AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 7(2): 2858–2877.
DOI: 10.3934/math.2022158
Received: 17 September 2021
Accepted: 09 November 2021
Published: 22 November 2021

Research article

Adaptive event-triggered state estimation for complex networks with nonlinearities against hybrid attacks

Yahan Deng, Zhenhai Meng* and Hongqian Lu

School of Information Engineering, Guangxi City Vocational University, Chongzuo 532100, China

* **Correspondence:** Email: gxccjj@163.com; Tel: +07717515030.

Abstract: This paper investigates the event-triggered state estimation problem for a class of complex networks (CNs) suffered by hybrid cyber-attacks. It is assumed that a wireless network exists between sensors and remote estimators, and that data packets may be modified or blocked by malicious attackers. Adaptive event-triggered scheme (AETS) is introduced to alleviate the network congestion problem. With the help of two sets of Bernoulli distribution variables (BDVs) and an arbitrary function related to the system state, a mathematical model of the hybrid cyber-attacks is developed to portray randomly occurring denial-of-service (DoS) attacks and deception attacks. CNs, AETS, hybrid cyber-attacks, and state estimators are then incorporated into a unified architecture. The system state is cascaded with state errors as an augmented system. Furthermore, based on Lyapunov stability theory and linear matrix inequalities (LMIs), sufficient conditions to ensure the asymptotic stability of the augmented system are derived, and the corresponding state estimator is designed. Finally, the effectiveness of the theoretical method is demonstrated by numerical examples and simulations.

Keywords: complex networks; adaptive event-triggered scheme; state estimation; deception attacks; denial-of-service attacks
Mathematics Subject Classification: 93C57, 93C65

1. Introduction

In recent decades, the development of information technology has brought great portability to people's production and life [1]. CNs can be used to portray smart grids, intelligent transportation, social networks and neural systems, etc., and have been given significant research significance and wide application context by academia and industry [2]. It is well known that nodes and connection relationships are two key factors that constitute CNs [3]. For example, in a power system network, power plants are connected to each other by transmission lines, where power plants can be abstractly considered as nodes, and similarly, transmission lines between power plants can be considered as

connection relations [4]. For a multi-robot system, each mobile robot is considered as a node in the network, and the mutual sensing and intercommunication between robots are seen as the connection relationship. When the number of controlled objects is large, the cooperation and formation maintenance for the multi-robot system can be studied with the help of the theory of CNs. Similarly, the above ideas are also applicable to the study of multi-UAS. It can be seen that the connection relations, nodes, and the interactions between connection relations and nodes constitute CNs [5]. From the perspective of control discipline, some works such as state estimation, synchronization and control, and topology identification of CNs are still widely studied [6–8]. In addition, many practical problems are inevitable in information transmission, such as channel redundancy, cyber-attacks, time delay, packet loss, and noise [9, 10]. The authors in [7] studied the partial-nodes-based state estimation problem on estimating the entire network state using partial outputs of the available nodes. In this paper, the impact of cyber-attacks and channel redundancy on the state estimation for CNs is discussed.

In practical engineering, the network bandwidth available to a system is usually limited [11, 12]. Due to the limitation of network resources, channel redundancy, data congestion, network-induced delay, and packet loss inevitably occur when the components within the system perform network access and information transmission [13, 14]. To mitigate the impact of these problems on system performance, various data transmission mechanisms have been proposed, such as event-triggered schemes (ETSs), communication protocol scheduling, and codec strategies. Currently, ETS is a common data transmission scheduling strategy in networked systems [15, 16]. The core idea of the scheme is to determine in real time whether the current system state satisfies the triggering conditions to control the task execution on demand and meet the system performance [17]. On this basis, data transmission strategies such as distributed ETS, AETS, self-triggered scheme, and dynamic ETS have been proposed one after another [18–21]. By introducing the AETS, a fuzzy dynamic output feedback controller is designed for the nonlinear system with actuator failure and packet loss [20]. In [21], the authors propose a co-design method for filter and distributed AETS for nonlinear interconnected systems.

ETSs bring great convenience to networked systems, but open networks are vulnerable to malicious attackers, which poses a potential security risk to networked systems [22, 23]. In networked systems, network attacks appear in various ways and affect or even destroy system performance, such as DoS attacks and deception attacks [24]. DoS attacks: attackers can block the transmission of information in the communication network between sensors and controllers (estimators), resulting in no available data [25]. Deception attack: attackers can tamper with the available data received by the controller (estimator) from the sensor, thus corrupting the integrity of the data [26]. In recent years, the security of networked systems has attracted widespread attention from the community, for example, on May 11, 2021, Belgium's public sector Internet service provider Belnet was subjected to a massive distributed DoS attack, which took all internal systems of the Belgian government and public-facing websites offline and forced many government websites and services in Belgium offline; on August 1, 2021, Italy The local vaccination appointment system was forced to shut down due to the cyber-attacks. In [10], the authors investigated the state estimation problem for a class of uncertain complex networks with partial node failures resistant to deception attacks. A co-design approach for dynamic ETS and observer-based PID controller against deception attacks has been presented in [27]. In [28], the authors studied the problem of state estimation for cyberphysical

systems constrained by communication resources, DoS attacks, and sensor saturation. The authors in [29] presented event-triggered control countermeasures for the multiple cyber-attacks that can occur in cyberphysical systems. Since large-scale CNs have a large number of nodes with intricate connections, their states are usually unmeasurable and only partial information about the network nodes can be obtained through the output of the communication channel [30]. Due to the limitation of network bandwidth and the threat of cyber-attacks, only part of the node information is generally measurable [31]. In order to solve the node state agnosticism, the design of state estimator for CNs is necessary. In this paper, we use two sets of Bernoulli distribution variables and arbitrary functions related to the system state to characterize randomly occurring DoS attacks and deception attacks.

Inspired by the above mentioned work, it can be seen that although event-triggered state estimation for CNs has been extensively studied, relevant research on CNs with multiple attack scenarios is very limited. Second, we also discuss how to efficiently conserve network resources under the condition of limited communication channel capacity. The above two points are the two motivations that motivate the completion of this paper.

Based on the above discussion, we focus on the design of event-triggered state estimators for CNs with malicious attacks. In addition, an AETS is introduced to avoid sensors from sending unnecessary packets to the remote estimator for the purpose of saving network bandwidth. Then, based on the derived sufficient conditions for system stability, a feasible approach for co-design is proposed. Finally, a numerical example verifies the effectiveness of the proposed method. The main contributions of this paper are as follows.

- In order to reflect the real network environment, multiple scenarios of possible malicious attacks in the transmission channel are considered. By introducing Bernoulli distribution variables and an arbitrary function based on the system state, a mathematical model of the deception attacks is developed. Then the action sequence of the DoS attacks is portrayed by introducing another set of Bernoulli variables. The so-called hybrid network attack is modeled.

- We incorporate the plant to be studied, the state estimator, the network resource scheduling policy, and the aforementioned attack model into a unified architecture and describe them through an augmented system.

- We derive sufficient conditions to ensure the asymptotic stability of the above system (Theorem I). Then we give a co-design method for computing the estimation gain of the estimator and the weight matrix of the AETS (Theorem II).

Notations: $\mathbb{R}^{n\times m}$ means $n \times m$ real matrix; $\mathbb{R}^n$ denotes n-dimensional Euclidean space; $A > 0 (A \geq 0)$ implies positive definite (positive semi-definite) symmetric matrix; $\mathbb{E}\{A\}$ represents mathematical expectation of random variable A; $col_N\{X_i\}$ and $diag_N\{Y_i\}$ stand for the block-column matrix $col\{X_1, X_2, \ldots, X_N\}$ and the block-diagonal matrix $col\{Y_1, Y_2, \ldots, Y_N\}$, respectively; $\otimes$ denotes Kronecker product.

2. Preliminaries

Consider the following class of CNs:

$$\begin{cases} \dot{x}_i(t) = D_i x_i(t) + g(x_i(t)) + \sum_{j=1}^{N} a_{ij}\Gamma, x_j(t) + E_i w_i(t), \\ y_i(t) = C_i x_i(t), \\ z_i(t) = M_i x_i(t), \\ x_i(t) = \phi_i(\theta), \theta \in (-\infty, 0], i = 1, 2, \ldots, N, \end{cases} \tag{2.1}$$

where $x_i(t)$, $y_i(t)$, and $z_i(t)$ denote, respectively, the state vector, the measurement output, and the output of the i-th node. $w_i(t) \in \mathcal{L}_2[0, \infty)$ denotes the disturbance noise. ϕ is the initial conditions. $g(\cdot)$ is the the nonlinear vector-valued function. $\Gamma = diag\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ is an inner-coupling matrix. $A = (a_{ij})_{N\times N}$ is thecoupled configuration matrix with $a_{ij} > 0 (i \neq j)$ but not all zero. As usual, the diagonal element is described by $a_{ii} = -\sum_{j=1, j\neq i}^{N} a_{ij}$. C_i, D_i, E_i, and M_i are the known matrices.

In a networked system, the instant information in the communication network is usually transmitted in an equal-period transmission scheme, which can cause unnecessary waste of limited network bandwidth. The event-based transmission strategy allows the communication channel not to be occupied all the time, thus reducing the network burden and achieving the goal of saving network resources. However, an open network environment also exposes the system to potential security risks, and for this reason, the impact of cyber attacks on the system is further discussed. The main work of this paper is to discuss a co-design approach of state estimators and AETS for a class of complex networks suffering from hybrid cyber attacks. Then, we incorporate the above-mentioned complex network model with AETS, hybrid cyber attack model and state estimator into a unified framework as shown in Figure 1. In the rest of this section, AETS, hybrid cyber attack modeling, and system modeling are discussed respectively. The details are as follows:

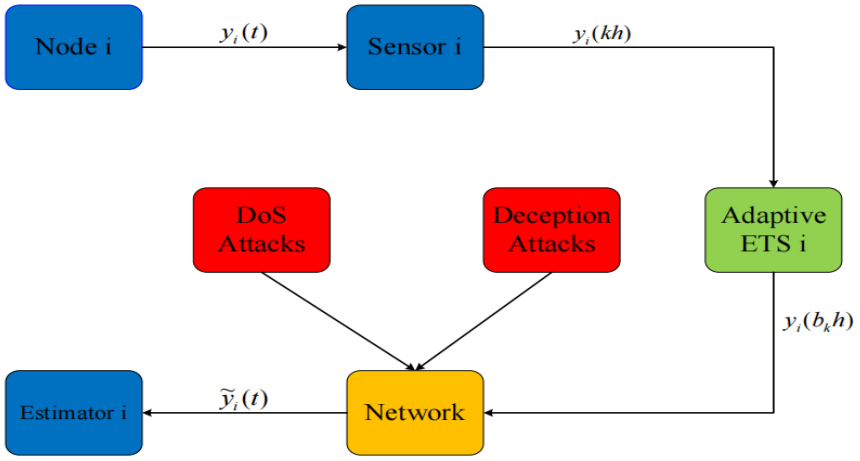

Figure 1. The systematic structure.

2.1. Adaptive event-triggered scheme

With the booming development of network technology, the ETS has been very effective in scheduling network resources. Under the ETS, the successful transmission of sampled data needs to

satisfy a triggering condition:

$$(y_i(b_kh) - y_i(b_kh + lh))^T \Omega_i (y_i(b_kh) - y_i(b_kh + lh)) - \varrho y_i^T(b_kh)\Omega_i y_i(b_kh) > 0. \tag{2.2}$$

Based on the traditional ETS, a new ETS with variable threshold is proposed to save more network resources. Under the AETS, the threshold in the triggering condition can be described as:

$$\dot{\varrho}(t) = \frac{1}{\varrho(t)}(\frac{1}{\varrho(t)} - \varpi)e_{ki}^T(t)\Omega_i e_{ki}(t), \tag{2.3}$$

where $0 < \varrho(0) \leq 1$, $\varpi > 0$, and $e_{ki}(t) = y_i(b_kh) - y_i(b_kh + lh)$.

Define that $\tau_k = t_k - b_kh$ and $\ell_k = b_{k+1} - b_k - 1$, where τ_k is network-induced delay, and $\tau_k \in [\tau_m, \tau_M]$. According to $t_k < t_{k+1}$, the interval $[t_k, t_{k+1})$ can be divided as $\bigcup_{l=0}^{\ell_k} \Im_l$, where

$$\Im_n = \begin{cases} [t_k + lh, t_k + (l+1)h), & l = 0, 1, \ldots, \ell_k - 1, \\ [t_k + lh, t_{k+1}), & l = \ell_k. \end{cases} \tag{2.4}$$

By setting $d(t) = t - (b_kh + lh)$, we have

$$d(t) = \begin{cases} t - b_kh, & t \in \Im_0, \\ t - b_kh - h, & t \in \Im_1, \\ \vdots & \vdots, \\ t - b_kh - \ell_kh, & t \in \Im_{\ell_k}, \end{cases} \tag{2.5}$$

$$e_{ki}(t) = \begin{cases} 0, & t \in \Im_0, \\ y_i(b_kh) - y_i(b_kh + h), & t \in \Im_1, \\ \vdots & \vdots, \\ y_i(b_kh) - y_i(b_kh + \ell_kh), & t \in \Im_{\ell_k}. \end{cases} \tag{2.6}$$

From (2.1)–(2.6), the actual measurement output under AETM can be expressed as:

$$\bar{y}_i(t) = y_i(t - d(t)) + e_{ki}(t), \tag{2.7}$$

where $0 < \tau_m \leq d(t) \leq h + \tau_M = d_M$.

Remark 1. *In the ith sensor-to-estimator channel, the ith trigger determines whether the current sampled data of the ith sensor corresponding to the node needs to be sent, i.e., whether the current sampled data in sensor i satisfies the ith adaptive event-triggered condition (2.2). The above scheme is introduced to ensure that the information transmission efficiency can be effectively improved under the limitation of network bandwidth.*

2.2. Hybrid cyber attack modeling

The AETS greatly facilitate the transfer of data between components in a networked system. However, the actual network network environment is complex and volatile, and there may be potential security threats. From the defender's standpoint, the attack type and attack moment cannot be

determined. For this reason, both deception attacks and DoS attacks are considered, both of which are the most common attack behaviors in network. Also, two sets of Bernoulli distributed variables are introduced to characterize the moment of occurrence of the two attack behaviors. Denote that $\mathscr{F} = f(y_i(t-\eta(t)))$. The hybrid attack model can be expressed as follows:

$$\tilde{y}_i(t) = (1-\beta_i(t))[(1-\alpha_i(t))\bar{y}_i(t) + \alpha_i(t)\mathscr{F}], \tag{2.8}$$

where, $\alpha_i(t)$ and $\beta_i(t)$ are BDVs, and satisfy the following statistical properties:

$$\begin{aligned} Pr\{\alpha_i(t)=1\} = \bar{\alpha}_i, Pr\{\alpha_i(t)=0\} = 1-\bar{\alpha}_i, \\ \mathbb{E}\{\alpha_i(t)\} = \bar{\alpha}_i, \mathbb{E}\{\alpha_i(t)-\bar{\alpha}_i\} = 0, \mathbb{E}\{(\alpha_i(t)-\bar{\alpha}_i)^2\} = \bar{\alpha}_i(1-\bar{\alpha}_i) = \delta_\alpha^2. \\ Pr\{\beta_i(t)=1\} = \bar{\beta}_i, Pr\{\beta_i(t)=0\} = 1-\bar{\beta}_i, \\ \mathbb{E}\{\beta_i(t)\} = \bar{\beta}_i, \mathbb{E}\{\beta_i(t)-\bar{\beta}_i\} = 0, \mathbb{E}\{(\beta_i(t)-\bar{\beta}_i)^2\} = \bar{\beta}_i(1-\bar{\beta}_i) = \delta_\beta^2. \end{aligned} \tag{2.9}$$

Remark 2. *Equation (2.8) is a hybrid-driven cyber-attack behavior, i.e., the deception attacks and the DoS attacks both switch with each other at different frequencies in the communication channel. The BDVs $\alpha(t)$ and $\beta(t)$ describe the occurrence sequence of deception attacks and DoS attacks, respectively. For example, if $\beta(t) = 1$, the communication network is under DoS attacks, which means that all transmission data is blocked. If $\alpha(t) = 1$, the communication network suffers from under deception attack, which means that the real transmission data is replaced by the deception attack signal.*

Remark 3. *For the hybrid attack model, a nonlinear function with time delay $\eta(t)$ on the interval $(0, \eta_M]$ is introduced to express the deception attack signal $\mathscr{F}$, and satisfies the following assumption:*

$$\|f(y_i(t-\eta(t)))\|_2 \le \|F_i y_i(t-\eta(t))\|_2, \tag{2.10}$$

where F is a known matrix.

2.3. System modeling

Under AETM and hybrid attacks, the estimator on the node i is given as follows:

$$\begin{cases} \hat{x}_i(t) = D_i\hat{x}_i(t) + g(\hat{x}_i(t)) + \sum_{j=1}^{N} a_{ij}\Gamma\hat{x}_j(t) + L_i(\tilde{y}_i(t) - \hat{y}_i(t)), \\ \hat{y}_i(t) = C_i\hat{x}_i(t), \\ \hat{z}_i(t) = M_i\hat{x}_i(t), \end{cases} \tag{2.11}$$

where $\hat{x} \in \mathbb{R}^n$ is the estimated state on the node i, $\hat{z}_i(t) \in \mathbb{R}^m$ is the estimate of $z_i(t)$, and L_i is the estimator gain to be designed.

Define

$$e_i(t) = x_i(t) - \hat{x}_i(t),$$

and

$$\tilde{z}_i(t) = z_i(t) - \hat{z}_i(t).$$

For simplicity, we denote that

$$\begin{aligned}
&e(t) = col_N\{e_i(t)\}, e_d(t) = col_N\{e_i(t-d(t))\},\\
&x(t) = col_N\{x_i(k)\}, x_d(t) = col_N\{x_i(t-d(t))\},\\
&\tilde{x}(t) = col_N\{\tilde{x}_i(t)\}, w(t) = col_N\{w_i(t)\}, z(t) = col_N\{z_i(t)\},\\
&C|D|E|L|M|\Omega = diag_N\{C_i|D_i|E_i|L_i|M_i|\Omega_i\},\\
&\alpha(t)|\beta(t) = diag_N\{\alpha_i(t)|\beta_i(t)\}, \bar{\alpha}|\bar{\beta} = diag_N\{\bar{\alpha}_i|\bar{\beta}_i\},\\
&e_k(t) = col_N\{e_{ki}(t)\}, f(y(t-\eta(t))) = col_N\{f(y_i(t-\eta(t)))\}.
\end{aligned}$$

Then, by combining (2.1)–(2.11) and utilizing Kronecker product, we have

$$\begin{cases}
\dot{e}(t) = (D + A\otimes\Gamma - LC)e(t) + g(e(t)) + LCx(t) + Ew(t)\\
\qquad\quad -\{(1-\beta(t))(1-\alpha(t))LC[x(t-d(t)) + e_k(t)] + (1-\beta(t))\alpha(t)L\mathscr{F}\},\\
\tilde{z}(t) = Me(t).
\end{cases} \tag{2.12}$$

Denote $\tilde{x}(t) = \begin{bmatrix} x(t) \\ e(t) \end{bmatrix}$, and the augmented system can be obtained from (2.1) and (2.11) as follows:

$$\begin{cases}
\dot{\tilde{x}}(t) = \mathscr{D}\tilde{x}(t) + g(\tilde{x}(t)) + \mathscr{E}w(t) - (1-\beta(t))(1-\alpha(t))\{\Lambda_1\tilde{x}(t-d(t)) + \Lambda_2 e_k(t)\}\\
\qquad\quad -(1-\beta(t))\alpha(t)\Lambda_3\mathscr{F}.\\
\tilde{z}(t) = \widetilde{M}\tilde{x}(t).
\end{cases} \tag{2.13}$$

where

$$\begin{aligned}
&\mathscr{D} = \begin{bmatrix} D + A\otimes\Gamma & 0 \\ LC & D + A\otimes\Gamma - LC \end{bmatrix}, \mathscr{E} = \begin{bmatrix} E \\ E \end{bmatrix}, \widetilde{M} = \begin{bmatrix} 0 & M \end{bmatrix},\\
&\Lambda_1 = \begin{bmatrix} 0 & 0 \\ LC & 0 \end{bmatrix}, \Lambda_2 = \begin{bmatrix} 0 \\ LC \end{bmatrix}, \Lambda_3 = \begin{bmatrix} 0 \\ L \end{bmatrix}, H = \begin{bmatrix} I & 0 \end{bmatrix},
\end{aligned}$$

system (2.13) can be written as:

$$\dot{\tilde{x}}(t) = \Pi_1 + (\alpha(t) - \bar{\alpha})\Pi_2 + (\beta(t) - \bar{\beta})\Pi_3 + (\alpha(t) - \bar{\alpha})(\beta(t) - \bar{\beta})\Pi_4, \tag{2.14}$$

where

$$\begin{aligned}
\Pi_1 =& \mathscr{D}\tilde{x}(t) + g(\tilde{x}(t)) + \mathscr{E}\omega(t) - (1-\bar{\beta})(1-\bar{\alpha})\{\Lambda_1\tilde{x}(t-d(t)) + \Lambda_2 e_k(t)\} - (1-\bar{\beta})\bar{\alpha}\Lambda_3\mathscr{F},\\
\Pi_2 =& (1-\bar{\beta})[\Lambda_1\tilde{x}(t-d(t)) + \Lambda_2 e_k(t) - \Lambda_3\mathscr{F}],\\
\Pi_3 =& (1-\bar{\alpha})[\Lambda_1\tilde{x}(t-d(t)) + \Lambda_2 e_k(t)] + \bar{\alpha}\Lambda_3\mathscr{F},\\
\Pi_4 =& -\Lambda_1\tilde{x}(t-d(t)) - \Lambda_2 e_k(t) + \Lambda_3\mathscr{F}.
\end{aligned}$$

Assumption 1. *[24] For positive diagonal maxtrix $U = diag\{\mu_1, \mu_2, \cdots, \mu_n\}$, the following inequality holds:*

$$\begin{bmatrix} \tilde{x}(t) \\ g(\tilde{x}(t)) \end{bmatrix}^T \begin{bmatrix} -UG_1 & * \\ G_2U & -U \end{bmatrix} \begin{bmatrix} \tilde{x}(t) \\ g(\tilde{x}(t)) \end{bmatrix} \geq 0, \tag{2.15}$$

where

$$G_1 = diag\{\nu_1^-\nu_1^+, \nu_2^-\nu_2^+, \cdots, \nu_n^-\nu_n^+\},$$
$$G_2 = diag\{\frac{\nu_1^- + \nu_1^+}{2}, \frac{\nu_2^- + \nu_2^+}{2}, \cdots, \frac{\nu_n^- + \nu_n^+}{2}\}.$$

Lemma 1. *[24] For any matrices $\Re_{1|2} > 0$, positive scalars $d_M|\eta_M$, and $d(t)|\eta(t) \in [0, d_M|\eta_M]$, if there exist matrices $\mathfrak{N}_{1|2} \in \mathbb{R}^{n\times n}$ such that $\begin{bmatrix} \Re_{1|2} & * \\ \mathfrak{N}_{1|2} & \Re_{1|2} \end{bmatrix} > 0$, the following inequality holds:*

$$-d_M|\eta_M \int_{t-d_M|\eta_M}^{t} \dot{\tilde{x}}^T(s)\Re_{1|2}\dot{\tilde{x}}(s)ds \leq \Xi^T \begin{bmatrix} -\Re_{1|2} & * & * \\ \Re_{1|2} - \mathfrak{N}_{1|2} & -2\Re_{1|2} + \mathfrak{N}_{1|2} + \mathfrak{N}_{1|2}^T & * \\ \mathfrak{N}_{1|2} & \Re_{1|2} - \mathfrak{N}_{1|2} & -\Re_{1|2} \end{bmatrix} \Xi. \tag{2.16}$$

where $\Xi = \begin{bmatrix} \tilde{x}(t) \\ \tilde{x}(t - d(t)|\eta(t)) \\ \tilde{x}(t - d_M|\eta_M) \end{bmatrix}$.

Lemma 2. *[11] For any positive-definite matrices $\mathcal{R}, \mathcal{Z}$ and scalar ϵ, the following inequality holds.*

$$-\mathcal{Z}\mathcal{R}^{-1}\mathcal{Z} \leq \epsilon^2\mathcal{R} - 2\epsilon\mathcal{Z}. \tag{2.17}$$

3. Main results

This section is concerned with the design problem for adaptive event-triggered state estimators such that the augmented dynamics (2.14) of the CNs (2.1) is asymptotically stable.

Theorem 1. *For given constants $d_M, \eta_M, \bar{\alpha}, \bar{\beta}, \varpi$, estimator gain L, and weighting matrix Ω, the augmented dynamics (2.14) is asymptotically stable if there exist matrices $\mathfrak{P} > 0, \mathfrak{Q}_i > 0, \Re_i > 0$, and $\mathfrak{N}_i$, such that the following inequalities are satisfied for $i = 1, 2$:*

$$\Theta = \begin{bmatrix} \Sigma & * & * & * & * \\ \Psi_1 & \Re^* & * & * & * \\ \Psi_2 & 0 & \Re^* & * & * \\ \Psi_3 & 0 & 0 & \Re^* & * \\ \Psi_4 & 0 & 0 & 0 & \Re^* \end{bmatrix} < 0, \tag{3.1}$$

$$\begin{bmatrix} \Re_1 & * \\ \mathfrak{N}_1 & \Re_1 \end{bmatrix} > 0, \tag{3.2}$$

$$\begin{bmatrix} \Re_2 & * \\ \mathfrak{N}_2 & \Re_2 \end{bmatrix} > 0, \tag{3.3}$$

where

$$
\begin{aligned}
\Sigma =&[(1.1) = \mathscr{D}^T\mathfrak{P} + \mathfrak{P}\mathscr{D} + \mathfrak{Q}_1 + \mathfrak{Q}_2 - UG_1 - \mathfrak{R}_1 - \mathfrak{R}_2 + \widetilde{M}^T\widetilde{M}\\
&(2.1) = -(1-\bar{\alpha})(1-\bar{\beta})\Lambda_1^T\mathfrak{P} + \mathfrak{R}_1 - \mathfrak{N}_1\\
&(2.2) = H^TC^T\Omega CH - 2\mathfrak{R}_1 + \mathfrak{N}_1 + \mathfrak{N}_1^T\\
&(3.1) = \mathfrak{N}_1, (3.2) = \mathfrak{R}_1 - \mathfrak{N}_1, (3.3) = -\mathfrak{R}_1 - \mathfrak{Q}_1\\
&(4.1) = \mathfrak{R}_2 - \mathfrak{N}_2, (4.4) = -2\mathfrak{R}_2 + \mathfrak{N}_2 + \mathfrak{N}_2^T + H^TC^TF^TFCH\\
&(5.1) = \mathfrak{N}_2, (5.4) = \mathfrak{R}_2 - \mathfrak{N}_2, (5.5) = -\mathfrak{Q}_2 - \mathfrak{R}_2\\
&(6.1) = -(1-\bar{\beta})(1-\bar{\alpha})\Lambda_2^T\mathfrak{P}, (6.6) = -\varpi\Omega\\
&(7.1) = -(1-\bar{\beta})\bar{\alpha}\Lambda_3^T\mathfrak{P}, (7.7) = -I\\
&(8.1) = \mathfrak{P} + G_2U, (8.8) = -U\\
&(9.1) = \mathscr{E}\mathfrak{P}, (9.9) = -\gamma^2],
\end{aligned}
$$

$$
\Psi_j = \begin{bmatrix} d_M\Gamma_j \\ \eta_M\Gamma_j \end{bmatrix},
$$

$$
\Gamma_1 = \begin{bmatrix} \mathfrak{P}\mathscr{D} & -(1-\bar{\beta})(1-\bar{\alpha})\mathfrak{P}\Lambda_1 & 0 & 0 & 0 & -(1-\bar{\beta})(1-\bar{\alpha})\mathfrak{P}\Lambda_2 & -(1-\bar{\beta})(1-\bar{\alpha})\mathfrak{P}\Lambda_3 & \mathfrak{P} & \mathfrak{P}\mathscr{E} \end{bmatrix},
$$

$$
\Gamma_2 = \begin{bmatrix} 0 & \delta_\alpha(1-\bar{\beta})\mathfrak{P}\Lambda_1 & 0 & 0 & 0 & \delta_\alpha(1-\bar{\beta})\mathfrak{P}\Lambda_2 & -\delta_\alpha(1-\bar{\beta})\mathfrak{P}\Lambda_3 & 0 & 0 \end{bmatrix},
$$

$$
\Gamma_3 = \begin{bmatrix} 0 & \delta_\beta(1-\bar{\alpha})\mathfrak{P}\Lambda_1 & 0 & 0 & 0 & \delta_\beta(1-\bar{\alpha})\mathfrak{P}\Lambda_2 & \delta_\alpha\delta_\beta\mathfrak{P}\Lambda_3 & 0 & 0 \end{bmatrix},
$$

$$
\Gamma_4 = \begin{bmatrix} 0 & -\delta_\alpha\delta_\beta\mathfrak{P}\Lambda_1 & 0 & 0 & 0 & -\delta_\alpha\delta_\beta\mathfrak{P}\Lambda_2 & \delta_\alpha\delta_\beta\mathfrak{P}\Lambda_3 & 0 & 0 \end{bmatrix},
$$

$$
\mathfrak{R}^* = diag\{-\mathfrak{P}\mathfrak{R}_1^{-1}\mathfrak{P}, -\mathfrak{P}\mathfrak{R}_2^{-1}\mathfrak{P}\}.
$$

Proof. Contruct an Lyapunov functional candidate:

$$
V(x(t), t) = \sum_{i=1}^{3} V_i(x(t), t) + V_4(t), \tag{3.4}
$$

where

$$
\begin{aligned}
V_1(x(t), t) =& \tilde{x}^T(t)\mathfrak{P}\tilde{x}(t),\\
V_2(x(t), t) =& \int_{t-d_M}^{t} \tilde{x}^T(s)\mathfrak{Q}_1\tilde{x}(s)ds + \int_{t-\eta_M}^{t} \tilde{x}^T(s)\mathfrak{Q}_2\tilde{x}(s)ds,\\
V_3(x(t), t) =& d_M\int_{-d_M}^{0}\int_{t+\theta}^{t} \dot{\tilde{x}}^T(s)\mathfrak{R}_1\dot{\tilde{x}}(s)dsd\theta + \eta_M\int_{-\eta_M}^{0}\int_{t+\theta}^{t} \dot{\tilde{x}}^T(s)\mathfrak{R}_2\dot{\tilde{x}}(s)dsd\theta,\\
V_4(t) =& \frac{1}{2}\varrho^2(t),
\end{aligned}
$$

The derivative and mathematical expectation of (3.4) can be calculated as:

$$\begin{aligned}\mathbb{E}\{\dot{V}(x(t),t)\} =& sym\{\tilde{x}^T(t)\mathfrak{P}\Pi_1\} + \tilde{x}^T(t)(\mathfrak{Q}_1+\mathfrak{Q}_2)\tilde{x}(t)\\ &- \tilde{x}^T(t-d_M)\mathfrak{Q}_1\tilde{x}(t-d_M) - \tilde{x}^T(t-\eta_M)\mathfrak{Q}_2\tilde{x}(t-\eta_M)\\ &+ \Pi_1^T\Xi\Pi_1 + \delta_\alpha^2\Pi_2^T\Xi\Pi_2 + \delta_\beta^2\Pi_3^T\Xi\Pi_3 + \delta_\alpha^2\delta_\beta^2\Pi_4^T\Xi\Pi_4\\ &+ \frac{1}{\varrho(t)}e_k^T(t)\Omega e_k(t) - \varpi e_k^T(t)\Omega e_k(t)\\ &- d_M\int_{t-d_M}^{t}\dot{\tilde{x}}^T(s)\Re_1\dot{\tilde{x}}(s)ds - \eta_M\int_{t-\eta_M}^{t}\dot{\tilde{x}}^T(s)\Re_2\dot{\tilde{x}}(s)ds,\end{aligned} \tag{3.5}$$

where $\Xi = d_M^2\Re_1 + \eta_M^2\Re_2$.

Then, the following inequality can be obtained from Remark 3:

$$\tilde{x}^T(t-\eta(t))H^TC^TF^TFCH\tilde{x}(t-\eta(t)) - \mathscr{F}^T\mathscr{F} \geq 0. \tag{3.6}$$

Combining (3.5) and (3.6), using Lemma 1 to estimate one cross term in (3.5), taking the adaptive triggering condition (2.2) and (2.3) to bound the term $\frac{1}{\varrho(t)}e_k^T(t)\Omega e_k(t)$ in (3.5), and adding (2.15) in Assumption 1 to the right-hand side of (3.5), one obtains

$$\begin{aligned}&\mathbb{E}\{\dot{V}(x(t),t)\} + \tilde{z}^T(t)\tilde{z}(t) - \gamma^2w^T(t)w(t)\\ &\leq \xi^T(t)\Sigma\xi(t) + \Pi_1^T\Xi\Pi_1 + \delta_\alpha^2\Pi_2^T\Xi\Pi_2 + \delta_\beta^2\Pi_3^T\Xi\Pi_3 + \delta_\alpha^2\delta_\beta^2\Pi_4^T\Xi\Pi_4,\end{aligned} \tag{3.7}$$

where $\xi(t) = \{\tilde{x}(t), \tilde{x}(t-d(t)), \tilde{x}(t-d_M), \tilde{x}(t-\eta(t)), \tilde{x}(t-\eta_M), e_k(t), \mathscr{F}, g(\tilde{x}(t)), w(t)\}$.

Utilizing Schur complement, we can obtain that (3.7) is equivalent to (3.1)–(3.3). When $w(t) = 0$, it can be seen that the system (2.14) is asymptotically stable from the LMIs (3.1)–(3.3). This completes the proof. □

So far, the stability analysis problem of augmented systems for state estimation about complex network has been solved. Based on Theorem 1, we can easily obtain the estimator gains. Details are as follows.

Theorem 2. *For given constants $d_M, \eta_M, \bar{\alpha}, \bar{\beta}, \varpi$, the estimator (2.11) for the system (2.14) can be designed if there exist matrices $\mathfrak{P} = diag\{\mathfrak{P}_1, \mathfrak{P}_2\} > 0, \mathfrak{Q}_i > 0, \Re_i > 0$, and $\Re_i$, such that the following inequalities are satisfied for $i = 1, 2$:*

$$\widehat{\Theta} = \begin{bmatrix}\widehat{\Sigma} & * & * & * & *\\ \widehat{\Psi}_1 & \widehat{\Re}^* & * & * & *\\ \widehat{\Psi}_2 & 0 & \widehat{\Re}^* & * & *\\ \widehat{\Psi}_3 & 0 & 0 & \widehat{\Re}^* & *\\ \widehat{\Psi}_4 & 0 & 0 & 0 & \widehat{\Re}^*\end{bmatrix} < 0, \tag{3.8}$$

(3.2) and (3.3), where

$$
\begin{aligned}
\widehat{\Sigma} =&[(1.1) = \Lambda_4 + \Lambda_4^T + \mathfrak{Q}_1 + \mathfrak{Q}_2 - UG_1 - \Re_1 - \Re_2 + \widetilde{M}^T\widetilde{M}\\
&(2.1) = -(1-\bar{\alpha})(1-\bar{\beta})\Lambda_5^T + \Re_1 - \mathfrak{N}_1\\
&(2.2) = H^TC^T\Omega CH - 2\Re_1 + \mathfrak{N}_1 + \mathfrak{N}_1^T\\
&(3.1) = \mathfrak{N}_1, (3.2) = \Re_1 - \mathfrak{N}_1, (3.3) = -\Re_1 - \mathfrak{Q}_1\\
&(4.1) = \Re_2 - \mathfrak{N}_2, (4.4) = -2\Re_2 + \mathfrak{N}_2 + \mathfrak{N}_2^T + H^TC^TF^TFCH\\
&(5.1) = \mathfrak{N}_2, (5.4) = \Re_2 - \mathfrak{N}_2, (5.5) = -\mathfrak{Q}_2 - \Re_2\\
&(6.1) = -(1-\bar{\beta})(1-\bar{\alpha})\Lambda_6^T, (6.6) = -\varpi\Omega\\
&(7.1) = -(1-\bar{\beta})\bar{\alpha}\Lambda_7^T, (7.7) = -I\\
&(8.1) = \mathfrak{P} + G_2U, (8.8) = -U\\
&(9.1) = \mathscr{E}\mathfrak{P}, (9.9) = -\gamma^2],
\end{aligned}
$$

$$
\widehat{\Psi}_j = \begin{bmatrix} d_M\widehat{\Gamma}_j \\ \eta_M\widehat{\Gamma}_j \end{bmatrix},
$$

$$
\widehat{\Gamma}_1 = \begin{bmatrix} \Lambda_4 & -(1-\bar{\beta})(1-\bar{\alpha})\Lambda_5 & 0 & 0 & 0 & -(1-\bar{\beta})(1-\bar{\alpha})\Lambda_6 & -(1-\bar{\beta})(1-\bar{\alpha})\Lambda_7 & \mathfrak{P} & \mathfrak{P}\mathscr{E} \end{bmatrix},
$$

$$
\widehat{\Gamma}_2 = \begin{bmatrix} 0 & \delta_\alpha(1-\bar{\beta})\Lambda_5 & 0 & 0 & 0 & \delta_\alpha(1-\bar{\beta})\Lambda_6 & -\delta_\alpha(1-\bar{\beta})\Lambda_7 & 0 & 0 \end{bmatrix},
$$

$$
\widehat{\Gamma}_3 = \begin{bmatrix} 0 & \delta_\beta(1-\bar{\alpha})\Lambda_5 & 0 & 0 & 0 & \delta_\beta(1-\bar{\alpha})\Lambda_6 & \delta_\alpha\delta_\beta\Lambda_7 & 0 & 0 \end{bmatrix},
$$

$$
\widehat{\Gamma}_4 = \begin{bmatrix} 0 & -\delta_\alpha\delta_\beta\Lambda_5 & 0 & 0 & 0 & -\delta_\alpha\delta_\beta\Lambda_6 & \delta_\alpha\delta_\beta\Lambda_7 & 0 & 0 \end{bmatrix},
$$

$$
\widehat{\Re}^* = diag\{\varepsilon^2\Re_1 - 2\varepsilon\mathfrak{P}, \varepsilon^2\Re_2 - 2\varepsilon\mathfrak{P}\},
$$

$$
\Lambda_4 = \begin{bmatrix} \mathfrak{P}_1D + \mathfrak{P}_1A\otimes\Gamma & 0 \\ XC & \mathfrak{P}_2D + \mathfrak{P}_2A\otimes\Gamma - XC \end{bmatrix},
$$

$$
\Lambda_5 = \begin{bmatrix} 0 & 0 \\ XC & 0 \end{bmatrix}, \Lambda_6 = \begin{bmatrix} 0 \\ XC \end{bmatrix}, \Lambda_7 = \begin{bmatrix} 0 \\ X \end{bmatrix}.
$$

In addition, the estimator gains can be obtained by $L_i = P_{2i}^{-1}X_i (i = 1, 2, \ldots, N)$.

Proof. By applying Lemma 2, replacing $-\mathfrak{P}\Re_1\mathfrak{P}$ in (3.1) by $\varepsilon\Re_1 - 2\varepsilon\mathfrak{P}$, a new $\widehat{\Re}^*$ is obtained as:

$$
\widehat{\Re}^* = diag\{\varepsilon^2\Re_1 - 2\varepsilon\mathfrak{P}, \varepsilon^2\Re_2 - 2\varepsilon\mathfrak{P}\}.
$$

Noticing that $X = P_2L$, (3.8) can be obtained. This completes the proof. □

4. Examples and simulations

In this section, we provide numerical simulations to demonstrate the validity of the theoretical approach. We take a complex network with three nodes as an example.

Example 1. *The system parameters are given as follows:*

$$\begin{aligned}
D_1 =&D_2 = D_3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},\\
\Gamma =& \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix},\\
a_{ij} =& \begin{cases} -2, i \neq j \\ 1, i = j \end{cases},\\
E_1 =& \begin{bmatrix} 0.3 \\ 0.3 \end{bmatrix}, E_2 = \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix}, E_3 = \begin{bmatrix} 0.4 \\ 0.4 \end{bmatrix},\\
C_1 =& \begin{bmatrix} 0.4 & 0.5 \end{bmatrix}, C_2 = \begin{bmatrix} -0.4 & 0.5 \end{bmatrix}, C_3 = \begin{bmatrix} 0.4 & -0.5 \end{bmatrix},\\
M_1 =&M_2 = M_3 = \begin{bmatrix} 0.3 & 0.7 \end{bmatrix},\\
g(x_i(t)) =& \begin{bmatrix} 0.5x_{i1}(t) - tanh(0.2x_{i1}(t)) + 0.2x_{i2}(t), \\ 0.95x_{i2}(t) - tanh(0.75x_{i1}(t)) \end{bmatrix}.
\end{aligned}$$

The deception attack signal is chosen as

$$f(x_i(t)) = \begin{bmatrix} -tanh(-0.3x_{i2}(t)) \\ -tanh(-0.3x_{i1}(t)) \end{bmatrix}.$$

Moreover, other parameters are selected by

$$\begin{aligned}
d_M = 0.1, \eta_M = 0.1, \bar{\alpha} = 0.2, \bar{\beta} = 0.2, \varpi = 7, \gamma = 4, \varepsilon = 1,\\
F = diag_N\{0.3, 0.3\}, G_1 = diag_N\{0, 0\}, G_2 = diag_N\{0.02, 0.02\}.
\end{aligned}$$

By utilizing the MATLAB LMI Toolbox, the feasible solutions can be obtained based on the constraints (3.8), (3.2) and (3.3) in Theorem 2.

$$\begin{aligned}
X_1 =& \begin{bmatrix} 11.4784 \\ 11.2668 \end{bmatrix}, X_2 = \begin{bmatrix} 0.1131 \\ 2.8645 \end{bmatrix}, X_3 = \begin{bmatrix} 0.1590 \\ -2.6171 \end{bmatrix}.\\
P_{21} =& 10^3 \times \begin{bmatrix} 2.5019 & -2.4698 \\ -2.4698 & 2.5020 \end{bmatrix},\\
P_{22} =& 10^3 \times \begin{bmatrix} 2.5087 & -2.4629 \\ -2.4629 & 2.5088 \end{bmatrix},\\
P_{23} =& 10^3 \times \begin{bmatrix} 2.5087 & -2.4628 \\ -2.4628 & 2.5089 \end{bmatrix},\\
\Omega_1 =& 52.0965, \Omega_2 = 839.7490, \Omega_2 = 950.6389.
\end{aligned}$$

Further, the estimator gains can be designed as:

$$L_1 = \begin{bmatrix} 0.3538 \\ 0.3538 \end{bmatrix}, L_2 = \begin{bmatrix} 0.0322 \\ 0.0327 \end{bmatrix}, L_3 = \begin{bmatrix} -0.0264 \\ -0.0270 \end{bmatrix}.$$

Given the initial state $x_1(0) = \begin{bmatrix} 1 & -1 \end{bmatrix}^T$, $x_2(0) = \begin{bmatrix} 1 & 0 \end{bmatrix}^T$, $x_3(0) = \begin{bmatrix} 0 & -1 \end{bmatrix}^T$, $\hat{x}_i(0) = \begin{bmatrix} 0 & 0 \end{bmatrix}^T$, *and* $\varrho_i(0) = 0.25(i = 1, 2, 3)$, *numerical simulations further verify the validity of our theoretical approach. Figures 2–4 show the state responses for node i. Figures 2–7 plot the output estimation error for node i. Figures 8 and 9 depict the occurring instants of deception attacks and DoS attacks, respectively. Figures 10–12 present the release instants and intervals under AETS for node i. In addition, the release instants and intervals of ETS are plotted in Figures 13–15, respectively. The average period, maximum release interval, and transmission rate by Theorem 2 and reported in [24] are listed in Table 1, which the transmission rate indicates* $\frac{\text{the transmitted data}}{\text{the sampled data}} \times 100\%$. *Obviously, the AETS can obtain a larger release interval than the traditional ETS, and have a lower data delivery rate.*

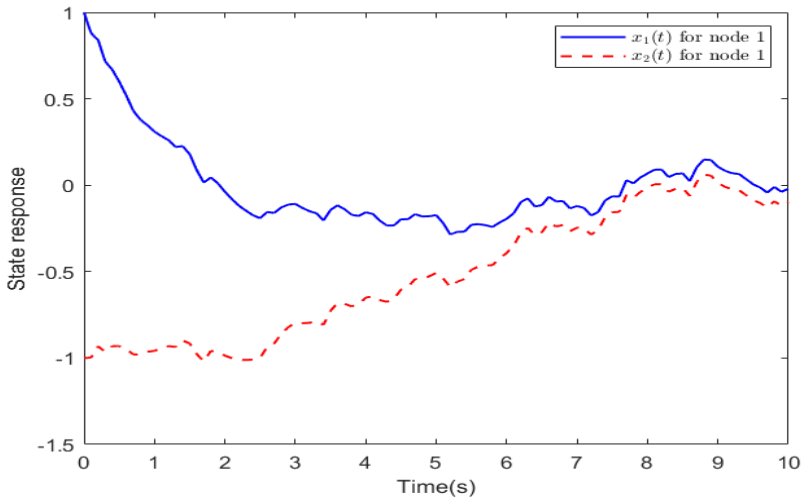

Figure 2. Response of $x(t)$ for node 1.

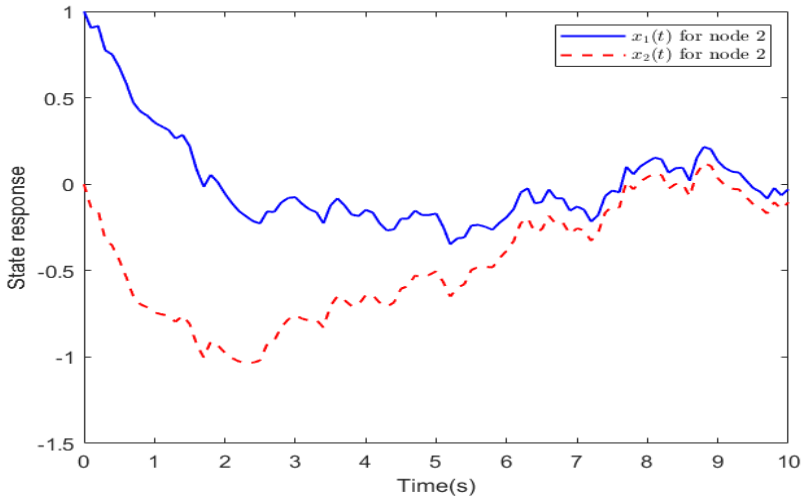

Figure 3. Response of $x(t)$ for node 2.

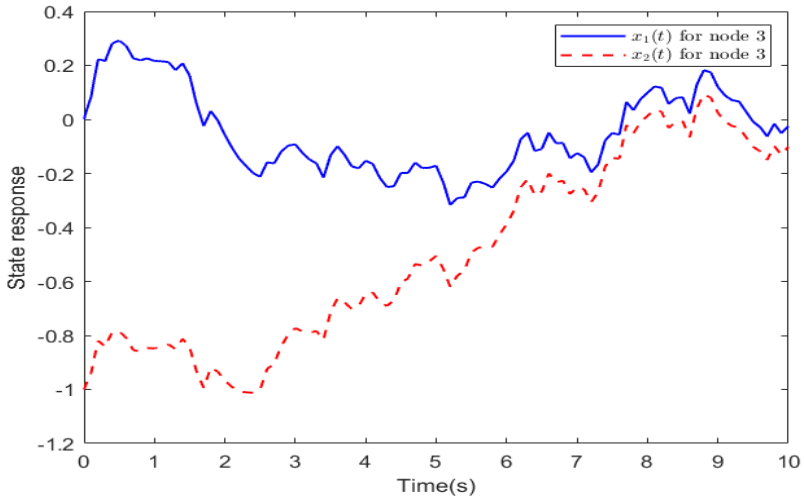

Figure 4. Response of $x(t)$ for node 3.

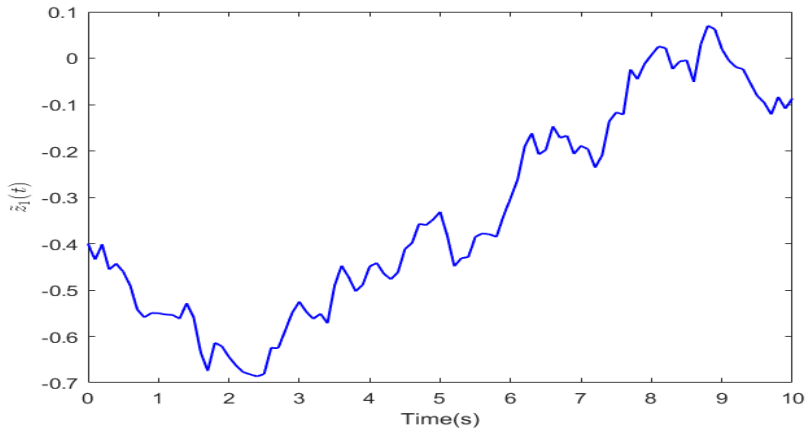

Figure 5. Output estimation error of $\tilde{z}(t)$ for node 1.

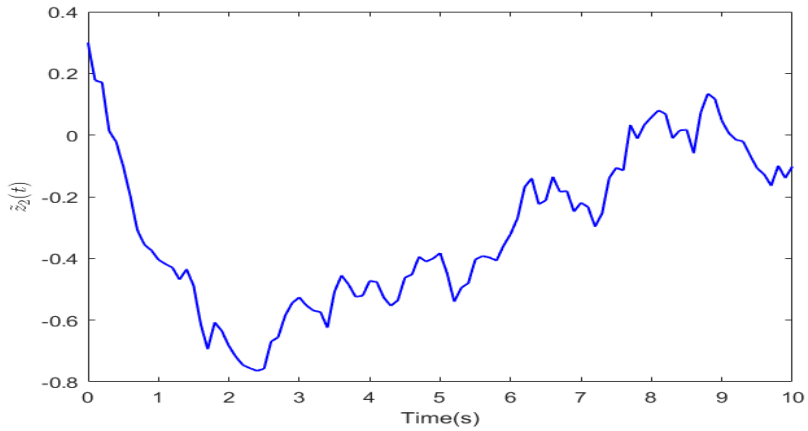

Figure 6. Output estimation error of $\tilde{z}(t)$ for node 2.

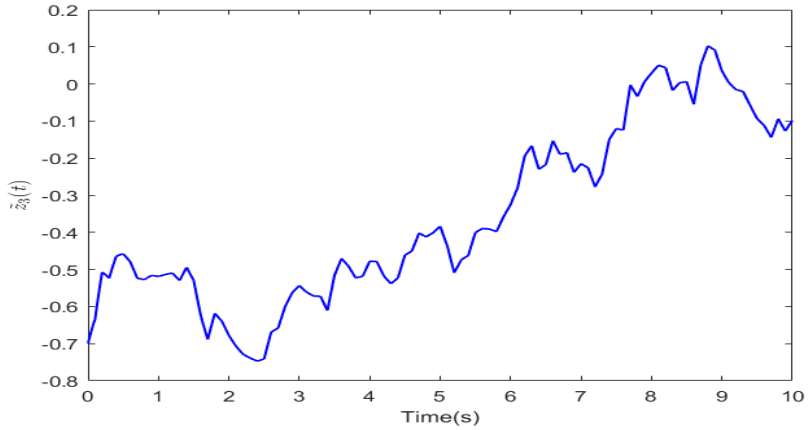

Figure 7. Output estimation error of $\tilde{z}(t)$ for node 3.

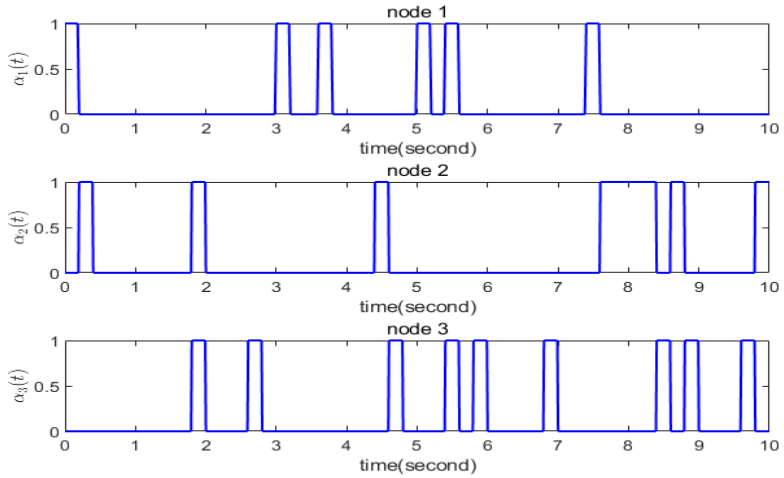

Figure 8. Occurring instants of deception attacks.

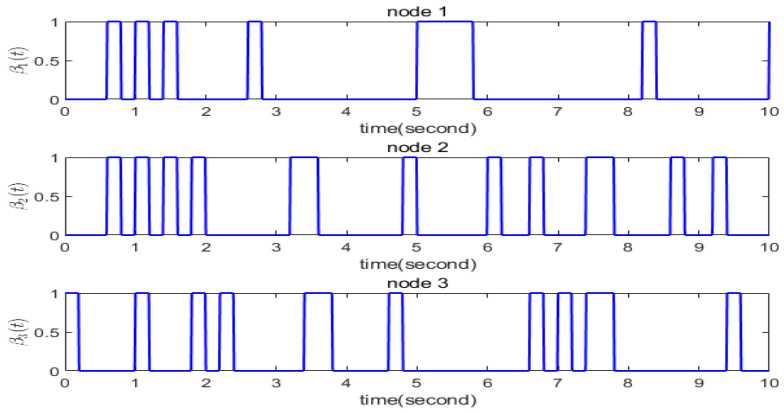

Figure 9. Occurring instants of DoS attacks.

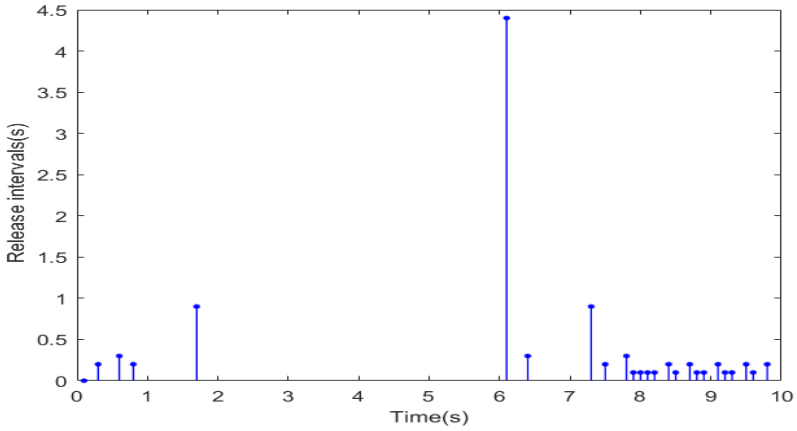

Figure 10. Release instants and intervals under AETS of node 1.

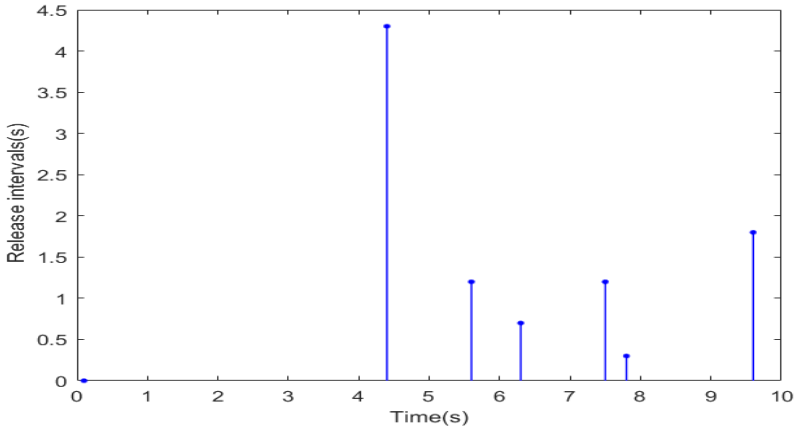

Figure 11. Release instants and intervals under AETS of node 2.

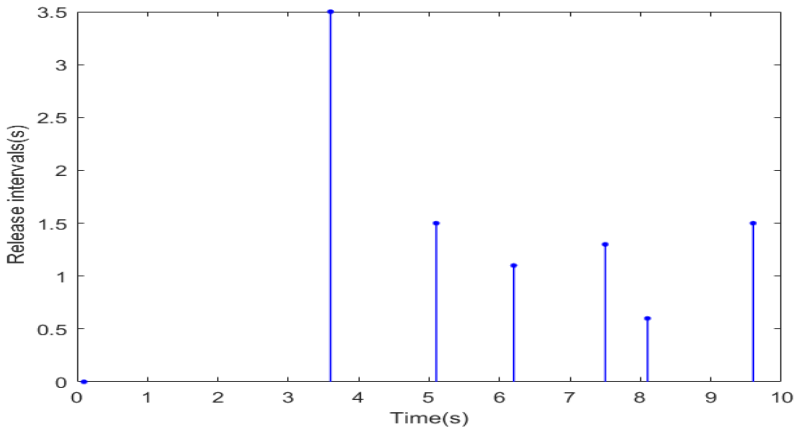

Figure 12. Release instants and intervals under AETS of node 3.

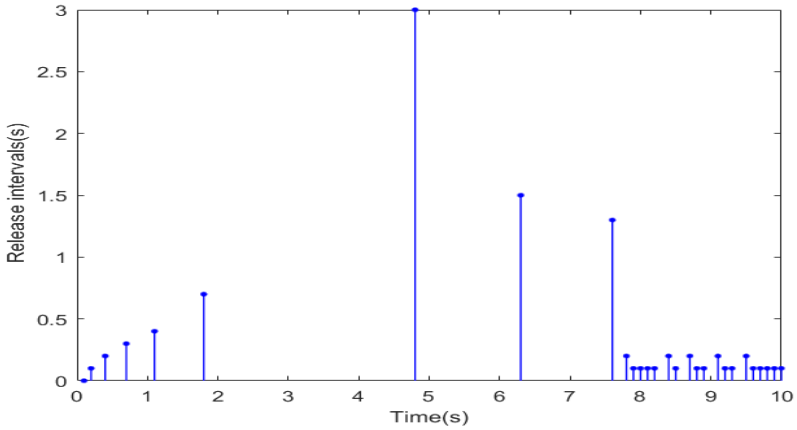

Figure 13. Release instants and intervals under ETS [24] of node 1.

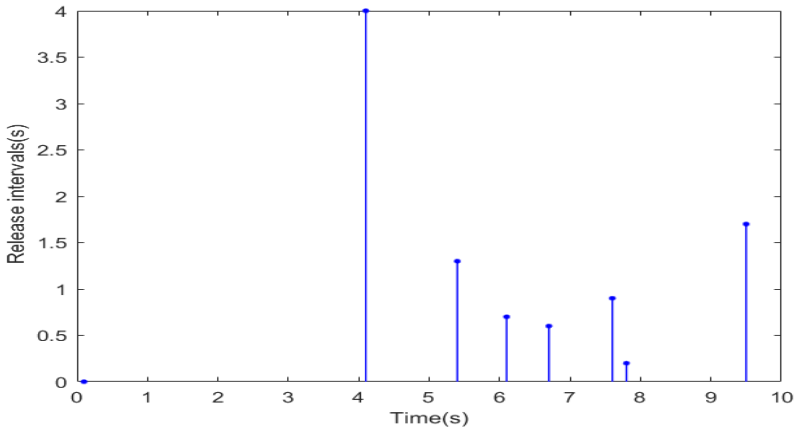

Figure 14. Release instants and intervals under ETS [24] of node 2.

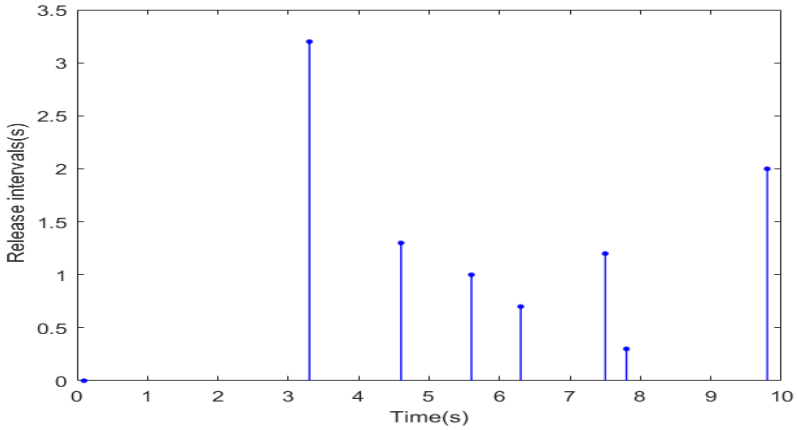

Figure 15. Release instants and intervals under ETS [24] of node 3.

Table 1. The average period, maximum release interval and transmission rate for different scheme in Example 1.

sampling period $h = 0.1s$	average period	maximum release interval	transmission rate
AETS in node 1	0.4000	4.4	25%
AETS in node 2	1.4285	4.3	7%
AETS in node 3	1.4285	3.5	7%
ETS [24] in node 1	0.3571	3.0	28%
ETS [24] in node 2	1.2500	4.0	8%
ETS [24] in node 3	1.2500	3.2	8%

5. Conclusions

The issue of event-triggered state estimation has been studied for CNs under hybrid cyber-attacks in this paper. AETS has been introduced to alleviate the network congestion problem. With the help of two sets of BDVs and an arbitrary function related to the system state, a mathematical model of the hybrid cyber-attacks has been established to portray randomly occurring DoS attacks and deception attacks. Then, CNs, AETS, hybrid cyber-attacks, and state estimators have been incorporated into a unified architecture. As a result, an augmented system has been presented. Furthermore, based on Lyapunov stability theory and LMIs, sufficient conditions to ensure the asymptotic stability of the augmented system have been derived, and the corresponding state estimator has been designed. Finally, the effectiveness of the theoretical method has been demonstrated by numerical examples and simulations. In the future, security state estimation problems for a class of CNs suffered by underlying attacks will be studied.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

1. H. Shen, M. P. Xing, Z. G. Wu, J. D. Cao, T. W. Huang, $l_2 - l_\infty$ state estimation for persistent Dwell-time switched coupled networks subject to round-robin protocol, *IEEE T. Neur. Net. Lear.*, **32** (2020), 2002–2014. doi: 10.1109/TNNLS.2020.2995708.
2. T. D. Wei, X. Xie, X. D. Li, Input-to-state stability of delayed reaction-diffusion neural networks with multiple impulses, *AIMS Mathematics*, **6** (2021), 5786–5800. doi: 10.3934/math.2021342.
3. H. L. Dong, N. Hou, Z. D. Wang, Fault estimation for complex networks with randomly varying topologies and stochastic inner couplings, *Automatica*, **112** (2020), 108734. doi: 10.1016/j.automatica.2019.108734.
4. J. Hu, Z. D. Wang, G. P. Liu, H. X. Zhang, Variance-constrained recursive state estimation for time-varying complex networks with quantized measurements and uncertain inner coupling, *IEEE T. Neur. Net. Lear.*, **31** (2020), 1955–1967. doi: 10.1109/TNNLS.2019.2927554.

5. R. Sakthivel, M. Sathishkumar, B. Kaviarasan, S. M. Anthoni, Synchronization and state estimation for stochastic complex networks with uncertain inner coupling, *Neurocomputing*, **328** (2017), 44–55. doi: 10.1016/j.neucom.2017.01.035.
6. L. Liu, X. W. Ding, W. N. Zhou, Prescribed-time cluster synchronization of uncertain complex dynamical networks with switching via pinning control, *Neurocomputing*, **419** (2021), 136–147. doi: 10.1016/j.neucom.2020.08.043.
7. Y. R. Liu, Z. D. Wang, Y. Yuan, F. E. Alsaadi, Partial-nodes-based state estimation for complex networks with unbounded distributed delays, *IEEE T. Neur. Net. Lear.*, **29** (2018), 3906–3912. doi: 10.1109/TNNLS.2017.2740400.
8. W. L. Li, Y. M. Jia, J. P. Du, State estimation for stochastic complex networks with switching topology, *IEEE T. Automat. Contr*, **62** (2017), 6377–6384. doi: 10.1109/TAC.2017.2649878.
9. F. E. Alsaadi, Z. D. Wang, D. Wang, F. E. Alsaadi, F. W. Alsaade, Recursive fusion estimation for stochastic discrete time-varying complex networks under stochastic communication protocol: The state-saturated case, *Inform. Fusion*, **60** (2020), 11–19. doi: 10.1016/j.inffus.2020.01.012.
10. N. Hou, Z. D. Wang, D. W. C. Ho, H. L. Dong, Robust partial-nodes-based state estimation for complex networks under deception attacks, *IEEE T. Cybernetics.*, **50** (2020), 2793–2802. doi: 10.1109/TCYB.2019.2918760.
11. H. Q. Lu, Y. H. Deng, W. N. Zhou, Hierarchical type stability and stabilization of networked control systems with event-triggered mechanism via canonical Bessel–Legendre inequalities, *J. Franklin I.*, **358** (2021), 6592–6611. doi: 10.1016/j.jfranklin.2021.06.024.
12. Y. S. Tan, S. M. Fei, J. L. Liu, Distributed hybrid-triggered state estimation for complex networked system with network attacks, *China Sci. Inf. Ser.*, **48** (2018), 1198–1213. doi: 10.1360/N112017-00279.
13. Y. S. Tan, Y. Liu, B. Niu, S. M. Fei, Event-triggered synchronization control for T–S fuzzy neural networked systems with time delay, *J. Franklin I.*, **357** (2020), 5934–5953. doi: 10.1016/j.jfranklin.2020.03.024.
14. W. Zhou, Y. Sun, X. Zhang, P. Shi, Cluster synchronization of coupled neural networks with L*é*vy noise via event-triggered pinning control, *IEEE T. Neur. Net. Lear.*, 2021. doi: 10.1109/TNNLS.2021.3072475.
15. G. Cena, A. Valenzano, Achieving round-robin access in controller area networks, *IEEE T. Ind. Electron*, **49** (2002), 1202–1213. doi: 10.1109/TIE.2002.804968.
16. M. E. M. B. Gaid, A. Cela, Y. Hamam, Optimal integrated control and scheduling of networked control systems with communication constraints: Application to a car suspension system, *IEEE T. Contr. Syst. T.*, **14** (2006), 776–787. doi: 10.1109/TCST.2006.872504.
17. H. Q. Lu, Y. Hu, C. Q. Guo, W. N. Zhou, Cluster synchronization for a class of complex dynamical network system with randomly occurring coupling delays via an improved event-triggered pinning control approach, *J. Franklin I.*, **357** (2020), 2167–2184. doi: 10.1016/j.jfranklin.2019.11.076.
18. N. Li, Q. Li, J. H. Suo, Dynamic event-triggered H_∞ state estimation for delayed complex networks with randomly occurring nonlinearities, *Neurocomputing*, **421** (2021), 97–104. doi: 10.1016/j.neucom.2020.08.048.

19. W. P. M. H. Heemels, K. H. Johansson, P. Tabuada, An introduction to event-triggered and self-triggered control, *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, 2012, 3270–3285. doi: 10.1109/CDC.2012.6425820.
20. Z. X. Zhang, H. L. Liang, C. W. Wu, C. K. Ahn, Adaptive event-triggered output feedback fuzzy control for nonlinear networked systems with packet dropouts and actuator failure, *IEEE T. Fuzzy Syst.*, **27** (2019), 1793–1806. doi: 10.1109/TFUZZ.2019.2891236.
21. Z. Gu, P. Shi, D. Yue, Z. T. Ding, Decentralized adaptive event-triggered h_∞ filtering for a class of networked nonlinear interconnected systems, *IEEE T. Cybernetics.*, **49** (2018), 1570–1579. doi: 10.1109/TCYB.2018.2802044.
22. M. H. Zhu, S. Martinez, On the performance analysis of resilient networked control systems under replay attacks, *IEEE T. Automat. Contr.*, **59** (2014), 804–808. doi: 10.1109/TAC.2013.2279896.
23. Y. S. Tan, Q. Y. Liu, D. S. Du, B. Niu, S. M. Fei, Observer-based finite-time H_∞ control for interconnected fuzzy systems with quantization and random network Attacks, *IEEE T. Fuzzy Syst.*, **29** (2019), 674–685. doi: 10.1109/TFUZZ.2019.2960719.
24. Y. H. Deng, H. Q. Lu, W. N. Zhou, Security event-triggered control for Markovian jump neural networks against actuator saturation and hybrid cyber attacks, *J. Franklin I.*, **358** (2021), 7096–7118. doi: 10.1016/j.jfranklin.2021.07.022.
25. C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, *IEEE T. Automat. Contr.*, **60** (2015), 2930–2944. doi: 10.1109/TAC.2015.2416924.
26. E. Tian, C. Peng, Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks, *IEEE T. Cybernetics*, **50** (2020), 4610–4618. doi: 10.1109/TCYB.2020.2972384.
27. D. Zhao, Z. D. Wang, G. L. Wei, Q. L. Han, A dynamic event-triggered approach to observer-based PID security control subject to deception attacks, *Automatica*, **120** (2020), 109128. doi: 10.1016/j.automatica.2020.109128.
28. J. L. Liu, T. T. Yin, M. Q. Shen, X. P. Xie, J. Cao, State estimation for cyber–physical systems with limited communication resources, sensor saturation and denial-of-service attacks, *ISA T.*, **104** (2020), 101–114. doi: 10.1016/j.isatra.2018.12.032.
29. M. M. Hamdan, M. S. Mahmoud, U. A. Baroudi, Event-triggering control scheme for discrete time cyberphysical systems in the presence of simultaneous hybrid stochastic attacks, *ISA T.*, 2021. In press. doi: 10.1016/j.isatra.2021.04.027.
30. R. Rakkiyappan, K. Sivaranjani, Sampled-data synchronization and state estimation for nonlinear singularly perturbed complex networks with time-delays, *Nonlinear Dyn.*, **84** (2016), 1623–1636. doi: 10.1007/s11071-015-2592-1.
31. K. Sivaranjani, R. Rakkiyappan, Delayed impulsive synchronization of nonlinearly coupled Markovian jumping complex dynamical networks with stochastic perturbations, *Nonlinear Dyn.*, **88** (2017), 1917–1934. doi: 10.1007/s11071-017-3353-0.

AIMS Press