Secure State Estimator for Uncertain Discrete-Time Linear Systems Based on Set-Valued Consistency Techniques

Nacim Meslem, Ahmad Hably, Nacim Ramdani

Secure State Estimator for Uncertain Discrete-Time Linear Systems Based on Set-Valued Consistency Techniques

Nacim Meslem and Ahmad Hably and Nacim Ramdani

***Abstract*— In a bounded error context, a secure set-valued state estimator for a class of systems described by a linear discrete-time difference inclusion is introduced in this contribution. The proposed design approach is based on set-valued computation combined with elimination by consistency techniques. More formally, we will show that a fusion between data provided by a set-valued predictor and those generated by a set-valued estimator allows one: (i) To obtain guaranteed state enclosures in the presence of additive and bounded state disturbance and measurement noise; (ii) To be able to detect faulty behaviors of the system and (iii) To be insensitive to a certain class of cyber-attacks. A numerical example is introduced to illustrate the performance of the proposed secure set-valued state estimator.**

I. Introduction

Security against malicious attacks is a crucial issue in nowaday networked and cyber-physical systems [24], [8], [26], [23], [5], [7], [14]. Cyber-physical systems refer to large platforms composed by an interconnection of physical entities, digital calculators and smart sensors. The interaction between these heterogeneous elements is made possible thanks to a communication network. In this context, several actuators are operated remotely by control laws computed from remotely collected data. Cyber-physical systems are used in industry as well as in the domestic and urban life (self-driving cars, etc.). As for a network of computers that could be attacked by viruses (malware), a cyber-physical system can be vulnerable due to its communication network. Indeed, a malicious attacker can unlawfully access and affect the system data that defines its desired behavior, which leads to degrade its performance. The consequence of a such interference could be fatal for the system safety. In fact, the corrupted data can be used to remotely operate the critical entities of the system, which could render the cyber-system completely unstable leading to explosion or disintegration. Some famous examples of cyber-attacks can be found in [12], [3], [11], [25].

This work aims at contributing to design novel state estimation strategies that are resilient against adversarial attacks, robust in the presence of process and measurement noise and are able to detect fault occurrences. Notice that, an attack can be defined as a discrete action taken by an agent and intended to significantly disrupt the normal behavior of the cyber-physical system without being detected by the classical monitoring system. Indeed, a typical characteristic of a cyber-attack is the concealment. That is, an attacker will tend to mask their intrusion by trying to mislead the supervision process of the cyber-physical system. For instance, by generating a faulty but plausible scenario of the system behavior. In this work, we will combine set-valued state estimation and prediction approaches [22], [19], [21] with consistency techniques to tackle the following key points in a bounded error context:

- Guarantee: Despite the presence of additive uncertainties, the objective is to provide reliable and bounded enclosures of the actual state vector of the considered class of dynamical systems.
- Fault detection: Based on set-membership tests, the occurrence of faults has to be detected and distinguished from cyber-attacks.
- Resilience: The designed set-valued estimator has to keep providing guaranteed state enclosure in the presence of adversarial attacks.
- Accuracy: Improve the tightness of the computed state enclosure by discarding inconsistent part between predicted and estimated data.

The remaining parts of this note are organized as follows. In Section II, first, we introduce the class of considered systems. Then, a set-valued predictor and a set-valued state estimator are presented, respectively. Section III is dedicated to introduce the main contribution of this work. The structure of the proposed algorithm is presented and its working principle is discussed. In addition, the performance of the introduced secure set-valued state estimator is illustrated in Section IV through a numerical example. Section V ends this paper with a conclusion and some perspectives.

II. Set-valued estimation

Consider the class of discrete-time systems whose dynamics can be described by the following difference inclusion

$$\begin{array}{lcl} \mathbf{x}_{k+1} & \in & \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \mathbf{E}\mathcal{W} \\ \mathbf{y}_k & \in & \mathbf{C}\mathbf{x}_k + \mathbf{F}\mathcal{V} \\ \mathbf{x}_0 & \in & \mathcal{X}_0 \end{array} \tag{1}$$

where $\mathbf{x}_k \in \mathbb{R}^{n_x}$, $\mathbf{u}_k \in \mathbb{R}^{n_u}$, $\mathbf{y}_k \in \mathbb{R}^{n_y}$ stand for the state vector, input vector and output of the system, respectively. The matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$, $\mathbf{E}$ and $\mathbf{F}$ are assumed constant with appropriate dimensions. The sets $\mathcal{W}$, $\mathcal{V}$ and $\mathcal{X}_0$ are assumed known a priori and defined as follows,

- $\mathcal{W}$ the feasible bounded set of the modeling error, which includes the state disturbances and process noise.
- $\mathcal{V}$ the feasible bounded set of the output error, which includes measurement noise and sensors inaccuracy.
- $\mathcal{X}_0$ the feasible bounded set of the initial state of the system. That is at $k = 0$.

Nacim Meslem and Ahamd Hably are with Univ. Grenoble Alpes, CNRS, Grenoble INP*, GIPSA-lab, Grenoble 38000, France, meslem.nacim@grenoble-inp.fr, ahmad.hably@grenoble-inp.fr

Nacim Ramdani is with University of Orléans, INSA Centre Val de Loire (CVL), PRISME, EA, 4229, Orléans, France nacim.ramdani@univ-orleans.fr

Unlike the classical point-valued state estimation approaches [16], [17], [10], set-valued methods [18], [4], [19], [20] aim at estimating a guaranteed enclosure of the actual state vector of the system without requiring any statistical property about the uncertain parts of the system. This objective is introduced more formally in the next subsection.

A. Objective

From a mathematical point of view, set-valued state estimation consists in characterizing outer approximations $\bar{\mathcal{X}}_k$ of the reachable sets $\mathcal{X}_k$ of the uncertain system (1) that are consistent with the available measurements. That is, we have to determine at each time instant k the following set:

$$\bar{\mathcal{X}}_k \supseteq \mathcal{X}_k = \left\{ \begin{array}{c} \mathbf{x}_k \mid \\ \textbf{Consistency with system dynamics} \\ \mathbf{x}_k = \mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{E}\mathbf{w}_{k-1}, \\ \mathbf{x}_{k-1} \in \mathcal{X}_{k-1} \\ \mathbf{w}_{k-1} \in \mathcal{W} \\ \text{and} \\ \textbf{Consistency with measurements} \\ \mathbf{C}\mathbf{x}_k \in \mathbf{y}_k^m - \mathbf{F}\mathcal{V} \end{array} \right\} \quad (2)$$

where $\mathbf{y}_k^m$ stands for the measured value of the system output at the time instant k. Moreover, set-valued state estimators have to guarantee the boundedness of the computed outer enclosure $\bar{\mathcal{X}}_k$ of the actual state vector $\mathbf{x}_k$.

B. Set-valued predictor

The state enclosure defined in (2) can be over-approximated without using measurement as stated in the following proposition.

Proposition 1: *[21] Let $\mathbf{b}_0 = \mathbf{B}\mathbf{u}_0$ and $\bar{\mathcal{F}}_0$ is a set satisfying $\bar{\mathcal{F}}_0 \supseteq \mathbf{E}\mathcal{W}$. Then, for all $k \geq 1$, the following set-valued predictor,*

$$\begin{array}{rcl} \bar{\mathcal{X}}_k^p & = & \mathbf{A}^k \bar{\mathcal{X}}_0 \oplus \bar{\mathcal{F}}_{k-1} + \mathbf{b}_{k-1} \\ \bar{\mathcal{F}}_k & = & \mathbf{A}^k \bar{\mathcal{F}}_0 \oplus \bar{\mathcal{F}}_{k-1} \\ \mathbf{b}_k & = & \mathbf{A}\mathbf{b}_{k-1} + \mathbf{B}\mathbf{u}_k, \end{array} \quad (3)$$

provides a tight over approximation of the reachable set of the uncertain discrete-time system (1)*. That is, $\forall \mathbf{w}_k \in \mathcal{W}$ and $\mathbf{x}_0 \in \mathcal{X}_0 \subseteq \bar{\mathcal{X}}_0$, the actual state vector of system* (1) *is inside the computed set $\bar{\mathcal{X}}_k^p$ ($\forall k \geq 0,\ \mathcal{X}_k \subseteq \bar{\mathcal{X}}_k^p$). Moreover, if $\mathbf{A}$ is a Schur stable matrix, the generated sets $\bar{\mathcal{X}}_k^p$ by* (3) *are bounded and their size is converging.*

Remark 1: Notice that, the symbol $\oplus$ used in (3) stands for the Minkowski sum between two sets. That is, the returned set by this operation is formed by adding each vector in the first set to each vector in the second set. ◦

Remark 2: In Proposition 1 and throughout the paper, by a size of a set we mean the largest distance between its center and its endpoints. Moreover, by convergence we mean that at the steady state, when k goes towards infinity, this size is lower than a given constant. ◦

Case of closed-loop systems: For the sake of simplicity, the proposed secure estimation strategy is presented in the case of open-loop linear systems. However, it is worth pointing out that, any closed-loop linear system with a measured state feedback control law,

$$\mathbf{u}_k = -\mathbf{K}\mathbf{x}_k^{mes} + \mathbf{H}\mathbf{y}_k^{ref} \quad (4)$$

where $\mathbf{K} \in \mathbb{R}^{n_u \times n_x}$ stand for the state feedback gain, $\mathbf{H} \in \mathbb{R}^{n_y \times n_u}$ is the pre-filter gain and the measured state vector $\mathbf{x}_k^{mes}$ satisfies

$$\mathbf{x}_k^{mes} \in \mathbf{x}_k \oplus \mathcal{V}^x \quad (5)$$

with $\mathcal{V}^x$ is the feasible set of the measurement error, can be also considered by Proposition (1). Indeed, it is straightforward to show the closed -loop dynamics can be written in the suitable form

$$\mathbf{x}_{k+1} \in \mathbf{A}_{cl}\mathbf{x}_k + \mathbf{B}_{cl}\mathbf{y}_k^{ref} + \mathbf{E}_{cl}\mathcal{W}_{cl} \quad (6)$$

where $\mathbf{A}_{cl} = \mathbf{A} - \mathbf{B}\mathbf{K}$, $\mathbf{B}_{cl} = \mathbf{B}\mathbf{H}$ and $\mathbf{E}_{cl} = [\mathbf{E},\ -\mathbf{B}\mathbf{K}]$. Notice that by $\mathcal{W}_{cl} = \{\mathcal{W}; \mathcal{V}^x\}$ one denotes a Cartesian set product in which the component $\mathcal{V}^x$ is related to the measurement error introduced in (5). Thus, in this case, under the controllability assumption on the pair $(\mathbf{A}, \mathbf{B})$ one can state that there always exists state feedback gains $\mathbf{K}$ such matrix $\mathbf{A}_{cl}$ is Schur stable. That is, the convergence property of Proposition 1 is guaranteed.

C. Set-valued estimator

In the case where measurement are available, under the observability assumption of the pair $(\mathbf{A}, \mathbf{C})$, Proposition 2 introduces a set-valued state estimator that characterizes the set defined in (2).

Proposition 2: *[22] Let $\mathbf{M} = \mathbf{A} - \mathbf{L}\mathbf{C}$, $\bar{\mathcal{E}}_0 = \bar{\mathcal{X}}_0 \oplus (-\hat{\mathbf{x}}_0)$ and $\bar{\mathcal{R}}_0 \supseteq \mathbf{G}\mathcal{D}$ where $\mathbf{G} = [\mathbf{E} - \mathbf{L}\mathbf{F}]$ and $\mathcal{D} = \{\mathcal{W}; \mathcal{V}\}$. Then, for all $k \geq 1$, the following set-valued estimator,*

$$\begin{array}{rcl} \hat{\mathbf{x}}_{k+1} & = & \mathbf{M}\hat{\mathbf{x}}_k + \mathbf{B}\mathbf{u}_k + \mathbf{L}\mathbf{y}_k^m \\ \bar{\mathcal{E}}_{k+1} & = & \mathbf{A}^{k+1}\bar{\mathcal{E}}_0 \oplus \bar{\mathcal{R}}_k \\ \bar{\mathcal{R}}_{k+1} & = & \mathbf{A}^{k+1}\bar{\mathcal{R}}_0 \oplus \bar{\mathcal{R}}_k \end{array} \quad (7)$$

generates accurate enclosures $\bar{\mathcal{X}}_{k+1}^e = \hat{\mathbf{x}}_{k+1} \oplus \bar{\mathcal{E}}_{k+1}$ of the reachable set of the uncertain discrete-time system (1)*. That is, $\forall \mathbf{w}_k \in \mathcal{W}$, $\mathbf{v}_k \in \mathcal{V}$ and $\mathbf{x}_0 \in \mathcal{X}_0 \subseteq \bar{\mathcal{X}}_0$, the actual state vector of system* (1) *is enclosed inside the estimated set $\bar{\mathcal{X}}_k^e$.*

Remark 3: Note that, matrix $\mathbf{L} \in \mathbb{R}^{n_x \times n_y}$ used in (7) stands for the observer gain that is applied to ensure the Schur stability of the matrix $\mathbf{M}$. ◦

III. Main results

Based on the generated state enclosures $\bar{\mathcal{X}}_k^p$ and $\bar{\mathcal{X}}_k^e$, we propose in this section a data fusion strategy that allows one to achieve the following objectives:

- Objective 1: Increase the accuracy of the computed enclosure of the actual state vector of the uncertain system. To reach that, inconsistent parts between the sets $\bar{\mathcal{X}}_k^p$ and $\bar{\mathcal{X}}_k^e$ has to be discarded.
- Objective 2: Detect adversarial attacks and remove corrupted data to be able to preserve the guarantee of the estimated state enclosure. That is, the designed state estimator has to be resilient against this kind of anomaly.
- Objective 3: Detect faults and alert the user about their presence. Furthermore, the designed estimator has to be able to distinguish between faults and adversarial attacks.

At this stage, it is worth pointing out that in this work faults and adversarial attacks are differentiated in the following manner:

- Cyber-attacks case: A malicious agent can inject corrupted data in the state estimation algorithm. That is, in this case, the Luenberger observer in (7) is supplied by wrong inputs defined by,

$$\begin{array}{rcl} \mathbf{u}_k^a & = & \mathbf{u}_k + \mathbf{a}_{uk} \\ \mathbf{y}_k^a & = & \mathbf{y}_k^m + \mathbf{a}_{yk} \\ \hat{\mathbf{x}}_{k+1} & = & \mathbf{M}\hat{\mathbf{x}}_k + \mathbf{B}\mathbf{u}_k^a + \mathbf{L}\mathbf{y}_k^a \end{array} \quad (8)$$

where $\mathbf{a}_{uk}$ and $\mathbf{a}_{yk}$ stand for the wrong data injected by an hacker. In this framework, the considered attacks are stealthy. That is, these attacks cannot be detectable by applying the classical analysis of the residual signal,

$$\mathbf{e}_k^y = \mathbf{y}_k^m - \hat{\mathbf{y}}_k. \tag{9}$$

where $\hat{\mathbf{y}}_k = \mathbf{C}\hat{\mathbf{x}}_k$. Notice that the ability of attacks to be stealthy is their main characteristic that allows one to distinguish them from classical faults.

- Faulty case: In this context, we consider the case where physical faults (breakdowns or deterioration) appear on the system actuators and sensors. That is, the actual inputs of the system are no more valid and the measured value of its outputs via the sensors are not correct. The faulty inputs/outputs of the system are defined by,

$$\begin{array}{rcl} \mathbf{u}_k^f & = & \mathbf{u}_k + \mathbf{f}_{ak} \\ \mathbf{y}_k^f & = & \mathbf{y}_k^m + \mathbf{f}_{sk} \end{array} \tag{10}$$

where $\mathbf{f}_{ak}$ stands for the actuators faults while $\mathbf{f}_{sk}$ stands for the sensor faults. In these situations one can represent the real system as follows,

$$\begin{array}{rcl} \mathbf{x}_{k+1} & = & \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k^f + \mathbf{E}\mathbf{w}_k \\ \mathbf{y}_k^f & = & \mathbf{C}\mathbf{x}_k + \mathbf{F}\mathbf{v}_k + \mathbf{f}_{sk} \end{array} \tag{11}$$

Moreover, we assume that these faults are detectable from the residual signal (9). Notice that, in the introduced set-valued framework, the detection test is defined as follows, that is:

$$\mathbf{y}_k^m \notin \bar{\mathcal{Y}}_k^p = \mathbf{C}\bar{\mathcal{X}}_k^p \tag{12}$$

Remark 4: It is worth pointing out that, in this setting, when the system is subject to attacks, the set-valued estimator (7) uses wrong data ($\mathbf{u}_k^a$, $\mathbf{y}_k^a$); and in the case of the faults occurrence it utilizes the faulty data ($\mathbf{u}_k^f$, $\mathbf{y}_k^f$). However, the set-valued predictor (3) does not depend either on the faulty data nor on the corrupted data by an malicious attacker. This difference between the two state enclosure generators (7) and (3) is the cornerstone on which the proposed secure state estimator in this work is designed. ∘

The proposed secure set-valued state estimator is structured in the following algorithm,

Algorithm 1: Secure set-valued state estimator

- **Require**: $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{E}$, $\mathbf{F}$, $\mathbf{L}$, $\mathbf{M}$, $\mathbf{u}_k$, $\mathbf{y}_k^m$, $\bar{\mathcal{X}}_0$, $\mathcal{V}$, $\mathcal{W}$
- **While** $k \geq 0$
  1. **Compute** the predicted state set $\bar{\mathcal{X}}_k^p$ by (3)
  2. **Compute** the predicted output set $\bar{\mathcal{Y}}_k^p = \mathbf{C}\bar{\mathcal{X}}_k^p$
  3. **If** $\mathbf{y}_k^m \notin \bar{\mathcal{Y}}_k^p$
     - **Display**: a faulty behavior is detected
     - **Shut down the system**
  4. **end**
  5. **Compute** the estimated state set $\bar{\mathcal{X}}_k^e$ by (7)
  6. **If** $\mathbf{y}_k^m \in \bar{\mathcal{Y}}_k^p$ **and** $\exists i \in \{1, \ldots, n\}$ such that
     $$\bar{\mathcal{X}}_k^e(i) \cap \bar{\mathcal{X}}_k^p(i) = \emptyset$$
     - **Display**: an attack is detected
     - **Set**: $\bar{\mathcal{X}}_k^e = \bar{\mathcal{X}}_k^p$
  7. **end**
  8. **Compute** $\bar{\mathcal{X}}_k^c = \bar{\mathcal{X}}_k^e \cap \bar{\mathcal{X}}_k^p$
  9. **Return** $\bar{\mathcal{X}}_k^c$
- **end**

and the main contribution of this work is stated in the next proposition.

Proposition 3: *Let assumptions used in Proposition 1 and 2 hold. Then, for any stealthy attack that deviates at least one component of the estimated state enclosure from the predicted state enclosure,*

$$\exists i \in \{1, \ldots, n\},\ \bar{\mathcal{X}}_k^e(i) \cap \bar{\mathcal{X}}_k^p(i) = \emptyset \tag{13}$$

Algorithm 1 is a secure set-valued state estimator for system (1) *that satisfies the requirements defined in Objectives 1, 2 and 3.*

Proof. For sake of simplicity, the achievement of each objective by Algorithm 1 is separately shown in the next three paragraphs.

a) Proof of Objective 1: By construction, both set-valued predictor (Line 1 of Algorithm 1) and set-valued estimator (Line 5 of Algorithm 1) provide guaranteed state enclosures of the actual state vector $\bar{\mathcal{X}}_k^p$ and $\bar{\mathcal{X}}_k^e$, respectively. That is, for all $k \geq 0$ one has $\mathbf{x}_k \in \bar{\mathcal{X}}_k^p$ and $\mathbf{x}_k \in \bar{\mathcal{X}}_k^e$. Thus, the following intersection operator (Line 8)

$$\bar{\mathcal{X}}_k^c = \bar{\mathcal{X}}_k^e \cap \bar{\mathcal{X}}_k^p \tag{14}$$

returns guaranteed and tighter set enclosures $\bar{\mathcal{X}}_k^c$ by discarding all inconsistent parts between the sets $\bar{\mathcal{X}}_k^e$ and $\bar{\mathcal{X}}_k^p$. That is, for all $k \geq 0$, Algorithm 1 preserves the guarantee of the estimated state enclosure ($\mathbf{x}_k \in \bar{\mathcal{X}}_k^c$) and increases its tightness $\bar{\mathcal{X}}_k^c \subseteq \bar{\mathcal{X}}_k^p$ and $\bar{\mathcal{X}}_k^c \subseteq \bar{\mathcal{X}}_k^e$.

b) Proof of Objective 2: First, note that in the proposed approach the predicted set $\bar{\mathcal{X}}_k^p$ (Line 1) does not depend on the online knowledge of the system outputs and therefore, if necessary, can be computed offline. Consequently, the predicted set of outputs $\bar{\mathcal{Y}}_k^p = \mathbf{C}\bar{\mathcal{X}}_k^p$ (Line 2) is not subjected to system faults and attacks. Second, in the considered set-valued framework, the classical residual detection test $\|\mathbf{e}_k^y\| > \epsilon$, where ϵ stands for the detection threshold, is substituted by the reliable set-membership test (12) (Line 3). Thus, if an attacker manages to deceive this fault detection output test by supplying the observer with wrong data such that $\mathbf{y}_k^m \in \bar{\mathcal{Y}}_k^p$, the proposed state test (13) (Line 6) is able to detect its impact on the internal behavior of the system. In this case, to ensure the resilience of Algorithm 1, the estimated set $\bar{\mathcal{X}}_k^e$ is discarded and replaced by the predicted one $\bar{\mathcal{X}}_k^p$. It is worth stressing that the attacks which do not violate the set-membership test (13) are considered as sensor uncertainties.

c) Proof of Objective 3: The presence of faults is characterized by the violation of the belonging test (12) (Line 3). That is, when the measured output value is outside of the predicted range. Notice that, the faults that do not deviate the measurement from the predicted output set $\bar{\mathcal{Y}}_k^p$ (Line 2) are considered as state disturbances or measurement noise. In this situation, the user could stop the system to preserve its safety. •

A. Discussion about Algorithm 1

As highlighted in Remark 4, the predicted state enclosures are computed from the system's model and its assumed perfect input $\mathbf{u}_k$, while the estimated state enclosures are provided from the system's model and its inputs/outputs available data ($\mathbf{u}_k$, $\mathbf{y}_k^m$). However, in real world environments the available data can be: (i) subjected to faults and thus the set-valued estimator will be driven by imperfect data ($\mathbf{u}_k^f$, $\mathbf{y}_k^f$); or corrupted by malicious attacks and in this situation the set-valued

estimator will be steered by wrong data ($\mathbf{u}_k^a$, $\mathbf{y}_k^a$). Therefore, based on a comparison between the predicted state enclosures and the estimated state enclosures, Algorithm 1 has to provide secure estimates of the actual state vectors of the system in the presence of state disturbance, measurements noise, sensor or actuator faults and cyber-attacks. Indeed, Algorithm 1 starts by computing the current predicted state enclosure by applying the set-valued reachable set predictor defined in (3), then in Line 2 it computes a predicted enclosure of the system outputs. A fault detection condition is evaluated in Line 3. This condition is based on a set-membership test. Indeed, since the set-valued predictor does not need external data, the computed state enclosure $\bar{\mathcal{X}}_k^p$ is reliable. Thus, if the measured output $\mathbf{y}_k^m$ is not inside the predicted output set $\bar{\mathcal{Y}}_k^p$, Algorithm 1 generates a failure occurrence alert and the user can stop or keep running the system. In the case where no failure is detected, an estimated state enclosure of the real state vector of the system is computed by applying the set-valued estimator (7). To detect the presence of a cyber-attack Algorithm 1 implements a set-intersection test in Line 6. That is, if the fault detection test does not observe any wrong behavior from the measured output but the intersection between the estimated and predicted enclosure returns an empty set, one can alert of the presence of a cyber-attack. In other words, in this case the hacker has succeed to inject wrong data into the estimation algorithm to deviate the estimated state enclosure but thanks to the predicted set the deviation is detected and eliminated by setting $\bar{\mathcal{X}}_k^e = \bar{\mathcal{X}}_k^p$. Finally, in order to improve the tightness of the state enclosure the result of the intersection between the predicted and estimated set is considered as a corrected state enclosure $\bar{\mathcal{X}}_k^c$ that contains the actual state vector of the system.

B. Numerical implementation

In this subsection, we use interval analysis [2], [9] to implement all the procedures of Algorithm 1. However, to get more accurate results, other geometrical forms like zonotopes [1], [13], ellipsoids [15], [6] could be also applied.

1) Interval analysis: By definition an interval vector (box) of dimension n denoted by $[\mathbf{a}]$ is a subset of $\mathbb{R}^n$,

$$[\mathbf{a}] := \{\mathbf{a} \in \mathbb{R}^n \mid \underline{\mathbf{a}} \leq \mathbf{a} \leq \overline{\mathbf{a}}, \;\; \underline{\mathbf{a}}, \; \overline{\mathbf{a}} \in \mathbb{R}^n\} = [\underline{\mathbf{a}}, \; \overline{\mathbf{a}}] \qquad (15)$$

The real vectors $\underline{\mathbf{a}}$ and $\overline{\mathbf{a}}$ in (15) represent respectively the lower and upper bounds the box $[\mathbf{a}]$. The sum between two boxes $[\mathbf{a}]$ and $[\mathbf{b}]$ in $\mathbb{R}^n$ returns a box $[\mathbf{c}]$ in $\mathbb{R}^n$ with endpoints $\overline{\mathbf{c}} = \overline{\mathbf{a}} + \overline{\mathbf{b}}$ and $\underline{\mathbf{c}} = \underline{\mathbf{a}} + \underline{\mathbf{b}}$. For a given real matrix $\mathbf{A}$ in $\mathbb{R}^{m \times n}$ and a box $[\mathbf{x}]$ of dimension n, one has

$$[\mathbf{z}] := \mathbf{A}[\mathbf{x}] = [\mathbf{A}^+\overline{\mathbf{x}} - \mathbf{A}^-\underline{\mathbf{x}}, \; \mathbf{A}^+\underline{\mathbf{x}} - \mathbf{A}^-\overline{\mathbf{x}}] \qquad (16)$$

where, $\mathbf{M}^+$ and $\mathbf{M}^-$ are non-negative matrices computed by $\mathbf{M}^+ = \max(\mathbf{0}, \mathbf{M})$ and $\mathbf{M}^- = \mathbf{M}^+ - \mathbf{M}$. Notice that, the $\max$ operator is applied component-wise.

2) Prediction algorithm: Let $[\mathbf{x}_0] = \bar{\mathcal{X}}_0$ and $[\mathbf{f}_0] = \bar{\mathcal{F}}_0$. Then, the use of interval analysis allows one to rewrite the algorithm in Proposition 1 in the following technical form:

Algorithm 1.1 (Set-valued predictor)

- **Require**: $\mathbf{A}$, $\mathbf{B}$, $\mathbf{b}_0$, $[\mathbf{x}_0]$, $[\mathbf{f}_0]$, T
- **while** $k < T$
  - $[\mathbf{x}_k^p] := \mathbf{A}^k[\mathbf{x}_0] + [\mathbf{f}_{k-1}] + \mathbf{b}_{k-1}$
  - $[\mathbf{f}_k] := \mathbf{A}^k[\mathbf{f}_0] + [\mathbf{f}_{k-1}]$
  - $\mathbf{b}_k := \mathbf{A}\mathbf{b}_{k-1} + \mathbf{B}\mathbf{u}_k$
- **End**

Remark 5: It is worthy to notice that this algorithm is not demanding in terms of computational resources. Indeed, all the used matrices and boxes are of constant dimensions and at each iteration only 1 matrix/matrix multiplication, 10 matrix/vector multiplications and 9 vector/vector sums are to be executed. ∘

3) Estimation algorithm: Considering the following outer approximations of the sets $[\mathbf{r}_0] = \bar{\mathcal{R}}_0$ and $[\mathbf{e}_0] = \bar{\mathcal{E}}_0$. Then, based on interval analysis the algorithm in Proposition 2 can be rewritten in the following more technical form:

Algorithm 1.2 (Set-valued state estimator)

- **Require**: $\mathbf{M}$, $\mathbf{B}$, $\mathbf{L}$, $[\mathbf{e}_0]$, $[\mathbf{r}_0]$, T
- **while** $k < T$
  - $\hat{\mathbf{x}}_{k+1} := \mathbf{M}\hat{\mathbf{x}}_k + \mathbf{B}\mathbf{u}_k + \mathbf{L}\mathbf{y}_k$
  - $[\mathbf{e}_{k+1}] := \mathbf{M}^{k+1}[\mathbf{e}_0] + [\mathbf{r}_k]$
  - $[\mathbf{r}_{k+1}] := \mathbf{M}^{k+1}[\mathbf{r}_0] + [\mathbf{r}_k]$
  - $[\mathbf{x}_k^e] := \hat{\mathbf{x}}_k + [\mathbf{e}_k]$
- **End**

Remark 6: In terms of complexity, Algorithm 1.2 is almost equivalent to Algorithm 1.1. Indeed, compared to Algorithm 1.1, Algorithm 1.2 requires only a few additional arithmetic operations at each iteration (1 matrix/vector multiplication and 3 vector/vector sum). ∘

4) Intersection operator: Based on interval analysis the intersection operator used in Algorithm 1 (Line 8) can be implemented as follows: $\forall i = \{1, \ldots, n\}$

$$[\mathbf{x}_k^c(i)] = [\max\{\underline{\mathbf{x}}_k^p(i), \underline{\mathbf{x}}_k^e(i)\}, \; \min\{\overline{\mathbf{x}}_k^p(i), \overline{\mathbf{x}}_k^e(i)\}] \qquad (17)$$

5) Fault detection test: Let define by $[\mathbf{y}_k^p] = \mathbf{C}[\mathbf{x}_k^p]$, then the fault detection test in Line 3 of Algorithm 1 can be carried out as follows,

$$\mathbf{y}_k^m \notin [\mathbf{y}_k^p] \Longleftrightarrow \left\{ \begin{array}{c} \exists i \in \{1, \ldots, n_y\} \\ \text{such that} \\ \mathbf{y}_k^m(i) < \underline{\mathbf{y}}_k^p(i) \text{ or } \mathbf{y}_k^m(i) > \overline{\mathbf{y}}_k^p(i) \end{array} \right\} \qquad (18)$$

6) Attack detection test: Notice that, cyber-attack detection step is preceded by the fault detection test. That is, if no fault is detected,

$$\mathbf{y}_k^m \in [\mathbf{y}_k^p] \Longleftrightarrow \left\{ \begin{array}{c} \forall i \in \{1, \ldots, n_y\} \\ \text{such that} \\ \left(\mathbf{y}_k^m(i) > \underline{\mathbf{y}}_k^p(i)\right) \text{ or } \left(\mathbf{y}_k^m(i) < \overline{\mathbf{y}}_k^p(i)\right) \end{array} \right\} \qquad (19)$$

the intersection test in Line 6 of Algorithm 1 is performed. Based on interval analysis, this set-membership test can be carried out as follows: $\forall i \in \{1, \ldots, n\}$

$$[\mathbf{x}_k^e(i)] \cap [\mathbf{x}_k^p(i)] = \emptyset \Longleftrightarrow \overline{\mathbf{x}}_k^e(i) < \underline{\mathbf{x}}_k^p(i) \text{ or } \overline{\mathbf{x}}_k^p(i) < \underline{\mathbf{x}}_k^e(i) \qquad (20)$$

IV. Illustrative example

Consider an unmanned aircraft system (UAS) borrowed from [14], the dynamics of the UAS can be defined by the following matrices,

$$\mathbf{A} = \begin{pmatrix} 1 & \epsilon & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \epsilon \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; \mathbf{B} = \begin{pmatrix} \epsilon^2/2 & 0 \\ \epsilon & 0 \\ 0 & \epsilon^2/2 \\ 0 & \epsilon \end{pmatrix}, \mathbf{E} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \qquad (21)$$

$$\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \; \mathbf{F} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad (22)$$

where $\epsilon = 0.2s$ is the sampling period. This system is controlled by a measured state feedback law (4) where,

$$\mathbf{K} = \begin{pmatrix} 0.5 & 1 & 0 & 0 \\ 0 & 0 & 0.5 & 1 \end{pmatrix}, \; \mathbf{H} = \begin{pmatrix} 40.5 & 0 \\ 0 & 40.5 \end{pmatrix} \qquad (23)$$

and the set-point is defined by

$$\mathbf{y}_k^{ref} = \left(0.1\sin(k/(5\pi)),\ 0.1\cos(k/(5\pi))\right)^T \tag{24}$$

The feasible domains of the unknown but bounded state disturbance, measurement noise and initial state of this system are defined as follows: $\forall k \geq 0$, $\mathbf{w}_k \in \mathcal{W} = [-0.01, 0.01]$,

$$\mathbf{v}_k \in \mathcal{V} = ([-0.01, 0.01], [-0.01, 0.01])^T,$$

$$\mathbf{v}_k^x \in \mathcal{V}^x = ([-0.01, 0.01], [-0.1, 0.1], [-0.01, 0.01], [-0.1, 0.1])^T,$$

$$\mathbf{x}_0 \in \mathcal{X}_0 = ([-10, 10], [-3, 3], [-10, 10], [-4, 4])^T.$$

Notice that, since $\mathbf{A} - \mathbf{BK}$ is a Schur stable matrix and the pair $(\mathbf{A}, \mathbf{C})$ is observable, the set-valued predictor and the set-valued estimator, (3) and (7), respectively, applied on this system provide bounded state enclosures of the actual state vector with converging sizes. Then, the estimation performance of Algorithm 1 can be evaluated on this system.

For simulation purpose the state disturbance and measurement noise are considered as uniformly distributed random variables. The initial state of the system is set at $\mathbf{x}_0 = (5, 0, 5, 0)^T$. On the other hand, the initial state of the Luenberger observer in (7) is set at $\hat{\mathbf{x}}_0 = (9, 0, -9, 0)^T$ and the applied observer gain is

$$\mathbf{L} = \begin{pmatrix} 0.9715 & 0 \\ 0.7188 & 0 \\ 0 & 0.9715 \\ 0 & 0.7188 \end{pmatrix}$$

Hereafter, three simulations are carried out to show the performance of the proposed secure set-valued estimation algorithm with respect to each aforementioned objective.

Remark 7: Notice that, interval computation introduced in Subsection III-B are applied to perform Algorithm 1. ○

A. Simulation results and discussions

1) First study case: For this first test, we consider the case where the system is not subject to any cyber-attack or faults. The objective is just to show that by merging the predicted and estimated data one can obtain tighter state enclosure. The simulation results are depicted in Figures 1 and 2. In Figure 1, the actual state vector is plotted together with the estimated and predicted state enclosures. Thus, from the observed curves in this figure, it is clear that the tightness of the state enclosure can be improved by considering only the intersection results between $[\mathbf{x}_k^p]$ and $[\mathbf{x}_k^e]$. This set-membership filtering operation is carried out by Algorithm 1 at Line 8 and its results are shown in Figure 2.

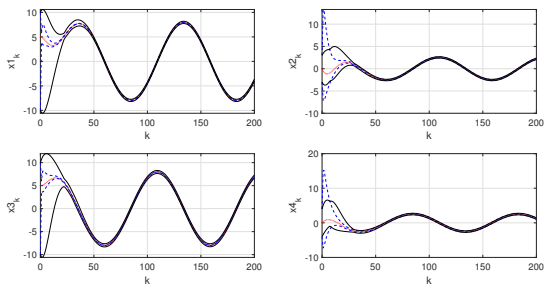

Fig. 1. State enclosures. Solid lines correspond to the predicted enclosure while the dashed blue ones represent the estimated enclosure. Dotted red lines plot the actual state variables of the system.

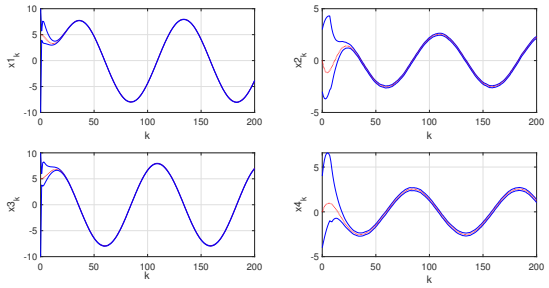

Fig. 2. Dotted red lines plot the actual state variables of the system while the solid lines show the corrected state enclosure.

2) Second study case: In this second simulation test, we consider the case of a cyber-attack. More precisely, we consider the case where a malicious agent succeeds to inject corrupted data in the measured output that is used by the Luenberger observer. That is, this latter is feed by $\mathbf{y}_k^m + \mathbf{a}_{yk}$ rather than $\mathbf{y}_k^m$. This attack appears at $k = 100$. At this time instant the hacker starts adding the value $\mathbf{a}_{yk} = 3$ to the measurement $\mathbf{y}_k^m$ sent to the observer. This attack is not observable from the set membership test $\mathbf{y}_k^m \notin [\mathbf{y}_k^p]$ as shown in Figure 3. However, its effect is detectable thanks to the intersection test $[\mathbf{x}_k^p] \cap [\mathbf{x}_k^e]$ as illustrated in Figure 4. In this situation, Algorithm 1 alerts

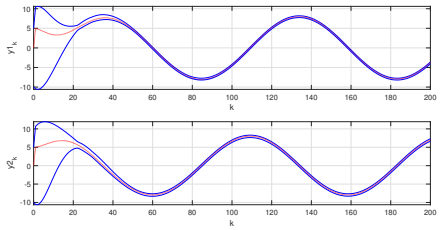

Fig. 3. Dotted red lines show the measured output vector of the system and the solid lines represent the predicted output enclosure.

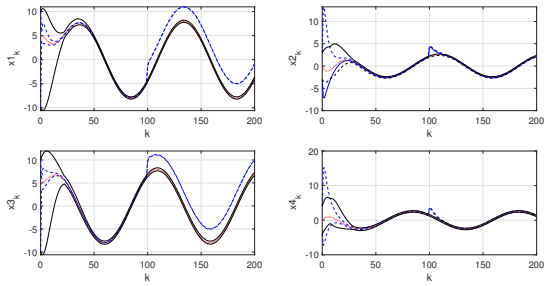

Fig. 4. State enclosures in the presence of cyber-attack. Solid lines correspond to the predicted enclosure while the dashed blue ones represent the estimated enclosure. Dotted red lines plot the actual state variables of the system.

the user about the presence of an adversarial attack and keep providing a guaranteed enclosure $[\mathbf{x}_k^c]$ of actual stat vector as shown in Figure 5. This fact illustrates the resilient capacity of the proposed estimator.

3) Third study case: Now, in this third simulation test, we show the performance of Algorithm 1 against the occurrence of an actuator fault. More precisely, we consider the case where the input of the system is subjected to a degradation represented

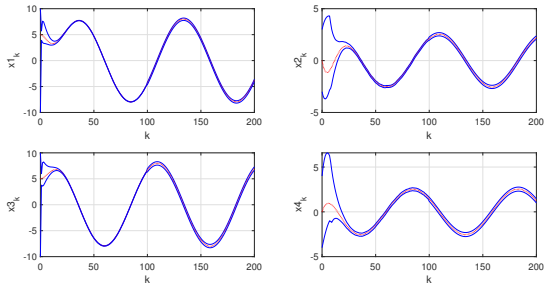

Fig. 5. Secure estimation in the presence of a cyber-attack. Dotted red lines plot the actual state variables of the system while the solid lines show the corrected state enclosure.

by $\mathbf{f}_{ak} = 1$ that occurs at time instants $k = 100$. As illustrated in Figure 6, Algorithm 1 detects the occurrence of a faulty behavior at the time instant $k = 103$ and generates an alert signal to stop running the system.

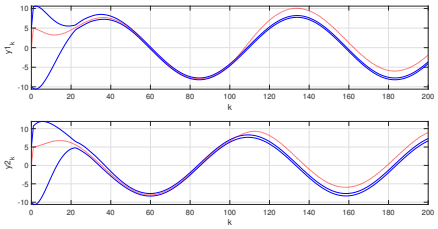

Fig. 6. Solid lines show the predicted output enclosure while the dotted red lines illustrate the measured output of the system.

V. Conclusion

In this work, a new methodology to design a secure set-valued state estimator has been proposed for the class of discrete-time linear systems described by a difference inclusion. Based on a set-valued predictor and a set-valued state estimator, different set-membership tests have been introduced to detect the occurrence of faulty behaviors on the system and to reveal the presence of some types of stealthy cyber-attacks. Simulation results have been given to support to proposed methodology and to show the performance of the designed algorithm. It is worth pointing out that the proposed method deals with open loop systems. Thus, it is of great interest to be able to consider the case of closed loop systems. This a more challenging problem will be tackled in forthcoming works. Moreover, in the future Algorithm 1 can be improved by new detection and isolation anomalies tests.

References

[1] T. Alamo, J. M. Bravo, and E. F. Camacho. Guaranteed state estimation by zonotopes. *Automatica*, 41:1035–1043, 2005.

[2] G. Alefeld and G. Mayer. Interval analysis: theory and applications. *Journal of Computational and Applied Mathematics*, 121:421–464, 2000.

[3] T. M. Chen and S. Abu-Nimeh. Lessons from stuxnet. *Computer*, 44(4):91–93, 2011.

[4] C. Combastel. Zonotopes and kalman observers: Gain optimality under distinct uncertainty paradigms and robust convergence. *Automatica*, 55:265–273, 2015.

[5] Derui Ding, Qing-Long Han, Xiaohua Ge, and Jun Wang. Secure state estimation and control of cyber-physical systems: A survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51:176 – 190, 2021.

[6] C. Durieu, E. Walter, and B. Polyak. Multi-input multi-output ellipsoidal state bounding. *Journal of Optimization Theory and Applications*, 111(2):273–303, 2001.

[7] Wenli Duso, MengChu Zhou, and Abdullah Abusorrah. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9:784–800, 2022.

[8] Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 59(6):1454 – 1467, 2014.

[9] L. Jaulin, M. Kieffer, O. Didrit, and E. Walter. *Applied interval analysis: with examples in parameter and state estimation, robust control and robotics*. Springer-Verlag, London, 2001.

[10] R.E. Kalman. A new approach to linear filtering and prediction problems. *Transactions of the ASME–Journal of Basic Engineering*, 82(Series D):35–45, 1960.

[11] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *IEEE Symposium on Security and Privacy (SP)*, pages 447–462, 2010.

[12] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *Security and Privacy IEEE*, 9(3):49–51, 2011.

[13] V. T. H. Le, C. Stoica, T. Alamo, E. F. Camacho, and D. Dumur. Zonotopic guaranteed state estimation for uncertain systems. *Automatica*, 49(1):3418–3424, 2013.

[14] Hao Liu, Yuzen Li, Qing-Long Han, and Tarek Raïssi. Watermark-based proactive defense strategy design for cyber-physical systems with unknown-but-bounded noises. *IEEE Transactions on Automatic Control*, 88:3300 – 3315, 2023.

[15] N. Loukkas, J.J. Martinez, and N. Meslem. Set-membership observer design based on ellipsoidal invariant sets. In *Proceedings of the IFAC 2017 World Congress*, pages 6471–6476, Toulouse, France, 2017.

[16] D.G. Luenberger. Observers for multivariable systems. *IEEE Transactions on automatic control*, 11(2):190 – 197, 1966.

[17] D.G. Luenberger. An introduction to observers. *IEEE Transactions on automatic control*, 16(6):596–602, 1971.

[18] F. Mazenc, T. N. Dinh, and S. I. Niculescu. Interval observers for discrete-time systems authors. *International journal of robust and nonlinear control*, 24:2867–2890, 2014.

[19] N. Meslem, A. Hably, and T. Raïssi. Zonotopic unknown input state estimator for discrete-time linear systems. *Systems & Control Letters*, 162:105168, 2022.

[20] N. Meslem, A. Hably, and T. Raïssi. State and unknown input set-valued estimation for uncertain linear discrete-time systems. *Journal of Systems and Control Engineering*, page https://doi.org/10.1177/09596518231153316, 2023.

[21] Nacim Meslem and John Martinez. Interval predictors for a class of uncertain discrete-time systems. *Acta Cybernetica*, 24(3):493–508, 2020.

[22] Nacim Meslem, Tarek Raïssi, and Gildas Besançon. Further results on the design of a class of discrete-time set-valued state estimators. *International Journal of Robust and Nonlinear Control*, 32(2):649–668, 2022.

[23] Shaunak Mishra, Yasser Shoukry, Nikhil Karamchandani, Suhas N. Diggavi, and Paulo Tabuada. Secure state estimation against sensor attacks in the presence of noise. *IEEE Transactions on Control of Network Systems*, 4(1):49 – 59, 2016.

[24] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715 – 2729, 2013.

[25] J. Slay and M. Miller. Lessons learned from the maroochy water breach. In *in Critical Infrast. Protection*, page 73–82, 2007.

[26] André Teixeira, Iman Shames, Henrik Sandberg, and Karl H. Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135–148, 2015.