Automatica 98 (2018) 124–129

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Secure Luenberger-like observers for cyber–physical systems under sparse actuator and sensor attacks☆

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

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

ARTICLE INFO

Article history:
Received 17 January 2017
Received in revised form 6 August 2018
Accepted 20 August 2018

Keywords:
Cyber–physical systems
Sparse actuator and sensor attacks
Secure state estimation
Secure Luenberger-like observer
Linear matrix inequality

ABSTRACT

This paper investigates the secure state estimation problem for cyber–physical systems (CPSs) under sparse actuator and sensor attacks. By introducing the notion of orthogonal complement matrix, a necessary and sufficient condition for the state observability is provided. Then, based on the least square technique, a new projection operator is proposed to reconstruct the state from a set of successive measurements. Besides, by constructing an augmented system where the attacks are seen as part of the augmented state vector, a novel secure Luenberger-like observer is proposed, and sufficient conditions for the existence of the desired observer are proposed in terms of linear matrix inequalities (LMIs). It is shown that the proposed observability condition can be reduced to the sparse observability. A distinguishing point is that the attacks may be still unavailable even if the state is observable, and besides estimating the state, the attacks are also reconstructed by the proposed algorithm and observer according to their observability automatically.

1. Introduction

Recently, cyber–physical systems (CPSs) have attracted much attention of the scientific community. Tight coupling of computation and communication substrates of CPSs has introduced significant changes in the standard design methods. Meanwhile, the integration between computation and physical processes means the deep interaction of all the physical and cyber components, i.e., power grids, water and gas distribution and deep sea exploiting systems (Yan et al., 2016). Thus, various problems have been studied, such as stability analysis (De Persis & Tesi, 2015; Farraj, Hammad, & Kundur, 2018), fault detection (Gu & Li, 2018; Manandhar, Cao, Hu, & Liu, 2014) and security problems (Amin, Cardenas, & Sastry, 2009; Sridhar, Hahn, & Govindarasu, 2012; Zheng, Deng, Anguluri, Zhu, & Pasqualetti, 2016).

Especially, the increasing set of functionalities, network interoperability, and system design complexity may introduce security vulnerabilities, and the interaction between information technology and physical world have made CPSs vulnerable to malicious attacks beyond the standard cyber attacks (Pajic et al., 2014). Thus, the need for novel methods to enhance the security of CPSs has motivated several research directions recently (Teixeira, Sou, Sandberg, & Johansson, 2015). Such as false-date injection attacks analysis (Sandberg, Teixeira, & Johansson, 2010), performance degradation under stealthy deception attacks (Mo & Sinopoli, 2016), secure control framework for resource-limited adversaries (Teixeira, Shames, Sandberg, & Johansson, 2015), observer-based attack detection and identification (Pasqualetti, Dörfler, & Bullo, 2013), and *secure state estimation* (Fawzi, Tabuada, & Diggavi, 2014).

Secure state estimation, which is to estimate the state from the corrupted measurements, has attracted considerable attention from the control community. While secure state estimation under sparse attacks is intrinsically a combinatorial problem, the strategies for such problem can be categorized into (i) brute force search: such as observer-based methods in Chong, Wakaiki, and Hespanha (2015), Lu and Yang (2017a) and Xie and Yang (2018), filter-based method in Mishra, Shoukry, Karamchandani, Diggavi, and Tabuada (2015), and L_0 decoder in Pajic et al. (2014); (ii) convex relaxations: such as L_1/L_r decoder in Fawzi et al. (2014) and Pajic, Lee, and Pappas (2017), and gradient descent algorithms in Shoukry and Tabuada (2016). On the one hand, estimating the state from the corrupted measurements by brute force search

☆ This work was supported in part by the Funds of National Science of China (Grant Nos. 61621004, 61420106016 and 61773097), and the Research Fund of State Key Laboratory of Synthetical Automation for Process Industries, PR China (Grant No. 2018ZCX03). The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Shreyas Sundaram under the direction of Editor Christos G. Cassandras.

* Corresponding author at: College of Information Science and Engineering, Northeastern University, Shenyang 110819, PR China.
E-mail addresses: luanyang1991@stumail.neu.edu.cn (A.-Y. Lu), yangguanghong@neu.edu.cn (G.-H. Yang).

https://doi.org/10.1016/j.automatica.2018.09.003
0005-1098/© 2018 Elsevier Ltd. All rights reserved.

suffers from scalability issues. On the other hand, the convex relaxations ensure that the state is reconstructed in polynomial time with correctness guarantees for reduced set of systems.

Since the actuators, sensors and controllers need to communicate with each other, in addition to sensor (sensor to controller communication link), actuator (controller to actuator communication link) may also be attacked. However, most previous results only consider the sensor attacks. Although some discussions on sparse actuator attacks have been given in Fawzi et al. (2014), sufficient and necessary conditions for the state observability under actuator attacks have not been studied. This is the main motivation of this paper. Besides, while the stability of CPSs may be destroyed by the actuator attacks even if the state is reconstructed accurately, besides estimating the state, estimating the attacks from the corrupted measurements is also meaningful. In Shoukry and Tabuada (2016), the sparse sensor attack estimations are provided by a convex projection operator, based on which Lu and Yang (2017b) provides a non-convex one. Moreover, a Luenberger-like observer is also provided in Shoukry and Tabuada (2016) to estimate the state and attacks for its higher promise of scalability for new measurements. Since these methods may not apply to CPSs under sparse actuator attacks, how to provide the attack estimations also motivates this study.

This paper investigates the secure state estimation problem under sparse actuator and sensor attacks. The main contributions can be summarized as follows:
(i) By extending the works in Fawzi et al. (2014) and Shoukry and Tabuada (2016) with both actuator and sensor attacks taken into account, a necessary and sufficient condition for the observability under sparse actuator and sensor attacks is constructed by introducing the notion of orthogonal complement matrix. It is shown that for the existence of actuator attacks, the state and attacks are not always available simultaneously.
(ii) For the systems under sparse actuator and sensor attacks, novel projection operator and secure Luenberger-like observer are proposed to estimate the state and attacks from the corrupted measurements. Especially, the proposed observer, obtained by solving a class of linear matrix inequalities (LMIs), can provide the state estimation with smaller time-delay than that in Shoukry and Tabuada (2016).

This paper is organized as follows. In Section 2, the system description and problem statement are presented. The main results are expressed in Sections 3 and 4. In Section 5, an example is given. Finally, Section 6 concludes this paper.

Notation. For a matrix $M \in \mathbb{R}^{p\times q}$, M^T denotes its transpose, $M > 0$ ($M < 0$) denotes positive (negative) definiteness, $\lambda_m(M)$ denotes its smallest eigenvalue, and $span(M) \subseteq \mathbb{R}^p$ is spanned by its columns. Given a vector $v \in \mathbb{R}^n$, $\|v\|$ is its Euclidean norm, $supp(v)$ is the support of v. For a set of vectors v_i, $(v_1, \ldots, v_n)$ denotes $[v_1^T \cdots v_n^T]^T$. $\mathbb{R}$ denotes the set of reals. $\hat{\star}$ denotes the estimation of $\star$. 0 and I are zero and unit matrices with appropriate dimensions, respectively. Besides, Table 1 provides some other frequently used symbols.

2. Preliminaries

2.1. System description

Consider the following linear discrete-time system:

$$
\begin{aligned}
x(t+1) &= Ax(t) + B(u(t) + a_u(t)) + B_d d(t) \\
y(t) &= Cx(t) + a_y(t) + Dd(t)
\end{aligned} \tag{1}
$$

where $x(t) \in \mathbb{R}^{n_x}$ is the state vector, $u(t) \in \mathbb{R}^{n_u}$ is the control input, $y(t) \in \mathbb{R}^{n_y}$ is the output, and $d(t) \in \mathbb{R}^{n_d}$ is the bounded disturbance. Matrices A, B, B_d, C and D represent the system matrices with appropriate dimensions, and (A, C) is observable. $a_u(t)$ and $a_y(t)$, satisfying $|supp(a_u(t))| \leq s_u$ and $|supp(a_y(t))| \leq s_y$, are the actuator and sensor attacks, respectively. The set of attacked channels is unknown but fixed.

Table 1
Table of notations.

$\mathbb{I}_u/\mathbb{I}_y$:	$\{1, 2, \ldots, n_u\}./\{1, 2, \ldots, n_y\}$.
$I_{\hat{\Gamma}}$:	Matrix consisting of rows indexed by $\hat{\Gamma}$ of I.
$\mathcal{I}_{\hat{\Gamma}}$:	$diag\{I_{\hat{\Gamma}}, \ldots, I_{\hat{\Gamma}}\}$ with τ blocks.
$\bar{\mathcal{I}}_{\Gamma_u,\Gamma_y}$:	$diag\{I, \mathcal{I}_{\Gamma_u}, \mathcal{I}_{\Gamma_y}\}$.

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

$$
\begin{aligned}
\mathcal{Y}(t) =& \mathcal{O}x(t-\tau+1) + F\mathcal{A}_u(t) + \mathcal{A}_y(t) + D_d\mathcal{D}(t) \\
=& Qz(t) + D_d\mathcal{D}(t)
\end{aligned} \tag{2}
$$

where $z(t) = (x(t-\tau+1), \mathcal{A}_u(t), \mathcal{A}_y(t))$, $Q = [\mathcal{O}\ F\ I]$, $D_d = F_d + diag\{D, \ldots, D\}$, $F = [0; [H\ 0]]$,

$$
\mathcal{O} = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{\tau-1} \end{bmatrix}, \; H = \begin{bmatrix} CB & 0 & \cdots & 0 \\ CAB & CB & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ CA^{\tau-2}B & CA^{\tau-3}B & \cdots & CB \end{bmatrix}
$$

F_d is defined as F with B replaced by B_d, $\mathcal{Y}(t) = \tilde{\mathcal{Y}}(t) - F\mathcal{U}(t)$, $\mathcal{U}(t) = (u(t-\tau+1), \ldots, u(t))$. $\tilde{\mathcal{Y}}(t)$, $\mathcal{A}_u(t)$, $\mathcal{A}_y(t)$ and $\mathcal{D}(t)$ are defined as $\mathcal{U}(t)$ with u replaced by y, a_u, a_y and d, respectively. It is assumed that $\|\mathcal{D}(t)\| \leq d_M$.

Definition 2.1 (*Shoukry & Tabuada, 2016*). If block vector $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_\tau) \in \mathbb{S}_s$, then $|\cup_{i\in\{1,\ldots,\tau\}} supp(\mathcal{A}_i)| \leq s$.

Definition 2.2 (*Orthogonal Complement Matrix*). For a matrix M, $M^\perp$ is an orthogonal complement matrix of M, and the following statements are available:
(i) $MM^\perp = 0$, and $\{v|Mv = 0\} = span(M^\perp)$,
(ii) setting $M^{\perp^2} = ((M^\perp)^T)^\perp$, $[M^{\perp^2}\ M^\perp]$ is an orthogonal matrix and $MM^{\perp^2}$ is of full column rank.

2.2. Problem statement

In this paper, our objective is to estimate the state from the measurements in the presence of sparse actuator and sensor attacks. In the following, two problems are provided. The first one is borrowed from Shoukry and Tabuada (2016) to analyze the observability. The second one is designing a secure Luenberger-like observer to estimate the state and attacks from the corrupted measurements under disturbance.

Problem 1 (*Static Batch Optimization*). Design a decoder to construct the state estimation $\hat{x}(t-\tau+1)$ from a batch of measurements in the noiseless case.

Similar to Shoukry and Tabuada (2016), Problem 1 will be solved by solving the following optimization problem:

$$
\arg \min_{\hat{z}\in\mathbb{R}^{n_x}\times\mathbb{S}_{s_u}\times\mathbb{S}_{s_y}} \|\mathcal{Y}(t) - Q\hat{z}(t)\|^2 \tag{3}
$$

where $\hat{z} = (\hat{x}(t-\tau+1), \hat{\mathcal{A}}_u(t), \hat{\mathcal{A}}_y(t))$.

Problem 2 (*Secure Luenberger-like Observer*). Construct a Luenberger-like observer such that

$$
\lim_{t\to\infty} \|x(t) - \hat{x}(t)\|^2 \leq \phi(d_M) \tag{4}
$$

where $\phi(d_M)$ ($\phi(0) = 0$) is a bounded function of d_M.