66(8), 3100-3112. https://doi.org/10.1109/TCSI.2019.2904946
28. Wen, G., Yu, W., Yu, X., Lu, J. Complex Cyber-Physical Networks: From Cybersecurity to Security Control. Journal of Systems Science and Complexity, 2017, 30(1), 46-67. https://doi.org/10.1007/s11424-017-6181-x
29. Wu, L., Fu, X. A Novel Approach for Synchronizing of Fractional Order Uncertain Chaotic Systems in the Presence of Unknown Time-Variant Delay and Disturbance. Information Technology and Control, 2022, 51(2), 221-234. https://doi.org/10.5755/j01.itc.51.2.29411
30. Xu, Y., Guo, G. Event Triggered Control of Connected Vehicles Under Multiple Cyber Attacks. Information Sciences, 2021, 582, 778-796. https://doi.org/10.1016/j.ins.2021.10.032
31. Yin, H., Jayawardhana, B., Reyes-Báez, R. Pinning Synchronization of Heterogeneous Multi-Agent Nonlinear Systems via Contraction Analysis. IEEE Control Systems Letters, 2022, 6, 157-162. https://doi.org/10.1109/LCSYS.2021.3053493
32. Yu, W., Chen, G., Lu, J. On Pinning Synchronization of Complex Dynamical Networks. Automatica, 2009, 45(2), 429-435. https://doi.org/10.1016/j.automatica.2008.07.016
33. Zhang, C. K., He, Y., Jiang, L., Wu, M. Stability Analysis of Discrete-Time Neural Networks with Time-Varying Delay via an Extended Reciprocally Convex Matrix Inequality. IEEE Transactions on Cybernetics, 2017, 47(10), 3040-3049. https://doi.org/10.1109/TCYB.2017.2665683
34. Zhang, T. Y., Ye, D. False Data Injection Attacks with Complete Stealthiness in Cyber-Physical Systems: A Self-Generated Approach. Automatica, 2020, 120, 109117. https://doi.org/10.1016/j.automatica.2020.109117