Multi-dimensional state estimation in adversarial environment

Yilin Mo

School of Electrical and Electronics Engineering
Nanayang Technological University

2015-07-28

Joint Work with Prof. Richard M. Murray

Motivation

- Sensor networks are becoming ubiquitous
- Sensors are usually cheap, distributed in space and physically exposed, which makes it difficult to ensure security for every single sensor
- Our goal: to design the optimal state estimator in the presence of compromised sensory data

System Model

- We assume that $x \in \mathbb{R}^n$ is the state
- m sensors are deployed to monitor the system. Denote $y_i \in \mathbb{R}$ as the measurement generated by sensor i.
- Denote $y = \begin{bmatrix} y_1 & \dots & y_m \end{bmatrix}^T$ as the collection of all sensory data.
- We assume the following sensor model

$$y = Hx + Gw + a,$$

where $\|w\| \leq \delta$ represents measurement noise and $\|a\|_0 \leq l$ is the bias injected by the adversary.

Estimation Error

- An estimator f is a mapping from sensory data y to a state estimate $\hat{x} = f(y)$.
- The estimation error can be defined as $e \triangleq x - f(y)$.
- Clearly the estimation error is a function of x, w, a and our choice of estimator f.
- In this presentation, we will consider the worst-case error defined as

$$e^*(f) = \sup_{x,w,a} \|e\|$$

.

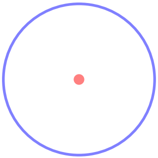
Some Preliminary Results

- Assume that $S \subset \mathbb{R}^n$ is bounded.
- We say that a ball $B(x, r)$ covers S if $S \subset B(x, r)$.
- For any point $x \in \mathbb{R}^n$, denote $\rho(x, S)$ as the radius of the minimum ball that centers at x and covers S.
- Define the Chebyshev center and the radius of S as

$$r(S) \triangleq \inf_{x \in \mathbb{R}^n} \rho(x, S),\ c(S) \triangleq \arg\min_{x \in \mathbb{R}^n} \rho(x, S).$$

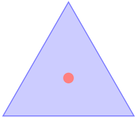
- We further define the diameter of S as $d(S) \triangleq \sup_{x, x' \in S} \|x - x'\|$.

Example



- A circle with radius 1.
- The radius $r(S)$ is 1 and diameter $d(S)$ is 2.
- Notice that the Chebyshev center may not in the set S.

Example



- A equilateral triangle with side length 1
- The radius $r(S)$ is $1/\sqrt{3}$ and diameter $d(S)$ is 1.
- For general set S in R^n, $r(S) \neq d(S)/2$.
- However, we can prove the following inequalities (Jung's Theorem):

$$\frac{d(S)}{2} \leq r(S) \leq \sqrt{\frac{n}{2n+2}} d(S) \leq \frac{1}{\sqrt{2}} d(S).$$

Estimator Design

- Let us denote $\mathbb{Y}$ as the set of all feasible measurements y, i.e., there exist x, $\|w\| \leq \delta$ and $\|a\|_0 \leq l$, such that $y = Hx + Gw + a$.
- For any $y \in \mathbb{Y}$, let us denote $\mathbb{X}(y)$ as the set of all feasible x that can generate y, i.e., there exist $\|w\| \leq \delta$ and $\|a\|_0 \leq l$, such that $Hx = y - Gw - a$.

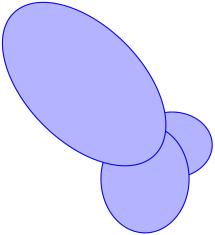


Figure : $\mathbb{X}(y)$

Estimator Design

- For a given $y \in \mathbb{Y}$, the worst-case error is $\sup_{x\in\mathbb{X}(y)} \|x - f(y)\|$.
- If $\mathbb{X}(y)$ is bounded, then the optimal estimator should be $f(y) = c(\mathbb{X}(y))$.
- Therefore, the worst-case error is

$$e^*(f) = \sup_{y\in\mathbb{Y}} r(\mathbb{X}(y)).$$

- How to efficiently compute the Chebyshev center?
- How to characterize the performance of the optimal estimator?

Some Definitions

- Let $\mathcal{I} = \{i_1, i_2, ..., i_j\} \subset \{1, 2, \dots, m\}$ be an index set.
- Define

$$y_{\mathcal{I}} \triangleq \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_j} \end{bmatrix}, a_{\mathcal{I}} \triangleq \begin{bmatrix} a_{i_1} \\ a_{i_2} \\ \vdots \\ a_{i_j} \end{bmatrix}, H_{\mathcal{I}} \triangleq \begin{bmatrix} h_{i_1} \\ h_{i_2} \\ \vdots \\ h_{i_j} \end{bmatrix}. G_{\mathcal{I}} \triangleq \begin{bmatrix} g_{i_1} \\ g_{i_2} \\ \vdots \\ g_{i_j} \end{bmatrix}.$$

The Shape of $\mathbb{X}(y)$

- Consider an index set $\mathcal{I} = \{i_1, \dots, i_{m-l}\}$.
- Define set $\mathbb{X}_{\mathcal{I}}(y) \subset \mathbb{R}^n$ as

$$\mathbb{X}_{\mathcal{I}}(y) \triangleq \{x : \exists \|w\| \leq \delta, a_{\mathcal{I}} = 0, \text{ such that } y = Hx + Gw + a\}.$$

- The set $\mathbb{X}$ can be seen as

$$\mathbb{X}(y) = \bigcup_{|\mathcal{I}|=m-l} \mathbb{X}_{\mathcal{I}}(y).$$

- Since $a_{\mathcal{I}} = 0$ and $a_{\mathcal{I}^c}$ could be any vector, $y = Hx + Gw + a$ is equivalent to

$$y_{\mathcal{I}} = H_{\mathcal{I}}x + G_{\mathcal{I}}w.$$

The Shape of $\mathbb{X}_\mathcal{I}(y)$

- Define

$$F_\mathcal{I} \triangleq G_\mathcal{I} G_\mathcal{I}^T,\ K_\mathcal{I} \triangleq \left(H_\mathcal{I}^T F_\mathcal{I}^{-1} H_\mathcal{I}\right)^{-1} H_\mathcal{I}^T F_\mathcal{I}^{-1},$$
$$P_\mathcal{I} \triangleq \left(H_\mathcal{I}^T F_\mathcal{I}^{-1} H_\mathcal{I}\right)^{-1},\ U_\mathcal{I} \triangleq (I - H_\mathcal{I} K_\mathcal{I})^T F_\mathcal{I}^{-1} (I - H_\mathcal{I} K_\mathcal{I}).$$

- Define

$$\hat{x}_\mathcal{I}(y) = K_\mathcal{I} y_\mathcal{I},\ \varepsilon_\mathcal{I}(y) = y_\mathcal{I}^T U_\mathcal{I} y_\mathcal{I}.$$

Theorem (The shape of $\mathbb{X}_\mathcal{I}(y)$)

If $\varepsilon_\mathcal{I}(y) > \delta^2$, then $\mathbb{X}_\mathcal{I}(y)$ is an empty set. Otherwise, $\mathbb{X}_\mathcal{I}(y)$ is an ellipsoid given by

$$\mathbb{X}_\mathcal{I}(y) = \{x : (x - \hat{x}_\mathcal{I}(y))^T P_\mathcal{I}^{-1} (x - \hat{x}_\mathcal{I}(y)) \le \delta^2 - \varepsilon_\mathcal{I}(y)\}.$$

How to Compute the Chebyshev Center of $\mathbb{X}(y)$.

Theorem (LMI Formulation)

A ball $B(x, r)$ covers $\mathbb{X}(y)$ if and only if for every index set $|\mathcal{I}| = m - l$, such that

$$\varepsilon_{\mathcal{I}}(y) \leq \delta^2,$$

there exists $\tau_{\mathcal{I}} \geq 0$, such that

$$\tau_{\mathcal{I}} \Omega_{\mathcal{I}} \geq \begin{bmatrix} I & -x & 0 \\ -x^T & -r^2 & x^T \\ 0 & x & -I \end{bmatrix},$$

where $\Omega_{\mathcal{I}}$ is defined as,

$$\Omega_{\mathcal{I}} = \begin{bmatrix} P_{\mathcal{I}}^{-1} & -P_{\mathcal{I}}^{-1} \hat{x}_{\mathcal{I}}(y) & 0 \\ -\hat{x}_{\mathcal{I}}(y)^T P_{\mathcal{I}}^{-1} & \hat{x}_{\mathcal{I}}(y)^T P_{\mathcal{I}}^{-1} \hat{x}_{\mathcal{I}}(y) + \varepsilon_{\mathcal{I}}(y) - \delta^2 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

An SDP Algorithm to Compute the Chebyshev Center

The Chebyshev center of $\mathbb{X}(y)$ can be computed via the following SDP:

SDP

$$
\begin{aligned}
\underset{\hat{x},\varphi,\tau_{\mathcal{I}}}{\text{minimize}} \quad & \varphi \\
\text{subject to} \quad & \varphi \geq 0, \\
& \tau_{\mathcal{I}} \geq 0, \\
& \tau_{\mathcal{I}}\Omega_{\mathcal{I}} \geq \begin{bmatrix} I & -\hat{x} & 0 \\ -\hat{x}^T & -\varphi & \hat{x}^T \\ 0 & \hat{x} & -I \end{bmatrix}, \text{ if } \varepsilon_{\mathcal{I}}(y) \leq \delta^2.
\end{aligned}
$$

where the radius of the Chebyshev ball is $r = \sqrt{\varphi}$.

The Performance of the Optimal Estimator

Theorem (Bounds on $e^*(f)$)

- *If there exists an index set $\mathcal{K} \subset \mathcal{S}$ with cardinality $m - 2l$, such that $H_{\mathcal{K}}$ is not of full column rank, then $e^* = \infty$.*
- *If for all $|\mathcal{K}| = m - 2l$, $H_{\mathcal{K}}$ is full column rank, then for all possible $y \in \mathbb{Y}$, we have*

$$\sup_{y \in \mathbb{Y}} d(\mathbb{X}(y)) = 2\delta \max_{|\mathcal{K}|=m-2l} \sqrt{\sigma(P_{\mathcal{K}})}.$$

Therefore, e^* satisfies

$$\max_{|\mathcal{K}|=m-2l} \delta\sqrt{\sigma(P_{\mathcal{K}})} \le e^* \le \max_{|\mathcal{K}|=m-2l} \delta\sqrt{2\sigma(P_{\mathcal{K}})},$$

where $\sigma(P)$ is the spectral radius of P.

Numerical Examples

- We consider the following system:

$$H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & -1 \end{bmatrix}, G = I.$$

- Assume 1 sensor is compromised.
- The y is chosen to maximize $r(\mathbb{X}(y))$:

$$y = \begin{bmatrix} -0.851 \\ 2.753 \\ 0.5257 \\ 0 \end{bmatrix}.$$

- The optimal state estimate is

$$\hat{x} = \begin{bmatrix} -0.851 \\ 1.376 \end{bmatrix},$$

and the corresponding error is 1.618.

Numerical Examples

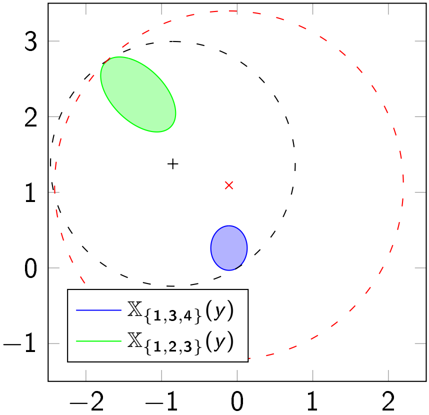


Figure : The performance of the optimal state estimator. The green ellipse corresponds to $\mathbb{X}_{\{1,3,4\}}(y)$ and the red ellipse corresponds to $\mathbb{X}_{\{1,2,3\}}(y)$. The set $\mathbb{X}_{\{2,3,4\}}(y)$ and $\mathbb{X}_{\{1,2,4\}}(y)$ is empty. The black "+" is the optimal state estimate while the black dashed line is the Chebyshev ball for $\mathbb{X}(y)$.

Conclusion and Future Work

- We consider the problem of state estimation from static sensory data, which could be compromised by an adversary.
- We provide an SDP algorithm to compute the optimal state estimate.
- We also characterize the performance of the optimal estimator.
- We would like to consider more general sensor model (stochastic sensor noise, non-linear sensor model) and dynamic state estimation problem in the future.