Modeling and control of cyber-physical systems
Project I

Sophie M. Fosson

June 3, 2023

In this project, we apply the mathematical models and algorithms discussed in class to estimate the state of a system, possibly in the presence of sensors attacks. In particular, we consider problems of target localization, in a two-dimensional indoor area.

The work is conceived for groups of 3-4 students. The choice of the programming language is free; we suggest MATLAB or Python.

Students are required to write a report ($\sim$ 4-5 pages) with the analysis of the obtained results.

Objectives

The goal of this activity is to learn to

1. implement algorithms for CPSs
2. enhance the algorithms to improve the performance (e.g., by a suitable tuning of the hyper-parameters)
3. analyse the obtained results
4. write a technical report

Requirements

1. Implement the algorithms and solve the proposed problems
2. Write a report ($\sim$ 4-5 pages) with the analysis of the obtained results
3. Upload the report and the code in the delivery page of the course, at least one week before the oral examination

Task 1: Implementation of IST

We start by implementing the iterative shrinkage/thresholding algorithm (IST) to solve a synthetic Lasso problem.

Given $C \in \mathbb{R}^{q,p}$, a k-sparse $\widetilde{x} \in \mathbb{R}^p$, and noisy measurements $y = C\widetilde{x} + \eta$, where $\eta \in \mathbb{R}^q$ is the measurement noise, the "weighted" LASSO problem is:

$$\min_{x \in \mathbb{R}^p} \frac{1}{2}\|Cx - y\|_2^2 + \Lambda^\top |x|$$

where $\Lambda \in \mathbb{R}^p$ is an hyper-parameter, $|x| = (|x_1|, \ldots, |x_p|)^\top$ and $\Lambda^\top |x|$ is a weighted ℓ_1-norm.

We can solve LASSO by implementing the algorithm IST.

Algorithm 1 IST

1: Initialization: $x_0 = 0 \in \mathbb{R}^p$
2: **for all** $t = 1, \ldots, T_{max}$ **do**
3: $\quad x_{t+1} = \mathbb{S}_{\tau\Lambda}\left[x_t + \tau C^\top (y - Cx_t)\right]$
4: **end for**

Given $x \in \mathbb{R}^p$, the shrinkage/thresholding operator $\mathbb{S}_\gamma : \mathbb{R}^p \mapsto \mathbb{R}^p$, for any $\gamma = (\gamma_1, \ldots, \gamma_p)^\top \in \mathbb{R}^p_+$, is defined as

$$\mathbb{S}_{\gamma_i}(x_i) := \begin{cases} x_i - \gamma_i & \text{if } x_i > \gamma_i \\ x_i + \gamma_i & \text{if } x_i < -\gamma_i \\ 0 & \text{if } |x_i| \leq \gamma_i \end{cases}$$

for each $i = 1, \ldots, p$.

Implement IST to solve LASSO; we suggest the following data and hyper-parameters:

1. $\tau = \|C\|_2^{-2} - \epsilon$, say $\epsilon = 10^{-8}$ (see slides)
2. $q = 10$, $p = 20$, $k = 2$, $\Lambda = \lambda(1, \ldots, 1)^\top$ with $\lambda = \frac{1}{100\tau}$, so that the shrinkage/thresholding hyper-parameter is $\tau\Lambda = 10^{-2}(1, 1, \ldots, 1)^\top$.
3. Generate the components of C according to a standard normal distribution $\sim \mathcal{N}(0, 1)$ (randn)
4. Generate the support S of the true $\widetilde{x}$ with uniform distribution and the non-zero components $i \in S$ such that $\widetilde{x}_i \in [-2, -1] \cup [1, 2]$, with uniform distribution

5. Measurement noise $\eta \sim \mathcal{N}(0, \sigma^2)$, $\sigma = 10^{-2}$ ($\sigma*$randn)
6. Stop criterion: $T =$ first time instant s.t. $\|x_{T+1} - x_T\|_2 < \delta$, $\delta = 10^{-12}$.

Repeat the experiment for at least 20 runs and analyse the mean results, by considering the following points:

1. Support recovery rate: how many times the support of $\widetilde{x}$ is correctly estimated?
2. Can we obtain 100% of success in the support recovery by increasing q?
3. Convergence time: how many iterations are required (mean, min, max)?
4. What happens if we decrease τ, by keeping $\lambda = \frac{1}{100\tau}$?
5. What happens if we increase λ, by keeping $\tau = \|C\|_2^{-2} - \epsilon$?

Task 2: Secure estimation under sparse sensor attacks

Reformulate the previous problem to estimate a (non-sparse) $\widetilde{x} \in \mathbb{R}^n$ under sparse sensor attacks, by using IST, given the measurements $y = C\widetilde{x} + \eta + a$

Suggested data and hyper-parameters:

1. $n = 10$, $q = 20$, $h = 2$ sensor attacks
2. $C \sim \mathcal{N}(0, 1)$; $\widetilde{x} \sim \mathcal{N}(0, 1)$
3. Support of the attack vector a: uniform distribution
4. How to perform the attacks?
   - "Unaware" attack: $a_i \in [-2, -1] \cup [1, 2]$, uniformly distributed
   - "Aware" attack: the attacker takes the sensor measurement y_i and corrupts it of a quantity equal to $\frac{1}{2}y_i$
5. $\tau\Lambda = \tau\lambda(0, \dots, 0, 1, \dots, 1)^\top \in \mathbb{R}^{n+q}$, $\tau\lambda = 2 \times 10^{-3}$
6. Measurement noise $\eta = 0$ and $\eta \sim \mathcal{N}(0, \sigma^2)$, $\sigma = 10^{-2}$ (σ *randn)

Repeat the experiment for at least 20 runs and analyse the mean results, by considering the following points:

1. Rate of attack detection: how many times the support of a is correctly estimated, i.e., we identify the sensors under attack?
2. Estimation accuracy: is the estimation of $\widetilde{x}$ accurate? Compute $\|\widetilde{x} - \hat{x}\|_2^2$ where $\hat{x}$ is the obtained estimate

Task 3: Target localization with real data

Consider an RSS fingerprinting setting. Consider the dictionary D built with $q = 6$ sensors for $p = 7$ cells saved in file task3realdata.mat. Consider the measurement vector y saved in task3realdata.m.

1. By formulating a suitable LASSO, recover how many targets are present and localize their position (= cell).
2. Add a single sensor attack ($h = 1$) that perturbs y_i of a quantity equal to $\frac{1}{5}y_i$

- Consider $\lambda = 1$. Moreover, apply a normalization of D, namely normalize(D), before solving LASSO. Similarly, in the presence of attacks, normalize $G = (D, I)$.

Repeat the experiment by placing the attack on each sensor and analyse the results.

Task 4: Sparse observer

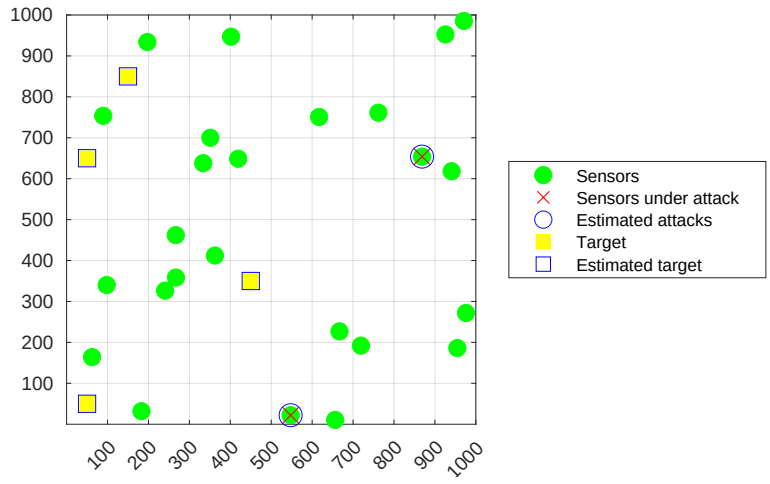
We propose a localization problem where $j = 4$ targets move in a square room with $p = 100$ cells. The vector $x(k) \in \{0, 1\}^p$ represents the current positions of the targets: if $x_i(k) = 1$, there is a target in the cell i. $q = 25$ sensors are randomly deployed in the room, and they take RSS measurements. We assume that $h = 2$ sensors are under attack; the sensors under attack are the same for the overall experiment.

The model is

$$x(k+1) = Ax(k)$$
$$y(k) = Dx(k) + \eta + a$$

A and D are given in the file task4data.mat
Other data:

- $G = [D, I] \rightarrow$ normalize G, e.g., by using normalize(G) in MATLAB
- $\hat{z}(k) = [\hat{x}(k)), \hat{a}(k)] \in \mathbb{R}^{p+q}$
- $\hat{z}(0) = 0$
- η is a measurement noise; $\eta \sim \mathcal{N}(0, \sigma^2)$, $\sigma = 0.2$ (MATLAB: σ* randn)



- Choice of which sensors are under attack: random
  - "Unaware" time-invariant attack: $a_i = 30$ for each sensor i under attac
  - Possible extension: "Aware" time-varying attack: the attacker takes the sensor measurement y_i and corrupts it of a quantity equal to, e.g., $0.5y_i$
- $T = 50$ (or more)
- $\tau = \|G\|_2^{-2} - \epsilon$
- $\Lambda = (10, \ldots, 10, 20, \ldots, 20)$
- Final refinement of the attacks: put to zero all the estimated components with magnitude below 2
- For the state estimation: take the $j = 4$ largest components

Algorithm 2 Sparse observer

for all $k = 1, \ldots, T$ **do**
  $\hat{z}(k + \frac{1}{2}) = \mathbb{S}_{\tau\Lambda}\left[\hat{z}(k) + \tau G^\top (y(k) - G\hat{z}(k))\right]$
  $\hat{x}(k + 1) = A\hat{x}(k + \frac{1}{2})$
  $\hat{a}(k + 1) = \hat{a}(k + \frac{1}{2})$
end for

Task 5: Distributed estimation

In this task, we consider the secure estimation problem of Task 2 and we solve it in-network, through the distributed IST (DIST) algorithm.

Our aim is to estimate a (non-sparse) $\widetilde{x} \in \mathbb{R}^n$ in the preseece of sparse sensor attacks, given the measurements $y = C\widetilde{x} + \eta + a \in \mathbb{R}^q$, where $\eta \in \mathbb{R}^q$ is a meausurement noise and $a \in \mathbb{R}^q$ is the attack vector.

We consider a distributed setting where each sensor node $i \in \{1, \dots, q\}$ knows C_i ($= i$th row of C) and $y_i \in \mathbb{R}$, and it does not share them.

We notice that the model $y = C\widetilde{x} + \eta + a \in \mathbb{R}^q$ respresent attacks a_i's that consist in a physical tampering of the sensor measurements $C_i\widetilde{x}$. We do not consider attacks on the communication links. This is a difference with respect to the centralized case, where a manipulation of $C_i\widetilde{x}$ can be done either on the sensor or in the transmission of the data to the fusion center.

In the file stochasticmatrices.mat, we provide 4 possible network topologies, described by 4 different stochastic matrices Q. Check whether these matrices solve the consensus problem, by analyzing their eigenvalues. Moreover, analyze their essential spectral radius to guess which one will yield faster convergence.

Repeat the task for each stochastic matrix.

Data and hyper-parameters:

1. $n = 10$, $q = 20$, $h = 2$ sensor attacks
2. $C \sim \mathcal{N}(0, 1)$; $\widetilde{x} \sim \mathcal{N}(0, 1)$
3. Support S of the attack vector a: random, uniformly distributed
4. Measurement noise $\eta \sim \mathcal{N}(0, \sigma^2)$, $\sigma = 10^{-2}$ ($\sigma*$ randn)
5. "Unaware" attack: $a_i \in [-2, -1] \cup [1, 2]$ for each $i \in S$, uniformly distributed
6. $\tau\Lambda = \tau\lambda(0, \dots, 0, 1, \dots, 1)^\top \in \mathbb{R}^{n+q}$, $\tau = 0.03$, $\lambda = \frac{2\times10^{-4}}{\tau}$
7. Final refinement of the attacks: set to zero all the estimated attack components with magnitude < 0.2

In the Algorithm 3, $z^{(i)}(k) = (x^{(i)}(k), a^{(i)}(k))^\top \in \mathbb{R}^{n+q}$ is the local estimate of both $\widetilde{x}$ and a, by node i, at time k. Moreover, $G = (D, I)$

Repeat the experiment for at least 20 runs and analyse the mean results, by considering the following points:

1. Is consensus achieved, i.e., do the nodes obtain (almost) the same estimate?

Algorithm 3 DIST

1: Initialization: for each node $i = 1, \dots, q$, $z^{(i)}(0) \in \mathbb{R}^{n+q}$, e.g., $z^{(i)}(0) = 0$
2: **for all** $k = 1, \dots, T$ **do**
3: **for all** $i = 1, \dots, q$ **do**
4: $$z^{(i)}(k+1) = \mathbb{S}_{\tau\Lambda}\left[\sum_{j=1}^{q} Q_{i,j} z^{(j)}(k) + \tau G_i^T (y_i - G_i z^{(i)}(k))\right]$$
5: **end for**
6: Stop criterion: $T =$ first time instant s.t. $\sum_{i=1}^{q} \|z^{(i)}(T+1) - z^{(i)}(T)\|_2 < \delta$, $\delta = 10^{-7}$. Since the algorithm may be very slow, set also a maximum $T = 10^5$
7: **end for**

2. Rate of attack detection: how many times the support of a is correctly estimated, i.e., we identify the sensors under attack?

3. Estimation accuracy: is the estimation of $\widetilde{x}$ accurate? Compute $\|\widetilde{x} - \bar{x}\|_2^2$ where $\bar{x}$ is the mean of the estimates of all the nodes.

4. Convergence time (= number of iterations): can you see a relationship between the essential spectral radius of Q and the convergence time?