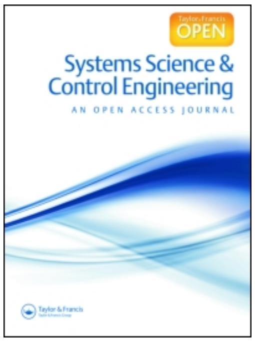


Taylor & Francis
Taylor & Francis Group

Systems Science & Control Engineering

An Open Access Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tssc20

Secure state estimation for cyber physical systems with state delay and sparse sensor attacks

Man Zhang & Chong Lin

SYSTEMS SCIENCE & CONTROL ENGINEERING: AN OPEN ACCESS JOURNAL
https://doi.org/10.1080/21642583.2020.1834465

Taylor & Francis
Taylor & Francis Group

Secure state estimation for cyber physical systems with state delay and sparse sensor attacks

Man Zhang and Chong Lin

Institute of Complexity Science, College of Automation, Qingdao University, Qingdao, Shandong, People's Republic of China

ABSTRACT
In this paper, the problem of secure state estimation for cyber physical systems (CPSs) with state delay and sparse sensor attacks is studied. An algorithm combining set cover approach and adaptive switching mechanism is proposed, which can realize off-line acquisition of candidate set and accurately locate the real attack mode. The contributions of this algorithm are that it can greatly reduce the search space, eliminate the impact of attacks on state estimation, improve the estimation speed and ensure the real-time performance of state estimation under the premise of effective estimation. The sufficient condition for the existence of the observer is obtained. Finally, the rapidity and effectiveness of the designed observer are verified by two examples.

ARTICLE HISTORY
Received 16 July 2020
Accepted 6 October 2020

KEYWORDS
Cyber physical systems; state delay; sparse sensor attacks; set cover approach; adaptive switching mechanism

1. Introduction

CPSs are a class of complex interconnected systems that fully integrate the information world and the physical world. They are widely used in smart power grid, intelligent transportation, energy systems and other different fields, and have been at the heart of the latest industrial revolution (Pasqualetti et al., 2013). As a bridge connecting the control system and equipment objects, sensors play an extremely important role in CPSs. In practical applications, sensor faults and sensor attacks occur from time to time, which are very similar to each other and may affect the stable operation of the system or even lead to major disasters. But there are differences between the two concepts (Huang & Dong, 2020). Sensor faults are generally considered to be random, benign, or independent. The sensor attackers are clever, and they are targeted at the vulnerability of some of the attacked systems carefully designed. Therefore, the classical sensor fault detection and estimation methods may not be suitable for sensor attacks. Meanwhile, CPSs features, such as complex structure, large amount of data transmission and environmental uncertainty, etc. will cause some delay in systems (Fei-Sheng et al., 2019; Mahmoud et al., 2019), and the real-time performance is difficult to be guaranteed.

The characteristics of modern industrial systems, such as large-scale, connected, complex and high speed, make the systems vulnerable to sensor attacks and cause the systems to generate time-delay phenomenon. The problems of attacks on different systems have been discussed in the field of automatic control. For example, Huang and Dong (2019) investigates multiagent systems with malicious attacks, and Huang and Dong (2020) studies T-S fuzzy-model-based nonlinear systems with simultaneous stealthy sensor and actuator attacks. More importantly, secure state estimation for CPSs under sparse sensor attacks has attracted much attention of the scientific community, and many effective methods have been obtained. The present methods can be classified into three classes: (1) brute force search, (2) computationally efficient relaxation and (3) search space reduction. Brute force search, including the literatures Pasqualetti et al. (2013), Chong et al. (2015), Lu and Yang (2017) and Shoukry and Tabuada (2015), ensures the correctness of the estimate, but it takes more time to perform a thorough search on the sensors to determine the attacked sensors, and it is difficult to achieve real-time observation. In order to accelerate the estimated speed, the method of relaxing the combinatorial problem into a convex optimization is proposed. Typical studies are L_1/L_r decoder (Fawzi et al., 2014), satisfiability modulo convex programming (Shoukry, Nuzzo, Sangiovanni-Vincentelli, et al., 2017) and gradient descent algorithm (Lu & Yang, 2018; Shoukry & Tabuada, 2015). However, those studies have relatively strict requirements on system structure. The third method is search space reduction, including satisfiability modulo

CONTACT Chong Lin ✉ linchong_2004@hotmail.com

theory approach (Shoukry, Nuzzo, Puggelli, et al., 2017), set cover approach (Lu & Yang, 2019b) and constrained set partitioning approach (An & Yang, 2018b), which can reduces computational complexity by reducing the search space. The above three methods are mainly used to solve the problem of secure state estimation of CPSs modelled by discrete-time linear systems. New adaptive algorithms are proposed by Tiwari et al. (2014) and An and Yang (2018a) for real-time estimation, which are suitable for continuous-time linear systems. However, for large CPSs under attacks, the adaptive switching algorithm proposed in An and Yang (2018a) is difficult to ensure the recovery of accurate state estimation in a short time. Therefore, further efforts are needed in the study of secure state estimation for CPSs.

The rapid development of network communication lays a foundation for the real-time characteristics of CPSs, but in reality, the network bandwidth is limited, and high-frequency data transportation is easy to cause network congestion and system delay. It's well known that Krasovskii approach (Hale, 1977) and its scaling approaches (Kharitonov, 2013; Melchor-Aguilar et al., 2010; Zhang et al., 2013; Zhou, 2016) have been successfully used for the stability analysis for time-delay systems. However, there are few studies on the time-delay of CPSs. In Fei-Sheng et al. (2019), the system considers input delay, and a resilient event-triggering scheme is used to enable the system to tolerate the data loss caused by the attacks. In Cao et al. (2015), the delay caused by DoS attacks is considered. Thus, there is a large space for the study of time delay in CPSs.

Based on the above analysis, the study of secure state estimation for linear continuous-time systems with time delay is challenging. Inspired by previous studies, the security and state delay of CPSs are considered in this paper, and a new algorithm is given to ensure the correctness of state estimation and reduce the computational complexity. Moreover, the system model studied is general and it is widely applicable to practical systems, such as joint robot system (Lu & Yang, 2018), unmanned ground vehicle system (Lu & Yang, 2019a) and IEEE 6 bus power system (An & Yang, 2018a), etc. Specific contributions are as follows:

(1) A real-time secure state observer for linear continuous-time delayed CPSs under sparse sensor attacks is designed.
(2) By combining a set cover approach and a adaptive switching operator, the attacked sensors can be found quickly and the computational complexity can be reduced.
(3) Based on the generalization of the Krasovskii classical stability theorem for stability analysis of time-delay systems, the sufficient condition for the existence of the observer can be determined, and the observation error can be converged within a certain range in the case of sparse attacks and bounded noises.

2. Preliminaries

2.1. System description

Consider a class of CPSs described in time-delay linear continuous-time form as

$$\begin{aligned}\dot{x}(t) &= Ax(t) + A_d x(t-d) + Bu(t) + \psi(t),\\ y(t) &= Cx(t) + a(t) + \varphi(t), \qquad (1)\\ x(t) &= x_0, \quad t \in [-d, 0],\end{aligned}$$

where $d \geq 0$ is the time-delay constant, $x(t) \in \mathbb{R}^{n_x}$(refer to Table 1), $u(t) \in \mathbb{R}^{n_u}, y(t) \in \mathbb{R}^{n_y}, \psi(t) \in \mathbb{R}^{n_x}, \varphi(t) \in \mathbb{R}^{n_y}$, $a(t) \in \mathbb{R}^{n_y}$ are the state vector, control input, measurable output, process noise, measurement noise and attack vector, respectively. And A, A_d, B and C are known matrices with appropriate dimensions.

For $a(t) = [a_1(t), a_2(t), \dots, a_{n_y}(t)]^{\mathrm{T}}$, if $a_i(t) = 0, i \in \{1, 2, \dots, n_y\}$, sensor i is not under attack, otherwise it is. In this paper, we assume that in reality the attacker's energy is limited and the noises are bounded.

For the sake of convenience, the notations used in this paper are listed in Table 1.

In order to design a secure state observer, the following assumptions, which are frequently used in the literatures Shoukry and Tabuada (2015), An and Yang (2018a, 2018b) and Lu and Yang (2019b), are essential.

Assumption 2.1: For $t \in (0, +\infty)$, there are positive constants $\bar{a}$, $\bar{\psi}$ and $\bar{\varphi}$ that make $\|a(t)\| \leq \bar{a}$, $\|\psi(t)\| \leq \bar{\psi}$ and $\|\varphi(t)\| \leq \bar{\varphi}$ true.

Assumption 2.2: For any set Ω_{2s}, $(A, C_{\bar{\Omega}_{2s}})$ is detectable.

Assumption 2.3: Among n_y sensors, the number of sensors attacked each time is s $(2s \leq n_y)$, but which sensors

Table 1. Table of notations.

1	$\mathbb{R}^n$:	the n-dimensional Euclidean space
2	$\mathbb{RC}([-d,0], \mathbb{R}^{n_x})$:	the space of $\mathbb{R}^{n_x}$-valued continuous functions defined on $[-d, 0]$
3	$\| \bullet \|$:	the Euclidean vector norm
4	$C^s_{n_y}$:	$\frac{n_y!}{s!(n_y-s)!}$, where ! is the factorial operator
5	$\lambda_{\min}(P)$:	the minimum eigenvalue of the matrix P
6	$\mathbb{I}$:	$\{1, 2, \dots, n_y\}$
7	$\lvert\mathbb{K}\rvert$:	the number of subsets or elements in $\mathbb{K}$
8	Ω_m :	a set that satisfies $m \in \mathbb{I}, \Omega_m \subset \mathbb{I}, \lvert\Omega_m\rvert = m$
9	$\bar{\Omega}_m$:	the absolute complement of set Ω_m in set $\mathbb{I}$
10	$I_{\Omega_s} \in \mathbb{R}^{(m-s)\times n}$:	the matrix obtained from $I \in \mathbb{R}^{m\times n}$ by removing all the rows indexed by the set Ω_s
11	supp(a):	the support of vector $a \in \mathbb{R}^{n_y}$
12	$\lceil m \rceil$:	the integer not less than m
13	mod(n, m) :	the remainder of $m \setminus n$

are attacked is unknown. Before each attack, the observer can achieve the desired stability estimate. After each attack, the attack mode will remain unchanged for a certain period of time.

Remark 2.1: In An and Yang (2018a), it is assumed that the sensor set under attack is fixed. But we consider the case that the sensor attack set is variable. Thus, Assumption 2.3 is an extension and improvement of that in An and Yang (2018a). In fact, sensor attacks have a certain periodicity, and the attack energy is also limited. It is possible that the observer has implemented stability estimation before a new set of attacks appears. Therefore, Assumption 2.3 proposed in this paper is reasonable and has practical significance.

2.2. *Methods described*

The objective of this paper is to design an observer for system (1) with s-sparse sensor attacks. The desired observer satisfies that when there is no noise, the estimated state will eventually converge to the real state; when there is noise, the estimated state will eventually converge to a neighbourhood of the real state. Motivated by Lu and Yang (2019b), An and Yang (2018a) and Hale (1977), a set cover approach will be used to reduce the search space, an adaptive switching mechanism will be introduced to find the set of sensors under attacks, and the generalization of the Krasovskii classical stability theorem will be applied to determine sufficient condition for the existence of the desired observer.

Lemma 2.1 ((Lu & Yang, 2019b) (Set Cover Problem)): *For given sets* $\mathbb{K}_1 = \{\Omega_s^1, \ldots, \Omega_s^{C_{ny}^s}\}, \mathbb{K}_2 = \{\Omega_{2s}^1, \ldots, \Omega_{2s}^{C_{ny}^{2s}}\}$ *and* $\mathbb{K}_2^{\Omega_{2s}} = \{\Omega_s^{(\Omega_{2s},1)}, \ldots, \Omega_s^{(\Omega_{2s},C_{2s}^s)}\}$, *where* $|\mathbb{K}_1| = C_{n_y}^s$, $|\mathbb{K}_2| = C_{n_y}^{2s}$, $|\mathbb{K}_2^{\Omega_{2s}}| = C_{2s}^s$ *and* $\Omega_s^{(\Omega_{2s},i)} \in \{\hat{\Omega}_s \subset \Omega_{2s} || \hat{\Omega}| = s\}, i \in \{1, 2, \ldots, C_{2s}^s\}$, *there is at least one set* $\mathbb{G}_0 \subset \mathbb{K}_2$ *that satisfies*

$$\bigcup_{\Omega_{2s} \in \mathbb{G}_0} \mathbb{K}_2^{\Omega_{2s}} = \mathbb{K}_1. \tag{2}$$

Remark 2.2: There are always more than one $\mathbb{G}_0$ that satisfy condition (2), so the minimum-size set $\mathbb{G}_0$ will be chosen as the candidate set $\mathbb{S}$.

In practice, the set cover problem can be approximated by greedy algorithm, the details are shown in Table 2.

We assume that $\mathbb{S} = \{\Omega_{2s}^2, \ldots, \Omega_{2s}^{\theta+1}\}$, where $|\Omega_{2s}^i| = 2s, i = \{2, 3, \ldots, \theta + 1\}$. In addition, Ω_{2s}^1 is used to indicate the case that no sensor has been attacked, so $\Omega_{2s}^1 = \emptyset$. For $\zeta \in \{1, 2, \ldots, \theta + 1\}$, the ζth sensor attack mode is represented by Ω_{2s}^{ζ} in this paper.

Table 2. Greedy algorithm.

```
step 1: set $\mathbb{S} = \emptyset, \tilde{\mathbb{K}}_2^{\Omega_{2s}} = \mathbb{K}_2^{\Omega_{2s}}$ for all $\Omega_{2s} \in \mathbb{K}_2$;
step 2: while $\bigcup_{\Omega_{2s} \in \mathbb{S}} \mathbb{K}_2^{\Omega_{2s}} \neq \mathbb{K}_1$ do
    reset $\hat{\Omega} = \arg\max_{\Omega_{2s}} |\tilde{\mathbb{K}}_2^{\Omega_{2s}}|, \mathbb{S} = \mathbb{S} \cup \{\hat{\Omega}\}$;
    reset $\tilde{\mathbb{K}}_2^{\Omega_{2s}} = \tilde{\mathbb{K}}_2^{\Omega_{2s}} \setminus \tilde{\mathbb{K}}_2^{\hat{\Omega}}$ for all $\Omega_{2s} \in \mathbb{K}_2$;
step 3: return $\mathbb{S}$
```

Remark 2.3: In Chong et al. (2015), the number of candidates is $C_{n_y}^s + C_{n_y}^{2s}$ for each time step with a switched Luenberger observer. While it has been reduced to $C_{n_y}^s$ with a novel adaptive switching mechanism in An and Yang (2018a). In this paper, the number of candidates will be reduced to less than $C_{n_y}^s/2$ with the help of set cover approach, greatly reducing the search space.

Corresponding to the ζth sensor attack mode Ω_{2s}^{ζ}, we define its switching function matrix as $J_\zeta = \text{diag}\{j_1(\zeta), \ldots, j_{n_y}(\zeta)\}$, where $j_i(\zeta) = \begin{cases} 0, & i \in \Omega_{2s}^{\zeta} \\ 1, & i \notin \Omega_{2s}^{\zeta} \end{cases}$, $i = 1, 2, \ldots, n_y$. Corresponding to the candidate sensor attack modes, the set of switching function matrices is defined as $\mathcal{J} = \{J_1, J_2, \ldots, J_{\theta+1}\}$.

It's easy to prove that when $\text{supp}(a(t)) = \Omega_{2s}^{\zeta}, J_\zeta a(t) = 0$. Therefore, the observer is designed as

$$\begin{aligned} \dot{\hat{x}}(t) &= A\hat{x}(t) + A_d\hat{x}(t-d) + Bu(t) + L_\zeta J_\zeta (y(t) - \hat{y}(t)), \\ \hat{y}(t) &= C\hat{x}(t), \end{aligned} \tag{3}$$

where $\hat{x}$ and $\hat{y}$ are estimates of the state and output of the system (1), $L_\zeta, \zeta \in \{1, 2, \ldots, \theta + 1\}$ are the observer gains.

According to (1) and (3), the observation error system is shown as

$$\begin{aligned} \dot{e}(t) &= \bar{A}e(t) + A_d e(t-d) + \phi(t) - L_\zeta J_\zeta a(t), \\ e_y(t) &= J_\zeta C e(t) + J_\zeta a(t) + J_\zeta \varphi(t), \end{aligned} \tag{4}$$

where $\bar{A} = A - L_\zeta J_\zeta C$, $\phi(t) = \psi(t) - L_\zeta J_\zeta \varphi(t)$, $e_y(t) = J_\zeta(y(t) - \hat{y}(t))$. It's easy to prove that there is a positive number $\bar{\phi}$ such that $\|\phi(t)\| \leq \bar{\phi}$, for $t \in (0, +\infty)$.

Next, we will focus on designing an adaptive switching mechanism, which can achieve the following goals: (1) If any sensor is attacked, the switching mechanism will be triggered; (2) If any sensor is attacked, the switching function will automatically vary from J_1 to $J_{\theta+1}$, until locating the proper entry mode; (3) If the real attack mode does not change, the observer will continue to operate in the proper entry mode, otherwise a new switch will begin. Therefore, an observed performance index $\hbar$ and a switching logic $\zeta(\hbar)$ will be introduced to assist in achieving the above objectives, which are specified as

$$\dot{\hbar}(t) = \mu \mathcal{N}_\sigma^2(e_y(t)) = \begin{cases} 0, & \|e_y(t)\| \leq \sigma, \\ \mu(\|e_y(t)\| - \sigma)^2, & \|e_y(t)\| > \sigma, \end{cases} \tag{5}$$

where μ and σ are constants to be designed, and

$$\zeta(\hbar) = \lceil \mathrm{mod}(\hbar, \theta + 1) \rceil. \tag{6}$$

And finally, the Krasovskii classical stability theorem will be given in Lemma 7.

Lemma 2.2 (Krasovskii Theorem, Th.2.1 in Hale (1977)): *The system (4) is globally uniformly asymptotically stable if there exist a continuous functional $V(t,z), t \in (0,\infty), z \in \mathbb{RC}([-d,0],\mathbb{R}^{n_x})$, and three $\mathcal{K}_\infty$-functions u, v, w such that the following two conditions are met for all $t \in (0,\infty)$:*

$$\begin{aligned} &u(|z(0)|) \le V(t,z) \le v(\|z\|), \quad z \in \mathbb{RC}([-d,0],\mathbb{R}^{n_x}), \\ &\dot{V}(t,e_t) \le -w(|e(t)|). \end{aligned} \tag{7}$$

3. Main results

Inspired by the Theorem 1 in Zhou (2016) and the Theorem 3 in Zhou and Egorov (2016), the sufficient condition for the existence of the desired observer will be given in this section.

Theorem 3.1: *For system* (1) *and its observer* (3), *under Assumptions 2.1–2.3, consider $\zeta, \zeta^{\divideontimes} \in \{1,2,\ldots,\theta+1\}$ and $\zeta^{\divideontimes} \neq 1$, $\zeta \neq \zeta^{\divideontimes}$. If there exist positive definite matrices P_ζ, U, a matrix N_ζ and positive constants η, $0 < p_1 \le p_2$ and $\rho \in (0,1)$ such that*

$$\begin{bmatrix} \begin{matrix} A^TP_\zeta + P_\zeta A - C^TJ_\zeta N_\zeta^T \\ -N_\zeta J_\zeta C - \alpha P_\zeta \end{matrix} & * & * & * \\ -UT_{\zeta\divideontimes}^T J_\zeta C + T_{\zeta\divideontimes}^T J_\zeta N_\zeta^T & -2U & * & * \\ P_\zeta & 0 & -\eta I & * \\ 0 & T_{\zeta\divideontimes}U & 0 & -\eta I \end{bmatrix} < 0 \tag{8}$$

$$p_1 I_{n_x} \le P_\zeta \le p_2 I_{n_x} \tag{9}$$

$$\eta \triangleq \frac{\rho - 1}{d} - \alpha \ge 0 \tag{10}$$

hold, where $T_{\zeta\divideontimes} = I^T_{\bar{\Omega}_{2s}^{\zeta\divideontimes}}$ and the adjustable parameter $\alpha < 0$, the state estimate error $e(t)$ in (4) will satisfy $\lim_{t\to\infty}\|e(t)\| \le \delta$, *with* $\delta = \sqrt{-\eta\frac{\sigma^2+\bar{\phi}^2+\bar{\varphi}^2}{\gamma p_1}}$, $\sigma = \|C\|$ $(-\gamma p_1)^{-1/2}\eta^{1/2}\bar{\phi} + \bar{\varphi}$, *and* $\gamma \triangleq \alpha + \eta + \frac{p_2}{\rho\eta p_1}\|A_d\|^2 < 0$. *In this design, the observer gains are selected as*

$$L_\zeta = P_\zeta^{-1} N_\zeta. \tag{11}$$

Proof: Choose the Lyapunov–Krasovskii functional $V(t)$ similar to that in Zhou and Egorov (2016):

$$\begin{aligned} &V(t) = V_1(t) + V_2(t), \quad V_1(t) = e^T(t)P_\zeta e(t), \\ &V_2(t) = \int_{t-d}^{t} f(t,\iota)\|A_d e(\iota)\|^2 \,\mathrm{d}\iota, \end{aligned} \tag{12}$$

where $f(t,\iota) = g_2 + \frac{\iota - t}{d}(g_2 - g_1)$ with the real numbers $g_1 \ge 0$ and $g_2 \ge 0$.

It can be easily obtained as

$$\|e(t)\| \le p_1^{-1/2} V(t)^{1/2}. \tag{13}$$

Suppose the $\zeta^\star$th attack mode is launched at time t_0. For time $t (t > t_0)$, there are two cases: whether or not the switching function can be switched to the correct entry mode, as described below.

Case 1. Suppose at time $t^\star (t^\star > t_0)$, the switching function matrix is $J_{\zeta^\star}$, and $J_{\zeta^\star} a = 0$. That is to say that the switching function locates the proper entry mode at time $t^\star$. In this case, the value of σ will be determined.

Based on the conditions (8) –(10), we define the parameters $g_1 = \frac{p_2}{\eta}$ and $g_2 = \frac{p_2}{\rho\eta}$, the derivative of the Lypaunov–Krasovskii functional (12) along with system (4) is calculated as

$$\begin{aligned} \dot{V}_1(t) &= e^T(t)(\bar{A}^T P_\zeta + P_\zeta \bar{A})e(t) + 2e^T(t)P_\zeta A_d e(t-d) \\ &\quad + 2e^T(t)P_\zeta \phi(t) \\ &\le (\alpha + \eta)V_1(t) + \eta\phi^T(t)\phi(t) + g_1\|A_d e(t-d)\|^2, \\ \dot{V}_2(t) &= g_2\|A_d e(t)\|^2 - g_1\|A_d e(t-d)\|^2 \\ &\quad - \int_{t-d}^{t} \frac{1}{d}(g_2 - g_1)\|A_d e(\iota)\|^2 \,\mathrm{d}\iota, \\ \dot{V}(t) &= \dot{V}_1(t) + \dot{V}_2(t) \\ &\le \gamma V(t) + \eta\phi^T(t)\phi(t) - \int_{t-d}^{t} q(t,\iota)\|A_d e(\iota)\|^2 \,\mathrm{d}\iota, \end{aligned} \tag{14}$$

where

$$q(t,\iota) = \gamma f(t,\iota) + \frac{1}{d}(g_2 - g_1).$$

For $\iota \in [t-d, t)$, one gets

$$\begin{aligned} q(t,\iota) &\ge (\alpha + \eta)\left[g_2 + \frac{\iota - t}{d}(g_2 - g_1)\right] + \frac{1}{d}(g_2 - g_1) \\ &\ge (\alpha + \eta)g_2 + \frac{1}{d}(g_2 - g_1) \\ &= 0. \end{aligned}$$

Therefore,

$$\dot{V}(t) \le \gamma V(t) + \eta\bar{\phi}^2. \tag{15}$$

Solving Equation (15), one has

$$\begin{aligned} V(t) &\le \left[V(t^\star) + \frac{\eta\bar{\phi}^2}{\gamma}\right] \mathrm{e}^{\gamma(t - t^\star)} - \frac{\eta\bar{\phi}^2}{\gamma} \\ &\le V(t^\star)\,\mathrm{e}^{\gamma(t - t^\star)} - \frac{\eta\bar{\phi}^2}{\gamma}. \end{aligned} \tag{16}$$

Then

$$\begin{aligned}\|e_y(t)\| &\le \|C\|\|e(t)| + \|\varphi(t)\| \\ &\le \|C\|p_1^{-1/2}V^{1/2}(t^\star)\,\mathrm{e}^{\gamma(t-t^\star)/2} + \sigma,\end{aligned} \tag{17}$$

where $\sigma = \|C\|(-\gamma p_1)^{-1/2}\eta^{1/2}\bar\phi + \bar\varphi$. If $\|e_y(t)\| > \sigma$, it can be known that

$$\begin{aligned}\dot\hbar(t) &= \mu\mathcal{N}_\sigma^2(e_y(t)) \\ &= \mu\|C\|^2 p_1^{-1}V(t^\star)\,\mathrm{e}^{\gamma(t-t^\star)}.\end{aligned} \tag{18}$$

It is easy to prove that $\lim_{t\to\infty}\dot\hbar(t) = 0$, so $\hbar(t)$ will converge to a positive scalar for $t\to\infty$.

Case 2. Suppose at time $t^\times\,(t_0 < t^\times < t^\star)$, the switching function matrix is $J_{\zeta^\times}$, and $J_{\zeta^\times}a \neq 0$. That is to say that the switching function locates the wrong entry mode at time $t^\times$. We will prove that the estimated error eventually converges to 0 when there is no noise.

In this case, if $\int_{t^\times}^{+\infty}\dot\hbar(\iota)\,\mathrm{d}\iota \le 1$ is no longer satisfied, ζ will be driven to switch to the next integer, until the correct attack mode is located at time $t^\star$, then $\int_{t^\star}^{+\infty}\dot\hbar(\iota)\,\mathrm{d}\iota \le 1$ will be satisfied.

For $(t_0 \le t^\times < t^\star)$, one gets

$$\begin{aligned}\dot V(t^\times) &= e^T(t^\times)[\bar A^T P_{\zeta^\times} + P_{\zeta^\times}\bar A]e(t^\times) \qquad (1)\\ &\quad - 2e^T(t^\times)P_{\zeta^\times}L_{\zeta^\times}J_{\zeta^\times}a(t^\times) \\ &\quad + 2e^T(t^\times)P_{\zeta^\times}A_d e(t^\times - d) + 2e^T(t^\times)P_{\zeta^\times}\phi(t^\times) \\ &\quad + g_2\|A_d e(t^\times)\|^2 - g_1\|A_d e(t^\times - d)\|^2 \qquad (2)\\ &\quad - \int_{t^\times - d}^{t^\times}\frac{1}{d}(g_2 - g_1)\|A_d e(\iota)\|^2\,\mathrm{d}\iota \\ &\le \gamma V(t^\times) + \eta\bar\phi^2 + 2e^T(t^\times)P_{\zeta^\times}L_{\zeta^\times}J_{\zeta^\times}a(t^\times).\end{aligned} \tag{19}$$

Take $\lambda_{JL} = \max\{\|J_{\zeta^\times}L_{\zeta^\times}^T P_{\zeta^\times}L_{\zeta^\times}J_{\zeta^\times}\|, \zeta^\times = 1, 2, \ldots, \theta+1\}$, to obtain

$$2e^T(t^\times)P_{\zeta^\times}L_{\zeta^\times}J_{\zeta^\times}a(t^\times) \le -\frac{\gamma}{2}e^T(t^\times)P_{\zeta^\times}e(t^\times) - \frac{2}{\gamma}\lambda_{JL}\bar a^2. \tag{20}$$

Combine (19) and (20) gets

$$\dot V(t^\times) \le \frac{\gamma}{2}V(t^\times) + \eta\bar\phi^2 - \frac{2}{\gamma}\lambda_{JL}\bar a^2. \tag{21}$$

Then

$$V(t^\star) \le \mathrm{e}^{(\gamma/2)(t^\star - t_0)}V(t_0) - \frac{2\eta\bar\phi^2}{\gamma} + \frac{4\lambda_{JL}\bar a^2}{\gamma^2}. \tag{22}$$

Based on (18) and (22), one has

$$\begin{aligned}\dot\hbar(t) &= \mu\|C\|^2 p_1^{-1} \\ &\quad\times\left[\mathrm{e}^{(\gamma/2)(t^\star - t_0)}V(t_0) - \frac{2\eta\bar\phi^2}{\gamma} + \frac{4\lambda_{JL}\bar a^2}{\gamma^2}\right]\mathrm{e}^{\gamma(t-t^\star)}.\end{aligned} \tag{23}$$

Then

$$\begin{aligned}\int_{t^\star}^{+\infty}\dot\hbar(\iota)\,\mathrm{d}\iota &\le -\frac{\mu\|C\|^2}{\gamma p_1} \\ &\quad\left[\mathrm{e}^{(\gamma/2)(t^\star - t_0)}V(t_0) - \frac{2\eta\bar\phi^2}{\gamma} + \frac{4\lambda_{JL}\bar a^2}{\gamma^2}\right].\end{aligned} \tag{24}$$

Introduce a variable $\mathcal{M}$ and assign it to

$$\mathcal{M} = -\frac{\|C\|^2}{\gamma p_1}\left[\mathrm{e}^{(\gamma/2)(t^\star - t_0)}V(t_0) - \frac{2\eta\bar\phi^2}{\gamma} + \frac{4\lambda_{JL}\bar a^2}{\gamma^2}\right]. \tag{25}$$

At the same time, in order to ensure that $\mu\mathcal{M} \le 1$, μ should be assigned to

$$\mu = \frac{-\gamma^3 p_1}{\|C\|^2[\gamma^2\kappa - 2\gamma\eta\bar\phi^2 + 4\lambda_{JL}\bar a^2]}, \tag{26}$$

where κ is a designed parameter that satisfies $\mathrm{e}^{(\gamma/2)(t^\star - t_0)}V(t_0) < \kappa$ for a sufficiently big $t^\star$.

Through the analysis of the two cases above, it can be known that there must exist a sufficiently big $t^\star$ such that $\int_{t^\star}^{+\infty}\dot\hbar(\iota)\,\mathrm{d}\iota \le 1$. At the same time, according to Equation (18), it can be deduced that $\lim_{t\to\infty}\mathcal{N}_\sigma^2(e_y(t)) = 0$, which means $\lim_{t\to\infty}\|e_y(t)\| \le \sigma$. In addition, when $\psi(t) = 0$, $\varphi(t) = 0$, we have $\sigma = 0$, $\lim_{t\to\infty}\|e_y(t)\| = 0$ and $\lim_{t\to\infty}\|e(t)\| = 0$.

Finally, the boundary value of $e(t)$ in the presence of noises is studied. Inspired by An and Yang (2020), the system (4) is reconstructed as an augmented system.

$$\tilde E\dot\chi(t) = \tilde A_{JJ*}\chi(t) + \tilde B e_y(t) + \Phi(t), \tag{27}$$

where $\chi(t) = [e^T(t), e^T(t-d), (T_{\zeta*}^T J_\zeta a(t))^T]^{\mathrm{T}}$, $\Phi(t) = [\phi^T(t), 0, -(T_{\zeta*}^T J_\zeta\varphi(t))^T]^{\mathrm{T}}$,

$$\tilde B = \begin{bmatrix}0\\0\\T_{\zeta*}^T\end{bmatrix},$$

$$\tilde A_{JJ*} = \begin{bmatrix}A - L_\zeta J_\zeta C & A_d & L_\zeta J_\zeta T_{\zeta*}\\ 0 & 0 & 0\\ -T_{\zeta*}^T J_\zeta C & 0 & -I_{2s}\end{bmatrix},$$

$$\tilde E = \begin{bmatrix}I & 0 & 0\\0 & 0 & 0\\0 & 0 & 0\end{bmatrix}.$$

Based on the Lyapunov–Krasovskii functional (12), it is calculated that

$$e^T(t)P_\zeta e(t) = \chi^T(t)\tilde E\tilde P_\zeta\chi(t), \quad \text{where } \tilde P_\zeta = \mathrm{diag}\{P_\zeta, U, U\};$$

$$\int_{t-d}^{t} f(t,\iota)\|A_d e(\iota)\|^2\,\mathrm{d}\iota = \int_{t-d}^{t} f(t,\iota)\|A_d\tilde E\chi(\iota)\|^2\,\mathrm{d}\iota.$$

Thus, the Lyapunov–Krasovskii functional (12) can be reconstructed as

$$\tilde{V}(t) = \chi^T(t)\tilde{E}\tilde{P}_\zeta \chi(t) + \int_{t-d}^{t} f(t,\iota)\|A_d\tilde{E}\chi(\iota)\|^2 \,\mathrm{d}\iota. \quad (28)$$

Similar to inequality (15), the derivative of the Lypaunov –Krasovskii functional (28) along with system (27) is as follows

$$\begin{aligned}\dot{V}(t) = \dot{\tilde{V}}(t) &= 2\chi^T(t)\tilde{P}_\zeta[\tilde{A}_{JJ*}\chi(t) + \tilde{B}e_y(t) + \Phi(t)] \\ &\quad - g_1\|A_d\tilde{E}\chi(t-d)\|^2 + g_2\|A_d\tilde{E}\chi(t)\|^2 \\ &\quad - \int_{t-d}^{t}\frac{1}{d}(g_2-g_1)\|A_d e(\iota)\|^2 \,\mathrm{d}\iota \\ &\le \gamma V(t) + \eta\|e_y(t)\|^2 + \eta(\bar{\varphi}^2 + \bar{\phi}^2). \quad (29)\end{aligned}$$

Based on the fact of $\lim_{t\to\infty}\|e_y(t)\| \le \sigma$, we have $\lim_{t\to\infty} V(t) \le -\eta\frac{\sigma^2+\bar{\varphi}^2+\bar{\phi}^2}{\gamma}$, and hence $\lim_{t\to\infty}\|e(t)\| \le \delta$, where $\delta = \sqrt{-\eta\frac{\sigma^2+\bar{\phi}^2+\bar{\varphi}^2}{\gamma p_1}}$. ■

Remark 3.1: In condition (8), there are θ^2 LMIs. In each LMI of (8), there are three unknown matrices P_ζ, U and N_ζ, in which the variables are, respectively, $\frac{n_x(1+n_x)}{2}$, $s(1+2s)$ and $n_x \times p$. The structure is simple and the calculation difficulty is low.

Remark 3.2: In the study of this paper, we need to determine a condition so that the designed functional satisfies the form $\dot{V}(t) \le aV(t) + b$, where $a<0$, $b>0$. Through research, we find that traditional Lyapunov functional methods, such as Liu et al. (2017) and Zhang et al. (2004), are difficult to obtain a feasible solution when applied to the system (1). In order to overcome this difficulty, a new Lyapunov–Krasovskii functional (12) is constructed in this paper, and the useful forms (15), (21) and (29) can be obtained through condition (8).

Remark 3.3: In the literature, most researches in solving security problems for CPSs adopt the method of analyzing the information in a finite length time window (Chong et al., 2015; Lu & Yang, 2017; Pajic et al., 2017; Shoukry, Nuzzo, Puggelli, et al., 2017). In the above methods, the state estimates obtained at time t are the estimated states of the actual system at time $t-\tau+1$ (τ is the window length), and the completion of each estimate requires processing of data at τ moments. So it is difficult to guarantee the real-time performance. In this paper, a new state observer is designed based on the set cover approach and adaptive switching mechanism. For each estimate, only the data at the current moment need to be processed. By using the greedy algorithm in Table 2 and solving a set of LMIs (8) , and computing an adaptive law (5) and (6) online, the designed observer has the ability to quickly identify attacks and locate the appropriate sensor attack mode. Therefore, the computation

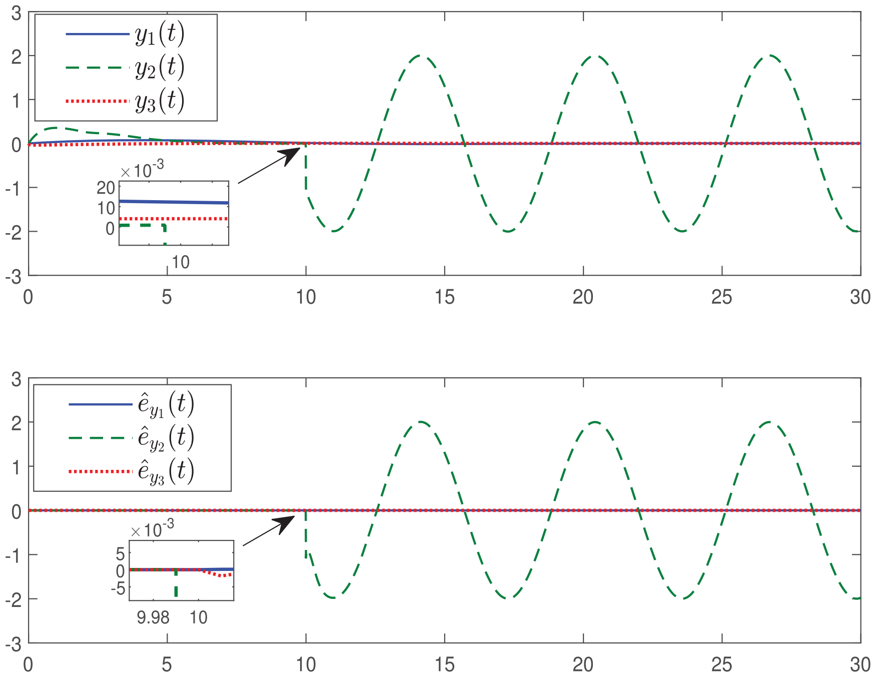


Figure 1. The system outputs and the errors.

burden is reduced and the real-time performance is guaranteed.

4. Simulation examples

In this section, two examples will be presented to verify the effectiveness and rapidity of the designed observer. The simulations are executed by using MATLAB on a desktop equipped with an Intel Core i7-6700 processor operating at 3.4 GHz and 16 GB of memory.

In Example 4.1, the effectiveness of the designed observer for system (1) will be tested. The IEEE 6 bus power system modified from Ao et al. (2016) is considered.

Example 4.1: Consider the system given by

$$\begin{bmatrix}\dot{\delta}(t)\\ \dot{w}(t)\end{bmatrix} = A\begin{bmatrix}\delta(t)\\ w(t)\end{bmatrix} + A_d\begin{bmatrix}\delta(t-d)\\ w(t-d)\end{bmatrix} + Bu(t) + \psi(t),$$

$$y(t) = C\begin{bmatrix}\dot{\delta}(t)\\ \dot{w}(t)\end{bmatrix} + a(t) + \phi(t), \tag{30}$$

where the input of the system is $u(t) = P_w(t) - L_{g1}L_{11}^{-1} P_\theta(t)$. $P_w(t) = [P_{w1}, P_{w2}, P_{w3}]^{\mathrm{T}}$ and $P_\theta(t) = [P_{\theta 1}, P_{\theta 2}, P_{\theta 3}, P_{\theta 4}, P_{\theta 5}, P_{\theta 6}]^{\mathrm{T}}$ describe the input power from generators

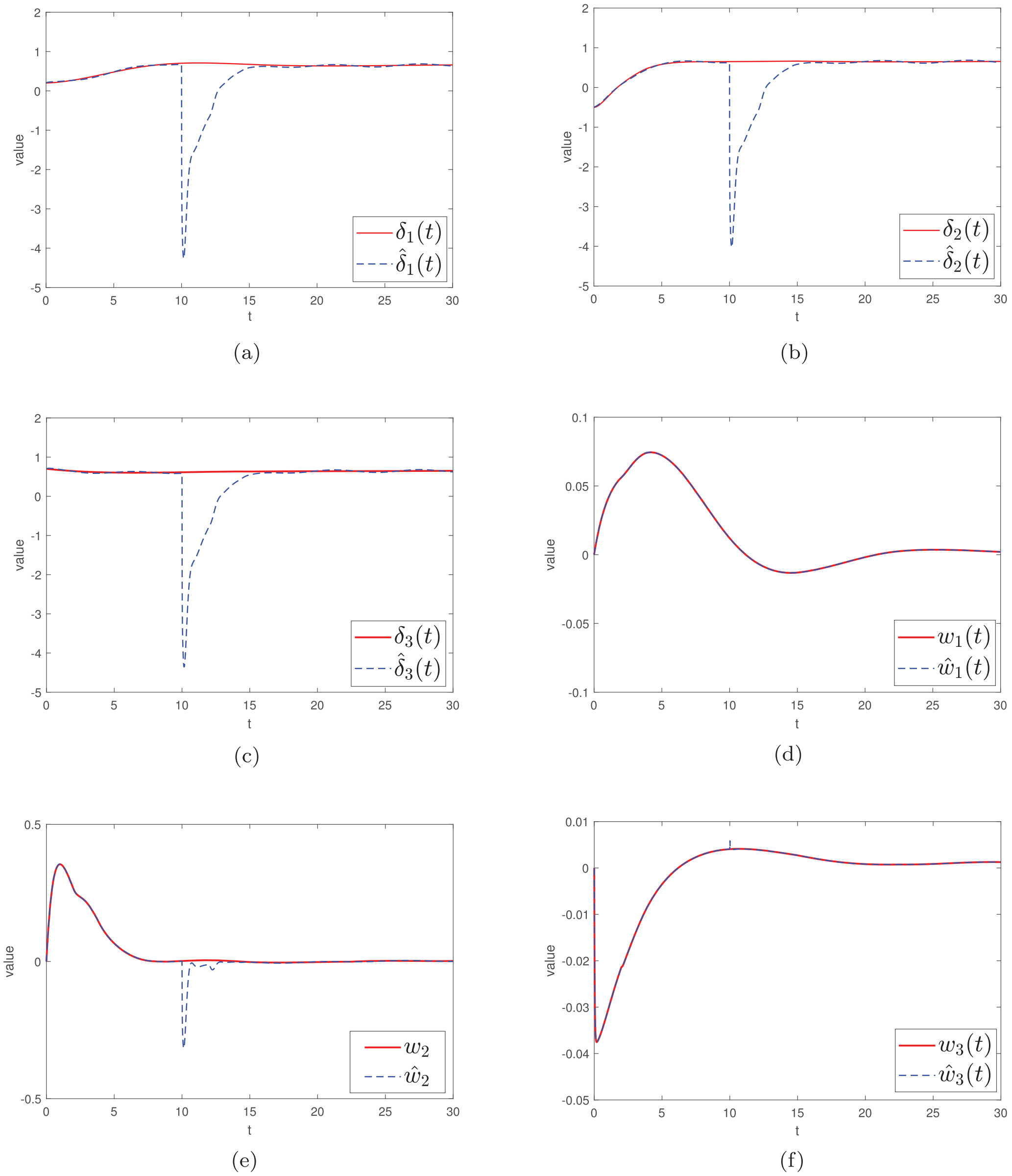
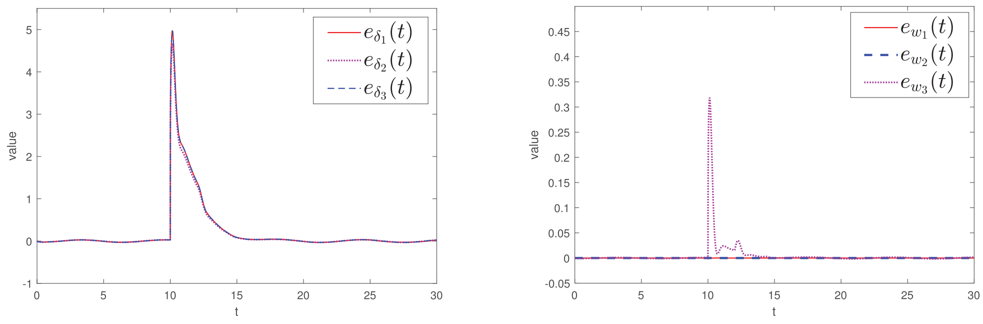


Figure 2. The system states and their estimations. (a) $\delta_1(t)$ and its estimation $\hat{\delta}_1(t)$. (b) $\delta_2(t)$ and its estimation $\hat{\delta}_2(t)$. (c) $\delta_3(t)$ and its estimation $\hat{\delta}_3(t)$. (d) $w_1(t)$ and its estimation $\hat{w}_1(t)$. (e) $w_2(t)$ and its estimation $\hat{w}_2(t)$. (f) $w_3(t)$ and its estimation $\hat{w}_3(t)$.



(a) (b)

Figure 3. The estimation errors of the system states. (a) The estimation errors $e_{\delta_1}(t), e_{\delta_2}(t)$ and $e_{\delta_3}(t)$. (b) The estimation errors $e_{w_1}(t), e_{w_2}(t)$ and $e_{w_3}(t)$.

and the actual power required by load. The generator rotor angles and frequencies are written as $\delta(t) = [\delta_1(t), \delta_2(t), \delta_3(t)]^{\mathrm{T}}$ and $w(t) = [w_1(t), w_2(t), w_3(t)]^{\mathrm{T}}$, respectively. At the same time, the matrices A, B, A_d and C are described as

$$A = \begin{bmatrix} 0 & I_3 \\ M_g^{-1}(L_{g1}L_{11}^{-1}L_{1g}) & -M_g^{-1}D_g \end{bmatrix}, \quad B = [0 \quad M_g^{-1}]^{\mathrm{T}},$$

$$A_d = \mathrm{diag}\{0_3, 0.5I_3\}, \quad C = [0_3 \quad I_3],$$

where the matrices set to $M_g = \mathrm{diag}\{0.125, 0.034, 0.016\}$ and $D_g = \mathrm{diag}\{0.125, 0.068, 0.048\}$ are generator inertial and damping coefficients. L_{gg}, L_{g1}, $L_{1g} = L_{g1}^T$ and L_{11} are set as the network susceptance matrices, assigned as

$$L_{gg} = \mathrm{diag}\{0.058, 0.063, 0.059\}, \quad L_{g1} = [-L_{gg}, 0_3],$$

$$L_{11} = \begin{bmatrix} 0.235 & 0 & -0.085 & 0 & -0.092 & 0 \\ 0 & 0.296 & 0 & -0.161 & 0 & -0.072 \\ 0 & 0 & 0.329 & 0 & -0.170 & -0.101 \\ -0.085 & -0.161 & 0 & 0.246 & 0 & 0 \\ -0.092 & 0 & -0.170 & 0 & 0.262 & 0 \\ 0 & -0.072 & -0.101 & 0 & 0 & 0.173 \end{bmatrix}.$$

In the test, $x_0 = [0.2, -0.5, 0.7, 0, 0, 0]^{\mathrm{T}}$ is the initial state condition, $\psi(t) = 0.02\sin(t)$ and $\varphi(t) = 0.01\cos(t)$ are the noises. Considering that only the second sensor of the three sensors is attacked at 10 seconds and remains unchanged, thus the attack vector is set as $a(t) = [0, 2\sin(t), 0]^{\mathrm{T}}$. Based on the greedy algorithm in Table 2, the candidate set is obtained as $\mathbb{S} = \{\{1,2\}, \{2,3\}\}$, then the set of corresponding switching matrices is $\mathcal{J} = \{j_1, j_2, j_3\} = \{\mathrm{diag}\{1,1,1\}, \mathrm{diag}\{0,0,1\}, \mathrm{diag}\{1,0,0\}\}$, and the index set is $\{1,2,3\}$. In addition, the designed parameters are set as $\alpha = -2.5$, $\eta = 2$, $d = 1$.

The sensor attack status can be shown in Figure 1, the values of $y_2(t)$ and $\hat{e}_{y_2}(t)$ ($\hat{e}_{y_i}(t) = y_i(t) - \hat{y}_i(t), i \in \{1,2,3\}$) are affected by the attacks, and their trajectories are seriously deviated from the original trajectories. This phenomenon poses a challenge to state estimation.

However, it can be seen from Figures 2 and 3 ($e_v(t) = v(t) - \hat{v}(t), v \in \{\delta_i, w_j\}, i, j \in \{1,2,3\}$) that there is a short period of large estimation errors in states $\delta_1(t), \delta_2(t), \delta_3(t)$ and $w_2(t)$ from the 10 s. The estimation errors recover to around zero at a fast speed, and the estimated values approximate the real state values. That's because starting at 10 seconds, the original entry mode is no longer correct, so switch is triggered until the index ζ is switched to 2. Since there is no change in attack mode for the rest of the period, the switch index remains at 2. In addition, if the attacked sensors of the system (30) change after 15 seconds, the observer system will repeat the above process. It can be seen from the above analysis that the observer designed in this paper can guarantee the secure state estimation.

Next, we will consider the system (1) without the time-delay term.

Example 4.2: Consider the system (1) with $A_d = 0$, where the matrices A, B and C are randomly generated with appropriate dimensions, $\psi(t) = 0.1\sin(t)$, $\varphi(t) = 0.2\cos(t)$, $n_x = 10$, $n_y = 5$, $s = 2$. The sampling time is 10, 15, 20, 25 and 30, respectively.

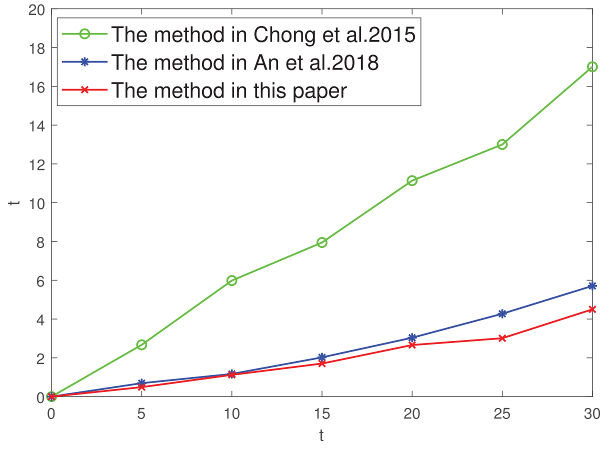


Figure 4. The comparisons of the execution times of the three methods.

For this example, three algorithms from Chong et al. (2015), An and Yang (2018a), and this paper are compared. The comparisons of execution times are shown in Figure 4. It can be seen that the algorithm designed in this paper has a shorter execution time. Especially, it has further advantage in execution speed when the sampling time is longer.

5. Conclusion

In this paper, a secure state observer is designed for CPSs with s-sparse sensor attacks modelled by time-delay linear continuous-time systems. An algorithm combining adaptive switching mechanism and set cover approach is proposed, which ensures the correct identification of attack modes and improves the state estimation speed. And two examples are given to verify the effectiveness and practicability of the designed observer. Finally, in CPSs, there is still room for research on the secure state estimation and control of actuator attacks systems as well as extensions to T-S fuzzy-model-based nonlinear systems (Li et al., 2020; Tong & Li, 2010; Tong et al., 2020). These interesting topics will be our future research.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported in part by the National Natural Science Foundation of China under [grant numbers 61673227 and 61873137]; the Taishan Scholar Project of Shandong Province of China.

References

An, L., & Yang, G. H. (2018a). Secure state estimation against sparse sensor attacks with adaptive switching mechanism. *IEEE Transactions on Automatic Control*, *63*(8), 2596–2603. https://doi.org/10.1109/TAC.2017.2766759.

An, L., & Yang, G. H. (2018b). State estimation under sparse sensor attacks: A constrained set partitioning approach. *IEEE Transactions on Automatic Control*, *64*(9), 3861–3868. https://doi.org/10.1109/TAC.2018.2885063.

An, L., & Yang, G. H. (2020). Supervisory nonlinear state observers for adversarial sparse attacks. *IEEE Transactions on Cybernetics*, (99), 1–13. https://doi.org/10.1109/TCYB.6221036

Ao, W., Song, Y., & Wen, C. (2016). Adaptive cyber-physical system attack detection and reconstruction with application to power systems. *IET Control Theory & Applications*, *10*(12), 1458–1468. https://doi.org/10.1049/iet-cta.2015.1147

Cao, R., Wu, J., Long, C., & Li, S. (2015). Stability analysis for networked control systems under denial-of-service attacks. In *2015 54th IEEE conference on decision and control* (pp. 7476–7481). Osaka, Japan.

Chong, M. S., Wakaiki, M., & Hespanha, J. P. (2015). Observability of linear systems under adversarial attacks. In *2015 American control conference* (pp. 2439–2444). Chicago, IL, USA.

Fawzi, H., Tabuada, P., & Diggavi, S. (2014). Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, *59*(6), 1454–1467. https://doi.org/10.1109/TAC.2014.2303233

Fei-Sheng, Y., Jing, W., Quan, P., & Pei-Pei, K. (2019). Resilient event-triggered control of grid cyber-physical systems against cyber attack. *Acta Automatica Sinica*, *45*(1), 110–119. https://doi.org/10.16383/j.aas.c180388

Hale, J. (1977). *Theory of functional differential equation*. Springer-Verlag.

Huang, X., & Dong, J. (2019). Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 89–99. https://doi.org/10.1109/TSMC.6221021

Huang, X., & Dong, J. (2020). An adaptive secure control scheme for TS fuzzy systems against simultaneous stealthy sensor and actuator attacks. *IEEE Transactions on Fuzzy Systems*. https://doi.org/10.1109/T-FUZZ.2020.2990772

Kharitonov, V. (2013). *Time-delay systems: Lyapunov functionals and matrices*. Birkhäuser.

Li, Y., Qu, F., & Tong, S. (2020). Observer-based fuzzy adaptive finite-time containment control of nonlinear multiagent systems with input delay. *IEEE Transactions on Cybernetics*. https://doi.org/10.1109/TCYB.2020.2970454

Liu, K., Seuret, A., & Xia, Y. (2017). Stability analysis of systems with time-varying delays via the second-order bessel –Legendre inequality. *Automatica*, *76*, 138–142. https://doi.org/10.1016/j.automatica.2016.11.001

Lu, A. Y., & Yang, G. H. (2017). Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer. *Information Sciences*, *417*, 454–464. https://doi.org/10.1016/j.ins.2017.07.029

Lu, A. Y., & Yang, G. H. (2018). Secure Luenberger-like observers for cyber-physical systems under sparse actuator and sensor attacks. *Automatica*, *98*, 124–129. https://doi.org/10.1016/j.automatica.2018.09.003

Lu, A. Y., & Yang, G. H. (2019a). Switched projected gradient descent algorithms for secure state estimation under sparse sensor attacks. *Automatica*, *103*, 503–514. https://doi.org/10.1016/j.automatica.2019.02.016.

Lu, A. Y., & Yang, G. H. (2019b). Secure switched observers for cyber-physical systems under sparse sensor attacks: A set cover approach. *IEEE Transactions on Automatic Control*, *64*(9), 3949–3955. https://doi.org/10.1109/TAC.2019.2891405.

Mahmoud, M. S., Hamdan, M. M., & Baroudi, U. A. (2019). Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing*, *338*, 101–115. https://doi.org/10.1016/j.neucom.2019.01.099

Melchor-Aguilar, D., Kharitonov, V., & Lozano, R. (2010). Stability conditions for integral delay systems. *International Journal of Robust and Nonlinear Control*, *20*(1), 1–15. https://doi.org/10.1002/rnc.1405

Pajic, M., Lee, I., & Pappas, G. J. (2017). Attack-resilient state estimation for noisy dynamical systems. *IEEE Transactions on Control of Network Systems*, *4*(1), 82–92. https://doi.org/10.1109/TCNS.2016.2607420

Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, *58*(11), 2715–2729. https://doi.org/10.1109/TAC.2013.2266831

Shoukry, Y., Nuzzo, P., Puggelli, A., Sangiovanni-Vincentelli, A. L., Seshia, S. A., & Tabuada, P. (2017). Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach. *IEEE Transactions on Automatic Control*, *62*(10), 4917–4932. https://doi.org/10.1109/TAC.2017.2676679

Shoukry, Y., Nuzzo, P., Sangiovanni-Vincentelli, A. L., Seshia, S. A., Pappas, G. J., & Tabuada, P. (2017). SMC: Satisfiability modulo convex optimization. In *Proceedings of the 20th international conference on hybrid systems: Computation and control* (pp. 19–28). Pittsburgh, Pennsylvania.

Shoukry, Y., & Tabuada, P. (2015). Event-triggered state observers for sparse sensor noise/attacks. *IEEE Transactions on Automatic Control*, *61*(8), 2079–2091. https://doi.org/10.1109/TAC.2015.2492159

Tiwari, A., Dutertre, B., Jovanović, D., de Candia, T., Lincoln, P. D., Rushby, J., & Seshia, S. (2014). Safety envelope for security. In *Proceedings of the 3rd international conference on high confidence networked systems* (pp. 85–94). Berlin, Germany.

Tong, S., & Li, Y. (2010). Robust adaptive fuzzy backstepping output feedback tracking control for nonlinear system with dynamic uncertainties. *Science China Information Sciences*, *53*(2), 307–324. https://doi.org/10.1007/s11432-010-0031-y

Tong, S., Min, X., & Li, Y. (2020). Observer-based adaptive fuzzy tracking control for strict-feedback nonlinear systems with unknown control gain functions. *IEEE Transactions on Cybernetics*. Online. https://doi.org/10.1109/TCYB.2020.2977175

Zhang, X., Lu, L., Gang, F., & Zhang, C. (2013). Output feedback control of large-scale nonlinear time-delay systems in lower triangular form. *Automatica*, *49*(11), 3476–3483. https://doi.org/10.1016/j.automatica.2013.08.026

Zhang, X., Wu, M., & He, Y. (2004). Delay dependent robust control for linear systems with multiple time-varying delays and uncertainties. *Control & Decision*, *19*(5), 496–500. https://doi.org/10.3321/j.issn:1001-0920.2004.05.004.

Zhou, B. (2016). On asymptotic stability of linear time-varying systems. *Automatica*, *68*, 266–276. https://doi.org/10.1016/j.automatica.2015.12.030

Zhou, B., & Egorov, A. V. (2016). Razumikhin and Krasovskii stability theorems for time-varying time-delay systems. *Automatica*, *71*, 281–291. https://doi.org/10.1016/j.automatica.2016.04.048