EasyChair Preprint

№ 14649

A Lasso Approach to Secure State Estimation for Cyber-Physical Systems

Vito Cerone, Sophie M. Fosson, Diego Regruto and Francesco Ripa

September 1, 2024

A Lasso approach to secure state estimation for cyber-physical systems

V. Cerone S. M. Fosson D. Regruto F. Ripa

***Abstract*— The development of algorithms for secure state estimation in vulnerable cyber-physical systems has been gaining attention in the last years. A consolidated assumption is that an adversary can tamper a relatively small number of sensors. In this paper, we propose a Lasso-based approach and we analyse its effectiveness. We theoretically derive conditions that guarantee successful attack/state recovery and we develop a sparse state observer. We compare the proposed methods to the state-of-the-art algorithm via numerical simulations.**

I. Introduction

A cyber-physical system (CPS) is a collection of computing devices that interact with the physical world, through sensors and actuators, and with one another, through communication networks. Applications of the CPS paradigm include industrial control processes, smart power grids, wireless sensor networks, electric ground vehicles and cooperative driving technologies. A relevant research line considers the problem of secure state estimation (SSE) for CPSs in the presence of sensor attacks, that inject false data to manipulate the measurements. We expect that an adversary conceives an unpredictable intrusion, that is, we have no information on its dynamics. The unique realistic assumption on sensor attacks is sparsity: only a relatively small number of sensors is accessible, due to, e.g., large dimensionality and physical deployment of CPSs.

The identification of the attack support, i.e., the subset of tampered sensors, is a combinatorial problem that does not scale well for large dimensional systems. By leveraging the sparsity assumption, one can exploit ℓ_1-based sparsity-promoting decoders to recast the problem into constrained convex optimization; see, e.g., [1], [2]. Since these approaches are still computationally intense, [3] introduces a faster event-triggered projected gradient (ETPG) approach, whose structure is prone to recursive SSE. The provided sufficient conditions for the convergence of ETPG are quite restrictive. The work [4] addresses this issue by a satisfiability modulo theory approach, called Imhotep-SMT, which is suitable for small/medium dimensional problems.

In this work, we propose a Lasso approach, see [5], to SSE of CPSs under sparse sensor attacks and we analyse its effectiveness. Moreover, we design a sparsity-promoting Luenberger-like observer by starting from the iterative soft thresholding algorithm for Lasso and we propose some numerical results.

* The authors are with the Dipartimento di Automatica e Informatica, Politecnico di Torino, corso Duca degli Abruzzi 24, 10129 Torino, Italy; e-mail: sophie.fosson@polito.it. This work is part of the project NODES which has received funding from the MUR – M4C2 1.5 of PNRR with grant agreement no. ECS00000036.

II. Problem Statement

As in [1], [3], we consider CPSs that can be modeled as

$$\begin{aligned} x(k+1) &= Ax(k) \\ y(k) &= Cx(k) + a(k) \end{aligned} \tag{1}$$

where $x(k) \in \mathbb{R}^n$ is the state, $y(k) \in \mathbb{R}^p$ is the measurement vector, $a(k) \in \mathbb{R}^p$ is the attack vector. We assume that each sensor i takes a measurement $y_i(k) \in \mathbb{R}$. If $a_i(k) \neq 0$, sensor i is under attack. The SSE problem is as follows.

Problem 1: For some $\tau \leq n$ and $k \geq \tau - 1$ given A, C and $y = (y(k-\tau+1)^\top, \dots, y(k)^\top)^\top \in \mathbb{R}^{p\tau}$, estimate $x(k-\tau+1)$ in the presence of sparse sensor attacks.

Let us denote $\widetilde{a} = (a(k-\tau+1)^\top, \dots, a(k)^\top)^\top \in \mathbb{R}^{p\tau}$ and $\widetilde{x} = x(k-\tau+1) \in \mathbb{R}^n$, while $I \in \{0,1\}^{p\tau, p\tau}$ is the identity matrix. We have $y = \begin{pmatrix} \mathcal{O} & I \end{pmatrix} \begin{pmatrix} \widetilde{x}^\top & \widetilde{a}^\top \end{pmatrix}^\top$ where $\mathcal{O} = \begin{pmatrix} C^\top & (CA)^\top & \cdots & (CA^{\tau-1})^\top \end{pmatrix}^\top \in \mathbb{R}^{p\tau, n}$. If $\tau = n$, $\mathcal{O}$ is the observability matrix of the attack-free system; we assume $\operatorname{rank}(\mathcal{O}) = n$.

III. Lasso approach

By taking into account the sparsity of $\widetilde{a}$, we propose the following Lasso formulation for Problem 1:

$$(x^\star, a^\star) = \underset{x \in \mathbb{R}^n, a \in \mathbb{R}^{p\tau}}{\operatorname{argmin}} \frac{1}{2} \|y - \mathcal{O}x - a\|_2^2 + \lambda \|a\|_1 \tag{2}$$

where $\lambda > 0$. An interesting feature of classic Lasso is that there is a tight condition, denoted as "irrepresentable", that guarantees the recovery of the correct support; see, e.g., [6]. In this work, we perform an irrepresentable condition analysis for (2), by taking into account the structure of the "sensing matrix" $\begin{pmatrix} \mathcal{O} & I \end{pmatrix}$ and the ℓ_1 regularization applied only to variables a.

In the following, $\mathcal{S}$ is the support of $\widetilde{a}$ and $\bar{\mathcal{S}}$ is its complementary set. $\mathcal{O}_\mathcal{S} \in \mathbb{R}^{h,n}$ and $\mathcal{O}_{\bar{\mathcal{S}}} \in \mathbb{R}^{p\tau-h,n}$ are the submatrices of $\mathcal{O}$ with *rows* in $\mathcal{S}$ and in $\bar{\mathcal{S}}$, respectively. Finally, we denote by $\|\cdot\|_\infty$ the ℓ_∞ matrix norm.The following result holds.

Theorem 1: Let us assume that $\begin{pmatrix} \mathcal{O} & I_\mathcal{S} \end{pmatrix} \in \mathbb{R}^{p\tau, n+h}$ is full rank. Lasso is successful, i.e., by solving it we identify the attack support, if $\left\| \mathcal{O}_{\bar{\mathcal{S}}}^{\dagger\top} \mathcal{O}_\mathcal{S}^\top \right\|_\infty < 1$ where $\mathcal{O}_{\bar{\mathcal{S}}}^{\dagger\top}$ is the right pseudo-inverse of $\mathcal{O}_{\bar{\mathcal{S}}}^\top$.

A qualitative interpretation of this result is that the rows of $\mathcal{O}_\mathcal{S}$ must be "sufficiently orthogonal" to the columns of $\mathcal{O}_{\bar{\mathcal{S}}}^\dagger$. We refer the reader to [7] for the proof of the theorem and extedend considerations.

IV. Sparse soft observer for online SSE

In this section, we move towards recursive, online SSE. We consider Problem 1 in a dynamic perspective: we aim at

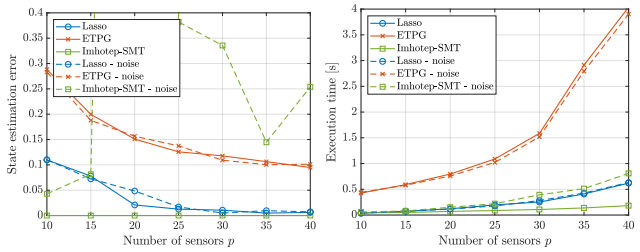

Fig. 1. Lasso vs ETPG vs Imhotep-SMT, $n = 20$, $s = p/5$ sensors under attack. The measurements are either noise-free and with noise bound 10^{-4}. The results are averaged over 50 runs.

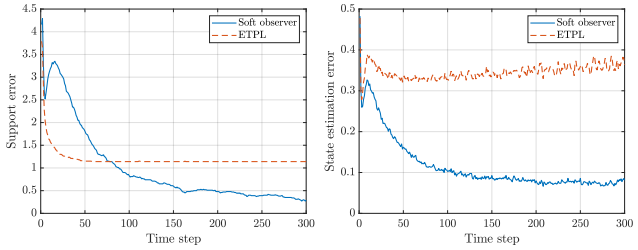

Fig. 2. Sparse soft observer vs ETPL; $n = 10$, $p = 15$, $s = 3$, $\tau = 1$. The results are averaged over 100 runs.

estimating the current state, or a delayed version, using the last $p\tau$ measurements. If $\tau = 1$, this an online (not delayed) SSE. This calls for fast recursive online algorithms.

In [3], the authors address this problem by developing a recursive version of ETPG, named ETPL. As an alternative, we develop an online version of the iterative soft thresholding algorithm (ISTA, [8]), that we name sparse soft observer, summarized in Alg. 1. We use the following notation: $\mathbf{a}(k) = (a(k-\tau+1)^\top, \dots, a(k)^\top)^\top$, $\mathbf{y}(k) = (y(k-\tau+1)^\top, \dots, y(k)^\top)^\top$.

Algorithm 1 Sparse soft observer

1: **for all** $k = \tau - 1, \tau, \dots$ **do**
2: Measurements and estimated measurements update

$$\begin{aligned} \mathbf{y}(k) &= \mathcal{O}x(k-\tau+1) + \mathbf{a}(k) \\ \hat{\mathbf{y}}(k) &= \mathcal{O}\hat{x}(k) + \hat{\mathbf{a}}(k) \end{aligned} \tag{3}$$

3: ISTA step: gradient step + soft thresholding

$$\begin{pmatrix} \hat{x}^+ \\ \hat{\mathbf{a}}^+ \end{pmatrix} = \begin{pmatrix} \hat{x}(k) \\ \hat{\mathbf{a}}(k) \end{pmatrix} - \nu \begin{pmatrix} \mathcal{O} & I \end{pmatrix}^\top [\hat{\mathbf{y}}(k) - \mathbf{y}(k)] \tag{4}$$

$$\hat{\mathbf{a}}(k+1) = \mathrm{S}_{\nu\lambda}\left[\hat{\mathbf{a}}^+\right] \tag{5}$$

4: State update

$$\hat{x}(k+1) = A\hat{x}^+ \tag{6}$$

5: **end for**

V. Numerical results

A. Lasso approach

We test the proposed Lasso approach on random, synthetic CPSs and we compare it to ETPG by [3] and Imhotep-SMT by [4]. We assume that the attack support is time-invariant with cardinality s. The attacks have magnitude in $[4, 5]$, which is sufficiently large to sabotage the state estimation, but not enough large to produce clear, plainly detectable outliers in the measurements. We assess the accuracy in terms of state estimation error $\|\hat{x} - \widetilde{x}\|_2 / \|\widetilde{x}\|_2$.

In Fig. 1, we see that Lasso outperforms ETPG both in accuracy and run time. Since we consider small/medium dimensions, Imhotep-SMT is the best approach to achieve the exact solution in fast time, in the noise-free case; nevertheless, it is not robust to noise. In contrast, Lasso and ETPG are robust to small noise.

B. Sparse soft observer

We test the proposed sparse soft observer for recursive and online SSE and we compare it to ETPL [3]. We consider th state estimation error $\|\hat{x} - \widetilde{x}\|_2 / \|\widetilde{x}\|_2$ and support error, defined as In Fig. 2 the corresponding state estimation error and support error $\sum_j |\mathbf{1}(\hat{\mathbf{a}}_j \neq 0) - \mathbf{1}(\widetilde{a}_j \neq 0)|$, where $\mathbf{1}(v) = 1$ if v is true and 0 otherwise. The sparse soft observer is more accurate and ETPL does not always converge to the right support. The execution times are $7 \cdot 10^{-5}$ seconds for ETPL and $4 \cdot 10^{-6}$ seconds for the sparse soft observer.

VI. Conclusions

We propose a Lasso approach for secure state estimation in cyber-physical systems under sparse sensor attacks. We analyse the properties of Lasso to identify the attack and, as a consequence, to recover the state. Furthermore, by starting from the iterative soft thresholding algorithm for Lasso, we develop a sparse soft observer to perform online estimation. Through numerical results, we show that the proposed Lasso approach is valuable with respect to state-of-the-art methods, although it exploits less information, e.g., on the sparsity pattern.

References

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

[2] M. Pajic, I. Lee, and G. J. Pappas, "Attack-resilient state estimation for noisy dynamical systems," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 82–92, 2017.

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

[4] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach," *IEEE Trans. Autom. Control*, vol. 62, no. 10, pp. 4917–4932, 2017.

[5] R. Tibshirani, "Regression shrinkage and selection via the Lasso," *J. Roy. Stat. Soc. Series B*, vol. 58, pp. 267–288, 1996.

[6] J. J. Fuchs, "On sparse representations in arbitrary redundant bases," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1341–1344, 2004.

[7] V. Cerone, S. M. Fosson, D. Regruto, and F. Ripa, "Lasso-based state estimation for cyber-physical systems under sensor attacks," in *Proc. SysID*, 2024.

[8] I. Daubechies, M. Defrise, and C. De Mol, "An iterative thresholding algorithm for linear inverse problems with a sparsity constraint," *Comm. Pure Appl. Math.*, vol. 57, no. 11, pp. 1413–1457, 2004.