Secure interval observer for linear continuous-time systems with discrete measurements subject to cyber-attacks

Djahid Rabehi, Nacim Meslem, Nacim Ramdani

Secure interval observer for linear continuous-time systems with discrete measurements subject to cyber-attacks

Djahid Rabehi, Nacim Meslem and Nacim Ramdani

Abstract

This paper addresses the design of a secure interval state estimator for linear continuous-time systems in the bounded error context with discrete-time measurements subject to external attacks. The attacker capabilities are assumed limited in the sense that only a subset of all the sensors can be attacked although this subset is unknown. For a given upper bound on the number of attacked sensors, we propose *a new selection strategy*, which is able to achieve resiliency to attacks, using the width of estimated intervals. The interval observer is modelled as an impulsive system, where impulsive corrections are made periodically using measurement. The nonnegativity of the observation error between two successive measurements is preserved by applying the internal positivity of the system. The theoretical result is supported by numerical simulations.

Index Terms

Secure estimation, Interval observers, LTI systems, sparse output measurements, cyber-physical systems.

I. Introduction

Cyber-physical systems (CPS) are integrations of computation, networking, and physical processes [1]. Due to the cyber-physical coupling and to the disrupting consequences of failures, security here is one of the primary concerns [2]. The problem of security is not new to the control systems field, particularly in the area of fault detection and identification (FDI) [3]. Recent works on the cyber security of control systems have been focused, in part, on the effect of specific types of attacks on stability and/or estimation, such that false data injection attacks [4], denial-of-service attacks [5] and integrity attacks [6], or, in general, to any adversarial attacks [7], [8], which is the case of our work.

This paper addresses the design of an interval state observer, in a sense to be defined later, for a linear time-invariant plant in presence of periodic discrete measurements affected by unknown-but-bounded noise with known bounds and subject to cyber-attacks (probably unbounded).

Interval observers are guaranteed state estimators in the sense that the existence of a solution can be verified and no solution can be lost. These observers have been introduced in [9] for continuous-time systems and extended to several classes of systems under the bounded-error framework (see the survey [10]). Basically, interval observers compute trajectory tubes that are proven to contain the plant state trajectory while taking into account all uncertainties and disturbances acting on the plant and the measurements. The design of interval observers must ensure by construction the nonnegativity of the estimation error and its stability as well.

To be able to reconstruct a guaranteed state enclosure of the actual state for continuous-time linear systems in presence of discrete-time measurement, we propose an *interval impulsive observer*. The impulsive behavior is the result of the discrete nature of the measurements. In between two consecutive

D. Rabehi, A and N. Ramdani are with the Université d'Orléans, INSA CVL, PRISME, EA 4229, F-45072 Orléans, France. {djahid.rabehi,nacim.ramdani}@univ-orleans.fr

N. Meslem is with the Université de Grenoble Alpes, CNRS, GIPSA-lab, F-38000 Grenoble, France. nacim.meslem@grenoble-inp.fr

measurement instants, the observer behaves as a predictor based only on the evolution model. Then, at the measurement instant, an impulsive correction adjusts the interval estimate.

The assumed scenario in this paper considers a continuous LTI system with $\mathbf{s}$ outputs, each measured by a potentially attacked sensor, under the assumption that only a subset S of $\mathbf{s_a}$ sensors are attacked such that $\mathbf{s} > 2\mathbf{s_a}$. This condition is issued from the *M-observability* [8] and the *s-sparse observability* [11]. Based on this assumption, at correction times, we provide as many interval estimates as sensors, then we select the attack-free estimate by a proposed attack-resilient strategy using interval analysis and the positivity of the interval estimation error. The proposed strategy is an *online* algorithm while the synthesis procedure that tunes the observation gain to ensure both positivity and stability of the estimation error is *offline*. The stability analysis of the estimation error is inspired by the work [12] while the positivity of the estimation error is ensured based on the internal positivity for dynamical systems as in [13], [14] with taking into account the attack influence. Then, the effect of the attacks is treated by an online set-membership strategy.

The *novelty* of this paper is twofold: First, a new LMI-design methodology of the observer gain in presence of discrete-time measurements is proposed, that guarantees both positivity and stability of the interval estimation error. Second, a new sensor attack-resilient strategy that selects online at measurements times the correct estimate among a set of estimates from the set of sensors under attacks.

The paper is organized as follows. Preliminaries are given in Section II. The investigated problem is stated in Section III. The structure of the proposed interval impulsive observer is introduced in Section IV. The observer design method is presented in Section V. The attack-resilient strategy is detailed in Section VI. Numerical illustrative examples are presented in Section VII.

II. Preliminaries

The set $\mathbb{R}$, $\mathbb{R}_{\geq}$ and $\mathbb{N}$ are the set of real scalars, positive real scalars and nonnegative integers including zero, respectively. The induced matrix norm for a matrix $A \in \mathbb{R}^{n\times n}$ will be denoted as $||\cdot||$. Any $p \times m$ matrix whose elements are all ones or zeros are simply denoted by $\mathbb{1}_{p,m}$ or $\mathbf{0}$, respectively. I_p denotes the identity matrix in $\mathbb{R}^{p\times p}$. Throughout this paper the inequality $A \geq B$ must be understood element-wise, for matrices as well as for vectors. $M = \max\{A,B\}$ is the matrix where each entry is $m_{i,j} = \max\{a_{i,j}, b_{i,j}\}$. Let us define $A^+ = \max\{A, \mathbf{0}\}$, $A^- = A^+ - A$; thus, $|A| = A^+ + A^-$ denotes the element-wise absolute value matrix. A matrix $M \in \mathbb{R}^{n\times n}$ is said to be Metzler if all its off-diagonal entries are nonnegative. A matrix M is an M-matrix if all of its off-diagonal elements are nonpositive and all of its diagonal elements are positive. A matrix $P \in \mathbb{R}^{n\times n}$ is said to be negative definite if $\upsilon^T P \upsilon < 0 \ \forall \upsilon \in \mathbb{R}^n \setminus \{0\}$ and it is denoted by $P \prec 0$. The distance of $x \in \mathbb{R}^n$ to the closed set $\mathscr{A} \subset \mathbb{R}^n$ is denoted as $|x|_{\mathscr{A}}$ and is defined by $|x|_{\mathscr{A}} := \inf_{y\in\mathscr{A}} |x-y|$. If $\mathscr{I}$ is a set, $card\{\mathscr{I}\}$ is the cardinality of $\mathscr{S}$. For two vectors $x_1, x_2 \in \mathbb{R}^n$ such that $x_1 \leq x_2$, the interval $\mathbf{int}(x_1, x_2)$ is the set of admissible values bounded by the vectors x_1 and x_2.

A. Definitions

A function $\alpha : \mathbb{R}_{\geq} \to \mathbb{R}_{\geq}$ belongs to class-$\mathscr{K}$ ($\alpha \in \mathscr{K}$) if it is continuous, zero at zero, and strictly increasing. It belongs to class-$\mathscr{K}_\infty$ ($\alpha \in \mathscr{K}_\infty$) if, in addition, it is unbounded. A function $\beta : \mathbb{R}_{\geq} \times \mathbb{R}_{\geq} \to \mathbb{R}_{\geq}$ belongs to class-$\mathscr{KL}$ ($\beta \in \mathscr{KL}$) if it satisfies: (i) for each $t \geq 0$, $\beta(\cdot, t)$ is non-decreasing and $\lim_{s\searrow 0} \beta(s,t) = 0$, and (ii) for each $s \geq 0$, $\beta(s,\cdot)$ is non-increasing and $\lim_{t\to\infty} \beta(s,t) = 0$.

In this paper we model the impulsive behaviour of the estimation error as a hybrid system. We consider the following formalism of hybrid systems introduced in [15]

$$\dot{x} = \mathscr{F}(x) \quad x \in \mathscr{C}, \quad x^+ = \mathscr{G}(x) \quad x \in \mathscr{D}, \tag{1}$$

where $x \in \mathbb{R}^n$ is the state. $\mathscr{F}$, $\mathscr{C}$, $\mathscr{G}$ and $\mathscr{D}$ are the *flow map*, the *flow set*, the *jump map* and the *jump set*, respectively. $\mathscr{F}$ and $\mathscr{C}$ are supposed to be continuous, $\mathscr{G}$ and $\mathscr{D}$ are closed sets. The solutions to system (1) are defined on so-called hybrid time domains.

Definition 1 (Cooperative dynamics)**.** A continuous-time linear system $\dot{x}(t) = Ax(t)$ (discrete-time linear system $x(t+1) = Ax(t)$), with the state $x \in \mathbb{R}^n$ and $A \in \mathbb{R}^{n\times n}$, is said to be cooperative if A is a Metzler (Nonnegative) matrix.

The solutions of cooperative autonomous systems, initiated at $x(t_0) \geq 0$, stay nonnegative: $x(t) \geq 0$ for all $t \geq t_0$.

III. Problem statement

Consider the multi-output linear time invariant system of the form

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) & \forall t \in [t_k, t_{k+1}] \\ y_\sigma(t_k) = C_\sigma x(t_k) + v_\sigma(t_k) + a_\sigma(t_k), & \forall k \in \mathbb{N}, \sigma \in \mathscr{I} \end{cases} \tag{2}$$

where $\mathscr{I} = \{1, \ldots, \mathbf{s}\}$ such that $\mathbf{s}$ is the number of sensors. $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$ and $y_\sigma \in \mathbb{R}$ is the state variables, the input, the discrete output of the system, respectively. $v_\sigma \in \mathbb{R}$ and $a_\sigma \in \mathbb{R}$ represent the output sensor noise and sensor attack, respectively. The goal is to provide a secure estimate of the system state from noisy discrete measurements and under sensors attack. To reach this objective, we propose a two-stage policy:

a) First: We design an interval impulsive observer for each output y_σ separately with $\sigma \in \mathscr{I}$ in the absence of attacks. To simplify notation we drop the subscript σ in this section and the next one. So, the system (2) without attack will be in the following form

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t_k) = Cx(t_k) + v(t_k), \end{cases} \quad \forall t \in [t_k, t_{k+1}]\ k \in \mathbb{N}, \tag{3}$$

In this step, we design as many observers as outputs.

b) Second: After designing observers for every output without attack, we propose a strategy based on interval analysis to recover the state estimate against the sensors attacks in (2) based on the following assumption.

Assumption 1. *The number of attacked sensors denoted by* $\mathbf{s_a}$ *is strictly lower than the half of the total number of sensors* $\mathbf{s}$ *without knowing which sensors are attacked (i.e.,* $\mathbf{s_a} < \mathbf{s}/\mathbf{2}$*).*

This assumption is the main condition for the *M-observability* for continuous-time systems [8] and *s-sparse observability* for discrete-time systems [11].

IV. Interval impulsive observer analysis

The observer is constructed to estimate the continuous state of the system from discrete measurements. To this aim, it is assumed that there exists a constant period of time between two consecutive measurement instants as follows.

Assumption 2. *Let* τ_m *be a real positive scalars satisfying*

$$t_{k+1} - t_k = \tau_m \ \forall k \in \mathbb{N}.$$

The goal of interval observers is to estimate an upper and a lower bound of the system state while ensuring the convergence of the estimation error. To do so, let first introduce an assumption on the boundedness of the measurement noise.

Assumption 3. *Let* $\bar{v} \in \mathbb{R}$ *be a given positive constant such that*

$$|v(t)| \leq \bar{v} \ \forall t \in \mathbb{R}_{\geq}.$$

The interval observer that we propose for system (3) works with two steps;

First step: the interval observer in-between two successive measurement instants behaves like an open-loop estimator as follows

$$\begin{cases} \dot{\underline{x}}(t) = A^M \underline{x}(t) - A^N \overline{x}(t) + Bu(t), \\ \dot{\overline{x}}(t) = A^M \overline{x}(t) - A^N \underline{x}(t) + Bu(t) \end{cases} \quad \forall t \in [t_k, t_{k+1}], k \in \mathbb{N} \tag{4}$$

where $A^M = d_A + (A - d_A)^+$ and $A^N = A^M - A$ with d_A is a diagonal matrix contains only the diagonal elements of A. In addition, the interval observer initial state at $k = 0$, i.e. at t_0, satisfies the inclusion

$$\underline{x}(t_0) \leq x(t_0) \leq \overline{x}(t_0). \tag{5}$$

The estimation errors dynamics over the inter-measurement time for both bounds $\underline{e}(t) = x(t) - \underline{x}(t)$ and $\overline{e}(t) = \overline{x}(t) - x(t)$ can be obtained from equations (3) and (4) by

$$\begin{bmatrix} \dot{\underline{e}}(t) \\ \dot{\overline{e}}(t) \end{bmatrix} = \overline{A} \begin{bmatrix} \underline{e}(t) \\ \overline{e}(t) \end{bmatrix}, \forall t \in [t_k, t_{k+1}] \; k \in \mathbb{N} \tag{6}$$

with $\overline{A} = \begin{bmatrix} A^M & A^N \\ A^N & A^M \end{bmatrix}$.

Note that, based on the construction of the matrices A^M and A^N as Metzler and nonnegative matrices, respectively, the matrix $\overline{A}$ is Metzler. Then, the solution to (6) is nonnegative which means that the lower and the upper bounds do not cross each other in the time interval $[t_k, t_{k+1}]$ provided that their initial conditions satisfy the inclusion $\underline{x}(t_k) \leq x(t_k) \leq \overline{x}(t_k)$.

Second step: using the output model in (3), the system state at the measurement time instants can be presented as

$$x(t_k^+) = x(t_k) + L^\bullet [Cx(t_k) + v(t_k) - y(t_k)] \quad k \in \mathbb{N} \tag{7}$$

with $L^\bullet \in \{\underline{L}, \overline{L}\}$, where $\underline{L},\ \overline{L} \in \mathbb{R}^{n \times 1}$ are observer gains to be designed for the lower and upper bound estimate, respectively.

Equation (7) helps establishing the discrete-time dynamics of the estimation error which is used only for synthesis phase. When the measurement is available, an impulsive correction of the estimated state enclosures will be done using the following correction equations

$$k \in \mathbb{N}, \quad \begin{cases} \underline{x}(t_k^+) = (I_n + \underline{L}C)^+ \underline{x}(t_k) - (I_n + \underline{L}C)^- \overline{x}(t_k) \\ \qquad\qquad - |\underline{L}| \overline{v} - \underline{L} y(t_k) \\ \overline{x}(t_k^+) = (I_n + \overline{L}C)^+ \overline{x}(t_k) - (I_n + \overline{L}C)^- \underline{x}(t_k) \\ \qquad\qquad + |\overline{L}| \overline{v} - \overline{L} y(t_k) \end{cases} \tag{8}$$

From (8) and (7), the estimation error dynamics at measurement instants can be described by the following dynamical system

$$\begin{bmatrix} \underline{e}(t_k^+) \\ \overline{e}(t_k^+) \end{bmatrix} = \Gamma(\underline{L}, \overline{L}) \begin{bmatrix} \underline{e}(t_k) \\ \overline{e}(t_k) \end{bmatrix} + \Upsilon(t_k) \tag{9}$$

where $\Gamma(\underline{L}, \overline{L}) = \begin{bmatrix} (I_n + \underline{L}C)^+ & (I_n + \underline{L}C)^- \\ (I_n + \overline{L}C)^- & (I_n + \overline{L}C)^+ \end{bmatrix}; \Upsilon(t_k) = \begin{bmatrix} |\underline{L}| \overline{v} + \underline{L} v(t_k) \\ |\overline{L}| \overline{v} - \overline{L} v(t_k) \end{bmatrix}$. The positivity property of the reset matrix allows to preserve the order relation $\underline{x}(t) \leq x(t) \leq \overline{x}(t)$ after experiencing the reset (for more details about IPR for linear systems, see [14]).

Let us now consider the augmented vector of the interval estimation error as $\xi = [\underline{e}^\top, \overline{e}^\top]^\top$. From equations (6) and (9), and after adding the time variable τ, the hybrid system modeling the dynamics of the estimation error is given by

$$\mathscr{H}: \begin{cases} f(z) = \begin{bmatrix} \overline{A}\xi \\ -1 \end{bmatrix} & \forall z \in \mathscr{C} \\ g(z) = \begin{bmatrix} \Gamma(\underline{L}, \overline{L})\xi + \Upsilon(t_k) \\ \tau_m \end{bmatrix} & \forall z \in \mathscr{D} \end{cases} \tag{10}$$

where $z = [\xi^\top, \tau]^\top$ is the state variable of the hybrid system, τ_m is the reset value of the timer based on Assumption 2.

The flow and jump sets are defined as

$$\begin{aligned} \mathscr{C} &= \left\{ (\xi, \tau) \in \mathbb{R}^{2n} \times \mathbb{R}_{\geq} \quad | \quad \tau \in [0, \tau_m] \right\} \\ \mathscr{D} &= \left\{ (\xi, \tau) \in \mathbb{R}^{2n} \times \mathbb{R}_{\geq} \quad | \quad \tau = 0 \right\}. \end{aligned} \tag{11}$$

It is worth noting that these sets do not force the system to jump until the timer violates the zero, then after the jump, the timer τ is reset to τ_m.

The convergence of the variable z will make use of the notion of distance to a set. Thus, with mild conditions, the stability analysis is straightforward under the hybrid system framework [15].

Let us define the closed set $\mathscr{A}$ that contains all admissible values for the timer when the $\xi-$system state is at the origin

$$\mathscr{A} = \left\{ z = (\xi, \tau) \in \mathbb{R}^{2n} \times \mathbb{R}_{\geq} \quad | \quad \xi = 0, \tau \in [0, \tau_m] \right\}. \tag{12}$$

Remark 1. The hybrid system (10) can be considered for the case of perfect measurement by omitting the term $\Upsilon(t_k)$.

We characterize the domain of solutions of (10) when $\Upsilon(t_k) = 0$. Indeed, the variable τ, acting as a timer, guarantees that for every initial condition $\phi(0,0) \in \mathscr{C} \cup \mathscr{D}$, the domain of every maximal solution ϕ to (10) when $\Upsilon(t_k) = 0$ can be written as follows:

$$\mathrm{dom}\phi = \bigcup_{j \in \mathbb{N}} ([t_j, t_{j+1}], j)$$

with $t_{j+1} - t_j = \tau_m, \quad \forall j \in \mathbb{N} \setminus \{0\}$. Furthermore, assuming $t_0 = 0$, the structure of the above hybrid time domain implies that for each $(t, j) \in \mathrm{dom}\phi$ we have $t \leq \tau_m(j+1)$. The latter relation will play a key role in establishing global exponential stability (GES) of the set $\mathscr{A}$ for hybrid system (10) when $\Upsilon(t_k) = \mathbf{0}$.

The idea of the stability proof in the following theorem is from [15, Proposition 3.29]. It allows for the Lyapunov function to increase locally, then, this increase is compensated by instantaneous decrease at jumps which renders the overall hybrid dynamics stable.

Theorem 1. *Let Assumption 2 and 3 hold. For given gain matrices* $\underline{L}$, $\overline{L} \in \mathbb{R}^{n \times 1}$, *if there exists a symmetric positive definite matrix* $P \in \mathbb{R}^{2n \times 2n}$ *such that*

$$\Gamma(\underline{L}, \overline{L})^\top e^{\overline{A}^\top \tau_m} P e^{\overline{A} \tau_m} \Gamma(\underline{L}, \overline{L}) - P \prec 0 \tag{13}$$

is satisfied, then the hybrid system (10)-(11) *is Input-to-State-Stable (ISS) with respect to the set* $\mathscr{A}$ *defined in* (12). *Thus, the system defined by Eq.* (4) *and* (8) *is an interval observer for the system* (3) *with ISS estimation error relatively to* $\mathscr{A}$ *provided that* $\underline{x}(t_0) \leq x(t_0) \leq \overline{x}(t_0)$. *Moreover, if* $v(t_k) = 0 \ \forall k \in \mathbb{N}$ *in* (3), *then the interval observer defined by Eq.* (4) *and* (8) *for the system* (3) *has a globally exponentially stable (GES) estimation error relatively to* $\mathscr{A}$.

The proof has been omitted due to lack of space.

Remark 2. A necessary condition on the existence of observers for the system (3) is the observability of the pair $(e^{A\tau_m}, Ce^{A\tau_m})$. More details can be found in [16].

So far, a verification method has been given. The synthesis of the observation gains $\underline{L}$, $\overline{L}$ cannot be achieved using convex solvers (CS) due to the decomposition of $(I_n + L^{\bullet}C)$. However, using the positive realization of these matrices, the synthesis is still possible using CS. In the following section, we propose a synthesis methodology.

V. Synthesis method

In this section, we propose a new design methodology as second contribution of this paper. We will show how to design the observer gain based on positive system theory.

A. Positive realization based synthesis

Let us now re-consider the generic reset equation of the system state at measurement instant in (7). By introducing $\underline{G} = [I + \underline{L}C]$ and $\overline{G} = [I + \overline{L}C]$, we can rewrite

$$\begin{aligned} x(t_k^+) &= G^{\bullet}x(t_k) + L^{\bullet}[v(t_k) - y(t_k)] \\ &= (G^{\bullet +} - G^{\bullet -})x(t_k) + L^{\bullet}[v(t_k) - y(t_k)] \quad k \in \mathbb{N} \end{aligned} \tag{14}$$

where $G^{\bullet +}$ and $-G^{\bullet -}$ are the positive and the negative part of the matrix $G^{\bullet} \in \{\underline{G},\ \overline{G}\}$, respectively.

Let us note that for any positive matrices $\underline{G}_p,\ \underline{G}_n,\ \overline{G}_p,\ \overline{G}_n \in \mathbb{R}^{n\times n}_{\geq}$ satisfying $\underline{G} = \underline{G}_p - \underline{G}_n$ and $\overline{G} = \overline{G}_p - \overline{G}_n$ there exist $\underline{\Delta},\ \overline{\Delta} \in \mathbb{R}^{n\times n}_{\geq}$ such that

$$G^{\bullet} = (G^{\bullet +} + \Delta^{\bullet}) - (G^{\bullet -} + \Delta^{\bullet}) \tag{15}$$

that is, the matrices $G_p^{\bullet}$ and $G_n^{\bullet}$ are any positive realization of the matrices $G^{\bullet +}$ and $G^{\bullet -}$, respectively. Under the positive realization of the reset matrix G, the reset equation of the estimation error (9) can be generalized by the following difference equation

$$\begin{bmatrix} \underline{e}(t_k^+) \\ \overline{e}(t_k^+) \end{bmatrix} = \Gamma(G_p^{\bullet}, G_n^{\bullet}) \begin{bmatrix} \underline{e}(t_k) \\ \overline{e}(t_k) \end{bmatrix} + \Upsilon(t_k) \tag{16}$$

where $\Gamma(G_p^{\bullet}, G_n^{\bullet}) = \begin{bmatrix} \underline{G}_p & \underline{G}_n \\ \overline{G}_n & \overline{G}_p \end{bmatrix}$

Therefore, the idea for the synthesis is to calculate numerically the positive matrices $G_p^{\bullet}$ and $G_n^{\bullet}$ that satisfy the stability conditions. Then, one can compute directly the matrices $G^{\bullet +}$ and $G^{\bullet -}$ from the relation $G^{\bullet} = G_p^{\bullet} - G_n^{\bullet}$.

Using $\Gamma(G_p^{\bullet}, G_n^{\bullet})$ instead of $\Gamma(\underline{L}, \overline{L})$ in inequality (13), the gain synthesis can now be performed by finding solution $\{P, \underline{G}_p, \underline{G}_n, \overline{G}_p, \overline{G}_n, \underline{L},\ \overline{L},\}$ to the following feasibility problem

$$\Phi(P, G_p^{\bullet}, G_n^{\bullet}) \prec 0, \tag{17a}$$
$$I_n + \underline{L}C = \underline{G}_p - \underline{G}_n, \tag{17b}$$
$$I_n + \overline{L}C = \overline{G}_p - \overline{G}_n, \tag{17c}$$
$$\underline{G}_p \geq 0,\ \underline{G}_n \geq 0, \tag{17d}$$
$$\overline{G}_p \geq 0,\ \overline{G}_n \geq 0, \tag{17e}$$
$$P \succ 0 \tag{17f}$$

where $\Phi(P, G_p^{\bullet}, G_n^{\bullet}) = \Gamma(G_p^{\bullet}, G_n^{\bullet})^{\top} e^{\overline{A}^{\top}\tau_m} P e^{\overline{A}\tau_m} \Gamma(G_p^{\bullet}, G_n^{\bullet}) - P$. From equation (15) and based on the definition of the positive matrices $G^{\bullet +}$ and $G^{\bullet -}$ and their positive realization $G_p^{\bullet}$ and $G_n^{\bullet}$, respectively, the reset

equation (16) can be seen as a positive discrete time system whose state matrix is perturbed by a nonnegative matrix as follows

$$\Gamma(G_p^\bullet, G_n^\bullet) = \Gamma(\underline{L}, \overline{L}) + \begin{bmatrix} \underline{\Delta} & \underline{\Delta} \\ \overline{\Delta} & \overline{\Delta} \end{bmatrix} \tag{18}$$

Remark 3. Since the matrices $\Delta^\bullet$ are nonnegative which implies that $\begin{bmatrix} \underline{\Delta} & \underline{\Delta} \\ \overline{\Delta} & \overline{\Delta} \end{bmatrix}$ is also nonnegative, it is always possible to enhance the interval observer dynamics at jumps in (16) by reducing the matrix $\Gamma(G_p^\bullet, G_n^\bullet)$ in (18) to its optimal realization $\Gamma(\underline{L}, \overline{L})$.

B. Design procedure

The semi-definite programming (SDP) (17) is subjected to a Nonlinear Matrix inequality, which is hard to solve. The constraint $\Phi \prec 0$ can be relaxed to a Linear Matrix Inequality (LMI) in the following Corollary. This relaxed constraints rely also on M-matrices which have inverses that are nonnegative matrices [17, Chapter 6].

Corollary 2. *Let Assumption 2 and 3 hold. If there exist nonnegative matrices* $\underline{U}_p, \underline{U}_n, \overline{U}_p, \overline{U}_n \in \mathbb{R}^{n\times n}$, *M-matrices* $F_1, F_2 \in \mathbb{R}^{2n\times 2n}$ *and two matrices* $\underline{X}, \overline{X} \in \mathbb{R}^{n\times 1}$ *such that the constraints*

$$\begin{bmatrix} e^{\overline{A}^\top \tau_m} P e^{\overline{A}\tau_m} - F - F^\top & U \\ \star & -P \end{bmatrix} \prec 0\,, \tag{19a}$$

$$F_1 + \underline{X}C = \underline{U}_p - \underline{U}_n\,, \tag{19b}$$

$$F_2 + \overline{X}C = \overline{U}_p - \overline{U}_n\,, \tag{19c}$$

with $U = \begin{bmatrix} \underline{U}_p & \underline{U}_n \\ \overline{U}_n & \overline{U}_p \end{bmatrix}$, $F = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix}$, *are feasible, then the interval observer of the form* (4), (5) *and* (8) *with gains* $\underline{L} = F_1^{-1}\underline{X}$, $\overline{L} = F_2^{-1}\overline{X}$ *for the system (resp. noise-free system)* (3) *has an ISS (resp. a GES) estimation error w.r.t. the set* $\mathscr{A}$.

The proof has been omitted due to lack of space.

VI. Online observer selection strategy

So far, we have designed an interval observer for each sensor under the assumption of attack-free sensors. Now, we return to the initial problem where an unknown subset of sensors in (2) are under attack. This subset is defined as $S \subset \mathscr{I}$ with $\text{card}(S) = \mathbf{s_a}$. The complement set of S relatively to $\mathscr{I}$ is $S^c = \mathscr{I} \setminus S$ such that $a_\sigma(t_k) = \mathbf{0}$ if $\sigma \in S^c$. Based on this assumption, there exist at least $\mathbf{s} - \mathbf{s_a}$ attack-free sensors that can provide the correct estimate. The idea of the proposed selection strategy is from $\mathbf{s}$ sensors select a combination of $\mathbf{s} - \mathbf{s_a}$ sensors and check their intersection using interval analysis. Thus, the number of combinations of sensors sets in which only one set contains attack-free sensors is $N_b = \binom{\mathbf{s}}{\mathbf{s}-\mathbf{s_a}}$.

Definition 2. A sensor attack a_σ is called distinguishable if the attacked estimates $(\underline{x}_\sigma^+(a_\sigma), \overline{x}_\sigma^+(a_\sigma))$ and the free-attack estimates $(\underline{x}_\sigma^+(a_{\sigma,0}), \overline{x}_\sigma^+(a_{\sigma,0}))$ satisfy

$$\mathbf{int}(\underline{x}_\sigma^+(a_\sigma), \overline{x}_\sigma^+(a_\sigma)) \cap \mathbf{int}(\underline{x}_\sigma^+(a_{\sigma,0}), \overline{x}_\sigma^+(a_{\sigma,0})) = \emptyset$$

where $a_\sigma \neq 0$ and $a_{\sigma,0} = 0$.

Remark 4. By nonnegativity argument of the interval estimation errors, the estimate enclosures from attack-free sensors always intersect. Based on Assumption 1, if there exist $\mathbf{s_a}$ attacked sensors with distinguishable attacks s.t. $\frac{\mathbf{s}}{2} - 1 \leq \mathbf{s_a} < \frac{\mathbf{s}}{2}$, then there exists only one set of $\mathbf{s} - \mathbf{s_a}$ free sensors whose all interval estimates

intersect. This makes the main idea of the proposed attack-resilient strategy in Algorithm 1. In the general case where the $\mathbf{s_a}$ sensors are not fully attacked, there exist at least one set of $\mathbf{s}-\mathbf{s_a}$ free sensors whose all interval estimates intersect.

Discussion of Algorithm 1: In this algorithm, we assume that all attacks are distinguishable. The algorithm receives corrections from $\mathbf{s}$ sensors. The combination of estimated intervals to be tested is calculated offline based on the knowledge of the number of attacked sensors $\mathbf{s_a}$. We define Σ as the family of sets $S^c \subset \mathscr{I}$ such that $\text{card}(S^c) = \mathbf{s}-\mathbf{s_a}$.

For instance, If we have a system with $\mathbf{s}=\mathbf{5}$ sensors in which $\mathbf{s_a}=\mathbf{2}$ attacked sensors, then we have $\mathscr{I} = \{1,2,3,4,5\}$ and $N_b = 10$ combination of sets as $S^c \in \Sigma = \{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\},\{1,4,5\},\{2,3,4\},\{2,4,5\},\{2,3,5\},\{3,4,5\}\}$. Thus, there exists at least one set with attack-free sensors.

- In line 1 - line 6, we compute the intersection of interval estimates $(\underline{x}^+_\sigma, \overline{x}^+_\sigma) \;\; \forall \sigma \in S^c$. This procedure is repeated for each combination set $S^c \subset \mathscr{I}$ with $\text{card}(S^c) = \mathbf{s}-\mathbf{s_a}$ for a total of N_b combinations.
- In line 7, we select only sets whose estimates intersect by checking the $zero-$norm of the vector W_{S^c}. If any vector W_{S^c} has a zero element, then its $zero-$norm is less than n. Thus, its corresponding set S^c is excluded from $\Sigma_\cap$.
- In line 8, we select the set S^c which has the minimum of intersection of estimates. This step is only executed in the case when the actual number of attacked sensors is less than $\mathbf{s_a}$ which is only an upper bound on the number of attacked sensors. By recalling the above example, if the number of actual attacked sensors is exactly $\mathbf{s_a}=\mathbf{2}$, to illustrate let suppose that the set of attacked sensors is $S=\{1,2\}$, then the sets with attack-free sensor are only $S^c=\{3,4,5\}$. Hence, we have $\Sigma^*_\cap = \Sigma_\cap = S^c$. Contrariwise, if the set of attacked sensors is $S=\{1\}$, then the sets with attack-free sensor are $S^c \in \{\{2,3,4\},\{2,4,5\},\ \{2,3,5\},\{3,4,5\}\}$. In this case we need to find the best set by selecting the one with the minimum intersection.
- In line 9, we select the tightest estimate.

Algorithm 1: Selection Strategy for attack-free estimate

Input : Correction using $\mathbf{s}$ sensors $(\underline{x}^+_\sigma, \overline{x}^+_\sigma) = Jump(\underline{x}_\sigma, \overline{x}_\sigma) \quad \sigma \in \mathscr{I}$
Number of sensor combination N_b

Output: Selection of the attack-resilient correction $(\underline{x}^+_{\sigma^*}, \overline{x}^+_{\sigma^*})$

1 **for** $i=1$ **to** N_b **do**
2 $\quad S^c \in \Sigma$;
3 $\quad \overline{\pi}_{S^c} := \{\overline{x}^+_\sigma | \sigma \in S^c\}$;
4 $\quad \underline{\pi}_{S^c} := \{\underline{x}^+_\sigma | \sigma \in S^c\}$;
5 $\quad W_{S^c} := \max\left[\mathbf{0}, \min(\overline{\pi}_{\mathbf{S^c}}) - \max(\underline{\pi}_{\mathbf{S^c}})\right]$;
6 **end**
7 Define the sets of intersected estimates $\Sigma_\cap := \{S^c \in \Sigma \;:\; ||W_{S^c}||_0 = n \}$;
8 Select the set with minimum width of intersection $\Sigma^*_\cap$;
9 The best estimate $\sigma^* := \underset{\sigma \in S^c, S^c \in \Sigma^*_\cap}{\text{argmax}} \; ||W_{S^c} - (\overline{x}^+_\sigma - \underline{x}^+_\sigma)||_2$;

VII. Illustrative examples

In order to illustrate the performance of the proposed observer, we consider the following examples.

Example 1: Unmanned Ground Vehicle (UGV) system borrowed from [18] and [11]:

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\end{bmatrix} = \begin{bmatrix}0 & 1\\ 0 & -\frac{b}{m}\end{bmatrix}\begin{bmatrix}x_1\\ x_2\end{bmatrix} + \begin{bmatrix}0\\ \frac{1}{m}\end{bmatrix} F$$

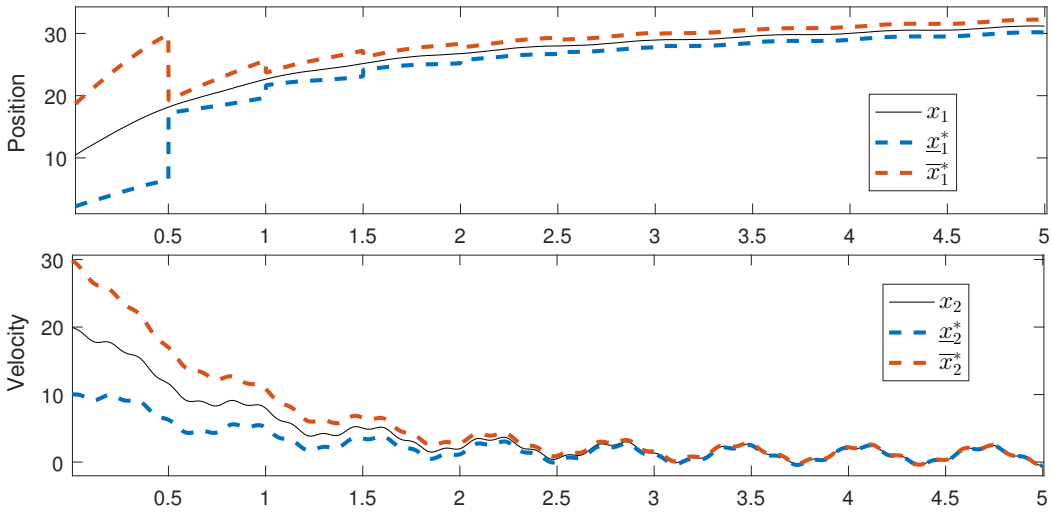

Figure 1. Simulation results for the UGV system: the attack-resilient estimate bounds for the position (top), and velocity (bottom).

where $x_1(t)$ and $x_2(t)$ are the UGV position and the linear velocity, respectively. m and b are the mechanical mass and the translational friction coefficient, respectively. The input to the UGV is the force F. The UGV is equipped with 3 GPS sensors, which measure its position in discrete times. The considered outputs are $\forall \sigma \in \mathscr{I} = \{1,2,3\}, \quad y_\sigma(t_k) = C_\sigma x(t_k) + v_\sigma(t_k) + a_\sigma(t_k)$, with $C_1 = C_2 = C_3 = [1 \quad 0]$, where $a_\sigma(t_k)$ are attack signals. $v_\sigma(t_k)$ are measurement noises. In our experiments, the parameters are specified as $m = 0.8$ and $b = 1$, the measurement period $t_{k+1} - t_k = \tau_m = 0.5$. We have the number of sensors $\mathbf{s} = card\{\mathscr{I}\} = 3$, thus the maximum attacked sensors is $\mathbf{s_a} = 1 < \frac{\mathbf{s}}{2}$.

The observability of the pairs $(e^{A\tau_m}, Ce^{A\tau_m}) \quad \forall \sigma \in \mathscr{I}$ are satisfied. To synthesize our set of interval observers, we solve the design problem in Corollary 2 only once due to the fact that $C = C_1 = C_2 = C_3$. The constraints (19) are solved using the YALMIP toolbox [19] based on the SDPT3 solver. The obtained observer gains are as follows $\underline{L}_1 = \underline{L}_2 = \underline{L}_3 = [-1 \quad 0.0006]^\top$ and $\overline{L}_1 = \overline{L}_2 = \overline{L}_3 = [-1 \quad 0.0002]^\top$.

The number of combinations is $N_b = 3$ with the sets of possible attacked sensors are $S \in \{\{1\},\{2\},\{3\}\}$ their complement are $S^c \in \{\{1,2\},\{2,3\},\{1,3\}\}$. In sets S^c there exists only one set with attack-free sensors. Our proposed selection strategy in Algorithm 1 selects the set S^c whose sensors provide the intersected interval estimates, then in the selected set, the best estimate is selected based on the criterion of line 9 in Algorithm 1.

For simulation, the output noise is $v_\sigma(t_k) = \cos(2t_k) \leq \bar{v}_\sigma = 1 \quad \forall \sigma$, and $F = 10(\sin(10t) + \cos(40t))$. The attack is simulated as $[a_1(t_k) \;\; a_2(t_k) \;\; a_3(t_k)]^\top = [0 \;\; 0 \;\; 0]^\top \forall t_k < 1.5s$ and $[a_1(t_k) \;\; a_2(t_k) \;\; a_3(t_k)]^\top = [0 \;\; 0 \;\; -20]^\top \forall t_k \geq 1.5s$

The simulation results are given in Figure 1 and 2. In Figure 1, the attack-free estimate bounds are selected by Algorithm 1, which guarantees the nonnegativity of the estimation errors. It is noticeable that the jump part of the interval impulsive observer contracts significantly the estimation errors comparing to the open-loop estimation. In Figure 2, it is shown how the attacked position estimate behaves comparing to the attack-resilient one.

The UGV systems in Example 1 is a cooperative system. In order to show the efficiency of the proposed method, we apply it on a non-cooperative system in the following.

Example 2: Academic system (Non-cooperative system) Let us consider the following system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} u$$

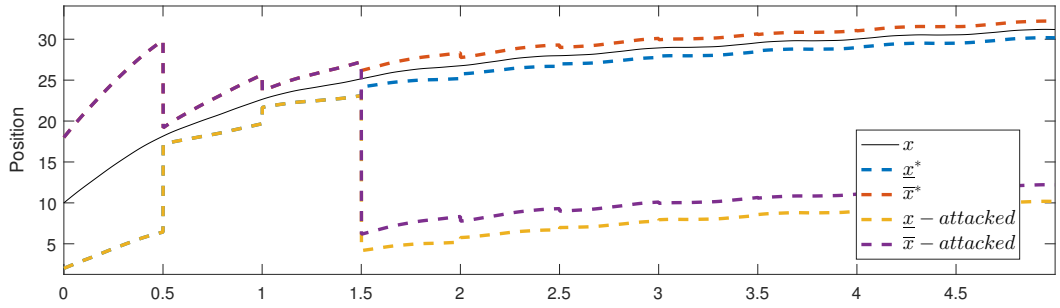

Figure 2. Position estimate bounds $(\cdot)^*$ selected by Algorithm 1 and the attacked position.

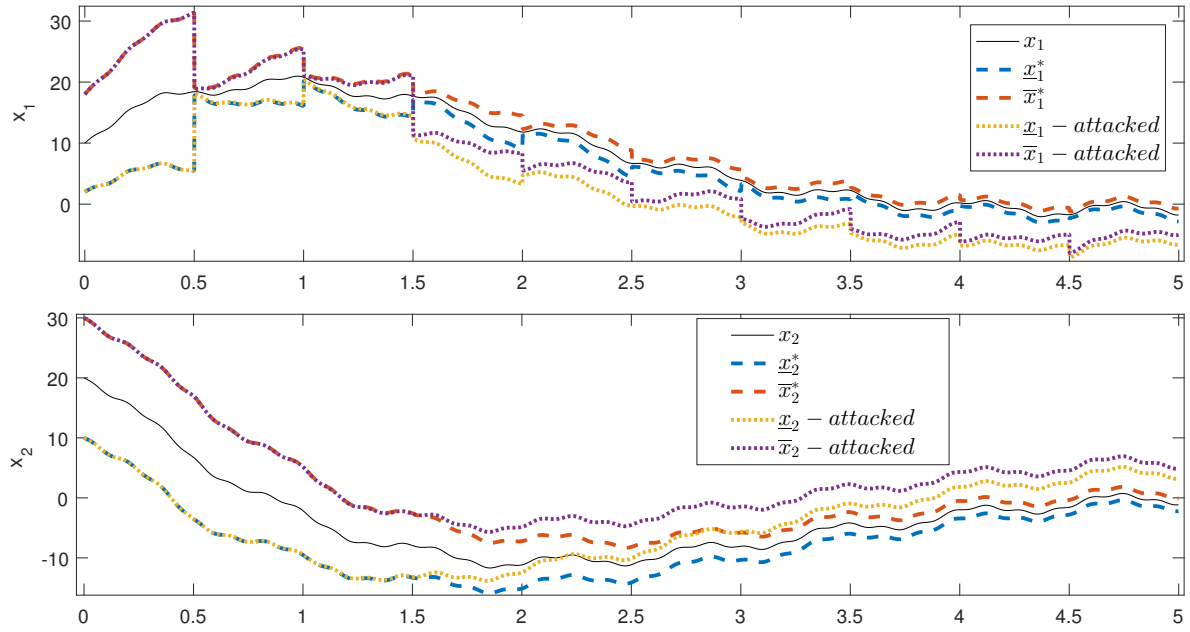

Figure 3. Simulation result for the academic system: the estimate bounds for the states x_1 (top) and x_2 (bottom), both attack-resilient estimate (dashed line) and attacked one (dotted line).

the outputs have the same form of (2) with $C_1 = [2 \quad 0]$, $C_2 = [1 \quad 0]$ and $C_3 = [3 \quad 0]$ which satisfy the observability condition in Remark 2. We solve the design problem in Corollary 2 for each output matrix ($\forall \sigma \in \mathscr{I}$) separately by picking $C = C_\sigma$. The designed observation gains are obtained as $\underline{L}_1 = \begin{bmatrix}-0.5 & 0.0004\end{bmatrix}^\top$, $\underline{L}_2 = \begin{bmatrix}-1 & 0.0007\end{bmatrix}^\top$, $\underline{L}_3 = \begin{bmatrix}-0.3333 & 0.0001\end{bmatrix}^\top$, $\overline{L}_1 = \begin{bmatrix}-0.5 & 0.0002\end{bmatrix}^\top$, $\overline{L}_2 = \begin{bmatrix}-1 & 0.0001\end{bmatrix}^\top$, $\overline{L}_3 = \begin{bmatrix}-0.3333 & 0.0002\end{bmatrix}^\top$. For brevity of presentation, we use the same condition of simulation of Example 1 with $u = F$. The simulation results are given in Figure 3. In Figure 3, it is clear that the observer whose sensor is under attack provides erroneous estimate bounds. On the other side, our proposed algorithm is able to provide correct estimate bounds from the set of sensors under cyber-attack.

VIII. Conclusions

In the paper, a new approach to design interval impulsive observers for linear continuous-time systems with discrete measurement has been introduced. Exploring the positivity of the interval estimation errors, a new strategy for sensor attack-resilient state estimation has been proposed. The synthesis of the observation gains is performed using LMIs. The proposed approach has relaxed the continuity assumption of

measurement in [8] while ensuring a continuous estimate. Simulation examples show the efficiency of the proposed secure estimation approach for a class of linear systems.

REFERENCES

[1] E. A. Lee and S. A. Seshia, *Introduction to embedded systems: A cyber-physical systems approach*. MIT Press, 2016.

[2] Y. Z. Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *Journal of Systems and Software*, vol. 149, pp. 174–216, 2019.

[3] M.-A. Massoumnia, G. C. Verghese, and A. S. Willsky, "Failure detection and identification," *IEEE transactions on automatic control*, vol. 34, no. 3, pp. 316–321, 1989.

[4] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans on Inform and Syst Security*, vol. 14, no. 1, p. 13, 2011.

[5] S. Amin, A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *HSCC*. Springer, 2009, pp. 31–45.

[6] Y. Mo, J. Hespanha, and B. Sinopoli, "Resilient detection in the presence of integrity attacks," *IEEE transactions on Signal Processing*, vol. 62, no. 1, pp. 31–43, 2014.

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

[8] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in *ACC*. IEEE, 2015, pp. 2439–2444.

[9] J. Gouzé, A. Rapaport, and Z. M. Hadj-Sadok, "Interval observers for uncertain biological systems," *Journal of Ecological Modelling*, vol. 133, pp. 45–56, 2000.

[10] D. Efimov and T. Raïssi, "Design of interval observers for uncertain dynamical systems," *Automation and Remote Control*, vol. 77, no. 2, pp. 191–225, 2016.

[11] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2079–2091, 2016.

[12] F. Ferrante, F. Gouaisbaut, R. G. Sanfelice, and S. Tarbouriech, "State estimation of linear systems in the presence of sporadic measurements," *Automatica*, vol. 73, pp. 101–109, 2016.

[13] N. Meslem and N. Ramdani, "Interval observer design based on nonlinear hybridization and practical stability analysis," *International Journal of Adaptive Control and Signal Processing*, vol. 25, no. 3, pp. 228–248, 2011.

[14] F. Cacace, A. Germani, and C. Manes, "A new approach to design interval observers for linear systems." *IEEE Trans. Automat. Contr.*, vol. 60, no. 6, pp. 1665–1670, 2015.

[15] R. Goebel, R. G. Sanfelice, and A. R. Teel, *Hybrid Dynamical Systems: modeling, stability, and robustness*. Princeton University Press, 2012.

[16] T. Raff and F. Allgower, "Observers with impulsive dynamical behavior for linear and nonlinear continuous-time systems," in *CDC*. IEEE, 2007, pp. 4287–4292.

[17] A. Berman and R. J. Plemmons, *Nonnegative matrices in the mathematical sciences*. SIAM, 1994, vol. 9.

[18] C.-H. Xie and G.-H. Yang, "Secure estimation for cyber-physical systems with adversarial attacks and unknown inputs: An L_2-gain method," *Int J Robust Nonlinear Control*, vol. 28, pp. 2131–2143, 2018.

[19] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. of the CACSD Conf.* IEEE, 2004, pp. 284–289.