State Estimation of Cyber-Physical Systems Under Sensor 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

May 25, 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: May 25, 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 "**State Estimation of Cyber-Physical Systems Under Sensor 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.

Date: May 25, 2020
Place: Kharagpur

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

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: **State Estimation of Cyber-Physical Systems Under Sensor Attack**

Thesis supervisor: **Professor Siddhartha Sen**

Month and year of thesis submission: **May 25, 2020**

Cyber-Physical systems form a crucial component of our daily lives. A malfunctioning of these systems is capable of directly impacting the economy of a nation. Therefore it is of great importance that any adversarial attacks are prevented. This report is concerned with a cyber-physical system whose sensors are under attack. It shows how it is algorithmic-ally possible to recover the correct state of the system, even though a subset of sensors of the system are compromised. The conditions for such recovery are discussed in this report. The algorithm is then simulated on a 12-state system, and the results are shown to be in accordance with the theoretical formulations. The theoretical framework used has been developed 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

Cyber-physical systems (CPS) are integrations of computation, networking, and physical processes. The key characteristic of cyber-physical systems is their seamless integration of both hardware and software resources for computational, communication and control purposes, all of them co-designed with the physical engineered components. 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 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, and the European Union has a similar vision on the importance of research on CPS. [11]

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. [11]

This work deals with the specific problem of estimating the state of the system, even when a subset of sensors is under attack. The theoretical foundations of this work are developed in [3], this work aims to verify the results by simulating it on a 12-state system, attacking it systematically and tabulating the results.

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

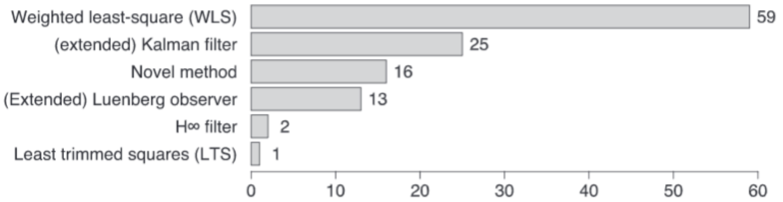

Figure 2.1: Distribution of studies according to state estimation method used, [11]

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

Designing the problem statement

3.1 Notations

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

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

3.2 Estimation Problem

For the initial portion of this report, we consider linear dynamical systems of the form (3.2).

$$\begin{aligned} x^{(t+1)} &= Ax^{(t)} \\ y^{(t)} &= Cx^{(t)} + e^{(t)} \end{aligned} \tag{3.2}$$

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 the results derived in [3] can be depicted by this system adequately. 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 initially 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 $x(T-1)$.

We then consider the problem statement (3.3)

$$\begin{aligned} x^{(t+1)} &= Ax^{(t)} + B(U^{(t)}(y^{(0)}, ..., y^{(t)})) \\ y^{(t)} &= Cx^{(t)} + e^{(t)} \end{aligned} \tag{3.3}$$

which is (3.1) without the actuator attacks. 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. Under conditions that the control law stabilizes the system at a sufficiently fast rate, it is shown that the system state is recovered.

Chapter 4

Correctibility and formulating the state decoder

This section describes the theoretical framework that this report has attempted to implement. The following sections will provide some general postulates regarding the error correction capabilities, and the method of state estimation. For proof of the mentioned concepts, refer to [3].

4.1 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 equation (3.1) and by equation(3.3). $e^{(t)}$ is the attack vector injected into the measured readings by the malicious agent.

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

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 $t = 0, ..., T-1$

Now, 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 $|K| \leq q$.

One of the important results derived in [3] is that the number of correctable errors is always less than half of the total sensors, that is, $p/2$, for any time window T.

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 $\mathbb{R}^{n \times n} \times \mathbb{R}^{p \times p}$.

4.2 The l_0 Decoder

For the problem statement given by equation(3.2), consider the decoder $D_0 : \mathbb{R}^n \to (\mathbb{R}^p)^T$ defined such that $D_0(y^{(0)}, ..., y^{(T-1)})$ is the optimal $\hat{x}$ solution of the following optimization problem:

$$\begin{aligned} &\min_{\hat{x} \in \mathbb{R}^n, \hat{K} \subset \{1, ..., p\}} |\hat{K}| \\ &\text{subject to } supp(y^{(t)} - CA^t \hat{x}) \subset \hat{K} \text{ for } t \in \{0, ..., T-1\} \end{aligned} \tag{4.1}$$

Observe that the decoder D_0 looks for the smallest set K of attacked sensors that can explain the received data $y^{(0)}, ..., y^{(T-1)}$. It is shown in [3] decoder D_0 is optimal in terms of error-correction capabilities.

For equation(3.3), the same optimal decoder takes the form:

$$\begin{aligned}
&\min_{\hat{x}\in\mathbb{R}^n,\hat{K}\subset\{1,...,p\}} |\hat{K}| \text{ subject to}\\
&supp(\hat{e}^{(t)}) \subset \hat{K}\\
&\hat{x}^{(t+1)} = A\hat{x}^{(t)} + B(U^{(t)}(y^{(0)},...,y^{(t)}))\\
&y^{(t)} = C\hat{x}^{(t)} + \hat{e}^{(t)}
\end{aligned} \tag{4.2}$$

The optimation variables are indicated by a "hat" (e.g. $\hat{x}^{(t)}$, the other variables are given. The optimization problem finds the simplest possible explanation of the received data $y^{(0)},...,y^{(T-1)}$, that is, the one with the smallest number of attacked nodes.

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

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.

4.3 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

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

For equation(3.3), the l_1 decoder takes the form:

$$\begin{aligned} &\text{minimize} \sum_{i=1}^{p} \parallel \hat{E}_i \parallel_{l_r} \text{ subject to} \\ &\hat{E}_i = (\hat{e}_i^{(0)}, ..., \hat{e}_i^{(T-1)}) \\ &\hat{x}^{(t+1)} = A\hat{x}^{(t)} + B(U^{(t)}(y^{(0)}, ..., y^{(t)})) \\ &y^{(t)} = C\hat{x}^{(t)} + \hat{e}^{(t)} \end{aligned} \tag{4.3}$$

For each i the auxiliary variables $\hat{E}_i \in \mathbb{R}^T$ carry the i'th components of the attack vectors over the time horizon $t = 0, ..., T-1$. Thus if $\parallel \hat{E}_i \parallel_{l_r} = 0$ then $\hat{e}_i^{(t)} = 0$ for all $t = 0, ..., T-1$ and the i'th sensor is not attacked. An additional constraint is provided for the control law:

$$\begin{aligned}&\parallel x^{(t)} \parallel \leq \kappa\alpha t \parallel x^{(0)} \parallel\\&\text{where } \kappa > 0 \text{ and where } 0 \leq \alpha < 1 \text{ is small enough:}\\&\alpha < min\{|\lambda|, \lambda \text{ eigenvalue of A}\}.\end{aligned} \tag{4.4}$$

Under this constraint of the control law, it is essentially shown that the problem of estimation and the problem of control is decoupled. 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.

Chapter 5

Numerical Simulations

5.1 Neglecting the control law

In this section we show the performance of the proposed relaxed decoder on a random system, which can be expressed by equation(3.2). The decoder is formulated as:

$$\begin{aligned}
&\phi^{(T)} : \mathbb{R}^n \rightarrow (\mathbb{R}^p)^T \\
&x \rightarrow [Cx \mid CAx \mid ... \mid CA^{T-1}x] \\
&Y^{(T)} = [y^{(0)} \mid y^{(1)} \mid ... \mid y^{(T-1)}] \in \mathbb{R}^{pT} \\
&D_{1,r}(y^{(0)}, ..., y^{(T-1)}) = arg \min_{\hat{x} \in \mathbb{R}^n} \parallel Y^{(T)} - \phi^{(T)}\hat{x} \parallel_{l_1/l_r}
\end{aligned} \tag{5.1}$$

The l_1/l_2 relaxed decoder has been used on 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. A graph has been generated of the fraction of states correctly estimated by the decoder vs the number of sensors attacked. For each chosen number of compromised sensors, the simulation was run 100 times, and the average number of recovered sensors was documented. For each of these simulations, a new A matrix, C matrix and attack error was generated, with a random normal distribution with mean 1 and standard deviation 0. The A matrix generated was normalised by its spectral radius. The attack vector $e^{(t)}$ was normal distributed, and the change of mean and deviation did not affect the results. For the given graph, the chosen mean and deviation for the attack vectors is 0 and 1

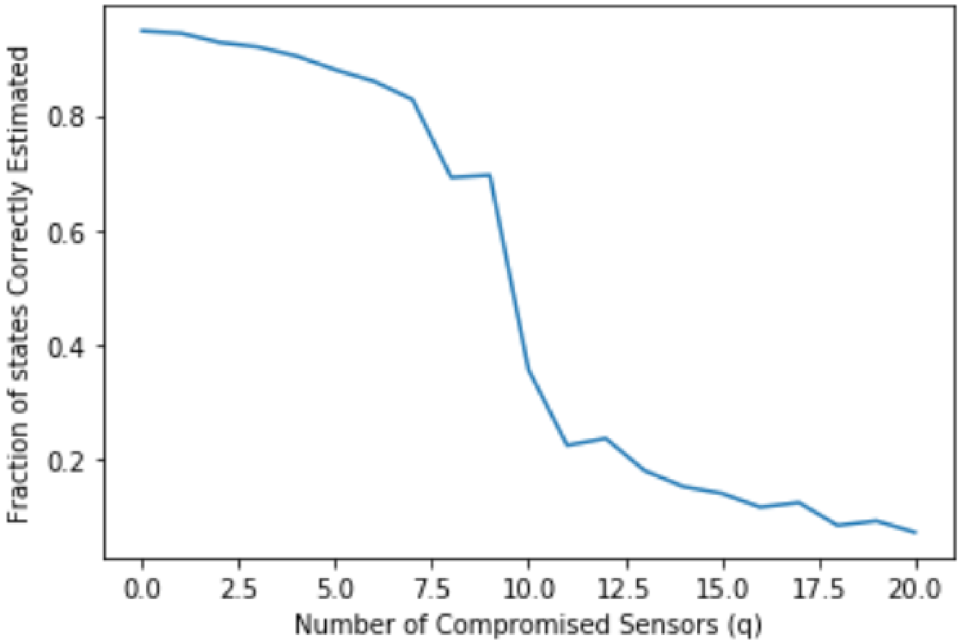

FIGURE 5.1: Fraction of correctly estimated states vs number of errors using l_1/l_2 decoder

respectively. The initial state has been randomly generated for every simulation and for every attacked sensor number as well, and the estimated state has been compared with this initial state to generate the error for plotting. The number of time steps T used to estimate the initial state is 15, although the correct state could have been well estimated with a lower T value as well. Figure 5.1 shows the resultant graph. Gradient descent has been used to run these simulations, and the code is mainly written using numpy tensors, in python.

The result is as expected. The state can be recovered only if less than half of the sensors are compromised, and this is evident in the graph obtained, which has a sharp fall at around the $9-10$ mark. (The total number of sensors $= 20$)

5.2 Including the control law

A multi-agent network has been used to simulate the results for the control problem given by equation(3.3). It has 4 agents, each with 3 outputs, therefore a total of 12 outputs and 12 states. The time steps chosen in this case is $T = 500$. The

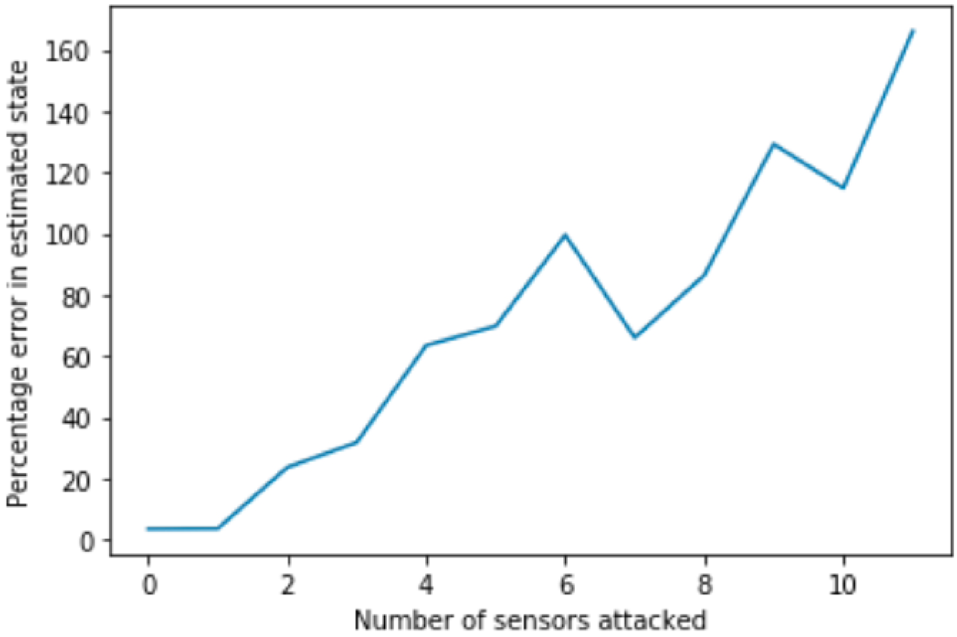

FIGURE 5.2: Fraction of correctly estimated states vs number of errors using l_1/l_2 decoder

attack vector has a standard deviation 3 times that of the initial state. For this simulation, for each of the chosen number of compromised sensor, the simulation has been run 10 times. The error vector has been random for each simulation, but the initial state has been kept constant. The given conditions for the control law have been satisfied for the system. The A matrix has nevertheless been normalised by its spectral radius. The learning rate was chosen to be 0.001 and the number of iterations for gradient descent was chosen to be 10000. These hyperparameters were chosen by trial and error. The obtained graph is as shown in figure 5.2. The graph is not smooth since, the x axis has only 12 values, and the average error has been computed over 10 simulations. However the increasing trend of error with number of sensors is evident. By the time the system reaches upto 6 sensors compromised, the error is as high as $80 - 100\%$. For lower number of attacked sensors, the system recovers most states with very small error ($< 0.01\%$)

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.