國 立 交 通 大 學

電信工程研究所

碩 士 論 文

智慧電網狀態估計之匿蹤攻擊與防護

Counter Counter-Measures against Stealth Attacks on State Estimation in Smart Grids

研 究 生：韓松俯

指導教授：蘇育德 教授

中 華 民 國 一〇二 年 七 月

智慧電網狀態估計之匿蹤攻擊與防護

Counter Counter-Measures against Stealth Attacks on State Estimation in Smart Grids

研究生：韓松俯　　Student：Sung-Fu Han

指導教授：蘇育德　　Advisor：Dr. Yu T. Su

國立交通大學
電信工程研究所
碩士論文

A Thesis

Submitted to the Institute of Communications Engineering

College of Electrical and Computer Engineering

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Communications Engineering

July 2013
Hsinchu, Taiwan, Republic of China

中華民國一Ｏ二年七月

智慧電網狀態估計之匿蹤攻擊與防護

學生：韓松俯　　　　　　　　　　　　　　　指導教授：蘇育德 博士

國立交通大學電信工程研究所碩士班

摘　　要

從傳統電力網路(Power Grid，以下簡稱電網)結合先進的通訊網路而演進到智慧電網(Smart Grid)後，電網內各設施的資訊不再經由獨立隔絕的電網電路或人力的方式而是透過公共的通訊網路傳送，資訊安全因此變得十分重要。目前最受矚目的資安議題之一便是針對電網狀態估計(State Estimation)的所謂假數據攻擊(False Data Injection Attack, FDIA)。只要攻擊者有電網結構的資訊又能夠及時串改部分電表的測量值，就可通過錯誤資訊判斷機制(Bad Data Detection)使得電力公司之控制中心估計出錯誤的狀態(States)致使能源管理系統(EMS)用這些錯誤狀態做出不正確的電力調整或控制決策。FDIA 若能通過 BDD 測試而不為 EMS 察覺，則稱為匿蹤攻擊。

這種匿蹤攻擊可以透過保護一定數量的電表或測量值來防止。但通常需保護的量測值相當龐大，費用很高，施工期也長。本文研究的重點即在電網管控單位因種種原因無法及時保護足夠數量之電表量測，而只能保護一定量的測量值的前提下去設計一保護電表選擇的策略以最大化攻擊者之成本(需竄改的測量值數量)提高此惡意攻擊之困難度。易言之，對這種攻擊測量值(counter-measures, CM)與保護測量值(counter counter-measures, CCM)間的賽局(game)，我們採取的是 max-min 策略，即迫使攻擊方提高(最大化)所需付出的最小代價，而其代價則以所需竄改(攻擊)的測量值(電表)數量為準。但若就防禦方（電網管理者）而言，其風險則反比於攻擊方之代價，即攻擊者所要竄改的量越少管理的風險越高。如此來說，我們的策略就變成 min-max 的形式，試圖盡量降低最大的可能風險。

由於要一次選出大量的保護值複雜度很高，我們的 max-min 解是一個逐步(incremental)選擇保護電表演算法。這個方法與每個電表的安全指數(SI)有關，SI 是指連帶竄改電表的數量，亦即 FDIA 為了要竄改某一測量值且通過錯誤資訊判斷機制所必須連帶竄改的最少電表數量。SI 的計算可透過將電網結構視為某種圖形而考慮電表在圖中之最小切法(minimum cut)而得。保護安全指數最低的電表便可迫使攻擊者尋找其他攻擊成本(即 SI)更高的攻擊方式。然因常有多個電表的安全指數同為最小的情況，我們進一步利用每個電表會通過多條最小切法的現象，發展出一套有效決定電表保護優先順序的演算法。

我們先探討攻擊者選擇攻擊對象的最佳化(即竄改最少電表而能達成目的)問題，將其從 NP hard，在無入射式電表電網(injection-free grids)中，簡化成多項式時間(polynomial time)即可解的等效問題。對一般有入射式電表(injection meter)之電網，我們先排除入射電表來決定保護策略再將其列入考慮以決定須保護之額外電表。但即使沒有額外之電表保護我們也可證明在無入射式電表的假設下所設計之保護策略也可保證攻擊者實際將付出更高之代價。易言之，我們的保護策略所估計之攻擊代價雖未將入射電表列入考慮，但事實上 FDIA 所需攻擊之電表數量一定高於我們的估計值，因此我們的演算法保證的是最低的電網安全指數。根據數種 IEEE 標準電網模型所進行的電腦模擬也證明我們的演算法相對於其他方法有遠為優異的效能表現。

Counter Counter-Measures against Stealth Attacks on State Estimation in Smart Grids

Student : Sung-Fu Han Advisor : Yu T. Su

Institute of Communications Engineering

National Chiao Tung University

Abstract

Security is of paramount importance in upgrading a power grid into a smart grid in which various wired and wireless communication links are used for control, monitoring and sensing applications. One of the key security concerns that has drawn much research attention is the so-called false data injection attack (FDIA) against state estimation. With the knowledge of the grid topology and by injecting proper false data into selected meters, an FDIA can pass bad data detection (BDD) and become stealth to the grid's Supervisory Control and Data Acquisition (SCADA) system. The Energy Management System (EMS) uses the state estimates evaluated by polluted measurements reported by tampered meters to perform grid configuration will result in incorrect, unreliable operations and may even lead to disastrous consequences.

Such a counter-measures (CM) can be prevented if sufficient number of meters (links) are protected. Unfortunately, protection of a large number of meters can be very expensive and time-consuming. We therefore focus on the scenario in which the grid can only protect a selected set of measurements smaller than that required by a FDIA-free system. A scheme that maximizes the attacker's cost (i.e., the number of tampered meters required to form a stealth meter data vector) is desired. Such a design goal is equivalent to counter the counter-measure carried by an FDIA with a max-min approach. From the grid operator's viewpoint, however, its risk is inverse proportional to the cost of an attacker as the easier an attacker can launch an FDIA the higher the risk of a grid. Whence our method is also min-max, trying to minimize the risk of being attacked. Our solution involves the notion of security index (SI) of a meter which specifies the minimum number of tampered meters, other than the meter of concern, needed in generating a legitimate attack vector that corrupts a state estimation. The evaluation of a meter's SI is done by representing the grid by a grid and then find the so-called minimum cuts associated with the branch (meter) of interest.

As the task of locating multiple measurements for protection is computational expensive, we adopt an incremental approach which tries to find, in each iteration, the single candidate meter for protection that costs the attacker least. Finding and protecting the most vulnerable meter (i.e., the one with the smallest SI) forces the attacker to tamper meters with higher SI in order to generate a legitimate false measurement thereby paying a higher cost. As oftentimes there are multiple meters with the same SI and a meter is involved with many minimum cuts of the equivalent grid graph that link other meters, we develop further criteria to select the protected (most vulnerable) meter.

Our approach transforms an NP-hard problem of optimizing a successful FDIA into one that can be solved in polynomial-time for injection-free grids. We thus starts with injection-free grids and then extends to the full-measurement and other practical grids. We show that our injection-free solution gives a low-bound on the number of meters any FDIA has to tamper with. Computer simulations based on some IEEE standard grids are performed to examine the efficiencies of our approaches and verify the numerical advantages with respect to other known methods.

誌謝

對於論文得以順利完成，首先感謝指導教授 蘇育德博士。老師的諄諄教誨使我對於通訊領域的研究有更深入的了解，也教導我們許多書上學不到的知識與人生道理，讓我受益良多。並感謝口試委員蘇賜麟教授、楊谷章教授、李大嵩教授及呂忠津教授給予的許多寶貴意見，以補足這份論文的缺失與不足之處。

由衷感謝實驗室的張致遠學長，於研究與人生等多方面的協助、建議與討論，使研究能夠順利完成，相處過程中寶貴回憶與恩惠將銘刻於心。感謝實驗室中的學長姐、同學、及學弟妹們，這兩年內的互相支持與鼓勵。

最後感謝我的家人及朋友，總是在背後默默的關心與支持，使我有動力可以努力向前進，在此僅獻上此論文，以代表我最深的敬意。

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

A smart grid is built on and upgraded from a traditional power grid with the help of advanced wireless technologies such as LTE-A and WiMAX to support machine to machine (M2M) communications amongst power meters and other grid devices. A smart grid is thus able to allow the grid operator to monitor the network status near real-time, and makes applications such as energy routing, network security assessment being performed more efficiently and intelligently.

The main purpose of the network's supervisory control and data acquisition (SCADA) system is tracing the current grid status by measurement collected from meters installed over the network. The meters report measurements to SCADA through wireless or wired links. The state estimated by SCADA are then used for, among others, anomaly detection and network energy management which includes automatic generation control (GSC), optimal flow analysis, and contingency analysis (CA).

The communication infrastructure brings a power grid from an isolated network into the public network in order to facilitate new innovative applications. However, such a move also exposes the power grid to many cyber threats. For example, attackers can tamper with meters remotely for energy theft purpose or to confuse the grid management by biasing state estimates. In fact, it has been reported in [28] that the attacks targeting at SCADA system already exist. Recent study by Liu *et al.* [3] pointed out that an attacker can launch a false data injection attack (FDIA) causing incorrect state estimates without triggering bad data detection (BDD) [17]-[21] if it has the complete knowledge of the network topology. Huang *et al.* [16] demonstrated that attackers can extract information of network topology from the correlations among power flow measurements. Intentionally-biased state estimates may mislead the energy routing process [4], result in the wrong operations which may cause very serious consequences such as the disastrous blackout of the U.S. in 2003 [29].

The problem of countering the counter-measure (CM) initiated by an FDIA can be solved from two perspectives, namely, protecting key measurements (meters) and developing new state estimation schemes which are immune to FDIAs. The first approach, which has been intensively investigated, selects a set of measurements for protection so that the attacker cannot inject false data into these measurements. Bobba *et al.* [5] defined the basic measurements as the set containing the minimum number of measurements needed to ensure observability of the network. Bi and Zhang [6] considered the scenario of preventing critical state variables being biased and proved the necessary and sufficient rank condition to select the protection measurements. They found the required minimum number of protected measurements if the grid operator only want to prevent the critical state variable from being shifted. In [7], Kim *et al.* proposed a greedy algorithm to select a protected measurement set and presented an unified attack formulation. Zhao *et al.* [10] include phasor measurement units (PMUs) in the attack problem, and show that, for any set of PMUs in place, the existence of an unobservable attack that is restricted to any given subset of the buses can be determined with probability one based solely on the network topology.

The second approach requires a new state estimation scheme which is insensitive to not only nature errors but also human-injected malicious errors. Talebi *et al.* [11] introduced the full rank condition based on the dynamic information structure to mislead the attackers and force attack vector to be zero. Tajer *et al.* [12] addressed the issue of attack detection and state recovery using distributed state estimation methods.

Recently, Sandberg *et al.* [13] introduced two security indices that quantify the least effort needed to achieve an attack goal without triggering BDD. It was later extended [9] to illustrate the communication infrastructure of routing measurements and security metrics that quantify the importance of individual substations and the cost of attacking individual measurements.

In a large and changing grid, it is difficult to protect the set of basic measurements simultaneously. A more practical approach for the grid operator would be to place critical measurement protections sequentially. The priority of protected measurements is thus of major concern. Before all essential measurements are protected, it is possible that the network suffers from FDIA. Our goal is to select a sequence of monotonic increasing subsets of measurements such that, for a given protection subset size, the selected subset forces an FDIA attacker to tamper the maximum number of unprotected measurements.

We formulate the problem of optimal attack in terms of the security index and prove that this problem is equivalent to that of [7]. Both the proposed attack problem and that of [7] are generally NP-hard. However, when the operator use only branch measurements to estimate states and an FDIA tampers branch meters only, the optimal attack problem has a polynomial time algorithm to derive the solution. In other words, the attacker problem of [7] has a polynomial time optimal solution for this special case. The algorithm in [7] requires that the attack information is available. The approach of [7] replaces the zero-norm by ℓ_1-norm to search for suboptimal choices of meters for protection while we are able to find the optimal zero-norm solution for injection-free networks and provide the grid operator the information about an FDIA's best attacking strategy so that a proper counter-measure can be launched.

An incremental approach that selects the meters to be protected one by one with backward compatibility is adopted. In other words, in selecting a new meter for protection, it is assumed that all the current chosen meters remain under protection. The approach is of low complexity as the number feasible subsets of meters is often extremely large. More importantly, we verify through simulation that the proposed incremental approach provides near-optimal performance. In particular, for the IEEE 14 network, the optimal result is achieved.

The proposed counter counter-measure (CCM) algorithm considers only injection-free networks and protect the most vulnerable branch meter. Nevertheless, we show that this strategy guarantee better security for any practical power grid in the sense that any attacker has to tamper more meters to be successfully in evading the BDD test.

This thesis is organized as follows. In the ensuing chapter, we introduce and formulate the state estimation problem and the FDIA in power grids. We also prove that hopping the reference bus cannot prevent an FDIA from passing BDD test, i.e., FDIA attackers do not have to know the reference bus index. In Chapter 3, we state the interaction between attackers and grid operator including the formal definition. We propose an incremental meter selection algorithm and give the associated simulation results in Chapter 4. Finally, we conclude our work in Chapter 5.

Chapter 2

Preliminaries

A smart grid is a combination of a conventional power grid, for example the one shown in Fig. 2.1, which connects generation plants, transmission and distribution net-

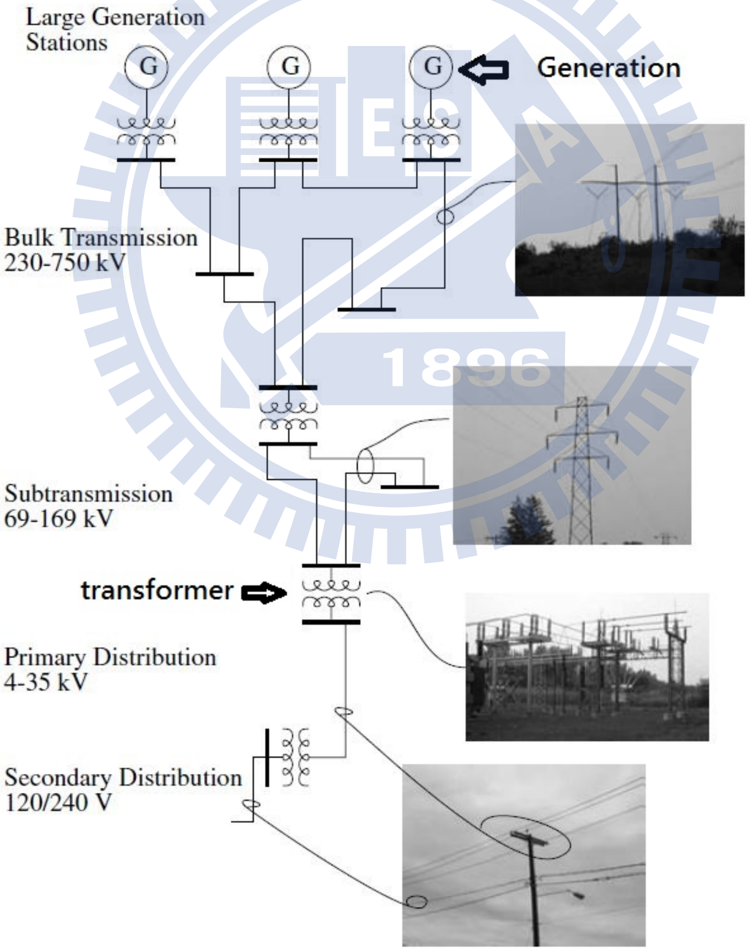

Figure 2.1: Overview of the electricity infrastructure [27].

works and the customers in a wide geographical region, and an advanced cellular network such as LTE and WIMAX supporting machine to machine (M2M) communications. The latter enables the establishment of an advanced metering infrastructure (AMI) which supports automatic measurement data reporting, two-way communications, demand response, and other new functions [1].

With the proliferation of world-wide research and implementation efforts, the scope of smart grid expands rapidly. Most research and development efforts focus on energy efficiency improvement, supply and demand balance and operation cost reduction [2]. Due to the availability of advanced communication technology, a grid operator can track the network status near real-time and perform more efficient and intelligent energy routing. In following sections, we describes in details how power system monitoring is carried out. In particular, we introduce the (network) state estimation problem and solution which is vital for power system monitoring. We also common criterion of the bad data detection (BDD) which is part of state estimation. Fig. 2.2 illustrates the complete process of system monitoring. Table 1 lists the notations and abbreviations used.

2.1 System Monitoring

The main issue of system monitoring is continuously tracing the current status of smart grid based on measurements reported from meters spreading over a wide geographical region for ensuring the reliability and stability of a smart grid and avoiding disruption. The meter placements depend on the grid's strategy and budget. The contents of measurements commonly involve voltages of buses, real and reactive power injections at buses, and real and reactive power flows along branches. The overall process of system monitoring is illustrated as follow step by step:

1. The supervisory control and data acquisition (SCSDA) system in control center obtains measurements from remote terminal units (RTUs) located at substations,

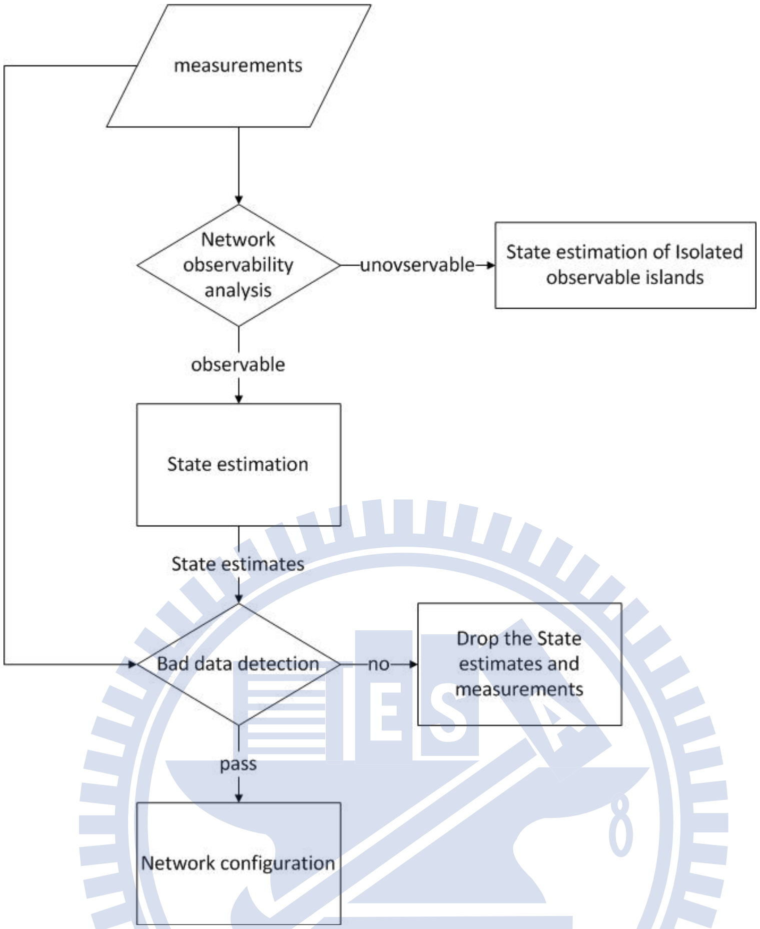
measurements
Network observability analysis
unovservable
State estimation of Isolated observable islands
observable
State estimation
State estimates
Bad data detection
no
Drop the State estimates and measurements
pass
Network configuration

Figure 2.2: Overview of system monitoring.

which gather the information of local meters.

2. The measurements are then passed to state estimator, and it will filter the faulty data by bad data detection and calculate the optimal state estimates.

3. The energy management system (EMS) use the states estimates to control the grid operations such as contingency analysis, optimal power flow and automatic generation control.

2.2 State Estimation

State estimation [23][24][26], part of system monitoring, is the process using measurements to best estimate the smart grid status. The estimates are state variables including bus voltage magnitudes and angles. In this thesis, we consider steady-state DC power system with $n+1$ buses, where one of buses is set to reference bus and the rest n buses are with n unknown state variables. We assume the bus voltage magnitudes are given, and the state variable of each bus i is simply a bus voltage angle denoted as x_i, $i = 1, ..., n$. There are m measurements consisting of the measurements of real power flows along branches and the measurements of real injections at buses. Each measurement is denoted as z_i, $i = 1, ..., m$. Note that, in DC power flow model, we don't consider reactive power flows and injections.

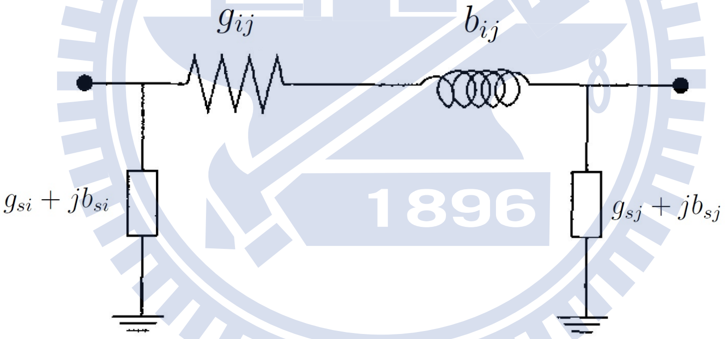

Figure 2.3: Two-port $\pi-$model of a branch [26]

According to the two-port π-model shown in Fig. 2.3 [26], the real power flow from bus i to bus j is given by

$$P_{i,j} = V_i^2(g_{si} + g_{ij}) - V_iV_j(g_{ij}\cos(x_i - x_j) + b_{ij}\sin(x_i - x_j)), \tag{2.1}$$

and the real power injection at bus i is

$$P_i = V_i \sum_{j \in \mathcal{N}_i} V_j(G_{ij}\cos(x_i - x_j) + B_{ij}\sin(x_i - x_j)), \tag{2.2}$$

where V_i, x_i is bus voltage magnitude and angle at bus i, $G_{ij} + jB_{ij}$ is the ijth element of the complex bus admittance matrix, $g_{ij} + jb_{ij}$ is the admittance of the series branch between bus i and bus j, $g_{si} + jb_{si}$ is the admittance of the shunt branch linked at bus i, and $\mathcal{N}_i$ is the set of all buses linked to bus i.

We apply several assumptions for DC model:

- We ignore the shunt admittance.
- In steady-state DC power system, the phase angle difference $x_i - x_j$ is small, $\forall i, j$.
- The resistance of each branch is typically smaller than its reactance.
- There are no losses.

The simplified real power flow from bus i to bus j becomes

$$P^s_{i,j} = V_i V_j b_{ij}(x_i - x_j), \tag{2.3}$$

and the simplified real power injection at bus i becomes

$$P^s_i = V_i \sum_{j \in \mathcal{N}_i} V_j b_{ij}(x_i - x_j) = \sum_{j \in \mathcal{N}_i} P^s_{i,j}. \tag{2.4}$$

In the control center, we assume both bus voltage magnitudes and branch reactance are given or can be measured. According to (2.3) and (2.4), the linear equations between measurements $P^s_{i,j}$, P^s_i and bus voltage angles x_i are derived.

The DC state estimation can be formulated as matrix form as follow:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \tag{2.5}$$

where $\mathbf{x} = (x_1, x_2, ..., x_{n+1})^T$, $\mathbf{z} = (z_1, z_2, ..., z_m)^T$ is a measurement vector consisting of P^s_i and $P^s_{i,j}$, $\mathbf{e} = (e_1, e_2, ..., e_m)^T$ is a random measurement error vector with zero mean Gaussian Distribution, and $\mathbf{H}$ is a $m \times (n+1)$ Jacobian matrix derived from (2.3) and (2.4). In the matrix $\mathbf{H}$, the columns correspond to the measurements and the rows correspond to the state variables (buses).

It is typically that the number of measurements is greater than the number of state variables, i.e., $m > n$; thus, the state estimation problem is over determined equations.

We want to minimize the sum of the square errors with different weight w_i as the function of $\mathbf{x}$

$$\min_{\mathbf{x}} J(\mathbf{x}) = \sum_{i=1}^{m} w_i e_i^2 = \mathbf{e}^T \mathbf{R}^{-1} \mathbf{e} = (\mathbf{z} - \mathbf{H}\mathbf{x})^T \mathbf{R}^{-1} (\mathbf{z} - \mathbf{H}\mathbf{x}), \tag{2.6}$$

where $\mathbf{R}^{-1} = diag(w_1, w_2, ..., w_m)$.

We perform noise whitening and choose the weight $w_i = \sigma_i^{-2}, i = 1, ..., m$ so that $\mathbf{R}$ is covariance matrix of $\mathbf{e}$ and the one step solution of weighted least-square (WLS) problem above [25] is

$$\hat{\mathbf{x}}_{\mathrm{r}} = (\mathbf{H}_{\mathrm{r}}^T \mathbf{R}^{-1} \mathbf{H}_{\mathrm{r}})^{-1} \mathbf{H}_{\mathrm{r}}^T \mathbf{R}^{-1} \mathbf{z}, \tag{2.7}$$

where $\mathbf{H}_{\mathrm{r}}$ is derived by removing last column of $\mathbf{H}$ by assuming that last bus is reference bus. The state estimates $\mathbf{x}_{\mathrm{r}} = [\hat{\mathbf{x}}_{\mathrm{r}}^T \ 0]^T$ are then used to smart grid configuration. We assume the smart grid network is observable ($Rank(\mathbf{H}) = Rank(\mathbf{H}_{\mathrm{r}}) = n$), i.e., $\hat{\mathbf{x}}$ can be uniquely determined by (2.7). Note that the identical estimator can be proved using maximum likelihood criterion and minimum variance criterion under the the assumption that measurement errors are Gaussian distributed with zero mean [25].

We give two examples of a 5-bus power system to illustrate how to derive Jacobian matrix $\mathbf{H}$ and determine if the network is observable. Consider the 5-bus power network in Fig. 2.4. where we assume that the network operates in steady-state and calculate the Jacobian matrix of DC model. For simplification, without loss of generality, we assume all bus voltages V_i and all admittances $b_{i,j}$ be 1. For the first example in Fig. 2.5, the network contains two meters, one injection meter and one branch meter.

The measurements reported by those meters are as follow:

$$z_1 = P_2^s = \sum_{j \in \mathcal{N}_2 = \{1,4\}} (x_2 - x_j) = 2x_2 - x_1 - x_4 \tag{2.8}$$

$$z_2 = P_{1,2}^s = x_1 - x_2 \tag{2.9}$$

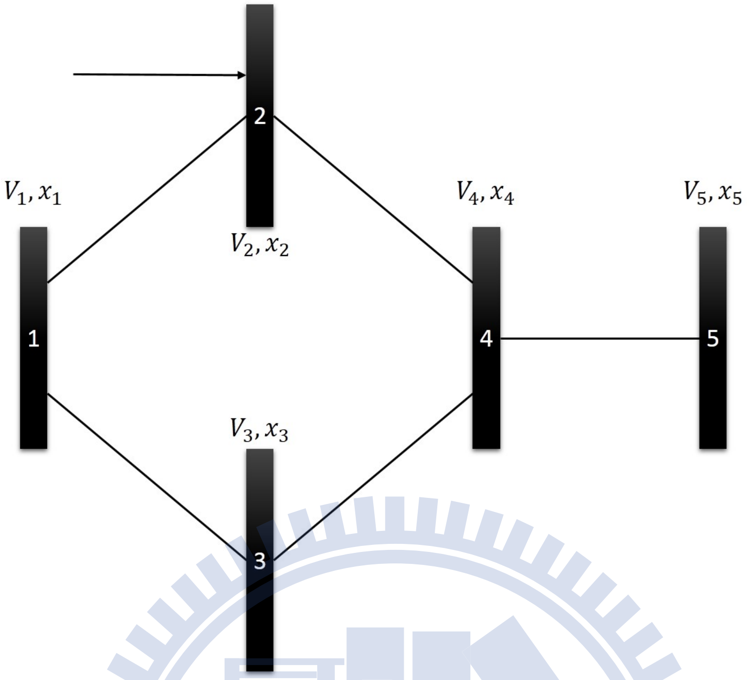

Figure 2.4: An example of 5-bus power network. Each bus owns a voltage V_i and a phase angle x_i.

The Jacobian matrix $\mathbf{H}_{\text{ex1}}$ can be derived from the DC model $\mathbf{z} = \mathbf{H}_{\text{ex1}}\mathbf{x} + \mathbf{e}$.

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} -1 & 2 & 0 & -1 & 0 \\ 1 & -1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} + \mathbf{e} \tag{2.10}$$

Using the last bus as the reference bus is equivalent to removing last column of $\mathbf{H}_{\text{ex1}}$ to get $\mathbf{H}_{\text{r,ex1}}$. Since $\mathbf{H}^T_{\text{r,ex1}}\mathbf{H}_{\text{r,ex1}}$ is not invertible, the state estimator can not to obtain an unique state estimate $\hat{\mathbf{x}}$. Therefore, we call the network configuration of Fig. 2.5 *unobservable*.

For the second example shown in Fig. 2.6, by following the same procedure above, we have

$$\mathbf{H}_{\text{ex2}} = \begin{bmatrix} -1 & 2 & 0 & -1 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix}, \mathbf{H}_{\text{r,ex2}} = \begin{bmatrix} -1 & 2 & 0 & -1 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2.11}$$

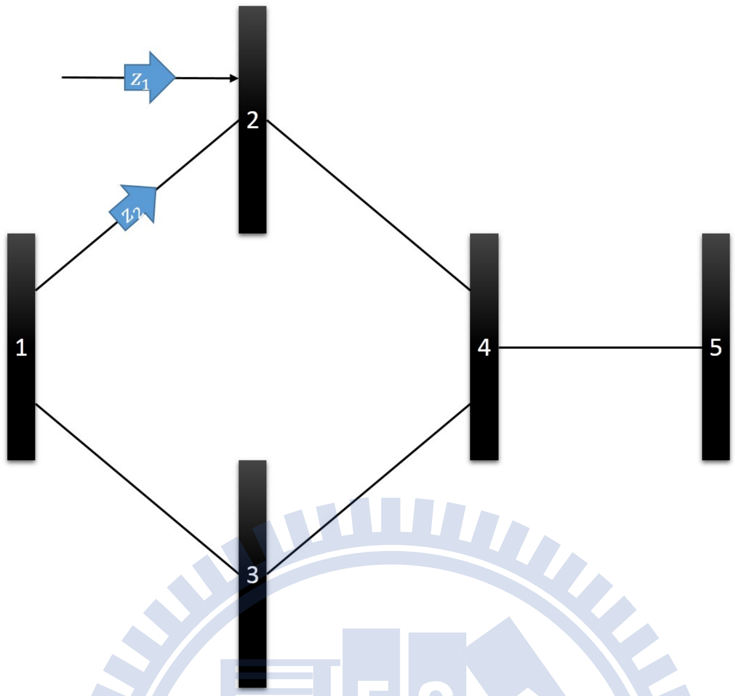

Figure 2.5: An unobservable example with two meters in the network.

Again, since $\mathbf{H}_{\mathrm{r,ex2}}^T\mathbf{H}_{\mathrm{r,ex2}}$ is invertible, there exists an unique state estimate. In other words, the network of Fig. 2.6 is *observable.*

Another way to define the Jacobian matrix is by using a graph model [14]. Regarding the buses in the network as as nodes and transmission lines as edges, we convert a power grid into a graph with n nodes and m_a edges. Note that m_a is the number of transmission lines and in general $m_a \neq m$. Define the incidence matrix $A \in \mathbb{R}^{n\times m_a}$ representing the graph (network) as

$$A(i,j) = \begin{cases} 1 & \text{if } j\text{th edge starts at } i\text{th node} \\ -1 & \text{if } j\text{th edge ends at } i\text{th node} \\ 0 & \text{otherwise} \end{cases} , \forall j = 1, \ldots, m_a. \tag{2.12}$$

Use the diagonal matrix $D \in \mathbb{R}^{m_a\times m_a}$ to describe the reactance of transmission lines whose diagonal entries are the reciprocal of the reactance of the edges. As a result, the Jacobian matrix $\mathbf{H}$ can now be expressed as

$$\mathbf{H} \triangleq \begin{bmatrix} P_1DA^T \\ -P_2DA^T \\ P_3ADA^T \end{bmatrix}_{m\times n+1} , m = 2m_a + n, \tag{2.13}$$

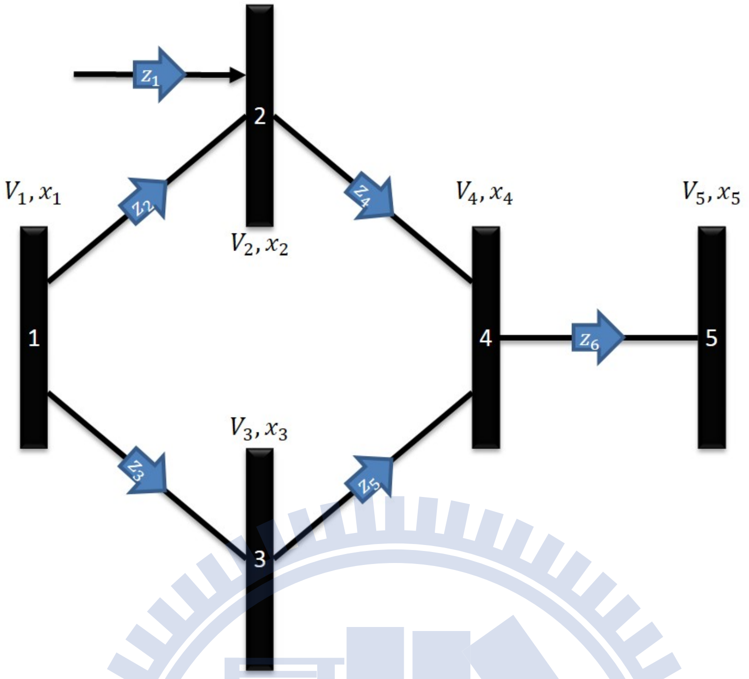

Figure 2.6: An observable example with six meters in the network.

where P_1, P_2 and P_3 consist of subsets of rows of identity matrices of proper dimensions, indicating which measurements are actually taken. The sub-matrix P_1DA^T represents the measurements putting on the same direction of the directed edge. Similarly, the sub-matrix $-P_2DA^T$ represents the measurements putting on opposite direction of the directed edge. The sub-matrix P_3ADA^T represents the injection measurements putting on the buses. In the rest of this paper, we use this representation of Jacobian matrix, and select measured meters by setting P_1, P_2 and P_3.

2.3 Bad Data Detection

The measurements sent by RTUs may incur distortions caused by random errors, malicious activities, and other faulty. To prevent the false state estimation, the state estimator uses BDD to check if the measurements is correct before computing the state estimates. Many works [17]-[21] have been reported regarding BDD. Liu *et al.* [3] found that these works actually use the same criterion to detect bad data. We define the residual r as

$$r = ||\mathbf{z} - \mathbf{H}\mathbf{x}||_2 = ||\mathbf{z} - \mathbf{H}_\mathrm{r}\mathbf{x}_\mathrm{r}||_2. \tag{2.14}$$

If $r > \tau$, then one declares that bad data is present, where τ is a predefined threshold.

2.4 False Data Injection Attacks

There are several ways to inject the false data [13], for examples, an attacker can

1. physically tamper with meters,
2. broadcasts strong jamming signal to take over the original measurement report, or
3. directly hacks into the SCADA system through possible routes.

The attack model [3] we consider in this thesis is

$$\mathbf{a} = \mathbf{H}_\mathrm{r}\mathbf{c}_\mathrm{r}, \tag{2.15}$$

where $\mathbf{a}$ is a $m \times 1$ attack vector and $\mathbf{c}_\mathrm{r}$ is a $n \times 1$ shift vector. Note that shift vector $\mathbf{c}_\mathrm{r}$ does not shift reference bus. The attacked measurements injected false data are

$$\mathbf{z}_\mathbf{a} = \mathbf{z} + \mathbf{a}. \tag{2.16}$$

It is shown by Liu *et al.* [3] that the attackers can pass BDD without being detected if they have the knowledge of network topology and can manipulate some measurements in the sense that the residual (2.14) doesn't change. The detail is shown as follow according to *Theorem 1* of [3]

$$\begin{aligned}
\|\mathbf{z}_\mathbf{a} - \mathbf{H}_\mathrm{r}\hat{\mathbf{x}}_{\mathrm{r,shift}}\|_2 &= \|\mathbf{z} + \mathbf{a} - \mathbf{H}_\mathrm{r}(\mathbf{H}_\mathrm{r}^T\mathbf{R}^{-1}\mathbf{H}_\mathrm{r})^{-1}\mathbf{H}_\mathrm{r}^T\mathbf{R}^{-1}(\mathbf{z} + \mathbf{a})\|_2 \\
&= \|\mathbf{z} + \mathbf{a} - \mathbf{H}_\mathrm{r}(\hat{\mathbf{x}}_\mathrm{r} + \mathbf{c}_\mathrm{r})\|_2 \\
&= \|\mathbf{z} - \mathbf{H}_\mathrm{r}\hat{\mathbf{x}}_\mathrm{r} + (\mathbf{a} - \mathbf{H}_\mathrm{r}\mathbf{c}_\mathrm{r})\|_2 \\
&= \|\mathbf{z} - \mathbf{H}_\mathrm{r}\hat{\mathbf{x}}_\mathrm{r}\|_2 \leq \tau, \qquad (2.17)
\end{aligned}$$

where $\hat{\mathbf{x}}_{\text{r,shift}}$ is the shifted state estimates estimated using attacked measurements $\mathbf{z}_{\mathbf{a}}$. The nature question here is that if FDIA still pass BDD, even though attackers don't know the index of reference bus. According to the following lemma 1, the answer is affirmative.

Lemma 1. *An FDIA does not change the residual even if it is not aware of the index of reference bus and perform FDIA by attack vector* $\mathbf{a}_i = \mathbf{H}_i\mathbf{c}_n$ *or* $\mathbf{a}_i = \mathbf{H}\mathbf{c}_{n+1}$*, where* $\mathbf{H}_i$ *is derived by removing* i*th column of* $\mathbf{H}$*,* $\mathbf{c}_n$ *is* $n \times 1$ *shift vector, and* $\mathbf{c}_{n+1}$ *is* $(n+1) \times 1$ *shift vector. In general,* i *is not the index of reference bus.*

Proof. We assume index of the reference bus will change, and attackers don't know when the index changes and which index is the next reference bus. The reformulated DC state estimation model is

$$\mathbf{z} = \mathbf{H}_j\mathbf{x}_j + \mathbf{e}, \tag{2.18}$$

where $\underbrace{\mathbf{H}_j}_{m\times n}$ is derived by removing jth column of $\underbrace{\mathbf{H}}_{m\times(n+1)}$ and j is index of reference bus. The corresponding LS-estimator is

$$\hat{\mathbf{x}}_j = (\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{H}_j)^{-1}\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{z}. \tag{2.19}$$

The received measurement is

$$\mathbf{z}_{\mathbf{a}} = \mathbf{z} + \mathbf{a}_i. \tag{2.20}$$

The biased state estimates becomes

$$\begin{aligned} \hat{\mathbf{x}}_{j,\text{shift}} &= (\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{H}_j)^{-1}\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{z}_{\mathbf{a}} \\ &= (\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{H}_j)^{-1}\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{z} + \mathbf{a} \\ &= \hat{\mathbf{x}}_j + (\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{H}_j)^{-1}\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{a}_i \end{aligned} \tag{2.21}$$

The BDD criteria is

$$\begin{aligned}
\|\mathbf{z_a} - \mathbf{H}_j\hat{\mathbf{x}}_{j,\text{shift}}\| &= \|\mathbf{z} + \mathbf{a}_i - \mathbf{H}_j(\hat{\mathbf{x}}_j + (\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{H}_j)^{-1}\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{a}_i)\| \\
&= \|(\mathbf{z} - \mathbf{H}_j\hat{\mathbf{x}}_j) + (\mathbf{a}_i - \mathbf{H}_j(\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{H}_j)^{-1}\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{a}_i)\| \\
& \quad \text{let } \mathbf{H}_j(\mathbf{H}_j^T\mathbf{R}^{-1}\mathbf{H}_j)^{-1}\mathbf{H}_j^T\mathbf{R}^{-1} = \underbrace{\mathbf{A}_j}_{m\times m} \\
&= \|(\mathbf{z} - \mathbf{H}_j\hat{\mathbf{x}}_j) + (\mathbf{a}_i - \mathbf{A}_j\mathbf{a}_i)\| \\
&= \|(\mathbf{z} - \mathbf{H}_j\hat{\mathbf{x}}_j) + (\mathbf{I}_m - \mathbf{A}_j)\mathbf{a}_i)\|
\end{aligned}$$

Note that $rank(\mathbf{A}_j) = n$, and $\mathbf{A}_j$ is a projection matrix, i.e., $\mathbf{A}_j^2 = \mathbf{A}_j$ [22].

We want to prove that $(\mathbf{I}_m - \mathbf{A}_j)\mathbf{a}_i = 0$ is always true in all cases. The possible cases that attackers may meet:

Case 1: Attacker knows the index of reference bus

$$\mathbf{a}_i = \mathbf{H}_j\mathbf{c}_n, \forall i = j \tag{2.22}$$

Case 2: Attacker doesn't know the index of reference bus

$$\mathbf{a}_i = \mathbf{H}_i\mathbf{c}_n, \forall i \neq j \tag{2.23}$$

Case 3: Attacker doesn't know the index of reference bus and tend to shift reference bus

$$\mathbf{a}_i = \mathbf{H}\mathbf{c}_{n+1} \tag{2.24}$$

Note that $rank(\mathbf{H}_i) = rank(\mathbf{H}_j) = rank(\mathbf{H}) = n$ and $\mathbf{H}\cdot\mathbf{1} = \mathbf{0}$. We divide the proof into two parts:

1. Given $rank(\mathbf{H}_i) = rank(\mathbf{H}_j) = rank(\mathbf{H}) = n$. If $\mathbf{H_i}, \mathbf{H_j}$ are both derived by removing ith and jth column of $\mathbf{H}$ respectively, then the column spaces of $\mathbf{H}_j, \mathbf{H}_i, \mathbf{H}$ are the same.

   proof 1. Since $rank(\mathbf{H}_i) = rank(\mathbf{H})$, it implies that the ith column of $\mathbf{H}$ $(\mathbf{h}_i)$ are linear combination of columns of $\mathbf{H}_i$, i.e., $\mathbf{h}_i$ lies in the column space of $\mathbf{H}_i$.

Therefore, column space of $\mathbf{H}$ is equal to column space of $\mathbf{H}_i$. Similarly, we can prove that column space of $\mathbf{H}$ is equal to column space of $\mathbf{H}_j$. Finally, the column spaces of $\mathbf{H}_j, \mathbf{H}_i, \mathbf{H}$ are the same. □

2. If the column spaces of $\mathbf{H}_j, \mathbf{H}_i, \mathbf{H}$ are the same, then the attackers can pass BDD without the knowledge of index of reference bus.

   proof 2. $\because$ the column spaces of $\mathbf{H}_j, \mathbf{H}_i, \mathbf{H}$ are the same, $\therefore$

$$\exists \mathbf{c'}_n \in \mathbb{R}^n : \mathbf{H}_i \mathbf{c}_n = \mathbf{H}_j \mathbf{c'}_n, \forall \mathbf{c}_n \in \mathbb{R}^n \tag{2.25}$$

$$\exists \mathbf{c'}_n \in \mathbb{R}^n : \mathbf{H}\mathbf{c}_{n+1} = \mathbf{H}_j \mathbf{c'}_n, \forall \mathbf{c}_n \in \mathbb{R}^n \tag{2.26}$$

   - Case 1: $\mathbf{A}_j \mathbf{H}_j \mathbf{c}_n = \mathbf{H}_j \mathbf{c}_n \Rightarrow (\mathbf{I} - \mathbf{A}_j)\mathbf{a}_i = 0$
   - Case 2: $\mathbf{A}_j \mathbf{H}_i \mathbf{c}_n = \mathbf{A}_j \mathbf{H}_j \mathbf{c'}_n = \mathbf{H}_j \mathbf{c'}_n = \mathbf{H}_i \mathbf{c}_n \Rightarrow (\mathbf{I} - \mathbf{A}_j)\mathbf{a}_i = 0$
   - Case 3: $\mathbf{A}_j \mathbf{H}\mathbf{c}_{n+1} = \mathbf{A}_j \mathbf{H}_j \mathbf{c'}_n = \mathbf{H}_j \mathbf{c'}_n = \mathbf{H}\mathbf{c}_{n+1} \Rightarrow (\mathbf{I} - \mathbf{A}_j)\mathbf{a}_i = 0$

□

□

Chapter 3

Security Index and Smart Attackers

In this chapter, we consider the scenario that an attacker is capable of tampering with multiple meters, has the knowledge of network topology including the indices of reference bus and the protected meters if exist. We assume that the grid operator can protect any chosen meter from being tampered. [5] has proved that no FDIA is possible if the size of properly selected protected measurements is greater than the number of state variables. We are interested in the case when the size of the protected measurements is less than the number of buses. In this case, [3, Theorem 2,] says that an FDIA is always feasible if the attacker can manipulate more than $m - n$ meters. In other word, an FDIA exists when the protection subset size is less than n. We consider the game in which a legitimate FDIA wants to minimize the number of tampered meters while the grid operator intends to force an FDIA to tamper as many measurements as possible, i.e., it wants to maximize the "cost" of a successful FDIA. The equivalent optimization problem from the attacker's viewpoint is given in the following section.

3.1 Game between Attackers and Grid Operator

We focus on the range that protection size is least than number of state variables, and want to maximize the number of meters that attackers need to tamper with in order to shift state variables without triggering BDD. Table 3.1 shows the objectives and

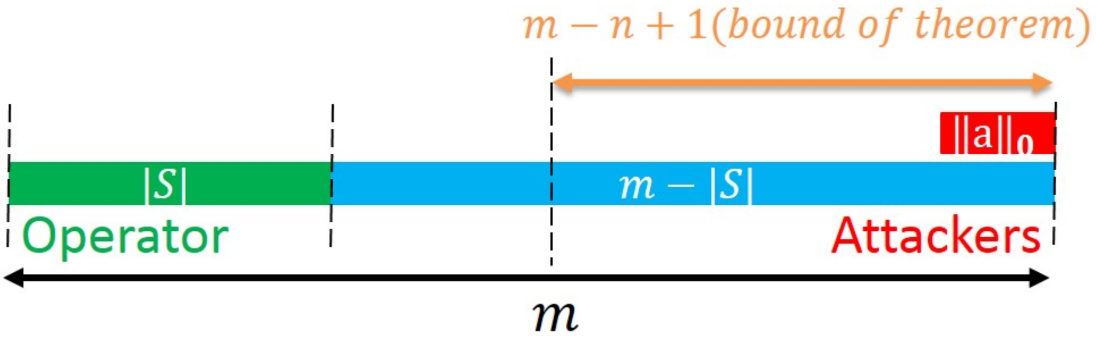

Figure 3.1: Meter competition. The line distance represents the number of meters. $|\mathcal{S}|$ is the number of protected meters, and $m - |\mathcal{S}|$ is number of available meters for attackers.

abilities of attackers and grid operator individually. In Fig. 3.1, it illustrates the battle field between attackers and grid operator. In smart grid, m meters are given, and grid operator can protect meters gradually, in this example $|\mathcal{S}|$. Consequently, the number of meters that attackers can tamper with is $m - |\mathcal{S}|$, called available meters. The bound of theorem indicates the existence of attack vector proved in theorem 2 in [3], that is, if attackers compromise more than or equal to $m - n + 1$ meters, it guarantees that attack vector always exists. On the other hand, if grid operator protect more than n meters, attackers no longer can tamper with more than $m - n$ meters. In this case, attack vector doesn't always exists. Actually, [5] shows that FDIA is no longer valid if protection set of n critical meters is carefully selected. Unfortunately, when protection size is less than n, if attackers only prefer to shift one or two state variables, it is common that number of tampered meters is far less than $m - n + 1$ due to the sparseness of Jacobian matrix

Table 3.1: Game between attackers and grid operator

Players	Attackers	Defender (Grid operator)
Goal of players	Minimize tampered measurements	Maximize minimal tampered measurements of attacker
Ability of players	Manipulate measurements	Protect meters
battle field	meters	
Field Factors	Random failure/Topology extension/etc.	

$\mathbf{H}$.

3.2 Attack Formulation

It is assumed that attackers are capable of tampering with several meters, have the knowledge of network topology including the index of reference bus, and know the index of protected meter if any. They can inject an attack vector $\mathbf{a}$ into tampered meters such that the measurements become $\mathbf{z_a} = \mathbf{z} + \mathbf{a}$. Recall (2.15),

$$\mathbf{a} = \mathbf{H}_\mathrm{r}\mathbf{c}_\mathrm{r}$$

if attack vector $\mathbf{a}$ is linear combination of columns of $\mathbf{H}$, then it does not change the residual in (2.14).

Due to the protection strategy provided by grid operator, invalidation of injecting false data into protected meters introduces the constraints for attackers

$$\mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0} \tag{3.1}$$

The rank analysis on constraint (3.1) presents the proofs in [5] and [3]. we assume that the network is observable, then there exist n linearly independent measurements. If operator carefully selects n meters to protect such that $rank(\mathbf{H}_\mathrm{r}^{\mathcal{S}}) = n$, then $\mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0}$ if and only if $\mathbf{c}_\mathrm{r} = \mathbf{0}$, that is, FDIA is no longer possible. Otherwise, when number of protected meter is less than n, $rank(\mathbf{H}_\mathrm{r}^{\mathcal{S}}) < n$, there always exists $\mathbf{c}_\mathrm{r} \neq \mathbf{0}$ such that $\mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0}$.

It is useless to shift state variables with little shift vector, the second constraint is meaningful attack that FDIA must shift at least a state variable not smaller than a threshold $\tau > 0$

$$\|\mathbf{c}_\mathrm{r}\|_\infty \geq \tau. \tag{3.2}$$

An attacker intends to find a sparsest attack vector $\mathbf{a}$ $(= \mathbf{H}_\mathrm{r}\mathbf{c}_\mathrm{r})$, i.e., it wants to manipulate as less meters as possible under the two constraints above. Thus, the optimization problem for attackers is

$$\min_{\mathbf{c}_{\mathrm{r}} \in \mathbb{R}^n} \quad ||\mathbf{H}_{\mathrm{r}}^{\bar{\mathcal{S}}} \mathbf{c}_{\mathrm{r}}||_0 \tag{3.3a}$$

$$s.t. \quad \mathbf{H}_{\mathrm{r}}^{\mathcal{S}} \mathbf{c}_{\mathrm{r}} = \mathbf{0} \tag{3.3b}$$

$$\|\mathbf{c}_{\mathrm{r}}\|_\infty \geq \tau. \tag{3.3c}$$

Kim *et al.* [7] combined the constraint of meaningful attack into the objective function, and the final form can be derived as

$$\min_{\mathbf{c}_{\mathrm{r},i} \in \mathbb{R}^{n-1}} \quad \|\mathbf{H}_{\mathrm{r},i}^{\bar{\mathcal{S}}} \mathbf{c}_{\mathrm{r},i} + \mathbf{h}_{\mathrm{r},i}^{\bar{\mathcal{S}}}\|_0 \tag{3.4a}$$

$$s.t. \quad \mathbf{H}_{\mathbf{r},i}^{\mathcal{S}} \mathbf{c}_{\mathrm{r},i} + \mathbf{h}_{\mathrm{r},i}^{\mathcal{S}} = \mathbf{0}. \tag{3.4b}$$

for $i = 1, ..., n$, where $\mathbf{H}_{\mathrm{r},i}^{\bar{\mathcal{S}}}$ is derived by removing ith column of $\mathbf{H}_{\mathrm{r}}^{\bar{\mathcal{S}}}$, $\mathbf{h}_i^{\bar{\mathcal{S}}}$ is ith column of $\mathbf{H}_{\mathrm{r}}^{\bar{\mathcal{S}}}$, $\mathbf{H}_{\mathrm{r},i}^{\mathcal{S}}$ and $\mathbf{h}_i^{\mathcal{S}}$ is as the same way, and $\mathbf{c}_{\mathrm{r},i}$ is derived by remove ith element of $\mathbf{c}_{\mathrm{r}}$. Nevertheless, the optimization problem of searching sparsest solution is NP-hard [8]. Consequently, the authors use the l_1 approximation to find $\mathbf{c}_{\mathrm{r},i}, \forall i = 1, .., n$.

$$\min_{\mathbf{c}_{\mathbf{r},i} \in \mathbb{R}^{n-1}} \quad \|\mathbf{H}_{\mathbf{r},i}^{\bar{\mathcal{S}}} \mathbf{c}_{\mathbf{r},i} + \mathbf{h}_{\mathbf{r},i}^{\bar{\mathcal{S}}}\|_1 \tag{3.5a}$$

$$s.t. \quad \mathbf{H}_{\mathbf{r},i}^{\mathcal{S}} \mathbf{c}_{\mathbf{r},i} + \mathbf{h}_{\mathbf{r},i}^{\mathcal{S}} = 0. \tag{3.5b}$$

However, the approximated attack vector may lead to the wrong protection strategy. In addition, the performance of design algorithm examining by approximated attack vector is judgeless, because we don't know whether the number of tampered meters is true minimum or not. The meter selection basically needs the attack information to decide which meter should be protected first. The approximated attack information may result in improper meter selection so that the corresponding protection strategy suffers true optimal attacks. Hence, before designing a meter selection algorithm, we need to develop a method to calculate minimal number of tampered meters under given protection set. In the following section we introduce the way to obtain optimal attack vector so that the meter selection algorithm determine the to-be-protected meter with optimal attack information, and the performance is meaningful.

3.3 $\mathcal{S}$-Security Index

We are interested in a method which solves (3.3) directly. However this problem is NP-hard. We try to use security indices [13] to construct attack vector. The definition of $\mathcal{S}$-security index of kth meter $\alpha_k(\mathcal{S})$ is

$$\begin{aligned} \alpha_k(\mathcal{S}) = \min_{\mathbf{c}\in\mathbb{R}^{n+1}} \quad & ||\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}||_0 \\ s.t. \quad & \mathbf{H}^{\mathcal{S}}\mathbf{c} = 0 \\ & \mathbf{H}(k,:)\mathbf{c} = 1. \end{aligned} \tag{3.6a}$$

where $\mathbf{H}(k,:)$ is the kth row of $\mathbf{H}$. Given a protection set $\mathcal{S}$, if attackers want to manipulate the measurement z_k without triggering BDD , $\alpha_k(\mathcal{S})$ is the minimum number of meters need to be corrupted. The index $\alpha_k(\mathcal{S})$ directly represents the degree of difficulty of manipulating kth measurement. If the index is large, it means the attackers need to manipulate many measurements in order to not trigger BDD. Otherwise, if the index is small, attackers prefer to forge that measurement due to low cost.

Before evaluating the optimal attack vector, we need to derive all security indices $\alpha_k, \forall k \in \bar{\mathcal{S}}$. Unfortunately, the problem (3.6) is also non-convex and NP-hard. However, the authors in [14] claim that when the Jacobian matrix only contains branch meters, security index problem can be transformed to node partitioning problem, and it can be exactly solved by MIN CUT. In the following, we illustrate how to use MIN CUT to calculate exact security index for each measurement. There are two steps:

1. use Proposition 2 in [14] to transform (3.6) into node partitioning problem, where the nodes are buses.

   Proposition 2 : Let $\mathbf{H}$ in (2.13) satisfy the injection-free assumption that $P_1 = P_2 = I$ and $P_3 = \mathbf{0}$. Consider the following restriction of problem (3.6) with 0-1 binary decision vector:

$$\tilde{\alpha}_k(\mathcal{S}) = \min_{\mathbf{c}\in\{0,1\}^{n+1}} \quad ||\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}||_0 \tag{3.7a}$$

$$s.t. \quad \mathbf{H}^{\mathcal{S}}\mathbf{c} = 0 \tag{3.7b}$$

$$\mathbf{H}(k,:)\mathbf{c} = 1. \tag{3.7c}$$

It holds that every optimal solution of (3.7) is an optimal solution of (3.6), i.e., $\tilde{\alpha}_k(\mathcal{S}) = \alpha_k(\mathcal{S}), \forall\mathcal{S}$.

2. transform the node partitioning problem into MIN CUT problem by defining corresponding graph and edge weights.

Recall that in (2.3) $P^s_{i,j} = V_iV_jb_{ij}(x_i - x_j)$ and (2.15) $\mathbf{a} = \mathbf{H}_{\rm r}\mathbf{c}_{\rm r}$, we have

$$a_k = V_sV_tb_{st}(c_s - c_t), k = \mathcal{M}(s,t), \tag{3.8}$$

where $\mathcal{M}(s,t)$ is the meter index from sth bus to tth bus. (3.7) represents that the kth meter is manipulated if and only if $c_s \neq c_t$, and we want to minimize the tampered meters, i.e., find a partitions of $\mathbf{c}$ so that the border of partitions passes through minimal meters. We now define the MIN CUT problem on weighted directed graph. Let $G(V,E)$ be a directed graph, where V is the set of bus nodes $\{v_1,\ldots,v_{n+1}\}$, and E denotes the set of directed edges (v_i,v_j). The edges are weighted with $w_{i,j}$ for all $(v_i,v_j)\in E$. Define two special nodes: a source node v_s and a sink node v_t. The MIN CUT problem is to find a partition of V, denoted as $P_k(\mathcal{S}) = \{V_1,V_0\}$, such that $V_1,\ V_0 \subset V,\ V_1\cap V_0 = \emptyset, V_1\cup V_0 = V$ and minimize the tampered meters:

$$\begin{aligned} \tilde{\alpha}_k(\mathcal{S}) = \min_{P_k(\mathcal{S})=\{V_1,V_0\}} \quad & N(P_k(\mathcal{S})) = \sum_{\{(v_i,v_j)\in E|v_i\in V_1, v_j\in V_0\}} w_{i,j} \\ s.t. \quad & V_1,\ V_0\subset V,\ V_1\cap V_0=\emptyset, V_1\cup V_0 = V \\ & v_s\in V_1, v_t\in V_0,\ \text{where } k=\mathcal{M}(s,t), \end{aligned} \tag{3.9}$$

where

$$w_{i,j} = \begin{cases} \infty & \mathcal{M}(i,j)\in\mathcal{S} \\ 2 & \mathcal{M}(i,j)\in\mathcal{M}\setminus\mathcal{S} \end{cases}$$

If $v_i \in V_1$, $v_j \in V_0$ for the edge (v_i, v_j), we call that the edge (v_i, v_j) is in the cut. For the clarification that in a directed graph an edge (v_i, v_j) is cut if $v_i \in V_1$ and $v_j \in V_0$ but not in the reverse case, where $v_j \in V_1$ and $v_i \in V_0$, and the cost $w_{i,j}$ is not incurred in that latter case. Currently, given a protection set $\mathcal{S}$, the exact security index $\tilde{\alpha}_k(\mathcal{S})$ can be evaluated only in injection-free case, i.e., $P_1 = P_2 = I$ and $P_3 = \mathbf{0}$. In addition, if $\mathcal{S} = \emptyset$, then the exact $\tilde{\alpha}_k(\emptyset)$ can be derived in full measurement case, i.e., $P_1 = P_2 = I$ and $P_3 = I$, by solving the MIN CUT with costly nodes problem with auxiliary graph [15].

[14] suggests 4 step to derive security indices $\tilde{\alpha}_k(\mathcal{S}), \forall k \in \bar{\mathcal{S}}$:

1. Define (v_i, v_j) and (v_j, v_i) as edges of the graph G, where (v_i, v_j) is an edge of the original power network graph. If the edge (v_i, v_j) is in protection set, let the weights $w_{i,j}$ be ∞; Otherwise let the weights $w_{i,j}$ be 2.

2. Denote (v_s, v_t) as the targeted arc corresponding kth measurement, where $k = \mathcal{M}(s, t)$. Recall that v_s and v_t are, respectively, the source and sink nodes in G.

3. Solve the MIN-CUT problem on $\mathcal{G}$. Let $\mathbf{c}_{\text{mc}}^{\tilde{\alpha}_k(\mathcal{S})}$ be the optimal MIN-CUT partition, $\mathbf{H_{arc}}$

$$\mathbf{H_{arc}} \triangleq \begin{bmatrix} DA^T \\ -DA^T \end{bmatrix}_{m' \times n+1}, m' = 2m_a \tag{3.10}$$

   and $\|\mathbf{H}_{\text{arc}} \mathbf{c}_{\text{mc}}^{\tilde{\alpha}_k(\mathcal{S})}\|_0$ is an exact security index $\tilde{\alpha}_k(\mathcal{S})$ of the edge (v_s, v_t) in injection-free case.

4. evaluate all MIN CUT partitions, $\forall k \in \bar{\mathcal{S}}$.

We give an example to illustrate how to solve the $\tilde{\alpha}_k(\mathcal{S})$ using MIN CUT. Consider the IEEE 9 case, the corresponding directed graph $G_{case9}(V, E)$ in injection-free case (branch meters only) is in the Fig. 3.2, which contains 9 vertices (9 buses) and 18 directed edges (9 transmission lines). Assume no meter is protected. According to (2.13), without loss of generality, let $D = I$ for convenience, and the Jacobian matrix of

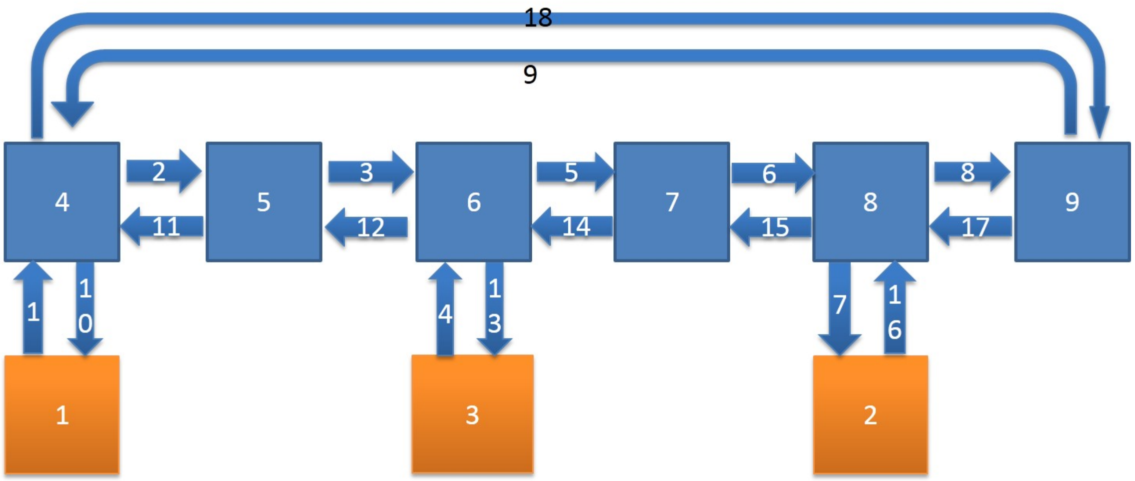

Figure 3.2: The directed graph $G_{case9}(V, E)$ of case 9 in injection-free case. No meter is protected.

case 9 in injection-free case is

$$\mathbf{H}_{\text{arc,case9}} = \begin{array}{c} 1\\2\\3\\4\\5\\6\\7\\8\\9\\10\\11\\12\\13\\14\\15\\16\\17\\18 \end{array} \left[\begin{array}{ccccccccc}
1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \\
\hline
-1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1
\end{array}\right] \tag{3.11}$$

Now calculate the $\tilde{\alpha}_2(\emptyset)$ as an example, we have the corresponding source node $v_s = v_4$ and sink node $v_t = v_5$, and we need to find a partition of V, denoted as $P_2(\emptyset) = \{V_1, V_0\}$, such that $V_0, V_1 \subset V$, $V_1 \cap V_0 = \emptyset$, $V_1 \cup V_0 = V$, $v_4 \in V_1$, $v_5 \in V_0$, and minimize the cost

$$C(P_2(\emptyset)) = \sum_{\{(v_i,v_j)\in E | v_i \in V_1, v_j \in V_0\}} w_{ij}. \tag{3.12}$$

Fig. 3.3 is the MIN CUT for $\tilde{\alpha}_2(\emptyset)$ of directed graph $G_{case9}(V, E)$ of case 9 in injection-free case. The cost is

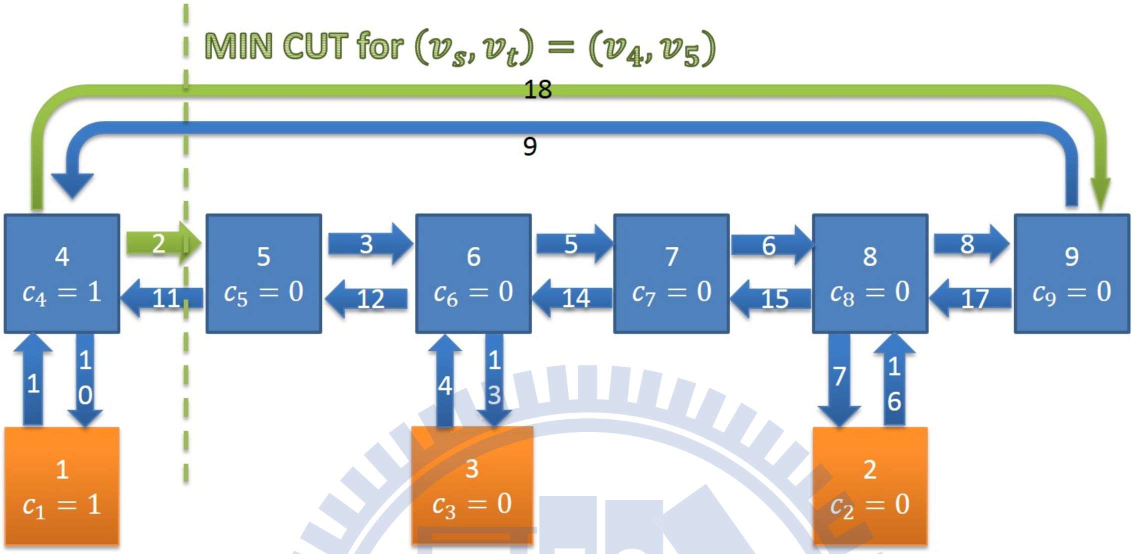

Figure 3.3: The MIN CUT for $\tilde{\alpha}_2(\emptyset)$ of directed graph $G_{case9}(V, E)$ of case 9 in injection-free case. The partition are $V_1 = \{v_1, v_4\}$ and $V_0 = \{v_2, v_3, v_5, v_6, v_7, v_8, v_9\}$.

$$C(P_2(\emptyset)) = \sum_{\{(v_i,v_j)\in E | v_i \in V_1, v_j \in V_0\}} w_{ij} = w_{4,5} + w_{4,9} = 4. \tag{3.13}$$

Again for clarification, the 9th edge (v_9, v_4) and the 11th edge (v_5, v_4) do not belong to the same cut, since $v_5, v_9 \notin V_1$ and $v_4 \notin V_0$. The optimal shift vector $\mathbf{c}_{\text{mc}}^{\tilde{\alpha}_2(\emptyset)}$

$$\mathbf{c}_{\text{mc}}^{\tilde{\alpha}_2(\emptyset)} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \\ c_9 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \tag{3.14}$$

and $\tilde{\alpha}_2(\emptyset) = ||\mathbf{H}_{\text{arc,case9}} \mathbf{c}_{\text{mc}}^{\tilde{\alpha}_2(\mathcal{S})}||_0 = 4 = C(P_2(\emptyset))$, which indicates that if attackers want to manipulate the 2th measurement of case 9, the minimum number of measurements they need to tamper with is 4, i.e., meter 2,9,11,18.

3.4 Optimal Attack Vector

In this section, we illustrate how to generate attack vector using security indices and prove that the corresponding optimization problem is the same as (3.3). For the beginning, we redefine the new security index $\alpha'_k(\mathcal{S})$ which is calculated under the restriction of shift vector $\mathbf{c_r} \in \{0,1\}^n$

$$\begin{aligned} \alpha'_k(\mathcal{S}) = \min_{\mathbf{c}_{\mathrm{r}} \in \{0,1\}^n} \quad & ||\mathbf{H}_{\mathrm{r}}^{\bar{\mathcal{S}}} \mathbf{c}_{\mathrm{r}}||_0 \\ s.t. \quad & \mathbf{H}_{\mathrm{r}}^{\mathcal{S}} \mathbf{c}_{\mathrm{r}} = 0 \\ & \mathbf{H}_{\mathrm{r}}(k,:)\mathbf{c}_{\mathrm{r}} = 1. \end{aligned} \tag{3.15}$$

The nature question will be arise that if the redefined version of security index $\alpha'_k(\mathcal{S})$ is equal to $\alpha_k(\mathcal{S})$. The answer is yes, if it is proved that the last element of shift vector $\mathbf{c}_k^*$ corresponding to each $\alpha_k(\mathcal{S})$ is always equal to 0 due to the fact $\mathbf{H_r c_r} = \mathbf{Hc}$ while the last element of $\mathbf{c}$ is 0. Actually, it is not guaranteed that the last element of shift vector $\mathbf{c}_k^*$ corresponding to each $\alpha_k(\mathcal{S})$ is always equal to 0. However, if there exists $\mathbf{c}_k^*$ whose last element is not 0, we can transform that $\mathbf{c}_k^*$ to $\bar{\mathbf{c}}_k^* = \mathbf{1} - \mathbf{c}_k^*$, where last element of $\bar{\mathbf{c}}_k^*$ is 0. Note that $\mathbf{c}_k^*, \bar{\mathbf{c}}_k^* \in \{0,1\}^{n+1}$. Further, we claim that the transformation of shift vector will not change the value of security index $\alpha_k(\mathcal{S})$ and the index of nonzero elements of attack vector corresponding to $\mathbf{c}_k^*$. The short proof are listed:

- The transformation of shift vector will not change the value of security index $\alpha_k(\mathcal{S})$

  Proof.

$$||\mathbf{H}^{\bar{\mathcal{S}}} \bar{\mathbf{c}}_k^*||_0 = ||\mathbf{H}^{\bar{\mathcal{S}}}(\mathbf{1} - \mathbf{c}_k^*)||_0 = ||-\mathbf{H}^{\bar{\mathcal{S}}} \mathbf{c}_k^*||_0 = ||\mathbf{H}^{\bar{\mathcal{S}}} \mathbf{c}_k^*||_0 \tag{3.16}$$

□

- The transformation of shift vector will not change the index of nonzero elements of attack vector corresponding to $\mathbf{c}_k^*$

Proof. Let the attack vector of security index $\alpha_k(\mathcal{S})$ be $\mathbf{a}_k^* = \mathbf{H}\mathbf{c}_k^*$ and the that of transformed version be $\bar{\mathbf{a}}_k^* = \mathbf{H}\bar{\mathbf{c}}_k^*$. Then

$$\bar{\mathbf{a}}_k^* = \mathbf{H}\bar{\mathbf{c}}_k^* = \mathbf{H}(\mathbf{1} - \mathbf{c}_k^*) = -\mathbf{H}\mathbf{c}_k^* = -\mathbf{a}_k^* \tag{3.17}$$

□

Thus the redefined version of the security index $\alpha_k'(\mathcal{S})$ is always equal to $\alpha_k(\mathcal{S})$ with the proper transformation of shift vector.

Define $\alpha_{\min}(\mathcal{S})$ as the $\mathcal{S}$-security index of the network. Let $\hat{\mathbf{c}}_{\mathbf{r},k}(\mathcal{S})$ be the best shift vector of $\mathcal{S}$-security index of kth meter, $\mathbf{a}_k(\mathcal{S})$ be the best attack vector to attack kth meter, and $\mathcal{A}_k(\mathcal{S})$ be the attack set composed by the indices of nonzero elements of attack vector $\mathbf{a}_k(\mathcal{S})$. We propose the attack formulation and the corresponding optimization problem is as follow:

- Outer minimization problem

$$\alpha_{\min}(\mathcal{S}) \quad = \quad \min_{k\in\bar{\mathcal{S}}} \alpha_k'(\mathcal{S}) \tag{3.18a}$$

$$k^*(\mathcal{S}) \quad = \quad \arg\min_{k\in\bar{\mathcal{S}}} \alpha_k'(\mathcal{S}) \tag{3.18b}$$

- Inner minimization problem for each meter $k \in \bar{\mathcal{S}}$

$$\mathcal{A}_k(\mathcal{S}) \quad = \quad \{i | a_{k,i}(\mathcal{S}) \neq 0\} \tag{3.18c}$$

$$\mathbf{a}_k(\mathcal{S}) \quad = \quad \mathbf{H}_\mathrm{r}\hat{\mathbf{c}}_{\mathrm{r},k}(\mathcal{S}) \tag{3.18d}$$

$$\hat{\mathbf{c}}_{\mathrm{r},k}(\mathcal{S}) = \quad \arg\min_{\mathbf{c}_\mathrm{r}\in\mathbb{R}^n} \quad ||\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\mathbf{c}_\mathrm{r}||_0 \tag{3.18e}$$

$$\alpha_k'(\mathcal{S}) = \quad \min_{\mathbf{c}_\mathrm{r}\in\mathbb{R}^n} \quad ||\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\mathbf{c}_\mathrm{r}||_0 \tag{3.18f}$$

$$s.t. \quad \mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0} \tag{3.18g}$$

$$\mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r} = 1 \tag{3.18h}$$

where $a_{k,i}(\mathcal{S})$ is ith element of $\mathbf{a}_k(\mathcal{S})$. The $k^*(\mathcal{S})$th meter is most attractive to attackers since attack can launch FDIA with minimal cost by forging $k^*(\mathcal{S})$th meter. Note that

$k^*(\mathcal{S})$ may not be unique. The proposed formulation is proved that optimization problem (3.18) is equal to (3.3). Furthermore, we use max flow solver [32] to derive exact $\alpha'_k(\mathcal{S})$, and the details have been given in the previous section. Therefore, the optimal attack vectors are derived. The proof needs to use property of meaningful attack condition as follow:

Property 1 (Property of Meaningful Attack Condition)**.** $\|\mathbf{c}_\mathrm{r}\|_\infty \geq \tau > 0$ *if and only if* $|a_k| = |\mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r}| \geq \xi > 0$, *for some* k*.*

Proof of property 1. $\mathbf{H_r}$ is full rank $\Rightarrow \mathbf{a} = \mathbf{H_r c_r} = \mathbf{0}$ iff $\mathbf{c}_\mathrm{r} = \mathbf{0}$

- $\because \|\mathbf{c}_\mathrm{r}\|_\infty \geq \tau \Leftrightarrow \mathbf{c}_\mathrm{r} \neq \mathbf{0} \therefore \mathbf{a} \neq \mathbf{0} \Leftrightarrow |a_k| \geq \xi$, for some k.
- $\because |a_k| \geq \xi$, for some $k \Leftrightarrow \mathbf{a} \neq \mathbf{0} \therefore \mathbf{c}_\mathrm{r} \neq \mathbf{0} \Leftrightarrow \|\mathbf{c}_\mathrm{r}\|_\infty \geq \tau$

□

The outline of the proof is transform the problem (3.3) to (3.18). Recall (3.3)

$$\begin{aligned} \min_{\mathbf{c}_\mathrm{r}\in\mathbb{R}^n} \quad & ||\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\mathbf{c}_\mathrm{r}||_0 \\ s.t. \quad & \mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = 0 \\ & \|\mathbf{c}_\mathrm{r}\|_\infty \geq \tau. \end{aligned}$$

First of all, we replace the meaningful attack constraint using property 1, and the problem becomes

$$\min_{\mathbf{c}_\mathrm{r}\in\mathbb{R}^n} \quad ||\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\mathbf{c}_\mathrm{r}||_0 \tag{3.19a}$$

$$s.t. \quad \mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0} \tag{3.19b}$$

$$|\mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r}| \geq \xi \quad , \ for\ some\ k \tag{3.19c}$$

We use the fact that scaling the constraint $|\mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r}| \geq \xi,\ for\ some\ k$ by ξ does not change the l_0 norm.

$$\begin{aligned} \min_{\mathbf{c}_\mathrm{r}\in\mathbb{R}^n} \quad & ||\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\mathbf{c}_\mathrm{r}||_0 && \text{(3.20a)} \\ s.t. \quad & \mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0} && \text{(3.20b)} \\ & |\mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r}| \geq 1 \quad , \ for\ some\ k && \text{(3.20c)} \end{aligned}$$

Second, it is desired that convert the constraint $|\mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r}| \geq 1,\ for\ some\ k$ to $\mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r} = 1,\ for\ some\ k$ such that the problem is

$$\begin{aligned} \min_{\mathbf{c}_\mathrm{r}\in\mathbb{R}^n} \quad & ||\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\mathbf{c}_\mathrm{r}||_0 && \text{(3.21a)} \\ s.t. \quad & \mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0} && \text{(3.21b)} \\ & \mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r} = 1 \quad , \ for\ some\ k && \text{(3.21c)} \end{aligned}$$

The constraint set of (3.20) is larger than that of (3.21). It means the minimum of the objective function in (3.21) is not smaller than that of (3.20). If (3.20) is feasible, let $\mathbf{c}_\mathrm{r}^*$ be the optimizer of (3.20) and $\mathbf{a}^* = \mathbf{H}_\mathrm{r}\mathbf{c}_\mathrm{r}^*$. Since $|a_k^*| \geq 1 > 0$, we can define $\bar{\mathbf{c}}_\mathrm{r}^* = \frac{\mathbf{c}_\mathrm{r}^*}{a_k^*}$ such that $\bar{\mathbf{a}}^* = \frac{\mathbf{H}_\mathrm{r}\mathbf{c}_\mathrm{r}^*}{a_k^*}$ satisfies the constraints of (3.21) and, furthermore, $\|\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\mathbf{c}_\mathrm{r}^*\|_0 = \|\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}\bar{\mathbf{c}}_\mathrm{r}^*\|_0$, which implies the constraint replacement. Finally the equivalence between (3.21) and (3.18) is verified by show the constraint sets of (3.21) and (3.18) are the same. The constraint set of (3.21) $S_{\mathbf{c}_\mathrm{r}}^{(3.21)}$ is

$$S_{\mathbf{c}_\mathrm{r}}^{(3.21)} = \{\mathbf{c}_\mathrm{r} | \bigcup_k \mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r} = 1, \mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0}\} \tag{3.22}$$

The constraint set of (3.18) $S_{\mathbf{c}_\mathrm{r}}^{(3.18)}$ is

$$S_{\mathbf{c}_\mathrm{r}}^{(3.18)} = \{\mathbf{c}_\mathrm{r} | \mathbf{H}_\mathrm{r}(k,:)\mathbf{c}_\mathrm{r} = 1, \forall\ k, \mathbf{H}_\mathrm{r}^{\mathcal{S}}\mathbf{c}_\mathrm{r} = \mathbf{0}\} \tag{3.23}$$

It is obviously that $S_{\mathbf{c}_\mathrm{r}}^{(3.21)} = S_{\mathbf{c}_\mathrm{r}}^{(3.18)}$, then the proof is completed. The proposed meter selection algorithm will be based on the information of (3.18) to determine the to-be-protected meter.

Chapter 4

Incremental Meter Protection

Even if the indices of critical meters which the full rank condition $rank(\mathbf{H}^{\mathcal{S}}) = n$ requires are known, it is often difficult if not impossible to protect so many meters in a short period. Before those meters are all protected, FDIA may occur by Theorem 2 in [3]. Fortunately, we are able to force an FDIA attacker to tamper a maximum number of measurements. In the following section, we introduce an algorithm that select protected meters incrementally that meet the above criterion.

4.1 Meter Selection Algorithm of Previous Work

[7] suggests a heuristic subset selection algorithm, which searches for the smallest number of measurements that need protecting so that the attacker will need to tamper with at least N_A meters to evade detection. For convenience, we call the algorithm as Kim's algorithm. Recall that in (3.5a) we have

$$\begin{aligned} \min_{\mathbf{c}_{\mathrm{r},i} \in \mathbb{R}^{n-1}} & \|\mathbf{H}^{\bar{\mathcal{S}}}_{\mathrm{r},i}\mathbf{c}_{\mathrm{r},i} + \mathbf{h}^{\bar{\mathcal{S}}}_{\mathrm{r},i}\|_1 \\ s.t.\ & \mathbf{H}^{\mathcal{S}}_{\mathrm{r},i}\mathbf{c}_{\mathrm{r},i} + \mathbf{h}^{\mathcal{S}}_{\mathrm{r},i} = 0. \end{aligned}$$

Let $\mathbf{c}^*_{\mathrm{r},i}$ be the best known solution of (3.5a) for the attack that modifies at least the ith state, $\mathbf{a}^*_i = \mathbf{H}^{\bar{\mathcal{S}}}_{\mathrm{r},i}\mathbf{c}^*_{\mathrm{r},i} + \mathbf{h}^{\bar{\mathcal{S}}}_{\mathrm{r},i}$, $N_{Ai} = \|\mathbf{a}^*_i\|_0$, and $\mathcal{A}_i$ is the index set of the indices of nonzero index in attack vector $\mathbf{a}^*_i$. The objective function is

$$\min_{\mathcal{S}} |\mathcal{S}| \ s.t. \min_{i \in \{1,\ldots,n\}} N_{Ai} \geq N_A. \tag{4.1}$$

The heuristic subset selection algorithm is listed as Algorithm 1.

Algorithm 1 Subset selection algorithm [7]

```
Require: $N_A$, $\mathbf{H}$
Ensure: $\mathcal{S}$, $\min_i N_{Ai}$
$\mathcal{S} = \emptyset$;
repeat
    $VulnerabilityArr$(1,...,$m$)=0;
    for $i = 1 \rightarrow n$ do
        find $\mathcal{A}_i$ and $N_{Ai}$ based on $\mathbf{H}$ and best known solver of attack strategy;
        if $N_{Ai} < N_A$ then
            $VulnerabilityArr(\mathcal{A}_i) \Leftarrow VulnerabilityArr(\mathcal{A}_i)$+1
        end if
    end for
    $k^* = \arg\max_k VulnerabilityArr(k)$ ;
    add $k^*$ to $\mathcal{S}$;
until $\min_i N_{Ai} \geq N_A$
return $\mathcal{S}$, $\min_i N_{Ai}$;
```

However, the algorithm is not designed for incremental protection, but for a given target N_A. Furthermore, the sequence of protection set of the algorithm in the order, called protection strategy, costs several steps and runs which implies high complexity. The complexity of deriving protection strategy of Kim's algorithm is $O(R_{N_A} \times r \times n(N_A, \mathbf{H}_\mathbf{r}^{\mathcal{S}}) \times m^2 \times n^2) \leq O(m \times r \times m^3 \times n^2) = O(r \times m^4 \times n^2)$, where R_{N_A} is the range of N_A, for example, if $R_{N_A} = 20$, the algorithm will execute for $N_A = 1, ..., 20$; r is for each N_A the algorithm will run for r times and select a protection set with minimal protection size; $n(N_A, \mathbf{H})$ is the number function of N_A and $\mathbf{H}$ bounded by m; and m and n are number of meters and buses respectively. Note that the complexity analysis in [7] is not for protection strategy, but for the algorithm itself.

4.2 Weakest Meter First (WMF) Algorithm

To force the attacker to tamper with most meters, we formulate a new optimization problem. Given a size of protection set A, we want to find a protection set $\mathcal{S}$ satisfying

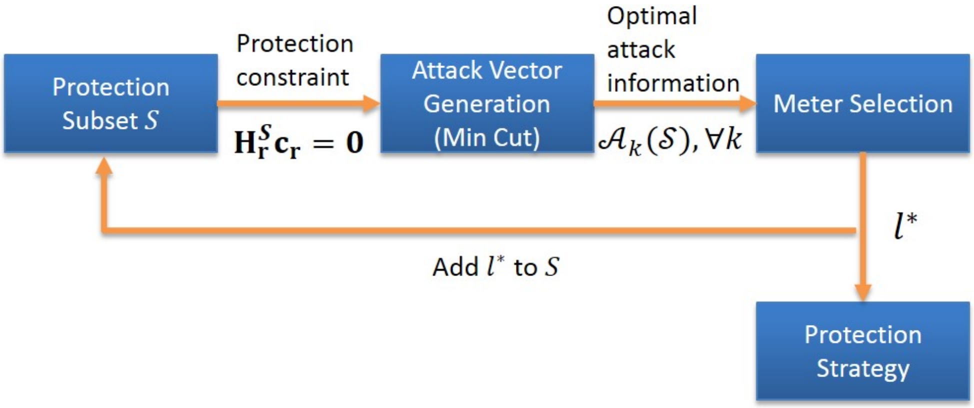
Protection Subset S
Protection constraint
$\mathbf{H}_\mathbf{r}^S\mathbf{c}_\mathbf{r} = \mathbf{0}$
Attack Vector Generation (Min Cut)
Optimal attack information
$\mathcal{A}_k(\mathcal{S}), \forall k$
Meter Selection
l^*
Add l^* to S
Protection Strategy

Figure 4.1: Meter Selection Procedure. Optimal attack set of $\alpha_k(\mathcal{S})$: $\mathcal{A}_k(\mathcal{S}) = \{i|a_{k,i}(\mathcal{S}) \neq 0\}$

$|\mathcal{S}| = A$ such that $\mathcal{S}$-security index of the network is maximize.

$$\max_{\mathcal{S}:|\mathcal{S}|=A} \alpha_{\min}(\mathcal{S}) \tag{4.2}$$

Recall, the $\mathcal{S}$-security index of the network $\alpha_{\min}(\mathcal{S})$

$$\alpha_{\min}(\mathcal{S}) = \min_{k\in\bar{\mathcal{S}}} \alpha_k(\mathcal{S})$$

The $\mathcal{S}$-security index of the kth meter $\alpha_k(\mathcal{S})$ [13], $k \in \bar{\mathcal{S}}$ is

$$\begin{aligned} \alpha_k(\mathcal{S}) = \min_{\mathbf{c_r}\in\mathbb{R}^n} \quad & ||\mathbf{H}_\mathbf{r}^{\bar{\mathcal{S}}}\mathbf{c_r}||_0 \\ s.t. \quad & \mathbf{H}_\mathbf{r}^{\mathcal{S}}\mathbf{c_r} = 0 \quad \text{(protection set)} \\ & \mathbf{H_r}(k,:)\mathbf{c_r} = 1 \quad \text{(must manipulate } k\text{th meter)} \end{aligned}$$

However, we currently cannot figure out the optimal solution of problem (4.2). Instead, following the continuous evolution of smart grid, a incremental meter selection algorithm, called weakest meter first (WMF) Algorithm, which is motivated by the characteristics of MIN CUT, is proposed to find sequence of protection sets. The algorithm protects a meter at a time. The flow chart of WMF is in Fig. 4.1.

The meter which is cut by minimal cut most frequently is defined as the weakest meter, which means it is most vulnerable. When such meter is protect, many cuts related to this meter will disappear, and the candidates of FDIA will be reduced.

Algorithm 2 Weakest meter first (WMF) algorithm

```
Require: $\mathbf{H_r}$
Ensure: $\mathcal{S}$
$\mathcal{S} = \emptyset$;
repeat
    initialize $\mathbf{v} = \mathbf{0}_m$ to count vulnerability of meters;
    find attack set $\mathcal{A}_k$ and $\alpha_k = |\mathcal{A}_k|$ using MIN CUT and $\mathbf{H}_\mathbf{r}^\mathcal{S}$, $\forall k \in \bar{\mathcal{S}}$;
    $\alpha_{\min} = \min_k(\alpha_k)$;
    find the meter index set $\mathcal{D} = \{k|\alpha_k = \alpha_{\min}\}$
    for $i = 1 \to |\mathcal{D}|$ do
        for $j = 1 \to |\mathcal{A}_{\mathcal{D}(i)}|$ do
            $\mathbf{v}(\mathcal{A}_{\mathcal{D}(i)}(j)) \Leftarrow \mathbf{v}(\mathcal{A}_{\mathcal{D}(i)}(j)) + 1$
        end for
    end for
    $l^* = \arg\max_{l \in \mathcal{M}} \mathbf{v}(l)$;
    add $l^*$ to $\mathcal{S}$;
until MIN CUT no longer find any solution
return $\mathcal{S}$;
```

For each iteration, the algorithm calculate the $\mathcal{S}$-security index for unprotected meters under the current protection set $\mathcal{S}$, which is empty at initial. We define an array $\mathbf{v}$ to count the vulnerability of each measurement for every iteration. The cut corresponding to minimal $\mathcal{S}$-security index will be selected to vote the array $\mathbf{v}$. The weakest meter is the meter whose votes is highest in $\mathbf{v}$, i.e., the weakest meter is cut most frequently, and this meter will be protected first. When the maximizer of $\mathbf{v}$ is not unique, we randomly choose one from all the maximizers. Therefore, the algorithm contain randomness. It is required to run only once to determine the protection strategy, which is different from that Kim's algorithm need to run many times for each N_A and select a minimum protection set.

By exploring more topology information, the enhanced WMF (EWMF) is proposed. The idea is that the more votes a meter get, the more cuts disappear when such meter is protected. We consider not only the minimum cuts of minimal $\mathcal{S}$-security index in an iteration, but all minimum cuts passing unprotected meters. Both WMF and EWMF contain randomness due to non-unique maximizers.

Algorithm 3 Enhanced weakest meter first (EWMF) algorithm

```
Require: $\mathbf{H_r}$
Ensure: $\mathcal{S}$
$\mathcal{S} = \emptyset$;
repeat
    initialize $\mathbf{v} = \mathbf{0}_m$ to count vulnerability of meters;
    find attack set $\mathcal{A}_k$ and $\alpha_k = |\mathcal{A}_k|$ using MIN CUT and $\mathbf{H}_\mathbf{r}^{\mathcal{S}}$, $\forall k \in \bar{\mathcal{S}}$;
    $\alpha_{\min} = \min_k(\alpha_k)$;
    find the meter index set $\mathcal{D} = \{k|\alpha_k = \alpha_{\min}\}$
    find the meter index set $\mathcal{F} = \{k|\alpha_k < \infty\}$
    for $i = 1 \rightarrow |\mathcal{F}|$ do
        for $j = 1 \rightarrow |\mathcal{A}_{\mathcal{F}(i)}|$ do
            $\mathbf{v}(\mathcal{A}_{\mathcal{F}(i)}(j)) \Leftarrow \mathbf{v}(\mathcal{A}_{\mathcal{F}(i)}(j)) + 1$
        end for
    end for
    $l^* = \arg\max_{l \in \mathcal{D}} \mathbf{v}(l)$;
    add $l^*$ to $\mathcal{S}$;
until MIN CUT no longer find any solution
return $\mathcal{S}$;
```

The best strategy from 100 times simulations and a single simulation are selected for comparison. The best protection strategy can force attackers manipulate most meters at each protection set, i.e., the best one has maximal $\sum_{|\mathcal{S}|=1}^{(n-1)} min_k \alpha_k(\mathcal{S})$. The IEEE standard grids [30] are used for simulations. We observe the protection strategy of WMF in Fig. 4.6-4.7. When protection size is from 0 to 250, the restriction of protection strategy doesn't discourage the attackers too much, called flat region. We observe that the numbers of intersections of minimal cuts of minimal security index is little in IEEE 300 bus. It results in that when a weakest meter is protected, the other minimal cuts still exist. Both WMF and EWMF contain flat region. However, in flat region, EWMF still eliminates minimal cuts in the "future", even though the S-security index in the network is dominated by the dispersed weakest meters. After flat region, the steeper slope of EWMF shows up due to fewer candidates of possible cuts. The comparison for other cases are given in Fig. 4.3-4.5.

The complexities of WMF and EWMF are the same, and the complexity of maximum flow solver is $O(n^2 \times m)$. We can derive the complexity of WMF is $O(m^2 \times n^3)$, which is smaller and more compatible with continuous evolution of smart grid than Kim's algorithm.

4.3 The Importance of Optimal Attack Vector

The performances of EWMF using optimal attack information and l_1-approximated attack information suffering optimal attack and l_1-approximated attack in injection-free grids are compared. The l_1-approximated attack vector is calculated by CVX tool [31] and optimal attack vector is derived by MatlabBGL [32].

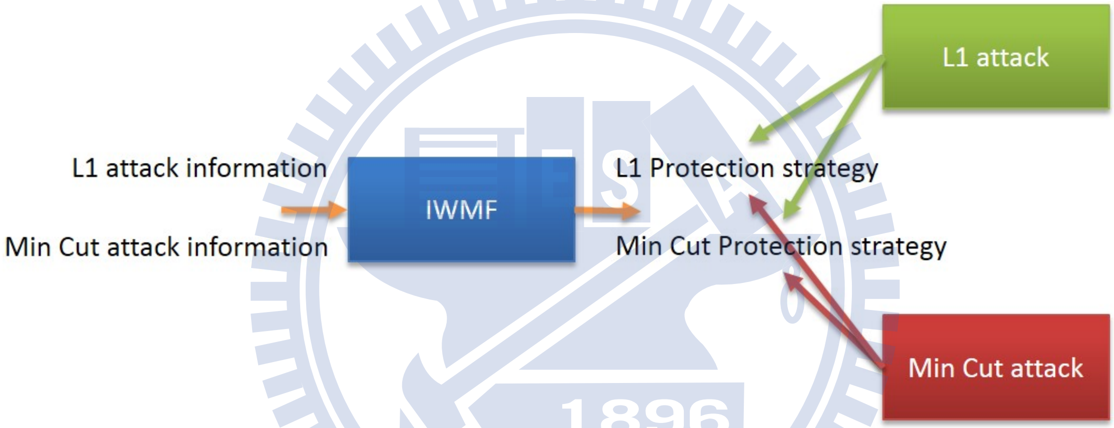

Figure 4.2: The overview of the simulation to reveal the importance of optimal attack vector.

All combinations in fig. 4.2 are simulated for IEEE 30, 57, 118 and 300 bus. Table 4.1 shows the number of meters for each case.

Table 4.1: Number of Injection and branch meters in full measurement case for each test benchmark

Test case	node (bus)	edge (transmission line)	♯ of Injection meters	♯ of branch meters
case 9	9	9	3	18
case 14	14	20	5	40
case 30	30	41	6	82
case 57	57	80	7	160
case 118	118	186	54	392
case 300	300	411	69	822

In Fig. 4.8-4.11, l_1-approximated attack can almost reach the same performance as optimal attack when the protection strategy calculated based on optimal attack information. However, when the protection strategy is evaluated based on l_1-approximated attack information, the l_1-approximated attack cannot find optimal attack vector sometimes, which results in non-smooth curve in Fig. 4.8 and 4.9. In the past, the optimal attack vector is infeasible, and the performance of protection strategy is examined by l_1-approximated attack, which may result in overestimation. In all simulation, it is observed that the optimal attack can find sparser attack vector than l_1-approximated attack. Furthermore, there exists the performance degradation due to attack information correctness. Since meter selection algorithm such as EWMF needs the attack information, and l_1 approximated attack information can't feed the "best" information to meter selection algorithm so that it selects an improper meter to protect that optimal attackers need NOT to tamper with. Even though grid operator protects meters, that meter is nothing to do with optimal attack. Therefore, the same optimal attack strategy can always be launched. Otherwise, if we feed the best information to meter selection block, the selected to-be-protected meter are always in the list of optimal attack strategy. It will force attackers to change their attack strategy.

4.4 Experimental Results for Difference Objective Function of Protection Strategy

In this section, we simulate the interaction between attackers and grid operator. All meters in the smart grid network are unprotected initially. The optimal attack information is applied for both algorithms, and injection-free case is considered to ensure the optimal attack information. Protection strategy of IEEE 30, 57, 118 and 300 bus for both EWMF and Kim's algorithm are given.

To begin with, we introduce how to derive protection strategy using Kim's algorithm by several steps. Because optimal attack vector generator is applied for Kim's algorithm, Kim's algorithm is modify in Algorithm 4.

Table 4.2: The table of protection set for each N_A in IEEE 30 bus. $R_{N_A} = 20, r = 10$

N_A	$\mathcal{S}$	$\lvert\mathcal{S}\rvert$	$\min_k \alpha_k$
2	[ ]	0	2
3	[34,16,13]	3	4
4	[34,16,13]	3	4
5	[33,37,5,19,2,22,23,26,9,10,24,36,11,29,4,39,32,20,16,13,34]	21	6
6	[5,22,23,19,37,33,2,27,8,32,17,35,11,26,24,10,1,39,34,16,13]	21	6
7	[33,19,37,2,5,22,35,23,40,41,29,31,4,30,21,24,14,9,17,39,34,16,13]	23	8
8	[33,5,10,35,2,27,41,31,22,23,37,19,26,8,1,30,25,14,38,17,34,13,16]	23	8
9	[5,33,3,8,15,37,10,35,25,29,41,31,30,32,2,19,20,1,26,11,22,38,24,16,34,13]	26	12
10	[5,1,8,15,33,2,4,19,22,35,32,37,31,23,24,30,40,41,20,14,27,38,21,34,16,13]	26	12
11	[5,1,15,33,8,19,2,6,22,23,11,21,31,35,32,25,20,30,37,40,10,38,29,34,16,13]	26	12
12	[5,15,22,8,1,2,9,19,33,23,31,36,10,35,27,30,32,37,39,26,17,14,25,34,16,13]	26	12
13	[5,1,19,4,2,15,21,17,25,24,23,20,31,30,27,36,32,12,37,33,10,41,8,38,11,13,34,16]	28	16
14	[5,15,19,1,8,21,31,33,9,36,35,27,30,32,26,22,23,37,14,4,17,40,39,25,13,16,34]	27	14
15	[5,8,15,19,21,33,31,9,36,35,25,24,23,27,30,32,26,41,2,37,40,17,39,1,14,13,16,34]	28	20
16	[5,1,33,15,19,22,23,17,32,21,25,24,4,3,8,9,36,35,10,40,31,37,27,11,38,16,34,13]	28	16
17	[5,8,15,19,22,17,25,33,32,31,36,3,35,30,21,26,10,40,2,37,38,29,11,24,1,34,16,13]	28	20
18	[5,33,3,8,15,19,21,17,25,24,23,18,31,30,36,35,32,12,2,37,29,38,10,14,1,34,13,16]	28	18
19	[5,19,8,15,21,31,25,17,24,23,27,36,35,30,32,26,33,10,41,1,2,9,37,14,39,34,16,13]	28	20
20	[5,33,19,1,8,15,2,3,17,21,25,24,23,22,6,11,36,35,10,41,31,28,37,27,32,38,16,13,34]	29	∞

Table 4.3: The protection Strategy of Kim's algorithm selected from Table 4.2

N_A	$\mathcal{S}$	$\lvert\mathcal{S}\rvert$	$\min_k \alpha_k$
2	[ ]	0	2
3	[34,16,13]	3	4
5	[33,37,5,19,2,22,23,26,9,10,24,36,11,29,4,39,32,20,16,13,34]	21	6
7	[33,19,37,2,5,22,35,23,40,41,29,31,4,30,21,24,14,9,17,39,34,16,13]	23	8
9	[5,33,3,8,15,37,10,35,25,29,41,31,30,32,2,19,20,1,26,11,22,38,24,16,34,13]	26	12
14	[5,15,19,1,8,21,31,33,9,36,35,27,30,32,26,22,23,37,14,4,17,40,39,25,13,16,34]	27	14
15	[5,8,15,19,21,33,31,9,36,35,25,24,23,27,30,32,26,41,2,37,40,17,39,1,14,13,16,34]	28	20
20	[5,33,19,1,8,15,2,3,17,21,25,24,23,22,6,11,36,35,10,41,31,28,37,27,32,38,16,13,34]	29	∞

Algorithm 4 Modified subset selection algorithm [7]

```
Require: $N_A$, $\mathbf{H_r}$
Ensure: $\mathcal{S}$, $\min_k \alpha_k$
$\mathcal{S} = \emptyset$;
repeat
    $VulnerabilityArr$(1,...,$m$)=0;
    for $k = 1 \to m$ do
        given $\mathbf{H}_\mathbf{r}^{\mathcal{S}}$, find $\mathcal{A}_k$ and $\alpha_k = |\mathcal{A}_k|$ using MIN CUT;
        if $\alpha_k < N_A$ then
            $VulnerabilityArr(\mathcal{A}_k) \Leftarrow VulnerabilityArr(\mathcal{A}_k)$+1
        end if
    end for
    $l^* = \arg\max_l VulnerabilityArr(l)$ ;
    add $l^*$ to $\mathcal{S}$;
until $\min_k \alpha_k \geq N_A$
return $\mathcal{S}$, $\min_k \alpha_k$;
```

For each N_A, Algorithm 4 returns a protection set $\mathcal{S}$ and $\min_k \alpha_k$. Taking IEEE 30 bus as an example in table 4.2, we run 10 times for each N_A, i.e., $r = 10$, and choose the protection set with minimal protection size. R_{N_A} is set to 20. The meter index in protection set is in order. For the same cardinality of protection set, we choose the one with maximum $min_k \alpha_k$. The protection strategy is showed in Table 4.3. The performance is plotted in Fig. 4.13.

It is necessary to emphasize that the protection strategy doesn't follow continuous evolution. Each protection set for different protection size is independent. Take the table 4.3 as an example, when grid operator protect 21 meters $[33, 37, 5, 19, 2, 22, 23, 26, 9, 10, 24, 36, 11, 29, 4, 39, 3$ (in protection order), and the grid operator get the additional budget to continuously protect others. The next protection size is 23, and the protection set is [33, 19,37,2,5,22,35,23,40,41,29,31,4,30,21,24,14,9,17,39,34,16,13]. Grid operator can't simply additionally protect 2 meters to force number of minimal tampered meters $\min_k \alpha_k$ to 8, since the different elements between those two protection sets are $[14, 17, 21, 30, 31, 35, 40, 41]$ whose size is more than 2. In other words, protection strategy of Kim's algorithm doesn't support backward compatibility due to independence of each protection set.

We now illustrate the protection strategy evaluated by one-shot algorithm: EWMF. The protection strategy is simply $\mathcal{S}$ which follows continuous evolution. We illustrate the algorithm for IEEE 30 bus, and the corresponding protection set is [34, 13,16,5,19,2,22,37,23,33,21,1,11,40,29,38,36,8,17,24,32,31, 35,15,4,20,30,25,9] in protection order. The performance is plotted in Fig. 4.13. The advantages of EWMF are low computational complexity, support backward compatibility and continuality of protection strategy. Backward compatibility here is that the next protection set with protection size $k+1$ contain all the meters of the previous protection set with protection size k. Continuality of protection strategy means that the protection strategy exists for any given protection size, i.e. A in (4.2) has no restriction.

We furtherr consider modified Kim's algorithm so that the protection strategy of Kim's algorithm support backward compatibility. It can be done by evaluating the protection strategies steps by steps. In the beginning, we evaluate the protection strategy and select the protection set with protection size 3, where the true point is located, as the first point of incremental protection strategy of Kim's algorithm; the second protection strategy is derived based on those 3 protected meters, i.e., the following protection set must contain those 3 meters. Follow the same steps, we finally can calculate the incremental protection strategy of Kim's algorithm in Fig. 4.13. We observe that the gradual protection strategy has little performance degradation due to the backward compatibility constraint. Because the Kim's algorithm is not designed for continuous evolution, the time complexity of modified Kim's algorithm is extremely high.

Thirdly, we use brute force algorithm to find the best protection strategy for IEEE 14 bus. The protection sets for each protection size similar to Kim's algorithm is independent, i.e. it is not necessary that the next protection set with protection size $k+1$ contains all the meters of the previous protection set with protection size k. For each protection size of brute force algorithm, we try all combinations of protection set to find the protection set that forces attackers to manipulate most meters. It is desired to check

Table 4.4: The pros and cons of Kim's algorithm, incremental Kim and EWMF.

Feature	Kim's algorithm	incremental Kim	EWMF
time complexity	High	High	Low
backward compatibility	No	Yes	Yes
strategy continuality	No	No	Yes

Table 4.5: Time complexity for each case under the PC with 3.33GHz quad-core CPU and 16G memory.$R_{N_A} = 20, r = 10$

Case / (sec)	Kim	incremental Kim	EWMF	EWMF 100 times
case 30	44.3445	113.5589	0.3396	29.8138
case 57	223.1978	621.8101	1.5318	158.8618
case 118 ($R_{N_A} = 20$)	1.3208×10^3	3.5016×10^3	9.8351	982.2705
case 118($R_{N_A} = 80$)	7.5740×10^3	2.4457×10^4	9.8351	982.2705
case 300 ($R_{N_A} = 20$)	9.3500×10^3	2.2437×10^4	63.2345	6.444×10^3
case 300($R_{N_A} = 80$)	6.2653×10^4	1.4503×10^5	63.2345	6.444×10^3

the gap of restriction between the Kim's algorithm, EWMF and brute force algorithm. It is show in Fig. 4.12 that all of them can provide the same restriction. Furthermore, the protection strategy of EWMF provides low time complexity, backward compatibility and continuality of protection strategy. Comparing to brute force algorithm, EWMF selects a meter at a time rather than all meter at once; the time complexity is significantly reduced, and the performance is the same as brute force algorithm in IEEE 14 bus.

Finally, we compare two meter selection algorithms with optimal attack information for IEEE 57,118 and 300 bus in Fig. 4.14-4.17. The performance of EWMF is almost near that of Kim's algorithm for each case. The pros and cons of all algorithms are concluded in table. 4.4-4.5. Note that the restriction provided by Kim's algorithm depends on R_{N_A}. when R_{N_A} is set to large number, the high restriction will be calculated.

4.5 Position of Injection-free Case

Protection strategy, which protects branch meters only, is evaluated using WMF in injection-free case. The nature question is that if the operator can adopt the protection strategy to real world? The answer is affirmative, and we guarantee that attackers need to manipulate more meters. To complete the proof, we define several matrixes. Let $\mathbf{H}_{\mathrm{r}}^{\mathrm{B}}$ be the Jacobian matrix of branch meters in all transmission lines, $\mathbf{H}_{\mathrm{r}}^{\mathrm{I,all}}$ be the Jacobian matrix of injection meters in all buses, i.e., $P_1 = P_2 = \mathbf{0}$ and $P_3 = \mathbf{0}$, and $\mathbf{H}_{\mathrm{r}}^{\mathrm{I,gen}}$ be the Jacobian matrix of injection meters in buses connecting to the generation. Define the Jacobian matrix in real world case as

$$\mathbf{H}_{\mathrm{r}}^{\mathrm{R}} = \begin{bmatrix} \mathbf{H}_{\mathrm{r}}^{\mathrm{B}} \\ \mathbf{H}_{\mathrm{r}}^{\mathrm{I,gen}} \end{bmatrix}, \tag{4.3}$$

i.e., $P_1 = P_2 = I_{m_a}$ and P_3 depends on the bus located at generations, and in injection-free case as

$$\mathbf{H}_{\mathrm{r}}^{\mathrm{N}} = \begin{bmatrix} \mathbf{H}_{\mathrm{r}}^{\mathrm{B}} \end{bmatrix}, \tag{4.4}$$

i.e., $P_1 = P_2 = I_{m_a}$ and $P_3 = \mathbf{0}$ depends on the bus located at generations. Let $\mathcal{S}$ be a protection set, which is one of any possible combinations of all meters in the network and $\mathcal{P}$ be a protection set, which is one of any possible combinations of branch meters in the network, where $\mathcal{S} \subseteq \mathcal{M}$, $\bar{\mathcal{S}} = \mathcal{M} \setminus \mathcal{S}$, $\mathcal{P} \subseteq \mathcal{M}^{\mathrm{B}}$, and $\bar{\mathcal{P}} = \mathcal{M}^{\mathrm{B}} \setminus \mathcal{P}$. We define security index in each case. The $\mathcal{S}$-security index of kth meter in real world case is

$$\begin{aligned} \alpha_k^{\mathrm{R}}(\mathcal{S}) = \min_{\mathbf{c}_{\mathrm{r}} \in \mathbb{R}^n} \quad & ||\mathbf{H}_{\mathrm{r}}^{\mathrm{R}\bar{\mathcal{S}}} \mathbf{c}_{\mathrm{r}}||_0 \\ s.t. \quad & \mathbf{H}_{\mathrm{r}}^{\mathrm{R}\mathcal{S}} \mathbf{c}_{\mathrm{r}} = \mathbf{0} \\ & \mathbf{H}_{\mathrm{r}}^{\mathrm{R}}(k,:) \mathbf{c}_{\mathrm{r}} = 1. \end{aligned} \tag{4.5}$$

Replacing the constraints in (4.5) we derive $\mathcal{P}$-security index of the kth meter for a practical power grid

$$\begin{aligned} \alpha_k^{\mathrm{R}}(\mathcal{P})' = \min_{\mathbf{c}_{\mathrm{r}} \in \mathbb{R}^n} \quad & ||\mathbf{H}_{\mathrm{r}}^{\mathrm{R}\bar{\mathcal{P}}} \mathbf{c}_{\mathrm{r}}||_0 \\ s.t. \quad & \mathbf{H}_{\mathrm{r}}^{\mathrm{N}\mathcal{P}} \mathbf{c}_{\mathrm{r}} = \mathbf{0} \\ & \mathbf{H}_{\mathrm{r}}^{\mathrm{N}}(k,:) \mathbf{c}_{\mathrm{r}} = 1. \end{aligned} \tag{4.6}$$

Define $\mathcal{P}$-security index of the kth meter in the injection-free case as

$$\begin{aligned} \alpha_k^{\mathrm{N}}(\mathcal{P}) = \min_{\mathbf{c}_{\mathrm{r}}\in\mathbb{R}^n} \quad & ||\mathbf{H}_{\mathrm{r}}^{\mathrm{N}\bar{\mathcal{P}}}\mathbf{c}_{\mathrm{r}}||_0 \\ s.t. \quad & \mathbf{H}_{\mathrm{r}}^{\mathrm{N}\mathcal{P}}\mathbf{c}_{\mathrm{r}} = \mathbf{0} \\ & \mathbf{H}_{\mathrm{r}}^{\mathrm{N}}(k,:)\mathbf{c}_{\mathrm{r}} = 1. \end{aligned} \tag{4.7}$$

With the same protection strategy, we want to show that attackers need to manipulate more meters in real world case than in injection-free case, i.e., $\min_{k\in\mathcal{M}\setminus\mathcal{P}} \alpha_k^{\mathrm{R}}(\mathcal{P}) \geq \min_{k\in\bar{\mathcal{P}}} \alpha_k^{\mathrm{N}}(\mathcal{P}), \forall\mathcal{P}$.

Lemma 2. *The best attack strategy in real world case can be selected only from $\mathcal{S}$-security index of branch meters.*

$$\min_{k\in\bar{\mathcal{S}}} \alpha_k^{\mathrm{R}}(\mathcal{S}) = \min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{S}), \forall\mathcal{S} \tag{4.8}$$

***Proof*.** It is obviously that $\min_{k\in\bar{\mathcal{S}}} \alpha_k^{\mathrm{R}}(\mathcal{S}) = \min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{S}), \forall\mathcal{S}$, if and only if

$$\min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{I}}} \alpha_k^{\mathrm{R}}(\mathcal{S}) \geq \min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{S}) \tag{4.9}$$

It is easier to prove (4.9) than (4.8). Therefore, we prove (4.9) by contradiction. Assume $\min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{I}}} \alpha_k^{\mathrm{R}}(\mathcal{S}) < \min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{S})$.

Then there exists at least one injection meter so that it's security index is minimal. Let the minimal one be $k_{\min}^{\mathrm{I}} \in \bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{I}}$ such that $\alpha_{k_{\min}^{\mathrm{I}}}^{\mathrm{R}}(\mathcal{S}) < \min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{S})$.

Let $\mathbf{c}_{\mathrm{r,min}}^{\mathrm{I}}$ be optimal solution of $\alpha_{k_{\min}^{\mathrm{I}}}^{\mathrm{R}}(\mathcal{S})$. $\because rank(\mathbf{H}_{\mathrm{r}}^{\mathrm{B}}) = n \therefore \mathbf{H}_{\mathrm{r}}^{\mathrm{B}}\mathbf{c}_{\mathrm{r,min}}^{\mathrm{I}} \neq \mathbf{0}$. This implies that if attackers want to manipulate $k_{\min}^{\mathrm{I}}$th injection meter, they must manipulate at least one branch meter.

Let one of branch meter in attack set $\mathcal{A}_{k_{\min}^{\mathrm{I}}}^{\mathrm{R}}(\mathcal{S})$ be $k_*^{\mathrm{B}} \in \bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}$ and $\mathbf{c}_{\mathrm{r},*}^{\mathrm{B}}$ be optimal solution of $\alpha_{k_*^{\mathrm{B}}}^{\mathrm{R}}(\mathcal{S})$. $\because ||\mathbf{H}_{\mathrm{r}}^{\mathrm{R}}\mathbf{c}_{\mathrm{r,min}}^{\mathrm{I}}||_0 = \alpha_{k_{\min}^{\mathrm{I}}}^{\mathrm{R}}(\mathcal{S}) < \min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{S})$ and $\min_{k\in\bar{\mathcal{S}}\cap\mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{S}) \leq \alpha_{k_*^{\mathrm{B}}}^{\mathrm{R}}(\mathcal{S}) = ||\mathbf{H}_{\mathrm{r}}^{\mathrm{R}}\mathbf{c}_{\mathrm{r},*}^{\mathrm{B}}||_0$. We can obtain that $||\mathbf{H}_{\mathrm{r}}^{\mathrm{R}}\mathbf{c}_{\mathrm{r,min}}^{\mathrm{I}}||_0 < \alpha_{k_*^{\mathrm{B}}}^{\mathrm{R}}(\mathcal{S}) = ||\mathbf{H}_{\mathrm{r}}^{\mathrm{R}}\mathbf{c}_{\mathrm{r},*}^{\mathrm{B}}||_0$, which conflicts with that $\mathbf{c}_{\mathrm{r},*}^{\mathrm{B}}$ is optimal solution of $\alpha_{k_*^{\mathrm{B}}}^{\mathrm{R}}(\mathcal{S})$ □

Corollary 1. *The constraint sets of* (4.5) *and* (4.6) *are the same,* $\forall k \in \bar{\mathcal{P}}, \forall \mathcal{P}$*. Therefore,*

$$\alpha_k^{\mathrm{R}}(\mathcal{P}) = \alpha_k^{\mathrm{R}}(\mathcal{P})', \forall k \in \bar{\mathcal{P}}, \tag{4.10}$$

which implies

$$\min_{k \in \bar{\mathcal{P}}} \alpha_k^{\mathrm{R}}(\mathcal{P}) = \min_{k \in \bar{\mathcal{P}}} \alpha_k^{\mathrm{R}}(\mathcal{P})', \forall \mathcal{P}. \tag{4.11}$$

Lemma 3. *The* $\mathcal{P}$*-security index of* k*th branch meter in real world case is always greater or equal to that in injection-free case,* $\forall k \in \bar{\mathcal{P}}, \forall \mathcal{P}$*.*

$$\alpha_k^{\mathrm{R}}(\mathcal{P})' \geq \alpha_k^{\mathrm{N}}(\mathcal{P}), \forall k \in \bar{\mathcal{P}}, \forall \mathcal{P}. \tag{4.12}$$

Proof. We prove by contradiction.

Assume $\alpha_k^{\mathrm{R}}(\mathcal{P})' < \alpha_k^{\mathrm{N}}(\mathcal{P}), \forall k \in \bar{\mathcal{P}}$.

Let $\mathbf{c}_{\mathrm{r},k}^{\mathrm{R}}$ be optimal solution of $\alpha_k^{\mathrm{R}}(\mathcal{S})'$, $\forall k \in \bar{\mathcal{P}}$. $\alpha_k^{\mathrm{R}}(\mathcal{S})' = ||\mathbf{H}_{\mathrm{r}}^{\mathrm{R}}\mathbf{c}_{\mathrm{r},k}^{\mathrm{R}}||_0 = ||\mathbf{H}_{\mathrm{r}}^{\mathrm{B}}\mathbf{c}_{\mathrm{r},k}^{\mathrm{R}}||_0 + ||\mathbf{H}_{\mathrm{r}}^{\mathrm{I,gen}}\mathbf{c}_{\mathrm{r},k}^{\mathrm{R}}||_0 \geq ||\mathbf{H}_{\mathrm{r}}^{\mathrm{B}}\mathbf{c}_{\mathrm{r},k}^{\mathrm{R}}||_0 = ||\mathbf{H}_{\mathrm{r}}^{\mathrm{N}}\mathbf{c}_{\mathrm{r},k}^{\mathrm{R}}||_0$.

Let $\mathbf{c}_{\mathrm{r},k}^{\mathrm{N}}$ be optimal solution of $\alpha_k^{\mathrm{N}}(\mathcal{P})$, $\forall k \in \bar{\mathcal{P}}$. The contradiction is that $||\mathbf{H}_{\mathrm{r}}^{\mathrm{N}}\mathbf{c}_{\mathrm{r},k}^{\mathrm{R}}||_0 \leq \alpha_k^{\mathrm{R}}(\mathcal{P})' < \alpha_k^{\mathrm{N}}(\mathcal{P}) = ||\mathbf{H}_{\mathrm{r}}^{\mathrm{N}}\mathbf{c}_{\mathrm{r},k}^{\mathrm{N}}||_0$, since $\mathbf{c}_{\mathrm{r},k}^{\mathrm{N}}$ is not optimal solution of $\alpha_k^{\mathrm{N}}(\mathcal{P})$. □

Theorem 4. $\mathcal{P}$ *be a protection set which can be one of any possible combinations of branch meters in the network, i.e.,* $\mathcal{P} \subseteq \mathcal{M}^{\mathrm{B}}$*,* $\mathcal{M}^{\mathrm{B}}$ *be universal set,* $\bar{\mathcal{P}}$ *be complement of* $\mathcal{P}$*, i.e.,* $\bar{\mathcal{P}} = \mathcal{M}^{\mathrm{B}} \setminus \mathcal{P}$*.* $\alpha_k^{\mathrm{R}}(\mathcal{P})$ *and* $\alpha_k^{\mathrm{N}}(\mathcal{P})$ *are the* $\mathcal{P}$*-security index of* k*th meter in real world case and in injection-free case respectively. The following inequality is always true.*

$$\min_{k \in \mathcal{M} \setminus \mathcal{P}} \alpha_k^{\mathrm{R}}(\mathcal{P}) \geq \min_{k \in \bar{\mathcal{P}}} \alpha_k^{\mathrm{N}}(\mathcal{P}), \forall \mathcal{P}. \tag{4.13}$$

Proof. According to **Lemma** 2, we only discuss on $\mathcal{P}$:

$$\min_{k \in \mathcal{M} \setminus \mathcal{P}} \alpha_k^{\mathrm{R}}(\mathcal{P}) = \min_{k \in (\mathcal{M} \setminus \mathcal{P}) \cap \mathcal{M}^{\mathrm{B}}} \alpha_k^{\mathrm{R}}(\mathcal{P}) = \min_{k \in \bar{\mathcal{P}}} \alpha_k^{\mathrm{R}}(\mathcal{P}), \forall \mathcal{P}. \tag{4.14}$$

Note that $\mathcal{P} \subseteq \mathcal{M}^{\mathrm{B}} \subseteq \mathcal{M}$ and $\mathcal{S} \subseteq \mathcal{M}$, i.e., $\mathcal{S}$ contains all possibility of $\mathcal{P}$. Therefore, (4.14) is always true.

From **Corollary** 1, we have

$$\min_{k\in\mathcal{M}\setminus\mathcal{P}} \alpha_k^{\mathrm{R}}(\mathcal{P}) = \min_{k\in\bar{\mathcal{P}}} \alpha_k^{\mathrm{R}}(\mathcal{P}) = \min_{k\in\bar{\mathcal{P}}} \alpha_k^{\mathrm{R}}(\mathcal{P})', \forall\ \mathcal{P}, \tag{4.15}$$

Lemma 3 implies

$$\min_{k\in\bar{\mathcal{P}}} \alpha_k^{\mathrm{R}}(\mathcal{P})' \geq \min_{k\in\bar{\mathcal{P}}} \alpha_k^{\mathrm{N}}(\mathcal{P}), \forall\ \mathcal{P}. \tag{4.16}$$

From (4.15) and (4.16), we obtain

$$\min_{k\in\mathcal{M}\setminus\mathcal{P}} \alpha_k^{\mathrm{R}}(\mathcal{P}) \geq \min_{k\in\bar{\mathcal{P}}} \alpha_k^{\mathrm{N}}(\mathcal{P}), \forall\mathcal{P}.$$

□

(4.13) indicates that applying the protection strategy of WMF in a practical power grid can force FDIA attackers to manipulate more meters than in a injection-free network. The full measurement case corresponds to the special case when all buses have generator attached. Therefore, (4.13) can be easily extended to the full measurement case and other practical cases. Note that each protection set $\mathcal{P}$ in the WMF protection strategy satisfies $\mathcal{P} \subseteq \mathcal{M}^{\mathrm{B}}$, since it does not protect injection meters.

If an operator has the knowledge to determine the protection strategy including injection meters, the restriction become further stronger. The explanation is as follow. Given a protection size A, let $\mathcal{S}$ and $\mathcal{P}$ be one of any possible combinations of all meters and branch meters only respectively such that $|\mathcal{S}| = |\mathcal{P}| = A$. It can be observed that $\min_k \alpha_k^{\mathrm{R}}(\mathcal{S}) \geq \min_k \alpha_k^{\mathrm{R}}(\mathcal{P})$, since the constraint diversity in former case is plentiful for grid operator, and operator has more choices to select a set of stricter constraints indicated by $\mathcal{S}$ to maximize $\min_k \alpha_k^{\mathrm{R}}(\mathcal{S})$.

4.6 Near Optimal Attack Vector for Practical Power Grid

The method to derive optimal attack vector is only in injection-free case. In this section, the near optimal attack vector in real world case which considers injection meters is illustrated. To derive such attack vector, we propose the following steps:

1. derive the shift vector $\hat{\mathbf{c}}_{\mathrm{r},k}(\mathcal{P})$ in injection-free case $(\mathbf{H}_{\mathrm{r}}^{\mathrm{N}})$

2. derive the attack vector $\mathbf{a}_k^{\mathrm{R}}(\mathcal{P})$ in real world case by

$$\mathbf{a}_k^{\mathrm{R}}(\mathcal{P}) = \mathbf{H}_{\mathrm{r}}^{\mathrm{R}}\hat{\mathbf{c}}_{\mathrm{r},k}(\mathcal{P}), \forall k \in \bar{\mathcal{P}} \tag{4.17}$$

3. select the sparest attack vector from (4.17) as the attack strategy in real world case.

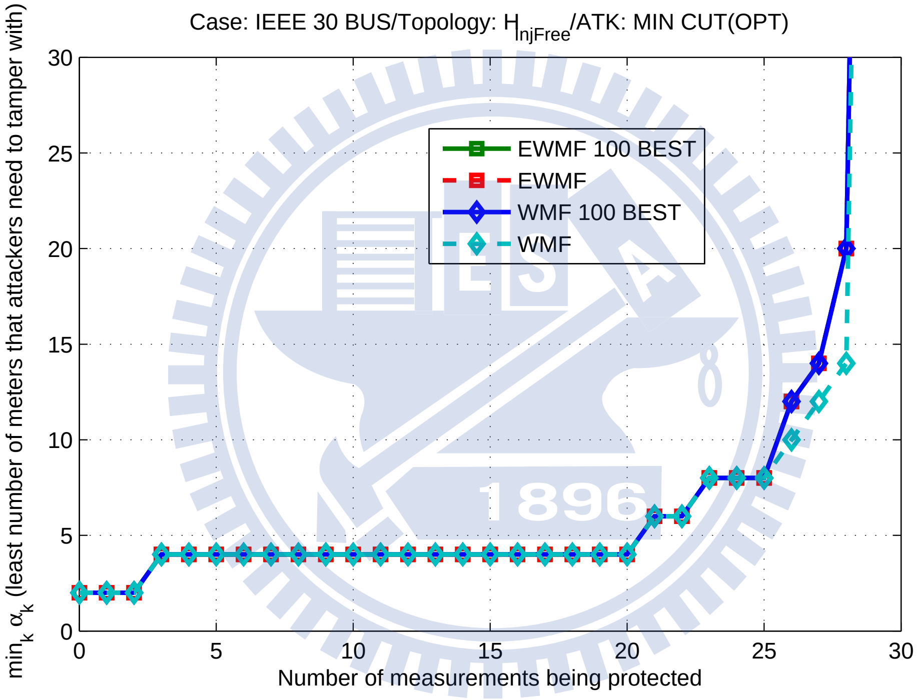

Figure 4.3: The performance of the protection strategies using WMF and EWMF respectively for case 30.

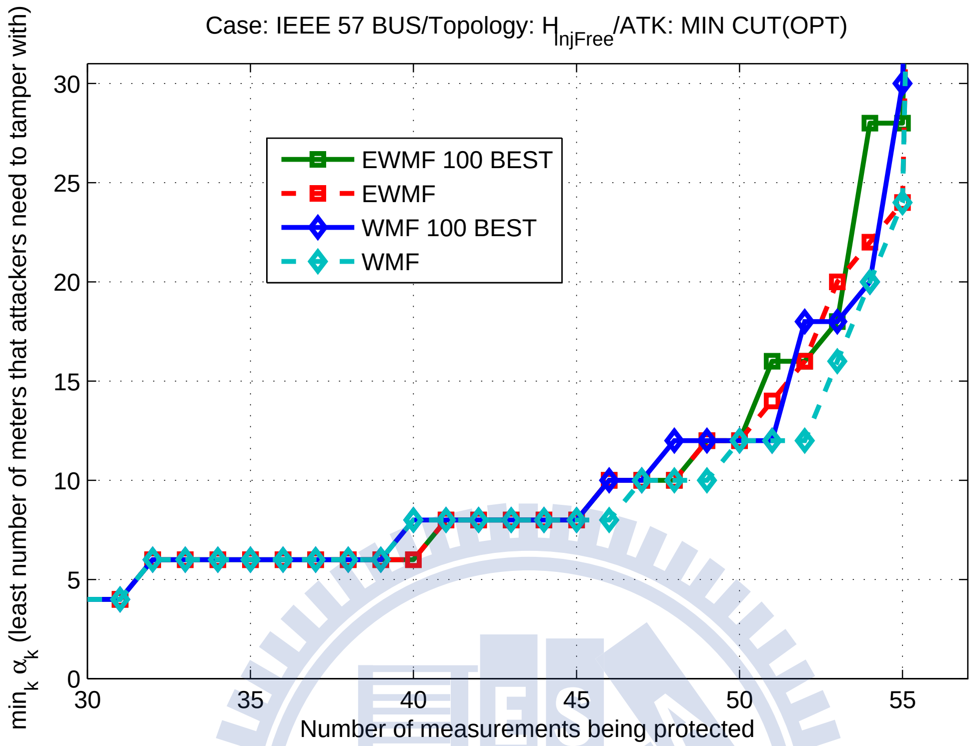

Figure 4.4: The performance of the protection strategies using WMF and EWMF respectively for case 57.

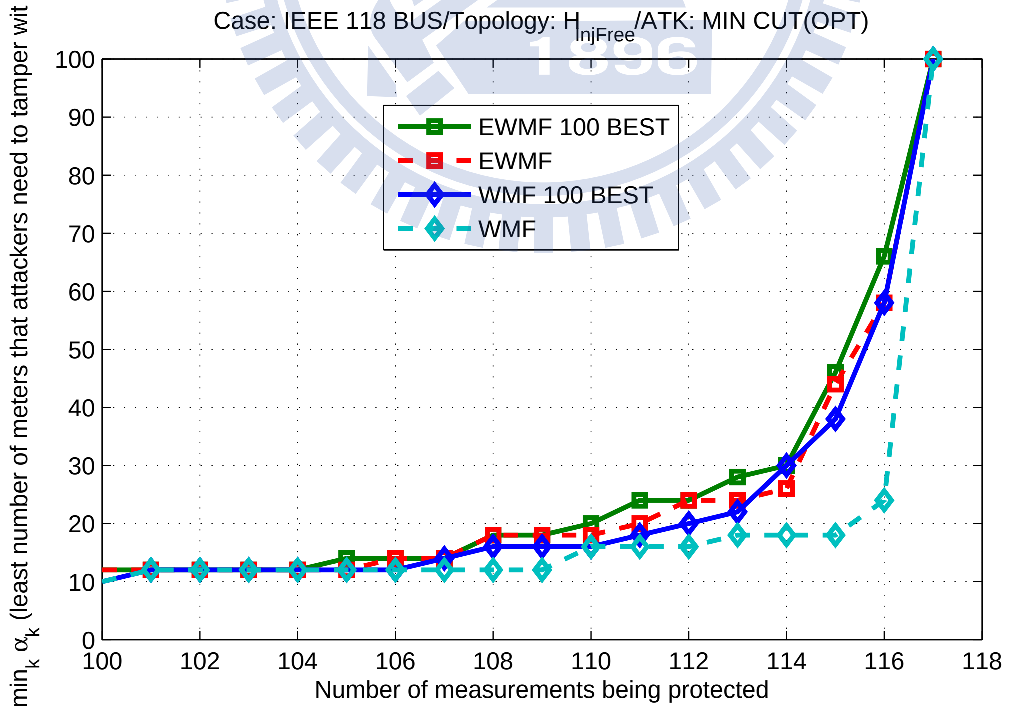

Figure 4.5: The performance of the protection strategies using WMF and EWMF respectively for case 118.

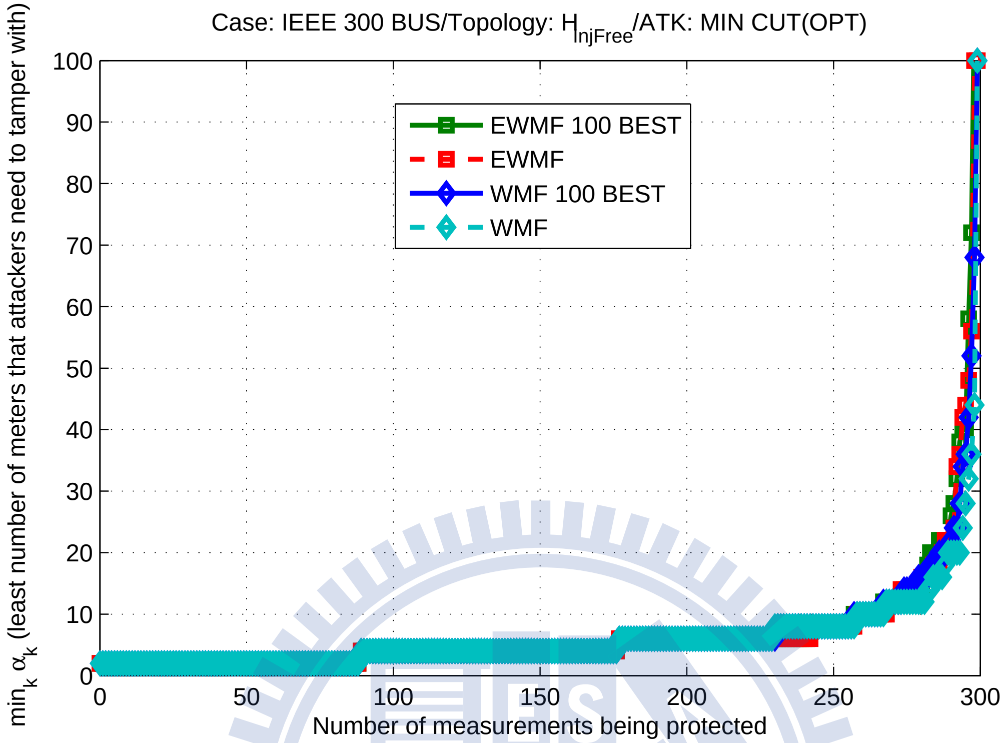

Figure 4.6: The performance of the protection strategies using WMF and EWMF respectively for case 300.

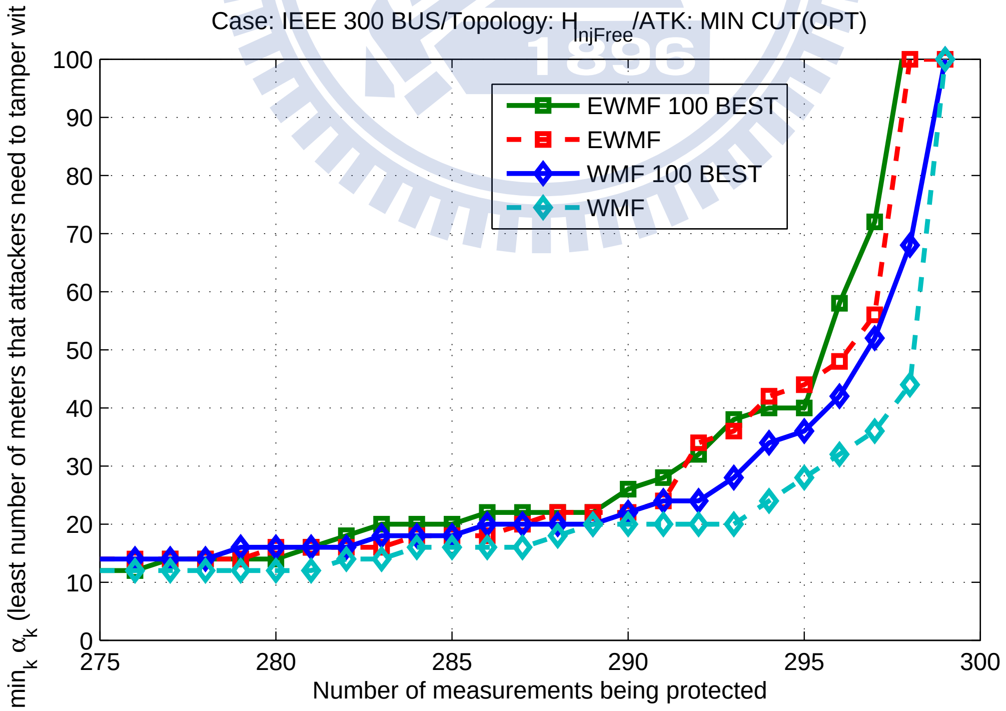

Figure 4.7: The performance of the protection strategies using WMF and EWMF respectively for case 300.

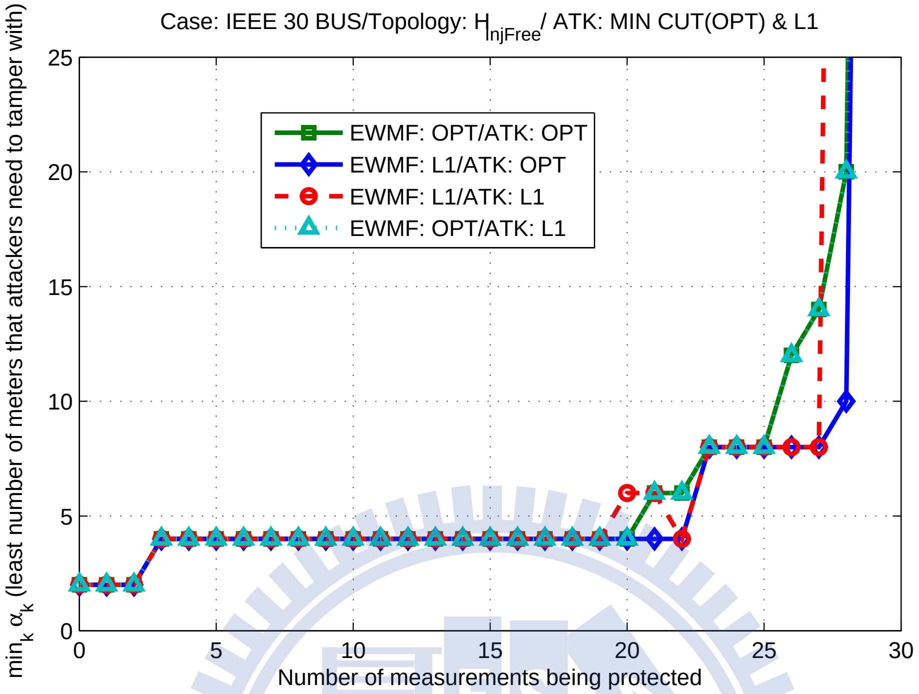

Figure 4.8: The performance of the protection strategies using optimal attack information and l_1 approximated attack information for case 30.

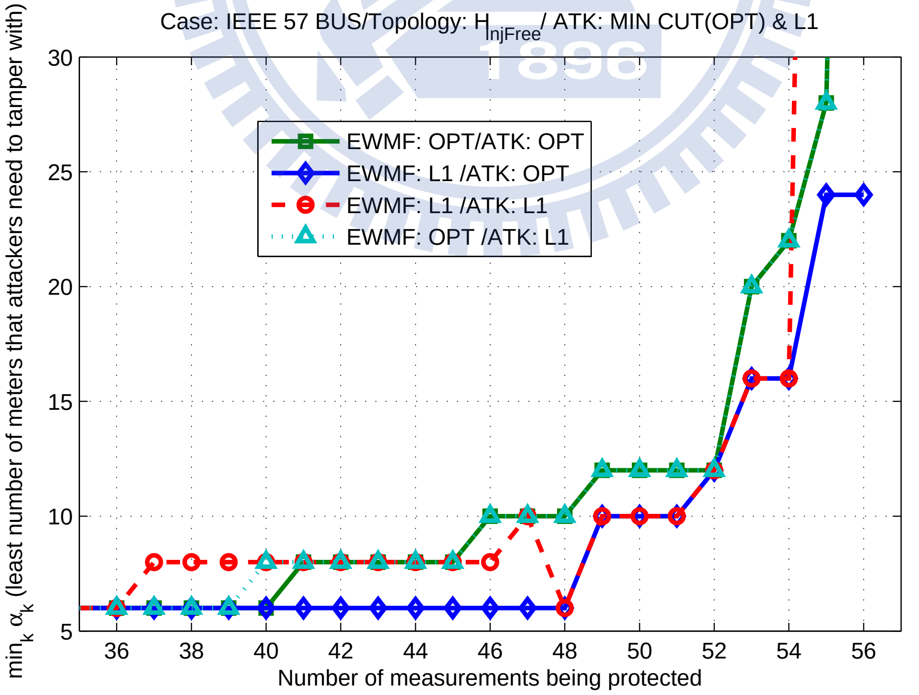

Figure 4.9: The performance of the protection strategies using optimal attack information and l_1 approximated attack information for case 57.

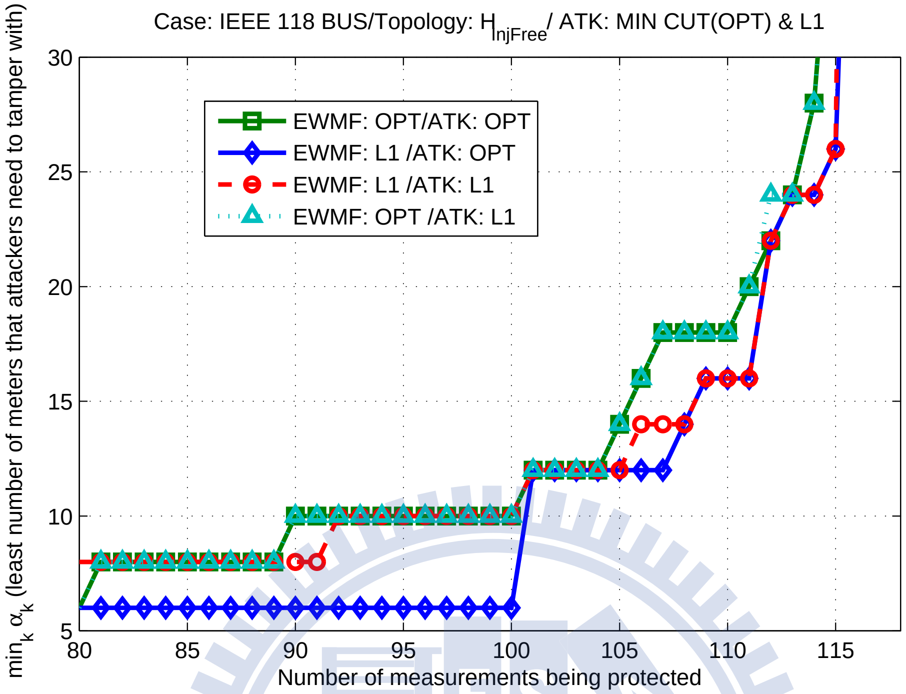

Figure 4.10: The performance of the protection strategies using optimal attack information and l_1 approximated attack information for case 118.

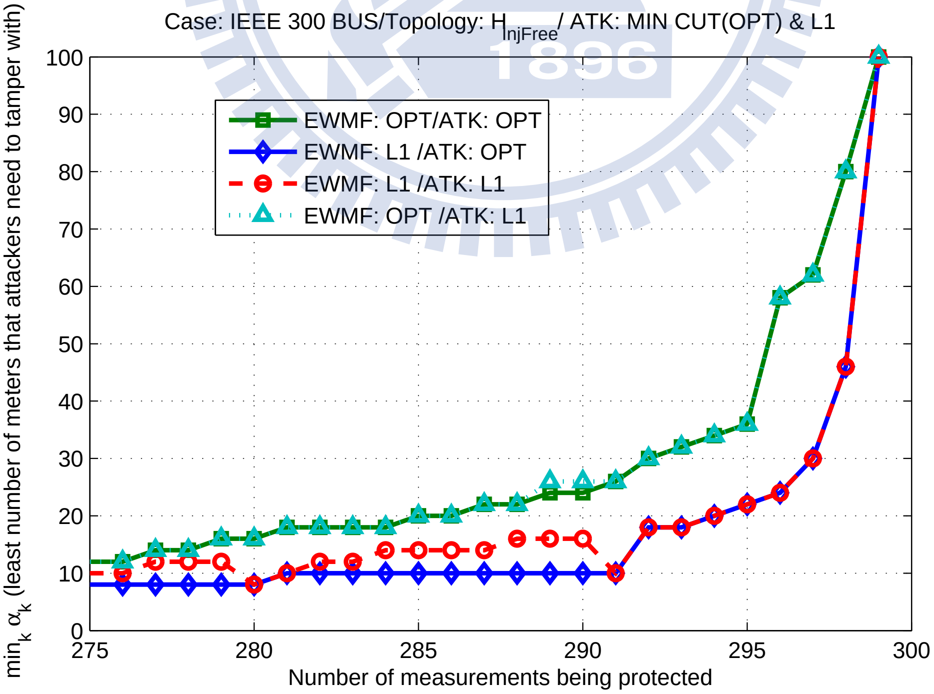

Figure 4.11: The performance of the protection strategies using optimal attack information and l_1 approximated attack information for case 300.

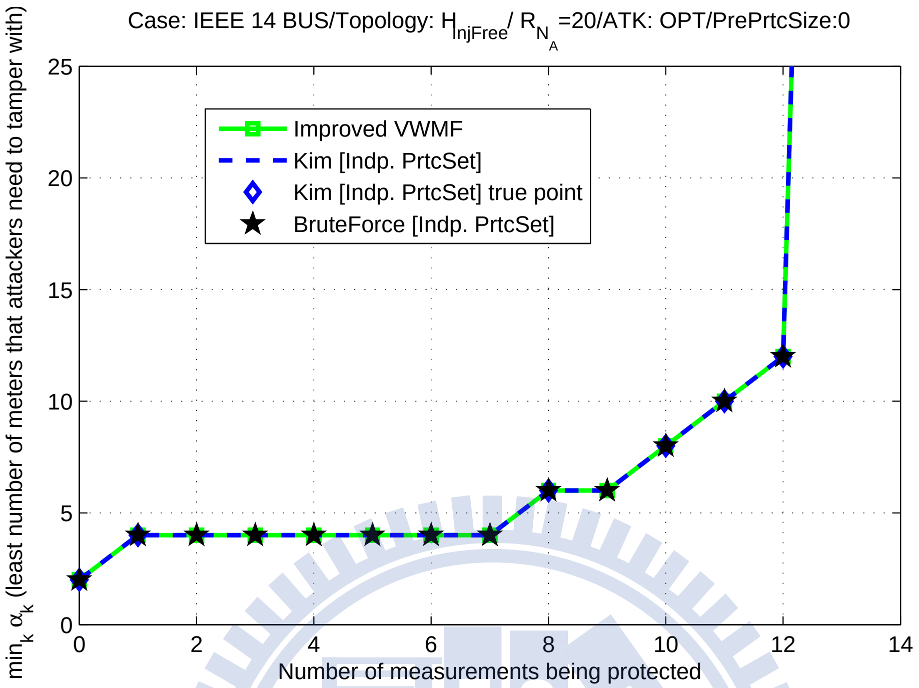

Figure 4.12: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 14. The protection strategy of brute force algorithm is added for comparison.

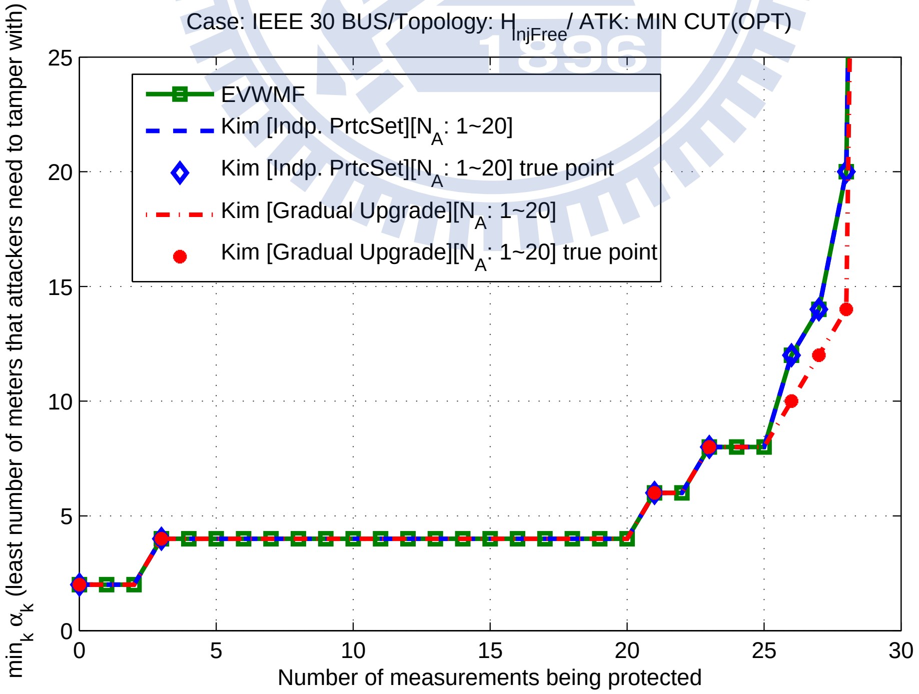

Figure 4.13: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 30. $R_{N_a} = 20, r = 10$

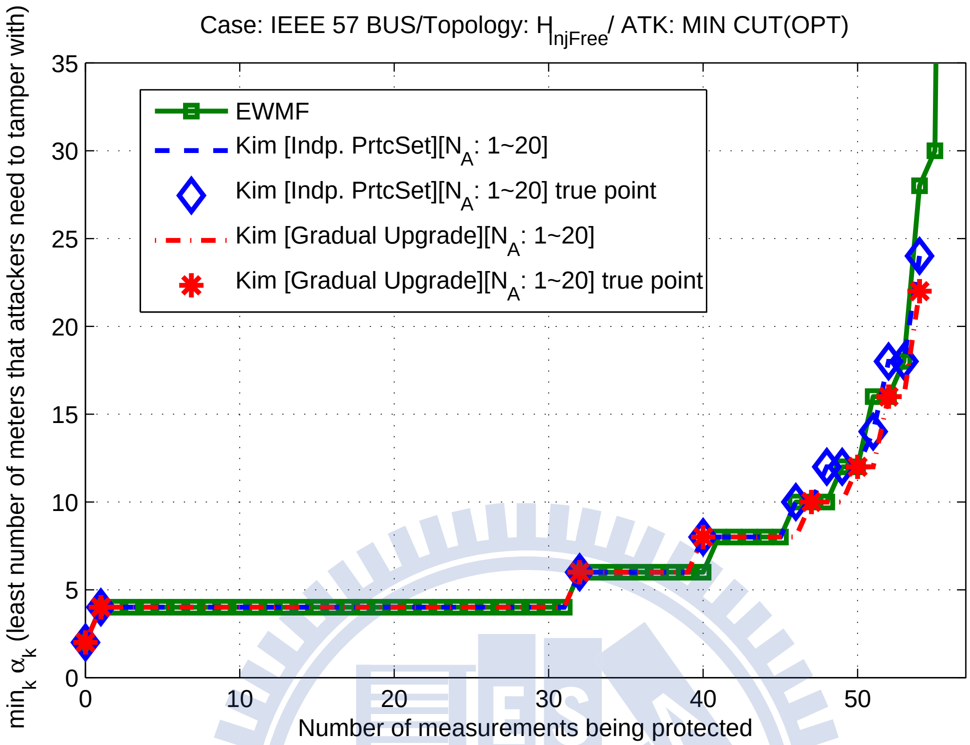

Figure 4.14: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 57. $R_{N_a} = 20, r = 10$

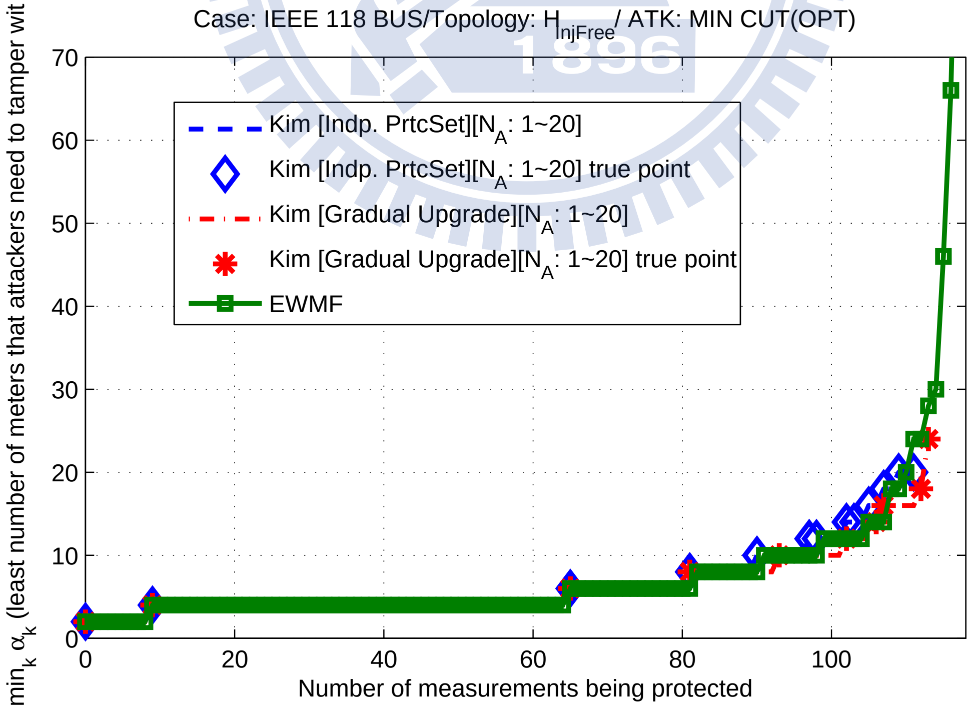

Figure 4.15: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 118. $R_{N_a} = 20, r = 10$

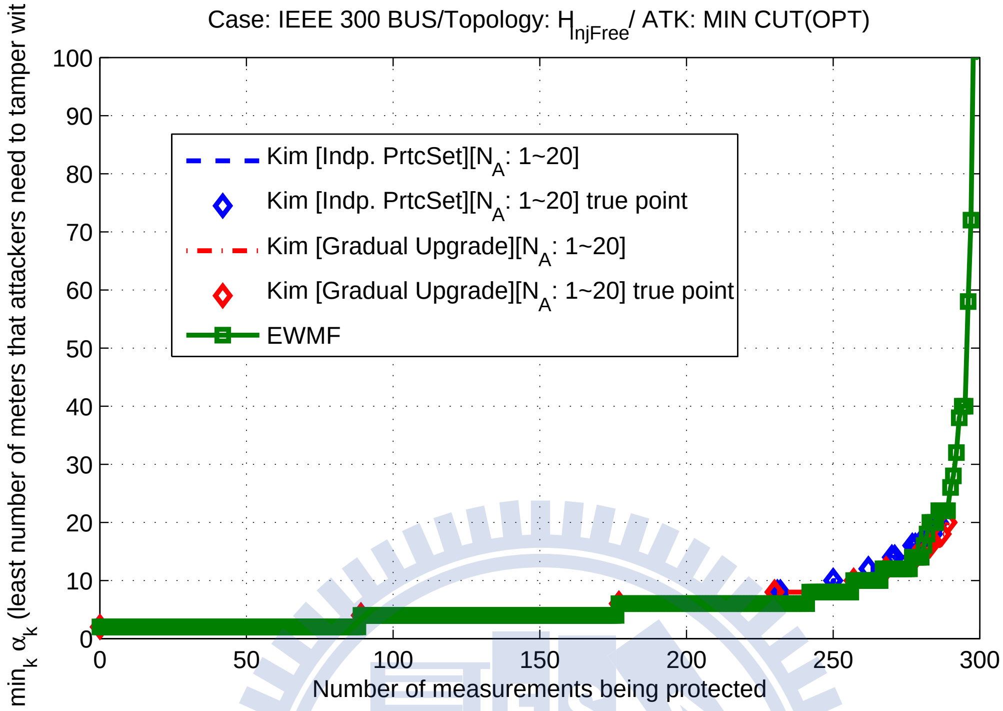

Figure 4.16: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 300. $R_{N_a} = 20, r = 10$

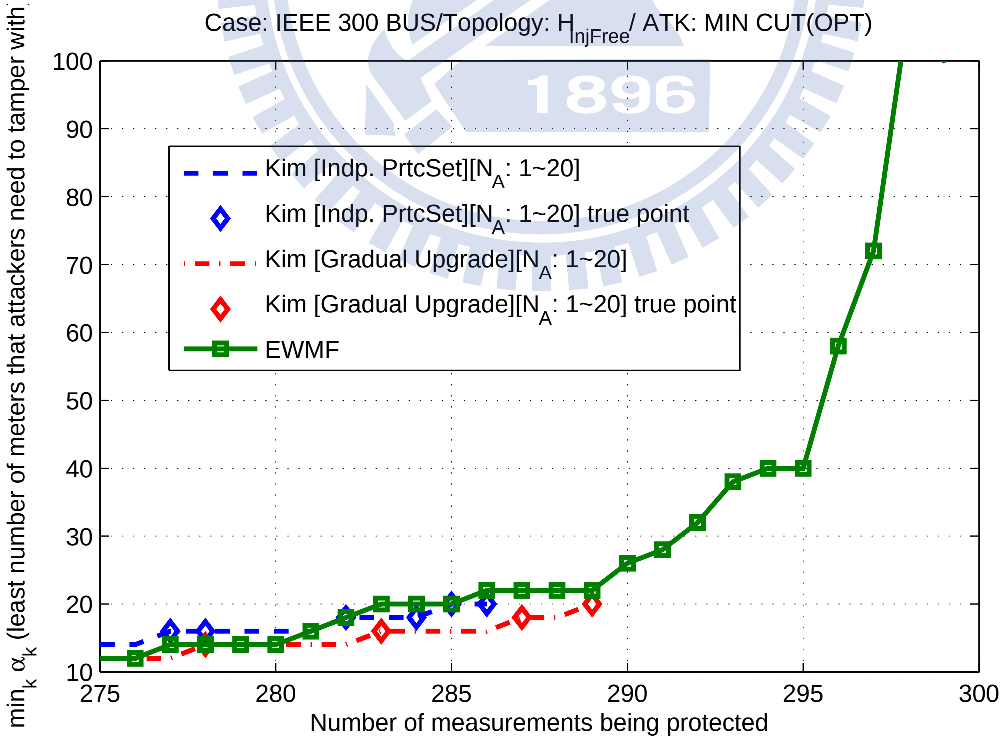

Figure 4.17: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 300. $R_{N_a} = 20, r = 10$

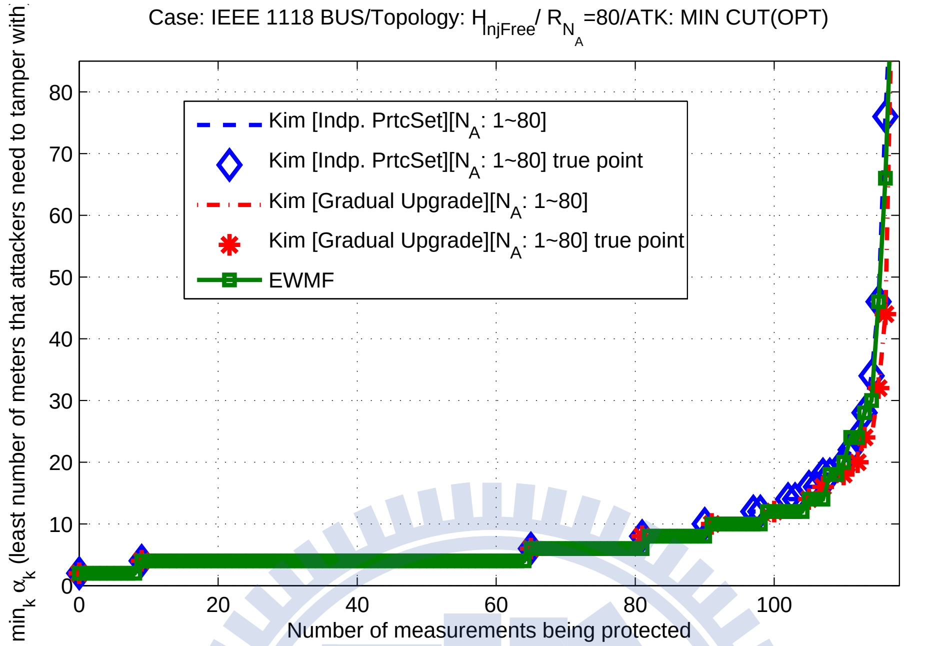

Figure 4.18: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 118. $R_{N_a} = 80, r = 10$

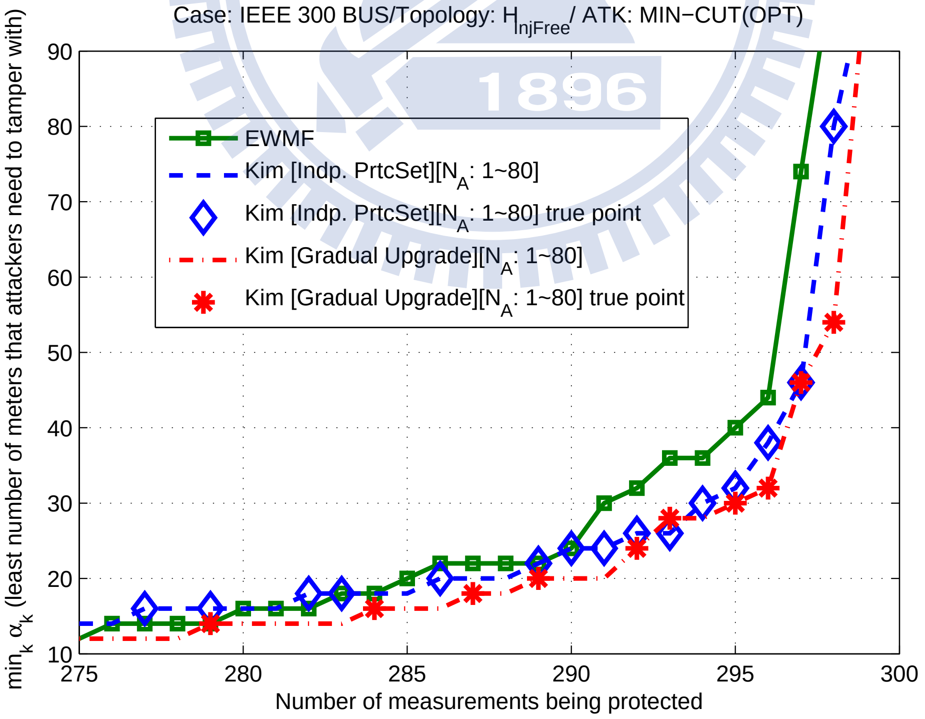

Figure 4.19: The performance of the protection strategies using Kim's algorithm and EWMF respectively in case 300. $R_{N_a} = 80, r = 10$

Chapter 5

Conclusion

5.1 Summary of Major Results

In this thesis, we consider the game between a CM called FDIA against state estimation of power grids and the corresponding CCM adopted by the grid operator. We define the $\mathcal{S}$-security index of a grid node and formulate the FDIA as an equivalence to the attack problem of [7]. Although both optimization problems are generally NP-hard, we manage to solve them for injection-free networks. Based on injection-free assumption, the performance of an optimal attack is evaluated via computer simulations on IEEE-standardized power networks. On the other hand, the counter counter-measures strategy is designed on a max-min formulation. We propose a incremental-based algorithm which selects the most vulnerable meter, one at a time, for protection. We prove that our CCM strategy guarantee a lower bound on the minimum number of measurements with which an FDIA has to tamper to pass the BDD test in any practical power grid. The numerical performance for IEEE 30, 57, 118 and 300 case is provided to validate the proposed approach.

5.2 Future Works

We have presented a practical solution for a grid operator to select protected measurements if it not feasible to protect all critical meters from a worst-case perspective. There remain many related issues that needed to be addressed. First of all, as we adopt an incremental approach, no general optimality for a fixed protected subset size can be claimed. For a practical power network with injection and branch meters, our scheme ensures a lower bound on the attacker's "cost" but not the maximum cost. Moreover, other CM objectives such as maximum attack impact can be evaluated and the AC model which is more realistic should be considered. Finally, phasor measurement unit (PMU) placement should be considered jointly to enhance the network security by forcing an attacker to gather more network information and increasing its computing requirement.

Table 1: Glossary

k	the number of tampered sensors (meters, measurements)
m_a	the number of directed arcs
m	the number of measurements (meters)
n	the number of state variables, note that number of buses is $(n+1)$
$\mathbf{H}$	$m \times (n+1)$ Jacobian matrix representing the topology
$\mathbf{H}_\mathrm{r}$	$m \times n$ matrix derived by removing last column of $\mathbf{H}$
$\mathbf{x}_\mathrm{r}$	$n \times 1$ vector of state variables
$\mathbf{x}$	$(n+1) \times 1$ vector derived by adding zero to tail of $\mathbf{x}_\mathrm{r}$, note that $\mathbf{Hx} = \mathbf{H}_\mathrm{r}\mathbf{x}_\mathrm{r}$
$\mathbf{z}$	$m \times 1$ vector of measurements
$\mathbf{e}$	$m \times 1$ vector of measurements errors, s.t., $\mathbf{z} = \mathbf{Hx} + \mathbf{e}$
$\hat{\mathbf{x}}_\mathrm{r}$	$n \times 1$ vector of estimated state variables, note that $\hat{\mathbf{x}}_\mathrm{r} = (\mathbf{H}_\mathrm{r}^T\mathbf{R}^{-1}\mathbf{H}_\mathrm{r})^{-1}\mathbf{H}_\mathrm{r}^T\mathbf{R}^{-1}\mathbf{z}$
$\mathbf{R}$	$m \times m$ diagonal covariance matrix, s.t., $r_{i,i} = \sigma_i^2$, where σ_i^2 is the variance of the ith measurement $(1 \leq i \leq m)$
τ	Threshold for the L_2-norm based detection of bad measurements
$\mathbf{z_a}$	$m \times 1$ measurement vector with bad measurements
$\mathbf{a}$	$m \times 1$ attack vector, s.t., $\mathbf{z_a} = \mathbf{z} + \mathbf{a}$
$\mathbf{c}_\mathrm{r}$	$n \times 1$ vector of estimation errors introduced due to $\mathbf{a}$, note that $\mathbf{a} = \mathbf{H}_\mathrm{r}\mathbf{c}_\mathrm{r}$
$\mathcal{M}$	the set of all meter indices in network
$\mathcal{M}^\mathrm{I}$	the set of injection meter indices in network
$\mathcal{M}^\mathrm{B}$	the set of branch meter indices in network
$\mathcal{S}$	the set of protected meter indices, $\mathcal{S} \subseteq \mathcal{M}$
$\lvert\mathcal{S}\rvert$	the number of protected meters
$\bar{\mathcal{S}}$	$\bar{\mathcal{S}} = \mathcal{M} \setminus \mathcal{S}$
$\mathcal{P}$	the set of protected meter indices, $\mathcal{P} \subseteq \mathcal{M}^\mathrm{B}$
$\bar{\mathcal{P}}$	$\bar{\mathcal{P}} = \mathcal{M}^\mathrm{B} \setminus \mathcal{P}$
$\mathbf{H}_\mathrm{r}^{\mathcal{S}}$	the matrix formed by the $\lvert\mathcal{S}\rvert$ rows of $\mathbf{H}_\mathrm{r}$ indicated by the indices in $\mathcal{S}$
$\mathbf{H}_\mathrm{r}^{\bar{\mathcal{S}}}$	the matrix formed by the $\lvert\bar{\mathcal{S}}\rvert$ rows of $\mathbf{H}_\mathrm{r}$ indicated by the indices in $\bar{\mathcal{S}}$
$\mathbf{H}_\mathrm{r}^\mathrm{B}$	the Jacobian matrix of branch meters in all transmission lines
$\mathbf{H}_\mathrm{r}^\mathrm{I,all}$	the Jacobian matrix of injection meters in all buses
$\mathbf{H}_\mathrm{r}^\mathrm{I,gen}$	the Jacobian matrix of injection meters in buses connecting to the generation
$\mathbf{H}_\mathrm{r}^\mathrm{R}$	the Jacobian matrix in real world case, $\mathbf{H}_\mathrm{r}^\mathrm{R} = \begin{bmatrix} \mathbf{H}_\mathrm{r}^\mathrm{B} \\ \mathbf{H}_\mathrm{r}^\mathrm{I,gen} \end{bmatrix}$
$\mathbf{H}_\mathrm{r}^\mathrm{F}$	the Jacobian matrix in full measurement case, $\mathbf{H}_\mathrm{r}^\mathrm{F} = \begin{bmatrix} \mathbf{H}_\mathrm{r}^\mathrm{B} \\ \mathbf{H}_\mathrm{r}^\mathrm{I,all} \end{bmatrix}$
$\mathbf{H}_\mathrm{r}^\mathrm{N}$	the Jacobian matrix in injection-free case, $\mathbf{H}_\mathrm{r}^\mathrm{N} = \begin{bmatrix} \mathbf{H}_\mathrm{r}^\mathrm{B} \end{bmatrix}$

Bibliography

[1] C. Bennett and D. Highfill, "Networking AMI smart meters," in *Proc. Energy 2030 Conf. (ENERGY)*, Atlanta, GA, USA, Nov. 2008, pp.1-8.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid-the new and improved power grid: a survey," *IEEE Commun. Surveys Tutor.*, vol. 14, no. 4, pp. 994-980, Oct. 2012.

[3] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power Grids," in *Proc. 16th ACM Conf. Comput. and Commun. Security*, Chicago, Illinois, USA, Nov. 2009, pp. 21-32.

[4] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. ACM/IEEE 3rd Int. Conf. Cyber-Physical Systems (ICCPS)*, Apr. 2012, pp.183-192.

[5] R. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Syst. (CPSWEEK)*, Stockholm, Sweeden, Apr. 2010.

[6] S. Bi and Y. J. Zhang, "Defending mechanisms sgainst galse-data injection attacks in the power system state estimation," in *Proc. IEEE Globecom SG-COMNETS*, Houston, TX, USA, Dec. 2011, pp. 1162-1167.

[7] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 326-333, Jun. 2011.

[8] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, pp. 4203-4215, Dec. 2005.

[9] O. Vukovic, K. Sou, G. Dan, and H. Sandberg, "Network-layer protection schemes against stealth attacks on state estimators in power systems," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108-1118, Jul. 2012.

[10] Y. Zhao, K. A. Goldsmith, and H. V. Poor, "Fundamental limits of cyber-physical security in smart power grids," *submitted to IEEE Trans. Autom. Control*, Feb. 2013.

[11] M. Talebi, C. Li and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in *Proc. 7th IEEE Sensor Array and Multichann. Sig. Process. Workshop (SAM)*, Hoboken, NJ, USA, Jun. 2012, pp. 393-396.

[12] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. 2nd IEEE Int. Conf. Smart Grid Commun.*, Brussels, Belgium, Oct. 2011, pp. 202-207.

[13] H. Sandberg, A. Teixeira and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst. (CPSWEEK)*, Stockholm, Sweeden, Apr. 2010.

[14] K. C. Sou and H. Sandberg and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. 50th IEEE Conf. Decision Control*, Orlando, FL, USA, Dec. 2011, pp. 4054-4059.

[15] K. C. Sou and H. Sandberg and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 856-865, Jun. 2013.

[16] Y. Huang *et al.* “Bad data injection in smart grid: attack and defense mechanisms,” *IEEE Commun. Mag.*, vol. 51, pp. 27-33, Jan. 2013.

[17] J. Chen and A. Abur, “Placement of pmus to enable bad data detection in state estimation,” *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608-1615, Nov. 2006.

[18] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, “Bad data analysis for power system state estimation,” *IEEE Trans. Power App. Syst.*, vol. 94, no. 2, pp. 329-337, Mar 1975.

[19] A. Monticelli and A. Garcia, “Reliable bad data processing for real-time state estimation,” *IEEE Trans. Power App. Syst.*, vol. PAS-102, no. 5, pp. 1126-1139, May 1983.

[20] T. Van Cutsem, M. Ribbens-Pavella, and L. Mili, “Hypothesis testing identification: A new method for bad data analysis in power system state estimation,” *IEEE Trans. Power App. Syst.*, vol. PAS-103, no. 11, pp. 3239-3252, Nov. 1984.

[21] N. Xiang, S. Wang, and E. Yu, “A new approach for detection and identification of multiple bad data in power system state estimation,” *IEEE Trans. Power App. Syst.*, vol. PAS-101, no. 2, pp. 454-462, Feb. 1982.

[22] C. Meyer, *Matrix Analysis and Applied Linear Algebra*, SIAM, 2001.

[23] A. Monticelli, “Electric power system state estimation,” in *Proc. IEEE*, vol. 88, no. 2, pp. 262-282, Feb. 2000.

[24] A. Monticelli, *State Estimation in Electric Power Systems: a Generalized Approach*, Kluwer Academic Publishers, 1999.

[25] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*, 2nd ed New York: Wiley, 1996.

[26] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, Marcel Dekker, Inc., 2004.

[27] T. A. Short, *Electric Power Distribution Handbook*, CRC Press LLC, 2004.

[28] L. C. Baldor. (2010, Aug. 3). *New threat: Hackers look to take over power plants* [Online]. Available: http://abcnews.go.com/Business/wireStory?id=11316203

[29] U.S. Canada Power System Outage Task Force. (2004, Apr.). *Final report on the August 14, 2003 blackout in the United States and Canada* [Online]. Available: https://reports.energy.gov/B-F-Web-Part1.pdf

[30] R. D. Zimmerman *et al.*. (2007, Sep.). *MATPOWER: Matlab power system simulation package* [Online]. Available: http://www.pserc.cornell.edu/matpower/

[31] M. Grant and S. Boyd. (2010, Aug.). *CVX: Matlab software for disciplined convex programming (version 1.21)* [Online]. Available: http://cvxr.com/cvx

[32] D. Gleich. (2006, Apr.). *MatlabBGL* [Online].
Available: http://www.mathworks.com/matlabcentral/fileexchange/10922

作者簡歷

■ 起源

韓松俯，高雄楠梓人，1989 年於台北松山出生，所以還是會被說成天龍人。
　　單親獨子，從小被寄養在高雄親戚家直到高中畢業。

2001 年畢業於高雄市立莒光國民小學
　　小時候常常與鄰居去後山玩，在街上打躲避球，有街頭電影時會拿板凳去搶個好位子。

2004 年畢業於高雄市立右昌國民中學
　　小有名氣的流氓國中，整天打架鬧事，班上有個大姊頭，迷片跟他要準沒錯的。

2007 年畢業於高雄市立新莊高級中學
　　被「念高中就是為了考大學」這鳥思想洗腦了，整天忙於課業與補習，慶幸有位精神支柱讓我能撐過這苦不堪言的日子。

2011 畢業於國立交通大學電信工程系
　　大學真的什麼人都有，視野在這階段開拓，交了許多朋友、聽了許多故事、學了許多專長，唯一的遺憾應該是沒有加入校隊練球了。

2013 畢業於國立交通大學電信工程研究所
　　幫實驗室開發新領域新方向，幸運地在蘇育德教授的引導下有了成果而順利畢業。

■ Graduate Course

- Digital communication
- Wireless communication
- Random process
- Adaptive signal processing
- Speech processing
- Mobile computing
- Algorithm
- Peer to peer computing