Consequences of False Data Injection on Power System State Estimation

by

Jingwen Liang

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved April 2015 by the
Graduate Supervisory Committee:

Lalitha Sankar, Co-Chair
Oliver Kosut, Co-Chair
Kory Hedman

ARIZONA STATE UNIVERSITY

May 2015

ABSTRACT

The electric power system is one of the largest, most complicated, and most important cyber-physical systems in the world. The link between the cyber and physical level is the Supervisory Control and Data Acquisition (SCADA) systems and Energy Management Systems (EMS). Their functions include monitoring the real-time system operation through state estimation (SE), controlling the system to operate reliably, and optimizing the system operation efficiency. The SCADA acquires the noisy measurements, such as voltage angle and magnitude, line power flows, and line current magnitude, from the remote terminal units (RTUs). These raw data are firstly sent to the SE, which filters all the noisy data and derives the best estimate of the system state. Then the estimated states are used for other EMS functions, such as contingency analysis, optimal power flow, etc.

In the existing state estimation process, there is no defense mechanism for any malicious attacks. Once the communication channel between the SCADA and RTUs is hijacked by the attacker, the attacker can perform a man-in-middle attack and send data of its choice. The only step that can possibly detect the attack during the state estimation process is the bad data detector. Unfortunately, even the bad data detector is unable to detect a certain type of attack, known as the false data injection (FDI) attacks.

Diagnosing the physical consequences of such attack, therefore, is very important to understand system stability. In this thesis, theoretical general attack models for AC and DC attacks are given and an optimization problem for the worst-case overload attack is formulated. Furthermore, physical consequences of FDI attacks, based on both DC and AC model, are addressed. Various scenarios with different attack targets and system configurations are simulated. The details of the research, results obtained and conclusions drawn are presented in this document.

TABLE OF CONTENTS

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

LIST OF SYMBOLS

a	the false data the attacker injects into the measurement
B_{ki}	the reactive part of the $(k,i)^{\text{th}}$ entry of Y_{bus}
b_{ki}	the active part admittance of the series branch connecting bus k and bus i
b_{sk}	the reactive part admittance of the shunt branch connected at bus k
c	the attack vector
e	the measurement error
$f(.)$	the generator cost function
G_{ki}	the active part of the $(k,i)^{\text{th}}$ entry of Y_{bus}
g_{ki}	the active part admittance of the series branch connecting bus k and bus i
g_{sk}	the active part admittance of the shunt branch connected at bus k
H	the measurement Jacobian for DC state estimation
$h(\cdot)$	the non-linear relationship between the states and power flows and injections
H_1	the matrix of dependencies between bus power injection and state variable
H_2	the matrix of dependencies between branch power flow and state variable
$\mathcal{I}_{\mathcal{S}}$	the set of measurement indices inside $\mathcal{S}$
$\mathcal{I}_P$	the set of measurement indices related to active power
J	the measurement Jacobian matrix for AC state estimation
$\mathcal{K}_{\text{load}}$	the set of load bus indices
$\mathcal{K}_{\mathcal{S}}$	the set of bus indices inside $\mathcal{S}$
L_S	the load shift limit factor
M	the measurement mismatch
N_0	the l_0-norm constraint integer
N_1	the l_1-norm constraint
n_{br}	the number of branch
n_b	the number of bus

n_g	the number of generator
$P_G^{\max}$	the generator upper bound of generator capacity
$P_G^{\min}$	the generator lower bound of generator capacity
P	the active power flow on branches
$P^{\max}$	the thermal limits on branches
$P_G^\star$	the optimal generation dispatch solved by DCOPF
P_G	the generation dispatch
P_L	the active load on each bus
Q_L	the reactive load on each bus
R	the branch thermal limit relaxation
$R^\star$	the optimal branch thermal limit relaxation
r_a	the estimated measurement residue with attack
r	the estimated measurement residue
$\mathcal{P}$	the penalty function of relaxing branch thermal limits
$\mathcal{S}$	a small sub-area of the system bounded by buses that the attacker has access of, i.e. the attack subgraph
$\mathcal{S}_k$	the attack subgraph with center bus k
$\hat{V}$	the estimated bus voltage magnitude
V	bus voltage magnitude
$\hat{x}$	the estimated state including bus voltage angle and magnitude
$\hat{x}^{(a)}$	the estimated state from attacker's local state estimation
x	system state including bus voltage angle and magnitude
Y_{bus}	the bus admittance matrix
$\tilde{z}$	the measurement chosen by attackers
z	the measurement
$z^{(a)}$	the false measurement
s	the additional slack variable to represent the absolute value of c
$\alpha^\pm$	the dual variable of the upper and lower bound of generator capacity

β the dual variable of the branch thermal limit relaxation

γ the weight of the norm of attack vector c

$\delta_{\alpha}^{\pm}$ the additional binary variable to represent the complementary slackness condition of generation capacity constraint

δ_{β} the additional binary variable to represent the complementary slackness condition of branch thermal limit relaxation

$\hat{\theta}$ the estimated bus voltage angle

θ bus voltage angle

$\theta^{\star}$ the optimal state solved by OPF

θ_{ki} the angle difference between bus k and bus i

$\lambda^{\pm}$ the dual variable for the upper and lower bound of the thermal limits constraint

σ the standard deviation of measurement error

τ the bad data detector residue threshold

υ the dual variable for equal constraints

Chapter 1

INTRODUCTION

1.1 Background

Advances in sensing, communications, and computing are enabling a smart electric power system with an intelligent cyber layer that is tightly integrated with the physical layer and is capable of real-time monitoring control, and actuation. In the electric power system, this is enabled by an Energy Management System (EMS) which acquires the operation status of the power system from Supervisory Control and Data Acquisition (SCADA) data. SCADA data includes measurements of voltage and current magnitudes and active and reactive power measurements in the physical power system. Because of the limited accuracy and quantity of measurements, a mathematical estimation technique referred to as state estimation (SE), is applied to estimate the physical system state (complex voltage) from the measurements with sufficiently high fidelity. This estimate is the beginning of a process to achieve situational awareness and obtain real-time operational data about the physical electric system so that operators can make control decisions. Lack of access to the system status will inevitably lead to system operation inefficiency, violation, and in the worst case, system blackout. Thus, the data acquisition, starting from SCADA data, in conjunction with the communication and control network that overlays the physical network, is crucial to the reliable functionality of the electric power system.

Despite the extreme importance of the cyber layer, the communication network overlaying the physical electrical grid makes it more vulnerable to cyber attacks that can compromise measurements, system states, and eventually the control and the actuation system. The "air gaps" between SCADA systems and the public Internet is being weakened and many of the devastating computer viruses have been specifi-

cally designed to compromise SCADA system [1]. Recently, there have been specific incidents on the electric power system, and we briefly discuss them.

- On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout [2]. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load and power has not been fully restored for 4 days. Estimates of total costs in the United States range between 4 billion and 10 billion dollars [2]. The U.S.-Canada Power System Outage Task Force identified "the inadequate situational awareness" as one of the most important causes of the blackout's initiation and a failure on the alarm system in the EMS contributed a lot to the black out [2].

- In 2007, researchers at the Idaho National Lab conducted the Aurora test, in which a virus manipulated the computer network systems that controlled diesel generators. The test intentionally switched the circuit breaker on and close it out-of-synchronism. As a result, the connected motor and generator may be damaged [3]. This test demonstrated the ability for a computer virus to manipulate power systems and to cause physical damage.

- In 2010, a computer worm named 'Stuxnet' targeting Siemens industrial control systems was "detected in the SCADA system of 14 plants in operation but without any malfunction of process and production" [4]. Nevertheless, this type of cyber attack was new and certainly introduced new threads to power system [5, 6].

- Since 2011, electric power system infrastructure within the United States and Europe has come under attack from a group of Russian hackers, known as

'Dragonfly'. This group has been conducting various cyber attacks against European governments, defense contractors, and U.S. health care firms. To date, it has been conducting Stuxnet-type attacks against the industrial control systems found with petroleum pipeline operators, grid operators, electricity generation firms and other critical energy companies [1].

From the above discussion, it is concluded that some of the major vulnerabilities of the power system stem directly from the cyber layer. This thesis focuses on a specific class of attacks, introduced in [7] and refered to as false data injection (FDI) attack. In theory, FDI attacks can bypass the existing state estimation and it cannot be detected by bad data detector [7]. However, the modular nature of cyber data processing in the grid can be exploited to observe attack consequences and potentially detect the attacks.

Therefore, assessment and evaluation of possible attacks and consequences before an actual attack happens is extremely instructive to the utilities: procedures for potential attack incidents and activities could be important supplements to the secure operation of the power system.

1.2 System Model

1.2.1 Temporal Nature of Processing in the Power System

Fig. 1.1 illustrates the temporal nature of processing in the power system, as well as the attack model. Assume a system with n_b buses, n_{br} branches, and n_g generators. Active and reactive load of each buses are represented by P_L and Q_L, respectively. Measurement and estimated measurement residue are denoted as z and r , respectively. In the bad date detector, τ is the residue threshold and $x = [V, \theta]^T$ is the system state, where V is bus voltage magnitude and θ is bus voltage angle. The function $h(\cdot)$ denotes the non-linear function that gives the measurements (power

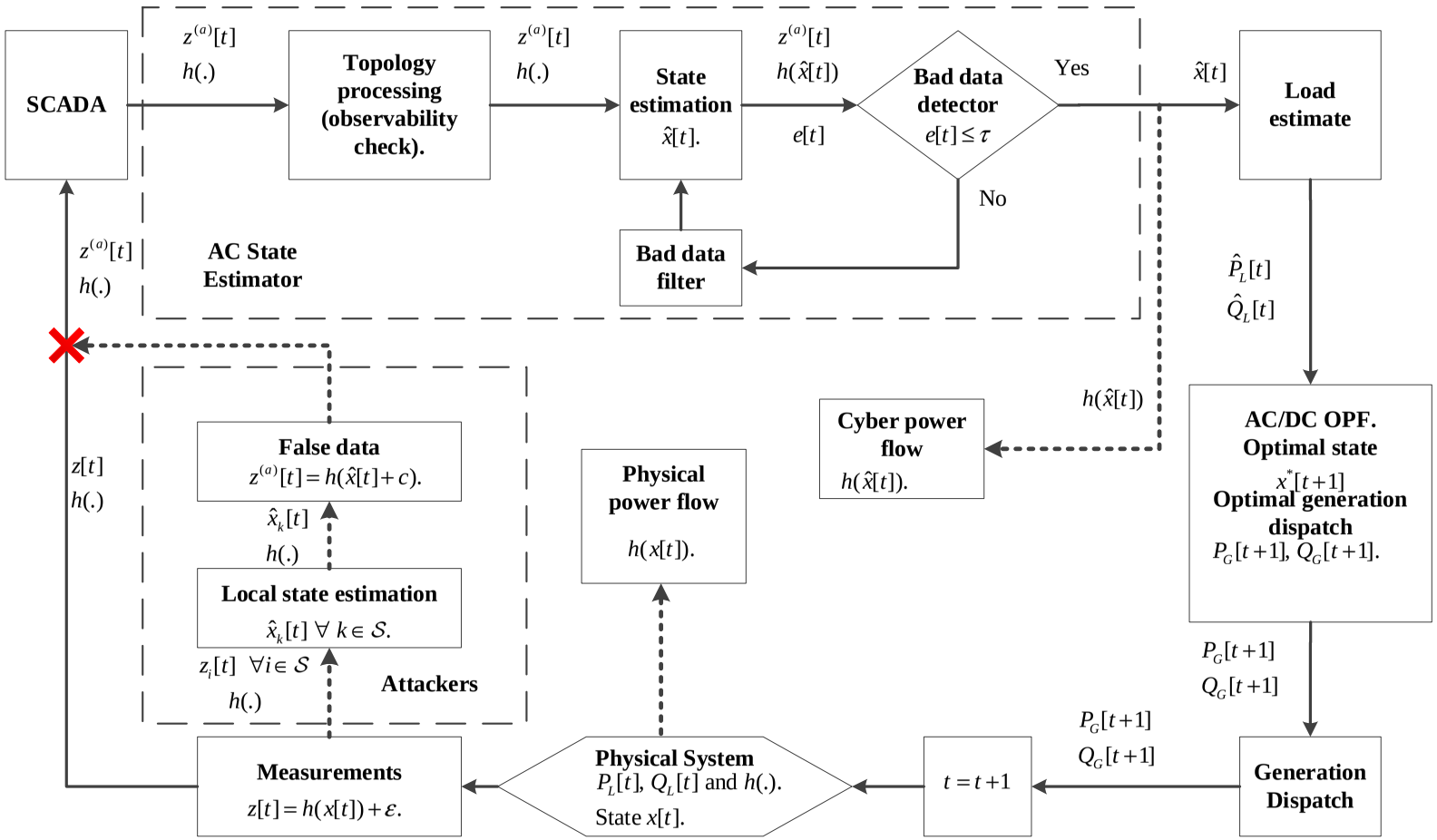

Figure 1.1: Illustration of Temporal Processing of the Power System and Attack Model.

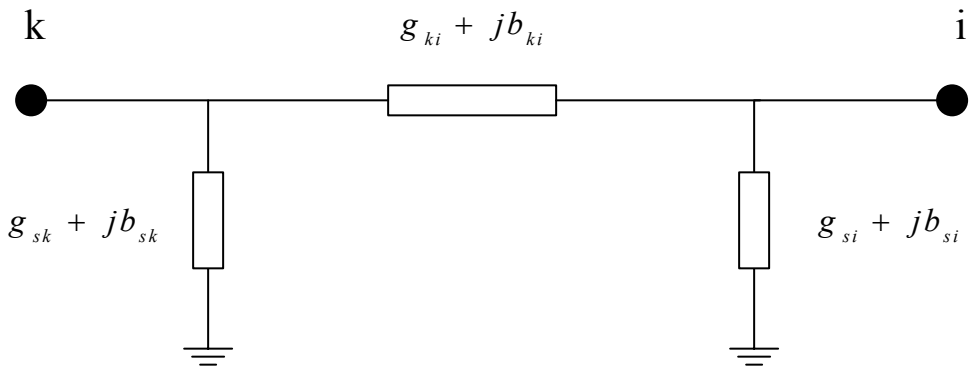

Figure 1.2: The Equivalent π-model of a Network Branch.

flows and injections) given the system state x. This function depends only on the system topology. Estimated values are denoted with a hat, e.g.$\hat{x}, \hat{V}, \hat{\theta}$.

As shown in Fig. 1.1, generation dispatch control decisions made at the control center depend on the noisy measurements provided by the SCADA system. If these measurements are corrupted by an attacker, then if they pass the bad data detector they can directly influence the control decisions for the next time interval. Since the process occurs in the same manner for each time t, we drop the functional dependence on t for the rest of this section. Time progression attacks will be illustrated simulations. The major blocks shown in Fig. 1.1 are discussed in detailed in the following subsections.

1.2.2 Measurements

Since power flow follows the non-linear mathematical dependencies, the AC measurement model is given by:

$$z = h(x) + e. \tag{1.1}$$

where z, e and x are $m \times 1$, $m \times 1$ and $n \times 1$ vectors with entries z_i, e_i and x_k, respectively $i \in \{1, \ldots, m\}$ and $k \in \{1, \ldots, n\}$. z_i is the i^{th} measurement of the system such as line power flows, bus voltage and line current magnitude, etc. e_i is the

i^{th} measurement error, assuming to be independent and Gaussian distributed with 0 mean and σ_i^2 standard deviation.

The expressions for function $h(.)$ below are assumed with an equivalent π circuit for a two-port network, shown in Fig. 1.2.

Real and reactive line power flows at branch from bus k to bus i:

$$P_{ki} = V_k^2(g_{sk} + g_{ki}) - V_k V_i(g_{ki}\cos\theta_{ki} + b_{ki}\sin\theta_{ki}) \tag{1.2}$$

$$Q_{ki} = -V_k^2(b_{sk} + b_{ki}) - V_k V_i(g_{ki}\sin\theta_{ki} - b_{ki}\cos\theta_{ki}) \tag{1.3}$$

Real and reactive power injection at bus k:

$$P_k = V_k \sum_{i\in\mathcal{N}_k} V_i(G_{ki}\cos\theta_{ki} + B_{ki}\sin\theta_{ki}) \tag{1.4}$$

$$Q_k = V_k \sum_{i\in\mathcal{N}_k} V_i(G_{ki}\sin\theta_{ki} - B_{ki}\cos\theta_{ki}) \tag{1.5}$$

Line current flow magnitude from bus k to bus i:

$$I_{ki} = \frac{\sqrt{P_{ki}^2 + Q_{ki}^2}}{V_k} \tag{1.6}$$

where $\theta_{ki} = \theta_k - \theta_i$, $G_{ki} + jB_{ki}$ is the $(k,i)^{\text{th}}$ entry of the bus admittance matrix, i,e. the Y_{bus} matrix. $g_{sk} + jb_{sk}$ is the admittance of the shunt branch connected at bus k and $g_{ki} + jb_{ki}$ is the admittance of the series branch connecting bus k and bus i, and $\mathcal{N}_k$ denotes the set of buses that are directly connected to bus k.

1.2.3 State Estimation

As illustrated in Fig. 1.1, a typical state estimator includes the following functions [8]:

- Topology processor: Collect the system breaker and switch status and generate network model.
- Observability check: Ensure the availability of measurement is sufficient to estimate the state of the whole system. If not, the several observable islands will be identified.
- State estimation solution: Acquire the optimal estimated state of the system.
- Bad data detector: Identify and eliminated bad and noisy measurements.

1.2.4 Implementation of State Estimation

Since the errors of measurement are independent, the following assumptions are made based on the statistical properties of e [8]:

- $E(e_i) = 0, \forall i \in \{1...m\}$;
- $E(e_i e_j) = 0$, thus, $Cov(e) = E(e \cdot e^T) = R = \text{diag}\{\sigma_1^2, \sigma_2^2, \ldots, \sigma_m^2\}$, where E is the expected value.

The standard deviation σ_i, thus, is a weight of the expected accuracy of the measuring device. The state variables are then solved as a weighted least square (WLS) problem with an objective function [8]

$$\hat{x} = \arg\min J(x) = (h(x) - z)^T R^{-1}(h(x) - z) \tag{1.7}$$

and $\hat{x} = [\hat{V}, \hat{\theta}]^T$ is the estimated state. At the minimum, the first-order optimality

$$g(\hat{x}) = \left.\frac{\partial J(x)}{\partial x}\right|_{x=\hat{x}} = H(\hat{x})R^{-1}(h(\hat{x}) - z) = 0 \tag{1.8}$$

must be satisfied, where $H(x) = \left.\frac{\partial h(x)}{\partial x}\right|_{x=\hat{x}}$. Expanding (1.8) into its Taylor series and neglecting the higher orders:

$$g(x) = g(x^k) + \frac{\partial g(x^k)}{\partial x} \cdot (x - x^k) = 0 \tag{1.9}$$

where a gain matrix is usually defined:

$$G(x) = \frac{\partial g(x^k)}{\partial x}. \tag{1.10}$$

$G(x)$ has to be sparse, positive definite, and symmetric for an observable system [8]. Thus, (1.8) can be rewritten as

$$(x^{k+1} - x^k) = G(x^k)^{-1} H^T(x^k) R^{-1}[z - h(x^k)] \tag{1.11}$$

where k is the iterative index and x^k is the solution at iteration k. The equation given by (1.11) is also referred as normal equation. To solve the normal equation, the initial value $x^{(0)} = [1, 0]$ is typically assumed, known as the cold start. In each iteration, the change of x is obtained and added to the previous value of x and (1.10) and (1.11) are updated. The iteration stops when the change of x is less than or equal to the pre-set tolerance.

In DC state estimation, the operation point is assumed to be near $\theta = 0$ and $V = 1$ and (1.1) can be approximated by

$$z_A = H_{AA}\theta + e_A \tag{1.12}$$

where z_A and e_A denote the active power related measurements and measurement errors, respectively. H_{AA} is the system Jacobian matrix around $\theta = 0$ and $V = 1$, which is a function of branch reactance only. Note that, in DC state estimation, reactive power flows are ignored since $V = 1$ for all buses. Therefore, expanding (1.8) around $\theta = 0$ we have

$$(H_{AA})^T R^{-1}(H_{AA}\hat{\theta} - z_A) = 0 \tag{1.13}$$

and

$$\hat{\theta} = (H_{AA}^T R^{-1} H_{AA})^{-1} H_{AA}^T R^{-1} z_A. \tag{1.14}$$

Thus, DC state estimation essentially solves for a solution for a linear and overdetermined system of equations. In order to simplify the notation, the subtitle of z_A, H_{AA}, and e_A are dropped in the rest of the thesis for all linear models.

1.2.5 Bad Data Detection

The bad data detector filters noisy measurement and guarantees the accuracy of estimation. One of these methods of detection is the χ^2 test. To pass a χ^2 test, the estimated measurement residue should satisfy

$$r = \sum_{i=1}^{m} \frac{(z_i - h_i(\hat{x}))^2}{\sigma_i^2} \leq \chi^2_{(m-n),p} \tag{1.15}$$

where $h_i(\hat{x})$ is the estimated measurements, p is the detection confidence of probability and $\chi^2_{(m-n),p}$ denotes the value in χ^2 distribution table corresponding to p and the degree of freedom $m - n$. Measurements that fail to pass the test will be considered erroneous and the measurement with the largest residue will be eliminated. Then the state will be re-estimated.

1.2.6 DC and AC Optimal Power Flow

The AC optimal power flow (OPF) solves for the minimum generation cost and balances the system power flow within its limit. The formulation of ACOPF is

$$\underset{P_G, Q_G, V, \theta}{\text{minimize}} \qquad f(P_G)$$

subject to

$$P_{G_k} = V_k \sum_{i \in \mathcal{N}_k} V_i (G_{ki} \cos\theta_{ki} + B_{ki} \sin\theta_{ki}) + P_{L_k} \tag{1.16}$$

$$Q_{G_k} = V_k \sum_{i \in \mathcal{N}_k} V_i (G_{ki} \sin\theta_{ki} - B_{ki} \cos\theta_{ki}) + Q_{L_k} \tag{1.17}$$

$$\begin{aligned} F_{ki} = {} & V_k^2 (g_{sk} + g_{ki}) - V_k V_i (g_{ki} cos\theta_{ki} + b_{ki} sin\theta_{ki}) \\ & + j[-V_k^2 (b_{sk} + b_{ki}) - V_k V_i (g_{ki} sin\theta_{ki} - b_{ki} cos\theta_{ki})], \end{aligned} \tag{1.18}$$

$$|F_{ki}| \leq F_{ki}^{\max} \tag{1.19}$$

$$P_G^{\min} \leq P_G \leq P_G^{\max} \tag{1.20}$$

$$Q_G^{\min} \leq Q_G \leq Q_G^{\max}. \tag{1.21}$$

In the above OPF problem, node balance constraints are (1.16)–(1.17), thermal limit constraints are (1.18)–(1.19) with the line thermal limit $F^{\max}$, and generator capacity constraints are (1.20)–(1.21) with the lower bound $P_G^{\min} + jQ_G^{\min}$ and upper bound $P_G^{\max} + jQ_G^{\max}$, respectively. The objective is to minimize the generation cost where $f(.)$ is the generation cost function. Similar to Section 1.2.4, DCOPF approximates the non-linear constraints (1.16)–(1.19) around $V = 1$ and $\theta = 0$ by their first order Taylor expansions and neglect the real part of the admittance matrix and the shunt elements:

$$\underset{P_G,\theta}{\text{minimize}} \qquad f(P_G)$$

subject to

$$P_{G_k} = \sum_{i \in \mathcal{N}_k} B_{ki}\theta_{ki} + P_{L_k},\ k = 1, ..., n_b \tag{1.22}$$

$$F_{ki} = b_{ki}\theta_{ki} \tag{1.23}$$

$$-F_{ki}^{\max} \leq F_{ki} \leq F_{ki}^{\max} \tag{1.24}$$

$$P_G^{\min} \leq P_G \leq P_G^{\max}. \tag{1.25}$$

To write in a more compact way, we define

- H_1, the matrix of dependencies between bus power injection and variable θ, as

$$H_{1(k,i)} = \begin{cases} \sum\limits_{i \in \mathcal{N}_k} -b_{ki} & \text{if } k = i \\ b_{ki} & \text{if } k \neq i \end{cases} \tag{1.26}$$

  where $g_{ki} + jb_{ki}$ is the branch admittance between bus k and bus i and $\mathcal{N}_k$ denotes the set of buses that are directly connected to bus k.

- H_2, the matrix of dependencies between branch power flow and variable θ, as

$$H_{2(j,t)} = \begin{cases} b_{ki} & \text{if } t = k \\ -b_{ki} & \text{if } t = i \\ 0 & \text{else} \end{cases} \tag{1.27}$$

  where branch j connects from-end bus k and to-end bus i.

Thus, the DCOPF problem can be rewritten as

$$\begin{aligned} \underset{P_G,\theta}{\text{minimize}} \quad & f(P_G) \\ \text{subject to} \quad & \\ & (1.25) \\ & -H_1\theta + P_G - P_L = 0 \qquad (1.28) \\ & -P^{\max} \leq H_2\theta \leq P^{\max} \qquad (1.29) \end{aligned}$$

where $P^{\max}$ is the thermal limits for every branch.

1.3 False Data Injection Attack

FDI attack is first introduced and studied by [7]. For state estimation using DC power flow model, if an attacker can inject the malicious data a into the measurement vector z such that the new measurement $z^{(a)}$ satisfies

$$z^{(a)} = z + a = z + Hc \tag{1.30}$$

where c is a non-zero attack vector, then the existing bad data detector is incapable of detecting such an attack.

A simple proof for the state above from [7] is summarized as follow. With a χ^2 test as the bad data detector, the residue computed from the compromised measurements

r_a is

$$r_a = \sum_{i=1}^{m} \frac{\left(z_i^{(a)} - H_i \hat{x}^{(a)}\right)^2}{\sigma_i^2} = \sum_{i=1}^{m} \frac{(z_i + a_i - H_i(\hat{x} + c))^2}{\sigma_i^2} = \sum_{i=1}^{m} \frac{(z_i - H_i \hat{x})^2}{\sigma_i^2} = r. \quad (1.31)$$

Thus, the false data an attacker injects in the the system will not change the residue of χ^2 test therefore can not be detected. The authors in [7] consider two realistic scenarios, both assumed the attacker's resource and ability are constrained, and show how to construct attack vector a efficiently. And they also test the probability of find such an attack in respect of the attacker's control over the system: into which meter that the attacker can inject the false data and how many meters over the test system that the attackers compromise. The simulation on test system shows successful attacks are made and the attacker can manipulate the system state in a predicted way.

1.4 Literature Review

Apart from what have been discussed in Sec. 1.3, the cyber security related topics has recently drawn a lot of attention.

In [9, 10], the authors study how many coordinated measurements have to be changed in order to hide a single changed power flow measurement. Then they define the security index based on the number of the coordinated measurements. They also propose an efficient algorithm to compute the security indices defined in and furthermore develop algorithms to find minimum attacks.

Also from the attacker's perspective, the authors in [11, 12] show the trade-offs that both attackers and operators have to face in practice: the attackers want to maximize their false data injection size while minimizing their detection rate and the operators want to maximize the detection rate while minimizing the false alarm rate, respectively.

Authors in [13] introduce a max-mim optimization into the defender-attacker scheme of power system. They formulate the mathematical model to identify the critical element of the system in respect of terroristic attacks. Then, they refine their model in [14] by incorporating a simple DCOPF with a cascading outage analysis model, therefore the attack's short-term effect is captured. Similarly, authors in [15, 16] formulate a load shift attack as a multilevel optimization problem. They model the attack as well as the system response in a time sequence: the attacker at each time interval chooses his optimal attack based on the system response to the attack.

In [17], the economic consequences of FDI attacks are assessed. The authors explain the connections between the system operation and attacks then quantify the change of local marginal price of each buses as the economic impact of the attack.

FDI attack may be cooperated with other attacks to hide topology change. Authors in [18] propose an unobservable topology attack. This attack is essentially preserving the state and change the status of the breaker on the line, therefore make the system seems to operate under a situation with one artificial line on or off.

FDI attacks on AC state estimator is also studied. In [19], the authors analyze the vulnerability of both DC and AC state estimator by studying the necessary information they attacker need to construct a FDI attack and the error that the attacker can introduce to the system.

Authors in [20, 21] discuss the how to change line power flows with local information and detect the attack when the state information is inaccurate. Their study show that though AC state estimator is vulnerable to FDI attack, it is more difficult to attack because of it requires the attacker to obtain the additional and accurate state information.

In [22], the authors find out the state information can be abstracted from the measurement and system configuration by the attacker and it requires as same information as DC attack. Therefore, they extend the attack to a more general way, including on AC and DC state estimator.

The detection of FDI attacks is another well studied topic in literature. In [18, 23], placing secure meters or placing Phasor Measurement Units (PMU) in the system is proposed and the optimal placements of such devices are discussed.

In [24, 25], the dynamic of state evolution is used to detect malicious data injection under the assumption that power system is inertial and the system states are almost "steady" in a short time period. They view the detection of false data as a matrix separation problem and solve for a sparse optimization problem.

1.5 Research Motivation and Objective

First of all, by the original definition, FDI attack only applies to DC state estimation, as Sec.1.3 describes. Authors in [19] analyze FDI attacks into AC state estimator and find out that, in order to make the attack unobservable, the attacker has to know additional information about system states. One objective of this thesis is to give a more general definition of FDI attack by extending it to attack AC state estimation.

Also, the consequences for FDI attacks is still unclear. Can FDI attacks actually damage the physical AC system and is it necessary to generate any metric against the attacks? These questions are still unsolved. Thus, another key objective of this thesis is to develop proper attack models and applied it on a test system to actually see the physical consequences. Therefore, the consequences of FDI attacks can be study and evaluated.

Finally, the worst-case attack scenario should be studied. In order to find the worst-case, the attacker's action as well as the system response should be modeled properly: the result of attack should be a combination of the two sides.

1.6 Outline of Thesis

Having introduced the system operation process, state estimation, bad data detector, OPF, and FDI attacks, in Chapter 2, the definition of FDI attack and formulates the AC and DC FDI attacks model are introduced. Scenarios for both attacks are simulated and comparison of them is made. Also, one of the physical consequences, generation re-dispatch, is shown. Chapter 3 gives the formulation of a two-level optimization problems that can solve for the worst-case line overload attacks. Chapter 4 presents the resulting attack against AC system model. Chapter 4 concludes the thesis and enumerates the contributions of this research. The possible future work in related topic is also discuss.

Chapter 2

PROBLEM FORMULATION FOR FDI ATTACKS

2.1 General Attack Model

We first assume that the attacker has following capabilities:

1. The attacker has access to all measurements and topology information of a small area $\mathcal{S}$ bounded by buses. The set of all measurement indices in $\mathcal{S}$ is denoted as $\mathcal{I}_{\mathcal{S}}$ and the set of all state indices in $\mathcal{S}$ is denoted as $\mathcal{K}_{\mathcal{S}}$.

2. The attacker can change or replace all measurements in $\mathcal{S}$.

3. The attacker has computational capability.

As discussed in [22], according to (1.1), suppose the i^{th} measurement prior to attack is $z_i = h_i(x) + e_i$, the general attack model changes the i^{th} measurement z_i to $z_i^{(a)}$ such that

$$z_i^{(a)} = \begin{cases} z_i & \text{if } i \notin \mathcal{I}_{\mathcal{S}} \\ \tilde{z}_i & \text{if } i \in \mathcal{I}_{\mathcal{S}} \end{cases} \tag{2.1}$$

where $\tilde{z}_i$ is chosen by attacker.

2.2 Unobservable Attack – a General Definition of FDI Attack

Here a general definition of unobservable attack is presented. Recall (1.1), an attack is *unobservable* for a measurement model $h(\cdot)$ if, in the absence of measurement noise, there exists a $c \neq 0$ such that $z_i^{(a)} = h_i(x + c)$ for all i.

Therefore, for the attacker to execute an unobservable attack, again assuming no measurement noise, (1.1) becomes

$$z_i^{(a)} = \begin{cases} z_i & \text{if } i \notin \mathcal{I}_{\mathcal{S}} \\ h_i(x + c) & \text{if } i \in \mathcal{I}_{\mathcal{S}}. \end{cases} \tag{2.2}$$

From (2.2), if the k^{th} state x_k is required to compute $h_i(x)$ for any $i \notin \mathcal{I}_{\mathcal{S}}$, then for any unobservable attack the corresponding k^{th} entry in attack vector must satisfy $c_k = 0$. Therefore, for a feasible attack, the attack region $\mathcal{S}$ must be chosen such that c is a non-zero vector.

However, to the buses without loads, their states are dependent from the rest of the system. For instance, a bus k with only a generator on is a PV bus: the voltage magnitude V_k and real power power injection P_k is known. Recall (1.4)–(1.5), thus the voltage angle θ_k at bus k is only dependent on the states of all the buses connected to it. Similarly, a bus without any load or generator on also has a state that depends on other neighbor buses. To identify such a collection of one or more buses in $\mathcal{S}$, we first distinguish between two types of buses based on the presence of load. We henceforth identify buses with load as *load buses*. $\mathcal{K}_{\text{load}}$ denotes the bus indices of load bus. An attacker can attack either type of bus. However, since the injections of non-load buses are known to the control center, attacking a non-load bus implies that the measurements at the closest load buses also need to be changed thus the nodal power balance is maintained. In [19], a method is introduced to identify a subgraph of the network that allows an attacker to perform an unobservable attack. We use a similar method, as summarized as follow. Let k be a target load bus, the corresponding *single-target-bus attack subgraph* $\mathcal{S}_k$ is constructed by following steps:

1. Include bus k in $\mathcal{S}_k$.

2. Extend $\mathcal{S}_k$ from bus k by including all buses and branches that are connected to bus k.

3. If there is a non-load bus on the boundary of $\mathcal{S}_k$, extend $\mathcal{S}_k$ to include all adjacent buses of this boundary bus.

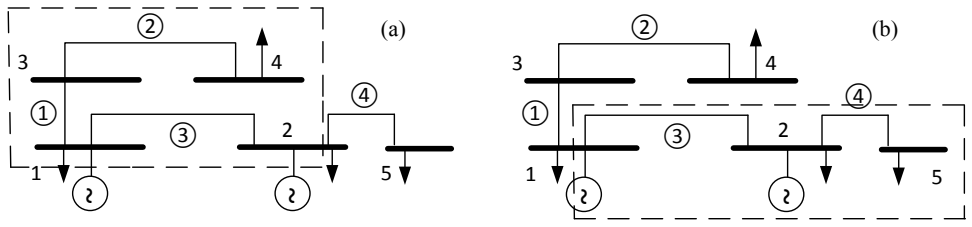

Figure 2.1: Examples of single-target-bus attack subgraph. Fig. 2(a) shows the subgraph with target bus 1 and Fig. 2(b) shows the subgraph with target bus 2.

4. Repeat step 3 until all buses on the boundary are load buses or $\mathcal{S}_k$ can not be extended anymore.

The steps above give an attack subgraph that includes the target load bus and is bounded by load buses. Fig. 2.1 shows two simple examples of single-target-bus attack subgraph. The choice of the final attack subgraph $\mathcal{S}$, however, can be a union of several single-target-bus attack subgraphs:

$$\mathcal{S} = \bigcup_{k \,:\, c_k \neq 0 \cap k \in \mathcal{K}_{\text{load}}} \mathcal{S}_k. \tag{2.3}$$

This choice of attack subgraph results in estimated load changes at all load bus within $\mathcal{S}$ while no net load changes in the system.

2.3 DC Attack

Since (2.2) is nonlinear and generally hard to solve, it is reasonable for the attacker to first consider a simplified DC attack. As [7] demonstrated, by knowing system Jacobian matrix H, an attacker can intelligently construct an unobservable attack vector $a = Hc$ such that $z_i^{(a)} = z_i + a$.

Thus, (2.2) becomes

$$z_i^{(a)} = \begin{cases} z_i & \text{if } i \notin \mathcal{I}_{SP} \\ z_i + H_{(i,:)}c & \text{if } i \in \mathcal{I}_{SP} \end{cases} \tag{2.4}$$

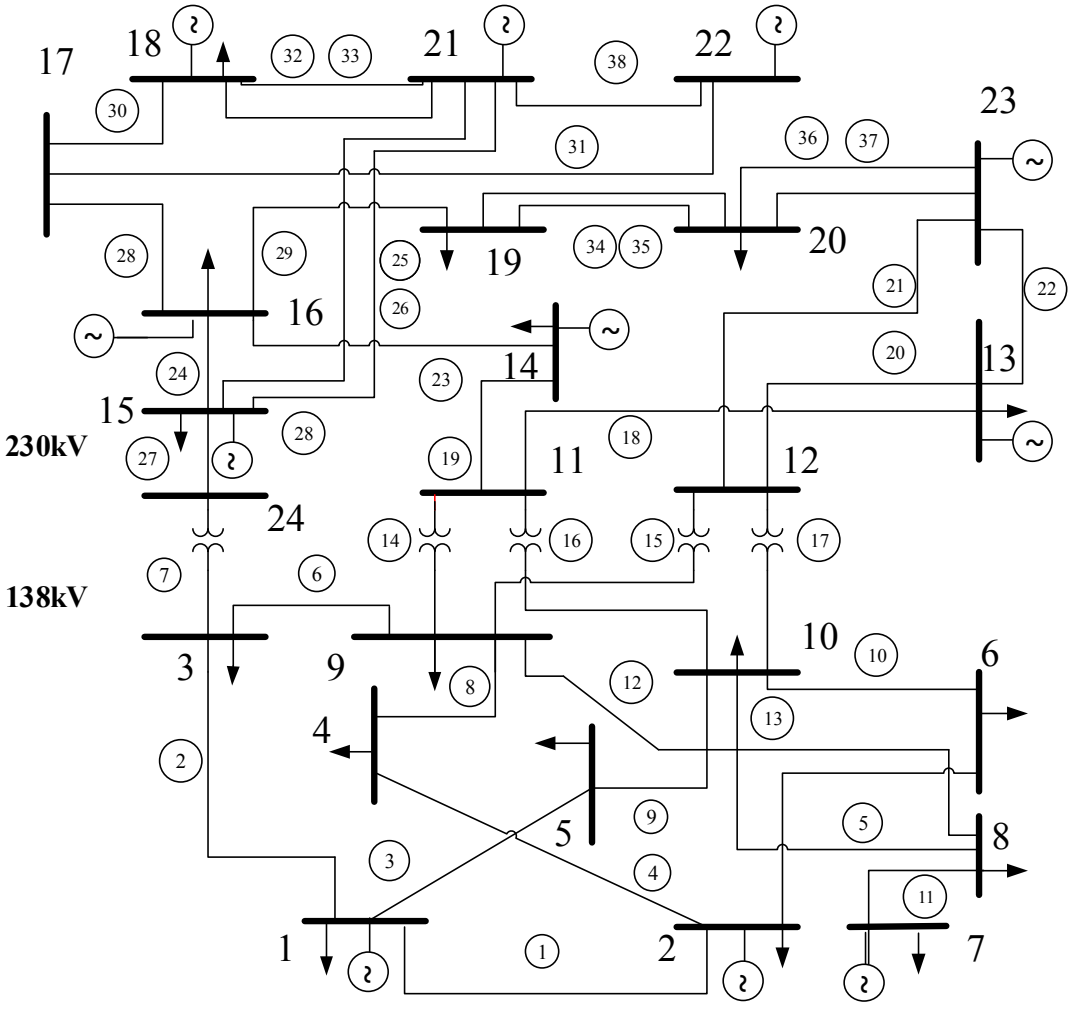

Figure 2.2: IEEE-RTS-24-bus system

where, $\mathcal{I}_P$ denotes the set of indices of active power measurements, $\mathcal{I}_{SP} = \mathcal{I}_S \cap \mathcal{I}_P$, and $H_{(i,:)}$ denotes the i^{th} row of H.

Though DC attack is easy to construct, it is not an unobservable attack for AC state estimator. Without taking reactive power flow into account, a DC attack will be detected when c is too large.

2.4 AC Attack

From (2.2), in contrary to DC attack, it seems that the attacker must know all the state values that appear in h_i, for all $i \in \mathcal{I}_{\mathcal{S}}$, to construct z_i precisely. However, this information is not available to the attacker. Thus, attacker can use the following steps to construct $z_i^{(a)}$:

1. The attacker first chooses the non-zero entries in c only for the load buses. These non-zero entries correspond to the center buses for the attack subgraph.

2. Use the protocol in Sec. 2.2 and choose $\mathcal{S}$ for the desired attack.

3. Given the measurements that are available to the attacker in $\mathcal{S}$, perform local AC state estimation to find $\hat{x}_k^{(a)}$. The slack bus may be chosen arbitrarily among all load buses.

4. For all load buses k, set $x_k^{(a)} = \hat{x}_k^{(a)} + c_k$.

5. Since the injection of non-load buses can not be changed, the states of non-load buses are dependent on the state of all the buses that connected to them. Therefore, according to (1.4) and (1.5), the attacker has the nodal balance equation for each non-load bus k in $\mathcal{S}$:

$$P_{\text{inj}_k} = V_k \sum_{i \in \mathcal{N}_k} V_i (G_{ki} \cos\theta_{ki} + B_{ki} \sin\theta_{ki}) = P_{G_k} \tag{2.5}$$

$$Q_{\text{inj}_k} = V_k \sum_{i \in \mathcal{N}_k} V_i (G_{ki} \sin\theta_{ki} - B_{ki} \cos\theta_{ki}) = Q_{G_k} \tag{2.6}$$

These equations can be solved by iterative methods such as Newton-Raphson method:

(a) set the initial value $x_k^{(a)}[0] = \begin{bmatrix} \theta_k[0] \\ V_k[0] \end{bmatrix} = \begin{bmatrix} \hat{\theta}_k^{(a)} \\ \widehat{V}_k^{(a)} \end{bmatrix}$

(b) compute the Jacobian matrix $J = \begin{bmatrix} \frac{\partial P_k}{\partial \theta_k} & \frac{\partial Q_k}{\partial \theta_k} \\ \frac{\partial P_k}{\partial V_k} & \frac{\partial Q_k}{\partial V_k} \end{bmatrix}$

(c) compute mismatch $M[t] = \begin{bmatrix} P_{\text{inj}_k}(x_k^{(a)}) \\ Q_{\text{inj}_k}(x_k^{(a)}) \end{bmatrix}$

(d) update $x_k^{(a)}[t+1] = x_k^{(a)}[t] + J^{-1}M[t]$

(e) repeat (5b) until $\|M[t]\|_\infty$ is less than the chosen limit.

6. With all the computed state information, the attacker can therefore compute the false measurements $z^{(a)}$ such that

$$z_i^{(a)} = \begin{cases} z_i & \text{if } i \notin \mathcal{I}_\mathcal{S} \\ h_i(x^{(a)}) & \text{if } i \in \mathcal{I}_\mathcal{S} \end{cases} . \tag{2.7}$$

2.5 Comparison of Attacks

In this subsection, we use the IEEE-RTS-24-bus system as test system and test both DC and AC attack on a AC state estimator. We assume that both active and reactive power flows are measured at two ends of each line and both active and reactive injection are measured at each load bus, which makes 186 measurements in total. All measurements are assumed to have an error $e_i \sim N(0, 10^{-4})$ and the χ^2 detector threshold is set to be 164.1 with 95% confidence of detection. In our simulation, we use MATPOWER to generate measurements, perform state estimation, and solve for false measurement.

In this simulation, we focus on the case $\|c\|_0 = 1$ and the only non-zero entry c_k corresponds to the voltage angle of bus k. Note that there are 17 load buses; we consider an attack centered at each one. To evaluate the performance of AC and DC attacks, we vary the value of c_k and compare the residual of the AC state estimator with χ^2 threshold.

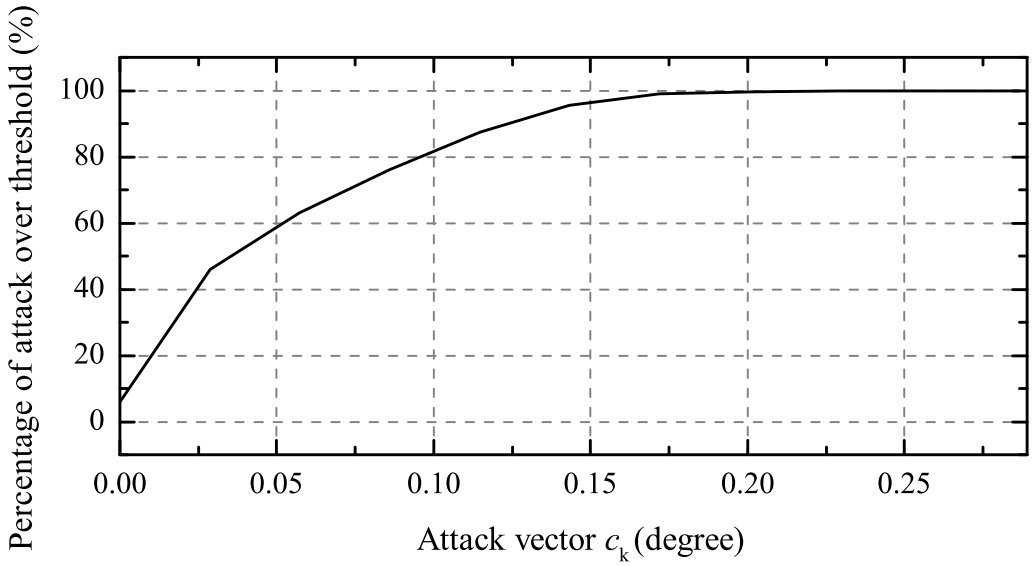

Figure 2.3: The percentage of attacks above threshold as the single state error c_i increases

DC Attack

We summarize results for DC attack model in Table 2.1. The table gives the size of attack subgraph for each attack scenario, as well as the value of c_k at which the mean residual crosses the χ^2 threshold. In Fig. 2.3, over 100 attack simulations per attack bus, we plot the percentage of attacks above the threshold as the function of attack magnitude $\|c\|$. Observe that the percentage above threshold increases quickly as $\|c\|$ increases; in fact, for $\|c\|$ as small as 0.2 degrees, virtually all DC attacks are detectable. Specifically, for buses 4 and 10 we plot the residual as a function of c in Figs. 2.4 and 2.5, respectively. Target buses 4 and 10 are representative of attacks on buses with relatively larger and smaller subgraph, respectively.

AC Attack

Also plotted in Figs. 2.4 and 2.5 are the residuals when the attacker uses a local AC state estimation for the same values of c_k. As expected, the residuals resulting from

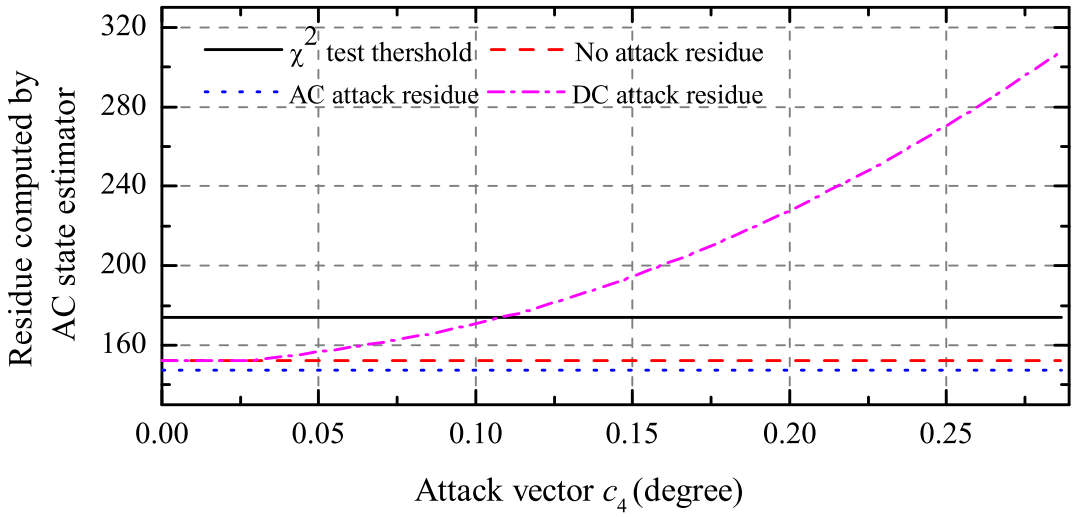

Figure 2.4: Residual for DC and AC attacks as the attacker increases the Voltage angle of bus 4.

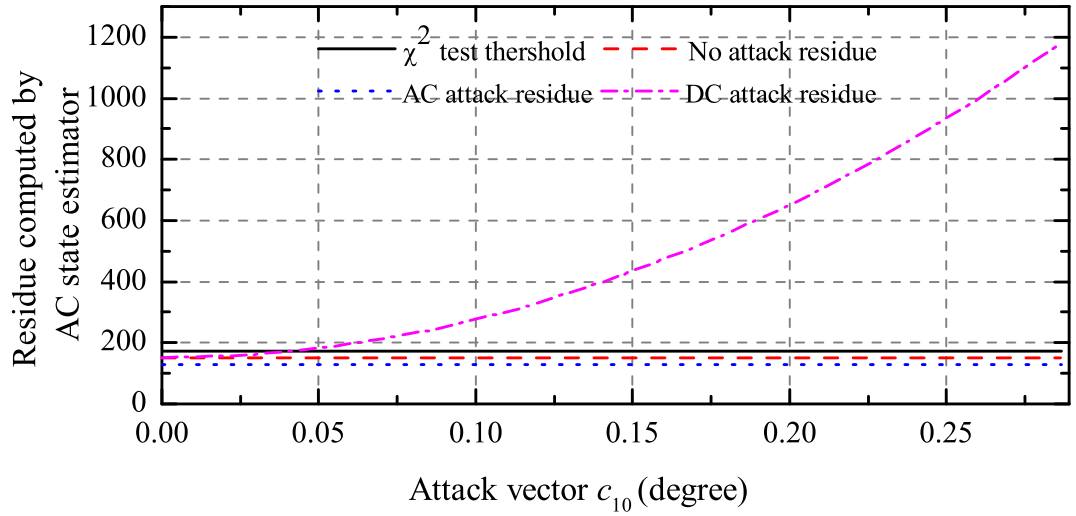

Figure 2.5: Residual for DC and AC attacks as the attacker increases the voltage angle of bus 10.

Table 2.1: Summary of DC attack

Center bus k	Number of buses in S_k	Number of branches in S_k	Post-threshold c_k (deg.)
1	4	3	0.0228
2	4	3	0.0228
3	5	4	0.0915
4	3	2	0.1145
5	3	2	0.0915
6	3	2	0.0915
7	2	1	0.1087
8	4	3	0.0743
9	10	13	0.0572
10	10	13	0.0457
14	6	5	0.0401
15	5	5	0.0228
16	7	6	0.0170
19	3	3	0.0228
20	3	4	0.0170

the AC attack model are always below the χ^2 threshold irrespective of the value of c_k. More interestingly, we note that the average residual is even smaller than the no attack case. This is due to the false data are directly constructed from the false state $x^{(a)} = x + c$ with a AC system model. Therefore, the measurements in $\mathcal{S}_k$ are noise-free in respect of the system model and contribute nothing in the residuals. By comparing Figs. 2.4 and 2.5, AC attack with a large attack subgraph has smaller

residual than the one with a small attack subgraph. DC attack, in contrary, with a large attack subgraph has much larger residual.

2.6 A Brief Discuss of Consequences for the Unobservable Attacks

We now describe a physical consequence of the AC attack model. We assume that the system is operating at normal state prior to the attack. After the attack is launched, it may trick the operator into thinking that the normal state has moved to an emergency state (some operational limits are violated) or a restorative state (partial or total blackout). Either way, it is possible that such an attack leads to additional control actions that changes the physical system, including topology, generation dispatch, load shedding schedule, and so forth.

For instance, suppose that the attacker injects false data such that the estimated voltage angle at bus 7 is increased by 4.01 degrees. The absolute power flow measured at bus 7 side of branch 7-8 is increased from 89.40 MVA to 196.19 MVA, which exceeds its long term rating of 175 MVA. The control center observes this abnormality and considers the system to be in emergency state in need of corrective. If the attacker has knowledge about emergency control procedure, then it is possible for the attacker to influence the dynamics of the physical system.

We simulate this emergency response at the control center as follows:

1. The system is modeled as operating at an optimal power flow situation and the load of the system is constant during the attack period.

2. An ACOPF with a minimum cost objective function is applied as an emergency or corrective control procedure to re-dispatch generation when the operator monitors any line limit violation.

3. The system is assumed to have congestion. Long term ratings of all lines are degraded proportionally to let one line be congested just prior to the attack,

specifically line 6-10. This assumption is made because the IEEE-RTS system has redundant transmission capacity.

Suppose the state estimator runs every time unit. At time $t = 1$, the attacker constructs an unobservable attack vector c such that $\|c\|_0 = 1$ and $c_7 = 2.865$ degree. The absolute power flow of line 7-8 (measured at bus 7 side) increases from 89.40 MVA to 165.00 MVA, which is 101.11% of the long-term rating. This attack causes the estimated load at bus 7 to decrease and estimated load at bus 8 to increase. It triggers an alarm and the emergency control is involved. Then, as a result, the control center re-dispatches the generation via ACOPF to eliminate the false line rating violation. Following this initial attack, the attacker continues to use the same strategy and injects the same c into the system at subsequent estimation intervals. As shown in Fig. 2.8, at time $t = 1$, the generation level at bus 7 reduces and that of bus 13 increases. Fig. 2.8 also shows that after time 1, changes in active power generation are minor and caused only by measurement errors. Thus, an unobservable attack on a single bus led to a physical generation re-dispatch. Specifically, the generators at bus 7 reduce generation to decrease line flow from bus 7. To ensure the power balance generators at bus 13 increase generation. Figs. 2.6 and 2.7 show some of the real states evolutions during the attack. Figs. 2.9 to 2.11 show a different case at bus 2 with $c_2 = 1.719$ degree.

In this chapter, it has been shown that the FDI attack with a AC attack model has influence on the physical system. Also, in the simulation, cases with real line overload after attack are observed. This indicates that a possible attack consequence is overloading lines. However, since the choice of the attack vector c in this chapter is simple and exhaustive, the overload is not guaranteed. Furthermore, the attack has some unrealistic side effects: for instance, in some cases with large generation re-dispatch, the load on a bus has to be changed from positive to negative at the moment

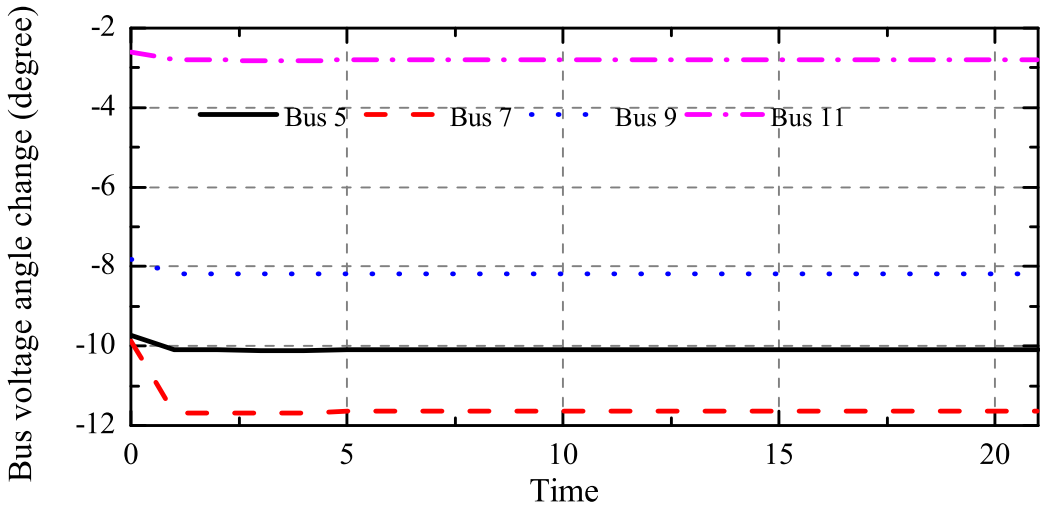

Figure 2.6: Real voltage angle evolution at bus 2, 7, 9, and 11 for attack centered at bus 7 (degree)

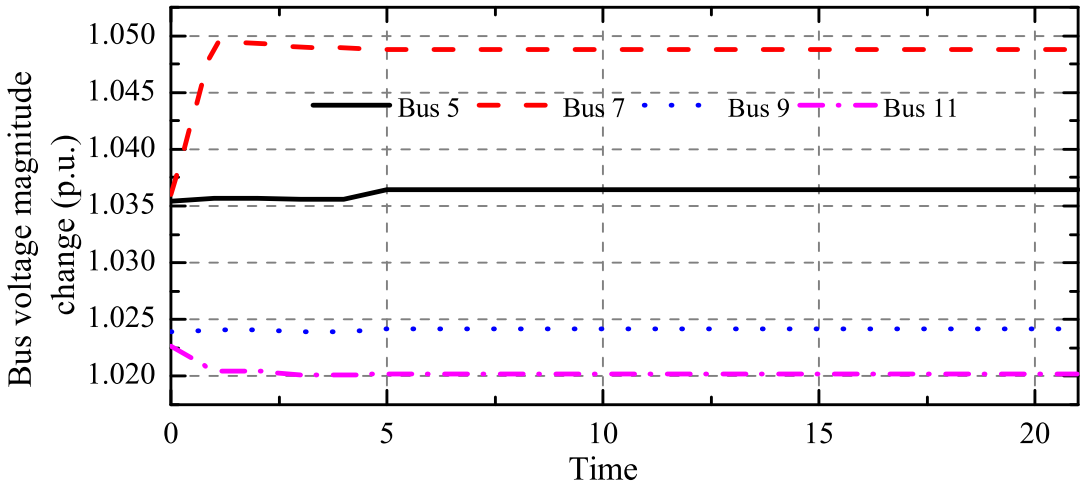

Figure 2.7: Real voltage magnitude evolution at bus 2, 7, 9, and 11 for attack centered at bus 7 (p.u.)

of attack, indicating a bus is suddenly generating power instead of consuming it. This is extremely peculiar in reality since the load in power system are generally inertial and such an huge change in load will immediately noticed by the operator. Therefore, a more intelligent and subtle way of choosing attack vector c should be considered.

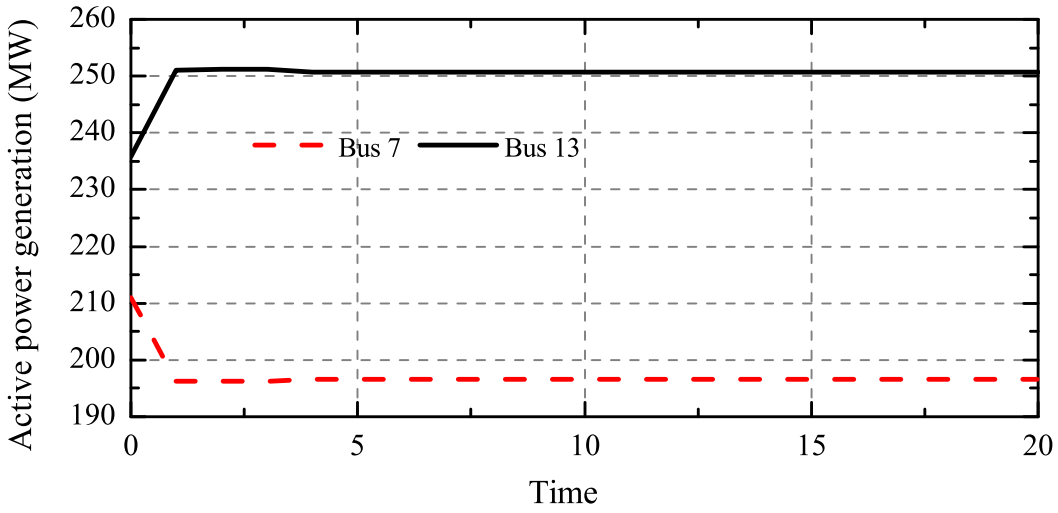

Figure 2.8: For attack centered at bus 7, active power generation dispatch before and after attack. Attack starts at $t = 1$

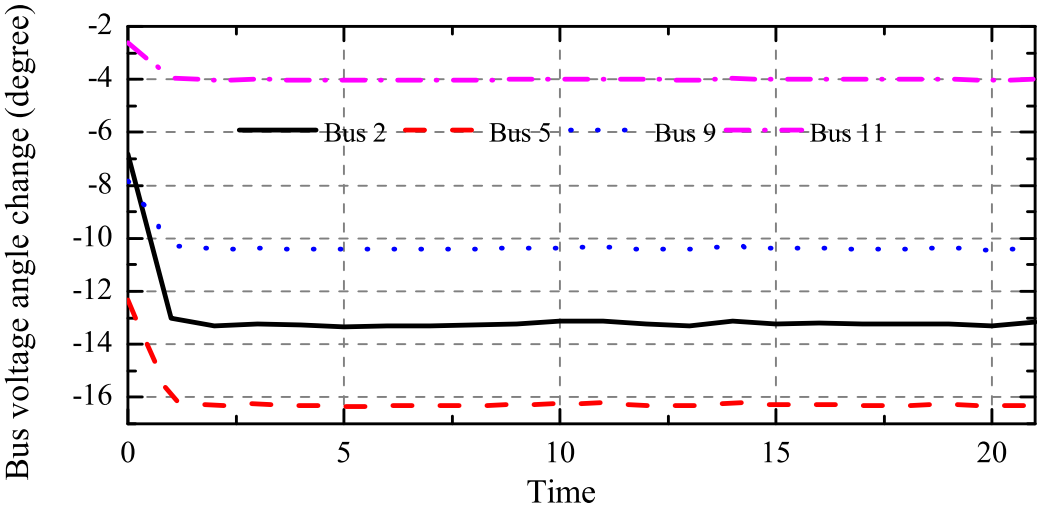

Figure 2.9: For attack centered at bus 2, real state evolution at bus 2, 5, 9, and 11: Angle (degree)

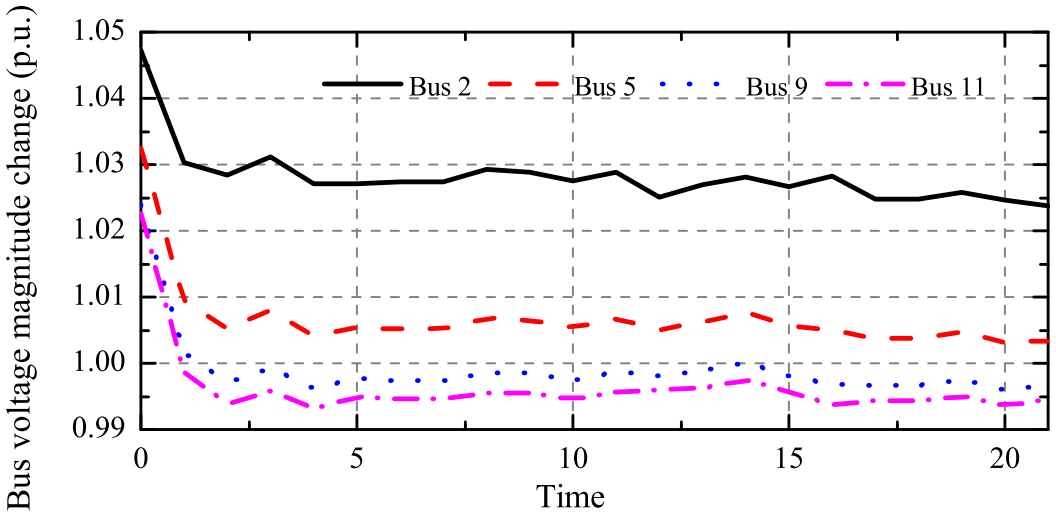

Figure 2.10: For attack centered at bus 2, real state evolution at bus 2, 5, 9, and 11: Magnitude (p.u.)

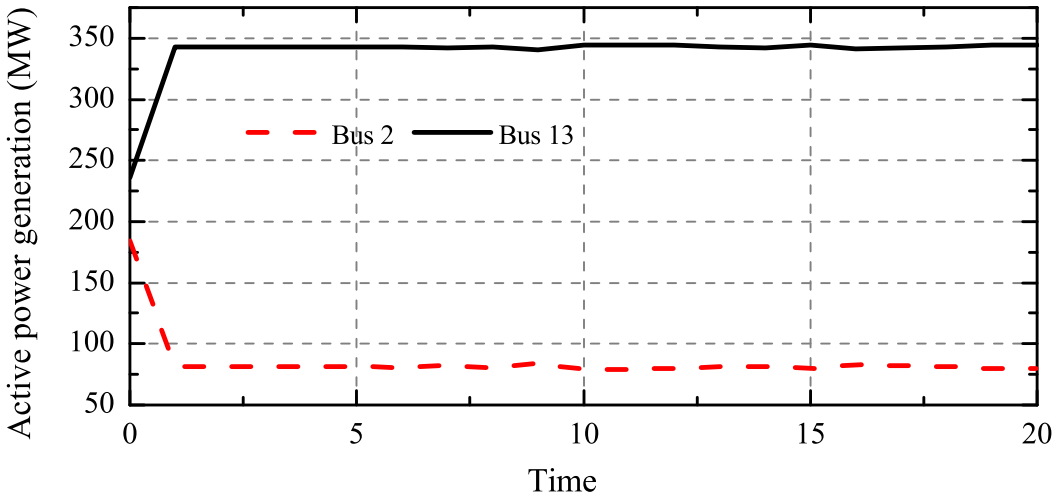

Figure 2.11: For attack centered at bus 2, active power generation dispatch before and after attack. Attack starts at $t = 1$

Chapter 3

OPTIMIZATION PROBLEM FOR THE WORST-CASE LINE OVERLOAD ATTACK

In Chapter 2, the attacker's influence over the physical system has been demonstrated. However, the random change of the system state seems pointless to a malicious attacker. A malicious and capable attacker will try to manipulate the physical system into an operation status as she desires. In this chapter, such an intelligent attack is discussed.

3.1 Problem Description

The aim of the unobservable attack is to maximize the physical line flow for a chosen line in the attack subgraph. However, the attacker, in general, has limited resources to change states; furthermore, the attacker would also like to design the attack to avoid detection over the various computing units in EMS. This leads to a constrained optimization problem. Specifically, we model the two conflicting goals of the attacker as follows: the limited resource constraint is modeled by a sparsity constraint in which we limit the number of center buses at which states can be changed. The detectability constraint is modeled by limiting the cyber load shifts that result from the FDI attacks. This is because a large deviation in estimated load from normal operational values will be detected as an anomalous event by the operators. The sparsity constraint capturing the limited resource is modeled as an l_0-norm constraint. This is, in general, intractable, and therefore, we relax it to an l_1-norm constraint. In addition to the two constraints, since the physical line flow is a consequence of the control center re-dispatch generation, the attack optimization process has to include the OPF subsequent to state estimation as a sub-problem. The resulting problem is a bi-level optimization problem.

Generally, an optimal dispatch can be the result of different load patterns. As a result, there are numerous solutions of attack vector that lead to the same physical line flow on the target line. Among these, the goal of the optimization is to choose the one with the smallest l_1-norm, and hence, l_0-norm to satisfy the limited resources constraint. This, in turn, requires a second entry in the objective function where we determine the sparest attack vector among the same maximal power flow on the target branch.

Finally, a linearized system model is used in the problem formulation. The DC model is an appropriate approximation of the AC model and it will simplify the problem and decrease the solving time. To test the accuracy of the solution, we substitute the DC solution into a AC model to validate the result. Details will be discussed in the Sec. 3.4.

3.2 Optimization Problem Formulation

The attacker's influences over the system can be formulated as an optimization problem (with attacker's objective) embedded with a sub-problem (with operator's objective). Similar to the authors in [13, 15], we model the optimal attack problem as a bi-level optimization problem with an objective to maximize the power flow on branch l while to change as few states as possible:

$$\text{Main Problem:} \quad \text{maximize} \quad P_l - \gamma \left\|c\right\|_0 \tag{3.1}$$

$$\text{subject to}$$

$$P = H_2(\theta^\star - c) \tag{3.2}$$

$$-L_S P \leq H_1 c \leq L_S P_L \tag{3.3}$$

$$\left\|c\right\|_0 \leq N_0 \tag{3.4}$$

$$\text{Sub-problem:} \quad \{\theta^\star, P_G^\star, R^\star\} = \arg\left\{\min_{\theta, P_G, R} \sum_{g=1}^{n_g} f_g(P_{G_g}) + \sum_{l=1}^{n_{br}} \mathcal{P}_l(R_l)\right\} \tag{3.5}$$

$$P_G - H_1(\theta - c) - P_L = 0 \qquad (\upsilon) \tag{3.6}$$

$$-P^{\max} - R \leq H_2\theta \leq P^{\max} + R \qquad (\lambda^+, \lambda^-) \tag{3.7}$$

$$P_G^{\min} \leq P_G \leq P_G^{\max} \qquad (\alpha^+, \alpha^-) \tag{3.8}$$

$$0 \leq R \qquad (\beta) \tag{3.9}$$

where the variables:

P	is the $n_{br} \times 1$ vector of branch power flow;
c	is the $n_b \times 1$ attack vector;
$\theta, \theta^\star$	are $n_b \times 1$ state variable vectors and optimal variable solved by DCOPF, respectively;
$P_G, P_G^\star$	are $n_g \times 1$ vectors of generation dispatch variable and optimal generation dispatch solved by DCOPF, respectively;
$R, R^\star$	are $n_{br} \times 1$ vectors of the line relaxation variable, and optimal line relaxation solved by DCOPF, respectively;
υ	is the $n_b \times 1$ dual variable vector for all equal constraints in DCOPF;
λ^+, λ^-	are $n_{br} \times 1$ dual variable vectors of the upper and lower bound of thermal limits, respectively;
α^+, α^-	are $n_g \times 1$ dual variable vectors of the upper and lower bound of generator capacity, respectively;

and the parameters:

L_S	is the load shift factor;
P_L	is the $n_b \times 1$ vector of active load at each bus;
N_0	is the l_0-norm constraint integer;
H_1	is the $n_b \times n_b$ matrix of dependencies between power injection measurement and state variable;
H_2	is the $n_{nb} \times n_b$ matrix of dependencies between power flow measurement and state variable,
f_g	is the cost function of the g^{th} generator,;
$\mathcal{P}_l$	is the penalty function of relaxing the l^{th} line;
$P^{\max}$	is the $n_{br} \times 1$ vector of line thermal limit;
$P_G^{\min}, P_G^{\max}$	are $n_g \times 1$ vectors of minimum and maximum generator output, respectively.
γ	the weight of the norm of attack vector c.

We define l_0-norm as appropriate quantities summed over only the load buses. Thus, the l_0-norm, $\|c\|_0$, of the attack vector c is defined as

$$\|c\|_0 = \sum_{k \in \mathcal{K}_{\text{load}}}^{n_b} 1(c_k \neq 0). \tag{3.10}$$

Recall the goal of optimization is to maximize P_l while finding the sparsest attack among all the possible attack vector. Thus, due to the trade-off between the maximum power flow and the corresponding sparest attack vector, thus the optimization objective is $P_l - \gamma \|c\|_0$. The weight γ is chosen to be a small and positive value such it in general contributes minimal to the objective. Note that (3.2)–(3.4) are the attack related constraints. The constraints in (3.2) model the unobservability of the attack and the constraints in (3.3)–(3.4) model the attacker's limited ability: the attacker can alter up to N_0 states (not necessarily alter all of them) and the resulting change in load shift is limited to $L_S P_L$. A standard DCOPF with a thermal limit relaxation

penalty is modeled by (3.5)–(3.9). The penalty function in (3.5) ensures the second level OPF converge thus the first level problem to return a solution.

Since (3.4) is a modified l_0-norm constraint, it is a complex non-linear constraint and generally non-convex. In this paper, we relax it to a corresponding l_1-norm constraint as

$$\|c\|_1 = \sum_{k \in \mathcal{K}_{\text{load}}} |c_k| \leq N_1 \tag{3.11}$$

where N_1 is non-negative. Since (3.11) is a non-linear constraint and we rewrite it as

$$-c_k \leq s_k \tag{3.12}$$

$$c_k \leq s_k \tag{3.13}$$

$$\sum_{k \in \mathcal{K}_{\text{load}}} s_k \leq N_1 \tag{3.14}$$

where s is a slack variable.

For the embedded OPF problem, the optimal solution can be found at the point which satisfies the KKT optimality condition with zero duality gap since it is a convex optimization problem [26]. We use this fact to further replace the embedded DCOPF problem in (3.5) with its KKT conditions below, along with (3.6)–(3.9), as

$$\left[\lambda^+; \lambda^-; \alpha^+; \alpha^-; \beta\right] \geq 0 \tag{3.15}$$

$$\text{diag}\left(\left[\lambda^+; \lambda^-\right]\right)\left([H_2; -H_2]\,\theta^\star - [P^{\max} + R^\star]\,[I; -I]\right) = 0 \tag{3.16}$$

$$\text{diag}\left(\left[\alpha^+; \alpha^-\right]\right)\left([I; -I]\,P_G^\star - \left[P_G^{\max}; -P_G^{\min}\right]\right) = 0 \tag{3.17}$$

$$-\text{diag}(\beta)R^\star = 0 \tag{3.18}$$

$$\begin{aligned} &\nabla\Big(\sum_{g=1}^{n_g} f_g(P_{G_g}^\star) + \sum_{l=1}^{n_{br}} \mathcal{P}_l(R_l^\star)\Big) \\ &+ \left[\lambda^+; \lambda^-\right]^T \nabla\left([H_2; -H_2]\,\theta^\star - [P^{\max} + R^\star]\,[I; -I]\right) \\ &+ \left[\alpha^+; \alpha^-\right]^T \nabla\left([I; -I]\,P_G^\star - \left[P_G^{\max}; -P_G^{\min}\right]\right) \end{aligned} \tag{3.19}$$

$$-\beta^T \nabla R^\star + \upsilon^T \nabla [P_G^\star - H_1(\theta^* - c) - P_L] = 0$$

where (3.16)–(3.18) are the complementary slackness condition for constraint (3.7)–(3.9) and (3.19) is the partial gradient optimal condition. Though (3.16)–(3.18) are non-linear, they have specially distinctive nature. For instance, the j^{th} equation in (3.18) can be separated into two conditions associated with a binary variable δ_{β_j}

$$\begin{cases} \beta_j \geq 0 \text{ and} -R_j^\star = 0, & \text{if } \delta_{\beta_j} = 0 \\ \beta_j = 0 \text{ and} -R_j^\star < 0, & \text{if } \delta_{\beta_j} = 1. \end{cases} \tag{3.20}$$

In [27], a procedure is proposed to write (3.20) in a mixed integer problem

$$\begin{cases} \delta_{\beta_j} = \{1, 0\} \\ \beta_j \leq C\delta_{\beta_j} \\ R_j^\star \leq C(1 - \delta_{\beta_j}) \end{cases} \tag{3.21}$$

If $\delta_{\beta_j} = 1$, substitute (3.9) and (3.15) into (3.21), we have

$$\begin{cases} \delta_{\beta_j} = 0 \\ 0 \leq \beta_j \leq 0 \\ 0 \leq R_j^\star \leq C_j. \end{cases} \tag{3.22}$$

Thus, if C_j is large enough to not effect the solution of $R_j^\star$, (3.22) is equivalent to the complementary slackness when the j^{th} constraint in (3.9) is not an active constraint.

Similarly, if $\delta_{\beta_j} = 1$ and substitute (3.9) and (3.15) into (3.26), we have

$$\begin{cases} \delta_{\beta_j} = 1 \\ 0 \leq \beta_j \leq C_j \\ 0 \leq R_j^\star \leq 0. \end{cases} \tag{3.23}$$

Again, if C_j is large enough to not effect the solution of β_j, (3.23) is equivalent to the complementary slackness when the j^{th} constraint in (3.9) is an active constraint. Therefore, (3.21) is equivalent to (3.18).

Thus, the whole problem becomes the mixed-integer linear program

$$\text{maximize} \qquad P_l - \gamma \sum_{k \in \mathcal{K}_{\text{load}}} s_k$$

subject to

$$(3.2)\text{–}(3.3),\ (3.6)\text{–}(3.9),\ (3.12)\text{–}(3.15),\ (3.19)$$

$$\begin{cases} \delta_{\lambda_l}^{\pm} = \{1, 0\} \\ \lambda^{\pm} \leq C\delta_{\lambda}^{\pm} \\ -H_2\theta^{\star} + P^{\max} + R^{\star} \leq C(1 - \delta_{\lambda}^{+}) \\ +H_2\theta^{\star} + P^{\max} + R^{\star} \leq C(1 - \delta_{\lambda}^{-}) \end{cases} \tag{3.24}$$

$$\begin{cases} \delta_{\alpha_l}^{\pm} = \{1, 0\} \\ \alpha^{\pm} \leq C\delta_{\alpha}^{\pm} \\ -P_G^{\star} + P_G^{\max} \leq C(1 - \delta_{\alpha}^{+}) \\ P_G^{\star} - P_G^{\min} \leq C(1 - \delta_{\alpha}^{-}) \end{cases} \tag{3.25}$$

$$\begin{cases} \delta_{\beta_j} = \{1, 0\} \\ \beta \leq C\delta_{\beta} \\ R^{\star} \leq C(1 - \delta_{\beta}) \end{cases} \tag{3.26}$$

where $\delta_{\lambda}^{\pm}$, $\delta_{\alpha_l}^{\pm}$ and δ_{β_l} are binary variables and C is a large constant.

3.3 Solutions of Optimization Problem

In this section, we run the optimization problem defined in Sec. 3.2 on the IEEE RTS-24-bus system to find an optimal attack vector c. Subsequently, we use this attack vector c to simulate an AC attack described in Sec. 2.4 and given by (2.7)

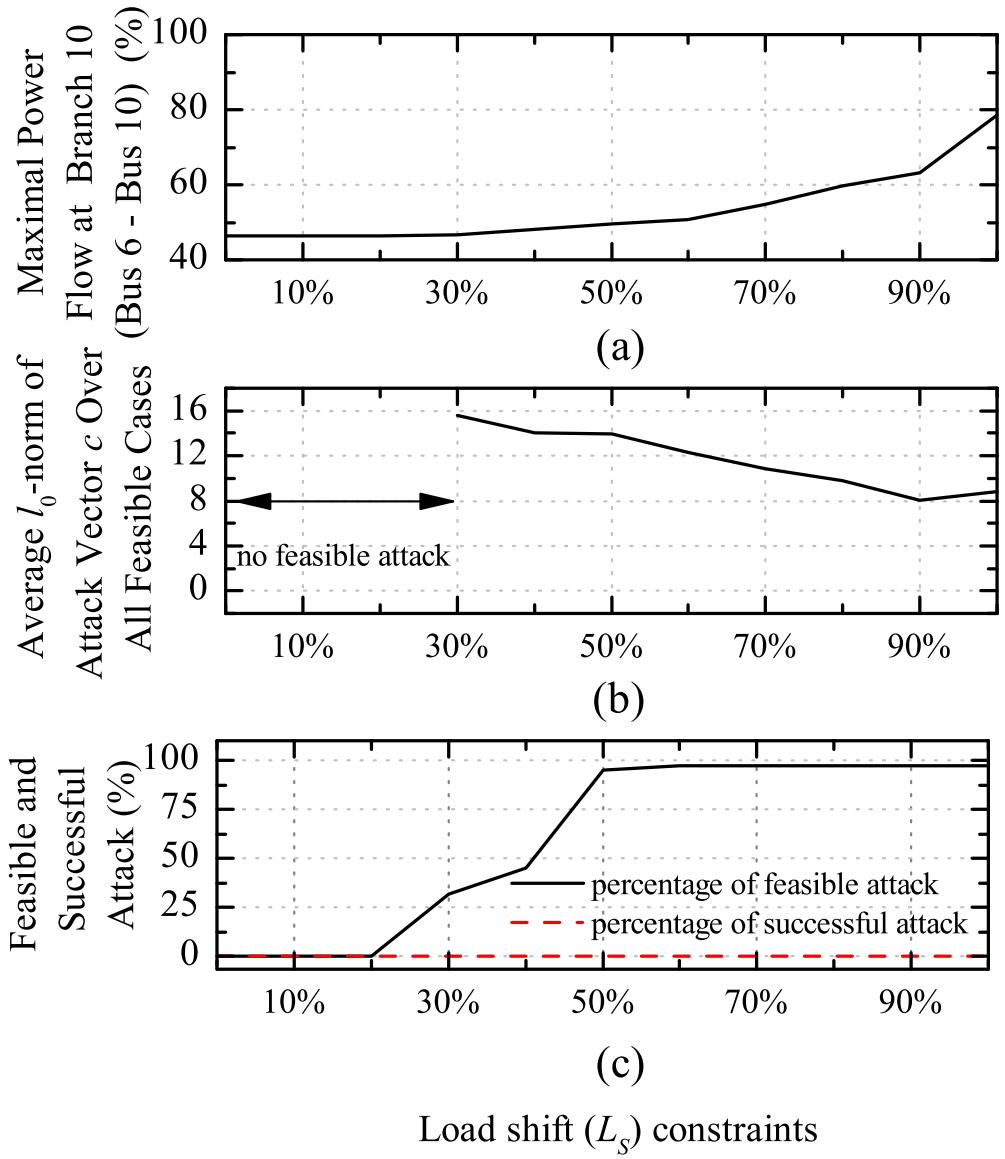

Figure 3.1: Statistic summary of 38 attack scenarios for the omnipotent attacker for a non-congested system.

against a non-linear system model involving AC state estimation and ACOPF. AC power flow, AC state estimation, and ACOPF are implemented with MATPOWER toolbox in MATLAB. For the optimization problem, we use CPLEX as the solver.

We highlight results of two scenarios for the RTS-24-bus system: one with original rating and one with reduced rating. The one with original rating represents a

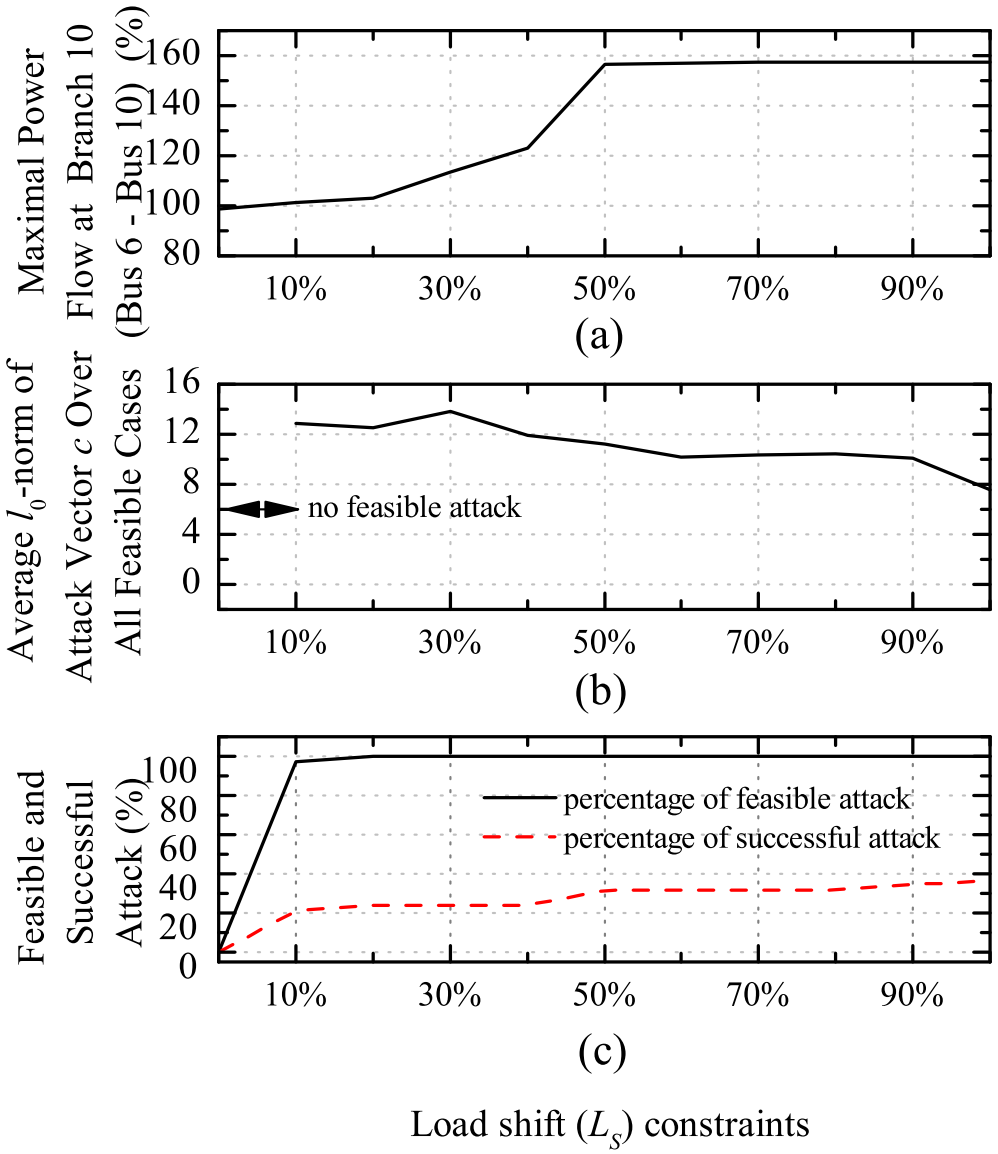

Figure 3.2: Statistic summary of 38 attack scenarios for the omnipotent attacker for a congested system with rating decreased by 50%.

system without congestion prior to attack and the one with reduced rating represent a congested system.

Second, we define an attack as *feasible* if the resulting change in power flow is more than 1% of the power flow value prior to the attack. This is to distinguish the cases with no or minor changes on target branch power flow P_l after attack from those with large changes. We furthermore define a feasible attack to be *successful* if the

target branch is overloaded after attack. We choose γ to be 1% of the original power flow value of the target branch.

Figs. 3.1 and 3.2 illustrate relevant statistics for the non-congested and congested systems, respectively, when the N_1 constraint is set to be infinite. That is, the attacker has control over all measurements of the system and can change as many measurements as it wishes. The congested system is modeled with all branch ratings decreased by 50%. There are three subplots in both Figs. 3.1 and 3.2. Subplot (a) shows the maximal power flow on branch 10 (based on our observation, this is the attack with the maximal power flow, i.e., the worst-case attack); subplot (b) shows the average l_0-norm of attack vector c over all feasible cases; and subplot (c) shows the percentage of feasible and successful attacks.

For both non-congested and congested scenarios, we observe that the maximal power flow increases as L_S constraint relaxes in Figs. 3.1(a) and 3.2(a). In Fig. 3.2(a), we observe a plateau after $L_S > 50\%$. It is due to the generator location and capacity limitation and the fact that the line flow on branch 10 cannot be increased anymore. From Figs. 3.1(b) and 3.2(b), as L_S constraint relaxes, it is easier to attack the system since the average l_0-norm decreases and the attacker needs to change fewer bus states. It is due to the fact, for some cases, that the maximal power is saturated when the L_S constraint relaxes. The attacker effectively concentrates the change of loads on fewer buses with heavy loads therefore changes fewer bus states. From Figs. 3.1(c) and 3.2(c), we observe that the attacker can find more feasible cases as L_S constraint relaxes. Even if the attacker has full control over the system meters, its influence over the system is extremely limited by the load shift constraint. For instance, from Fig. 3.1(c), when $L_S = 20\%$, the attacker cannot find any feasible attacks while the attacker can find 12 feasible attacks when $L_S = 30\%$.

Comparing Figs. 3.1 and 3.2, the congested system is more vulnerable to our FDI attack. For a non-congested system, from Fig. 3.1(c), the attacker cannot generate any successful attack. On the other hand, in Fig. 3.2(c), the feasible and successful attack percentage increases as L_S constraint increases for the congested system. This is expected because the RTS-24-bus system has redundant transmission capacity for reliability reasons and reducing all the line ratings proportionally will create a more stressed system. In conclusion, a congested system is naturally favored by the attacker. Thus, for the rest of the simulation, we only consider the congested system to illustrate the attack consequences.

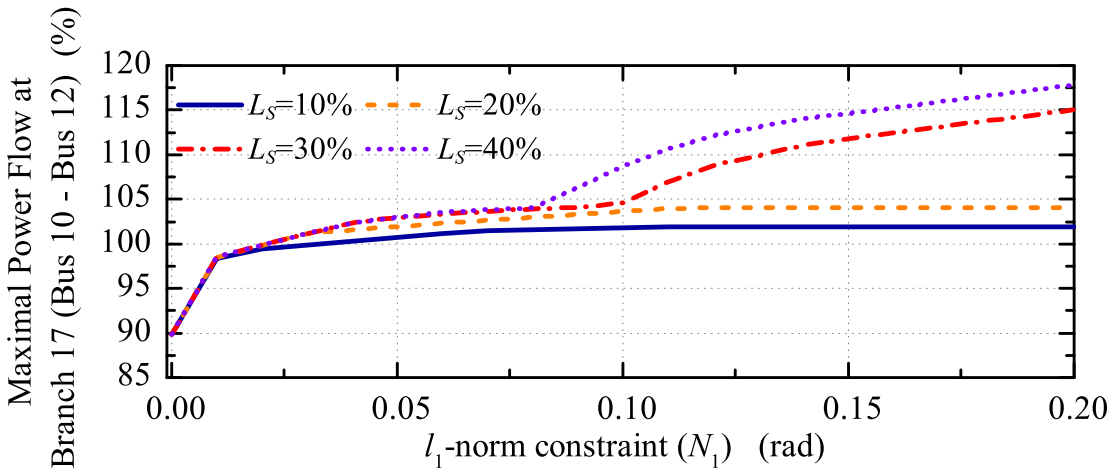

Figure 3.3: The maximal power flow v.s. the l_1-norm constraint (N_1) for different value of load shift (L_S) at target branch 17 (bus 10–bus 12).

Now we discuss the l_1-norm constraint. To understand the effect of the sparsity constraint, we fix the L_S constraint, and we solve the proposed optimization problem for different l_1-norm constraint (N_1) and for all target branches. Figs. 3.3 and 3.4 show two of the successful attacks with target branches 17 and 23, respectively. Figs. 3.3 and 3.4 show that, as N_1 relax, the attacker can increase the power flow in some degree while the L_S constraint restricts the maximal power flow on the target branches. And in fact that these two branches are congested (branch 23) or

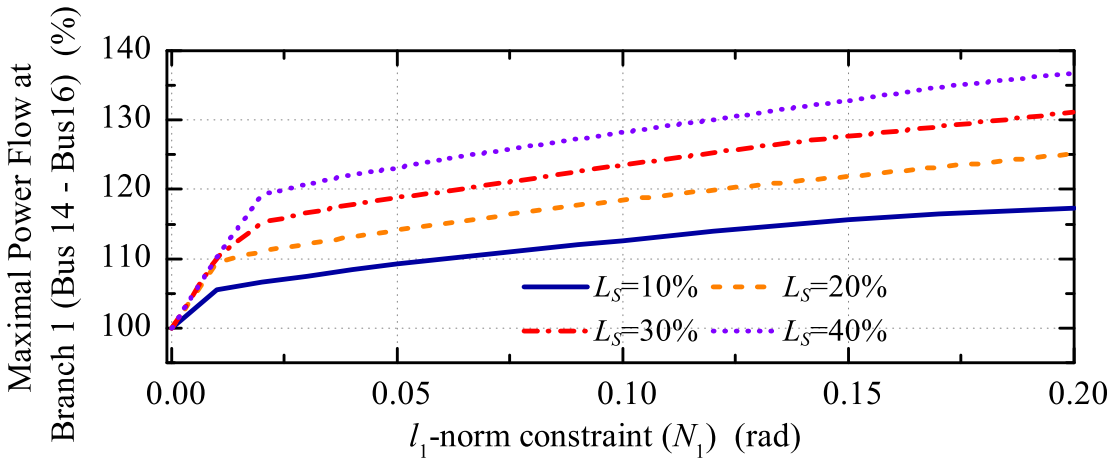

Figure 3.4: The maximal power flow v.s. the l_1 -norm constraints with different load shift tolerance at target branch 23 (bus 14–bus 16).

nearly congested (branch 17 with 89% of its transmission capacity occupied) prior to attack is mainly the result why the attacks are successful. Moreover, the kink in Fig. 3.3 represents point of which the attack is large enough to cause a different set of generators to be dispatched.

In Figs. 3.5 and 3.6, we illustrate the l_1-norm constraint on the maximal power flow for the chosen branches, the l_0-norm and the l_1-norm of the attack vector for target branches 17 and branch 23, respectively. In each sub-plot, we plot the two solutions: one with γ (black solid line)and one without γ (blue dashed line) in the objective function. Recall, as detailed in Sec. 3.2, the l_0-norm and l_1-norm computed in (3.10) and (3.11) are only for the load buses and γ is the coefficient of the objective function. In Fig. 3.5a, the two solutions overlaps, thus highlighting the choice of γ does not effect the maximal power flow on target branch. Fig. 3.5b illustrates that γ entry effectively chooses the minimal l_1-norm attack vector: with γ, l_1-norm of attack vector c stops increasing when the solution of maximal power flow stops increasing; however, when $\gamma = 0$ when the l_1-norm of attack vector c keeps increasing even though the power flow on branch 17 cannot be increased anymore. As a result, the minimal

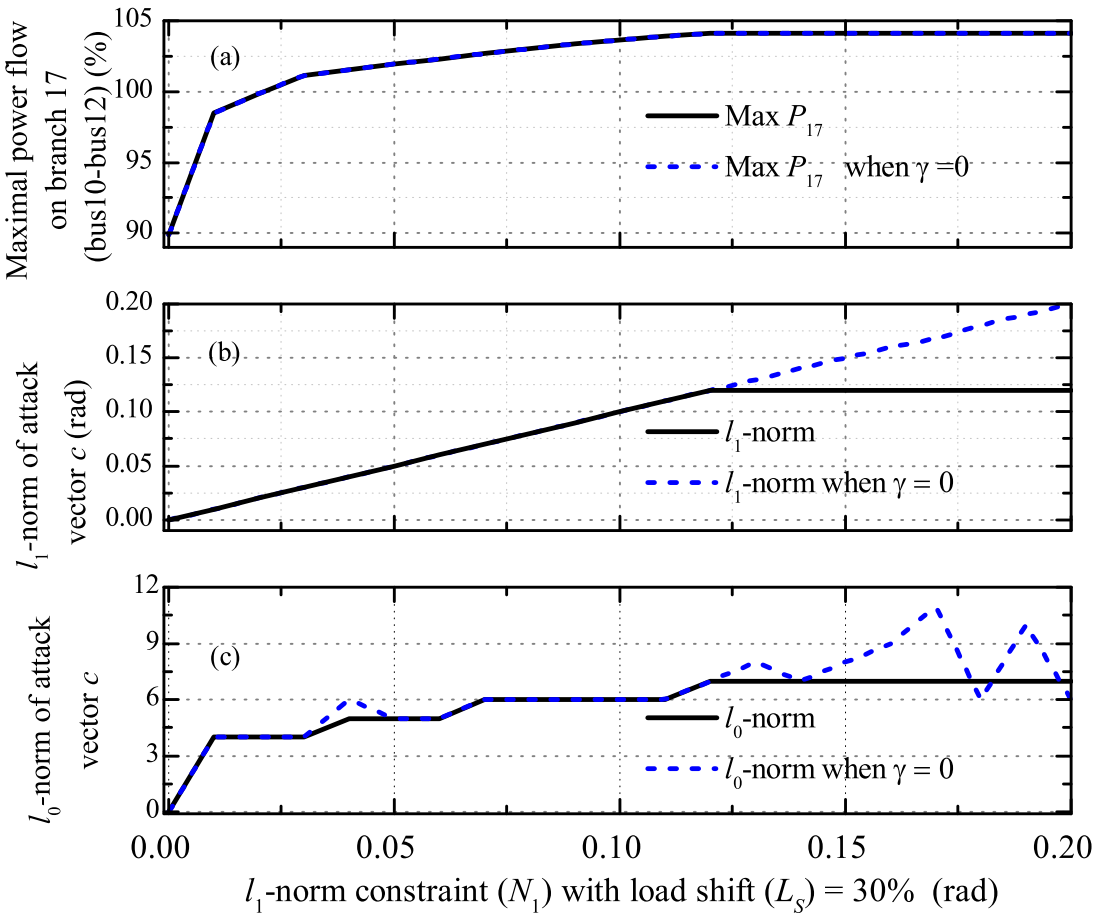

Figure 3.5: The l_1-norm and l_0-norm of solved attack vector c v.s. the l_1 -norm constraint (N_1) when load shift (L_S) is limited to 30 %; target branch 17 (bus 10–bus 12).

l_0-norm attack vector is obtained, as shown Fig. 3.5c. Comparing Figs. 3.5b and 3.5c, it is shown that the l_1-norm can not perfectly track l_0-norm. This is due to a radial branch 11 (bus 7–bus 8) in the attack subgraph. For branch 11, a voltage angle decrease on bus 7 and a voltage angle increase on bus 8 can lead to a same power flow change on branch 11. The corresponding attack vectors have the same l_1-norm and in fact result in same load shift on buses 7 and 8. Fig. 3.6 show another successful attack with branch 23 (bus14 –bus16). In this scenario, the l_1-norm constraint tracks l_0-norm constraint well and the sparsity patterns of c are exactly the same not matter γ entry is in objective function or not.

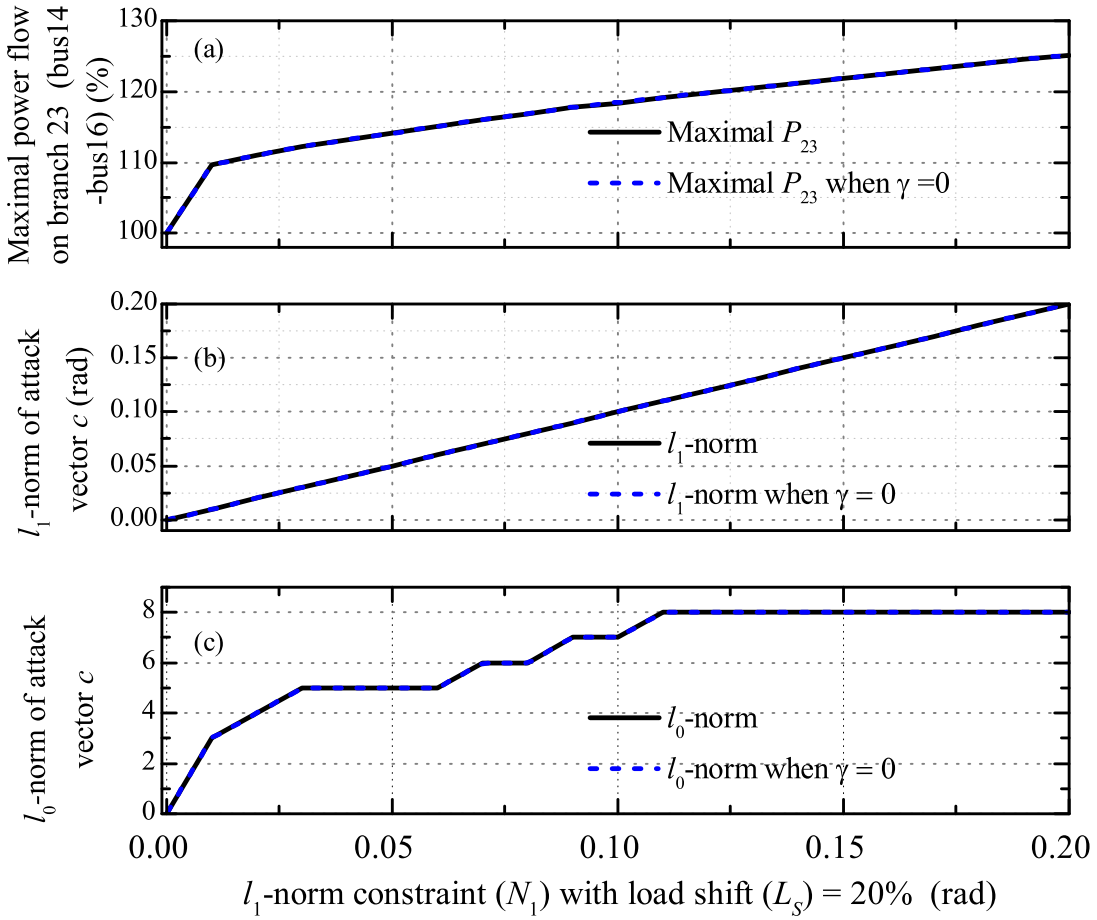

Figure 3.6: The l_1-norm and l_0-norm of solved attack vector c v.s. the l_1-norm constraint (N_1) when load shift (L_S) is limited by 20%; target branch 23 (bus 14–bus 16).

3.4 Simulation of Consequences of Non-linear Model

We now use the attack vector from the optimization problem to perform the AC attack described in Sec. 2.4. If the attacker keeps injecting false data, the attack as well as the overload on the branches will be sustained until the system configuration changes.

In this subsection, we assume a system with a complete set of measurements, i.e., both active and reactive power flows are measured at two ends of each branch and both active and reactive injection are measured at each load bus, which makes 186 measurements in total. All measurements are assumed to have an error $e_i \sim$

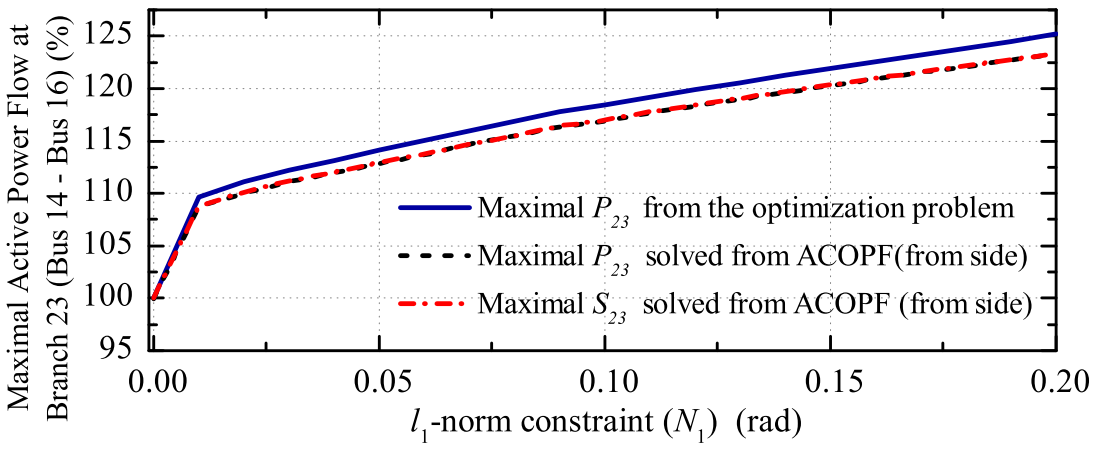

Figure 3.7: Comparison of DC optimization solution and AC maximal active/absolute power flow on target branch 23

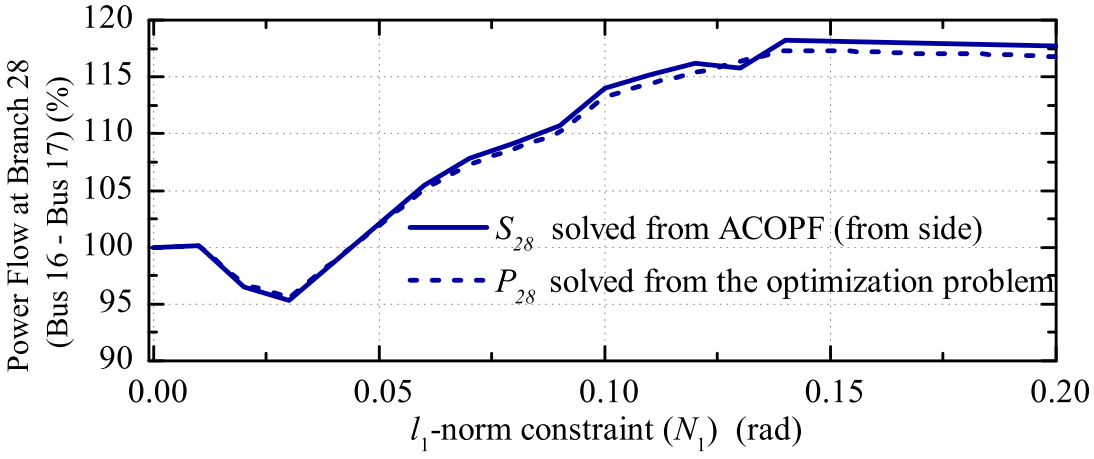

Figure 3.8: Power flow on branch 28

$N(0, 10^{-4})$ and the χ^2 detector threshold τ is set to be 167.52 with 95% confidence of detection rate. During the simulation, we assume the physical load is static. Note that, to make the system congested, all ratings of the branches has been decreased by 50%. Since there is no reactive power in DCOPF, the decrease of rating can not guarantee ACOPF converge. Thus, in order to compare AC and DC attack, certain ratings of branches in ACOPF have to be relaxed manually. Similar to what we did in Sec. 3.3, we solve the optimization problem with target branch 23, for $L_S = 20\%$. The

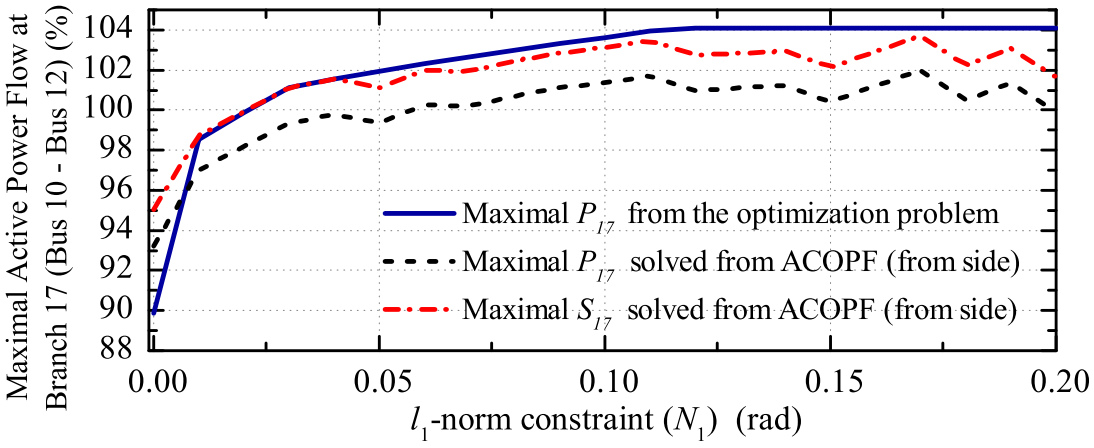

Figure 3.9: Comparison of DC Optimization Solution and AC Maximal Active/Absolute Power Flow on Target Branch 17

detail solutions from the DC optimization problem are summarized in Table A.1. Fig. 3.7 compares the maximal power flow on target branch 23 solved by the optimization problem and the physical power flow after attack with the AC attack and system model. In this scenario, the rating of branch 10 (bus 6 – bus 10) has been relaxed to 150 MVA. Note that in the absent of the attack, i.e., $N_1 = 0$, the power flow for AC and DC OPFs result in sightly different power flow, however, as the attacker size is increased, the power flows closely track each other. Since branch 23 mainly delivers active power, the absolute power flow curve on it is almost overlapping with the curve of active power flow. Another interesting observation is that branch 28 is also overload even the attacker does not target on it, as shown in Fig. 3.8. Since branch 28 is connected with branch 23 and is also congested prior attack, the optimization problem tends to include it in the attack subgraph; therefore, once the line flow on the cyber level seems less than the actual line power, the OPF will dispatch branch 28 to deliver more power.

Fig. 3.9 shows other attack scenarios with target branch 17 and $L_S = 30\%$. The detail solutions from the DC optimization problem are summarized in Table A.2. In

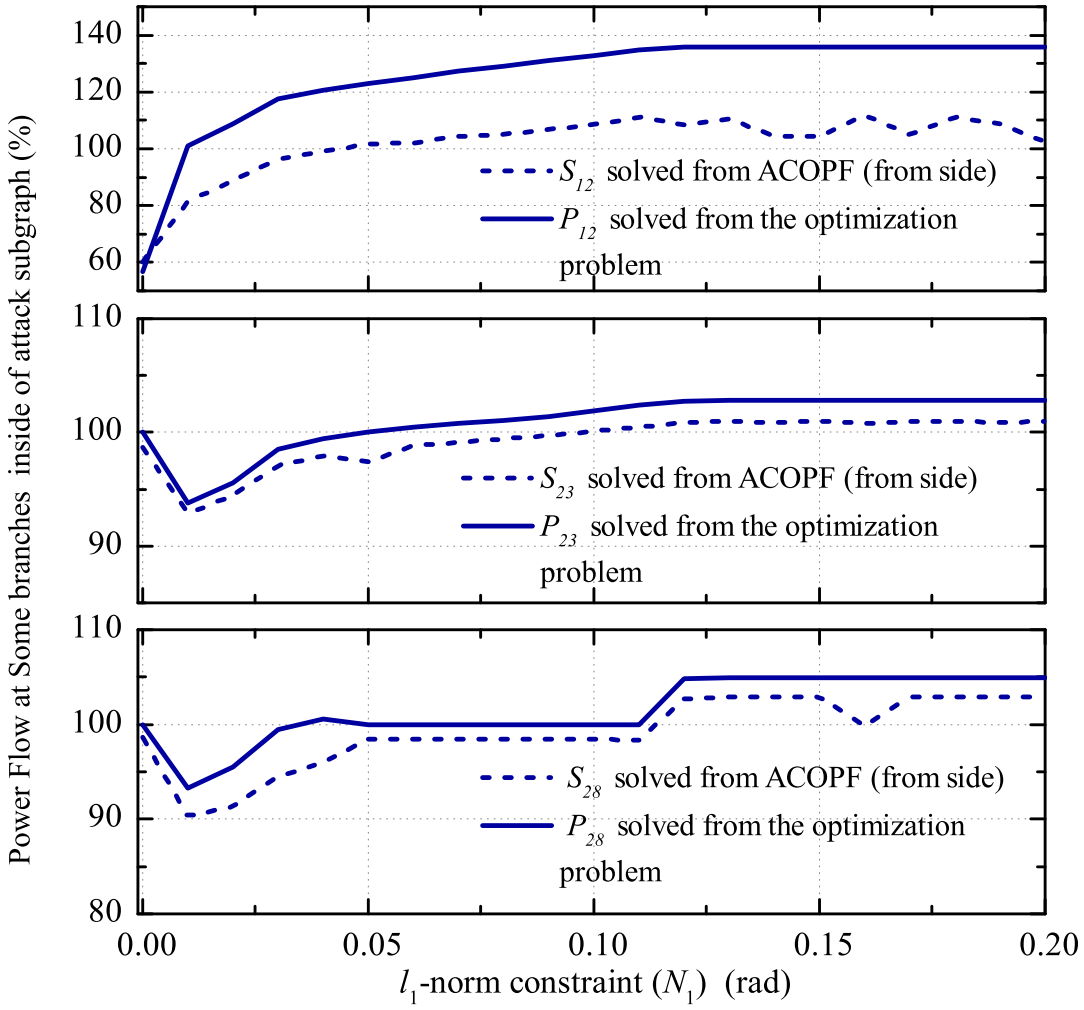

Figure 3.10: Power flow on branch 12, 23, and 28

this scenario, the rating of branch 10 (bus 6–bus 10) has been relaxed to 145 MVA. In this case, the power flow for AC and DC power flows still track each other closely. In particularly, this attack scenario generates three extra overloaded branches, branch 12, 23, and 28, as shown in Fig. 3.10. Branch 23 and 28 are overloaded because of the prior-to-attack congestion; a little generation dispatch change may cause the power flow fluctuates on these branches. Branch 12, however, is caused by the generation decrease on bus 7, as shown in Fig, 3.11. Therefore, in order to meet load demand on

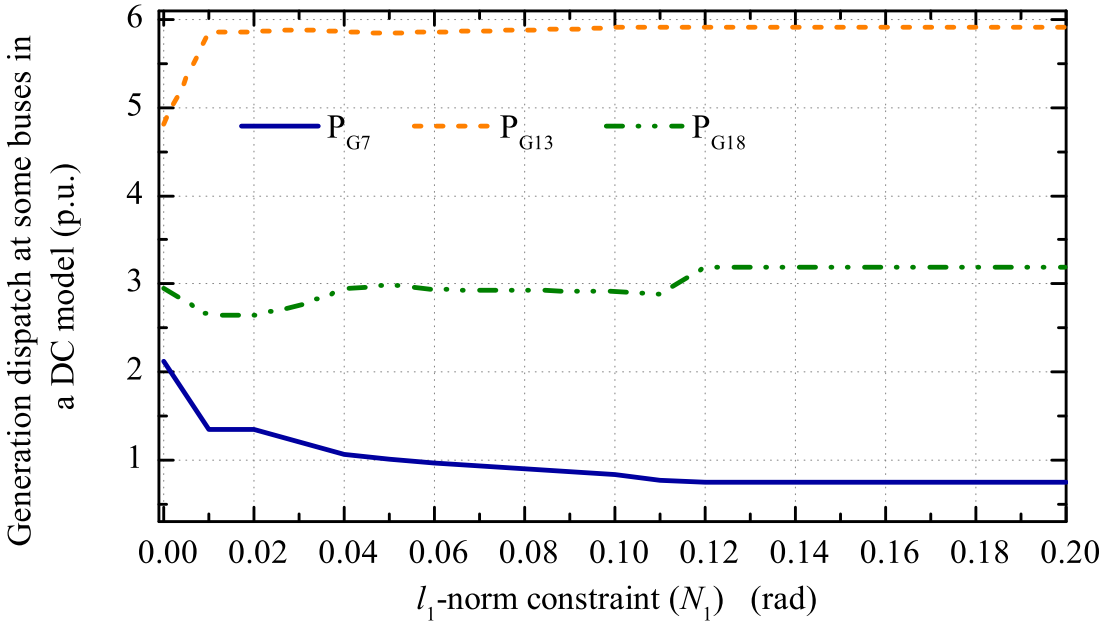

Figure 3.11: Generation dispatch v.s l_1-norm constraint

bus 7 and 8, branch 12 and 13 are dispatched to deliver a lot of power which finally result in a overload on branch 12.

Chapter 4

CONCLUSIONS AND FUTURE WORK

4.1 Conclusions

The topics of this thesis are two-fold. First, an attack framework was introduced in which the attacker matches the non-linear AC system characteristics by implementing local AC state estimation to a small number of measurements. Secondly, a linear optimization problem was formulated for the worst-case line overload attack. Numerical simulation was performed to test the attack on IEEE-RTS-24-bus system.

It is showed that, with limited resources and changes, the attacker is able to create branch overload by manipulating the generation dispatch. By exhaustively searching for all worst-case attack scenarios with different target branches, we found that, aside from the size of the attack subgraph, the constraint that an attack not cause significant observed load shift at the control center significantly impacts the attacker's ability to overload a branch. Still, there exists attacks with mild load shift that cause overloads.

Also, we find out the congested or nearly congested lines are most vulnerable to this type of attack. In reality, operating with congestion is desired: it represents the system is operating efficiently and transmission capacity is fully used. These lines deliver a large a mount of power prior to attack, suggesting these lines are the critical for the system and they are the most efficient path to deliver power. Thus, the attackers will favor congested lines and target on them.

4.2 Future Work

As discussed in the last part of the simulation result, this work can be extended by modifying the optimization problem. For instance, the attacker can change the objective correspondingly to fit her desire like maximize the system operation cost, etc. Another possible modification is to use false system configuration. Similar to

[18], the (2.2) becomes:

$$z_i^{(a)} = \begin{cases} z_i & \text{if } i \notin \mathcal{I}_{\mathcal{S}} \\ h_i^{(a)}(x+c) & \text{if } i \in \mathcal{I}_{\mathcal{S}} \end{cases} \tag{4.1}$$

where $h^a(.)$ is a false measurement model of the attacker's choice. In [18], the state-preserving attack is in fact following (4.1) with $c = 0$:

$$z_i^{(a)} = \begin{cases} z_i & \text{if } i \notin \mathcal{I}_{\mathcal{S}} \\ h_i^{(a)}(x) & \text{if } i \in \mathcal{I}_{\mathcal{S}}. \end{cases} \tag{4.2}$$

Extensions also include attacks targeted to overload multiple lines; this was an inadvertent side effect of our attacks, but a more targeted effort may cause more extreme damage or even cascading outages.

Additionally, the linear optimization problem may be extended to a more accurate non-linear problem.

Finally, using accurate load statistics to detect abnormal load patterns caused by FDI attacks could further restrict the space of undetectable attacks.

REFERENCES

[1] The Center for the Study of the Presidency and Congress, "Secure the U.S. electric grid," Oct 2014. 1.1

[2] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the United States and Canada: Causes and recommendations," 2004. 1.1

[3] M. Donolo, A. Guzman, V. Mynam, and D. Salmon, "Mitigating the aurora vulnerability with existing technology," 2009. 1.1

[4] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," 2010. 1.1

[5] A. Anwar and A. N. Mahmood, "Vulnerabilities of smart grid state estimation against false data injection attack," *CoRR*, 2014. 1.1

[6] A. Anwar and A. N. Mahmood, "Cyber security of smart grid infrastructure," *CoRR*, 2014. 1.1

[7] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *in Proc. 16th ACM Conference on Computer and Communication Security*, pp. 21–32, 2009. 1.1, 1.3, 1.3, 1.3, 2.3

[8] A. Abur and A. G. Expósito, *Power system state estimation: theory and implementation*. CRC, 2000. 1.2.3, 1.2.4, 1.2.4

[9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst.*, 2010. 1.4

[10] G. Dan and H. Sandberg, "Steath attacks and protection shcemes for state estimators in power systems," in *Proc. 1st IEEE SmartGrid Comm.*, 2010. 1.4

[11] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference onw*, pp. 220–225, Oct 2010. 1.4

[12] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grids," *IEEE Transactions on Smart Grid*, vol. 2, pp. 645–658, 2011. 1.4

[13] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *Power Systems, IEEE Transactions on*, vol. 19, pp. 905–912, May 2004. 1.4, 3.2

[14] Y. Wang and R. Baldick, "Interdiction analysis of electric grids combining cascading outage and medium-term impacts," *Power Systems, IEEE Transactions on*, vol. 29, pp. 2160–2168, Sept 2014. 1.4

[15] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *Smart Grid, IEEE Transactions on*, vol. 2, pp. 382–390, June 2011. 1.4, 3.2

[16] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, pp. 1731–1738, Sept 2012. 1.4

[17] A. Giani, R. Bent, M. Hinrichs, M. McQueen, and K. Poolla, "Metrics for assessment of smart grid data integrity attacks," in *Power and Energy Society General Meeting, 2012 IEEE*, pp. 1–8, July 2012. 1.4

[18] J. Kim and L. Tong, "On topology attack of a smart grid: undetectable attacks and countermeasures," *Selected Areas in Communications, IEEE Journal on*, vol. 31, pp. 1294–1305, July 2013. 1.4, 4.2, 4.2

[19] G. Hug and J. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012. 1.4, 1.5, 2.2

[20] K. Davis, K. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pp. 342–347, Nov 2012. 1.4

[21] M. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *Power and Energy Society General Meeting (PES), 2013 IEEE*, pp. 1–5, July 2013. 1.4

[22] J. Liang, O. Kosut, and L. Sankar, "Cyber attack on AC state estimation: Unobservability and physical consequences," in *Power and Energy Society General Meeting, 2014 IEEE*, July 2014. 1.4, 2.1

[23] S. Bi and Y. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pp. 1162–1167, Dec 2011. 1.4

[24] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *Control of Network Systems, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2014. 1.4

[25] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *Smart Grid, IEEE Transactions on*, vol. 5, pp. 612–621, March 2014. 1.4

[26] L. V. Stephen Boyd, *Convex Optimization*. Cambridge University Press, 2004. 3.2

[27] J. Fortuny-Amat and B. McCarl, "A representation and economic interpretation of a two-level programming problem," *The Journal of the Operational Research Society*, vol. 32, no. 9, pp. pp. 783–792, 1981. 3.2

APPENDIX A

SOLUTION TABLES FOR THE OPTIMIZARIONB PROBLEM

Table A.1: Table of Attack Vector c: Target Branch 23, $L_S = 20\%$ (rad), $\gamma = 0.038$

c \ N_1	0.01	0.02	0.03	0.04	0.05	0.06	0.07
c_1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_6	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_8	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_9	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0011
c_{10}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0016
c_{11}	0.0033	0.0025	0.0019	0.0013	0.0008	0.0003	0.0005
c_{12}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0006
c_{13}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{14}	0.0095	0.0071	0.0053	0.0038	0.0023	0.0008	0.0000
c_{15}	-0.0004	-0.0092	-0.0114	-0.0147	-0.0179	-0.0211	-0.0234
c_{16}	0.0001	-0.0036	-0.0065	-0.0090	-0.0114	-0.0139	-0.0155
c_{17}	0.0000	-0.0014	-0.0035	-0.0081	-0.0127	-0.0174	-0.0206

c_{18}	0.0000	0.0000	-0.0016	-0.0075	-0.0133	-0.0192	-0.0232
c_{19}	0.0000	-0.0001	-0.0051	-0.0051	-0.0051	-0.0051	-0.0052
c_{20}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{21}	-0.0001	-0.0031	-0.0050	-0.0099	-0.0148	-0.0197	-0.0231
c_{22}	-0.0001	-0.0024	-0.0044	-0.0092	-0.0140	-0.0188	-0.0221
c_{23}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0001
c_{24}	-0.0002	-0.0057	-0.0071	-0.0091	-0.0111	-0.0131	-0.0144
c \ N_1	0.08	0.09	0.1	0.11	0.12	0.13	0.14
c_1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_6	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_8	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_9	0.0065	0.0085	0.0081	0.0083	0.0082	0.0080	0.0079
c_{10}	0.0017	0.0044	0.0018	0.0044	0.0045	0.0046	0.0046
c_{11}	0.0014	0.0022	0.0010	0.0013	0.0009	0.0005	0.0001
c_{12}	0.0018	0.0028	0.0022	0.0027	0.0025	0.0024	0.0022

c_{13}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{14}	0.0000	-0.0002	-0.0020	-0.0025	-0.0036	-0.0047	-0.0059
c_{15}	-0.0246	-0.0260	-0.0291	-0.0307	-0.0326	-0.0346	-0.0365
c_{16}	-0.0164	-0.0174	-0.0199	-0.0212	-0.0230	-0.0247	-0.0265
c_{17}	-0.0224	-0.0244	-0.0289	-0.0310	-0.0335	-0.0359	-0.0383
c_{18}	-0.0254	-0.0280	-0.0337	-0.0362	-0.0390	-0.0418	-0.0446
c_{19}	-0.0054	-0.0055	-0.0054	-0.0062	-0.0076	-0.0090	-0.0104
c_{20}	0.0000	0.0000	0.0000	-0.0005	-0.0015	-0.0026	-0.0037
c_{21}	-0.0250	-0.0272	-0.0320	-0.0342	-0.0367	-0.0392	-0.0417
c_{22}	-0.0240	-0.0261	-0.0308	-0.0329	-0.0354	-0.0379	-0.0404
c_{23}	0.0002	0.0003	0.0002	-0.0001	-0.0010	-0.0019	-0.0028
c_{24}	-0.0152	-0.0160	-0.0180	-0.0190	-0.0202	-0.0214	-0.0225

c \ N_1	0.15	0.16	0.17	0.18	0.19	0.2
c_1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_6	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

c_8	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_9	0.0077	0.0075	0.0073	0.0072	0.0070	0.0068
c_{10}	0.0046	0.0047	0.0047	0.0047	0.0048	0.0048
c_{11}	-0.0003	-0.0007	-0.0011	-0.0015	-0.0019	-0.0023
c_{12}	0.0019	0.0016	0.0013	0.0009	0.0006	0.0003
c_{13}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{14}	-0.0070	-0.0080	-0.0091	-0.0102	-0.0113	-0.0124
c_{15}	-0.0380	-0.0396	-0.0412	-0.0427	-0.0443	-0.0458
c_{16}	-0.0283	-0.0300	-0.0317	-0.0334	-0.0351	-0.0368
c_{17}	-0.0400	-0.0417	-0.0433	-0.0450	-0.0466	-0.0483
c_{18}	-0.0463	-0.0479	-0.0495	-0.0512	-0.0528	-0.0544
c_{19}	-0.0127	-0.0151	-0.0174	-0.0198	-0.0222	-0.0245
c_{20}	-0.0054	-0.0072	-0.0090	-0.0108	-0.0126	-0.0144
c_{21}	-0.0433	-0.0449	-0.0465	-0.0481	-0.0497	-0.0513
c_{22}	-0.0420	-0.0436	-0.0452	-0.0469	-0.0485	-0.0501
c_{23}	-0.0042	-0.0057	-0.0072	-0.0086	-0.0101	-0.0116
c_{24}	-0.0235	-0.0245	-0.0254	-0.0264	-0.0274	-0.0283

Table A.2: Table of Attack Vector c: Target Branch 17, $L_S = 30\%$ (rad), $\gamma = 0.016$

c \ N_1	0.01	0.02	0.03	0.04	0.05	0.06	0.07
c_1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_6	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0003
c_7	0.0000	0.0000	0.0000	0.0066	0.0136	0.0199	0.0259
c_8	0.0013	0.0128	0.0169	0.0207	0.0248	0.0286	0.0322
c_9	0.0000	0.0000	-0.0085	-0.0089	-0.0083	-0.0077	-0.0072
c_{10}	0.0027	0.0029	0.0032	0.0032	0.0033	0.0034	0.0037
c_{11}	-0.0012	-0.0005	-0.0009	-0.0010	-0.0009	-0.0006	-0.0003
c_{12}	0.0006	0.0006	-0.0012	-0.0012	-0.0011	-0.0010	-0.0008
c_{13}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{14}	-0.0049	-0.0028	0.0000	0.0000	0.0000	0.0004	0.0008
c_{15}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{16}	0.0011	0.0015	0.0014	0.0006	0.0000	0.0000	0.0000
c_{17}	0.0004	0.0005	0.0005	0.0002	0.0000	0.0000	0.0000

c_{18}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{19}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{20}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{21}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{22}	0.0002	0.0002	0.0002	0.0001	0.0000	0.0000	0.0000
c_{23}	0.0001	0.0001	-0.0001	-0.0001	-0.0001	-0.0001	-0.0001
c_{24}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c \ N_1	0.08	0.09	0.1	0.11	0.12	0.13	0.14
c_1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_6	0.0012	0.0020	0.0028	0.0035	0.0040	0.0040	0.0040
c_7	0.0311	0.0363	0.0416	0.0469	0.0494	0.0494	0.0494
c_8	0.0355	0.0388	0.0421	0.0454	0.0470	0.0470	0.0470
c_9	-0.0066	-0.0060	-0.0054	-0.0048	-0.0045	-0.0045	-0.0045
c_{10}	0.0046	0.0055	0.0063	0.0071	0.0076	0.0076	0.0076
c_{11}	0.0000	0.0004	0.0008	0.0012	0.0015	0.0015	0.0015
c_{12}	-0.0004	-0.0001	0.0002	0.0005	0.0007	0.0007	0.0007

c_{13}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{14}	0.0010	0.0013	0.0018	0.0023	0.0027	0.0027	0.0027
c_{15}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{16}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{17}	0.0000	0.0000	0.0000	0.0000	-0.0031	-0.0032	-0.0032
c_{18}	0.0000	0.0000	0.0000	0.0000	-0.0048	-0.0049	-0.0049
c_{19}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{20}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{21}	0.0000	0.0000	0.0000	0.0000	-0.0032	-0.0032	-0.0032
c_{22}	0.0000	0.0000	0.0000	0.0000	-0.0031	-0.0032	-0.0032
c_{23}	0.0000	0.0000	0.0000	0.0000	0.0001	0.0001	0.0001
c_{24}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

c \ N_1	0.15	0.16	0.17	0.18	0.19	0.2
c_1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_5	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_6	0.0040	0.0040	0.0040	0.0040	0.0040	0.0040
c_7	0.0494	0.0494	0.0494	0.0494	0.0494	0.0494

c_8	0.0470	0.0470	0.0470	0.0470	0.0470	0.0470
c_9	-0.0045	-0.0045	-0.0045	-0.0045	-0.0045	-0.0045
c_{10}	0.0076	0.0076	0.0076	0.0076	0.0076	0.0076
c_{11}	0.0015	0.0015	0.0015	0.0015	0.0015	0.0015
c_{12}	0.0007	0.0007	0.0007	0.0007	0.0007	0.0007
c_{13}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{14}	0.0027	0.0027	0.0027	0.0027	0.0027	0.0027
c_{15}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{16}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{17}	-0.0032	-0.0032	-0.0032	-0.0032	-0.0032	-0.0032
c_{18}	-0.0049	-0.0049	-0.0049	-0.0049	-0.0049	-0.0049
c_{19}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{20}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
c_{21}	-0.0032	-0.0032	-0.0032	-0.0032	-0.0032	-0.0032
c_{22}	-0.0032	-0.0032	-0.0032	-0.0032	-0.0032	-0.0032
c_{23}	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001
c_{24}	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000