Secure State Estimation for Cyber-Physical Systems Under Attack

Project-II (IE47006) report submitted to

Indian Institute of Technology Kharagpur

in partial fulfilment for the award of the degree of

Bachelor of Technology

in

Instrumentation Engineering

by

Adnan M. Lokhandwala

(16IE10003)

Under the supervision of

Professor Siddhartha Sen

Department of Electrical Engineering

Indian Institute of Technology Kharagpur

Spring Semester, 2019-2020

March 18, 2020

DECLARATION

I certify that

(a) The work contained in this report has been done by me under the guidance of my supervisor.

(b) The work has not been submitted to any other Institute for any degree or diploma.

(c) I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.

(d) Whenever I have used materials (data, theoretical analysis, figures, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references. Further, I have taken permission from the copyright owners of the sources, whenever necessary.

Date: March 18, 2020	(Adnan M. Lokhandwala)
Place: Kharagpur	(16IE10003)

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR
KHARAGPUR - 721302, INDIA

CERTIFICATE

This is to certify that the project report entitled "**Secure State Estimation for Cyber-Physical Systems Under Attack**" submitted by **Adnan M. Lokhandwala** (Roll No. 16IE10003) to Indian Institute of Technology Kharagpur towards partial fulfilment of requirements for the award of degree of Bachelor of Technology in Instrumentation Engineering is a record of bona fide work carried out by him under my supervision and guidance during Spring Semester, 2019-2020.

Professor Siddhartha Sen
Department of Electrical Engineering
Indian Institute of Technology Kharagpur
Kharagpur - 721302, India

Date: March 18, 2020
Place: Kharagpur

Abstract

Name of the student: **Adnan M. Lokhandwala** Roll No: **16IE10003**

Degree for which submitted: **Bachelor of Technology**

Department: **Department of Electrical Engineering**

Thesis title: **Secure State Estimation for Cyber-Physical Systems Under Attack**

Thesis supervisor: **Professor Siddhartha Sen**

Month and year of thesis submission: **March 18, 2020**

The vast majority of today's critical infrastructure is supported by numerous feedback control loops and an attack on these control loops can have disastrous consequences. This is a major concern since modern control systems are becoming large and decentralized and thus more vulnerable to attacks. This report is concerned with the estimation and control of linear systems when some of the sensors or actuators are corrupted by an attacker. In particular, this report provides the implementation results of a state estimation algorithm and the mathematical foundations behind it, as shown in [3].

Acknowledgements

This document is prepared by the inspiration received from Professor Siddhartha Sen, Department of Electrical Engineering, Indian Institute of Technology Kharagpur.

Heartfelt gratitude to my friends and family for their constant support

Contents

Chapter 1

Introduction

The economic and societal potential of cyber-physical systems is astonishing, and major investments are being made worldwide to develop the technology. For instance, the December 2010 report of the U.S. President's Council of Advisors on Science and Technology[4] called for continued investment in CPS research because of its scientific and technological importance as well as its potential impact on grand challenges in a number of sectors critical to U.S. security and competitiveness, including aerospace, automotive, chemical production, civil infrastructure, energy, healthcare, manufacturing, materials and transportation. Also, the anticipated funding to research and education projects on CPS amounts to approximately $34,000,000 each year [7], and the European Union has a similar vision on the importance of research on CPS[9].

It goes without saying that in this type of systems security is a primary concern and, because of the tight cyber-physical coupling, it is one of the main scientific challenges. Indeed, CPS security is attracting several research efforts from different and independent areas (e.g., secure control, intrusion detection in SCADA systems, etc.), each of them with specific peculiarities, features, and capabilities.

This work deals with a specific problem of state estimation when the system is under attack. It's main focus is on the implementation of [3]. This paper deals with theoretical as well as algorithmic aspects of estimation and control of linear plants subject to attacks. On the theoretical side, it gives a new characterization of the maximum resilience of a system to attacks and proves new results concerning the separation of estimation and control. On the algorithmic side it adopts a novel point of view inspired from error-correction over the reals and proposes a new estimation algorithm that is robust against attacks and that is also computationally efficient.

Chapter 2

Literature Survey

Literature on physics-based cyber-physical system security is heavily focused on the power grid application field, that is power transmission, power distribution, power generation and the electricity market. Other papers deal with generic linear dynamic systems, and a small fraction of papers deal with applications such as (unmanned) aerial and ground vehicles, irrigation and water supply and building automation.

The attention to power grids are due to many reasons. Power grids are drivers for sustained economic prosperity, quality of life and global competitiveness of a nation. The models used in power grids are well known and the market growth in renewable energy devices brings with it novel problems in design and management, providing a boost to academic research on topics such as performance, safety and security. [11]

Security can be seen as a composition of three main attributes, namely confidentiality, integrity and availability [5]. Regardless of the adopted point of view (attack, defense or both), every study on CPS security deals with attacks in order to either implement or to counteract them. Each attack threats one or more primary security attributes. More specifically, the best known attack on availability is the denial of service (DoS) attack, that renders inaccessible some or all the components of a control system by preventing transmissions of sensor or/and control data over the network. To launch a DoS an adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood with network traffic some devices[1]. Attacks on data integrity are known as

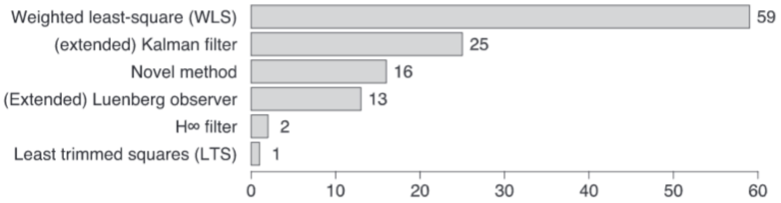

Figure 2.1: Distribution of studies according to state estimation method used, [11]

deception attacks and represent the largest class of attacks on cyber-physical systems, including false data injection attacks. The attacks on confidentiality alone are often referred to as disclosure attacks, i.e. eavesdropping.

[11] surveyed 108 papers, and analysed the state estimation techniques used by them, as presented in Figure 2.1. Among the novel state estimation methods, [8] showed that implementation issues such as jitter, latency and synchronization errors can be mapped into parameters of the state estimation procedure that describe modeling errors, and provides a bound on the state estimation error caused by modeling errors. [6] constructed an optimal estimator of a scalar state that minimizes the "worst-case" expected cost against all possible manipulations of measurements by the attacker, while [10] introduced a minimum mean-squared error resilient (MMSE-R) estimator for stochastic systems, whose conditional mean squared error from the state remains finitely bounded and is independent of additive measurement attacks.

Chapter 3

Formal Settings and notation

Consider the linear control system given by the equations (3.1)

$$\begin{aligned} x^{(t+1)} &= Ax^{(t)} + B(U^{(t)}(y^{(0)}, ..., y^{(t)}) + w^{(t)}) \\ y^{(t)} &= Cx^{(t)} + e^{(t)} \end{aligned} \tag{3.1}$$

Here $x^{(t)} \in \mathbb{R}^n$ represents the state of the system at time $t \in \mathbb{N}$, and $y^{(t)} \in \mathbb{R}^p$ is the output of the sensors at time t. The control input applied at time t depends on the past measurements $(y^{(\tau)})_{0 \leqslant \tau \leqslant t}$ through the output feedback map $U^{(t)}$. The vector $e^{(t)} \in \mathbb{R}^p$ represents the attacks injected by the attacker in the different sensors, and the vector $w^{(t)} \in \mathbb{R}^m$ represents the attacks injected in the actuators. Note that if sensor $i \in \{1, ..., p\}$ is not attacked then necessarily $e_i^{(t)} = 0$ and the output $y_i^{(t)}$ of sensor i is not corrupted, otherwise $e_i^{(t)}$ (and therefore $y_i^{(t)}$) can take any value. The same observation holds for the attacks on actuators $w^{(t)}$.

We will assume that the set of attacked nodes does not change over time. Moreover, since we are dealing with a malicious agent, we will not assume the attacks $e_i^{(t)}$ or $w_j^{(t)}$ (for an attacked sensor i or actuator j) to follow any particular model and we will simply take them to be arbitrary real numbers. The only assumption concerning the malicious agent will be about the number of nodes that were attacked.

We use the following notations throughout the paper. If S is a set, we denote by $|S|$ the cardinality of S and by S^c the complement of S. For a vector $x^{(t)} \in \mathbb{R}^n$, the support of x, denoted by $supp(x)$, is the set of nonzero components of x and the l_0 norm of x is the number of nonzero components of x

$$supp(x) = \{i \in \{1, ..., n\} | x_i \neq 0\}$$
$$\parallel x \parallel_{l_0} = |supp(x)|$$

For a matrix $M \in \mathbb{R}^{m \times n}$ we denote by $M_i \in \mathbb{R}^n$ the i'th row of M, for $\{i \in \{1, ..., m\}$. We define the *rowsupport* of M to be the set of nonzero rows of M and we denote by $\parallel M \parallel_{l_0}$ the cardinality of the row support of M

$rowsupp(M) = \{i\{1, ..., m\} | M_i \neq 0\}$
$\parallel M \parallel_{l_0} = |rowsupp(M)|$

Chapter 4

Estimation Problem

In this section we deal with the problem of estimating the state of a linear dynamical system in the presence of attacks. Throughout the main part of this section we will assume that attacks only occur on the sensors (i.e., no attacks on actuators) for ease of exposition. At the end of the section though we show how to extend the results to the case where there are also attacks on the actuators. We consider in this section linear dynamical systems of the form (4.1)

$$\begin{aligned} x^{(t+1)} &= Ax^{(t)} \\ y^{(t)} &= Cx^{(t)} + e^{(t)} \end{aligned} \tag{4.1}$$

As mentioned before, $e^{(t)} \in \mathbb{R}^p$ are the attack vectors injected by the malicious agent in the sensors. For simplicity we have also discarded the control input $BU^{(t)}(y^{(0)}, ..., y^{(t)})$ since it does not affect the results in this section. Indeed, the results presented here hold for any linear affine system where the state evolves according to $x^{(t+1)} = Ax^{(t)} + v^{(t)}$ where $v^{(t)}$ is a known input.

The problem that we consider in this section is to reconstruct the initial state $x^{(0)}$ of the plant from the corrupted observations $(y^{(t)})_{t=0,...,T-1}$. Note that since the matrix A is known, the problem of reconstructing the current state $x^{(t)}$ or the initial state $x^{(0)}$ are—at least theoretically, when A is invertible—equivalent. Therefore, there is no loss of generality in focusing on the reconstruction of $x^{(0)}$ instead of the current state $x(T-1)$.

Chapter 5

Error Correction and Number of Correctable Attacks

Let $x^{(0)} \in \mathbb{R}^n$ be the initial state of the plant and let $(y^{(t)})_{t=0,...,T-1} \in \mathbb{R}^p$ be the first T measurements that are transmitted from the sensors to the receiver device. The objective of the receiver device is to reconstruct the initial state $x^{(0)}$ from these measurements. These vectors are given by

$$y^{(t)} = CA^t x^{(0)} + e^{(t)}$$

where e(t) represent the error vector

Recall that $supp(e^{(t)}) \subset K$ with $K \subset \{1, ..., p\}$ being the set of sensors that are attacked and whose data is unreliable.

Having received the T vectors $y^{(0)}, ..., y^{(T-1)}$, the receiver uses a decoder $D : (\mathbb{R}^p)^T \to \mathbb{R}^n$ in order to estimate the initial state $x^{(0)}$ of the plant. The decoder correctly estimates the initial state if $D(y^{(0)}, ..., y^{(T-1)}) = x^{(0)}$.

5.1 Definition 1

We say that q errors are correctable after T steps by the decoder $D : (\mathbb{R}^p)^T \to \mathbb{R}^n$ if for any $x^{(0)} \in \mathbb{R}^n$, any $K \subset \{1, ..., p\}$ with $|K| \leq q$, and any sequence of vectors

$e^{(0)}, ..., e^{(T-1)}$ in $\mathbb{R}^p$ such that $supp(e^{(t)}) \subset K$, we have $D(y^{(0)}, ..., y^{(T-1)}) = x^{(0)}$. where $y^{(t)} = CA^t x^{(0)} + e^{(t)}$ for $t = 0, ..., T-1$

Let $E_{q,T}$ denote the set of error vectors $(e^{(0)}, ..., e^{(T-1)}) \in (\mathbb{R}^p)^T$ that satisfy $\forall t \in \{0, ..., T-1\}$, $supp(e^{(t)}) \subset K$ for some $K \subset \{1, ..., p\}$ with $|K| \leq q$.

5.2 Characterization of the Number of Correctable Errors

Observe that, by definition 1, the existence of a decoder that can correct q errors is equivalent to saying that the following map:

$$\begin{aligned} \mathbb{R}^n \times E_{q,T} &\to (\mathbb{R}^p)^T \\ (x^{(0)}, e^{(0)}, ..., e^{(T-1)}) &\to (y^{(0)}, ..., y^{(T-1)}) = \\ &(Cx^{(0)} + e^{(0)}, ..., CA^{T-1}x^{(0)} + e^{(T-1)}) \end{aligned} \tag{5.1}$$

is invertible, or, more precisely, that it has an inverse for the first n components of its domain. Thus expressing injectivity of this map is equivalent to saying that q errors are correctable. This gives the following proposition

5.3 Proposition 1

Let $T \in \mathbb{N} \setminus \{0\}$. The following are equivalent:

(i) There is no decoder that can correct q errors after T steps;

(ii) There exists x_a, $x_b \in \mathbb{R}^n$ with $x_a \neq x_b$, and error vectors $(e_a^{(0)}, ..., e_a^{(T-1)}) \in E_{q,T}$ and $(e_b^{(0)}, ..., e_b^{(T-1)}) \in E_{q,T}$ such that $A_a^t + e_a^{(t)} = A^t x_b + e_b^{(t)}$ for all $t \in \{0, ..., T-1\}$.

The proposition above simply says that it is not possible to unambiguously recover the state $x^{(0)}$ if there are two distinct values x_a and x_b with $x_a \neq x_b$ that can, with less than q corrupted sensors, explain the received data.

We now give a necessary and sufficient condition for q errors to be correctable that is simpler than the one in proposition 1.

5.4 Proposition 2

Let $T \in \mathbb{N} \setminus \{0\}$. The following are equivalent:

(i) There is a decoder that can correct q errors after T steps;

(ii) For all $z \in \mathbb{R}^n \setminus \{0\}$, $|supp(Cz) \cup supp(CAz) \cup ... \cup supp(CA^{T-1}z)| > 2q$.

Please refer to [3] for detailed proofs.

Observe also that the characterization of proposition 2 shows that the maximum number of correctable errors cannot increase beyond $T = n$ measurements. Indeed, this is a direct consequence of the Cayley-Hamilton theorem since we have for any z and for $t \geq n$, $supp(CA^t z) \subset supp(Cz) \cup supp(CAz) \cup ... \cup supp(CA^{n-1}z)$

Finally, one can also directly see from the same proposition that the number of correctable errors is always less than $p/2$, for any T.

5.5 Proposition 3

For almost all pairs $(A, C) \in \mathbb{R}^{n\times n} \times \mathbb{R}^{p\times p}$ the number of correctable errors after T = n steps is maximal and equal to $\lceil p/2 - 1 \rceil$

That is, except on a set of Lebesgue measure zero in $\mathbb{R}^{n\times n} \times \mathbb{R}^{p\times p}$. Note that the Proposition does not apply if we are only interested in matrices (A, C) that have a particular structure (e.g., lie in a certain subspace of $\mathbb{R}^{n\times n} \times \mathbb{R}^{p\times p}$) since the set of pairs with such structure can itself have a zero Lebesgue measure in $\mathbb{R}^{n\times n} \times \mathbb{R}^{p\times p}$.

Chapter 6

Optimization Formulation of the Optimal Decoder

6.1 The l_0 Decoder

Consider the decoder $D_0 : \mathbb{R}^n \rightarrow (\mathbb{R}^p)^T$ defined such that $D_0(y^{(0)}, ..., y^{(T-1)})$ is the optimal $\hat{x}$ solution of the following optimization problem:

$$\begin{aligned} &\min_{\hat{x}\in\mathbb{R}^n, \hat{K}\subset\{1,...,p\}} |\hat{K}| \\ &\text{subject to } supp(y^{(t)} - CA^t\hat{x}) \subset \hat{K} \text{ for } t \in \{0, ..., T-1\} \end{aligned} \tag{6.1}$$

Observe that the decoder D_0 looks for the smallest set K of attacked sensors that can explain the received data $y^{(0)}, ..., y^{(T-1)}$. We show in the next proposition that the decoder D_0 is optimal in terms of error-correction capabilities.

6.2 Proposition 4

Assume that q errors are correctable after T steps, i.e., that (4) holds. Then the decoder D_0 corrects q errors, i.e., for any $x^{(0)} \in \mathbb{R}^n$, and any $(e^{(0)}, ..., e^{(T-1)}) \in \mathbb{R}^p$

such that $supp(e^{(t)}) \subset K$ with $|K| \leq q$, we have $D_0(y^{(0)}, ..., y^{(T-1)}) = x^{(0)}$ where $y^{(t)} = CA^t x^{(0)} + e^{(t)}$ for $t = 0, ..., T-1$

Refer to [3] for the detailed proof.

The proposition above therefore shows that the decoder D_0 is the best decoder in terms of error-correction capabilities, since if any decoder can correct q errors, then D_0 can as well. One issue however is that the optimization problem is not practical since it is NP-hard in general.

However, [2] proposed to replace the l_0 "norm" by an l_1 norm, thereby transforming the problem into a convex program that can be efficiently solved

$\min_{\hat{x} \in \mathbb{R}^n} \parallel y - C\hat{x} \parallel_{l_1}$

It was then shown in that if the matrix C satisfies certain conditions, then the solution of this convex program is the same as the one given by the l_0 optimal decoder. In the next section we consider this relaxation in the context of our problem.

6.3 The l_1 Decoder: A Relaxation of the Optimal Decoder

For $T \in \mathbb{N} \setminus \{0\}$, consider the linear map $\phi^{(T)}$ defined by

$\phi^{(T)} : \mathbb{R}^n \to (\mathbb{R}^p)^T$

$x \to [Cx \mid CAx \mid ... \mid CA^{T-1}x]$

Furthermore, if $y^{(0)}, ..., y^{(T-1)} \in \mathbb{R}^p$, let $Y^{(T)}$ the $p \times T$ matrix formed by concatenating the $y^{(t)}$'s in columns

$Y^{(T)} = [y^{(0)} \mid y^{(1)} \mid ... \mid y^{(T-1)}] \in \mathbb{R}^{pT}$

Recall that for a matrix $M \in \mathbb{R}^{pT}$ with rows $M_1, ..., M_p \in \mathbb{R}^T$ the 0 "norm" of M is the number of nonzero rows in M

$\parallel M \parallel_{l_0} = |rowsupp(M)| = |\{i \in \{1, ..., p\} | M_i \neq 0\}|$

Observe that the optimal decoder D_0 introduced in the previous section can be written as

$$D_0(y^{(0)}, ..., y^{(T-1)}) = arg\min_{\hat{x}\in\mathbb{R}^n} \parallel Y^{(T)} - \phi^{(T)}\hat{x} \parallel_{l_0}$$

As we saw in the previous section, this decoder finds the minimum number of attacked sensors that can explain the received data $(y^{(0)}, ..., y^{(T-1)})$. Analogously to [2], we can define an l_1 decoder which, instead of minimizing the number of nonzero rows, minimizes the sum of the magnitudes of each row. Specifically, if we measure the magnitude of a row by its l_r norm in $\mathbb{R}^T$ (for $r \geq 1$), we obtain the following decoder $D_{1,r}$:

$$D_{1,r}(y^{(0)}, ..., y^{(T-1)}) = arg\min_{\hat{x}\in\mathbb{R}^n} \parallel Y^{(T)} - \phi^{(T)}\hat{x} \parallel_{l_1/l_r}$$

where, by definition, $\parallel M \parallel l_1/l_r$ is the sum of the l_r norms of the rows of the matrix M

$$\parallel M \parallel_{l_1/l_r} = \sum_{i=1}^{p} \parallel M_i \parallel_{l_r}$$

Chapter 7

THE CONTROL PROBLEM WITH OUTPUT-FEEDBACK

7.1 Problem Formulation

In this section we consider general linear control systems with output feedback of the form

$$\begin{aligned} x^{(t+1)} &= Ax^{(t)} + B(U^{(t)}(y^{(0)}, ..., y^{(t)})) \\ y^{(t)} &= Cx^{(t)} + e^{(t)} \end{aligned} \tag{7.1}$$

One of the main questions that we address in this section is to determine whether for a given system (A, B, C), there exists a control law (i.e., a family $(U^{(t)})_{t=0,1,...}$) that drives the state of the system 7.1 to the origin even if some of the sensors are attacked. Observe that the sensor attacks can affect the control inputs (since the control inputs are function of the $y^{(t)}$'s) which can in turn deviate the state $x^{(t)}$ from its nominal path.

Note that if there were attacks on the actuators then such a stabilizing control law does not exist in general, and that is why we focus only on sensor attacks in this section.

7.2 Separation of Estimation and Control

We are now ready to state our result on separation of estimation and control. Theorem 1: Let A, B, C be three matrices of appropriate sizes and assume that a control strategy given by the $(U^{(t)})_{t=0,1,...}$ is such that: for any $x^{(0)} \in \mathbb{R}^n$ and for any sequence of error vectors $e \in E_{q,T}$, the sequence $(x^{(t)})$ defined by

$$\begin{aligned} x^{(t+1)} &= Ax^{(t)} + B(U^{(t)}(y^{(0)}, ..., y^{(t)})) \\ y^{(t)} &= Cx^{(t)} + e^{(t)} \end{aligned} \tag{7.2}$$

satisfies $\parallel x^{(t)} \parallel \leq \kappa \alpha t \parallel x^{(0)} \parallel$

where $\kappa > 0$ and where $0 \leq \alpha < 1$ is small enough: $\alpha < min\{|\lambda| \,|\lambda$ eigenvalue of A $\}$. Then necessarily q errors are correctable after n steps.

For detailed proof, please refer to [3]

Chapter 8

Numerical Simulations

In this section we show the performance of the proposed decoding algorithm first on a random system. We consider the l_1/l_2 decoder on a system of size $n = 25$, $p = 20$ where $A \in \mathbb{R}^{25\times25}$ and $C \in \mathbb{R}^{20\times25}$ have iid Gaussian entries. For different values q of attacked sensors, we tested the decoder on 100 different initial conditions $x^{(0)}$ and attacked sensors $K \subset \{1, ..., p\}$ with $|K| = q$. The initial conditions $x^{(0)}$ were randomly generated from the standard Gaussian distribution, and the attack sets were chosen uniformly at random from the set of subsets of $\{1, ..., p\}$ of size q. 8.1 shows the fraction of initial conditions that were correctly recovered by the l_1/l_2 decoder in less than $T = 5$ time steps for the different values of q.

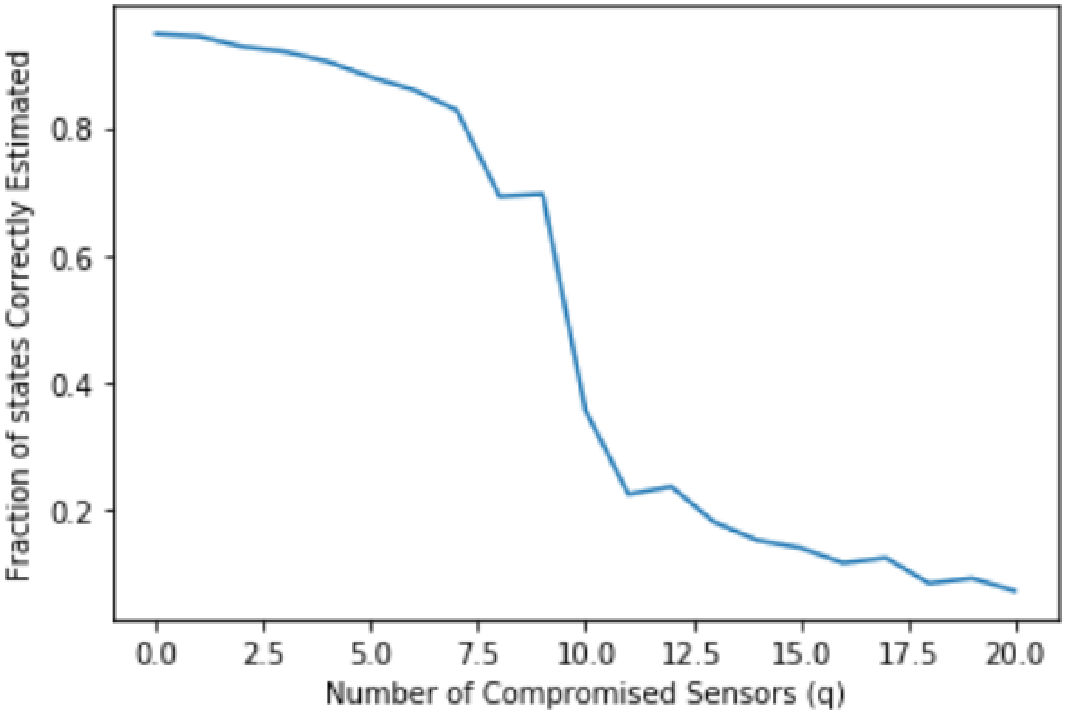

Figure 8.1: Fraction of correctly estimated states vs number of errors using l_1/l_2 decoder

Bibliography

[1] Amin, Saurabh, Alvaro A. Cárdenas, and S. Shankar Sastry. ”Safe and secure networked control systems under denial-of-service attacks.” International Workshop on Hybrid Systems: Computation and Control. Springer, Berlin, Heidelberg, 2009.

[2] Candes, Emmanuel J., and Terence Tao. ”Decoding by linear programming.” IEEE transactions on information theory 51.12 (2005): 4203-4215.

[3] Fawzi, Hamza, Paulo Tabuada, and Suhas Diggavi. ”Secure estimation and control for cyber-physical systems under adversarial attacks.” IEEE Transactions on Automatic control 59.6 (2014): 1454-1467.

[4] Holdren, John P., Eric Lander, and Harold Varmus. ”Designing a digital future: Federally funded research and development in networking and information technology.” President's Council of Advisors on Science and Technology, Washington, DC (2010).

[5] Laprie, Jean-Claude, Brian Randell, and Carl Landwehr. ”Senior Member-basic concepts and taxonomy of dependable and secure computing-rivista: IEEE transactions on dependable and secure computing”

[6] Mo, Yilin, and Bruno Sinopoli. ”Secure estimation in the presence of integrity attacks.” IEEE Transactions on Automatic Control 60.4 (2014): 1145-1151.

[7] NSF:Cyber-Physical Systems (CPS) Program Solicitation, NSF 16-549, National Science Foundation (2016)

[8] Pajic, Miroslav, et al. ”Attack-resilient state estimation in the presence of noise.” 2015 54th IEEE Conference on Decision and Control (CDC). IEEE, 2015.

[9] Vision, Strategic. ”Business Drivers for 21st Century Cyber-Physical Systems.” Report from the Executive Roundtable on Cyber-Physical Systems (2013).

[10] Weimer, James, et al. ”Attack-resilient minimum mean-squared error estimation.” 2014 American Control Conference. IEEE, 2014.

[11] Zacchia Lun, Yuriy & D’Innocenzo, Alessandro & Smarra, Francesco & Malavolta, Ivano & Benedetto, Maria. (2018). ”State of the Art of Cyber-Physical Systems Security: an Automatic Control perspective.” Journal of Systems and Software. 149. 10.1016/j.jss.2018.12.006.