Zhou *et al*. *Complex Eng Syst* 2023;3:14
DOI: 10.20517/ces.2023.16

Complex Engineering Systems

Research Article

Open Access

Event-triggered state estimation for complex networks under deception attacks: a partial-nodes-based approach

Lu Zhou, Bing Li

School of Mathematics and Statistics, Chongqing Jiaotong University, Chongqing 400074, China.

Correspondence to: Prof. Bing Li, Department of Applied Mathematics, Chongqing Jiaotong University, No. 66, XueFu Avenue, Chongqing 400074, China. E-mail: libingcnjy@163.com

How to cite this article: Li B, Zhou L. Event-triggered state estimation for complex networks under deception attacks: a partial-nodes-based approach. *Complex Eng Syst* 2023;3:14. http://dx.doi.org/10.20517/ces.2023.16

Received: 26 May 2023 **First Decision:** 19 Jun 2023 **Revised:** 20 Jul 2023 **Accepted:** 22 Aug 2023 **Published:** 29 Aug 2023

Academic Editor: Hamid Reza Karimi, Yurong Liu **Copy Editor:** Fanglin Lan **Production Editor:** Fanglin Lan

Abstract

This paper addresses the issue of state estimation for a kind of complex network (CN) with distributed delays and random interference through output measurements. In the data transmission, the deception attacks are taken into account by resorting to a sequence of Bernoulli random variables with a given probability. Considering the complexity of the network, the fact that only partial output measurements are available in practical environments presents a new challenge. Therefore, the partial-nodes-based (PNB) state estimation problem is proposed. For the sake of data collision avoidance and energy saving, a general event-triggered scheme is adopted in the design of the estimator. A novel estimator is constructed to consider both cyber attacks and resource limitations, filling the gap in previous results on PNB state estimation. By using the Lyapunov method and several stochastic analysis techniques, a few sufficient conditions are derived to guarantee the desired security and convergency performance for the overall estimation error. The estimator gains are obtained by solving a set of matrix inequalities with nonlinear constraints. At last, two examples and simulations are presented to further show the efficiency of the proposed method.

Keywords: Complex networks (CNs), deception attacks, partial-nodes-based (PNB) estimation, event-triggered scheme, finite-distributed delays

1. INTRODUCTION

Over the past few decades, complex networks (CNs) have gained significant research interest due to their diverse applications in natural and artificial systems, including but not limited to sensor networks, biological networks, and social networks, among others[1–6]. Generally speaking, a CN is composed of numerous nodes that can be described as various types of topologies. In CNs, each individual node exhibits intricate and diverse dynamical behavior[7,8], which results in plenty of dynamics, including synchronization, chaos, and so on. Furthermore, it is widely acknowledged that time delays are an inevitable factor in data transmission. This can lead to a decline in performance and introduce additional challenges during analysis. So far, a great deal of research effort has been devoted to dynamic analysis and control for CNs with delays[9–16].

In practical engineering, state information plays a key role in the analysis and design of CNs. However, the full state information is usually unavailable because of the large size of CNs, complex coupling relation, and inaccuracy of models. To cope with this issue, one possible solution is to estimate the state by using some available measurement outputs[17–23]. For example, in[17], a finite-time H_∞ state estimation problem has been investigated for genetic regulatory networks under stochastic communication protocols. In[18,19], the state estimation problems have been examined for different classes of CNs subject to both discrete and distributed time delays. For the state estimation of CNs, it should be noted that the majority of the existing literature has assumed the outputs of all nodes are accessible[24]. However, when a CN possesses a huge number of nodes, it might be unreasonable (even impossible) to get all outputs. Additionally, the sensor failure can also result in some output not being obtained. Taking these problems into consideration, a partial-node-based (PNB) state estimation, which implements the state estimation only via partial measurements of CNs, has attracted more and more research attention[25–29].

In the networked communication environment, the components are usually interconnected through a shared communication network. On the one hand, during information transmission, opponents or attackers may capture and manipulate interchanged information between components, which causes degraded network performance or even destabilization of the system[30]. A lot of research works have been done to focus on cyber attacks[31–39]. For instance, the state estimation issue has been investigated for large-scale systems subjected to deception attacks in[33]. In[38], H_∞ state estimation problems have been studied for memristive neural networks with randomly occurring denial-of-service (DoS) attacks. On the other hand, because of limited communication resources, it is crucial to reduce the burden of communication resources and alleviate data congestion in data transmission. Recently, the event-triggered mechanism (ETM) has been extensively used for saving communication resources while maintaining the desired performance[40–42]. Compared with the traditional periodic triggered mechanism, the most distinguishing feature of ETMs is to transmit information only when certain triggered conditions are met, which allows a considerable reduction of the network resource occupancy. However, from the perspective of security levels against cyber attacks, the event-triggered PNB state estimation for CNs has rarely been investigated, which is the main motivation of this paper[43–46].

To sum up the above discussions, this paper aims to investigate the event-triggered PNB state estimation problem for CNs under deception attacks. There are two significant contributions of the current research: (1) By employing partial output measurements, an event-triggered state estimator is designed for CNs subjected to deception attacks; (2) With the aid of stochastic analysis techniques and the Lyapunov method, the gain matrices and the event-triggered parameters are co-designed (by resorting to solutions of matrices inequalities) to ensure the desired secure performance of closed-loop systems under the deception attacks and the aperiodic data updating. The rest of this paper is presented as follows. Section 2 gives the problem formulation. In Section 3, an event-triggered PNB state estimation scheme is put forward for CNs against deception attacks. Two numerical simulation examples are presented in Section 4 to further demonstrate the effectiveness of the proposed method. Finally, several conclusions are derived in Section 5.

Notation: $\mathbb{N}^0$ denotes the set of nonnegative integers. $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ represent the n-dimensional Euclidean space and the set of all $n\times m$ real matrices, respectively. I denotes the identity matrix of compatible dimension. $\|\cdot\|$ denotes the Euclidean norm. $\mathbb{E}\{x\}$ is the expectation of the stochastic variable x. diag$\{\cdots\}$ describes a block-diagonal matrix. $\lambda_{min}(\cdots)(\lambda_{max}(\cdots))$ means the smallest (largest) eigenvalue. $A > 0$ means that A is positive definite. The symbol "$\otimes$" stands for the Kronecker product.

2. MODEL DESCRIPTION

Consider a class of discrete-time CNs with N coupled nodes as follows:

$$\begin{cases} x_i(k+1) = A_i x_i(k) + f(x_i(k)) + A_{di}\sum_{s=1}^{\tau(k)} g(x_i(k-s)) + \sum_{j=1}^{N} w_{ij}\Gamma x_j(k) + B_i v_i(k) \\ \bar{y}_i(k) = C_i x_i(k) + D_i v_i(k) \\ z_i(k) = E_i x_i(k), i = 1,2,\ldots,N \\ x_i(r) = \phi_i(r), \forall r \in [-\tau_M, 0] \end{cases} \tag{1}$$

where $x_i(k) \in \mathbb{R}^n$ represents the state of the ith node, $\bar{y}_i(k) \in \mathbb{R}^m$ $(1 \le m \le n)$ denotes the measurement output, and $z_i(k) \in \mathbb{R}^q$ is the controlled output. The nonlinear vector-valued functions $f(\cdot)$ and $g(\cdot)$ are continuous and satisfy the conditions $f(0) = 0$, $g(0) = 0$, as well as

$$[f(x) - f(y) - U_1(x-y)]^T \times [f(x) - f(y) - U_2(x-y)] \le 0 \tag{2}$$

$$\|g(x) - g(y)\| \le \|\varphi(x-y)\|, \quad \forall x, y \in \mathbb{R}^n \tag{3}$$

where U_1, U_2, and $\varphi = diag\{\varphi_1, \varphi_2, \ldots, \varphi_n\} > 0$ are known constant real matrices with appropriate dimensions. The inner-coupling matrix $\Gamma = diag\{t_1, t_2, \ldots, t_n\} \ge 0$ denotes the linking of the state variable for jth $(j = 1,2,\ldots,n)$ node if $t_j \ne 0$. $v_i(k) \in \mathbb{R}$ is a Gaussian white noise sequence with $\mathbb{E}\{v_i(k)\} = 0$ and $\mathbb{E}\{v_i^2(k)\} \le \varepsilon^2$, $\varepsilon > 0$. Here, $A_i, A_{di}, B_i, C_i, D_i$, and E_i are parameter matrices with appropriate dimensions, $\phi_i(r)$ $(\forall r \in [-\tau_M, 0], i = 1,2,\ldots,N)$ are the initial conditions. The symmetric matrix $W = [w_{ij}] \in \mathbb{R}^{N\times N}$ is for the outer-coupling configuration of the CNs with $w_{ij} \ge 0$ $(i \ne j)$ but not all zero and satisfies $\sum_{j=1}^{N} w_{ij} = \sum_{j=1}^{N} w_{ji} = 0$ for $i = 1,2,\ldots,N$. The distributed delay $\tau(k)$ satisfies $\tau_m \le \tau(k) \le \tau_M$, where $\tau_m > 0$ and $\tau_M > 0$ are known integers.

Actually, the issue of data safety usually arises in networked environments since the data may be subject to malicious cyber attacks during the transmission. In this paper, we assume that the measurement from the output sensors is affected by deception attacks as follows:

$$y_i(k) = \bar{y}_i(k) + \vartheta(k)\varrho(k), \quad 1 \le i \le l_0 \tag{4}$$

where $\varrho(k) = -\bar{y}_i(k) + \xi(k)$ stands for the deceptive attack signal injected by the hostile attacker. $y_i(k) \in \mathbb{R}^m$ denotes the measurement signal received by neighboring nodes, $\xi(k) \in \mathbb{R}^m$ is deception data and satisfies

$$\|\xi(k)\| \le \varepsilon_1 \tag{5}$$

in which ε_1 is a given positive scalar for describing the intensity of deception attacks. $\vartheta(k)$ is a Bernoulli stochastic variable sequence, satisfying

$$Prob\{\vartheta(k) = 0\} = 1 - \bar{\vartheta}, \quad Prob\{\vartheta(k) = 1\} = \bar{\vartheta}$$

with $\bar{\vartheta} \in [0, 1)$.

Remark 1: From (4), it is noticeably known that $\vartheta(k) = 1$ represents deception attacks occur; the real data $\bar{y}_i(k)$ is replaced by false signal $\xi(k)$ from deception attacks. When $\vartheta(k) = 0$, the real measurement signal will be available.

For the purpose of saving limited communication resources, an ETM is introduced during the data transmission. For clarity, the triggering instant sequence for node i is denoted by $0 = k_0^i \leq \cdots \leq k_p^i \leq \ldots$, which is determined as follows

$$k_{p+1}^i = min\left\{k \in \mathbb{N}^0 | k > k_p^i,\ \pi_i(\mu_i(k), \delta_i) > 0\right\} \tag{6}$$

in which the event generator function $\pi_i(\cdot,\cdot)$ is constructed to be

$$\pi_i(\mu_i(k), \delta_i) = \mu_i^T(k)\mu_i(k) - \delta_i y_i^T(k) y_i(k) \tag{7}$$

with $\mu_i(k) = y_i(k) - y_i(k_p^i)$ and $\delta_i > 0$. Here, $y_i(k_p^i)$ is the final measurement of node i received by the estimator at the latest instant.

Remark 2: From the perspective of reducing the data transmission rate, it has been proven that the event-triggered scheme is an effective implementation approach under which the data transmission is permitted only if a prescribed condition is met. For clarity, let k_p^i be the latest triggering instant. For $k = k_p^i$, the event does not occur due to $(y_i(k)-y_i(k_p^i))^T(y_i(k)-y_i(k_p^i)) = 0$. When $(y_i(k)-y_i(k_p^i))^T(y_i(k)-y_i(k_p^i))-\delta_i(y_i^T(k)y_i(k))) \leq 0$ for some $k_p^i < k < k^*$ but $(y_i(k) - y_i(k_p^i))^T(y_i(k) - y_i(k_p^i)) - \delta_i(y_i^T(k)y_i(k))) > 0$ at k^*, the event occurs at time k^*. Thus, the output data received by estimators maintains $y_i(k_p^i)$ from k_p^i to $k^* - 1$ and then is updated to $y_i(k^*)$. In other words, the signals are only updated at some necessary instants. As such, the event-triggered scheme shows a significant advantage via reducing unnecessary information exchange between the sensors and estimators.

Within the event-triggered PNB scheme, the state estimator is constructed as follows:

$$\begin{cases} \hat{x}_i(k+1) = A_i\hat{x}_i(k) + f(\hat{x}_i(k)) + A_{di}\sum\limits_{s=1}^{\tau(k)} g(\hat{x}_i(k-s)) + \sum\limits_{j=1}^{N} w_{ij}\Gamma\hat{x}_j(k) \\ \qquad + K_i\left(y_i(k_p^i) - C_i\hat{x}_i(k)\right), \quad i = 1, 2, \ldots, l_0 \\ \hat{x}_i(k+1) = A_i\hat{x}_i(k) + f(\hat{x}_i(k)) + A_{di}\sum\limits_{s=1}^{\tau(k)} g(\hat{x}_i(k-s)) + \sum\limits_{j=1}^{N} w_{ij}\Gamma\hat{x}_j(k), \\ \qquad i = l_0+1, l_0+2, \ldots, N \\ \hat{z}_i(k) = E_i\hat{x}_i(k) \end{cases} \tag{8}$$

where $\hat{x}_i(k)$ denotes the estimated state of $x_i(k)$, and $K_i \in \mathbb{R}^{n\times m}$ $(i = 1, \ldots, l_0)$ are the gain matrices to be designed.

We denote by $e_i(k) = x_i(k) - \hat{x}_i(k)$ and $\tilde{z}_i(k) = z_i(k) - \hat{z}_i(k)$ the state and output error, respectively. For convenience of later analysis, let

$$
\begin{aligned}
&\mathfrak{I} = \begin{bmatrix}\mathfrak{I}_1^T & \mathfrak{I}_2^T & \cdots & \mathfrak{I}_N^T\end{bmatrix}^T (\mathfrak{I} = x(k), v(k), e(k), \tilde{z}(k)) \\
&\mathfrak{R} = \begin{bmatrix}\mathfrak{R}_1^T & \mathfrak{R}_2^T & \cdots & \mathfrak{R}_{l_0}^T\end{bmatrix}^T (\mathfrak{R} = \mu(k), y(k)), \quad \bar{C} = [C \quad 0] \\
&R(x(k)) = \begin{bmatrix}r^T(x_1(k)) & \cdots & r^T(x_N(k))\end{bmatrix}^T, \quad \bar{K} = \begin{bmatrix}K^T & 0\end{bmatrix}^T, \quad \bar{D} = [D \quad 0] \\
&R(e(k)) = \begin{bmatrix}\tilde{r}^T(e_1(k)) & \cdots & \tilde{r}^T(e_N(k))\end{bmatrix}^T (R = F, G; r = f, g) \\
&\aleph = diag\{\aleph_1, \aleph_2, \ldots, \aleph_N\} (\aleph = A, A_d, B, E), \quad S_1 = [I \quad I \quad \cdots \quad I]^T_{m\times l_0 m} \\
&\Omega = diag\left\{\delta_1 I, \delta_2 I, \ldots, \delta_{l_0} I\right\}, \quad \mho = diag\left\{\mho_1, \mho_2, \ldots, \mho_{l_0}\right\} (\mho = K, C, D) \\
&\tilde{f}(e_i(k)) = f(x_i(k)) - f(\hat{x}_i(k)), \quad \tilde{g}(e_i(k)) = g(x_i(k)) - g(\hat{x}_i(k)).
\end{aligned}
$$

The error system is obtained as follows:

$$
\begin{cases}
e(k+1) = Ae(k) + F(e(k)) + A_d \sum_{s=1}^{\tau(k)} G(e(k-s)) \\
\qquad + W\otimes\Gamma e(k) + Bv(k) - \bar{K}\bar{C}e(k) - (1-\bar{\vartheta})\bar{K}\bar{D}v(k) \\
\qquad + (\vartheta(k)-\bar{\vartheta})\bar{K}\bar{D}v(k) + (\vartheta(k)-\bar{\vartheta})\bar{K}\bar{C}x(k) + \bar{\vartheta}\bar{K}\bar{C}x(k) \\
\qquad - (\vartheta(k)-\bar{\vartheta})\bar{K}S_1\xi(k) - \bar{\vartheta}\bar{K}S_1\xi(k) + \bar{K}\mu(k), \\
\tilde{z}(k) = Ee(k).
\end{cases} \tag{9}
$$

By defining $\eta(k) = \begin{bmatrix}x^T(k) & e^T(k)\end{bmatrix}^T$ and $R(\eta(k)) = \begin{bmatrix}R^T(x(k)) & R^T(e(k))\end{bmatrix}^T$ $(R = F, G)$, we derive the following augmented system:

$$
\begin{cases}
\eta(k+1) = \mathcal{A}\eta(k) + (\vartheta(k)-\bar{\vartheta})\mathcal{C}\eta(k) + F(\eta(k)) + \mathcal{A}_d \sum_{s=1}^{\tau(k)} G(\eta(k-s)) \\
\qquad + (\mathcal{B} - (1-\bar{\vartheta})\mathcal{D})v(k) + (\vartheta(k)-\bar{\vartheta})\mathcal{D}v(k) - \bar{\vartheta}\mathcal{S}_1\xi(k) \\
\qquad - (\vartheta(k)-\bar{\vartheta})\mathcal{S}_1\xi(k) + \mathcal{S}_2\vec{\mu}(k) \\
\tilde{z}(k) = \bar{E}\eta(k)
\end{cases} \tag{10}
$$

where

$$
\begin{aligned}
&\mathcal{A} = \begin{bmatrix} A + W\otimes\Gamma & 0 \\ \bar{\vartheta}\bar{K}\bar{C} & A + W\otimes\Gamma - \bar{K}\bar{C}\end{bmatrix}, \\
&\mathcal{A}_d = diag\{A_d,\ A_d\},\ \bar{E} = \begin{bmatrix} 0 & E \end{bmatrix},\ \mathcal{B} = \begin{bmatrix} B^T & B^T \end{bmatrix}^T, \\
&\mathcal{C} = \begin{bmatrix} 0 & 0 \\ \bar{K}\bar{C} & 0 \end{bmatrix},\ \mathcal{D} = \begin{bmatrix} 0 \\ \bar{K}\bar{D} \end{bmatrix},\ \mathcal{S}_1 = \begin{bmatrix} 0 \\ \bar{K}S_1 \end{bmatrix}, \\
&\mathcal{S}_2 = \begin{bmatrix} 0 & 0 \\ 0 & \bar{K} \end{bmatrix},\ \bar{\mathcal{C}} = \begin{bmatrix} \bar{C} & 0 \end{bmatrix},\ \vec{\mu}(k) = \begin{bmatrix} 0 & \mu^T(k) \end{bmatrix}^T.
\end{aligned}
$$

Remark 3: It is obviously noted that the estimation error system (9) is a subsystem of the augmented system (10). That is to say, the evolution of errors can be derived by analyzing the dynamic of the augmented system (10).

The definition and lemmas presented in this context play a crucial role in the stability analysis of the augmented system (10) and the design of an appropriate estimator.

Definition 1 [36]*:* For given constants $\varepsilon, \varepsilon_1, \varepsilon_2$, and ε_3, the augmented system (10) is said to be $(\varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3)$-secure if for $i = 1, 2, \ldots, N, \mathbb{E}\{v_i^2(k)\} \leq \varepsilon^2, \|\xi(k)\| \leq \varepsilon_1$, and the initial condition $\sup_{r=-\tau_M,-\tau_M+1,\ldots,-1,0} \mathbb{E}\{\|\phi_i(r)\|^2\} \leq \varepsilon_2^2$ imply that $\mathbb{E}\{\|\tilde{z}(k)\|^2\} \leq \varepsilon_3^2, k \geq \tau_M + 1$.

Remark 4: The parameter ε plays a crucial role in determining the overall disturbance bound. Specifically, ε_1 is employed for the level of deception attack, while ε_2 shows the impact of the initial error states. Lastly, ε_3 stands for the required performance of security.

Lemma 1 [47]*:* For a matrix $Q > 0$, integers l_1 and l_2 $(l_2 \geq l_1 \geq 0)$ and $x(\iota) \in \mathbb{R}^n$ for $\iota = i-l_2, i-l_2+1, \ldots, i-l_1$, the following inequality is valid:

$$-(l_2 - l_1 + 1) \sum_{k=i-l_2}^{i-l_1} x^T(k) Q x(k) \leq -\left(\sum_{k=i-l_2}^{i-l_1} x(k)\right)^T Q \left(\sum_{k=i-l_2}^{i-l_1} x(k)\right). \tag{11}$$

Lemma 2 [36]*:* For constants $M > 0$, $b > 0$ $(b \leq M-1)$, a scalar $a > 1$, and vectors $x(\zeta)$ $(\zeta = -b, \ldots, M-2)$, we have

$$\sum_{k=0}^{M-1} \sum_{\zeta=k-b}^{k-1} a^k \mathbb{E}\left\{\|x(\zeta)\|^2\right\} \leq \frac{a^b - 1}{a - 1}\left(\sum_{\zeta=-b}^{-1} \mathbb{E}\left\{\|x(\zeta)\|^2\right\} + 2a \sum_{k=0}^{M-1} a^k \mathbb{E}\left\{\|x(k)\|^2\right\}\right)$$

3. ANALYSIS AND RESULTS

In this section, by resorting to the stochastic analysis techniques, we shall provide the analysis result to guarantee that the augmented system (10) is $(\varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3)$-secure. For ease of subsequent analysis, we denote

$$\Theta_0 = \begin{bmatrix} \Theta_{011} & \Theta_{012} \\ \Theta_{021} & \Theta_{022} \end{bmatrix}, \quad \bar{P} = I_{4\times 4} \otimes P, \quad \gamma^2 = \lambda_1 N \varepsilon^2 + \lambda_2 \varepsilon_1^2$$

$$\Theta_{011} = \begin{bmatrix} \Pi_{011} & \lambda_3(I \otimes \bar{U}_2) & 0 \\ \lambda_3(I \otimes \bar{U}_2^T) & -\lambda_3 I & 0 \\ 0 & 0 & \theta Q - \lambda_4 I \end{bmatrix}, \quad \tilde{\vartheta} = \sqrt{\bar{\vartheta}(1-\bar{\vartheta})}$$

$$\Theta_{012} = \begin{bmatrix} 0 & \lambda_5\psi_1 \bar{C}^T \Omega \bar{D} & \lambda_5 \psi_2 \bar{C}^T \Omega S_1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \psi_3 = \bar{\vartheta}^2, \quad \psi_1 = (1-\bar{\vartheta})^2$$

$$\Theta_{021} = \begin{bmatrix} 0 & 0 & 0 \\ \lambda_5 \psi_1 \bar{D}^T \Omega \bar{C} & 0 & 0 \\ \lambda_5 \psi_2 S_1^T \Omega \bar{C} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \hat{U}_2 = \frac{U_1^T U_2 + U_2^T U_1}{2}, \quad \bar{U}_2 = \frac{U_2^T + U_1^T}{2}$$

$$\Theta_{022} = \begin{bmatrix} -\frac{1}{\tau_M} Q & 0 & 0 & 0 \\ 0 & -\lambda_1 I + \lambda_5 \psi_1 \bar{D}^T \Omega \bar{D} & \lambda_5 \psi_2 \bar{D}^T \Omega S_1 & 0 \\ 0 & \lambda_5 \psi_2 S_1^T \Omega \bar{D} & -\lambda_2 I + \lambda_5 \psi_3 S_1^T \Omega S_1 & 0 \\ 0 & 0 & 0 & -\lambda_5 I \end{bmatrix}$$

$$\Pi_{011} = -P - \lambda_3 (I \otimes \hat{U}_2) + \lambda_4 (I \otimes (\varphi^T \varphi)) + \lambda_5 \psi_1 \bar{C}^T \Omega \bar{C}, \quad \Theta_1 = \begin{bmatrix} \Theta_{111} & \Theta_{112} \\ 0 & \Theta_{122} \end{bmatrix}$$

$$\theta = 2\tau_M - \tau_m + \frac{(\tau_M - \tau_m)(\tau_m + \tau_M - 1)}{2}, \quad \Theta_{112} = \begin{bmatrix} 0 & -\tilde{\vartheta} \mathcal{S}_1 & 0 \\ 0 & -\tilde{\vartheta} \mathcal{S}_1 & 0 \end{bmatrix}$$

$$\Theta_{111} = \begin{bmatrix} \mathcal{A} & I & 0 & \mathcal{A}_d \\ \tilde{\vartheta} \mathcal{C} & 0 & 0 & 0 \end{bmatrix}, \quad \Theta_{122} = \begin{bmatrix} \mathcal{B} - (1-\bar{\vartheta})\mathcal{D} & 0 & 0 \\ \tilde{\vartheta} \mathcal{D} & 0 & \mathcal{S}_2 \end{bmatrix}, \quad \psi_2 = (\bar{\vartheta} - \bar{\vartheta}^2).$$

For the $(\varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3)$-security of the dynamic system (10), we have the following results.

Theorem 1: Let positive constants ε, ε_1, ε_2, ε_3 and matrices K_i $(i = 1, 2, \ldots, l_0)$ be known. The dynamic system (10) is $(\varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3)$-secure provided that there exist positive definite matrices P, Q and positive scalars λ_i $(i = 1, \cdots, 5)$ satisfying

$$\begin{cases} \Theta = \Theta_0 + \Theta_1^T \bar{P} \Theta_1 < 0 \\ \lambda_{max}(\bar{E}^T \bar{E}) max\{\bar{\varpi}(b_0), \bar{b}_0\} \le \varepsilon_3^2 \end{cases} \tag{12}$$

in which

$$\bar{\varpi}(b_0) = \frac{\varpi(b_0)}{\lambda_{min}(P)}, \qquad \bar{b}_0 = \frac{b_0 \gamma^2}{(b_0 - 1)\lambda_{min}(P)}, \tag{13}$$

the constant $b_0 > 1$ is determined as

$$\begin{aligned} & - b_0 \lambda_{min}(-\Theta) + (b_0 - 1)\lambda_{max}(P) + 2b_0(b_0^{\tau_M} - 1) \\ & \quad \times \lambda_{max}(Q)(\tau_M + (\tau_M - \tau_m) \times (\tau_M - 1))\lambda_{max}(I \otimes (\varphi^T \varphi)) \\ & = 0 \end{aligned} \tag{14}$$

and $\varpi(b_0)$ is given as follows:

$$\begin{aligned} \varpi(b_0) = {} & 2N\varepsilon_2^2(\tau_M \lambda_{max}(Q)(\tau_M + (\tau_M - \tau_m)(\tau_M - 1)) \times \lambda_{max}(I \otimes (\varphi^T \varphi))(b_0^{\tau_M} - 1) + \tau_M \\ & \times max\{\lambda_{max}(P), \lambda_{max}(Q)(\tau_M + (\tau_M - \tau_m) \times (\tau_M - 1))\lambda_{max}(I \otimes (\varphi^T \varphi))\}). \end{aligned}$$

Proof: We choose the Lyapunov-Krasovskii functional $V(\eta(k)) = \sum_{\iota=1}^{3} V_\iota(\eta(k))$ with

$$\begin{aligned} & V_1(\eta(k)) = \eta^T(k) P \eta(k), \qquad V_2(\eta(k)) = \sum_{j=1}^{\tau(k)} \sum_{i=k-j}^{k-1} G^T(\eta(i)) Q G(\eta(i)) \\ & V_3(\eta(k)) = \sum_{v=\tau_m+1}^{\tau_M} \sum_{j=1}^{v-1} \sum_{i=k-j}^{k-1} G^T(\eta(i)) Q G(\eta(i)). \end{aligned}$$

Here, $V_1(\eta(k))$ is chosen for the energy of the error system, $V_2(\eta(k))$ and $V_3(\eta(k))$ are adopted to deal with the evolution of state with distributed delays. By considering the difference of $V(\eta(k))$ with the system (10), and combing with the mathematical expectation, one has

$$\begin{aligned} \mathbb{E}\{\Delta V_1(\eta(k))\} & = \mathbb{E}\{V_1(\eta(k+1)) - V_1(\eta(k))\} \\ & = \mathbb{E}\left\{\eta^T(k+1) P \eta(k+1) - \eta^T(k) P \eta(k)\right\} \\ & = \mathbb{E}\left\{\bar{\eta}^T(k) \Theta_1^T \bar{P} \Theta_1 \bar{\eta}(k) - \eta^T(k) P \eta(k)\right\} \end{aligned} \tag{15}$$

where

$$\bar{\eta}(k) = \left[\eta^T(k) \quad F^T(\eta(k)) \quad G^T(\eta(k)) \quad \left(\sum_{s=1}^{\tau(k)} G(\eta(k-s)) \right)^T \quad v^T(k) \quad \xi^T(k) \quad \vec{\mu}^T(k) \right]^T. \tag{16}$$

For the differences of $V_2(\eta(k))$ and $V_3(\eta(k))$, we get

$$\begin{aligned}
\mathbb{E}\{\Delta V_2(\eta(k))\} &= \mathbb{E}\{V_2(\eta(k+1)) - V_2(\eta(k))\} \\
&= \mathbb{E}\left\{\sum_{j=1}^{\tau(k+1)}\sum_{i=k+1-j}^{k} G^T(\eta(i))QG(\eta(i)) - \sum_{j=1}^{\tau(k)}\sum_{i=k-j}^{k-1} G^T(\eta(i))QG(\eta(i))\right. \\
&\left. + \sum_{j=1}^{\tau(k)}\sum_{i=k+1-j}^{k} G^T(\eta(i))(Q-Q)G(\eta(i))\right\} \\
&= \mathbb{E}\left\{\sum_{j=1}^{\tau(k+1)}\sum_{i=k+1-j}^{k-1} G^T(\eta(i))QG(\eta(i)) + \sum_{j=1}^{\tau(k+1)} G^T(\eta(k))QG(\eta(k))\right. \\
&\left. - \sum_{j=1}^{\tau(k)}\sum_{i=k-j}^{k-1} G^T(\eta(i))QG(\eta(i)) + \sum_{j=1}^{\tau(k)}\sum_{i=k+1-j}^{k} G^T(\eta(i))QG(\eta(i))\right\} \\
&\leq \mathbb{E}\left\{\sum_{j=\tau_m+1}^{\tau_M}\sum_{i=k+1-j}^{k-1} G^T(\eta(i))QG(\eta(i)) + \tau_M G^T(\eta(k))QG(\eta(k))\right. \\
&\left. + \sum_{j=\tau_m}^{\tau_M} G^T(\eta(k))QG(\eta(k)) - \sum_{j=1}^{\tau(k)} G^T(\eta(k-j))QG(\eta(k-j))\right\} \\
&\leq \mathbb{E}\left\{\sum_{j=\tau_m+1}^{\tau_M}\sum_{i=k+1-j}^{k-1} G^T(\eta(i))QG(\eta(i))\right. \\
&\left. +(2\tau_M - \tau_m)G^T(\eta(k))QG(\eta(k)) - \sum_{j=1}^{\tau(k)} G^T(\eta(k-j))QG(\eta(k-j))\right\}
\end{aligned} \tag{17}$$

and

$$\begin{aligned}
\mathbb{E}\{\Delta V_3(\eta(k))\} &= \mathbb{E}\{V_3(\eta(k+1)) - V_3(\eta(k))\} \\
&= \mathbb{E}\left\{\sum_{v=\tau_m+1}^{\tau_M}\sum_{j=1}^{v-1}\sum_{i=k+1-j}^{k} G^T(\eta(i))QG(\eta(i))\right. \\
&\left. - \sum_{v=\tau_m+1}^{\tau_M}\sum_{j=1}^{v-1}\sum_{i=k-j}^{k-1} G^T(\eta(i))QG(\eta(i))\right\} \\
&\leq \mathbb{E}\left\{\frac{(\tau_M-\tau_m)(\tau_m+\tau_M-1)}{2}G^T(\eta(k))QG(\eta(k))\right. \\
&\left. - \sum_{j=\tau_m+1}^{\tau_M}\sum_{i=k+1-j}^{k-1} G^T(\eta(i))QG(\eta(i))\right\}.
\end{aligned} \tag{18}$$

Furthermore, it can be inferred from Lemma 1 that

$$-\sum_{j=1}^{\tau(k)} G^T(\eta(k-j))QG(\eta(k-j)) \leq -\frac{1}{\tau_M}\left(\sum_{j=1}^{\tau(k)} G(\eta(k-j))\right)^T Q\left(\sum_{j=1}^{\tau(k)} G(\eta(k-j))\right). \tag{19}$$

Combining with $\mathbb{E}\{v_i^2(k)\} \leq \varepsilon^2$ and (5), it is observed $v^T(k)v(k) \leq N\varepsilon^2$ and $\xi^T(k)\xi(k) \leq \varepsilon_1^2$. By following from (2) and (3), one has

$$\Lambda_1 = \begin{bmatrix} \eta(k) \\ F(\eta(k)) \end{bmatrix}^T \begin{bmatrix} I \otimes \hat{U}_2 & I \otimes (-\bar{U}_2) \\ * & I \end{bmatrix} \begin{bmatrix} \eta(k) \\ F(\eta(k)) \end{bmatrix} \le 0, \tag{20}$$

$$\Lambda_2 = \begin{bmatrix} \eta(k) \\ G(\eta(k)) \end{bmatrix}^T \begin{bmatrix} -I \otimes (\varphi^T\varphi) & 0 \\ * & I \end{bmatrix} \begin{bmatrix} \eta(k) \\ G(\eta(k)) \end{bmatrix} \le 0. \tag{21}$$

Combining (15)-(19), we have

$$\begin{aligned} \mathbb{E}\{\Delta V(\eta(k))\} \le \mathbb{E}\Bigg\{ & \bar{\eta}^T(k)\Theta_1\bar{P}\Theta_1\bar{\eta}(k) - \eta^T(k)P\eta(k) + (2\tau_M - \tau_m)G^T(\eta(k))QG(\eta(k)) \\ & + \frac{(\tau_M - \tau_m)(\tau_m + \tau_M - 1)}{2}G^T(\eta(k))QG(\eta(k)) \\ & - \frac{1}{\tau_M}\left(\sum_{j=1}^{\tau(k)} G(\eta(k-j))\right)^T Q\left(\sum_{j=1}^{\tau(k)} G(\eta(k-j))\right)\Bigg\}. \end{aligned} \tag{22}$$

Bearing in mind (20) and (21), it stems from (22) that

$$\begin{aligned} \mathbb{E}\{\Delta V(\eta(k))\} \le \mathbb{E}\Bigg\{ & \bar{\eta}^T(k)\Theta_1\bar{P}\Theta_1\bar{\eta}(k) - \eta^T(k)P\eta(k) + (2\tau_M - \tau_m)G^T(\eta(k))QG(\eta(k)) \\ & + \frac{(\tau_M - \tau_m)(\tau_m + \tau_M - 1)}{2}G^T(\eta(k))QG(\eta(k)) \\ & - \frac{1}{\tau_M}\left(\sum_{j=1}^{\tau(k)} G(\eta(k-j))\right)^T Q\left(\sum_{j=1}^{\tau(k)} G(\eta(k-j))\right) \\ & - \lambda_1\left(v^T(k)v(k) - N\varepsilon^2\right) - \lambda_2\left(\xi^T(k)\xi(k) - \varepsilon_1^2\right) - \lambda_3\Lambda_1 \\ & - \lambda_4\Lambda_2 - \lambda_5\left(\mu^T(k)\mu(k) - y^T(k)\Omega y(k)\right)\Bigg\} \\ & \le \mathbb{E}\Big\{\bar{\eta}^T(k)\Theta\bar{\eta}(k) + \gamma^2\Big\}. \end{aligned} \tag{23}$$

Recalling (12) gives

$$\mathbb{E}\{\Delta V(\eta(k))\} \le -\lambda_{min}(-\Theta)\mathbb{E}\Big\{||\eta(k)||^2\Big\} + \gamma^2. \tag{24}$$

In addition, taking (21) into consideration, we have

$$\begin{aligned} V(\eta(k)) \le & \lambda_{max}(P)\mathbb{E}\Big\{||\eta(k)||^2\Big\} + \lambda_{max}(Q)(\tau_M + (\tau_M - \tau_m)(\tau_M - 1)) \\ & \times \lambda_{max}(I \otimes (\varphi^T\varphi)) \times \sum_{i=k-\tau_M}^{k-1} \mathbb{E}\Big\{||\eta(i)||^2\Big\}. \end{aligned} \tag{25}$$

It is readily derived from (24) and (25) that for a real number $b > 1$

$$\begin{aligned} & \mathbb{E}\left\{b^{k+1}V(\eta(k+1))\right\} - \mathbb{E}\left\{b^k V(\eta(k))\right\} \\ & \le \epsilon_1(b)b^k\mathbb{E}\Big\{||\eta(k)||^2\Big\} + b^{k+1}\gamma^2 + \epsilon_2(b) \times \sum_{i=k-\tau_M}^{k-1} b^k\mathbb{E}\Big\{||\eta(i)||^2\Big\} \end{aligned} \tag{26}$$

where

$$\epsilon_1(b) = -b\lambda_{min}(-\Theta) + (b-1)\lambda_{max}(P),$$
$$\epsilon_2(b) = (b-1)\lambda_{max}(Q)(\tau_M + (\tau_M - \tau_m)(\tau_M - 1)) \times \lambda_{max}(I \otimes (\varphi^T\varphi)).$$

For any integer $N_0 \geq \tau_M + 1$, (26), together with Lemma 2, we get

$$\begin{aligned}
&\mathbb{E}\left\{b^{N_0}V(\eta(N_0))\right\} - \mathbb{E}\left\{V(\eta(0))\right\} \\
&\leq \frac{b(b^{N_0}-1)\gamma^2}{b-1} + \frac{\tau_M\epsilon_2(b)(b^{\tau_M}-1)}{b-1}\sup_{-\tau_M\leq i\leq 0}\mathbb{E}\left\{||\eta(i)||^2\right\} \\
&+ \epsilon(b)\sum_{k=0}^{N_0-1} b^k\mathbb{E}\left\{||\eta(i)||^2\right\}
\end{aligned} \tag{27}$$

where $\epsilon(b) = \epsilon_1(b) + \frac{2b\epsilon_2(b)(b^{\tau_M}-1)}{b-1}$.

Noting that $\epsilon(1) = -\lambda_{min}(-\Theta) < 0$ and $\lim_{b\to\infty}\epsilon(b) = +\infty$, there is a scalar $b_0 > 1$ such that $\epsilon(b_0) = 0$. For such a scalar $b_0 > 1$, it is concluded

$$\mathbb{E}\left\{b_0^{N_0}V(\eta(N_0))\right\} - \mathbb{E}\left\{V(\eta(0))\right\} \leq \frac{b_0(b_0^{N_0}-1)\gamma^2}{b_0-1} + \frac{\tau_M\epsilon_2(b_0)(b_0^{\tau_M}-1)}{b_0-1}\sup_{-\tau_M\leq i\leq 0}\mathbb{E}\left\{||\eta(i)||^2\right\}.$$

Since $\sup_{-\tau_M\leq i\leq 0}\mathbb{E}\left\{||\eta(i)||^2\right\} \leq 2N\varepsilon_2^2$, $\mathbb{E}\left\{b_0^{N_0}V(\eta(N_0))\right\} \geq \lambda_{min}(P)b_0^{N_0}\mathbb{E}\left\{||\eta(N_0)||^2\right\}$, and

$$\begin{aligned}
\mathbb{E}\{V(\eta(0))\} \leq \tau_M max\Big\{&\lambda_{max}(P), \lambda_{max}(Q)(\tau_M + (\tau_M - \tau_m)(\tau_M - 1)) \\
&\times \lambda_{max}(I \otimes (\varphi^T\varphi))\Big\} \times \sup_{-\tau_M\leq i\leq 0}\mathbb{E}\left\{||\eta(i)||^2\right\},
\end{aligned}$$

it is observed that

$$\begin{aligned}
\mathbb{E}\left\{||\tilde{z}(N_0)||^2\right\} &\leq \lambda_{max}(\bar{E}^T\bar{E})\mathbb{E}\left\{||\eta(N_0)||^2\right\} \\
&\leq \lambda_{max}(\bar{E}^T\bar{E})\left(b_0^{-N_0}(\varpi(b_0) - \bar{b}_0) + \bar{b}_0\right) \\
&\leq \lambda_{max}(\bar{E}^T\bar{E})max\{\varpi(b_0), \bar{b}_0\}.
\end{aligned} \tag{28}$$

By following from (12), we get $\mathbb{E}\{||\tilde{z}(N_0)||^2\} \leq \varepsilon_3^2$, indicating that the dynamic system (10) is (ε, ε_1, ε_2, ε_3)-secure. Therefore, the proof is considered finished.

For analysis simplification, we denote

$$\Lambda = \begin{bmatrix} \Lambda_{11} & P & 0 & P\mathcal{A}_d & 0 & -\tilde{\vartheta}L_2 & 0 \\ \tilde{\vartheta}L_3 & 0 & 0 & 0 & 0 & -\tilde{\vartheta}L_2 & 0 \\ 0 & 0 & 0 & 0 & \Lambda_{35} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\vartheta}L_4 & 0 & L_5 \end{bmatrix}$$

$$\Lambda_{11} = P\mathcal{A}_1 + L_1, \quad \Lambda_{35} = P\mathcal{B} - (1-\tilde{\vartheta})L_4$$

$$\mathcal{A}_1 = diag\{A + W\otimes\Gamma, A + W\otimes\Gamma\}$$

$$L_1 = \begin{bmatrix} 0 & 0 \\ \tilde{\vartheta}\bar{X}\bar{C} & -\bar{X}\bar{C} \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 \\ \bar{X}S_1 \end{bmatrix}$$

$$L_3 = \begin{bmatrix} 0 & 0 \\ \bar{X}\bar{C} & 0 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 0 \\ \bar{X}\bar{D} \end{bmatrix}, \quad L_5 = \begin{bmatrix} 0 & 0 \\ 0 & \bar{X} \end{bmatrix}.$$

In what follows, a method is proposed for designing the gain matrix of an estimator for the augmented system (10).

Theorem 2: Let positive constants ε, ε_1, ε_2, and ε_3 be given. The system (10) is $(\varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3)$-secure if there are positive definite matrices Q, $P_1 = diag\{P_{11}, P_{12}, \ldots, P_{1N}\}$, $P_2 = diag\{P_{21}, P_{22}, \ldots, P_{2N}\}$, matrix $X = diag\{X_1, X_2, \ldots, X_{l_0}\})$, and positive scalars λ_1, λ_2, λ_3, λ_4, λ_5, κ satisfying:

$$\begin{cases} \Xi = \begin{bmatrix} \Theta_0 & * & * & * \\ \Lambda & -\bar{P} & * & * \\ 0 & 0 & -\kappa I & * \\ 0 & 0 & 0 & -\kappa I \end{bmatrix} < 0 \\ \lambda_{max}(\bar{E}^T\bar{E}) max\{\bar{\varpi}(b_0), \bar{b}_0\} \le \varepsilon_3^2 \end{cases} \tag{29}$$

where $P = diag\{P_1, P_2\}$, $\bar{X} = [X^T \quad 0]^T$, and the solution for the constant $b_0 > 1$ in (29) is obtained as follows:

$$\begin{aligned} &- b_0\lambda_{min}(-\Xi) + (b_0 - 1)\lambda_{max}(P) + 2b_0(b_0^{\tau_M} - 1) \\ &\quad \times \lambda_{max}(Q)(\tau_M + (\tau_M - \tau_m) \times (\tau_M - 1))\lambda_{max}(I \otimes (\varphi^T\varphi)) \\ &= 0 \end{aligned} \tag{30}$$

In addition, the matrices K_i $(i = 1, 2, \ldots, l_0)$ can be designed as

$$K_i = P_{2i}^{-1} X_i. \tag{31}$$

Proof: Recalling (12) and denoting $\bar{\Theta}_1 = \bar{P}\Theta_1$, it follows from the Schur Complement Lemma that

$$\begin{bmatrix} \Theta_0 & * \\ \bar{\Theta}_1 & -\bar{P} \end{bmatrix} < 0 \tag{32}$$

where $\bar{\Theta}_{135} = P\mathcal{B} - (1 - \bar{\vartheta})P\mathcal{D}$ and

$$\bar{\Theta}_1 = \begin{bmatrix} P\mathcal{A} & P & 0 & P\mathcal{A}_d & 0 & -\bar{\vartheta}P\mathcal{S}_1 & 0 \\ \tilde{\vartheta}PC & 0 & 0 & 0 & 0 & -\tilde{\vartheta}P\mathcal{S}_1 & 0 \\ 0 & 0 & 0 & 0 & \bar{\Theta}_{135} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\vartheta}P\mathcal{D} & 0 & P\mathcal{S}_2 \end{bmatrix}.$$

By applying the Schur Complement Lemma, (32) is valid only if the subsequent inequality is satisfied:

$$\begin{bmatrix} \Theta_0 & * & * & * \\ \bar{\Theta}_1 & -\bar{P} & * & * \\ 0 & 0 & -\kappa I & * \\ 0 & 0 & 0 & -\kappa I \end{bmatrix} < 0. \tag{33}$$

It is worth noting that $\bar{X} = P_2\bar{K}$. In other words, (33) is implied by (29). The rest part of the proof follows immediately from Theorem 2.

The model establishment and consensus analysis are finally completed with the help of (29) (an important property of the Laplacian matrix). The gain matrices are designed by resorting to the feasible solutions of (30), which obviously depends on the Laplacian matrix. Both of them show the influence of the network communication topology.

Remark 5: Theorem 2 proposes an easy-to-check approach for designing the PNB- and-ETM-based state estimator, which enables the error system to achieve the desired convergence and security performance even in the presence of random deception attacks. The gain matrix for the estimator is determined by considering feasible solutions to the inequalities (29) and (30). These solutions are heavily influenced by various factors, including network parameters, external disturbances, inherent nonlinearities, the coupling Laplacian matrix, delay bounds, the intensity and frequency of deception attacks, and the event-triggering threshold.

Remark 6: Theorem 2 proposes an effective method to design state estimators for CNs by using the output of partial nodes. It differs significantly from the state estimators proposed in [10,11,13,17]. Compared with the results of PNB state estimation for CNs in [27–29], our result stands out by considering both deception attacks and event-triggering mechanisms simultaneously. This notable feature makes Theorem 2 more practical and feasible for network environments that are constrained by limited resources and susceptible to network attacks.

4. EXAMPLES AND SIMULATIONS

In this section, two examples are presented to demonstrate the validity of our method.

Example 1

Consider a CN with $N = 5$, $l_0 = 3$, and the relevant parameters are given as follows:

$$A_1 = A_2 = \begin{bmatrix} 0.003 & -0.004 & -0.003 \\ 0.002 & 0.004 & -0.001 \\ 0.001 & 0.002 & -0.002 \end{bmatrix}, D_1 = \begin{bmatrix} 0.1 \\ 0.2 \end{bmatrix}, D_2 = \begin{bmatrix} 0.2 \\ 0.1 \end{bmatrix}$$

$$A_3 = A_4 = \begin{bmatrix} 0.001 & -0.002 & -0.001 \\ 0.001 & -0.002 & -0.001 \\ 0.001 & 0.002 & -0.001 \end{bmatrix}, D_3 = \begin{bmatrix} 0.2 \\ 0.2 \end{bmatrix}, B_1 = B_2 = \begin{bmatrix} 0.001 \\ 0.002 \\ 0.002 \end{bmatrix}$$

$$A_5 = \begin{bmatrix} -0.001 & -0.001 & -0.002 \\ 0.001 & 0.002 & -0.002 \\ -0.001 & 0.002 & -0.002 \end{bmatrix}, B_5 = \begin{bmatrix} 0.002 \\ 0.001 \\ 0.001 \end{bmatrix}, B_3 = B_4 = \begin{bmatrix} 0.001 \\ 0.002 \\ 0.001 \end{bmatrix}$$

$$A_{d1} = A_{d2} = \begin{bmatrix} 0.001 & 0.001 & 0.004 \\ 0.001 & -0.001 & 0.001 \\ 0.002 & 0.004 & 0.001 \end{bmatrix}, A_{d3} = A_{d4} = \begin{bmatrix} 0.002 & 0.002 & 0.001 \\ 0.002 & -0.003 & 0.001 \\ 0.001 & 0.004 & 0.003 \end{bmatrix}$$

$$A_{d5} = \begin{bmatrix} 0.001 & 0.002 & 0.003 \\ 0.001 & -0.001 & 0.002 \\ 0.001 & 0.002 & 0.003 \end{bmatrix}, E_3 = \begin{bmatrix} 0.1 & 0.2 & 0.1 \end{bmatrix}, E_5 = \begin{bmatrix} 0.1 & 0.2 & 0.1 \end{bmatrix}$$

$$C_1 = C_2 = C_3 = \begin{bmatrix} 2 & 0 & 0 \\ 3 & 0 & 2.4 \end{bmatrix}, \Gamma = 0.55I,\ \bar{\vartheta} = 0.4,\ \varepsilon = 0.4,\ \varepsilon_1 = 0.2,\ \varepsilon_2 = 0.3,\ \varepsilon_3 = 11$$

$$\tau_m = 2, \tau_M = 5,\ \delta_1 = \delta_2 = \delta_3 = 3,\ E_1 = \begin{bmatrix} 0.1 & 0.2 & 0.2 \end{bmatrix}, E_4 = \begin{bmatrix} -0.2 & -0.2 & 0.2 \end{bmatrix}$$

$$E_2 = \begin{bmatrix} 0.2 & 0.1 & 0.3 \end{bmatrix}, W = \begin{bmatrix} -0.006 & 0.001 & 0.002 & 0.001 & 0.002 \\ 0.001 & -0.007 & 0.002 & 0.002 & 0.002 \\ 0.002 & 0.002 & -0.005 & 0 & 0.001 \\ 0.001 & 0.002 & 0 & -0.005 & 0.002 \\ 0.002 & 0.002 & 0.001 & 0.002 & -0.007 \end{bmatrix}.$$

Table 1. Triggering frequencies and estimation errors with different threshold parameters

Values of δ_i	Triggering of Node1	Triggering of Node2	Triggering of Node3	Total Error
$\delta_1 = \delta_2 = \delta_3 = 0.8$	83%	83%	83%	0.0122
$\delta_1 = \delta_2 = \delta_3 = 3$	20%	13.3%	23.3%	0.0416
$\delta_1 = \delta_2 = \delta_3 = 6$	13.3%	10%	10%	0.0609

Here, we choose $f(\cdot)$ and $g(\cdot)$ to be

$$f(x_i(k)) = \begin{bmatrix} f_1(x_i(k)) \\ sin(-0.1x_{i2}(k)) \\ sin(-0.2x_{i3}(k)) \end{bmatrix}$$
$$f_1(x_i(k)) = -0.1x_{i1}(k)+0.1(|x_{i1}(k)+2| - |x_{i1}(k)-2|) + 0.1x_{i2}(k)$$

and

$$g(x_i(k)) = \begin{bmatrix} -0.2cos(x_{i1}(k)) \\ 0.2cos(x_{i2}(k)) \\ 0.1cos(x_{i3}(k)) \end{bmatrix}.$$

It is not difficult to verify that conditions (2) and (3) can be met with

$$U_1 = \begin{bmatrix} 0.1 & 0.1 & 0 \\ 0 & -0.2 & 0 \\ 0 & 0 & -0.2 \end{bmatrix}, U_2 = \begin{bmatrix} -0.1 & 0.1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \varphi = \begin{bmatrix} 0.1 & 0 & 0 \\ 0 & 0.2 & 0 \\ 0 & 0 & 0.1 \end{bmatrix}.$$

According to (29) and using the Matlab software (with the YALMIP toolbox), we obtain the gain matrices for the estimator as follows

$$K_1 = \begin{bmatrix} 0.0000 & -0.0001 \\ 0.0006 & 0.0274 \\ 0.0000 & -0.0000 \end{bmatrix}, K_2 = \begin{bmatrix} 0.0000 & -0.0001 \\ 0.0006 & 0.0273 \\ 0.0000 & -0.0000 \end{bmatrix}, K_3 = \begin{bmatrix} 0.0000 & -0.0000 \\ 0.0006 & 0.0274 \\ 0.0000 & 0.0000 \end{bmatrix}.$$

Let initial values be $\phi_i(r) = [0.1 \quad 0.1 \quad 0.1]^T$ $(\forall r \in [-5, 0], i = 1, \ldots, 5)$. The simulation results are illustrated in Figures 1-4. To be more specific, the values of $\vartheta(k)$ are recorded in Figure 1, in which $\vartheta(k) = 1$ stands for the occurrence of the deception attacks while $\vartheta(k) = 0$ shows the deception attacks do not occur. Figure 2 shows the triggering time sequences on the first three nodes with the thresholds δ_i $(i = 1, 2, 3)$ being taken as 3. Figure 3 displays the evolution of the estimation error outputs $\tilde{z}_i(k)$. For the estimation error, Figure 4 shows the evolution of the mean square $\mathbb{E}\{||\tilde{z}(k)||^2\}$ and the root mean square $\sqrt{\sum_{i=1}^{5} e_i^2(k)}$ with the upper bound ε_3^2, which implies the convergency and security performance are met.

In order to explain the relationship between the number of event triggerings and the estimation accuracy, we provide the following Table 1 to record the triggering frequency and the estimation error. It is readily observed that the larger number of triggerings usually indicates better estimation accuracy. Generally speaking, the threshold parameters δ_i can be delicately tuned to achieve a trade-off between the desired estimation performance and the energy-saving target.

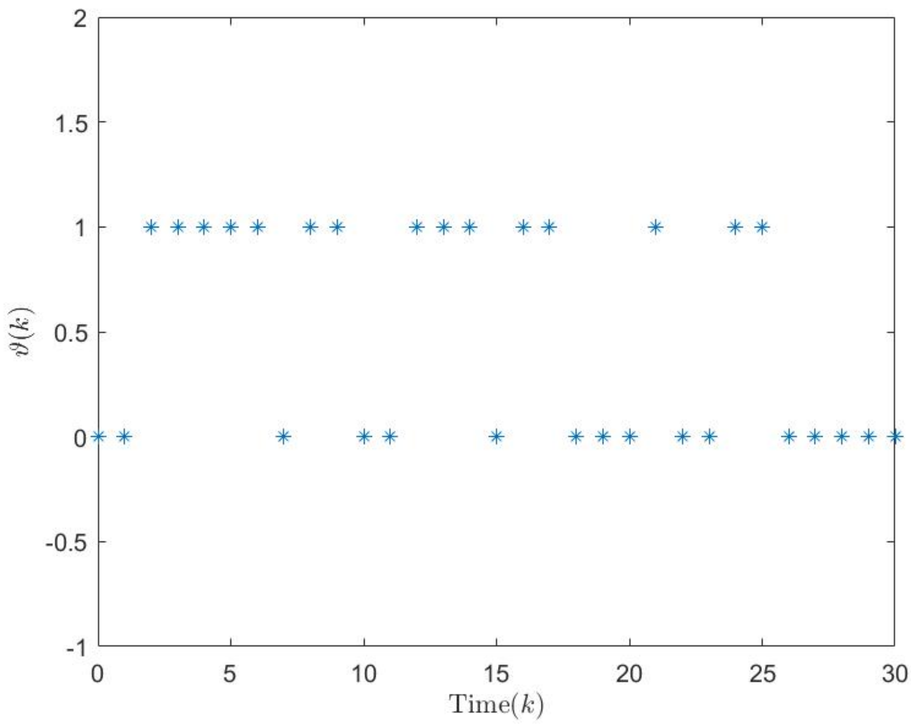

Figure 1. Occurrence of the deception attacks.

Example 2

Consider a CN with 5-node discrete-time Chua's circuits borrowed from [29] and let $l_0 = 3$. The relevant parameters are given as follows:

$$A_1 = A_2 = \begin{bmatrix} 0.3 & 0.2 & 0 \\ 0.1 & 0.2 & 0.2 \\ 0 & -3.4 & 0.4 \end{bmatrix}, A_3 = A_4 = A_5 = \begin{bmatrix} 0.4 & 0.2 & 0 \\ 0.25 & 0.45 & 0.2 \\ 0 & -0.2 & 0.5 \end{bmatrix}$$

$$W = \begin{bmatrix} -0.7 & 0.15 & 0.2 & 0.15 & 0.2 \\ 0.15 & -0.6 & 0.15 & 0.2 & 0.1 \\ 0.2 & 0.15 & -0.5 & 0 & 0.15 \\ 0.15 & 0.2 & 0 & -0.5 & 0.15 \\ 0.2 & 0.1 & 0.15 & 0.15 & -0.6 \end{bmatrix}, B_i = A_{di} = 0 (i = 1, 2, \ldots, 5)$$

$$f(x_i(k)) = \begin{bmatrix} -0.2x_{i1} + 0.3(|x_{i1} + 2| - |x_{i1} - 2|) \\ 0 \\ 0 \end{bmatrix}, g(x_i(k)) = \begin{bmatrix} 0 \\ 0 \\ 0.5sin(0.2x_{i1}(k)) \end{bmatrix}$$

$$C_1 = C_2 = C_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \Gamma = I, \tau_m = 2, \tau_M = 3, D_i = 0 (i = 1, 2, 3)$$

and other parameters are set as the same as in Example 1.

Without any difficulties, we derive that conditions (2) and (3) are satisfied with

$$U_1 = \begin{bmatrix} -0.8 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, U_2 = \begin{bmatrix} -0.2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \varphi = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0.1 \end{bmatrix}.$$

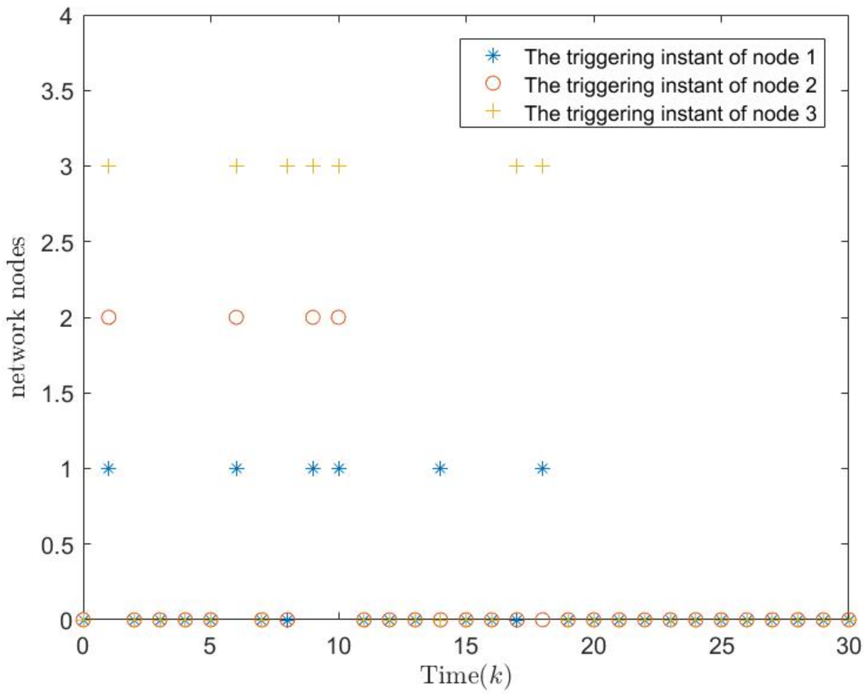

Figure 2. Triggering instants for the first three nodes.

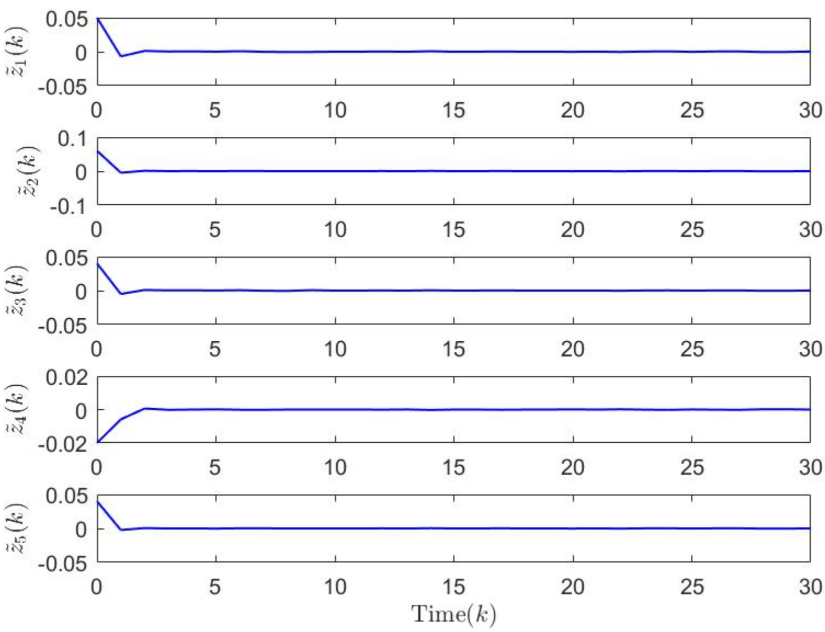

Figure 3. Output estimation errors of five nodes.

By using the Matlab toolbox, the estimator gain matrices are derived as follows

$$K_1 = \begin{bmatrix} -0.0003 & 0.0005 \\ -0.0094 & 0.0008 \\ 0.0330 & 0.0027 \end{bmatrix}, K_2 = \begin{bmatrix} 0.0006 & -0.0004 \\ -0.0024 & 0.0013 \\ 0.0035 & 0.0024 \end{bmatrix}, K_3 = \begin{bmatrix} 0.0006 & -0.0001 \\ -0.0008 & 0.0019 \\ -0.0076 & 0.0050 \end{bmatrix}.$$

For the aim of simulation, we choose initial states to be $\phi_i(r) = [0.1 \quad 0.1 \quad 0.1]^T$ for $r \in [-3, 0]$, $i =$

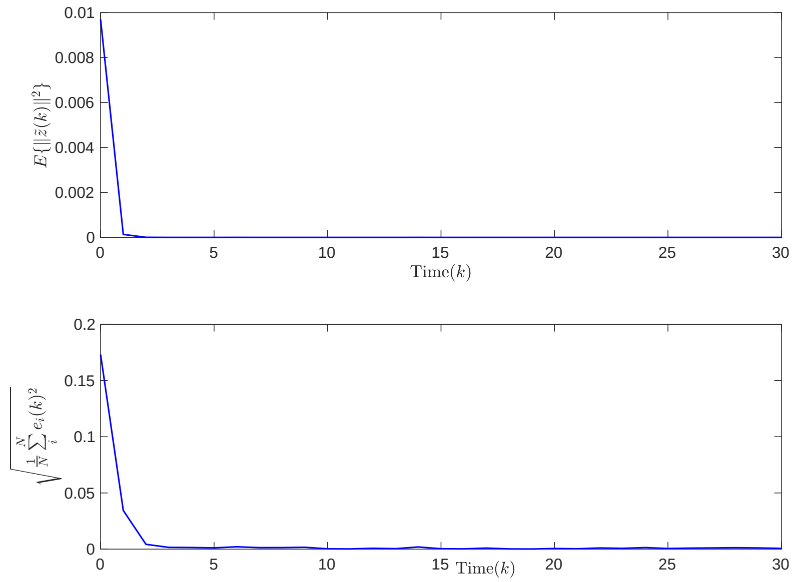

Figure 4. The norm square and root mean square of the estimated error.

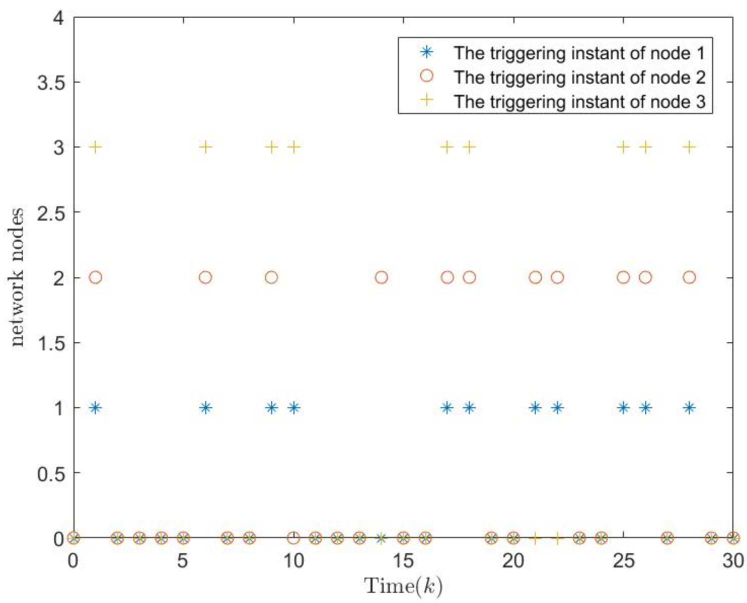

Figure 5. Triggering instants for the first three nodes.

1, ..., 5. Without loss of generality, let the occurrence of deception attacks be the same as in Example 1. In Figure 5, the instants for event triggering are illustrated by taking the thresholds $\delta_i = 3$ ($i = 1, 2, 3$). It is readily seen that the updating frequency of sensors is reduced dramatically. The evolution of the estimation error output $\tilde{z}_i(k)$ is given in Figure 6, from which we see estimation errors tend to zero with small oscillations. Figure 7 shows that the mean square $\mathbb{E}\{||\tilde{z}(k)||^2\}$ and the root mean square $\sqrt{\sum_{i=1}^{5} e_i^2(k)}$ approach zero ultimately; that is, the performance of secure estimation is realized.

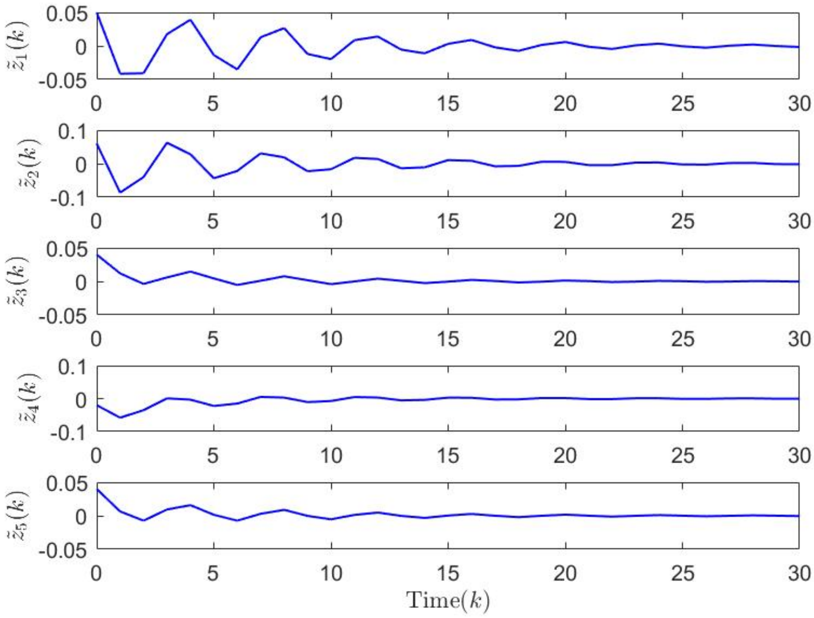

Figure 6. Output estimation errors of five nodes.

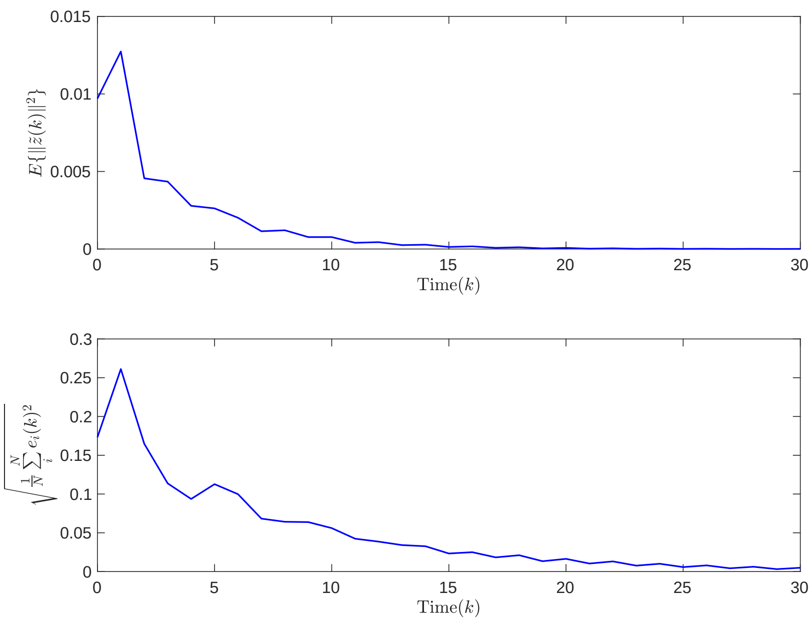

Figure 7. The norm square and the root mean square of the estimated error.

5. CONCLUSIONS

The event-triggered PNB state estimation problem has been studied in this paper for a class of discrete-time CNs under deception attacks. A novel state estimator has been designed based on the measurement outputs from the fraction of nodes. A general event-triggering scheme has also been taken into account in the design of the estimator such that the communication resources are saved dramatically. Sufficient conditions have been established (in the form of matrix inequalities) to ensure the existence of the desired state estimator. Finally, a numerical example and simulations are presented to further demonstrate the effectiveness of the proposed method. Several future research topics include the state estimation of complex systems subjected to complexity attacks or communication protocols.

DECLARATIONS

Authors' contributions

Made substantial contributions to the conception and design of the study and performed data analysis and interpretation: Zhou L, Li B

Performed data acquisition and provided administrative, technical, and simulation: Zhou L

Availability of data and materials

Not applicable.

Financial support and sponsorship

This work was supported in part by the National Natural Science Foundation of China under Grants 62273066, in part by the Science and Technology Research Program of Chongqing Municipal Education Commission under Grants KJZD-M202100701, in part by the Group Building Scientific Innovation Project for universities in Chongqing under Grant CXQT21021, and in part by the Joint Training Base Construction Project for Graduate Students in Chongqing under Grant JDLHPYJD2021016.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

REFERENCES

1. Zhang HT, Yu T, Sang JP, Zou XW. Dynamic fluctuation model of complex networks with weight scaling behavior and its application to airport networks. *Physica A: Statist Mech Appl* 2014;393:590–9. DOI
2. Eagle N, Pentland A. Reality mining: sensing complex social systems. *Pers Ubiquit Comput* 2005;10:255–68. DOI
3. Pastor-Satorras R, Smith E, Solé R. Evolving protein interaction networks through gene duplication. *J Theor Biol* 2003;222:199–210. DOI
4. Strogatz SH. Exploring complex networks. *Nature* 2001;410:268–76. DOI
5. Ding YL, Fu MH, Luo P, Wu FX. Network learning for biomarker discovery. *IJNDI* 2023;2:51–65. DOI
6. Pinto ER, Nepomuceno EG, Campanharo AS. Individual-based modelling of animal brucellosis spread with the use of complex networks. *IJNDI* 2022;1:120–9. DOI
7. Aldana M. Boolean dynamics of networks with scale-free topology. *Physica D* 2003;185:66. DOI
8. Wang, X, Sun Y, Ding D. Adaptive dynamic programming for networked control systems under communication constraints: a survey of trends and techniques. *IJNDI* 2022;1:85–98. DOI
9. Huang C, Ho D, Lu JQ, Kurths J. Pinning synchronization in T-S fuzzy complex networks with partial and discrete-time couplings. *IEEE Trans Fuzzy Syst* 2015;23:1274–85. DOI
10. Dong HL, Hou N, Wang ZD, Ren WJ. Variance-constrained state estimation for complex networks with randomly varying topologies. *IEEE Trans Neural Netw Learn Syst* 2018;29:2757–68. DOI

11. Wang LC, Wang ZD, Huang TW, Wei GL. An event-triggered approach to state estimation for a class of complex networks with mixed time delays and nonlinearities. *IEEE Trans Cybern* 2016;46:2497–2508. DOI
12. Yu WW, Chen GR, Lü JH, Kurths J. Synchronization via pinning control on general complex networks. *SIAM J Control Optim* 2013;51:1395–416. DOI
13. Burbano-L. DA, Russo G, Bernardo M. Pinning controllability of complex network systems with noise. *IEEE Trans Control Netw Syst* 2019;6:874–83. DOI
14. Wang J. Synchronization of delayed complex dynamical network with hybrid-coupling via aperiodically intermittent pinning control. *J Frankl I* 2017;354:1855. DOI
15. Zhang XM, Han QL. Event-triggered H_∞ control for a class of nonlinear networked control systems using novel integral inequalities. *Int J Robust Nonlinear Control* 2017;27:679–700. DOI
16. Liu YF, Shen B, Zhang P. Synchronization and state estimation for discrete-time coupled delayed complex-valued neural networks with random system parameters. *Neural Netw* 2022;150:181–93. DOI
17. Wan XB, Wang ZD, Han QL, Wu M. Finite-time H_∞ state estimation for discrete time-delayed genetic regulatory networks under stochastic communication protocols. *IEEE Trans Circuits Syst I* 2018;65:3481–91. DOI
18. Ramasamy S, Nagamani G, Zhu QX. Robust dissipativity and passivity analysis for discrete-time stochastic T–S fuzzy Cohen–Grossberg Markovian jump neural networks with mixed time delays. *Nonlinear Dyn* 2016;85:2777–99. DOI
19. Neyir O. Stability analysis of Cohen–Grossberg neural networks of neutral-type: Multiple delays case. *Neural Netw* 2019;113:20–27. DOI
20. Ma NN, Liu ZB, Chen L. Robust and non-fragile finite time H_∞ synchronization control for complex networks with uncertain inner coupling. *Comp Appl Math* 2018;37:5395–409. DOI
21. Liu D, Liu Y, Alsaadi FE. Recursive state estimation based on the outputs of partial nodes for discrete-time stochastic complex networks with switched topology. *J Franklin I* 2018;355:4707. DOI
22. Hu J, Liu GP, Zhang HX, Liu HJ. On state estimation for nonlinear dynamical networks with random sensor delays and coupling strength under event-based communication mechanism. *Inf Sci* 2020;511:283. DOI
23. Li W, Jia YM, Du JP. Variance-constrained state estimation for nonlinearly coupled complex networks. *IEEE Trans Cybern* 2018;48:818–24. DOI
24. Wang MY, Wang HY, Zheng HR. A mini review of node centrality metrics in biological networks. *IJNDI* 2022;1:99–110. DOI
25. Liu HJ, Ge Y, Hou N, Li JH, Dong HL. Finite-horizon resilient state estimation for complex networks with integral measurements from partial nodes. *Sci China Inf Sci* 2022;65. DOI
26. Yu LY, Liu YR, Cui Y, Alotaibi ND, Alsaadi FE. Intermittent dynamic event-triggered state estimation for delayed complex networks based on partial nodes. *Neurocomputing* 2021;459:59–69. DOI
27. Hou N, Dong HL, Wang ZD, Liu HJ. A partial-node-based approach to state estimation for complex networks with sensor saturations under random access protocol. *IEEE Trans Neural Netw Learn Syst* 2021;11:5167–78. DOI
28. Zou L, Wang ZD, Hu J, Dong HL. Partial-node-based state estimation for delayed complex networks under tntermittent measurement outliers: a multiple-order-holder approach. *IEEE Trans Neural Netw Learn Syst* 2022;1–15. DOI
29. Liu YR, Wang ZD, Ma LF, Alsaadi FE. A partial-nodes-based information fusion approach to state estimation for discrete-time delayed stochastic complex networks. *Inform Fusion* 2019;48:240–8. DOI
30. Zhang XM, Han QL. State estimation for static neural networks with time-varying delays based on an improved reciprocally convex inequality. *IEEE Trans Neural Netw Learn Syst* 2018;29:1376–81. DOI
31. Dolk VS, Tesi P, Persis CD, Heemels W. Event-triggered control systems under denial-of-service attacks. *IEEE Trans Control Netw Syst* 2017;4:93–105. DOI
32. Chatterjee K, Singh VK, Prasun P, Kamal S, Ghosh S, Dinh TN. Fixed-time event-triggered control under denial-of-service attacks. *Eur J Control* 2022;32:1209–28. DOI
33. Xiao HC, Wei GL, Ding DR, Dong HL. Adaptive event-triggered state estimation for large-scale systems subject to deception attacks. *Sci China Inf Sci* 2022;65. DOI
34. Hou N, Wang ZD, Ho D, Dong HL. Robust partial-nodes-based state estimation for complex networks under deception attacks. *IEEE Trans Cybern* 2020;50:2793–802. DOI
35. Geng S, Zhu C, Jin Y, Wang L, Tan H. Gaze control system for tracking Quasi-1D high-speed moving object in complex background. *Syst Sci Control Eng* 2022;10:367–76. DOI
36. Wang D, Wang ZD, Shen B, Alsaadi FE. Security-guaranteed filtering for discrete-time stochastic delayed systems with randomly occurring sensor saturations and deception attacks. *Int J Robust Nonlinear Control* 2017;27:1194–208. DOI
37. Zhu MH, Martinez S. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Trans Automat Contr* 2014;59:804–8. DOI
38. Tao H, Tan H, Chen Q, Liu H, Hu J. H_∞ state estimation for memristive neural networks with randomly occurring DoS attacks. *Syst Sci Control Eng* 2022;10:154–65. DOI
39. Deng YH, Mo ZK, Lu HQ. Robust H_∞ state estimation for a class of complex networks with dynamic event-triggered scheme against hybrid attacks. *Chinese Phys B* 2022;31. DOI
40. Sun J, Shen B, Liu YR, Alsaadi FE. Dynamic event-triggered state estimation for time-delayed spatial-temporal networks under encoding-decoding scheme. *Neurocomputing* 2022;500:868–76. DOI
41. Li N, Li Q, Suo JH. Dynamic event-triggered H_∞ state estimation for delayed complex networks with randomly occurring nonlinearities.

Neurocomputing 2021;421:97–104. DOI

42. Han, ZC, Zhang SB, Jin ZW, Hu YY. Secure state estimation for event-triggered cyber-physical systems against deception attacks. *J Franklin I* 2022;359:11155–85. DOI
43. Lin N, Chen DY, Hu J, Jia CQ. Partial-nodes-based state estimation for stochastic coupled complex networks with random sensor delay: an event-triggered communication method. *Circuits Syst Signal Process* 2022;29:3726–37. DOI
44. Liu Jl, Cao J, Wu Z, Qi Q. State estimation for complex systems with randomly occurring nonlinearities and randomly missing measurements. *Int J Syst Sci* 2014;45:1364–74. DOI
45. Liu JL, Liu QH, Cao J, Zhang YY. Adaptive event-triggered H_∞ filtering for T–S fuzzy system with time delay. *Neurocomputing* 2016;189:86–94. DOI
46. Guan ZH, Chen CY, Feng G, Li T. Optimal tracking performance limitation of networked control systems with limited bandwidth and additive colored white Gaussian noise. *IEEE Trans Circuits Syst I* 2013;60:189–198. DOI
47. Yue D, Tian E, Zhang YJ. A piecewise analysis method to stability analysis of linear continuous/discrete systems with time-varying delay. *Int J Robust Nonlinear Control* 2009;19:1493–518. DOI