Analysis of resilience for a State Estimator for Linear Systems

Alexandre Kircher, Laurent Bako, Eric Blanco, Mohamed Benallouch, Anton Korniienko

Analysis of resilience for a State Estimator for Linear Systems

Alexandre Kircher[1], Laurent Bako[1], Éric Blanco[1], Mohamed Benallouch[2], Anton Korniienko[1]

***Abstract*— This paper proposes to analyze the resilient properties of a specific state estimator for LTI discrete-time systems. The dynamic equation of the system is assumed to be affected by a bounded process noise. As to the available measurements, they are potentially corrupted by a noise of both dense and impulsive natures. In this setting, we define an estimator as the map which associates to the measurements, the minimizing set of an appropriate (convex) performance function. It is then shown that the proposed estimator enjoys the property of resilience, that is, it induces an estimation error which, under certain conditions, is independent of the extreme values of the (impulsive) measurement noise. Therefore, the estimation error may be bounded while the measurement noise is virtually unbounded. Moreover, the expression of the bound depends explicitly on the degree of observability of the system being observed and on the considered performance function. Finally, a few simulation results are provided to illustrate the resilience property.**

***Index terms*—Secure state estimation, sensor attacks, outliers, resilient estimators, Cyber-physical systems.**

I. Introduction

We consider in this work the problem of designing state estimators which would be resilient against an (unknown) sparse noise sequence affecting the measurements. By sparse noise we refer here to a signal sequence which is of impulsive nature, that is, a sequence which is most of the time equal to zero, except at a few instants where it can take on arbitrarily large values. The problem is relevant for example, in the supervision of Cyber-Physical Systems [5]. In this application, the supervisory data may be collected by spatially distributed sensors and then sent to a distant processing unit through some communication network. During the transmission, the data may incur intermittent packet losses or adversarial attacks consisting in e.g., the injection of arbitrary signals.

This estimation problem was investigated through many different approaches. Since the measurements are assumed to be affected by a sequence of outliers which is sparse in time, a natural scheme of solution to the state estimation problem may be to first detect the occurrences of the nonzero instances of that sparse noise, remove the corrupted data and then proceed with classical estimation methods such as the Kalman filter or Luenberger type of observer [15], [17]. Another category of approaches, which are inspired by some recent results in compressive sampling [4], [9], rely on sparsity-inducing optimization techniques. A striking feature of these methods is that they do not treat separately the tasks of detection, data cleaning and estimation. Instead, an implicit discrimination of the wrong data is induced by some specific properties of the to-be-minimized cost function. One of the first works that puts forward this approach for the resilient state estimation problem is the one reported in [8]. There, it is assumed that only a fixed number of sensors are subject to attacks (sparse but otherwise arbitrary disturbances) in an offline estimation setting. The challenge then resides in the fact that at each time instant, one does not know which sensor is compromised. Note however that the assumptions in [8] were quite restrictive as no process noise or measurement noise (other than the sparse attack signal) was considered. These limitations open ways for later extensions in many directions. For example, [21] suggests a reformulation which reduces computational cost by using the concept of event-triggered update; [16] considers an observation model which includes dense noise along with the sparse attack signal. In [6], the assumption of a fixed number of attacked sensors is relaxed. Finally, the recent paper [12] proposes a unified framework for analyzing resilience capabilities of most of these optimization-based estimators. Although a bound on the estimation error was derived in this paper, it is not quantitatively related to the properties (e.g., observability) of the dynamic system being observed.

The goal of the current paper is to study, in a new way, the resilient properties of a specific (convex) optimization-based estimator for LTI discrete-time systems. The available model of the system assumes bounded noise in both the dynamics and the observation equation with the latter being possibly affected by an unknown but sparse attack signal. Contrary to the settings in some existing works, we did not impose here any restriction on the number of sensors which are subject to attacks, that is, any sensor can be compromised at any time. Our main theoretical result states that the estimation error associated with the proposed estimator is, under certain circumstances, insensible to the amplitude of the attack signal. We obtain an upper bound on this estimation error which, although necessarily conservative, has the important advantage of being explicitly expressible in function of the properties of the considered dynamic system. This makes it a valuable qualitative tool for assessing the impact of the estimator's design parameters and that of the system matrices on the quality of the estimation. For example, it reflects the intuition that the more observable the system is, the larger the number of instances of gross values (of the output noise) it can handle and the smaller the error bound.

Outline. The rest of the paper is organized as follows. The estimation setting is defined in Section II. In Section III we elaborate on the proposed optimization-based estimator:

1. A. Kircher, L. Bako, E. Blanco and A. Korniienko are with Université de Lyon, Laboratoire Ampère (Ecole Centrale Lyon, CNRS UMR 5005), Ecully F-69134. E-mail: alexandre.kircher@ec-lyon.fr

2. M. Benallouch is with ECAM Lyon, 40 Montée Saint-Barthélémy, 69321 Lyon, France.

Necessary technical tools are introduced in Section III-A for the statement and the proof of the main result in Section III-B. Section IV illustrates the performance of the estimation method in simulation; Section V provides some concluding remarks.

Notations. Throughout this paper, $\mathbb{R}_{\geq 0}$ (respectively $\mathbb{R}_{>0}$) designates the set of nonnegative (respectively positive) reals. We note $\mathbb{R}^a$ the set of (column) vectors with a real elements and for any vector z in $\mathbb{R}^a$, z_i with i in $\{1, ..., a\}$ is the i-th component of z. Moreover, $\mathbb{R}^{a\times b}$ is the set of real matrices with a rows and b columns. If $M \in \mathbb{R}^{a\times b}$, then $M^\top$ will designate the transposed matrix of M. Notation $\|\cdot\|$ will represent a given norm over a given set (which will be specified when necessary). $\|\cdot\|_2$ is the Euclidean norm, defined by $\|z\|_2 = \sqrt{z^\top z}$ for all z in $\mathbb{R}^a$. $\|\cdot\|_1$ will designate the ℓ_1-norm, defined by $\|z\|_1 = \sum_{i=1}^a |z_i|$ for $z \in \mathbb{R}^a$. For a finite set $\mathcal{S}$, the notation $|\mathcal{S}|$ will refer to the cardinality of $\mathcal{S}$.

II. The estimation Problem

Consider the following discrete-time Linear Time-Invariant (LTI) system

$$\Sigma : \left\{ \begin{array}{rl} x_{t+1} & = Ax_t + w_t \\ y_t & = Cx_t + f_t \end{array} \right. \tag{1}$$

where $x_t \in \mathbb{R}^n$ is the state vector at time t, $y_t \in \mathbb{R}^{n_y}$ is the output vector at time t; $A \in \mathbb{R}^{n\times n}$ the dynamic matrix of the system and $C \in \mathbb{R}^{n_y\times n}$ is the observation matrix. $w_t \in \mathbb{R}^n$ and $f_t \in \mathbb{R}^{n_y}$ model respectively the process noise and the output noise, both of which are unknown. The estimation setting considered in the current paper is similar to the one in [14]. It is assumed that the noise sequence $\{w_t\}$ is bounded. As to the noise sequence $\{f_t\}$ can take on potentially arbitrarily large values, that is, no explicit bound is imposed on its amplitude. This type of noise can model for example, ordinary measurement noise together with faulty measurements, attack signals or packet losses on data transmitted over a communication network. For convenience, one can also view f_t as the sum of two noise components

$$f_t = v_t + s_t, \tag{2}$$

v_t being a dense noise induced by the sensors, which can be bounded or gaussian, and s_t being a *sparse noise* sequence, *i.e.* a noise whose instances are equal to zero most of the time but whose non-zero elements can take on arbitrary values.

Problem. The problem considered in this paper is one of estimating the states $x_0, \ldots, x_{T-1}$ of the system (1) on a time period $\mathcal{T}$ given T measurements $y_0, ..., y_{T-1}$ of the system output. We shall seek an accurate estimate of the state despite the uncertainties in the system equations (1) modeled by w_t and f_t the characteristics of which are described above. In particular, we would like the to-be-designed estimator to produce an estimate such that the estimation error is, when possible, independent of the maximum amplitude of $\{f_t\}$. Such an estimator will then be called resilient.

III. Resilient optimization-based estimator

We propose a convex optimization-based solution to the state estimation problem defined above. Given the system matrices A and C and T output measurements $y_0, ..., y_{T-1}$, consider a performance function $F : \mathbb{R}^{n_y\times T} \times \mathbb{R}^{n\times T} \to \mathbb{R}_{\geq 0}$ defined by

$$F(Y, Z) = \lambda \sum_{t\in\mathcal{T}'} \|z_{t+1} - Az_t\|_2^2 + \sum_{t\in\mathcal{T}} \|y_t - Cz_t\|_1 , \tag{3}$$

with $\mathcal{T} = \{0, \ldots, T-1\}$, $\mathcal{T}' = \{0, \ldots, T-2\}$ and $Z = \begin{pmatrix} z_0 & \cdots & z_{T-1} \end{pmatrix}$, i.e., the vectors $z_t \in \mathbb{R}^n$ are the columns of the matrix Z. Z represents a state trajectory candidate (optimization variable) for the system. Here, $\lambda > 0$ is a user-defined parameter which aims at balancing the contributions of the two terms involved in the expression of the performance index F. This idea of weighting the terms contained in F could also be done differently depending on the time index, for example by taking terms of the form $\|W_t(z_{t+1} - Az_t)\|_2^2$ and $\|V_t(y_t - Cz_t)\|_1$, where W_t and V_t would be positive-definite weighting matrices.

Let $\mathcal{P}(\mathbb{R}^{n\times T})$ denote the collection of all subsets of $\mathbb{R}^{n\times T}$. Then the proposed estimator is defined as the set-valued map $\Psi : \mathbb{R}^{n_y\times T} \to \mathcal{P}(\mathbb{R}^{n\times T})$ which maps the available measurements $Y \triangleq \begin{pmatrix} y_0 & \cdots & y_{T-1} \end{pmatrix}$ to the subset $\Psi(Y)$ of $\mathbb{R}^{n\times T}$ defined by

$$\Psi(Y) = \underset{Z\in\mathbb{R}^{n\times T}}{\arg\min}\, F(Y, Z). \tag{4}$$

By assuming that the pair (A, C) is observable, it can be checked that F is coercive, *i.e.* it satisfies $\lim_{\|Z\|\to+\infty} F(Y, Z) = +\infty$ for any norm $\|\cdot\|$ on $\mathbb{R}^{n\times T}$ and for all Y in $\mathbb{R}^{n_y\times T}$. It follows that the estimator Ψ expressed in (4) is well-defined in the sense that the underlying optimization problem in (4) admits a solution [19, Thm 1.9, Cor 3.27]). Note however that the minimizer need not be unique. Moreover, since the objective function F is convex with respect to Z, the elements of the so-defined state estimator $\Psi(Y)$ can be determined efficiently for a given Y. Many numerical solvers can be used for this purpose, see e.g. [11], [1], [22] for the computational aspects.

We note that similar estimators to (4) have been studied in the literature [7][14]. However, the focus of the paper is about assessing the resilience properties of the estimator (4) in a new framework. For this purpose we need some preliminary technical results.

A. Preliminaries

To begin with the analysis, we introduce some useful technical tools, the first of which is the class of $\mathcal{K}_\infty$ functions (see, e.g., [13]). This class of functions will be used to measure the increasing rate of the estimation error.

Definition 1 (class-$\mathcal{K}_\infty$ functions)**.** *A function $\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to be of class-$\mathcal{K}_\infty$ if it is continuous, zero at zero, strictly increasing and satisfies $\lim_{s\to+\infty} \alpha(s) = +\infty$.*

Using this definition we can state a technical lemma which will play an important role in the analysis.

Lemma 1. *Let $G : \mathbb{R}^{n\times m} \to \mathbb{R}_{\geq 0}$ be a nonnegative continuous function satisfying the following properties:*

- *Positive definiteness: $G(S) = 0$ if and only if $S = 0$*
- *Relaxed homogeneity: There exists a $\mathcal{K}_\infty$ function σ such that $G(S) \geq \sigma(\frac{1}{\eta})G(\eta S)$ for all $\eta \in \mathbb{R}_{>0}$.*

Then for any norm $\|\cdot\|$ on $\mathbb{R}^{n\times m}$, there exists $d > 0$ such that for all $S \in \mathbb{R}^{n\times m}$, $G(S) \geq d\sigma(\|S\|)$.

Proof. We start by observing that the unit hypersphere $\mathcal{D} = \{S \in \mathbb{R}^{n\times m} : \|S\| = 1\}$ is a compact set in the topology induced by the norm $\|\cdot\|$. By the extreme value theorem [18, Thm 3.9], G being continuous, admits necessarily a minimum value on $\mathcal{D}$, i.e., there is $S^\star \in \mathcal{D}$ such that $G(S) \geq d \triangleq G(S^\star) > 0$ for all $S \in \mathcal{D}$. For any nonzero $S \in \mathbb{R}^{n\times m}$, $\frac{S}{\|S\|} \in \mathcal{D}$ so that $G(\frac{S}{\|S\|}) \geq d$. On the other hand, by the relaxed homogeneity of G,

$$G(S) \geq \sigma(\|S\|)G(\frac{S}{\|S\|}) \geq d\sigma(\|S\|).$$

Moreover, this inequality holds for $S = 0$. It therefore holds true for any $S \in \mathbb{R}^{n\times m}$. □

For future uses in the paper, consider now the function $H : \mathbb{R}^{n\times T} \to \mathbb{R}_{\geq 0}$ defined by

$$H(Z) = \frac{\lambda}{2}\sum_{t\in\mathcal{T}'} \|z_{t+1} - Az_t\|_2^2 + \sum_{t\in\mathcal{T}} \|Cz_t\|_1 \qquad (5)$$

H is a function that will be of use in the later theoretical developments of the paper. Note that although $F(Z)$ and $H(Z)$ resemble each other, there are indeed different. A key property of H which will help the analysis is how it can be lower bounded, as stated in the following lemma:

Lemma 2 (Lower Bound on H)**.** *Let $\|\cdot\|$ be a norm on $\mathbb{R}^{n\times T}$. Consider the function H defined in* (5) *under the assumption that (A, C) is observable. Then*

$$H(Z) \geq Dq(\|Z\|) \quad \forall Z \in \mathbb{R}^{n\times T} \qquad (6)$$

where $q : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is the function defined by

$$\forall \alpha \in \mathbb{R}_{\geq 0},\ q(\alpha) = \min(\alpha, \alpha^2) \qquad (7)$$

and

$$D = \min_{\|Z\|=1} H(Z) > 0. \qquad (8)$$

Proof. The idea of the proof is to check that H satisfies the conditions of Lemma 1 and then apply that lemma to conclude. First, note that continuity and nonnegativity of H are obvious. As to the relaxed homogeneity property, it can be checked straightforwardly that it holds with $\sigma = q$. Finally, setting $H(Z) = 0$ implies that $z_{t+1} = Az_t$ and $Cz_t = 0$ for all $t = 0, \ldots, T-1$. It immediately follows that $CA^t z_0 = 0$ and so, $\mathcal{O}z_0 = 0$ where $\mathcal{O} = \begin{pmatrix} C^\top & \cdots & (CA^{n-1})^\top \end{pmatrix}^\top$ is the observability matrix of the system. By the observability assumption, we get that $z_0 = 0$ and consequently, that $Z = 0$. Therefore H is positive-definite. The statement of the lemma now follows by applying Lemma 1. □

To proceed further, let us introduce a few notations. We use the notation $\mathcal{I} = \{1, \ldots, n_y\}$ to denote a label set for the sensors described by the observation equation in (1). For $i \in \mathcal{I}$, $c_i^\top$ denotes the i-th row of the observation matrix C. The next definition introduces a parameter to gauge the resilience properties of an estimator of the form defined in (4).

Definition 2 (r-Resilience index p_r)**.** *Let r be a nonnegative integer. Assume that the system Σ in* (1) *is observable. We define the r-Resilience index of the estimator Ψ in* (4) *(when applied to Σ) as the real number p_r given by*

$$p_r = \sup_{\substack{Z\neq 0 \\ Z\in\mathbb{R}^{n\times T}}} \sup_{\substack{\Lambda_r\subset\mathcal{I}\times\mathcal{T} \\ |\Lambda_r|=r}} \frac{\sum_{(i,t)\in\Lambda_r} \left|c_i^\top z_t\right|}{H(Z)} \qquad (9)$$

where H is as defined in (5)*. The supremum is taken here over all nonzero Z in $\mathbb{R}^{n\times T}$ and over all subsets Λ_r of $\mathcal{I}\times\mathcal{T}$ with cardinality r.*

The index p_r can be interpreted as a quantitative measure of the observability of the system Σ. The observability is needed here to ensure that the denominator $H(Z)$ of (9) is different from zero whenever $Z \neq 0$ (see the positive definiteness proof of H in the proof Lemma 2 above). Furthermore, it should be remarked that $\sum_{(i,t)\in\Lambda_r} \left|c_i^\top z_t\right| \leq H(Z)$ for any $\Lambda_r \subset \mathcal{I}\times\mathcal{T}$, which implies that the defining suprema of p_r are well-defined. The lower p_r is, the more resilient the estimator is expected to be. The next section gives more background to the introduction of p_r and which role it plays in the resilience analysis of the estimator.

Obtaining p_r requires solving a combinatorial optimization problem which is also nonconvex. This is indeed a common characteristic of the concepts which are usually used to assess resilience; for example the popular Restricted Isometry Property (RIP) constant [3] is comparatively as hard to evaluate. Nevertheless, if we restrict our attention to estimation problems where the process noise $\{w_t\}$ would be identically equal to zero, then by adding in (9) the additional constraint that $z_{t+1} = Az_t$, p_r can be exactly computed using the method in [20] or more cheaply overestimated using the one in [2].

Remark. The case where only a known set of sensors is affected by f_t is a special case of the current framework: indeed, this information would restrict the search set of Λ_r from $\mathcal{I}\times\mathcal{T}$ to $\mathcal{I}'\times\mathcal{T}$ with $\mathcal{I}'$ the set of attacked sensors.

B. Characterization of the resilience property

The main result of this paper consists in the characterization of the resilience property of the state estimator (4). More specifically, our result states that the estimation error, *i.e.*, the difference between the real state trajectory and the estimated one, is upper bounded by a bound which does not depend on the amplitude of the outliers contained in $\{f_t\}$ provided that the number of such outliers is below some threshold.

Before stating the main theorem, let us introduce a last notation to be used in the analysis. Let $\varepsilon \geq 0$ be a given number. For any sequence $\{f_t\}_{t\in\mathcal{T}}$ in (1), we can split the index set $\mathcal{I}\times\mathcal{T}$ into two disjoint label sets,

$$\mathcal{J}_\varepsilon = \{(i,t) \in \mathcal{I}\times\mathcal{T} : |f_{it}| \leq \varepsilon\}, \qquad (10)$$

indexing those f_{it}[1] which are bounded by ε and $\mathcal{J}_\varepsilon^c = \{(i,t) \in \mathcal{I} \times \mathcal{T} : |f_{it}| > \varepsilon\}$ indexing those f_{it} which are possibly unbounded. It is important to keep in mind that ε is just a parameter for decomposing the noise sequence in two parts in view of the analysis (and not a bound on f_{it}). The particular situation where $\varepsilon = 0$ reflects the approach where one would view any nonzero f_{it} as an outlier.

Theorem 1 (Upper bound on the estimation error)**.** *Consider the system Σ defined by* (1) *with output measurement Y and consider the estimator* (4)*. Let $\varepsilon \in \mathbb{R}_{\geq 0}$ and $r = |\mathcal{J}_\varepsilon^c|$. If Σ is observable and $p_r < 1/2$, then for all $\hat{X} = \begin{pmatrix}\hat{x}_0 & \cdots & \hat{x}_{T-1}\end{pmatrix} \in \Psi(Y)$,*

$$\|E\| \leq h\left(\frac{2\beta_\Sigma(\varepsilon)}{D(1-2p_r)}\right) \tag{11}$$

where $E = \begin{pmatrix}\hat{x}_0 - x_0 & \cdots & \hat{x}_{T-1} - x_{T-1}\end{pmatrix}$, $\|\cdot\|$ is any given norm on $\mathbb{R}^{n\times T}$, $\beta_\Sigma(\varepsilon)$ is defined by

$$\beta_\Sigma(\varepsilon) = \lambda \sum_{t\in\mathcal{T}'} \|w_t\|_2^2 + \sum_{(i,t)\in\mathcal{J}_\varepsilon} |f_{it}|, \tag{12}$$

the function $h : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is defined by

$$\forall \alpha \in \mathbb{R}_{\geq 0},\ h(\alpha) = \max\left(\alpha, \sqrt{\alpha}\right) \tag{13}$$

and D is given as in (8) *from the norm $\|\cdot\|$.*

Proof. By definition (4) of the estimator Ψ, it holds that for all $\hat{X} \in \Psi(Y)$, $F(Y,\hat{X}) \leq F(Y,X)$, that is,

$$\begin{aligned}\lambda \sum_{t\in\mathcal{T}'} \|\hat{x}_{t+1} - A\hat{x}_t\|_2^2 + \sum_{t\in\mathcal{T}} \|y_t - C\hat{x}_t\|_1 \\ \leq \lambda \sum_{t\in\mathcal{T}'} \|x_{t+1} - Ax_t\|_2^2 + \sum_{t\in\mathcal{T}} \|y_t - Cx_t\|_1 \\ = \lambda \sum_{t\in\mathcal{T}'} \|w_t\|_2^2 + \sum_{t\in\mathcal{T}} \|f_t\|_1 .\end{aligned} \tag{14}$$

Next, we derive a lower bound on the left hand side of (14). For every t in $\mathcal{T}$, let $e_t = \hat{x}_t - x_t$. Then

$$\begin{aligned}\|\hat{x}_{t+1} - A\hat{x}_t\|_2^2 &= \|\hat{x}_{t+1} - x_{t+1} - A(\hat{x}_t - x_t) + w_t\|_2^2 \\ &\geq \|e_{t+1} - Ae_t + w_t\|_2^2 \\ &\geq \frac{1}{2}\|e_{t+1} - Ae_t\|_2^2 - \|w_t\|_2^2.\end{aligned} \tag{15}$$

The last inequality uses Lemma 3 in Appendix A which yields, with $G = \|\cdot\|_2^2$,

$$\|z_1 - z_2\|_2^2 \geq \frac{1}{2}\|z_1\|_2^2 - \|z_2\|_2^2 \ \forall (z_1, z_2) \in \mathbb{R}^n \times \mathbb{R}^n. \tag{16}$$

Similarly, we can write

$$\begin{aligned}\|y_t - C\hat{x}_t\|_1 &= \|y_t - Cx_t - C(\hat{x}_t - x_t)\|_1 \\ &= \|f_t + Ce_t\|_1\end{aligned}$$

As a consequence, the second term of the left-hand-side of (14) is expressible as

$$\sum_{t\in\mathcal{T}} \|y_t - C\hat{x}_t\|_1 = \sum_{(i,t)\in\mathcal{I}\times\mathcal{T}} \left|f_{it} + c_i^\top e_t\right|.$$

[1] f_{it} denotes the i-th entry of the vector f_t.

Now, depending on if the couple (i,t) belongs to $\mathcal{J}_\varepsilon$ or not, we apply the triangle inequality property of the absolute value differently, the two cases being

$$\begin{aligned}\forall (i,t) \in \mathcal{J}_\varepsilon, \quad \left|f_{it} + c_i^\top e_t\right| \geq |c_i^\top e_t| - |f_{it}| \\ \forall (i,t) \in \mathcal{J}_\varepsilon^c, \quad \left|f_{it} + c_i^\top e_t\right| \geq |f_{it}| - |c_i^\top e_t|\end{aligned}$$

It follows that

$$\begin{aligned}\sum_{t\in\mathcal{T}} \|y_t - C\hat{x}_t\|_1 \geq \sum_{(i,t)\in\mathcal{J}_\varepsilon} |c_i^\top e_t| - \sum_{(i,t)\in\mathcal{J}_\varepsilon^c} |c_i^\top e_t| \\ - \sum_{(i,t)\in\mathcal{J}_\varepsilon} |f_{it}| + \sum_{(i,t)\in\mathcal{J}_\varepsilon^c} |f_{it}|.\end{aligned}$$

Combining this with (14) and (15) and re-arranging, yields

$$\begin{aligned}\frac{\lambda}{2} \sum_{t\in\mathcal{T}'} \|e_{t+1} - Ae_t\|_2^2 + \sum_{(i,t)\in\mathcal{J}_\varepsilon} |c_i^\top e_t| - \sum_{(i,t)\in\mathcal{J}_\varepsilon^c} |c_i^\top e_t| \\ \leq 2\Big(\lambda \sum_{t\in\mathcal{T}'} \|w_t\|_2^2 + \sum_{(i,t)\in\mathcal{J}_\varepsilon} |f_{it}|\Big)\end{aligned} \tag{17}$$

On the right hand side of (17), we recognize $2\beta_\Sigma(\varepsilon)$ as in (11). As to the term on the left hand side, it is equal to $H(E) - 2\sum_{(i,t)\in\mathcal{J}_\varepsilon^c} |c_i^\top e_t|$.

Independently, $|\mathcal{J}_\varepsilon^c| = r$ so by definition (9) of the index p_r,

$$\sum_{(i,t)\in\mathcal{J}_\varepsilon^c} |c_i^\top e_t| \leq p_r H(E) \tag{18}$$

Consequently, it follows from (17) and (18) that

$$(1-2p_r)H(E) \leq H(E) - 2\sum_{(i,t)\in\mathcal{J}_\varepsilon^c} |c_i^\top e_t| \leq 2\beta_\Sigma(\varepsilon).$$

Since p_r is assumed to be smaller than $1/2$, $1 - 2p_r > 0$. Therefore, we can write

$$H(E) \leq \frac{2\beta_\Sigma(\varepsilon)}{1-2p_r} \tag{19}$$

Thanks to Lemma 2, we have $H(E) \geq Dq(\|E\|)$ for any given norm $\|\cdot\|$ on $\mathbb{R}^{n\times T}$. This implies that

$$q(\|E\|) \leq \frac{2\beta_\Sigma(\varepsilon)}{D(1-2p_r)}$$

Now observe that the function h defined in (13), is the inverse function of q, meaning that for every $\lambda \in \mathbb{R}_{\geq 0}$, $h(q(\lambda)) = \lambda$. Moreover, h is an increasing function. Applying h to both members of the previous inequality gives the desired result. □

The resilience property of the estimator (4) lies here in the fact that, under the conditions of Theorem 1, the bound in (11) on the estimation error does not depend on the magnitudes of the extreme values of the noise sequence $\{f_{it}\}_{(i,t)\in\mathcal{I}\times\mathcal{T}}$. Considering in particular the function $\beta_\Sigma(\varepsilon)$, we remark that it can be overestimated as follows

$$\beta_\Sigma(\varepsilon) \leq \lambda \sum_{t\in\mathcal{T}'} \|w_t\|_2^2 + |\mathcal{J}_\varepsilon|\varepsilon. \tag{20}$$

We recognize two terms in the upper bound of $\beta_\Sigma(\varepsilon)$: (i) the first one is a sum which simply represents the uncertainty brought by the (bounded) dense noise w_t over the whole state

trajectory and which does not depend on ε; (ii) the second one is a bound on the sum of those instances of f_{it} whose magnitude is smaller than ε.

Because β_Σ is a function of ε, the bound in (11) represents indeed a family of bounds parametrized by ε. The theorem holds true for any $\varepsilon > 0$ *as long as* the system is resilient enough, *i.e.* p_r is smaller than $1/2$ for $r = |\mathcal{J}_\epsilon^c|$. Since ε is a mere analysis device, a question would be how to select it for the analysis to achieve the smallest bound. Such values, say $\varepsilon^\star$, satisfy

$$\varepsilon^\star \in \arg\min_{\varepsilon \geq 0} \left\{ h\Big(\frac{2\beta_\Sigma(\varepsilon)}{D(1-2p_r)}\Big) \,:\, r = |\mathcal{J}_\varepsilon^c|,\ p_r < 1/2 \right\}.$$

As already mentioned, checking numerically the assumption $p_r < 1/2$ requires solving a hard combinatorial problem. Nevertheless, one can retain the intuition that $p_r < 1/2$ is all the more likely to hold as the r is small (i.e., ε is large).

Another interesting point is that the inequality stated by Theorem 1 holds for any norm on $\mathbb{R}^{n\times T}$. Note though that the value of the bound depends (through the parameter D defined in (8)) on the specific norm used to measure the estimation error. Moreover, different choices of the performance-measuring norm will result in different geometric forms for the uncertain set, that is, the ball (in the chosen norm) centered at the true state with radius equal to the upper bound displayed in (11).

We also observe that the smaller the parameter p_r is, the tighter the error bound will be, which suggests that the estimator is more resilient when p_r is lower. A similar reasoning applies to the number D which is desired to be large here. These two parameters p_r and D reflect properties of the system whose state is being estimated. They can be interpreted, to some extent, as measures of the degree of observability of the system. In conclusion, the estimator inherits partially its resilience property from characteristics of the system being observed. This is consistent with the well-known fact that the more observable a system is, the more robustly its state can be estimated from output measurements.

Finally, an interesting property of the estimator can be stated in the absence of dense noise:

Corollary 1. *Consider the system* Σ *defined by* (1) *and let* $r = |\mathcal{J}_0^c|$ *(which means that we consider every nonzero occurrence of* f_{it} *as an outlier). If* $p_r < 1/2$*, and if* $w_t = 0$ *for all* t*, then the estimator defined by* (4) *retrieves exactly the state trajectory of the system.*

Proof. This follows directly from the fact that $\beta_\Sigma(0) = 0$ in the case where there is no dense noise w_t and $\varepsilon = 0$. □

Therefore, we have the exact recoverability of every state of the system (1) by the estimator when there is no process noise. According to our analysis, the number of outliers that can be handled by the estimator in this case can be underestimated by

$$\max\big\{r : p_r < 1/2\big\}. \tag{21}$$

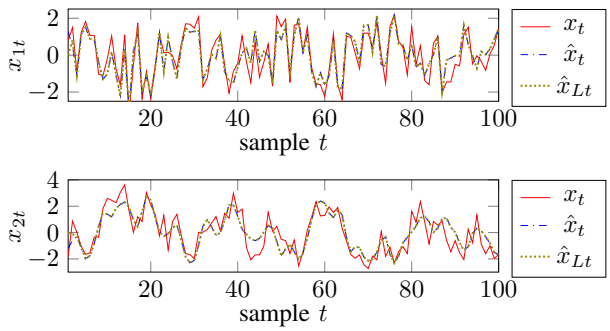

Fig. 1: State of the system and its estimates ($\hat{x}$ through the resilient estimator and $\hat{x}_L$ through the smoother) in absence of sparse noise

IV. Simulation Results

In this section, we present the simulation results in two cases, with and without a sparse component in f_t. The structure of the studied system is identical to (1) with

$$A = \begin{pmatrix} -0.11 & -0.34 \\ -0.34 & 0.46 \end{pmatrix},\ C = \begin{pmatrix} 1.4 & -0.94 \end{pmatrix}$$

The system is simulated on a time-horizon equal to $T = 100$, w_t is the realization of a uniform random variable over $[-2; 2]$, v_t is a gaussian white noise of signal-to-noise ratio equal to 30dB, and the initial state of the system is a gaussian random variable of unit vaiance. The estimated states were then obtained by directly solving the optimisation problem defined in (4) with $\lambda = 1/5$ through CVX [11].

Simulation without s_t. This case aims at showing the good results of the resilient estimator in an unattacked setting. To give a basis for comparison, we also estimated the state of the system through a Rauch-Tung-Striebel (RTS) smoother which is an extension of the Kalman filter to offline estimation [10]. Figure 1 presents the results obtained, *i.e.* the real state x, the state $\hat{x}$ estimated through (4) and the state $\hat{x}_L$ estimated through the RTS smoother. Estimator $\Psi(Y)$ provides similar results to the RTS Smoother in this example, which is very interesting given that it was designed to deal with attacks in the first place.

Simulation with s_t. In this case, s_t is nonzero: the time indexes when s_t is non-zero are uniformly randomly chosen to fit a ratio of 20% non-zero values. Each value is then decided by a uniform random variable between -50 and 50. Figure 2 now presents the results associated with this case. We provided $y_{wt} = Cx_t + v_t$, the unattacked output of the system, and s_t on the same graph (bottom) to showcase the difference in values. In this setting, the Mean Square Error[2] of the RTS smoother is equal to 70 for the first state and 27 for the second state: this explains why it is not represented on Figure 2, given it strongly diverges. In comparison, the resilient estimator (4) has a MSE of 0.5 and 1 for first and second states respectively: even in the presence of corrupted measurements of arbitrarily large magnitude, the estimator

[2]We define the Mean Square Error (MSE) associated with the i-th state as $m_i = 1/T \cdot \sum_{t=0}^{T-1} (x_{it} - \hat{x}_{iLt})^2$

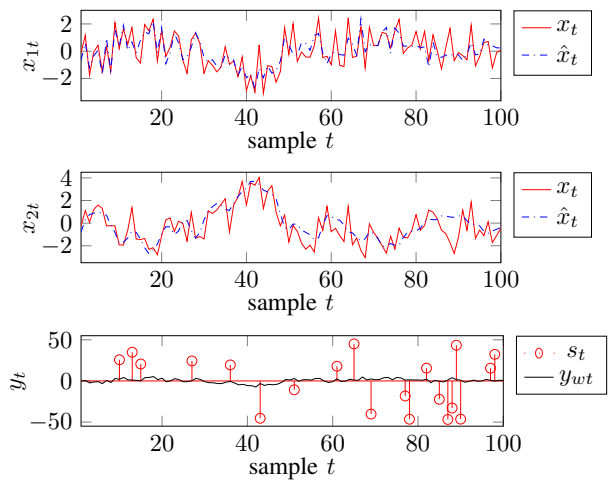

Fig. 2: State, estimated state $\hat{x}$ through resilient estimation and output of the system in presence of sparse noise

still manages to efficiently track the trajectory of the real states, showing that its performance are not really degraded in that case.

V. Conclusion

In this paper, we considered the problem of estimating the state of linear discrete-time systems in the face of uncertainties modeled as process and measurement noise in the system equations. The measurement noise sequence assumes values of possibly arbitrarily large amplitude which occur sparsely in time and between sensors. To address this problem, we introduced an estimator based on the resolution of a convex optimization problem and then analyzed its resilience properties in a new framework. In particular, we proved that the resulting estimation error is bounded by a bound which is independent of the extreme values of the measurement noise given that the number of occurrences (over time and over the whole set of sensors) of such extreme values is limited with regards to a parameter linked to the observability of the system. Future works will aim at generalizing this analysis of resilient properties to a wider class of estimators and applying the estimation framework to relevant practical cases.

Acknowledgements

The authors acknowledge financial support from the École Doctorale Électronique, Électrotechnique & Automatique (ED-EEA) of the Université de Lyon.

Appendix

A. Additional elements to the proof of Theorem 1

Lemma 3. *Let $G : \mathbb{R}^{n\times m} \to \mathbb{R}_{\geq 0}$ be a convex nonnegative continuous function satisfying the properties of positive definiteness and relaxed homogeneity (for a given $\mathcal{K}_\infty$ function σ) as both defined in Lemma 1. Then, for all $(S_1, S_2) \in \mathbb{R}^{n\times m} \times \mathbb{R}^{n\times m}$,*

$$G(S_1 - S_2) \geq 2\sigma(1/2)G(S_1) - G(S_2) \tag{22}$$

Proof. As G is convex,

$$G\left((S_1 - S_2)/2 + S_2/2\right) \leq G(S_1 - S_2)/2 + G(S_2)/2 \tag{23}$$

which can be rewritten as

$$G(S_1 - S_2) \geq 2G(S_1/2) - G(S_2) \tag{24}$$

Moreover, by assumption, G verifies the relaxed homogeneity property with a $\mathcal{K}_\infty$ function σ: it entails that $\forall S_1 \in \mathbb{R}^{n\times m}$, $G(S_1/2) \geq \sigma(1/2)G(S_1)$ which, when injected in (24), gives the desired result. □

References

[1] M. ApS. The MOSEK optimization toolbox for MATLAB.
[2] L. Bako. On a class of optimization-based robust estimators. *IEEE Transactions on Automatic Control*, 62(11):5990–5997, 2017.
[3] E. J. Candes. The restricted isometry property and its implications for compressed sensing. *Comptes rendus mathematique*, 346(9-10):589–592, 2008.
[4] E. J. Candès and M. B. Wakin. An introduction to compressive sampling. *IEEE Signal Processing Society*, 25:21–30, 2008.
[5] A. Cardenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *International Conference on Distributed Computing Systems Workshops, Beijing, China*, pages 495–500, 2008.
[6] Y. H. Chang, Q. Hu, and C. J. Tomlin. Secure estimation based kalman filter for cyber–physical systems against sensor attacks. *Automatica*, 95:399–412, 2018.
[7] S. Farahmand, G. B. Giannakis, and D. Angelosante. Doubly robust smoothing of dynamical processes via outlier sparsity constraints. *IEEE Transactions on Signal Processing*, 59(10):4529–4543, 2011.
[8] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 59(6):1454–1467, 2014.
[9] S. Foucart and H. Rauhut. *A mathematical introduction to compressive sensing*. Birkhäuser, 2013.
[10] A. Gelb. *Applied optimal estimation*. MIT press, 1974.
[11] M. C. Grant and S. P. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. 2017.
[12] D. Han, Y. Mo, and L. Xie. Convex optimization based state estimation against sparse integrity attacks. *IEEE Transaction on Automatic Control* , 64(6): 2334–3303, 2019.
[13] C. M. Kellett. A compendium of comparison function results. *Mathematics of Control, Signals, and Systems*, 26:339–374, 2014.
[14] J. Mattingley and S. P. Boyd. Real-time convex optimization in signal processing. *IEEE Signal processing magazine*, 27(3):50–61, 2010.
[15] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada. Secure state estimation against sensor attacks in the presence of noise. *IEEE Transactions on Control of Network Systems*, 4(1):49–59, 2017.
[16] M. Pajic, I. Lee, and G. J. Pappas. Attack-resilient state estimation for noisy dynamical systems. *IEEE Transactions on Control of Network Systems*, 4(1):82–92, 2017.
[17] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.
[18] M. H. Protter, C. B. Morrey *A First Course in Real Analysis* New York: Springer, 1977, p. 57.
[19] R. T. Rockafellar, and J.-B. Wets. *Variational Analysis*. 3rd ed., Berlin Heidelberg: Springer Verlag, 2009, pp.11–92.
[20] Y. Sharon, J. Wright, and Y. Ma. Minimum sum of distances estimator: Robustness and stability. In *American Control Conference, St. Louis, MO, USA*, pages 524–530, 2009.
[21] Y. Shoukry and P. Tabuada. Event-triggered state observers for sparse sensor noise/attacks. *IEEE Transactions on Automatic Control*, 61(8):2079–2091, 2016.
[22] J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization methods and software*, 11(1-4):625–653, 1999.