Information Sciences 417 (2017) 454–464

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer

An-Yang Lu [b], Guang-Hong Yang [a,b,*]

[a] State Key Laboratory of Synthetical Automation of Process Industries, Northeastern University, Shenyang, Liaoning, 110819, China
[b] College of Information Science and Engineering, Northeastern University, Shenyang, 110819, China

ARTICLE INFO

Article history:
Received 27 December 2016
Revised 14 July 2017
Accepted 25 July 2017
Available online 26 July 2017

Keywords:
Cyber-physical systems
Sparse sensor attack
Projection operator
Switched Luenberger observer
Linear matrix inequalities

ABSTRACT

This paper investigates the secure state estimation problem for cyber-physical systems (CPSs) under disturbance and sparse sensor attacks. Both the fixed and switched target attacks are taken into account. Compared with the fixed target attacks, the switched target attacks, which are not considered in most existing results, change the attack targets at a limited frequency. The basic idea is designing a switched Luenberger observer for an augmented system where attacks are seen as part of its states. A new projection operator is proposed to ensure the sparsity of the attack estimations. Then, sufficient conditions for the existence of the desired switched observer are proposed in terms of linear matrix inequalities (LMIs) where the techniques for the switched systems with stable and unstable subsystems are introduced for tackling the switched target attacks. Compared with the existing results, no iterative algorithm is required here, and the proposed observer estimates the state well even under switched target attacks.

1. Introduction

Nowadays, cyber-physical systems (CPSs) which integrate computation, networking and physical processes tightly have attracted much attention of the scientific community. The integration does not mean the simple convergence of the physical world and the cyber space, but the deep interaction of all the physical and cyber components, i.e., power grids, deep sea exploiting systems [21], electric ground vehicle [28] and selective catalytic reduction system [27]. Meanwhile, CPSs need to guarantee the execution of multiple control policies and communications with sensors and actuators at a suitable rate, and optimize the performance of control, security and management function. For the diverse application areas of CPSs, various problems for CPSs have been considered, such as stability analysis [2,7], observer design [15], fault detection [8] and security problems [10,17,29].

Especially, since cyber components are also the source of unprecedented vulnerabilities to malicious attacks which can even affect the physical world, security in CPSs is more important than that in general computing systems [10]. Thus, substantial research has been devoted to security problems, such as malware attack defense [5], cyber attack mitigation [6], observer-based attack detection and identification [14], resilience and performance analysis under integrity attacks [4], performance degradation under stealthy deception attacks [11], and secure state estimation [3,9,15,16]. It is shown that secure

* Corresponding author.
E-mail addresses: neu-luanyang@foxmail.com (A.-Y. Lu), yangguanghong@ise.neu.edu.cn, yangguanghong@mail.neu.edu.cn (G.-H. Yang).

http://dx.doi.org/10.1016/j.ins.2017.07.029
0020-0255/

sate estimation which estimates the state of the underlying physical system from the corrupted measurements has attracted considerable attention from the control community.

On the one hand, a class of observer-based methods, showing a higher promise of scalability for that they can incorporate new information as it becomes available, have been proposed in [1,9,15]. On the other hand, by analyzing the sensor information collected within a time window of finite length, algorithm-based methods also attract much attention, for instance, [13] estimated the state by solving an L_0 optimization problem (non-convex) which is transformed into an L_1/L_r optimization problem (convex) in [3], and a class of projected gradient descent algorithms is proposed in [16]. While Chong et al. [1] and Mishra et al. [9] run multiple observers in parallel, and a major drawback of the algorithm-based methods in [3,16] solving the secure state estimation problem in polynomial time, is the loss of correctness guarantees, how to estimate the state through running an observer with guarantees on the soundness and completeness is the first motivation of this paper.

In this paper, it is assumed that attackers can implement the switched target attacks changing the set of attacked channels at a limited frequency. While all the aforementioned results only consider the fixed target attacks compromising a fixed set of channels over time, these methods fail to estimate the state in the presence of switched target attacks, which brings new challenges in secure state estimation. Thus, how to estimate the state well despite the switched target attacks is the second and main motivation of this paper.

This paper investigates the secure state estimation problem under disturbance and sparse sensor attacks. Both the fixed and switched target attacks are considered. To estimate the state from the corrupted measurements, a novel switched Luenberger observer is proposed for an augmented system which is constructed by treating attacks as part of the states of the augmented system. The contributions can be summarized as follows: (i) Inspired by Shoukry and Tabuada [16], a new projection operator is proposed to ensure the sparsity of the attack estimations. With the help of such operator, the proposed switched observer, where a switching law is introduced to reduce the conservatism, estimates the state well despite the fixed target attacks. (ii) Inspired by the techniques for the switched systems with stable and unstable subsystems, sufficient conditions for the existence of the desired switched observer such that the error system under switched target attacks stable, are proposed in terms of linear matrix inequalities (LMIs). Finally, two examples are given to show the effectiveness of the proposed methods. It is shown that the proposed observer estimates the state well despite sparse sensor attacks.

This paper is organized as follows. In Section 2, the system description and problem statement are presented. The main results are expressed in Section 3. Section 4 provides two examples . Finally, Section 5 concludes this paper.

Notation. For a matrix P, P^T denotes its transpose. $P>0$ and $P<0$ denote positive definiteness and negative definiteness, respectively. $rank(P)$ is the rank of P. Given a vector $v\in\mathbb{R}^n$, $||v||$ is its Euclidean norm, $supp(v)$ is the support of v, and v is s-sparse, if v has at most s nonzero elements ($|supp(x)|\le s$). Given two sets Γ and Γ_1, $\Gamma\backslash\Gamma_1$ denotes the relative complement of Γ_1 in Γ, and $|\Gamma|$ is denoted as the cardinality of Γ. For a discrete time interval $\Xi=[t_1,t_2)$, $|\Xi|=t_2-t_1$ (t_1, t_2 are integers) is the number of time points over Ξ. $C_n^m=\frac{n!}{m!(n-m)!}$ where ! is the factorial operator. $\hat{\chi}$ represents the estimation of χ.

2. Preliminaries

2.1. System description

Consider a class of CPSs described in linear discrete-time form

$$\begin{aligned} x(t+1) &= Ax(t)+Bu(t)+B_d d(t)\\ y(t) &= Cx(t)+Dd(t)+a(t) \end{aligned} \tag{1}$$

where $x(t)\in\mathbb{R}^{n_x}$ is the state, $u(t)\in\mathbb{R}^{n_u}$ is the control input, $y(t)\in\mathbb{R}^{n_c}$ is the measured output. n_c is the number of transmission channels. $a(t)\in\mathbb{R}^{n_c}$ is the attack signal and there is no assumption on $a(t)$ other than being s-sparse. $d(t)\in\mathbb{R}^{n_d}$ represents the disturbance and it is assumed to be bounded. A, B, B_d, C and D represent the system matrices with appropriate dimensions. Referring to Shoukry and Tabuada [16], the following assumption is introduced to ensure that the secure state estimation problem is solved.

Assumption 1. [16](s-Sparse Observable) For every set $\Gamma_s\subset\mathbb{I}$, the pair $(A,C_{\mathbb{I}\backslash\Gamma_s})$ is observable (Γ_s and $C_{\mathbb{I}\backslash\Gamma_s}$ are defined in Table 1).

By collecting τ successive observations (from $t-\tau+1$ to t, $t\ge\tau$), the output can be rewritten as follows:

$$\tilde{\mathcal{Y}}(t)=Ox(t-\tau+1)+F\mathcal{U}(t)+(F_d+\tilde{D})\mathcal{D}(t)+\mathcal{A}(t) \tag{2}$$

where $\tilde{D}=diag\{D,\cdots,D\}$ with τ blocks,

$$O=\begin{bmatrix} C\\ CA\\ \vdots\\ CA^{\tau-1}\end{bmatrix},\ F=\begin{bmatrix} 0 & 0 & \cdots 0 & 0\\ CB & 0 & \cdots 0 & 0\\ \vdots & \vdots & \ddots & \vdots\\ CA^{\tau-2}B & CA^{\tau-3}B & \cdots & CB & 0\end{bmatrix},\ \mathcal{U}(t)=\begin{bmatrix} u(t-\tau+1)\\ u(t-\tau+2)\\ \vdots\\ u(t)\end{bmatrix}$$

Table 1
Table of notations.

$\mathbb{I}$:	$\mathbb{I} = \{1, 2, \cdots, n_c\}$.
Γ_l :	$\lvert\Gamma_l\rvert = l$, $\Gamma_l \subseteq \mathbb{I}$, $l \in \{1, 2, \cdots, n_c\}$.
$C_{\hat{\Gamma}}$:	sub-matrix consisting of rows indexed by $\hat{\Gamma}$ of C.
$I_{\hat{\Gamma}}$:	sub-matrix consisting of rows of $I \in \mathbb{R}^{n_c \tau}$.
	$I_{\hat{\Gamma}}$ satisfies $I_{\hat{\Gamma}} O = O_{\hat{\Gamma}}$ where $O_{\hat{\Gamma}}$ is obtained from O by replacing C with $C_{\hat{\Gamma}}$.
$\mathcal{I}_{\hat{\Gamma}}$:	$\mathcal{I}_{\hat{\Gamma}} = diag\{I, I_{\hat{\Gamma}}^T\}$ and $Q\mathcal{I}_{\hat{\Gamma}} = [O\ I_{\hat{\Gamma}}^T]$.
*	$\hat{\Gamma}$ is a subset of $\mathbb{I}$.

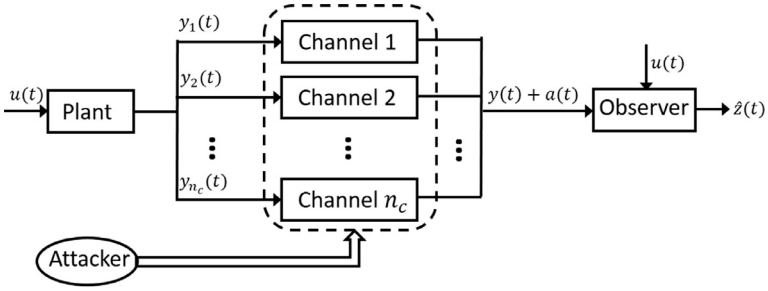

Fig. 1. Secure state estimation under sensor attacks.

F_d is defined as F with B replaced by B_d; $\tilde{\mathcal{Y}}(t)$, $\mathcal{A}(t)$ and $\mathcal{D}(t)$ are defined as $\mathcal{U}(t)$ with u replaced by y, a and d, respectively. Then, since $\tilde{\mathcal{Y}}(t)$ and $\mathcal{U}(t)$ are known, setting $\mathcal{Y}(t) = \tilde{\mathcal{Y}}(t) - F\mathcal{U}(t)$, (2) can be simplified as

$$\mathcal{Y}(t) = Ox(t - \tau + 1) + (F_d + \bar{D})\mathcal{D}(t) + \mathcal{A}(t). \tag{3}$$

Definition 1. [16](Block s-Sparse Set $\mathbb{S}_s$): If the block vector $\mathcal{A} = [\mathcal{A}_1^T, \cdots, \mathcal{A}_\tau^T]^T \in \mathbb{S}_s$, then there exits a set Γ_s (defined in Table 1) such that $\forall\ i \in \mathbb{I}$, $supp(\mathcal{A}_i) \subset \Gamma_s$.

Next, based on (3), system (1) can be rewritten as follows

$$\begin{aligned} z(t+1) =& \bar{A}z(t) + \bar{B}\bar{u}(t) + \bar{B}_d\bar{d}(t) \\ \mathcal{Y}(t) =& Qz(t) + (F_d + \bar{D})\mathcal{D}(t) \end{aligned} \tag{4}$$

where $Q = [O\ I]$, $z(t) = [x^T(t - \tau + 1)\ \mathcal{A}^T(t)]^T \in \mathbb{R}^{n_x} \times \mathbb{S}_s$ is the vector to be estimated, $\bar{u}(t) = [\mathcal{U}^T(t)\ y^T(t+1)]^T$, $\bar{d}(t) = [\mathcal{D}^T(t)\ d^T(t+1)]^T$,

$$\bar{A} = \begin{bmatrix} A & 0 & 0 \\ 0 & 0 & I \\ -CA^\tau & 0 & 0 \end{bmatrix}, \bar{B} = \begin{bmatrix} B_0 & 0 \\ 0 & 0 \\ H & I \end{bmatrix}$$

$B_0 = [B\ 0\ \cdots\ 0]$, $H = [-CA^{\tau-1}B\ -CA^{\tau-2}B\ \cdots\ -CB]$, and $\bar{B}_d$ is defined as $\bar{B}$ with B and I replaced by B_d and $-D$, respectively. In the first equation of (4), the facts that $[0\ I\ 0]z(t+1) = [0\ 0\ I]z(t)$ and $a(t+1) = y(t+1) - Cx(t+1) - Dd(t+1)$ are utilized. Since $d(t)$ is bounded, it is assumed that $||\bar{d}(t)|| \le d_M$.

Remark 1. It is easy to see that (2) and (3) are reduced to (3)-(6) in [16] if $\mathcal{D}(t) = 0$. In this paper, if there exists $\mathcal{A}_d(t)$ satisfying $||\mathcal{D}(t) + \mathcal{A}_d(t)|| \le \tilde{d}$, where $\tilde{d}$ is the maximum allowable disturbance bound, such that $\mathcal{A}(t) - \mathcal{A}_d(t) \in \mathbb{S}_s$, then some weak attacks are also allowed by treating them as disturbance. Similarly, partial disturbance $\mathcal{D}_a(t)$, which is obtained by replacing partial rows of $\mathcal{D}(t)$ with 0 and satisfies $\mathcal{A}(t) + \mathcal{D}_a(t) \in \mathbb{S}_s$, can be treated as attacks.

The following table provides the frequently-used notations in this paper.

2.2. Problem statement

In this paper, as shown in Fig. 1, our objective is to estimate the state and attack vectors from the measurements in the presence of sparse sensor attacks. Compared with the filter-based methods in [19,20], designing Luenberger observers is more direct. Thus, inspired by the robust observer design techniques in [12,18,26], a robust switched Luenberger observer is proposed to solve this problem.

Problem 1: Based on the system (4), construct the following switched Luenberger observer

$$\begin{aligned} \tilde{z}(t+1) =& \bar{A}\hat{z}(t) + \bar{B}\bar{u}(t) + L_{\sigma(t)}(\mathcal{Y}(t) - \hat{\mathcal{Y}}(t)) \\ \hat{z}(t+1) =& \Pi(\tilde{z}(t+1), P) \\ \hat{\mathcal{Y}}(t+1) =& Q\hat{z}(t+1) \end{aligned} \tag{5}$$

such that

$$\lim_{t\to\infty} ||z(t) - \hat{z}(t)|| \le \phi(d_M) \tag{6}$$

where $\tilde{z}(t) = [\tilde{x}^T(t-\tau+1)\ \tilde{\mathcal{A}}^T(t)]^T \in \mathbb{R}^{n_x+n_c\tau}$, $\hat{z}(t) = [\hat{x}^T(t-\tau+1)\ \hat{\mathcal{A}}^T(t)]^T \in \mathbb{R}^{n_x} \times \mathbb{S}_s$, $\sigma(t) \subset \mathbb{I}$ is the switching law, L_{Γ_s} are the observer gains, $\Pi(\tilde{z}(t), P)$ is the projection operator, and $\phi(d_M)$ ($\phi(0) = 0$) is a function of d_M. $\sigma(t)$, L_{Γ_s}, P and $\phi(d_M)$ will be defined in Section 3. $\Pi(\tilde{z}(t), P)$ is defined in Definition 2.

Definition 2. Given a vector $\tilde{z} \in \mathbb{R}^{n_x+n_c\tau}$, $\Pi(\tilde{z}, P)$ denotes the element of $\mathbb{R}^{n_x} \times \mathbb{S}_s$ closest to $\tilde{z}$ under the weighted matrix $P > 0$: for any $z \in \mathbb{R}^{n_x} \times \mathbb{S}_s$

$$(\Pi(\tilde{z}, P) - \tilde{z})^T P(\Pi(\tilde{z}, P) - \tilde{z}) \le (z - \tilde{z})^T P(z - \tilde{z}). \tag{7}$$

Based on the least square method, the following method is provided to execute $\Pi(\tilde{z}, P)$.

Method 1: For all $\Gamma_s \subset \mathbb{I}$, set $\hat{z}_{\Gamma_s} = \mathcal{I}_{\Gamma_s}\bar{z}_{\Gamma_s}$ where $\bar{z}_{\Gamma_s} = (P_{lr})^{-1}P_l\tilde{z}$, $P_{lr} = \mathcal{I}_{\Gamma_s}^T P \mathcal{I}_{\Gamma_s}$ and $P_l = \mathcal{I}_{\Gamma_s}^T P$, then

$$\Pi(\tilde{z}, P) = \arg\min_{\hat{z}_{\Gamma_s}} (\hat{z}_{\Gamma_s} - \tilde{z})^T P(\hat{z}_{\Gamma_s} - \tilde{z}). \tag{8}$$

Proof. For any $z \in \mathbb{R}^{n_x} \times \mathbb{S}_s$, there must exist $\Gamma_s \subset \mathbb{I}$ and $\bar{z}_{\Gamma_s} \in \mathbb{R}^{n_x+s}$ such that $z = \mathcal{I}_{\Gamma_s}\bar{z}_{\Gamma_s}$ and

$$(z - \tilde{z})^T P(z - \tilde{z}) = ||P_1\mathcal{I}_{\Gamma_s}\bar{z}_{\Gamma^s} - P_1\tilde{z}|| \tag{9}$$

where $P_1 = P^{\frac{1}{2}}$. Then, minimizing $(z - \tilde{z})^T P(z - \tilde{z})$ can bee seen as a least square problem: find $\bar{z}_{\Gamma_s} \in \mathbb{R}^{n_x+s}$ such that $||P_1\mathcal{I}_{\Gamma_s}\bar{z}_{\Gamma_s} - P_1\tilde{z}||$ reaches the minimum. By the least square method, it is obtained that $\bar{z}_{\Gamma_s} = (\mathcal{I}_{\Gamma_s}^T P_1^T P_1 \mathcal{I}_{\Gamma_s})^{-1}\mathcal{I}_{\Gamma_s}^T P_1^T P_1 \tilde{z} = (P_{lr})^{-1}P_l\tilde{z}$. Then, (8) provides $\Pi(\tilde{z}, P)$ which minimizes the right side of (7). □

Remark 2. In (5), the projection operator $\Pi(\tilde{z}(t), P)$ is utilized to ensure that the attack estimation $\hat{\mathcal{A}}(t) \in \mathbb{S}_s$. If $P = I$, $\Pi(\tilde{z}, I)$ can be obtained easily as shown in Example 4.2 in [16]. Otherwise, Method 1 can be adopted. Besides, it should be noted that while Chong et al. [1] and Mishra et al. [9] run $C_{n_c}^s$ observers in parallel for CPSs under s-sparse attacks, the proposed observer-based method runs only one observer at the same time.

Although the observer-based algorithm in [16] also provides $\hat{z}(t)$, some disadvantages should be noted: (i) Executing iterative algorithm is time-consuming. (ii) Only the time-delay state estimation $\hat{x}(t-\tau+1)$, where τ should be large enough such that O is full column rank, is obtained at time t. (iii) The set of attacked channels is assumed to remain unchanged over time. Therefore, this paper pays more attention on these three points. Besides, the disturbance which has not been considered in [16] is also taken into account here.

3. Switched Luenberger observer design

For the secure state estimation problem under sparse sensor attacks, most existing results assume that the set of attacked channels is unknown, but fixed, such as [3,9,15,16]. However, while the present attack is not satisfactory to the attackers, the attackers may abandon the present attacks and try to attack other channels. In this section, both the fixed and switched target attacks are considered.

3.1. Fixed target attacks

In this subsection, it is assumed that $supp(a(t)) \subseteq \Gamma \subset \mathbb{I}$ where $|\Gamma| = s$. Then, the following theorem provides the switched Luenberger observer (5) for the fixed target attacks.

Theorem 3.1. *For given positive scalars $\alpha_0 \in (0, 1)$, β and ϵ, if there exist a symmetric positive definite matrix $P \in \mathbb{R}^{(n_x+n_c\tau)\times(n_x+n_c\tau)}$ and matrices $S_{\Gamma_s} \in \mathbb{R}^{(n_x+n_c\tau)\times n_c\tau}$ such that*

$$\begin{bmatrix} \Upsilon_{\Gamma_{2s}}^{11} & \Upsilon_{\Gamma_s,\Gamma_{2s}}^{12} \\ * & -P/4 \end{bmatrix} < 0 \tag{10}$$

$$\epsilon I < \mathcal{I}_{\Gamma_{2s}}^T P \mathcal{I}_{\Gamma_{2s}} \tag{11}$$

where $\Upsilon_{\Gamma_{2s}}^{11} = diag\{-(1-\alpha_0)\mathcal{I}_{\Gamma_{2s}}^T P \mathcal{I}_{\Gamma_{2s}}, -\beta I\}$, $\Upsilon_{\Gamma_s,\Gamma_{2s}}^{12} = [(P\bar{A} - S_{\Gamma_s}Q)\mathcal{I}_{\Gamma_{2s}}\ \ P\bar{B}_d - [S_{\Gamma_s}(F_d + \bar{D})\ \ 0]]^T$, and $\Gamma_s \subset \Gamma_{2s}$, then the switched Luenberger observer (5) provides the estimation $\hat{z}(t)$ satisfying (6) with $\phi(d_M) = \beta d_M^2/(\epsilon\alpha_0)$. In this design, the observer gains are selected as

$$L_{\Gamma_s} = P^{-1}S_{\Gamma_s} \tag{12}$$

and the switching law is designed as

$$\sigma(t) = supp(\hat{a}(t)). \tag{13}$$

Proof. Based on (13), assume that $\sigma(t) = supp(\hat{a}(t)) = \Gamma_s$ at t. Combining (4) with (5), the error system is obtained

$$\tilde{e}(t+1) = \bar{A}\hat{e}(t) + \bar{B}_d\bar{d}(t) - L_{\Gamma_s}(\mathcal{Y}(t) - \hat{\mathcal{Y}}(t)) = [\bar{A}_{L_{\Gamma_s}} \ \bar{B}_{L_{\Gamma_s}}]\bar{e}(t) \tag{14}$$

where $\bar{A}_{L_{\Gamma_s}} = \bar{A} - L_{\Gamma_s}Q$, $\bar{B}_{L_{\Gamma_s}} = \bar{B}_d - [L_{\Gamma_s}(F_d + \bar{D}) \ 0]$, $\tilde{e}(t) = z(t) - \tilde{z}(t)$, $\hat{e}(t) = z(t) - \hat{z}(t)$, and $\bar{e}(t) = [\hat{e}^T(t) \ \bar{d}^T(t)]^T$. Besides, since $z(t), \hat{z}(t) \in \mathbb{R}^{n_x} \times \mathbb{S}_s$, $supp(a(t)) \subset \Gamma$ and $supp(\hat{a}(t)) = \Gamma_s$, there exists a set $\Gamma_{2s} = \Gamma \cup \Gamma_s$ such that $\hat{e}(t) = \mathcal{I}_{\Gamma_{2s}}(\mathcal{I}^T_{\Gamma_{2s}}\hat{e}(t))$. Thus, setting $\bar{e}_{\Gamma_{2s}}(t) = [(\mathcal{I}^T_{\Gamma_{2s}}\hat{e}(t))^T \ \bar{d}^T(t)]^T$, (14) can be rewritten as

$$\tilde{e}(t+1) = [\bar{A}_{L_{\Gamma_s}}\mathcal{I}_{\Gamma_{2s}} \ \bar{B}_{L_{\Gamma_s}}]\bar{e}_{\Gamma_{2s}}(t). \tag{15}$$

Choosing $V(t) = \hat{e}^T(t)P\hat{e}(t)$ as the Lyapunov function candidate, one can deduce that

$$\Delta V(t) = V(t+1) - V(t) = \hat{e}^T(t+1)P\hat{e}(t+1) - \hat{e}^T(t)P\hat{e}(t). \tag{16}$$

Since $\hat{e}(t) = \tilde{e}(t) + (\tilde{z}(t) - \hat{z}(t))$, one has

$$\hat{e}^T(t)P\hat{e}(t) \le 2\tilde{e}^T(t)P\tilde{e}(t) + 2(\tilde{z}(t) - \hat{z}(t))^T P(\tilde{z}(t) - \hat{z}(t)) \overset{(a)}{\le} 4\tilde{e}^T(t)P\tilde{e}(t) \tag{17}$$

where (a) is obtained by using (7). Then, it is obtained that

$$\begin{aligned}
&\Delta V(t) + \alpha_0 V(t) - \beta\bar{d}^T(t)\bar{d}(t) \\
&\overset{(a)}{\le} \bar{e}^T_{\Gamma_{2s}}(t)(4[\bar{A}_{L_{\Gamma_s}}\mathcal{I}_{\Gamma_{2s}} \ \bar{B}_{L_{\Gamma_s}}]^T P[\bar{A}_{L_{\Gamma_s}}\mathcal{I}_{\Gamma_{2s}} \ \bar{B}_{L_{\Gamma_s}}] - diag\{(1-\alpha_0)\mathcal{I}^T_{\Gamma_{2s}}P\mathcal{I}_{\Gamma_{2s}}, \beta I\})\bar{e}_{\Gamma_{2s}}(t) \\
&\overset{(b)}{\le} \bar{e}^T_{\Gamma_{2s}}(t)(4\Upsilon^{22}_{\Gamma_s,\Gamma_{2s}}P^{-1}(\Upsilon^{22}_{\Gamma_s,\Gamma_{2s}})^T + \Upsilon^{11}_{\Gamma_{2s}})\bar{e}_{\Gamma_{2s}}(t) \overset{(c)}{\le} 0
\end{aligned} \tag{18}$$

where (a) is obtained by substituting (15) and (17) into (16); (b) is obtained by substituting (12) into (a); and by Schur complement, (10) yields (c). Then, it follows from (18) that

$$\begin{aligned}
V(t+1) &\overset{(a)}{\le} (1-\alpha_0)V(t) + \beta||\bar{d}(t)||^2 \\
&\overset{(b)}{\le} (1-\alpha_0)^m V(t-m+1) + \sum_{i=1}^{m}(1-\alpha_0)^{i-1}\beta d_M^2 \\
&\overset{(c)}{\le} (1-\alpha_0)^{t+1}V(0) + \frac{\beta d_M^2}{\alpha_0}
\end{aligned} \tag{19}$$

where (b) is obtained by using (a) recursively (d_M is defined before Remark 1), and (c) holds for that $\sum_{i=1}^{t+1}(1-\alpha_0)^{i-1} \le 1/\alpha_0$.

Finally, since $\hat{e}(t) = \mathcal{I}_{\Gamma_{2s}}(\mathcal{I}^T_{\Gamma_{2s}}\hat{e}(t))$, (11) implies

$$V(t) = (\mathcal{I}^T_{\Gamma_{2s}}\hat{e}(t))^T\mathcal{I}^T_{\Gamma_{2s}}P\mathcal{I}_{\Gamma_{2s}}(\mathcal{I}^T_{\Gamma_{2s}}\hat{e}(t)) \ge \epsilon||\mathcal{I}^T_{\Gamma_{2s}}\hat{e}(t)||^2 = \epsilon||\hat{e}(t)||^2 \tag{20}$$

Combining (19) with (20) yields $\lim_{t\to\infty}||\hat{e}(t)||^2 \le \lim_{t\to\infty}V(t)/\epsilon \le \beta d_M^2/(\epsilon\alpha_0)$ which completes the proof. □

Remark 3. Compared with [16], Theorem 3.1 provides a class of LMIs to obtain the desired observer gains such that the error system (15) is stable under the fixed target attacks instead of executing an iterative algorithm (corresponding to (i) after Remark 2). It should be also noted that while the switching law (13) is introduced to reduce the conservatism, replacing S_{Γ_s} in (10) with S can reduce the computation complexity and the common observer gain $L = P^{-1}S$ is obtained with some conservatism introduced.

Remark 4. Since the requirement that τ should be large enough such that O is full column rank in [3,15,16] is unnecessary in Theorem 3.1, the proposed observer (5) with smaller τ can provide the state estimation $\hat{x}(t-\tau+1)$ more timely (corresponding to (ii) after Remark 2). Especially, if $\tau = 1$, the observer (5) provides the state estimation $\hat{x}(t)$ in real time. However, it is worth noting that the observer (5) with $\tau > 1$ which means that more information is utilized provides better disturbance rejection performance than $\tau = 1$. This fact will be verified in Section 4.

3.2. Switched target attacks

In this subsection, a class of switched target attacks is taken into account. It is assumed that each attacker can only attack one channel at the same time. Since $a(t)$ is assumed to be s-sparse after (1), there are at most s attackers. To facilitate the following study, some notions are introduced first.

Definition 3. Given $0 \le t_1 < t_2 \in \mathbb{R}$, $n_q(t_1, t_2)$ denotes the target switching times of the qth attacker during the interval $[t_1, t_2)$.

It is reasonable to assume that the target switching frequency is limited (there exists a dwell time T_q between two successive target switches of the qth attacker). Referring to the dwell time assumption in [22,23], the following assumption is introduced.

Assumption 2. There exists a scalar $T_q \geq \tau$ such that $n_q(t_1, t_2) \leq \frac{t_2 - t_1}{T_q}$ for all $0 \leq t_1 < t_2 \in \mathbb{R}$.

Compared with Section 3.1, in this section, the major difference is that $supp(a(t))$ changes over time. Then, $z(t) \in \mathbb{R}^{n_x} \times \mathbb{S}_s$ is not guaranteed any more, and this is the main difficulty. We are now ready to state the main result of this section, which is an extension of Theorem 3.1.

Theorem 3.2. *For given positive scalars $\alpha_0 \in (0, 1)$, β, ϵ and scalars α_r, if there exist a scalar θ, a symmetric positive definite matrix $P \in \mathbb{R}^{(n_x+n_c\tau)\times(n_x+n_c\tau)}$, and matrices $S_{\Gamma_s} \in \mathbb{R}^{(n_x+n_c\tau)\times n_c\tau}$ such that*

$$\begin{bmatrix} \Upsilon^{11}_{\Gamma_{2s+r}} & \Upsilon^{12}_{\Gamma_s,\Gamma_{2s+r}} \\ * & -P/4 \end{bmatrix} < 0 \tag{21}$$

$$\epsilon I < \mathcal{I}^T_{\Gamma_{2s+s_c}} P \mathcal{I}_{\Gamma_{2s+s_c}} \tag{22}$$

$$\tilde{\alpha}_r = \ln\left(\frac{1-\alpha_r}{1-\alpha_0}\right) \leq \theta r, \ \ r \geq 1 \tag{23}$$

$$\tilde{\alpha}_0 = \sum_{q=1}^{s} \frac{(\tau-1)\theta}{T_q} + \ln(1-\alpha_0) < 0 \tag{24}$$

where $\Upsilon^{11}_{\Gamma_{2s+r}}$ ($\Upsilon^{12}_{\Gamma_s,\Gamma_{2s+r}}$) is defined as $\Upsilon^{11}_{\Gamma_{2s}}$ ($\Upsilon^{12}_{\Gamma_s,\Gamma_{2s}}$) in Theorem 3.1 with α_0 and Γ_{2s} replaced by α_r and Γ_{2s+r}, respectively, $\Gamma_s \subset \Gamma_{2s+r}$, $r \in \{0, 1, \cdots, s_c\}$, and $s_c = \min\{s, n_c - 2s\}$, then the switched Luenberger observer (5) provides the estimation $\hat{z}(t)$ satisfying (6) with $\phi(d_M) = \beta d_M^2/(\epsilon(1-e^{\tilde{\alpha}_0}))$. The observer gains and switching law are given in (12) and (13), respectively.

Proof. Define $\Xi_r(t_1, t_2)$ (t_1, t_2 are integers, $r \in \{0, 1, \cdots, s\}$) as the subset of $[t_1, t_2)$ such that for $t \in \Xi_r(t_1, t_2)$, r attackers switch their target channels during $(t-\tau+1, t]$. Since there are at most s attackers, one has

$$\bigcup_{r=0}^{s} \Xi_r(t_1, t_2) = [t_1, t_2), \ \ \sum_{r=0}^{s} |\Xi_r(t_1, t_2)| = t_2 - t_1. \tag{25}$$

Besides, it is easy to see that each target switch destroys the s-sparsity of $z(t)$ for $\tau - 1$ steps (for example, if the qth attacker switches his target at t_q, then, such switch occurs during $(t-\tau+1, t]$ for all $t \in [t_q, t_q + \tau - 1)$). Then, based on Assumption 2, one can deduce that the total number of the target switches during $(t-\tau+1, t]$:

$$\sum_{r=1}^{s} r|\Xi_r(t_1, t_2)| = \sum_{q=1}^{s} (\tau-1) n_q(t_1, t_2) \leq \sum_{q=1}^{s} \frac{(\tau-1)(t_2-t_1)}{T_q}, \forall t \in [t_1, t_2). \tag{26}$$

While r attackers ($r \leq s_c$) switch their target channels during $(t-\tau+1, t]$, only $z(t) \in \mathbb{R}^{n_x} \times \mathbb{S}_{s+r}$ is guaranteed. Then, considering that $\hat{z}(t) \in \mathbb{R}^{n_x} \times \mathbb{S}_s$, we have $\hat{e}(t) \in \mathbb{R}^{n_x} \times \mathbb{S}_{2s+r}$. Similar to the proof of Theorem 3.1, from (21), it is obtained that

$$\Delta V(t) < -\alpha_r V(t) + \beta \bar{d}^T(t)\bar{d}(t). \tag{27}$$

While more than s_c attackers switch their target channels during $(t-\tau+1, t]$, it is easy to obtain that $\hat{e}(t) \in \mathbb{R}^{n_x} \times \mathbb{S}_{2s+s_c}$ and

$$\Delta V(t) < -\alpha_{s_c} V(t) + \beta \bar{d}^T(t)\bar{d}(t). \tag{28}$$

Since α_r ($r \geq 1$) may be negative, the error system (15) may be unstable for some time. Thus, the error system (14) can be seen as a switched system with stable and unstable subsystems. Then, according to the techniques for the switched system with stable and unstable subsystems in [24,25], using (27) and (28) iteratively yields

$$V(t+1) < \prod_{r=0}^{s} (1-\alpha_r)^{|\Xi_r(t-m+1,t)|} V(t-m+1) + \sum_{i=1}^{m} \prod_{r=0}^{s} (1-\alpha_r)^{|\Xi_r(t-i+2,t)|} \beta d_M^2. \tag{29}$$

where $\alpha_r = \alpha_{s_c}$ for $r \geq s_c$. Combining (23) with (26), one has

$$\sum_{r=1}^{s} |\Xi_r(t_1, t_2)| \ln\left(\frac{1-\alpha_r}{1-\alpha_0}\right) < \theta \sum_{r=1}^{s} r|\Xi_r(t_1, t_2)| < \sum_{q=1}^{s} \frac{(\tau-1)\theta}{T_q}(t_2 - t_1) \tag{30}$$

which yields that

$$\begin{aligned} \prod_{r=0}^{s} (1-\alpha_r)^{|\Xi_r(t_1,t_2)|} &= e^{\ln(\prod_{r=0}^{s}(1-\alpha_r)^{|\Xi_r(t_1,t_2)|})} = e^{\sum_{r=0}^{s}|\Xi_r(t_1,t_2)|\ln(1-\alpha_r)} \\ &\overset{(a)}{=} e^{\sum_{r=1}^{s}|\Xi_r(t_1,t_2)|\ln(\frac{1-\alpha_r}{1-\alpha_0})+(t_2-t_1)\ln(1-\alpha_0)} \overset{(b)}{<} e^{\tilde{\alpha}_0(t_2-t_1)} \end{aligned} \tag{31}$$

Table 2
Execution time (s) for random systems.

n_x	10	15	20	25	30
Algorithm 1	0.1897	0.8003	2.0150	4.5063	8.9664
PGD algorithm	0.2155	0.9335	2.4939	6.4965	13.361
L_1/L_r decoder	62.467	69.105	84.989	98.950	111.15

where (a) is obtained from (25), (b) is obtained from (30). Substituting (31) into (29) yields

$$\begin{aligned} V(t+1) &< e^{\bar{\alpha}_0 m} V(t-m+1) + \sum_{i=1}^{m} e^{\bar{\alpha}_0 (i-1)} \beta d_M^2 \\ &\overset{(a)}{<} e^{\bar{\alpha}_0 (t+1)} V(0) + \frac{\beta d_M^2}{1 - e^{\bar{\alpha}_0}} \end{aligned} \tag{32}$$

where (a) is similar to (c) of (19). Finally, referring to the proof of Theorem 3.1, it follows from (22) that

$$\lim_{t \to \infty} ||\hat{e}(t)||^2 \leq \frac{\beta d_M^2}{(1 - e^{\bar{\alpha}_0})\epsilon} \tag{33}$$

which completes the proof. □

Remark 5. Inspired by the techniques for the switched systems with stable and unstable systems [24,25], the secure state estimation problem under the switched target attacks is transformed into designing an appropriate observer such that $\bar{\alpha}_0 < 0$ guaranteeing that the error system (15) is stable in the presence of switched target attacks which have not been considered in [3,16] (corresponding to (iii) after Remark 2). Moreover, it is easy to see that if $\tau = 1$, (24) is independent of T_q, and the proposed observer is effective for any $T_q \geq 1$. However, as discussed in Remark 4, compared with $\tau > 1$, $\tau = 1$ leads to worse disturbance rejection performance. Thus, a trade-off between the target switching frequency and the disturbance rejection performance should be made in practice.

Remark 6. It is easy to see that Theorem 3.2 is reduced to Theorem 3.1 when $s_c = 0$. While $s_c > 1$, solving (21)–(24) in Theorem 3.2 is much more difficult than solving (10) and (11) in Theorem 3.1. Then, we can reduce the computational burden through (i) designing the common observer as discussed in Remark 3, (ii) replacing α_r $(r \in \{1, 2, \cdots, s_c - 1\})$ by α_{s_c} ((21)–(24) hold for $r \in \{0, n_c\}$). However, it should be noted that adopting (i) and (ii) introduces some conservatism. Besides, it is shown that for given α_0, α_r such that (21) holds, (22)–(24) are guaranteed to be feasible by setting ϵ small and β, T_q large enough. Nonetheless, larger T_q means that lower target switching frequency is allowed, and smaller ϵ and larger β lead to worse disturbance rejection performance.

Finally, based on the projection operator (8) and the observer (5) obtained by using Theorems 3.1 or 3.2, the following algorithm (switched observer, SO) is provided to estimate the state from the corrupted measurements:

$$\{\hat{z}(t+1), \sigma(t+1)\} = SO(\hat{z}(t), \bar{u}(t), \mathcal{Y}(t), \sigma(t)). \tag{34}$$

4. Example

Example 1. In this example, to compare the efficiency of the proposed observer-based method against the projected gradient descent (PGD) algorithm in [16] and the L_1/L_r decoder in [3], we randomly generate 50 linear systems with increasing dimension of the state ranging from 10 to 30 ($n_x = 10, 15, 20, 25, 30$ and each case contains 10 systems generated randomly). It is assumed that $y = x$, $d(t) = 0$ and the number of attacked channels $s = 3$. The tests are performed by using MATLAB on a desktop equipped with an Intel Core i7-6700 processor operating at 3.4 GHz and 4GB of memory. Besides, in each test, the support set for the attack vector, the attack signals, and the initial condition are chosen randomly. Then, by estimating the states from $t = 1$ to $t = 200$, the following table provides a comparison of the averaged execution time among the proposed observer-based method (Algorithm 1), the PGD algorithm (Algorithm 2 in [16]: while it fails to estimate the state for most

Algorithm 1 $SO(\hat{z}(t), \bar{u}(t), \mathcal{Y}(t), \sigma(t))$.

1: $\tilde{z} = \bar{A}\hat{z}(t) + \bar{B}\bar{u}(t) + L_{\sigma(t)}(\mathcal{Y}(t) - Q\hat{z}(t))$;
2: $\hat{z} = \Pi(\tilde{z}, P)$, $\sigma = supp(\hat{a})$;
3: **return** $\{\hat{z}, \sigma\}$
* $\hat{a} \in \mathbb{R}^{n_y}$ is the last vector block of $\hat{z}$.

systems generated randomly, the projection operator (8) is adopted instead of that in [16]), and the L_1/L_r decoder. Table 2 shows that the proposed observer-based method requires less execution time than the existing methods in [3,16].

Table 3
Minimal β for different τ.

τ	1	2	3	4
$\beta^c_{\min}$	15.56	1.594	0.617	0.335
$\beta^s_{\min}$	9.630	1.485	0.603	0.325

* $\beta^c_{\min}$ and $\beta^s_{\min}$ are for the observer (5) with common and switched observer gains, repectively.

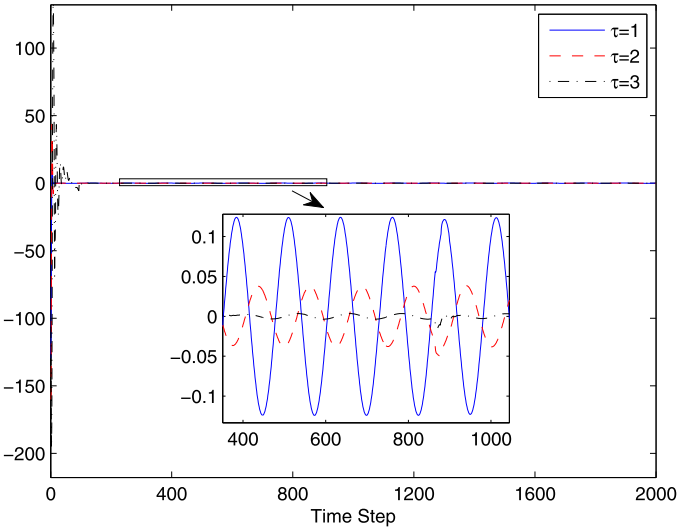

Fig. 2. The errors between the linear velocity v and its estimations for different τ (**Case I**).

Example 2. In this example, an Unmanned Ground Vehicle (UGV) example borrowed from Shoukry and Tabuada [16] is presented to illustrate the effectiveness of the proposed methods. By assuming that the UGV moves along straight lines and completely stops before rotating, the dynamics of the UGV can be described as follows

$$\begin{aligned}\begin{bmatrix}\dot{x}\\ \dot{v}\end{bmatrix} &= \begin{bmatrix}0 & 1\\ 0 & \frac{-b}{M}\end{bmatrix}\begin{bmatrix}x\\ v\end{bmatrix} + \begin{bmatrix}0\\ \frac{1}{M}\end{bmatrix}(F + d_a)\\ \begin{bmatrix}\dot{\theta}\\ \dot{\omega}\end{bmatrix} &= \begin{bmatrix}0 & 1\\ 0 & \frac{-b_r}{J}\end{bmatrix}\begin{bmatrix}\theta\\ \omega\end{bmatrix} + \begin{bmatrix}0\\ \frac{1}{J}\end{bmatrix}T\\ y_i(t) &= C_i x(t) + a_i(t) + D_{2i} d_c\end{aligned} \tag{35}$$

where x, v, θ, ω are the states of the UGV corresponding to position, linear velocity, angular position and angular velocity, respectively, $x = [x\ v\ \theta\ \omega]$. M, J, b and b_r denote the mechanical mass, inertia, translational friction coefficient and rotational friction coefficient, respectively, and it is assumed $M = 1$, $J = 2$, $b = 1$, $b_r = 1$ here. The force F and torque T are the inputs of (35), and d_a, d_c are the actuator and sensor disturbances, respectively. Besides, 5 transmission channels with $C_1 = [1\ 0\ 0\ 0]$, $C_2 = [2\ 0\ 0\ 0]$, $C_3 = [1\ 0\ 1\ 0]$, $C_4 = [0\ 0\ 1\ 0]$, $C_5 = [0\ 0\ 2\ 0]$, $D_{2i} = 0.1$ ($i \in \{1, 2, 3, 4, 5\}$) are considered.

It is assumed that the UGV goal is moving to the point ($x = 5$ or $x = -5$) which is 5m away from the origin, stop and perform 180° rotation and repeat this pattern. Similar to Shoukry and Tabuada [16], to obtain the discrete-time model, the continuous-time model (35) is discretized by assuming a zero-order hold for inputs F and T and using a time step 0.05s. Through some validation, the obtained discrete-time system is 2-sparse observable. In the following, t and $t_p = 0.05(t-1)$ represent the step number and the present time (s), respectively. We set $x(0) = [5\ 0\ 0\ 0]^T$ and $d(t) = (d_a, d_c) = (0.1sin(t_p), 0.5cos(t_p))$.

Case I: (Fixed target attacks) $a_i(t) = 0$ ($i \neq 3$) and $a_3(t) = 10cos(t_p)$. Based on Theorem 3.1, the following table is obtained by solving (10) and (11) with $\alpha_0 = 0.5$ and $\epsilon = 0.5$.

Table 3 and Fig. 2 show that the disturbance rejection performance β decreases as τ increases. This fact verifies Remark 4. Besides, Table 3 also shows that the proposed switched observer is better than the common one. Fig. 3 shows that the proposed switched observer method provide better performance than the PGD algorithm in [16] and the L_1/L_r decoder in [3]. Meanwhile, it is worth noting that the existing methods in [3,16] only work for $\tau \geq 2$.

Case II: (Switched target attacks) An attack signal $10cos(t_p)$ and 5 attack patterns (channel 1 → channel 2 → ⋯ → channel 5 → channel 1 → ⋯, the target is switched every 10 steps) are considered here. Adopting Theorem 3.2, (21)–

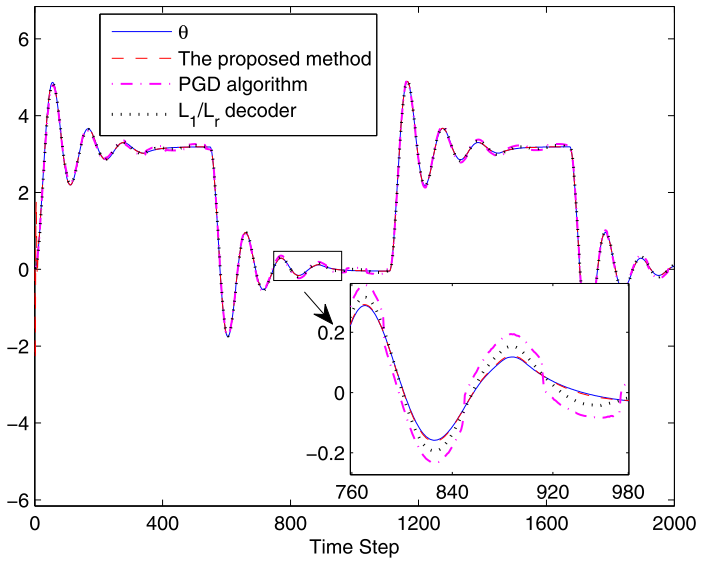

Fig. 3. The angular position θ and its estimations obtained by using different methods (**Case I**, $\tau = 2$).

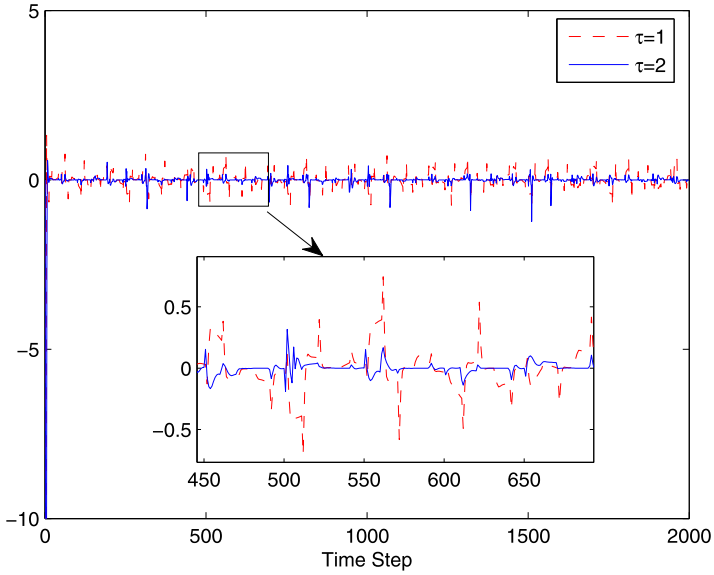

Fig. 4. The errors between linear velocity v and its estimations for $\tau = 1$ and $\tau = 2$ (**Case II**).

(24) are solvable with $\tau = 2$, $\alpha_0 = 0.5$, $\alpha_1 = -4$, $\beta = 3$ and $T_1 = 4$. For comparison, the observer (5) with $\tau = 1$ obtained in **Case I** is also adopted here. As shown in Fig. 4, although the observer (5) with $\tau = 1$ obtained in **Case I** also works for the switched target attacks, the observer obtained by solving (21)–(24) with $\tau = 2$ provides better disturbance rejection performance. Moreover, Fig. 5 shows that the existing methods in [3,16] fail to estimate the state from the measurements in the presence of the switched target attacks.

5. Conclusions

In this paper, the secure state estimation problem for CPSs under disturbance and sparse sensor attacks has been investigated. To solve this problem, a novel switched Luenberger observer has been proposed for an augmented system where attacks are seen as part of the states of the augmented system. First, a new projection operator has been proposed to ensure the sparsity of the attack estimation. Second, for the fixed target attacks, instead of using iterative algorithm, the convergence of the estimation error is guaranteed by the observer obtained by using LMI techniques. Third, the switched target attacks have been considered, and sufficient conditions for the existence of the desired observer such that the error system

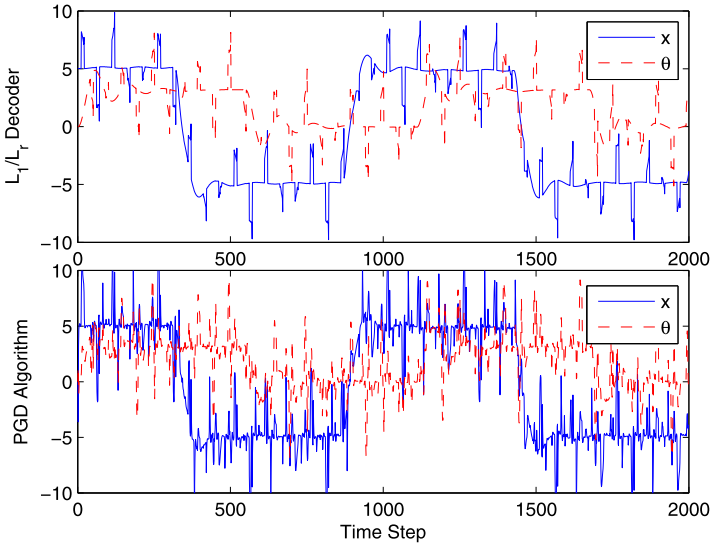

Fig. 5. The estimations of x and θ obtained by using the existing methods (**Case II**, $\tau = 2$).

stable have been proposed. Finally, two illustrative examples have been given to show the effectiveness of the proposed methods. It is shown that the proposed switched observer estimates the state well even under switched target attacks.

Acknowledgments

This paper was supported in part by National Natural Science Foundation of China (Grant nos. 61420106016 and 61621004) and the Research Fund of State Key Laboratory of Synthetical Automation for Process Industries (Grant no. 2013ZCX01).

References

[1] M. Chong, M. Wakaiki, J. Hespanha, Observability of linear systems under adversarial attacks, in: Proceedings of American Control Conference (ACC),Chicago, IN, 2015, pp. 2439–2444.
[2] A. Farraj, E. Hammad, D. Kundur, A cyber-physical control framework for transient stability in smart grids, IEEE Trans. Smart Grid (2016), doi:10.1109/TSG.2016.2581588.
[3] H. Fawzi, P. Tabuada, S. Diggavi, Secure estimation and control for cyber-physical systems under adversarial attacks, IEEE Trans. Autom. Control 59 (6) (2014) 1454–1467.
[4] D. Han, Y. Mo, L. Xie, Resilience and performance analysis for state estimation against integrity attacks, IFAC-PapersOnLine 49 (22) (2016) 55–60.
[5] S. Huda, S. Miah, M.M. Hassan, R. Islam, J. Yearwood, M. Alrubaian, et al., Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data, Inf. Sci. 379 (2017) 211–228.
[6] C. Kwon, I. Hwang, Cyber attack mitigation for cyber-physical systems: hybrid system approach to controller design, IET Control Theory Appl. 10 (7) (2016) 731–741.
[7] H.S. Li, L.F. Lai, H.V. Poor, Multicast routing for decentralized control of cyber physical systems with an application in smart grid, IEEE J. Sel. Areas Commun. 30 (6) (2012) 1097–1107.
[8] K. Manandhar, X. Cao, F. Hu, Y. Liu, Detection of faults and attacks including false data injection attack in smart grid using kalman filter, IEEE Trans. Control Netw. Syst. 1 (4) (2014) 370–379.
[9] S. Mishra, Y. Shoukry, N. Karamchandani, S. Diggavi, Secure state estimation: optimal guarantees against sensor attacks in the presence of noise, IEEE Int. Symp. Inf. Theory 46 (7) (2015) 611–614.
[10] Y. Mo, T.H.J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, et al., Cyber-physical security of a smart grid infrastructure, Proc. IEEE 100 (1) (2012) 195–209.
[11] Y. Mo, B. Sinopoli, On the performance degradation of cyber-physical systems under stealthy integrity attacks, IEEE Trans. Autom. Control 61 (9) (2016) 2618–2624.
[12] S. Mondal, Robust adaptive observer for nonlinear time-delay systems with disturbances and uncertainties, J. Control Decis. 4 (2) (2017) 100–113.
[13] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, et al., Robustness of attack-resilient state estimators, in: Proceedings of ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS),Berlin, Germany, 2014, pp. 163–174.
[14] F. Pasqualetti, F. Dörfler, F. Bullo, Attack detection and identification in cyber-physical systems, IEEE Trans. Autom. Control 58 (11) (2013) 2715–2729.
[15] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A.L. Sangiovanni-vincentelli, S.A. Seshia, J.P. Hespanha, P. Tabuada, SMT-based observer design for cyber–physical systems under sensor attacks, in: Proceedings of 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 2016.
[16] Y. Shoukry, P. Tabuada, Event-triggered state observers for sparse sensor noise/attacks, IEEE Trans. Autom. Control 61 (8) (2016) 2079–2091.
[17] S. Sridhar, A. Hahn, M. Govindarasu, Cyber-physical system security for the electric power grid, Proc. IEEE 100 (1) (2012) 210–224.
[18] L.K. Wang, J.L. Peng, X.D. Liu, H.G. Zhang, An approach to observer design of continuous-time takagi-sugeno fuzzy model with bounded disturbances, Inf. Sci. 324 (2015) 108–125.
[19] Y. Wei, J. Qiu, H.R. Karimi, M. Wang, Filtering design for two-dimensional markovian jump systems with state-delays and deficient mode information, Inf. Sci. 269 (4) (2014) 316–331.
[20] Y. Wei, J. Qiu, H.R. Karimi, Quantized h_∞ filtering for continuous-time markovian jump systems with deficient mode information, Asian J. Control 17 (5) (2015) 1914–1923.

[21] J. Yan, C.L. Chen, X.Y. Luo, X. Yang, C.C. Hua, X.P. Guan, Distributed formation control for teleoperating cyber-physical system under time delay and actuator saturation constrains, Inf. Sci. 370–371 (2016) 680–694.
[22] X. Zhao, H. Liu, J. Zhang, H. Li, Multiple-mode observer design for a class of switched linear systems, IEEE Trans. Autom. Sci. Eng. 12 (1) (2015) 272–280.
[23] D. Zhai, A.Y. Lu, J. Dong, Q.L. Zhang, Dynamic output feedback h_∞ control for switched t-s fuzzy systems via discretized lyapunov function technique, Neurocomputing 177 (2016a) 651–669.
[24] D. Zhai, A.Y. Lu, J.H. Li, Q.L. Zhang, State and dynamic output feedback control of switched linear systems via a mixed time and state-dependent switching law, Nonlin. Anal. Hybrid Syst. 22 (2016b) 228–248.
[25] L. Zhang, P. Shi, Stability, l_2-gain and asynchronous h_∞ control of discrete-time switched systems with average dwell time, IEEE Trans. Automatic Control 54 (9) (2009) 2192–2199.
[26] H. Zhang, G. Zhang, J. Wang, $\mathcal{H}_\infty$ observer design for LPV systems with uncertain measurements on scheduling variables: application to an electric ground vehicle, IEEE/ASME Trans. Mechatron. 21 (3) (2016) 1659–1670.
[27] H. Zhang, J. Wang, Adaptive sliding-mode observer design for a selective catalytic reduction system of ground-vehicle diesel engines, IEEE/ASME Trans. Mechatron. 21 (4) (2016) 2027–2038.
[28] H. Zhang, J. Wang, Active steering actuator fault detection for an automatically-steered electric ground vehicle, IEEE Trans. Veh. Technol. 66 (5) (2017) 3685–3702.
[29] B. Zheng, P. Deng, R. Anguluri, Q. Zhu, F. Pasqualetti, Cross-layer codesign for secure cyber-physical systems, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. 35 (5) (2016) 699–711.