Interval Observers for Secure Estimation in Cyber-Physical Systems

Kwassi Holali Degue, Denis Efimov, Jerome Le Ny, Eric Féron

Interval Observers for Secure Estimation in Cyber-Physical Systems

Kwassi H. Degue, Denis Efimov, Jerome Le Ny and Eric Feron

***Abstract*— Stealthy attacks on the sensors and actuators embedded in cyber-physical systems could hinder the safe operation of these systems if the state estimators monitoring them cannot detect such attacks in time. In this paper, we study stealthy attacks in the framework of interval observers. We consider two classes of attacks: when a malicious agent compromises the sensors and when it is able to alter the system's actuators. For each type of attack, we design a dedicated interval observer for the system's state and we construct bounds for the attack signal. We investigate the ability of such interval observer to provide accurate estimates when the system is under the attack. Numerical simulations for a lateral model of an aircraft illustrate the capabilities of the synthesized observers.**

I. Introduction

Security vulnerabilities in Cyber-Physical Systems (CPS), i.e., systems that tightly integrate computing and communication resources to control physical processes, allow for new types of cyberattacks that can lead to disastrous physical damage. Some recent examples include the StuxNet malware [1] and the Maroochy Sewage Control Incident [2]. Smaller systems such as commercial drones [3] and military vehicles [4] were also targeted.

CPS security is a currently active research area, and several attack strategies and defense mechanisms have been studied. Standard fault detection algorithms, while generally useful, may in some cases be unsuccessful against the attacks of a smart adversary [5]. Classical bad data detection strategies, such as the largest residue test [6], have been applied extensively to static linear models with Gaussian noise, e.g., in the context of state estimation for power systems. Nevertheless, an adversary who is acquainted with the configuration of a power grid for example might be able to carry out a false-data injection attack [7], i.e., inject a *stealthy* input into the measurements to alter the state estimator of the power grid while leaving the residue unchanged [8].

To carry out false-data injection attacks on a dynamical system, an attacker must select attack vectors that are consistent not only with static observations but also with the state dynamics at all times [7]. This type of attack is discussed in [9] for noiseless models. The authors of [10] considered dynamic false-data injection attacks, assuming that the statistical properties of the disturbances are available, and [11] designed optimal *stealthy* attack strategies against CPS by making the same assumption. However, for physical and economical reasons, state disturbances of industrial system models are often modeled as bounded stochastic signals [12] for control design. Robust failure detection algorithms are based on the ability to handle disturbance and noise that are *a priori* bounded [13], [14]. This allows an intelligent adversary to hide an attack within these bounds, remaining undetected while causing serious harm. An analysis of stealthy attacks in a set-membership-based framework is performed in [5]. For state estimation, set-membership approaches take the measurements into account by computing the set of states consistent with the model and the measurements [15]. However, this technique can be difficult to apply in practice to design Fault Detection and Isolation (FDI) systems, where simpler observers with tunable gains are more common. On the other hand, interval observers [16]–[18], which are a subclass of set-membership estimators, take into account the measurements by using observer gains explicitly, and have become one of the most common approach for FDI during the last decade [15]. In this paper, we focus on secure estimation under stealthy attacks with interval observers.

The first contribution of this paper lies in designing interval observers resilient to stealthy sensor attacks. State estimation has been developed for dynamical systems under attacks with bounded noise in [19]. However, stealthy attacks have not been discussed in [19], where it is assumed that there is no uncertainty on the initial value of the state, which is a drawback in applications where only bounds on $x(0)$ are known. In contrast, we assume un-

This work was supported in part by NSERC under Grant RGPIN 435905-13, the Fonds de Recherche du Québec - Nature et Technologies (FRQNT) international internships fellowship (Energy/Digital/Aerospace), the Government of Russian Federation (Grant 08-08) and the Ministry of Education and Science of Russian Federation (Project 14.Z50.31.0031).

K. H. Degue and J. Le Ny are with the department of Electrical Engineering, Polytechnique Montreal and GERAD, QC H3T-1J4, Montreal, Canada kwassi-holali.degue,jerome.le-ny@polymtl.ca

D. Efimov is with Inria, Univ. Lille, CNRS, UMR 9189 - CRIStAL, F-59000 Lille, France. He is also with the Department of Control Systems and Informatics, Saint-Petersburg State University of Information Technologies, Mechanics and Optics (ITMO), 49 Kronverkskiy av., 197101 Saint Petersburg, Russia Denis.Efimov@inria.fr

E. Feron is with School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, USA eric.feron@aerospace.gatech.edu

certain initial conditions as well as uncertain time-varying inputs in the continuous-time dynamics. Furthermore [19] computes the state estimate by solving a combinatorial l_0-norm minimization problem at each iteration, which requires sufficient computing resources. Here we solve the problem by designing interval estimators, whose gains can be computed efficiently by using linear programming. The second contribution of this paper lies in designing, for the first time, interval observers resilient to actuator attacks.

Section II presents the problem statement and some results from interval estimation theory. These results are applied to design interval state observers and to construct bounds for stealthy attacks in the case of sensor attacks in Section III and actuator attacks in Section IV. Finally, Section V presents numerical simulations for a lateral aircraft model to illustrate the performance of our algorithms.

Notation: We denote the real and integer numbers by $\mathbb{R}$ and $\mathbb{Z}$ respectively, $\mathbb{R}_+ = \{\tau \in \mathbb{R} : \tau \geq 0\}$ and $\mathbb{Z}_+ = \mathbb{Z} \cap \mathbb{R}_+$. The Euclidean norm for a vector $x \in \mathbb{R}^n$ is written $|x|$. The symbol I_n denotes the $n \times n$ identity matrix. For a bounded vector-valued signal $u : \mathbb{R}_+ \to \mathbb{R}^n$ the symbol $||u||_{[t_0,t_1]}$ denotes its L_∞ norm $||u||_{[t_0,t_1]} = \sup_{t\in[t_0,t_1]} |u(t)|$, and if $t_1 = +\infty$ then we simply write $||u||$. We denote by $\mathcal{L}_\infty^n$ the set of all vector-valued signals u with the property $||u|| < \infty$. The symbols $\underline{u}$ and $\overline{u}$ denote lower and upper bounds of the signal u component-wise. A matrix $A \in \mathbb{R}^{n\times n}$ is called Metzler if all its elements outside the main diagonal are nonnegative, i.e., $A_{i,j} \geq 0$ for $1 \leq i \neq j \leq n$. For two vectors $x_1, x_2 \in \mathbb{R}^n$ or matrices $A_1, A_2 \in \mathbb{R}^{n\times n}$, the relations $x_1 \leq x_2$ and $A_1 \leq A_2$ are understood element-wise.

II. Background

A. System Model

Consider the following system for $t \geq 0$

$$\begin{aligned} \dot{x}(t) &= Ax(t) + w(t), \\ y(t) &= Cx(t), \end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $w : \mathbb{R}_+ \to \mathbb{R}^n$ is an *unknown* input in $\mathcal{L}_\infty^n$, $y(t) \in \mathbb{R}^p$ is the output signal available for measurements, and $A \in \mathbb{R}^{n\times n}$, $C \in \mathbb{R}^{p\times n}$ are known constant matrices. Denote by $x(t, x_0, w)$ the solution of the system (1) corresponding to an initial condition $x_0 \in \mathbb{R}^n$ and the input $w \in \mathcal{L}_\infty^n$ at the time instant $t \geq 0$, and $y(t, x_0, w) = Cx(t, x_0, w)$. A monitoring system is estimating the state using the measurements y from the sensors, under the following assumptions.

Assumption 1. *The state $x \in \mathcal{L}_\infty^n$ and the initial conditions satisfy $\underline{x}_0 \leq x_0 \leq \overline{x}_0$, where $\underline{x}_0, \overline{x}_0 \in \mathbb{R}^n$ are given constant vectors.*

Assumption 2. *Two functions $\underline{w}$, $\overline{w} : \mathbb{R}_+ \to \mathbb{R}^n$ in $\mathcal{L}_\infty^n$ are given such that*

$$\underline{w}(t) \leq w(t) \leq \overline{w}(t), \quad \forall t \geq 0.$$

Assumption 1 implies that the state $x(t, x_0, w)$ is bounded and that the initial conditions are constrained to belong to some known interval $[\underline{x}_0, \overline{x}_0]$. Assumption 2 states that the input of the system (1) is known up to some interval error $\overline{w}(t) - \underline{w}(t)$.

B. Problem Statement

In the sequel, we assume that an adversary is capable of adding an attack signal to the sensor measurements or the dynamics of (1). The attack signal, denoted as $a(t)$, is assumed to belong to a (possibly unknown) interval $[\underline{a}, \overline{a}]$, corresponding to the desire of the adversary to remain undetected. The subscript a is used to denote signals of the system under attack. Thus, the output of the system under attack is denoted as $y_a(t, x_0, w, a)$.

In the first part of this paper, we assume that the adversary compromises the sensor by adding a malicious signal $a \in \mathcal{L}_\infty^p$ to the measured signal:

$$\begin{aligned} \dot{x}_a(t) &= Ax_a(t) + w(t), \\ y_a(t) &= Cx_a(t) + a(t). \end{aligned} \tag{2}$$

The aim of the attacker is to degrade the state estimate while remaining undetected. Following [20], we define stealthy sensor attacks as those that produce a plausible output signal, as follows:

Definition 1. *A sensor attack $a \in \mathcal{L}_\infty^p$ is called* stealthy *if there exist some initial conditions $\xi_1, \xi_2 \in [\underline{x}_0, \overline{x}_0]$ and inputs $w_1, w_2 \in [\underline{w}, \overline{w}]$ for* (2) *and* (1) *respectively, such that*

$$y_a(t, \xi_1, w_1, a) = y(t, \xi_2, w_2) \quad \forall t \geq 0, \tag{3}$$

where y_a is an output of (2) *and y of* (1)*.*

The second part of this work is devoted to the study of attacks where the adversary is able to compromise the actuator signals with a malicious signal $a \in \mathcal{L}_\infty^n$:

$$\begin{aligned} \dot{x}_a(t) &= Ax_a(t) + w(t) + a(t), \\ y_a(t) &= Cx_a(t). \end{aligned} \tag{4}$$

For the system (4), denote the solution corresponding to initial condition $x_0 \in \mathbb{R}^n$, the input $w \in \mathcal{L}_\infty^n$ and attack signal $a \in \mathcal{L}_\infty^n$ by $x_a(t, x_0, w, a)$.

Definition 2. *An actuator attack $a \in \mathcal{L}_\infty^n$ is called* stealthy *if there exist some initial conditions $\xi_1, \xi_2 \in [\underline{x}_0, \overline{x}_0]$ and inputs $w_1, w_2 \in [\underline{w}, \overline{w}]$ for* (4) *and* (1) *respectively, such that the output derivatives coincide. That is, the relation*

$$\dot{y}_a(t, \xi_1, w_1, a) = \dot{y}(t, \xi_2, w_2) \tag{5}$$

holds for almost all $t \geq 0$, where y_a is an output of (4) *and y of* (1)*.*

Note that relation (5) is a consequence of (3), but the converse is not true. As a result, Definition 2 imposes fewer restrictions than Definition 1 on the output signals that the attacker is allowed to produce while remaining "stealthy".

Problem: For a given system assumed under attack, we aim at: (i) designing an interval observer when the monitoring system knows a priori the bounds $\underline{a}$ and $\overline{a}$ on the attack signal; (ii) providing a method to estimate $\underline{a}$ and $\overline{a}$ as well.

In the rest of this section, we review some basic facts from the theory of interval estimation.

C. Interval Relations

For a matrix $A \in \mathbb{R}^{m\times n}$, define $A^+ = \max\{0, A\}$ applied element-wise, $A^- = A^+ - A$ (we use the same definition for vectors) and denote the matrix of all elements' absolute values by $A^\star = A^+ + A^-$.

Lemma 1. [21] *Let $x \in \mathbb{R}^n$ be a vector with $\underline{x} \leq x \leq \overline{x}$ for some $\underline{x}, \overline{x} \in \mathbb{R}^n$. If $A \in \mathbb{R}^{m\times n}$ is a matrix, then*

$$A^+\underline{x} - A^-\overline{x} \leq Ax \leq A^+\overline{x} - A^-\underline{x}. \tag{6}$$

D. Nonnegative Linear Systems

Consider the linear time-invariant system

$$\dot{x}(t) = Ax(t) + \omega(t),\ \omega : \mathbb{R}_+ \to \mathbb{R}^n_+,\ \omega \in \mathcal{L}^n_\infty, \tag{7}$$

where the matrix $A \in \mathbb{R}^{n\times n}$ is Metzler. Its solution $x(t) \in \mathbb{R}^n_+$ (is element-wise nonnegative), $\forall t \geq t_0$, for every initial condition $x(t_0) \in \mathbb{R}^n_+$ [22], [23]. In this case, the dynamical system (7) is called cooperative or monotone.

E. Standard Interval Observer Design

We need the following assumption.

Assumption 3. *For A, C defined in* (1)*, there exists a matrix $L \in \mathbb{R}^{n\times p}$ such that the matrix $(A-LC)$ is Hurwitz and Metzler.*

Assumption 3 is essential for the interval estimation approach, but it is rather restrictive. It can be relaxed using a coordinate transformation [16], [18], which is omitted here for brevity and simplicity of notation.

If the monitoring system does not take into account the presence of an attack, it believes the system model to be (1), whereas it measures in fact y_a from (2) or (4). It can then design an interval observer of the form

$$\begin{aligned}\dot{\underline{x}}(t) =&(A - LC)\underline{x}(t) + Ly_a(t) + \underline{w}(t),\ \underline{x}(0) = \underline{x}_0\\ \dot{\overline{x}}(t) =&(A - LC)\overline{x}(t) + Ly_a(t) + \overline{w}(t),\ \overline{x}(0) = \overline{x}_0,\end{aligned} \tag{8}$$

where $\underline{x}(t) \in \mathbb{R}^n$ and $\overline{x}(t) \in \mathbb{R}^n$ are the lower and the upper interval estimates of the system for the state $x(t)$. When the bounds $\underline{x}$ and $\overline{x}$ do not satisfy any stability property, they are called framers [24]. Define the errors $\overline{e}(t) = \overline{x}(t) - x(t)$ and $\underline{e}(t) = x(t) - \underline{x}(t)$.

Theorem 1. [25], [26] *Let Assumptions 1–3 be satisfied, and suppose $a \equiv 0$. Then we have for* (1)

$$\underline{x}(t) \leq x(t) \leq \overline{x}(t), \quad \forall t \geq 0, \tag{9}$$

provided that $\underline{x}_0 \leq x(0) \leq \overline{x}_0$, and moreover $\overline{e}, \underline{e} \in \mathcal{L}^n_\infty$.

Unfortunately, in the presence of an attack signal, the guarantees of Theorem 1 become generally invalid, i.e., we do not necessarily have $\underline{x} \leq x_a \leq \overline{x}$ for the observer (8). The next sections discuss how to take the attack signal into account.

III. Stealthy Sensor Attacks

A. Interval Estimation of x_a with Knowledge of $\underline{a}$ and $\overline{a}$

Consider the case in which the monitoring system knows $\underline{a}$ and $\overline{a}$ while estimating x_a. The equations of an interval observer for (2) can take the form

$$\begin{aligned}\dot{\underline{x}}_a(t) =& (A - LC)\underline{x}_a(t) + Ly_a(t) + \underline{w}(t)\\ &- L^+\overline{a}(t) + L^-\underline{a}(t),\ \ \underline{x}_a(0) = \underline{x}_0,\\ \dot{\overline{x}}_a(t) =& (A - LC)\overline{x}_a(t) + Ly_a(t) + \overline{w}(t)\\ &- L^+\underline{a}(t) + L^-\overline{a}(t),\ \ \overline{x}_a(0) = \overline{x}_0,\end{aligned} \tag{10}$$

where $\underline{x}_a(t) \in \mathbb{R}^n$ and $\overline{x}_a(t) \in \mathbb{R}^n$ are respectively the lower and the upper interval estimates for the state $x_a(t)$. Define $\overline{e}_a(t) = \overline{x}_a(t) - x_a(t)$ and $\underline{e}_a(t) = x_a(t) - \underline{x}_a(t)$.

Theorem 2. *Let Assumptions 1–3 be satisfied. Then we have, for* (2) *and* (10)*,*

$$\underline{x}_a(t) \leq x_a(t) \leq \overline{x}_a(t), \quad \forall t \geq 0, \tag{11}$$

provided that $\underline{x}_0 \leq x_a(0) \leq \overline{x}_0$, and moreover the errors $\overline{e}_a, \underline{e}_a \in \mathcal{L}^n_\infty$.

We skip the proofs of our results due to space limitations. The interval observer (10) answers Problem (i) for sensor attacks.

B. Estimation of $\underline{a}$ and $\overline{a}$ for Stealthy Sensor Attacks

Consider now the case in which the monitoring system does not know $\underline{a}$ and $\overline{a}$ a priori, while estimating x_a. After for estimating $\underline{a}$ and $\overline{a}$. The results of this section are useful for both the attacker and the monitoring system (the defender). These results represent a way for the adversary to make sure its attack is stealthy and at the same time a way for the monitoring system to obtain a priori bounds on a, in order to design a proper interval estimator.

Using Definition 1, for the model (2), a stealthy sensor attack means that $y(t,\xi_1,w_1)+a(t)=y(t,\xi_2,w_2),\forall t\geq 0$, which implies

$$a(t)=Ce(t) \text{ with } e(t)=x(t,\xi_2,w_2)-x(t,\xi_1,w_1),$$

where ξ_1,ξ_2 are valid initial conditions for the dynamics of (1) or (2) in the interval $[\underline{x}_0,\overline{x}_0]$, and w_1,w_2 are valid input signals with values at any time t in $[\underline{w}(t),\overline{w}(t)]$. The difference $e(t)$ satisfies

$$\dot{e}(t)=Ae(t)+w_2(t)-w_1(t).$$

We need the following assumptions to construct a framer for a.

Assumption 4. *There exists a nonsingular matrix $S\in\mathbb{R}^{n\times n}$ such that $D=SAS^{-1}$ is Hurwitz and Metzler.*

Note that Assumption 4 is true when A is Hurwitz and diagonalizable. Introduce a transformed state difference for (1) with $\epsilon=Se$, then

$$\begin{aligned}\dot{\epsilon}(t)&=D\epsilon(t)+S(w_2(t)-w_1(t)),\\ a(t)&=CS^{-1}\epsilon(t),\end{aligned}\tag{12}$$

and Assumption 2 implies, for all $t\geq 0$,

$$\underline{w}(t)-\overline{w}(t)\leq w_2(t)-w_1(t)\leq\overline{w}(t)-\underline{w}(t),$$

while

$$-S^\star(\overline{x}_0-\underline{x}_0)=\underline{\epsilon}_0\leq\epsilon(0)\leq\overline{\epsilon}_0=S^\star(\overline{x}_0-\underline{x}_0)$$

under Assumption 1.

Theorem 3. *Let Assumptions 1, 2 and 4 be satisfied. Then a stealthy sensor attack in the sense of Definition 1 must satisfy $\underline{a}(t)\leq a(t)\leq\overline{a}(t),\forall t\geq 0$, where*

$$\begin{aligned}\underline{a}(t)&=(CS^{-1})^+\underline{\epsilon}(t)-(CS^{-1})^-\overline{\epsilon}(t),\\ \overline{a}(t)&=(CS^{-1})^+\overline{\epsilon}(t)-(CS^{-1})^-\underline{\epsilon}(t),\\ \dot{\underline{\epsilon}}(t)&=D\underline{\epsilon}(t)-S^\star(\overline{w}(t)-\underline{w}(t)),\ \ \underline{\epsilon}(0)=\underline{\epsilon}_0\\ \dot{\overline{\epsilon}}(t)&=D\overline{\epsilon}(t)+S^\star(\overline{w}(t)-\underline{w}(t)),\ \ \overline{\epsilon}(0)=\overline{\epsilon}_0.\end{aligned}\tag{13}$$

Moreover, $\epsilon(t)$, the attack signal $a(t)$ and the error signals $\overline{\delta}(t)=\overline{\epsilon}(t)-\epsilon(t)$, $\underline{\delta}(t)=\epsilon(t)-\underline{\epsilon}(t)$, $a(t)-\underline{a}(t)$ and $\overline{a}(t)-a(t)$ all belong to $\mathcal{L}_\infty^p$.

Theorem 3 answers Problem (ii) for sensor attacks, under the additional Assumption 4.

IV. Stealthy Actuator Attacks

A. Interval Estimation of x_a with Knowledge of $\underline{a}$ and $\overline{a}$

First, we address the case in which the monitoring system knows $\underline{a}$ and $\overline{a}$ while estimating x_a. Under Assumptions 1-3, an interval observer for (4) takes the form

$$\begin{aligned}\dot{\underline{x}}_a(t)&=(A-LC)\underline{x}_a(t)+Ly_a(t)+\underline{w}(t)+\underline{a}(t),\\ \dot{\overline{x}}_a(t)&=(A-LC)\overline{x}_a(t)+Ly_a(t)+\overline{w}(t)+\overline{a}(t),\end{aligned}\tag{14}$$

where $\underline{x}_a(t)\in\mathbb{R}^n$ and $\overline{x}_a(t)\in\mathbb{R}^n$ are respectively the lower and the upper interval estimates for the state $x_a(t)$. Define once again the error signals $\overline{e}_a(t)=\overline{x}_a(t)-x_a(t)$ and $\underline{e}_a(t)=x_a(t)-\underline{x}_a(t)$.

Theorem 4. *Let Assumptions 1-3 be satisfied. Then we have, for* (4) *and* (14)*,*

$$\underline{x}_a(t)\leq x_a(t)\leq\overline{x}_a(t),\quad\forall t\geq 0,\tag{15}$$

provided that $\underline{x}_0\leq x_a(0)\leq\overline{x}_0$, and moreover the errors $\overline{e}_a,\underline{e}_a\in\mathcal{L}_\infty^n$.

The interval observer (14) answers Problem (i) for actuator attacks. Next, we consider the situation where $\overline{a}$, $\underline{a}$ are not initially known.

B. Estimation of $\underline{a}$ and $\overline{a}$

In this subsection, we denote by $x_a(t)=x_a(t,\xi_1,w_1,a)$ the solution of (4) and by $x_2(t)=x(t,\xi_2,w_2)$ any plausible state trajectory of the nominal model (1) such that Definition 2 holds. They satisfy the differential equations

$$\begin{aligned}\dot{x}_a(t)&=Ax_a(t)+w_1(t)+a(t),\\ \dot{x}_2(t)&=Ax_2(t)+w_2(t),\end{aligned}\tag{16}$$

for corresponding initial conditions $\xi_1,\xi_2\in[\underline{x}_0,\overline{x}_0]$, inputs $w_1,w_2\in\mathcal{L}_\infty^n$, $w_1(t),w_2(t)\in[\underline{w},\overline{w}]$ and outputs respectively $y_a(t,\xi_1,a,w_1)$ and $y(t,\xi_2,w_2)$. In addition, we make the following assumption to construct a framer for a.

Assumption 5. *In (4), the matrix $C=I_n$.*

Let $e(t)=x_2(t)-x_a(t)$. For $C=I_n$, the constraint of Definition 2 imposes

$$\dot{e}(t)\ =\ 0.\tag{17}$$

Therefore, we have $e(t)=\xi_2-\xi_1$, $\forall t\geq 0$. As a result, e satisfies

$$\underline{e}\leq e(t)\leq\overline{e},$$

with $\underline{e}:=\underline{x}_0-\overline{x}_0$, $\overline{e}:=\overline{x}_0-\underline{x}_0$. On the other hand, (16) implies

$$\dot{e}(t)=Ae(t)+w_2(t)-w_1(t)-a(t).$$

Since $\dot{e}=0$, we obtain

$$a(t)=Ae(t)+w_2(t)-w_1(t).\tag{18}$$

Theorem 5. *Let Assumptions 1, 2 and 5 be satisfied. Then, a stealthy actuator attack in the sense of Definition 2 must satisfy $\underline{a}\leq a(t)\leq\overline{a}$, $\forall t\geq 0$, where*

$$\begin{aligned}\underline{a}&=A^+\underline{e}-A^-\overline{e}+\underline{w}-\overline{w},\\ \overline{a}&=A^+\overline{e}-A^-\underline{e}+\overline{w}-\underline{w}.\end{aligned}\tag{19}$$

In addition, the attack signal $a(t)$ and the errors signals $\underline{\zeta}(t) = a(t) - \underline{a}$ and $\overline{\zeta}(t) = \overline{a} - a(t)$ belong to $\mathcal{L}_\infty^n$.

The bounds $\overline{a}, \underline{a}$ of Theorem 5 answer Problem (ii) for actuator attacks, under the additional Assumption 5.

V. Simulations

This section presents some simulation results illustrating the results of this paper. Consider a simplified version of a lateral model of the Boeing-767 aircraft [27], where the dynamics of the roll angle and the yaw rate are neglected. The matrices A and C are defined as follows

$$A = \begin{bmatrix} -0.1245 & 0.035 \\ -15.2138 & -2.0587 \end{bmatrix}, \; C = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

and $x(t) = \begin{bmatrix} \beta(t) & p(t) \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$ where $\beta(t)$ represents the angle of sideslip (in degrees) and $p(t)$ the roll rate (in degrees per second), respectively. The unknown input signal is $w(t) = \begin{bmatrix} \delta_1 \sin(2t + \frac{\pi}{3}) & \delta_2 \cos(3t) \end{bmatrix}^{\mathrm{T}}$ with $\delta_1 = 3$ and $\delta_2 = 10$ two given bounds. Thus, we have $\overline{w}(t) = \begin{bmatrix} \delta_1 & \delta_2 \end{bmatrix}^{\mathrm{T}}$ and $\underline{w}(t) = -\overline{w}(t)$. Assumption 3 is verified for $L = \begin{bmatrix} 5 & -16 \end{bmatrix}^{\mathrm{T}}$, i.e., the matrix $A - LC = \begin{bmatrix} -5.1245 & 0.035 \\ 0.7862 & -2.0587 \end{bmatrix}$ is Hurwitz and Metzler. The (imperfectly known) initial condition is $x_a(0) = \begin{bmatrix} 30 & 30 \end{bmatrix}^{\mathrm{T}}$ and $\overline{x}_0 = \begin{bmatrix} 30 & 30 \end{bmatrix}^{\mathrm{T}}$, $\underline{x}_0 = \begin{bmatrix} 0 & 0 \end{bmatrix}^{\mathrm{T}}$.

Let us apply the stealthy sensor attack of Section III to the system. Since A is diagonalizable, Assumption 4 is satisfied with

$$S = \begin{bmatrix} 12.0519 & 0.2633 \\ 11.9886 & 1.2622 \end{bmatrix}, \; D = \begin{bmatrix} -0.4569 & 0 \\ 0 & -1.7263 \end{bmatrix}.$$

Fig. 1 illustrates the effects of a stealthy sensor attack. The solid blue line represents the true system state, and the dashed blue lines the state bounds provided by the interval observer (10) with the bounds $\underline{a}$, $\overline{a}$ provided by Theorem 3. For this simulation, we select $a(t) = y(t, x(0), w) - y(t, x_a(0), w)$. Note that another choice could be $a(t) = \frac{\underline{a}(t) + \overline{a}(t)}{2}$. The dashed red line are the bounds provided by the interval observer (8), which assumes that no attack is present. These bounds are clearly violated during the transient regime. On the other hand, the bounds assuming the presence of an attack signal are much more conservative, even in steady-state.

Let us consider now the actuator attack of Subsection IV-B. Note that $C = I_2$ for this case. Assumption 3 is verified for $L = \begin{bmatrix} 5 & 0 \\ -16 & 0 \end{bmatrix}$, i.e., the matrix $A - LC = \begin{bmatrix} -5.1245 & 0.035 \\ 0.7862 & -2.0587 \end{bmatrix}$ is Hurwitz and Metzler. In Fig. 2, the effects of such an actuator attack on the system are demonstrated, where the solid blue line represents the true system state, and the dashed blue lines the state bounds provided by the interval observer (14) with the bounds $\underline{a}$, $\overline{a}$ provided by Theorem 5. For this simulation, we select $a(t) = \frac{\underline{a}(t) + \overline{a}(t)}{2}$. The dashed red line are the bounds provided by the interval observer (8), which assumes that no attack is present. These bounds are clearly violated again in this case.

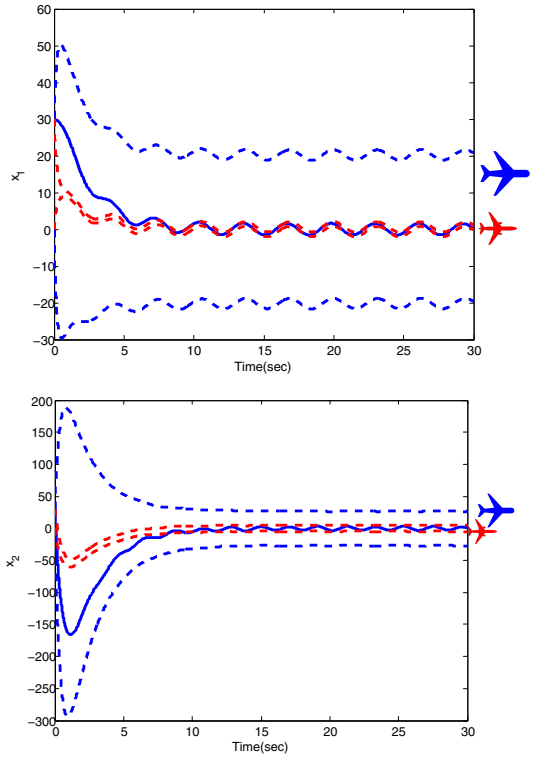

Fig. 1. Trajectory estimates without and under the stealthy sensor attack.

VI. Conclusion

In this paper, we consider the problem of state estimation under stealthy attacks in the interval observer framework. We construct framers for stealthy attack signals and we design interval observers for the state of the system under sensor and actuator attacks respectively. As a direction of future research, the problem of designing interval observers resilient to actuator attacks for the case where $C \neq I_n$ can be posed.

References

[1] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, Hong Kong, China, 2011, pp. 355–366.

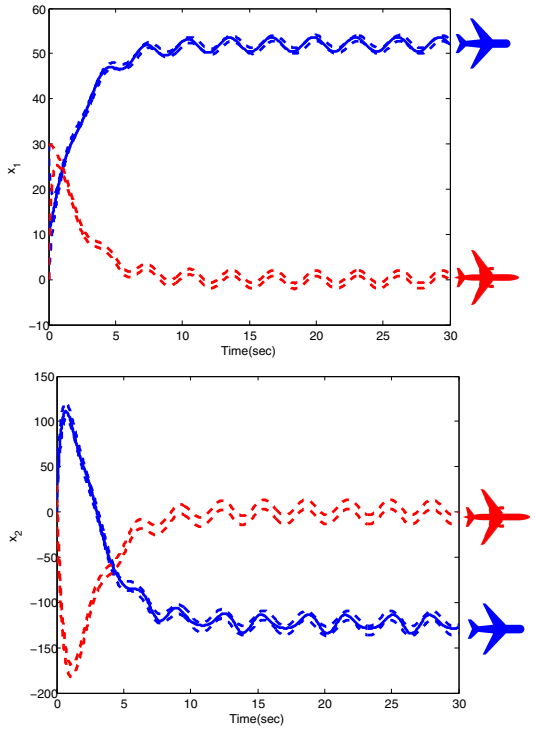

Fig. 2. Trajectory estimates without and under the stealthy actuator attack.

[2] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd Conference on Hot Topics in Security*, San Jose, CA, USA, 2008.

[3] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Drone hack," *GPS World*, vol. 23, no. 8, pp. 30–33, 2012.

[4] S. Peterson and P. Faramarzi, "Iran hijacked US drone, says iranian engineer," *The Christian Science Monitor*, vol. 15, Dec. 2011.

[5] A. Dutta and C. Langbort, "Stealthy output injection attacks on control systems with bounded variables," *International Journal of Control*, vol. 90, no. 7, pp. 1389–1402, 2017.

[6] A. Abur and A. G. Exposito, *Power system state estimation:Theory and implementation*. Boca Raton, FL: CRC Press, Mar. 2004.

[7] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems*, vol. 35, no. 1, pp. 93–109, Feb. 2015.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2009, pp. 21–32.

[9] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[10] A. Teixeira, D. György, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 11 271–11 277, 2011.

[11] Y.Chen, S. Kar, and J. M. F. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems," *IEEE Transactions on Control of Network Systems*, vol. PP, no. 99, pp. 1–1, 2017.

[12] V. Puig, F. Nejjari, P. Guerra, and S. Montes de Oca, "Robust fault detection for LPV systems using a consistency-based state estimation approach and zonotopes," in *Proc. of the 10th European Control Conference (ECC)*, Budapest, Hungary, Aug. 2009, pp. 3184–3189.

[13] K. H. Degue, D. Efimov, and J. Le Ny, "Interval observer approach to output stabilization of linear impulsive systems," in *Proc. of the 20th World Congress of the IFAC*, Toulouse, France, July 2017.

[14] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 46–65, Feb. 2015.

[15] M. Pourasghar, V. Puig, and C. Ocampo-Martinez, "Comparison of set-membership and interval observer approaches for state estimation of uncertain systems," in *Proc. of the 15th European Control Conference (ECC)*, Jun. 2016, pp. 1111–1116.

[16] F. Mazenc and O. Bernard, "Interval observers for linear time-invariant systems with disturbances," *Automatica*, vol. 47, no. 1, pp. 140–147, 2011.

[17] T. Raïssi, D. Efimov, and A. Zolghadri, "Interval state estimation for a class of nonlinear systems," *IEEE Trans. Automatic Control*, vol. 57, no. 1, pp. 260–265, 2012.

[18] K. H. Degue, D. Efimov, and J.-P. Richard, "Stabilization of linear impulsive systems under dwell-time constraints: Interval observer-based framework," *European Journal of Control*, vol. 42, pp. 1–14, Jul. 2018.

[19] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," *IEEE Control Systems*, vol. 37, no. 2, pp. 66–81, Apr. 2017.

[20] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[21] D. Efimov, L. Fridman, T. Raïssi, A. Zolghadri, and R. Seydou, "Interval estimation for LPV systems applying high order sliding mode techniques," *Automatica*, vol. 48, pp. 2365–2371, 2012.

[22] L. Farina and S. Rinaldi, *Positive Linear Systems: Theory and Applications*. New York: Wiley, 2000.

[23] H. Smith, *Monotone Dynamical Systems: An Introduction to the Theory of Competitive and Cooperative Systems*, ser. Surveys and Monographs. Providence: AMS, 1995, vol. 41.

[24] F. Mazenc and O. Bernard, "Asymptotically stable interval observers for planar systems with complex poles," *IEEE Transactions on Automatic Control*, vol. 55, no. 2, pp. 523–527, 2010.

[25] T. Raïssi, G. Videau, and A. Zolghadri, "Interval observers design for consistency checks of nonlinear continuous-time systems," *Automatica*, vol. 46, no. 3, pp. 518–527, 2010.

[26] D. Efimov, T. Raïssi, and A. Zolghadri, "Control of nonlinear and LPV systems: interval observer-based framework," *IEEE Trans. Automatic Control*, vol. 58, no. 3, pp. 773–782, 2013.

[27] T. I. Fossen, "Mathematical models for control of aircraft and satellites," Department of Engineering Cynernetics, Norwegian University of Science and Technology, Tech. Rep., Jan. 2011.