A Design of Theft Detection Framework for Smart Grid Network

by

Victor Zikun Xu

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2015

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Energy loss and energy theft are two serious problems in modern grid which produce huge waste and cost. The smart grid with its ability to collect information about the behaviors of suppliers and customers is expected to be better equipped than the existing grid to detect loss and theft. The following two questions are the main focus of our works: 1). "Can we locate the source of theft ?" 2)."How much energy is stolen?" We deal with two types of theft: tampering with a smart meter and tapping a line.

For tampering, we propose a framework based on the measurement of energy, electric current and voltage to make theft detection feasible. In this framework, when measurements (of energy, electric current and voltage) are available everywhere, theft can be easily detected. The interesting case is, if measurements are not everywhere, theft detection is still feasible under some conditions. For different cases of measurement scenarios, we propose different solutions and provide the conditions under which our solutions work. In particular, assuming that the smart grid has a tree structure and has a single source of energy, we show via simulation the following results: 1) With the measurement of electric current at the entry of each user and at the source of energy, we can locate the source of theft if the electric power is stolen in a constant rate and the measurement noise is comparatively small; 2) With the measurement of the energy production and each user's energy consumption plus the measurement of electric current at the entry of each user, we can accurately estimate the resistance of each link as long as the amount of stolen energy is comparatively small; 3) With the measurement of the voltage and electric current at the source of energy and at the entry of each user, we can accurately estimate the resistance of each transmission link if there is no theft.

For tapping, we apply clustering algorithms to analyze the anomalies in the usage data of all customers. We propose a hierarchical clustering algorithm which recursively bi-partitions the data along the principle eigenvector and separate the usage data of normal users and abnormal users.

Our theft detection framework employs the ℓ_1 minimization under non-negative constraint, i.e., $\min_{x\geq 0} \|Y - Ax\|_{\ell_1}$. As a theoretical verification of our work, we prove that under some suitable conditions on the matrix A, the ℓ_1 minimization problem has a unique minimizer and the unique minimizer is equal to the real underlying result.

Acknowledgments

I would like to thank all the little people who made this possible.

Dedication

This is dedicated to the one I love.

Table of Contents

List of Tables **ix**

List of Figures **x**

1 Introduction **1**

1.1 Smart Grid 1

1.2 Issues Linked to Electricity Theft 2

1.3 Challenges in Theft Detection 4

1.4 Literature Review 4

1.5 Contribution 5

2 A Framework for Theft Detection **9**

2.1 Physical Laws in Electricity 10

2.1.1 The Single-layer Topology 10

2.1.2 The Multi-layer Topology 12

2.2 Estimation of Path Loss Rate 12

2.3 Estimation of Tampering Ratio 15

2.4 Estimation of The Transmission Resistances in A Single-layer System 18

2.4.1 On the Measurement of Electric Current and Energy 18

2.4.2 On the Measurement of Electric Current and Voltage 20

2.5 Estimation of Transmission Resistance in Multi-layer System 24

2.5.1 On the Measurement of Electric Current and Energy 24

2.5.2 On the Measurement of Electric Current and Voltage 26

2.6 A Big Picture 28

3 ℓ_1 Minimization in Non-negative Space **30**
3.1 Linear Programming and ℓ_1 Minimization . . . 30
3.1.1 Linear Program . . . 30
3.1.2 KKT Conditions . . . 31
3.2 Exact Reconstruction Based on Sparsity . . . 32
3.2.1 Decoding by Linear Programming . . . 33
3.2.2 Non-negativity . . . 36
3.3 Robustness to Outliers . . . 42
3.4 Hyperplane Separation By ℓ_1 Minimization . . . 45

4 Clustering and Anomaly Detection **48**
4.1 K-Means . . . 49
4.2 Spectral Clustering . . . 50
4.2.1 Graph Laplacian . . . 51
4.2.2 Ratio Cut . . . 51
4.3 Bi-partition along the Principle Component . . . 52
4.4 Hierarchical Clustering −An Extension of 1D Bipartition along Principle Component . . . 54

5 Numerical Results **57**
5.1 Description of the Data . . . 57
5.2 Estimation of Tampering Ratio . . . 58
5.2.1 Constant Tampering Ratio . . . 58
5.2.2 Discrete Time-varying Tampering Ratio . . . 60
5.2.3 Continuous Time-varying Tampering Ratio . . . 60
5.3 Estimation of The Resistance . . . 63
5.3.1 Estimation Based on Electric Current and Energy . . . 63
5.3.2 Estimation based on Voltage and Electric Current . . . 66
5.4 Clustering . . . 72
5.4.1 Test 1—Different Electric Current Patterns of Power Theft . . . 72
5.4.2 Test 2—An Explore of Clustering Accuracy VS Many Thieves . . . 73
5.4.3 Test 3—An Explore of Clustering Accuracy VS Number of Thieves . . . 75

6 Conclusion **76**

References **78**

List of Tables

5.1 Constant Tampering Ratio 59
5.2 Estimation of Recovery Parameter by Time-invariant Method 61
5.3 Estimation of Recovery Parameters by Time-varying Method 61
5.4 Estimation of Resistance Using Measurement of Voltage 1 64
5.5 Estimation of Resistance Using Measurement of Voltage 2 64
5.6 Estimation of Transmission Resistance Using Measurement of Voltage 3 . . . 71
5.7 Estimation of Transmission Resistance Using Measurement of Voltage 4 . . . 71
5.8 Accuracy of Three Clustering Methods for Alternative Theft Patterns 73
5.9 Accuracy of Three Clustering Methods for Standard Data Set 73
5.10 Partition Results of Hierarchy Clustering 74
5.11 Hierarchy Clustering VS Number of Theives 74

List of Figures

1.1 Diagram of an electric power system [1] 2

1.2 Tree Topology of the Distribution Network 3

1.3 Three Senarios of Different Available Measurements 7

2.1 Three Senarios of Different Available Measurements 11

2.2 *The nodes that are not at the bottom layer represents distribution transformers. The nodes located at the bottom of the tree are the leaves and they represent customers. The measurement points are located at the red points, i.e., at the root and the leaves.* 13

2.3 *The circle **A** represents a smart meter. A smart meter measures energy based on the voltage at the meter and the electric current flowing through it. If we tamper with the meter by connecting both ends of it, then the electric current flowing through the meter becomes less and hence the energy recorded by the meter is less than the real consumption.* 15

2.4 BigMap 29

4.1 *The circle **A** represents a smart meter. User 2 directly draw the energy from the point S, which is ahead of the smart meter of user 1. User 2 could also draw the energy from the point P_3, which is ahead his own smart meter. Thus the power does not flow through the smart meter located at the entry of user 2, which is supposed to record the energy consumption of user 2.* . . 49

4.2 *The instantaneous current of each user is observed every half an hour. We have 289 observations for each user. The X-axis of each subplot represents the observation number from 0 to 288, the Y-axis represents the instantaneous current at each observation. In this figure, the first 9 users are normal users while the 10th one(the one in the first column and the fourth row) is the thief.* 54

4.3 ***Shift1**, **Shift2** and **Shift3** are obtained by shifting the theft pattern appearing in figure 4.2 to different phases; **Periodic1**, **Periodic2** and **Periodic3** are designed to simulate periodic theft patterns; **Victim1**, **Victim2** and **Victim3** are generated by adding periodic theft to normal user pattern.* 56

5.1 Continuous Time-varying Recovery of Electric Current 62

5.2 *The X-axis of this figure represents the theft frequency while the Y-axis stands for the relative estimation error of resistance. The green plot is the result of least squares estimation while the red plot is the result of ℓ_1 minimization. As we can see, the estimation error of ℓ_1 minimization is less than the estimation error of least squares estimation overall. In addition, the estimation error of ℓ_1 minimization is more robust than least squares estimation with the increase of theft frequency.* 65

5.3 *The X-axis of this figure stands for the theft rate while the Y-axis corresponds to the relative estimation error of resistance. The green plot is the result by the least squares estimation while the red plot is the result of ℓ_1 minimization. As we can see, the estimation error of least squares estimation increases rapidly with the increase of theft rate while the estimation error of ℓ_1 minimization is robust against the increase of theft ratio.* 67

5.4 *The X-axis of this figure represents the time interval number while the Y-axis stands for the estimation error of theft in a time interval. The green plot is the result of least squares estimation while the red plot is the result of the ℓ_1 minimization. As we can see, the estimation error of ℓ_1 minimization is smaller than least squares estimation overall.* 68

5.5 Topology for the Simulation in Section 4.4 70

5.6 Recursion Tree 74

Chapter 1

Introduction

1.1 Smart Grid

With the increasing demand for energy in different areas, power loss in smart grid has become an issue. Energy loss can be caused by various reasons such as leaks, theft, and inefficiencies. With the development of new sensing, communication and control infrastructure for the power grid, a large amount of information become observable for us to localize the source of loss. A smart meter is an embedded electronic device that regularly records electric energy consumption of each user in every fixed time interval. Each customer's usage information recorded by the smart meter is sent back to the hydro company for billing [26]. Located at the customer ends of the smart grid, the smart meters can play an essential role in monitoring anomalies in the electric power system.

Electric power systems produce and distribute electricity to consumers. Figure 1.1 [1] shows a simple diagram of an electric power system. Electricity is produced at the generating station (the red part of the figure) and transmitted to customers via the transmission lines. In order to reduce the energy loss during the transmission, the step-up transformer boosts up the voltage to over 10 kilovolt (KV). The extremely high voltage is not suitable for customers to use. Then the step-down transformer at the other end of the transmission lines lowers down the voltage to 200~240 volt and delivers the electric power to customers.

In the following, we focus on a distribution system and assume a tree topology, as shown in Figure 1.2, to model the electric power system. The distribution transformers are at the non-leaf nodes while the customers are at the leaves. Input power is supplied to the distribution transformer (DT) at the root. The distribution transformers transfer the energy from top to bottom layer by layer and the electrical power finally reaches the leaves. The measurement points (MPs) are set at the red points in Figure 1.2, i.e., at the root and at the leaves.

The power in an alternating current (AC) circuit consists of two components, the active power and the reactive power [15]. The portion of the power that transfers net energy only

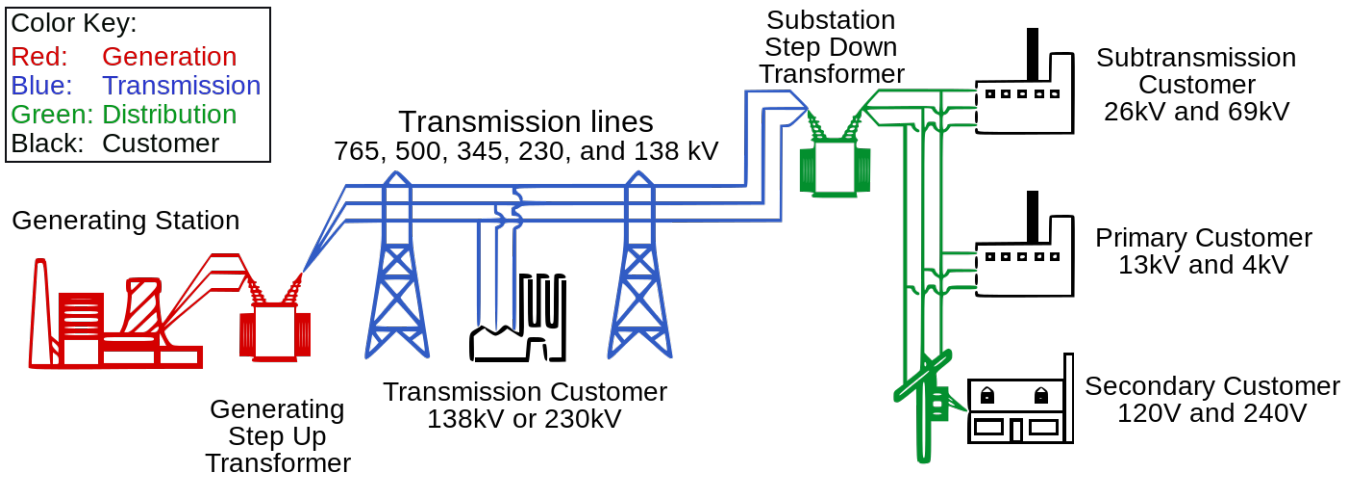


Figure 1.1: Diagram of an electric power system [1]

in the single direction towards customers is known as active power. Reactive power occurs when reactive currents flow back to the source of energy production due to stored energy. If the loads of the grid are purely resistive, then only active power is transferred. If the loads of the grid are purely reactive, then only reactive power flows. In practice, the loads of the grid have both resistance and reactance, and hence both active and reactive power exist. In this thesis, the distribution network that we measure is assumed to be purely resistive and thus only active power is considered.

1.2 Issues Linked to Electricity Theft

Electricity theft refers to the dishonest behavior of a customer that prevents the utility company from correctly measuring his (her) real energy consumption and thus gets himself (herself) fully or partially free from payment. There are various ways to steal electrical power, including tampering with the energy meter or tapping a line. Electricity theft is an illegal, dangerous and environmentally unfriendly activity.

Electricity theft brings huge amount of economic losses globally each year. Currently, the utility companies all over the world lose 89.3 billion dollars per year due to electricity theft [22]. In the developing countries, electricity theft is especially severe and it causes an annual loss of 58.7 billion dollars [22]. For example, in Southeast Asia the amount of theft can even reach 40% [20]; in India only 55% of energy production is billed [12]. A significant amount of electricity theft also takes place in the developed countries. In Canada, B.C Hydro, a utility company located in British Columbia (BC), identified over 2,600 electricity thefts from 2008 to 2013. They announced that the cost of electricity theft had grown from 500 GWh (gigawatt-hours) in 2006 to at least 850 GWh in 2013 [13]. In Netherlands, electricity thieves are skillful, well organized and mostly related to some

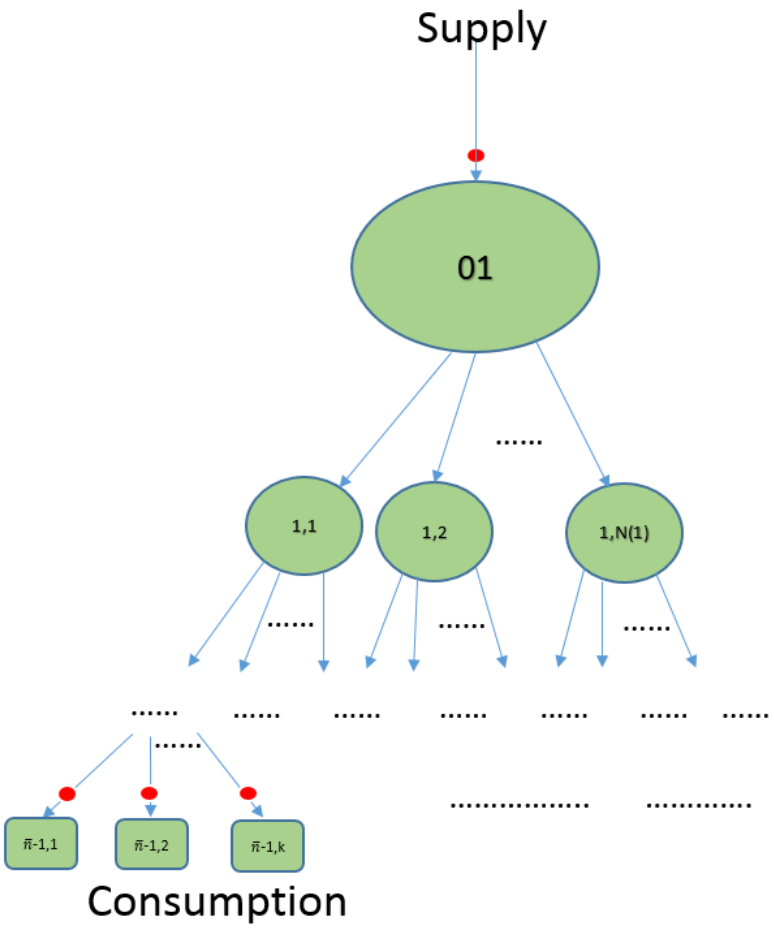


Figure 1.2: Tree Topology of the Distribution Network

The non-leaf nodes represent the distribution transformers. The leaves represent the customers. The energy is supplied at the root of the tree. The DTs distribute the electricity layer by layer and eventually deliver the energy to the leaves. The measurement points are located at the red points, i.e., at the root and the leaves.

other criminal activity such as illegal drugs. Different camouflaging techniques plus rapid changes of the theft locations make the detection more difficult [12].

Electricity theft also poses potential dangers to the community [22]. When electricity theft occurs, stronger electric currents may flow through the lines than the maximum that the grid can safely handle. The overloads may cause fires and even explosions. In addition, illegal connections to the power grid are usually installed by unprofessional people and hence create a potential of electricity leaks. This is dangerous to anyone who may get close to the illegal connections, especially young children.

1.3 Challenges in Theft Detection

In the traditional grids, only energy (the supply and consumption) is measured at time intervals of an hour or less. The inconsistency between the supply and total consumption is called loss. The losses mainly consist of two components, technical and non-technical losses. Technical losses includes ohmic losses caused by the resistance of transmission lines, conversion losses at distribution transformers, leaks due to imperfect isolation and so forth [20]. Technical losses occur naturally during transmission and hence are inevitable. Non-technical losses are caused by human actions such as electricity theft, non-payment by customers, and record errors, and hence can be easily eliminated (or largely decreased) once detected. Measuring only supply (at the root) and consumption (at the leaves) cannot distinguish theft from technical losses. As a result we need additional types of measurements to estimate the technical losses. The amount of stolen energy can potentially be estimated from the inconsistency between the supply and total consumption with the exclusion of the estimated technical losses.

Tampering with the smart meter and tapping from a line are two typical types of electricity theft. Using the conservation of electric current, which says the input electric current (to the grid) is equal to the sum of electric currents that flow to each smart meter, we may detect and locate the tampering of a smart meter. However, the unknown illegal connections may break the conservation of electric current. That is to say, if two types of theft occur simultaneously, then the prior knowledge of the physical laws in electricity are not applicable and this makes the detection very difficult.

1.4 Literature Review

In this section, we review the previous works related to theft detection.

Smart meters normally measure energy production and energy consumption only. Using the measurements of energy production and each customer's energy consumption, Arya et al. provide a solution to estimate the path loss rate and localize the lossy links [3]. Their estimation of path loss rate results from the least squares solution to an over-determined

linear system. The localization of lossy links is based on a strong assumption that the lossy links are sparse and thus it does not always work. In addition, Arya et al. does not mention how to distinguish theft from the total losses [3].

Salinas et al. propose a theft detection method which estimates each customer's honesty coefficient [24], where the honesty coefficient is actually the multiplicative inverse of the path loss rate. They require an extra measurement point (MP) to measure the total energy consumption of the customers in a certain service area. The energy consumption of each customer is measured as well. If a customer's honesty coefficient is one, then this user is honest; if a customer's honesty coefficient is much higher than one, then he (she) is suspected to be a thief [24]. The estimation of each user's honesty coefficient in [24] shares much similarity with the estimation of path loss rate in [3]. Both of them formulate an over-determined system based on the conservation of energy and estimate the unknowns by least squares estimation. The limitation of the method in [24] is that the technical losses such as ohmic losses that occur at the transmission line between the extra MP (that measures the total energy consumption) and each customer's smart meter are ignored.

Nizar et al. apply several supervised machine learning methods to classify customers into a group of thieves and a group of honest users [21]. Without considering the topology of distribution network as well as the physical laws in electricity, Nizar et al. just simply applied the existing popular machine learning models such as support vector machine and neural network to the theft detection problem. Even though they obtain small errors in training the model, the testing accuracy is not satisfactory.

Based on the measurements of each user's consumption and the electric current that flows to each user, Nikovski et al. propose a theft detection method to determine when theft occurs and estimate how much energy is stolen [20]. However, the theft detection method by Nikovski et al. is only limited to the single-layer system where there is only one distribution transformer. In practice, smart distribution networks have multiple layers of distribution transformers. Worse still, their method fails to locate the source of theft, which is unhelpful for the removal of theft.

1.5 Contribution

This thesis deals with mainly two types of theft: tampering with the smart meter and tapping a line. In particular, our objective is to estimate the resistance of each link, estimate the theft amount and locate the users who are stealing energy.

To deal with the theft in the form of tampering with the smart meter, we propose a unified theft detection framework based on the measurements of supply, consumption, transmission voltage and electric current. This framework provides different approaches to estimate theft based on the types of measurements that are available. Our model makes the following assumptions:

- The power distribution system has a *tree* structure. The source of electricity energy is provided at the root and the customers are located at the leaves. All the leaves are located at the same layer. Each intermediate node represents a distribution transformer and each edge represents a link.

- Electricity theft occurs only in the form of tampering with the smart meter; that is to say, this framework assumes an unknown link is never introduced.

Our framework provides three alternative solutions for the three scenarios depicted in Figure 1.3. In these three scenarios, the energy is supplied to the root of the tree, distributed from the top to the bottom of the tree and consumed at the leaves; the measurement points (MP) marked as the red points are set at the root and the leaves of the tree. Here are the difference of these three scenarios:

- As indicated in Figure 1.3a, the MP at the root measures the energy supply; the smart meters at the leaves record each customer's energy consumption (KWatt-h) at time intervals of half an hour.

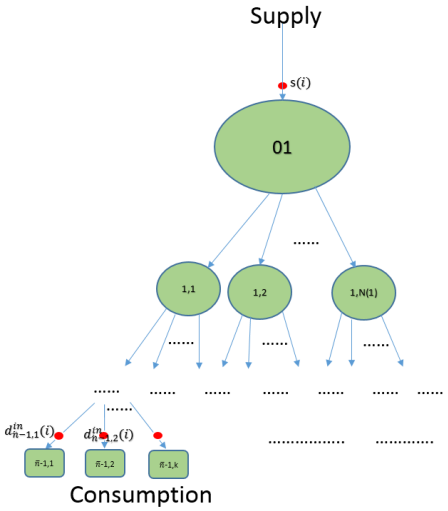
- As indicated in Figure 1.3b, the MP at the root measures the energy supply; the smart meters at the leaves record each customer's energy consumption (KWatt-h) at time intervals of half an hour and the incoming instantaneous electric current every half an hour.

- As indicated in Figure 1.3c, the MP at the root and the smart meters at the leaves measure the voltage and the incoming instantaneous electric current every half an hour.

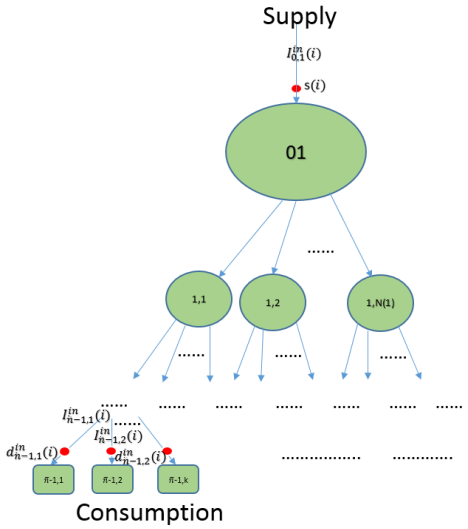
Our theft detection framework may not be able to locate an unknown link that is secretly introduced by a known user. To deal with the theft in the form of tapping into a power line from a point ahead of the energy meter by a known user, we apply clustering algorithms to analyze the anomalies in the usage data of all customers. We make a hypothesis that the usage data of a user who is stealing energy by directly hooking to a line indicates an abnormal pattern compared to the honest users who are not stealing energy. Under our hypothesis, we run clustering algorithms on the usage data of all customers and partition the data points into two groups, where one group is expected to correspond to the honest users and the other group is expected to include the suspects.

The main contributions of this thesis are listed as follows:

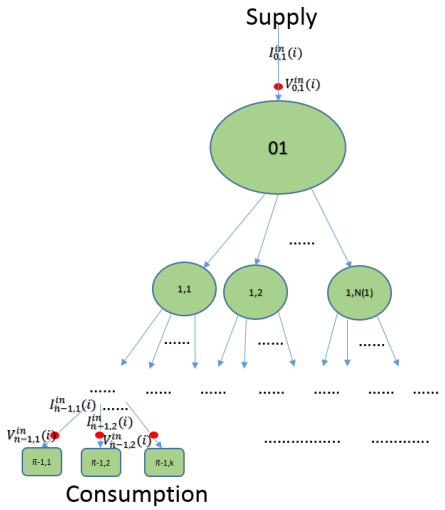
- We propose a measurement-driven framework of theft detection that provides a solution according to which of the above three scenarios of measurements is given. This framework extends the previous theft detection model for a one-layer tree topology [20] to a more general model based on a multi-layer tree topology.



(a) Scenario 1: energy



(b) Scenario 2: energy and current



(c) Scenario 3: energy, current and voltage

Figure 1.3: Three Senarios of Different Available Measurements

The energy is supplied to the root of the tree. The non-leaf nodes represent the distribution transformers. They distribute the energy layer by the layer and eventually deliver the energy to the leaves. The leaves represent the customers. The measurement points are located at the red points, i.e., at the root and the leaves. $s(\cdot), d(\cdot), I(\cdot), V(\cdot)$*, respectively, represent the measurements of energy supply, energy consumption, electric current and voltage. In Figure 1.3a, the energy supply is measured at the root, and the the smart meter at the entry of each leaf measures the energy consumption. In Figure 1.3b , in addition to the measurement of energy, the incoming electric current is also measured at the measurement points. In Figure 1.3c, both the voltage and the incoming electric current are measured at the measurement points.*

- With respect to each of the above three scenarios of measurements, we provide a theoretical analysis to investigate under what conditions our framework correctly estimate the transmission resistance and detect the theft.
- We propose a hyperplane separation method, which recursively looks for a hyperplane to detect time-varying theft.
- In the simulated tests based on real data recorded by smart meters, we demonstrate the effectiveness of our framework in locating the source of electricity theft, estimating the transmission resistance and recognizing the time-varying theft.
- We propose a novel hierarchical bi-partition algorithm based on the principle eigenvector to detect anomaly patterns in the energy usage of customers. In the simulated tests, we show that our clustering method is effective in discovering and locating the anomalies in the usage data of customers.

The structure of this thesis is as follows.

In Chapter 2, we give three different formulations of the theft detection problem based on three different sets of measurements, where the three different sets of measurements are shown in Figure 1.3 and the three different formulations respectively estimate the loss along each path from the root to a leave in the tree, locate the source of stealing, and estimate the resistance of each link in the distribution network. These three different formulations have a unified mathematical expression, $\min_{x\geq 0} \|y - Ax\|_1$, where the unknown variable x has different meanings for different scenarios.

In Chapter 3, we first review linear programming and ℓ_1 minimization. As a theoretical verification of our work, we prove that under some suitable conditions on the matrix A, the ℓ_1 minimization problem $\min_{x\geq 0} \|y - Ax\|_1$ has a unique minimizer and the unique minimizer is equal to the real underlying result that we want to estimate. This theoretical result is fundamental to the theft detection problem since the problem in different scenarios can be formulated into the same form $\min_{x\geq 0} \|y - Ax\|_1$, which is an ℓ_1 minimization problem under the non-negativity constraint. The unique minimizer to $\min_{x\geq 0} \|y - Ax\|_1$ presumes that the electricity theft is time independent. In the rest of chapter 3, we propose an algorithm to estimate time-varying electricity theft.

In Chapter 4, we first introduce two existing popular clustering algorithms, K-means and spectral clustering, then we propose a simple two-group clustering that projects to the data points to their first principle eigenvector and bi-partition the one dimensional projection by minimizing the sum of the variance of two groups; we also extends our bi-partition method to hierarchical clustering which recursively bi-partitions the data points until the variance of each group is lower than a manually tuned threshold.

In Chapter 5, we simulate electric power theft based on real smart grid data. We present the testing results of our theft detection framework as well as the clustering results.

Chapter 2

A Framework for Theft Detection

In this chapter, assuming that the theft occurs only in the form of tampering with the smart meter, we propose a unified theft detection framework based on the measurements of supply, consumption, voltage and electric current. This framework provides different solutions to estimate theft based on what types of measurements are available. The measurement points of this framework are set the at the root and the leaves of the tree, and measurements are made every half an hour. This framework deals with the following three scenarios:

1. Only energy is measured;
2. Energy and instantaneous electric current are measured;
3. Instantaneous voltage and electric current are measured.

The formulations of the theft detection problems in scenario 1 and scenario 2 have already been discussed in existing literature [3] [20]. We propose a simple improvement for the existing formulation [20] of the problem in scenario 2. Scenario 3 has not been considered in existing literature, and we propose a novel formulation for the problem in this scenario. The outline of this chapter is as follows.

In Section 2.1, we describe the basic physical laws that the system should satisfy. In Section 2.2, with respect to scenario 1, we review how to estimate path loss rate from the measurements of energy supply and energy consumption of each customer [3]. In Section 2.3, with respect to scenario 2, we show how to locate the electricity theft from the measurements of the electric currents that flow to the root distribution transformer and all the customers. In Section 2.4, with respect to scenario 2 and 3, we show how to estimate the resistance of each link in the electrical grid based on single-layer tree topology. In Section 2.5, still with respect to scenario 2 and 3, we extend the work in Section 2.4 to a multi-layer tree topology.

2.1 Physical Laws in Electricity

This section describes the physical laws that the system should satisfy if there is no theft.

2.1.1 The Single-layer Topology

The single-layer tree topology is shown in Figure 2.1. The root of the tree represents the distribution transformer (DT). There are n branches at the root and each branch directly goes to a leaf of the tree. The leaves represents the customers. The MPs are set at the red points. The DT is configured with a constant distribution parameter α, which can be known in advance. The distribution parameter α is the ratio of input voltage potential and output voltage potential of the DT. In a sequence of time $t_1, t_2, \cdots, t_m$, we let $V_0^{in}(i)$ denote the real voltage at the entry of the root at time t_i, $V_0^{out}(i)$ denote the real output voltage of the root at time t_i , then the equation

$$\alpha = \frac{V_0^{in}(i)}{V_0^{out}(i)} \tag{2.1}$$

holds at any time t_i. Let $I_0^{in}(i)$ be the real electric current that flows to the root at time t_i, $I_j^{in}(i)$ be the real electric current that flows to the leaf at the jth branch at time t_i. Since the input power and output power of the DT should be equal, if there is no theft, then it follows that

$$\begin{aligned} & I_0^{in}(i)V_0^{in}(i) = V_0^{out}(i)\sum_{j=1}^{n} I_j^{in}(i), \\ \Rightarrow \quad & I_0^{in}(i)(\alpha V_0^{out}(i)) = V_0^{out}(i)\sum_{j=1}^{n} I_j^{in}(i), \\ \Rightarrow \quad & \alpha I_0^{in}(i) = \sum_{j=1}^{n} I_j^{in}(i), \end{aligned}$$

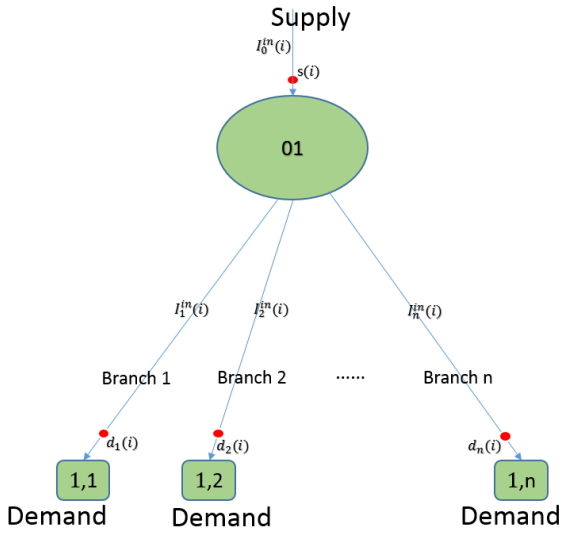
at any time t_i. Thus the distribution parameter can be equivalently written as

$$\alpha = \frac{\sum_{j=1}^{n} I_j^{in}(i)}{I_0^{in}(i)}. \tag{2.2}$$

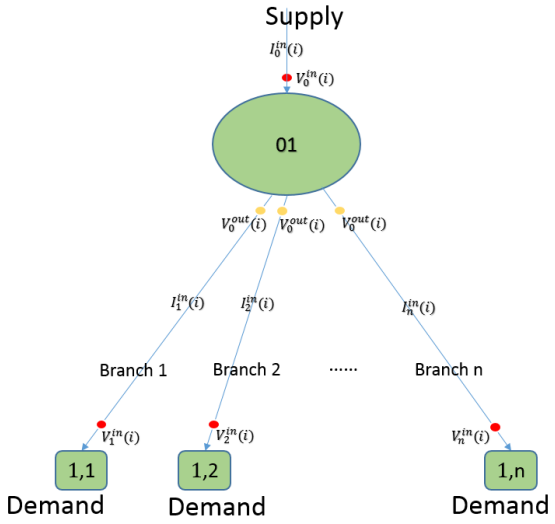
Let R_j be the resistance of the link on the jth branch (in Figure 2.1b), $V_j^{in}(i)$ be the real voltage at the entry of the leaf located at the jth branch (in Figure 2.1b)) at time t_i, for all $1 \le j \le n$. Then the Ohm's law says that

$$\alpha V_0^{in}(i) - V_j^{in}(i) = I_j^{in}(i)R_j(i), \qquad \forall 1 \le j \le n, \tag{Ohm}$$

at any time t_i.



(a) Scenario 1: energy and current



(b) Scenario 2: energy, current and voltage

Figure 2.1: Three Senarios of Different Available Measurements

The energy is supplied to the root of the tree. The root represents the DT. The leaves represent the customers. The DT distributes the energy to the customers. The measurement points are located at the red points, i.e., at the root and the leaves. $s(\cdot), d(\cdot), I(\cdot), V(\cdot)$, *respectively, represent the measurements of energy supply, energy consumption, electric current and voltage. In Figure 2.1a , in addition to the measurement of energy, the incoming electric current is also measured at the measurement points. In Figure 2.1b, both the voltage and the incoming electric current are measured at the measurement points.*

2.1.2 The Multi-layer Topology

The structure of the multi-layer tree topology is shown in Figure 2.2. The tree is full and complete. It has $\bar{n}$ layers, $\bar{n} > 2$. Let the layer number range from 0 to $\bar{n}-1$, i.e., the root is at layer 0 while the leaves are at layer $\bar{n}-1$. The root and intermediate nodes (the nodes located at the layers from layer 1 to layer $\bar{n}-2$) of the tree represents the DTs. MPs are set at the red points as indicated in Figure 2.2. The physical laws introduced in the single-layer tree topology are also applicable to each layer of the multi-layer tree.

Each DT is configured with a constant distribution parameter. For simplicity, we suppose that the DTs located at the same layer have the same distribution parameter. Let the distribution parameter of the DTs located at layer l be α_l for all $0 \leq l < \bar{n}-1$. We label the leaves from 1 to n. In a sequence of time $t_1, t_2, \cdots, t_m$, $I_j^{in}(i)$ denotes the real electric current that flows to the jth leaf at time t_i, $I_0^{in}(i)$ denotes the electric current that flows to the root at time t_i. If there is no theft, then we can apply Equation (2.2) at each node that is not a leaf from top to bottom (of the tree), layer by layer, and get

$$I_0^{in}(i) = \sum_{j=1}^{n}(\prod_{l=0}^{\bar{n}-2}\frac{1}{\alpha_l})I_j^{in}(i).$$

Let $\alpha := \prod_{l=0}^{\bar{n}-2}\alpha_l$, then

$$\alpha = \frac{\sum_{j=1}^{n} I_j^{in}(i)}{I_0^{in}(i)} \tag{2.3}$$

Notice that Equation (2.2) and (2.3) have the same form. To make the meaning of these two equations consistent, we define the **distribution parameter of the entire system** to be the product of the distribution parameters of the DTs at all layers. In a single-layer system, we only have one layer of DT, thus the distribution parameter of the entire system is the distribution parameter of the DT at the root. As we have shown above, the distribution parameter of the entire system can be written as the ratio of the sum of the electric currents flowing to the leaves to the electric current flowing to the root.

2.2 Estimation of Path Loss Rate

Energy loss is the difference between the supplied energy and the energy consumption. Path loss refers to the energy loss that occurs on a path while path loss rate refers to the ratio of path loss to the total energy transferred along this path. In this section, we first review the model in [3], which uses the measurements of energy supply and each user's energy consumption to estimate the path loss rate of each path from the root to a user. Then we propose a simple improvement to the model in [3] by adding a non-negativity constraint.

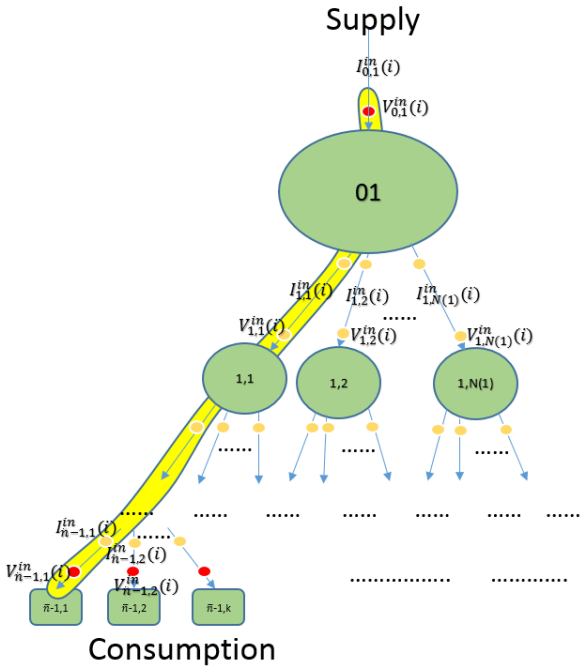


Figure 2.2: *The nodes that are not at the bottom layer represents distribution transformers. The nodes located at the bottom of the tree are the leaves and they represent customers. The measurement points are located at the red points, i.e., at the root and the leaves.*

Settings of Our Model

The tree model introduced in [3], which we call ***Arya Tree Model***, is defined as follows.

Definition 1 *The tree topology of **Arya Tree Model** is depicted by Figure 1.3a, where the distribution transformers are located at the non-leaf nodes while the users are at the leaves. There are n leaves in the tree and the leaves are correspondingly labeled as $1, 2, \cdots, n$. The MPs are set at the root and the leaves, i.e., the red points in Figure 1.3a. The supplied energy and the energy consumption are regularly measured at the MPs at a time interval of length T, and m measurements are collected in total, namely, the measurements of energy are taken at the time intervals $[t_0, t_1]$,$[t_1, t_2]$, $\cdots$, $[t_{m-1}, t_m]$, where $t_i = i \cdot T$, $0 \le i \le m$. P_j denotes the path from the root node to the leaf labeled as j, $1 \le j \le n$.*

In this section, we use the settings described by Definition 1 to model the smart grid.

For any $1 \le i \le m$ and $1 \le j \le n$, $\beta_j(i)$ denotes the fraction of the total supplied energy flowing to the leaf labeled as j along the path P_j in the time interval $[t_{i-1}, t_i]$; $s(i)$ denotes the measurement of the energy supply of the entire grid in the time interval $[t_{i-1}, t_i]$; $d_j(i)$ denotes the measurement of the energy consumption of the user at the leaf node labeled

as j in the time interval $[t_{i-1}, t_i]$; $\pi_j(i)$ denotes the path loss rate of P_j in the time interval $[t_{i-1}, t_i]$.

Assumptions and Objective

The assumptions we make for this model is also the same as [3]. We assume $m \geq n$. We assume the conservation of energy $\sum_{1 \leq j \leq n} \beta_j(i) = 1$ holds for all $1 \leq i \leq m$. Given only the measurements $s(i)$ and $d_j(i)$ for all $1 \leq i \leq m, 1 \leq j \leq n$, our objective is to estimate path loss rate $\pi_j(i)$ for all $1 \leq i \leq m, 1 \leq j \leq n$.

Formulation

We first review the formulation of the problem in [3].

The equation for the amount of energy reaching the node labeled as j in the time interval $[t_{i-1}, t_i]$ is

$$s(i)\beta_j(i)(1 - \pi_j(i)) = d_j(i).$$

Rearranging the equation, we can get

$$s(i)\beta_j(i) = \frac{d_j(i)}{1 - \pi_j(i)}, \forall 1 \leq i \leq m, 1 \leq j \leq n.$$

We sum the equations up for all leaves

$$\sum_{1 \leq j \leq n} s(i)\beta_j(i) = \sum_{j \in L} \frac{d_j(i)}{(1 - \pi_j(i))}, \forall 1 \leq i \leq m.$$

Notice that $\sum_{1 \leq j \leq n} s(i)\beta_j(i) = s(i) \sum_{1 \leq j \leq n} \beta_j(i) = s(i)$. Consequently we have the following simplification

$$\sum_{1 \leq j \leq n} \frac{d_j(i)}{(1 - \pi_j(i))} = s(i), \forall 1 \leq i \leq m.$$

Let $b_i = s(i), x_i = \begin{bmatrix} d_1(i) & d_2(i) & \dots & d_n(i) \end{bmatrix}^\top \in \mathbb{R}^n$ for $1 \leq i \leq m$, and

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}, X = \begin{bmatrix} x_1^\top \\ x_2^\top \\ \vdots \\ x_m^\top \end{bmatrix}.$$

Also let

$$\theta^{(i)} = \begin{bmatrix} \frac{1}{1-\pi_1(i)} \\ \frac{1}{1-\pi_2(i)} \\ \vdots \\ \frac{1}{1-\pi_n(i)} \end{bmatrix},$$

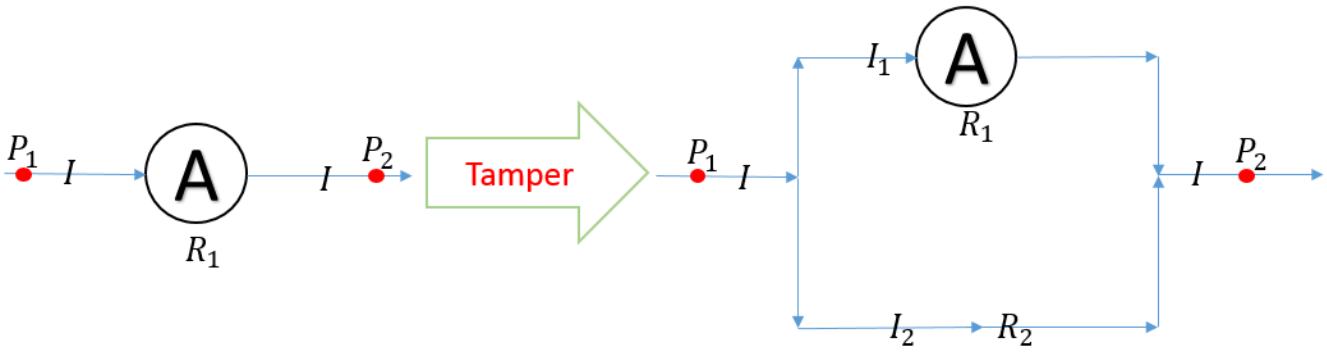


Figure 2.3: *The circle* ***A*** *represents a smart meter. A smart meter measures energy based on the voltage at the meter and the electric current flowing through it. If we tamper with the meter by connecting both ends of it, then the electric current flowing through the meter becomes less and hence the energy recorded by the meter is less than the real consumption.*

for $1 \le i \le m$, then ${\theta^{(i)}}^\top x_i = b$. That is to say, x_i locates at the hyperplane ${\theta^{(i)}}^\top x = b$. Then we have two cases as below: 1) $\theta^{(i)}$ does not change with time; 2) $\theta^{(i)}$ is time-varying.

If $\theta^{(i)}$ does not change with time, then $\theta^{(1)} = \theta^{(2)} = \ldots = \theta^{(m)}$. For convenience, we just let $\theta := \theta^{(1)}$. Thus we have the following linear system of equations

$$X\theta = b, \tag{2.4}$$

where X and b are known and θ is unknown. We use $\tilde{X}$ and $\tilde{b}$ to represent the measurement of X and b respectively. In practice, we have m much larger than n and the measurement is noisy, consequently the equation does not strictly hold and instead it provides that $\tilde{X}\theta \approx \tilde{b}$. In other words, the linear system is over-determined. The paper [3] uses least squares estimation to estimate θ. Here we adopt ℓ_1-minimization to minimize $\|X\theta - b\|_1$. Moreover, by the definition of the path loss rate, we have $\frac{1}{\pi_j(i)} \ge 1, \forall 1 \le i \le m, 1 \le j \le n$. Thus we impose the constraint that $\theta \ge \mathbb{1}_n$, where $\mathbb{1}_n \in \mathbb{R}^n$ is a vector of all ones. We estimate θ by solving the following optimization problem

$$\min_{\theta \ge \mathbb{1}_n} \|\tilde{X}\theta - \tilde{b}\|_1, \tag{2.5}$$

and the minimizer $\hat{\theta}$ of this problem is our estimation of the path loss rate.

If $\theta^{(i)}$ is time-varying, then different x_i $(1 \le i \le m)$ are lying on different hyperplanes. This is the hyperplane separation problem that we will discuss in section 3.4.

2.3 Estimation of Tampering Ratio

A smart meter usually measures the energy consumption of each user. The difference between supply and the sum of consumption consists of two components, the technical

losses and non-technical losses such as electricity theft. The measurements of energy does not provide enough information to distinguish non-technical losses from the total energy losses and thus cannot pin down the locations of the thieves. Hence we need additional type of measurements to locate the theft. In this section, we propose a novel solution to locate the tampering of smart meters by measuring instantaneous electric current.

Figure 2.3 shows a normal way to tamper with a smart meter. Suppose the electric current that flows from the point P_1 to the point P_2 is I. If we set a smart meter **A** between P_1 and P_2, then the electric current measured by **A** should be I. Suppose the resistance of the smart meter **A** is R_1 and we connect both ends of **A** with a piece of wire whose resistance is R_2. After connection, suppose the current flowing through the smart meter becomes I_1 and the current flowing though R_2 is I_2. The conservation of electric current gives that $I = I_1 + I_2$ and ohmic law says that $I_1R_1 = I_2R_2$. Thus we can get that $I = \frac{R_1+R_2}{R_2}I_1$. I is equal to the sum of the electric current that passes through the smart meter and the electric current that bypasses the smart meter, and we call it the **real** value of the electric current that flows from P_1 to P_2. I_1 only refers to the electric current that passes through the smart meter, and we call it the **measured** value of the electric current that flows from P_1 to P_2. If R_1 and R_2 are constants, then ratio of measured value to real value is a constant $\frac{R_2}{R_1+R_2} < 1$. That is to say, the measured value after tampering is underestimated by a constant rate.

We define the tampering ratio of a user's smart meter to be

$$r := \frac{I_{measure}}{I_{real}},$$

where I_{real} is the real value of the electric current that flows into this user, and $I_{measure}$ is the measured value of I_{real}. If a user's tampering ratio is very close to one, then this user is very unlikely to be a thief. If a user's tampering ratio is far less than one, then he (she) is very likely to be stealing energy.

Settings of Our Model

The settings described by Definition 1 also apply here. In addition, the electric current is measured at the MPs as well, at time $t_1, t_2, \cdots, t_m$. The tree model used in this section is depicted by Figure 1.3b. Also, let α denote the distribution parameter of the entire system.

For any $1 \le i \le m, 1 \le j \le n$, $I_0^{in}(i)$ denotes the real electric current at the entry of the root at time $t = t_i$; $I_j^{in}(i)$ denotes the real electric current at the entry of the leaf node labeled as j at time $t = t_i$; $\tilde{I}_0^{in}(i)$ and $\tilde{I}_j^{in}(i)$ respectively denote the measurements of $I_0^{in}(i)$ and $I_j^{in}(i)$ recorded by smart meters; $r_j(i)$ denotes the tampering ratio of the smart meter located at the entry of the leaf node labeled as j at time $t = t_i$.

Assumptions and Objective

We assume $m \geq n$. We assume the conservation of electric current $\alpha \sum_{1 \leq j \leq n} I_j^{in}(i) = I_0^{in}(i)$ holds for all $1 \leq i \leq m$. We assume the measurement of $I_0^{in}(i)$ cannot be tampered with by users. That is to say, $I_j^{in}(i) = \tilde{I}_j^{in}(i)$. Given the measurements $\tilde{I}_0^{in}(i)$ and $\tilde{I}_j^{in}(i)$, our objective is to estimate tampering ratio $r_j(i)$, for all $1 \leq i \leq m, 1 \leq j \leq n$.

Formulation

We propose a novel formulation to estimate the tampering ratio of each user as follows.

By the definition of tampering ratio, we have $r_j(i) = \frac{\tilde{I}_j^{in}(i)}{I_j^{in}(i)}$. Thus $I_j^{in}(i) = \frac{\tilde{I}_j^{in}(i)}{r_j(i)}$. Then it follows that

$$\frac{1}{\alpha}\tilde{I}_0^{in}(i) = \frac{1}{\alpha}I_0^{in}(i) = \sum_{j=1}^{n} I_j^{in}(i) = \sum_{j=1}^{n} \frac{1}{r_j(i)}\tilde{I}_j^{in}(i), \forall 1 \leq i \leq m. \tag{2.6}$$

Let

$$b = \begin{bmatrix} \frac{1}{\alpha}\tilde{I}_0^{in}(1) \\ \frac{1}{\alpha}\tilde{I}_0^{in}(2) \\ \vdots \\ \frac{1}{\alpha}\tilde{I}_0^{in}(m) \end{bmatrix}, X = \begin{bmatrix} \tilde{I}_1^{in}(1) & \tilde{I}_2^{in}(1) & \dots & \tilde{I}_n^{in}(1) \\ \tilde{I}_1^{in}(2) & \tilde{I}_2^{in}(2) & \dots & \tilde{I}_n^{in}(2) \\ \dots & & & \\ \tilde{I}_1^{in}(m) & \tilde{I}_2^{in}(m) & \dots & \tilde{I}_n^{in}(m) \end{bmatrix}, \beta^{(i)} = \begin{bmatrix} \frac{1}{r_1(i)} \\ \frac{1}{r_2(i)} \\ \dots \\ \frac{1}{r_n(i)} \end{bmatrix}, \forall 1 \leq i \leq m.$$

Then we have two cases as below: 1) $\beta^{(i)}$ does not change with time; 2) $\beta^{(i)}$ is time-varying.

If $\beta^{(i)}$ does not change with time, then we can just simplify it to β and we have the following linear system about β

$$X\beta = b. \tag{2.7}$$

Due to the measurement noise, the above linear system does not strictly hold. We adopt ℓ_1-minimization to minimize $\|X\beta - b\|_1$. Moreover, since the tampering ratio cannot be greater than 1, we have $\beta \geq \mathbb{1}_n$, where $\mathbb{1}_n \in \mathbb{R}^n$ is a vector of all ones. Thus we estimate β by solving the following problem

$$\min_{\beta \geq \mathbb{1}_n} \|X\beta - b\|_1, \tag{2.8}$$

and the minimizer $\hat{\beta}$ of this problem contains our estimation of each user's tampering ratio. The numerical results of solving Problem (2.8) are shown in Section 5.2.1.

If $\beta^{(t)}$ is time-varying, then different rows of X are actually lying on different hyperplanes. This is the hyperplane separation problem that we will discuss in section 3.4.

Note that the estimation of path loss rate and the estimation of tampering ratio have the same mathematical formulation but the physical meanings of them are different. The path losses includes both technical losses and theft and thus the theft cannot be distinguished from the technical losses. But the tampering ratio can fully reflect whether a customer is stealing energy. In other words, the violation of the conservation of energy does not necessarily imply theft but the violation of the conservation of electric current fully implies the tampering activity.

2.4 Estimation of The Transmission Resistances in A Single-layer System

By estimating the tampering ratio, we can locate the theft. Other than the location of theft, we are also interested in how much energy is stolen. The difference between energy supply and energy consumption is equal to the sum of technical losses and power theft. The majority of technical losses comes from the ohmic losses. The ohmic losses are related to transmission resistance. In this section, we provide two solutions to estimate the transmission resistance based on two different sets of available measurements. Using the estimation of transmission resistance together with the measurements of instantaneous electric current, we can estimate the ohmic losses. With the ohmic losses excluded from the total energy losses, we can approximately tell the amount of theft.

Note that the work in the previous two sections are not limited to single-layer system, but the work of this section is only limited to one-layer system. In the next section, we will extend the one-layer model to a multi-layer model.

2.4.1 On the Measurement of Electric Current and Energy

In this subsection, we first review the model in [20], which uses the measurements of energy supply, each user's energy consumption and the instantaneous electric current at the entry of each user to estimate the transmission resistance of the link to each user. Then we propose a simple improvement of the model in [20] by adding a non-negativity constraint. We assume that the measurement of electric current is not tampered with. If the measurement of electric current is tampered with, then we can first estimate the tampering ratio, and divide each measurement by the tampering ratio to recover the measurement before tampering. That is, the electric current flowing to the user j at time t_i can be recovered by

$$\hat{I}_j^{in}(i) = \frac{\tilde{I}_j^{in}(i)}{r_j(i)}. \tag{2.9}$$

Setting of Our Model

The settings described by Definition 1 also apply here. In addition, the tree topology adopts a single-layer structure. And the electric current is measured at the MPs as well, at time $t_1, t_2, \cdots, t_m$. The tree model used in this section is depicted by Figure 2.1a. Also, let α denote the distribution parameter of the entire system.

For any $1 \le i \le m, 1 \le j \le n$, $s(i)$ denotes the measurement of the energy supply of the whole grid in time interval $[t_{i-1}, t_i]$; $d_j(i)$ denotes the measurement of the energy consumption of the user (leaf) at the jth branch at time interval $[t_{i-1}, t_i]$. For any $0 \le i \le m, 1 \le j \le n$, $I_j^{in}(i)$ denotes the input current to the user (leaf) at the jth branch at time t_i; $\tilde{I}_j^{in}(i)$ denotes the measurement of $I_j^{in}(i)$; R_j denotes the resistance of the edge on the jth branch.

$\mathcal{T}_j(i)$ denotes the theft on the jth branch of DT at the time interval $[t_{i-1}, t_i]$.

Assumptions and Objective

We assume $m \geq n$. We assume that the measurements of $I_j^{in}(i)$ for all $1 \leq i \leq m, 1 \leq j \leq n$ are not tampered with. That is to say, $I_j^{in}(i) = \tilde{I}_j^{in}(i)$. We assume there is no unknown link secretly introduced. Given the measurements $\tilde{I}_j^{in}(i), s(i), d_j(i)$ for all $0 \leq i \leq m, 1 \leq j \leq n$, our objective is to estimate the transmission resistance $R_1, R_2, \cdots, R_n$.

Formulation

We first review the formulation of the problem in [20].

With the measurements of instantaneous current at the entry of user j at the start and end of the interval $[t_{i-1}, t_i]$, we estimate the instantaneous current at the entry of user j at each moment of the time interval $[t_{i-1}, t_i]$ by linear approximation

$$\hat{I}_j(t) = \tilde{I}_j(i-1) + \zeta_j(i)(t - t_{i-1}), \qquad t_{i-1} \leq t \leq t_i,$$

where ζ_j denotes the slope of the current at the time interval $[t_{i-1}, t_i]$ and ζ_j is defined as

$$\zeta_j(i) := \frac{\tilde{I}_j(i) - \tilde{I}_j(i-1)}{t_i - t_{i-1}}.$$

The estimated amount of ohmic losses of branch j at time interval $[t_{i-1}, t_i]$ is

$$\hat{L}_j(i) = \int_{t_{i-1}}^{t_i} \hat{I}_j(t)^2 R_j dt, \tag{2.10}$$

Since we have $t = \frac{\tilde{I}_j(t) - \tilde{I}_j(t_{i-1})}{\zeta_j(i)} + t_{i-1}$ at time interval $[t_{i-1}, t_i]$, Equation (2.22) can be re-written as

$$\begin{aligned}
\hat{L}_j(i) &= \frac{1}{\zeta_j(i)} \int_{\tilde{I}_j(i-1)}^{\tilde{I}_j(i)} \hat{I}_j(t)^2 R_j d\hat{I}_j(t) \\
&= \frac{R_j}{3\zeta_j(i)} [\tilde{I}_j(i)^3 - \tilde{I}_j(i-1)^3] \\
&= \frac{(t_i - t_{i-1}) R_j}{3[\tilde{I}_j(i) - \tilde{I}_j(i-1)]} [\tilde{I}_j(i)^3 - \tilde{I}_j(i-1)^3] \\
&= \frac{(t_i - t_{i-1}) R_j}{3} [\tilde{I}_j(i)^2 + \tilde{I}_j(i)\tilde{I}_j(i-1) + \tilde{I}_j(i-1)^2]
\end{aligned}$$

Then at any time t_i $(1 \leq i \leq m)$, we have the following equation by conservation of energy

$$\begin{aligned}
s(i) - \sum_{j=1}^{n} d_j(i) &= \sum_{j=1}^{n} \hat{L}_j(i) + \sum_{j=1}^{n} \mathcal{T}_j(i) + L_0 \\
&= \sum_{j=1}^{n} \frac{R_j}{3\zeta_j(i)} [\tilde{I}_j(i)^3 - \tilde{I}_j(i-1)^3] + \sum_{j=1}^{n} \mathcal{T}_j(i) + L_0
\end{aligned}$$

where L_0 is the amount of time-independent non-ohmic technical losses in a time interval. We construct the following vectors

$$Y = \begin{bmatrix} s(1) - \sum_{j=1}^{n} d_j(1) \\ s(2) - \sum_{j=1}^{n} d_j(2) \\ \vdots \\ s(m) - \sum_{j=1}^{n} d_j(m) \end{bmatrix}, x = \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \\ L_0 \end{bmatrix}, T = \begin{bmatrix} \sum_{j=1}^{n} \mathcal{T}_j(1) \\ \sum_{j=1}^{n} \mathcal{T}_j(2) \\ \vdots \\ \sum_{j=1}^{n} \mathcal{T}_j(m) \end{bmatrix}, \tag{2.11}$$

and the following matrix

$$H = \begin{bmatrix} \frac{\tilde{I}_1(1)^3 - \tilde{I}_1(0)^3}{3\zeta_1(1)} & \frac{\tilde{I}_2(1)^3 - \tilde{I}_2(0)^3}{3\zeta_2(1)} & \cdots & \frac{\tilde{I}_n(1)^3 - \tilde{I}_n(0)^3}{3\zeta_n(1)} & 1 \\ \frac{\tilde{I}_1(2)^3 - \tilde{I}_1(1)^3}{3\zeta_1(2)} & \frac{\tilde{I}_2(2)^3 - \tilde{I}_2(1)^3}{3\zeta_2(2)} & \cdots & \frac{\tilde{I}_n(2)^3 - \tilde{I}_n(1)^3}{3\zeta_n(2)} & 1 \\ \cdots & \cdots & \cdots & \cdots & 1 \\ \frac{\tilde{I}_1(m)^3 - \tilde{I}_1(m-1)^3}{3\zeta_1(m)} & \frac{\tilde{I}_2(m)^3 - \tilde{I}_2(m-1)^3}{3\zeta_2(m)} & \cdots & \frac{\tilde{I}_n(m)^3 - \tilde{I}_n(m-1)^3}{3\zeta_n(m)} & 1 \end{bmatrix}.$$

Thus the time series of the technical losses $\hat{L} \in \mathbb{R}^m$ can be approximated as

$$\hat{L} \approx Hx \tag{2.12}$$

By conservation of energy, we have

$$Y = \hat{L} + T \approx Hx + T,$$

where Y and H are known, x and T are unknown. [20] uses the least squares estimation to estimate x. Since the amount of power theft T, the transmission resistance as well as the amount of technical non-ohmic losses are non-negative, we impose the following two constraints $Y \geq Hx$ and $x \geq 0$ for x. Consequently we estimate x by solving the following optimization problem

$$\begin{aligned} \underset{x \in \mathbb{R}^n}{\text{minimize}} \quad & \|Y - Hx\|_1, \\ \text{subject to} \quad & Hx \leq Y, x \geq 0. \end{aligned} \tag{2.13}$$

The minimizer of this problem contains the estimation of the resistance of each transmission link and the time-independent non-ohmic technical loss. The numerical results of solving Problem (2.13) are shown in Section 5.3.1.

2.4.2 On the Measurement of Electric Current and Voltage

With the measurement of energy and electric current, an accurate estimation of resistance depends on the sparsity of occurrence of theft. In this subsection, we propose a solution to estimate transmission resistance using the measurement of electric current and voltage.

Given the measurements of the electric current and voltage at the entry of the root and each user, our objective is to estimate the resistance of each transmission link. In this subsection, we assume that the measurements of voltage and the measurements of the input electric current at the root are not tampered with. In fact, it is normally difficult to tamper with voltage measurements.

Setting of Our Model

The settings described by Definition 1 also apply here. In addition, the tree topology adopts a single-layer structure. And the electric current and the voltage are measured at the MPs as well, at time $t_1, t_2, \cdots, t_m$. The tree model used in this section is depicted by Figure 2.1b. Also, let α denote the distribution parameter of the entire system.

For any $0 \le i \le m, 1 \le j \le n$, $I_0^{in}(i)$ denotes the input current to the root at time t_i; $I_j^{in}(i)$ denotes the input current to the user (leaf) at the jth branch at time t_i; $V_0^{in}(i)$ denotes the voltage at the entry of the root at time t_i; $V_j^{in}(i)$ denotes the voltage at the entry of the user (leaf) at the jth branch at time t_i; $\tilde{I}_0^{in}(i), \tilde{I}_j^{in}(i), \tilde{V}_0^{in}(i)$, and $\tilde{V}_j^{in}(i)$ respectively denotes the measurements of $I_0^{in}(i), I_j^{in}(i), V_0^{in}(i)$, and $V_j^{in}(i)$; R_j denotes the resistance of the link at the jth branch.

Assumptions and Objective

We assume $m \ge n$. We assume the measurement of the voltage cannot be tampered with. We assume that there is no unknown link secretly introduced. Different from Subsection 2.4.1, we do not assume that the measurement of electric current is not tampered with. Given the measurements $\tilde{I}_0^{in}(i), \tilde{I}_j^{in}(i), \tilde{V}_0^{in}(i), \tilde{V}_j^{in}(i)$ for all $1 \le i \le m, 1 \le j \le n$, our objective is to estimate the transmission resistance $R_1, R_2, \ldots, R_n$.

Formulation

We propose a novel formulation to estimate the resistance of each link in a single-layer tree topology as follows.

If $\tilde{I}_j^{in}(i)$ is not tampered with at time t_i for $1 \le j \le n$, then $\alpha\tilde{I}_0^{in}(i)$ and $\sum_{j=1}^{n} \tilde{I}_j^{in}(i)$ are equal within a tolerance of small measurement noise $f \in \mathbb{R}^n$, that is

$$\alpha\tilde{I}_0^{in}(i) = \sum_{j=1}^{n} \tilde{I}_j^{in}(i) + f, \tag{2.14}$$

Thus the difference between $\alpha\tilde{I}_0^{in}(i)$ and $\sum_{j=1}^{n} \tilde{I}_j^{in}(i)$ reflects the accuracy of measurement at time t_i. If there exists some t_i when Equation (2.14) holds for small f, then we assume the measurements $\tilde{V}_0^{in}(i), \tilde{V}_j^{in}(i), \tilde{I}_0^{in}(i), \tilde{I}_j^{in}(i)$ are accurate. Then the measurement at time t_i will be sufficient for us to estimate the resistance. Thus R_j can be estimated by

$$\hat{R}_j = \frac{\alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(i)}{\tilde{I}_j^{in}(i)}, \forall 1 \le j \le n. \tag{2.15}$$

After the estimation $\hat{R}_j$ (of resistance R_j) is obtained, we can estimate the electric current of the jth branch at time t_i by

$$\hat{I}_j^{in}(i) = \frac{\alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(i)}{\hat{R}_j}$$

for any $1 \le i \le m$. Then we compare the estimated $\hat{I}_j^{in}(i)$ with the measurement $\tilde{I}_j^{in}(i)$. If $\tilde{I}_j^{in}(i) \approx \hat{I}_j^{in}(i)$, then no theft occur at the jth branch at time t_i; otherwise theft may occur at the jth branch at time t_i.

However, if tampering occurs all the time, then (2.15) cannot be used to estimate the resistance from the measurement of current. One way to deal with this situation is to estimate the tampering ratios and recover the real currents flowing to the thieves. In addition, we propose another method to detect tampering as follows.

According to our prior knowledge about this system, the following constraints should hold

$$\begin{aligned} \tilde{I}_0^{in}(i) &\ge \sum_{j=1}^{n} \frac{\alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(i)}{R_j}, \\ \alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(i) &\ge \tilde{I}_j^{in}(i)R_j, \forall 1 \le j \le n, \end{aligned}$$

which can be rephrased to

$$\sum_{j=1}^{n} \frac{\alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(t)}{R_j} \le \tilde{I}_0^{in}(i), \tag{2.16}$$

$$-\frac{\alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(i)}{R_j} \le -\tilde{I}_j^{in}(i), \forall 1 \le j \le n, \tag{2.17}$$

At time t_i $(1 \le i \le m)$, we want to minimize the following objective

$$\sum_{j=1}^{n} \left[\frac{\alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(i)}{R_j} - \tilde{I}_j^{in}(i) \right]$$

To vectorize the above expression, we set the vector $\tilde{I}^{out}(i) \in \mathbb{R}^n$ whose jth entry is $\tilde{I}_j^{in}(i)$ for all $1 \le j \le n$, and the diagonal matrix $D(i) \in \mathbb{R}^{n\times n}$ whose diagonal entries are

$$(D(i))_{jj} = \alpha\tilde{V}_0^{in}(i) - \tilde{V}_j^{in}(i), \forall 1 \le j \le n.$$

In other words,

$$\tilde{I}^{out}(i) = \begin{bmatrix} \tilde{I}_1^{in}(i) \\ \tilde{I}_2^{in}(i) \\ \vdots \\ \tilde{I}_n^{in}(i) \end{bmatrix}, D(i) = \begin{bmatrix} \alpha\tilde{V}_0^{in}(i) - \tilde{V}_1^{in}(i) & 0 & 0 & 0 \\ 0 & \alpha\tilde{V}_0^{in}(i) - \tilde{V}_2^{in}(i) & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \alpha\tilde{V}_0^{in}(i) - \tilde{V}_n^{in}(i) \end{bmatrix}.$$

We set the unknown vector $x \in \mathbb{R}^n$ as

$$x = \begin{bmatrix} \frac{1}{R_1} \\ \frac{1}{R_2} \\ \vdots \\ \frac{1}{R_n} \end{bmatrix}.$$

Then the objective can be vectorized as ${\mathbb{1}_n}^\top (D(i) \cdot x - \tilde{I}^{out}(i))$, where $\mathbb{1}_n \in \mathbb{R}^n$ is a vector of all ones, and the constraints (2.16) and (2.17) can also be rewritten as

$$\begin{aligned} -D(i) \cdot x &\leq -\tilde{I}^{out}(i), \ \forall 1 \leq i \leq m, \\ \mathbb{1}_n^\top D(i) \cdot x &\leq \tilde{I}^{out}(i), \ \forall 1 \leq i \leq m. \end{aligned}$$

At each time t_i, there is such an objective that we want to minimize, however, the weight of the objective at each moment differs. If the equation $\tilde{I}_0^{in}(i) - {\mathbb{1}_n}^\top \tilde{I}^{out}(i)$ is small at time t_i, then the weight of the objective at this moment is high and we want to minimize the objective at t_i as much as possible; otherwise the weight of the objective is low and we would spend less effort to minimize this objective than other objective with higher weight. That is to say, we need to assign a weight to the objective of each moment such that the objective has high weight whenever $\tilde{I}_0^{in}(i) - {\mathbb{1}_n}^\top \tilde{I}^{out}(i)$ is small. As a result, we assign the following weight to the objective at time t_i

$$\frac{1}{(\tilde{I}_0^{in}(i) - {\mathbb{1}_n}^\top \tilde{I}^{out}(i))^k},$$

where k is a parameter that we need to tune. As a whole, the objective that we want to minimize among all the m observations is a function about x,

$$f(x) \coloneqq \sum_{i=1}^{m} \frac{{\mathbb{1}_n}^\top (D(i) \cdot x - \tilde{I}^{out}(i))}{(\tilde{I}_0^{in}(i) - \sum_{j=1}^{n} \tilde{I}_j^{in}(i))^k}.$$

Note that $\tilde{I}^{out}(i)$ is independent of x, it does not affect the result of optimization if we remove $\tilde{I}^{out}(i)$ from $f(x)$. We construct the following matrices

$$A = \begin{bmatrix} \frac{D(1)}{(\tilde{I}_0^{in}(t_1) - \sum_{j=1}^{n} \tilde{I}_j^{in}(t_1))^k} \\ \frac{D(2)}{(\tilde{I}_0^{in}(t_2) - \sum_{j=1}^{n} \tilde{I}_j^{in}(t_2))^k} \\ \vdots \\ \frac{D(m)}{(\tilde{I}_0^{in}(t_m) - \sum_{j=1}^{n} \tilde{I}_j^{in}(t_m))^k} \end{bmatrix} \in \mathbb{R}^{mn \times n}, \ A_1 = \begin{bmatrix} -D(1) \\ -D(2) \\ \vdots \\ -D(m) \end{bmatrix} \in \mathbb{R}^{mn \times n}, \ A_2 = \begin{bmatrix} {\mathbb{1}_n}^\top D(1) \\ {\mathbb{1}_n}^\top D(2) \\ \vdots \\ {\mathbb{1}_n}^\top D(m) \end{bmatrix} \in \mathbb{R}^{m \times n},$$

and the following vectors

$$b_1 = \begin{bmatrix} -\tilde{I}^{out}(1) \\ -\tilde{I}^{out}(2) \\ \vdots \\ -\tilde{I}^{out}(m) \end{bmatrix} \in \mathbb{R}^{mn}, \ b_2 = \begin{bmatrix} \tilde{I}^{in}(1) \\ \tilde{I}^{in}(2) \\ \vdots \\ \tilde{I}^{in}(m) \end{bmatrix} \in \mathbb{R}^{m},$$

then $f(x)$ can be vectorized as $f(x) \coloneqq \mathbb{1}_{mn}{}^{\top} Ax$, where $\mathbb{1}_{mn} \in \mathbb{R}^{mn}$ is a vector of all ones, and the optimization problem about resistance can be formulated as follows

$$\begin{aligned} \min_{x} \quad & f(x) \coloneqq \mathbb{1}_{mn}{}^{\top} Ax \\ \text{subject to} \quad & A_1 x \le b_1, \\ & A_2 x \le b_2. \end{aligned} \tag{2.18}$$

This is a linear program which can be efficiently solved by existing algorithms. The numerical results of solving Problem (2.18) are shown in Section 5.3.2.

2.5 Estimation of Transmission Resistance in Multi-layer System

In this section, we extend the formulations described in Section 2.4 to a multi-layer tree topology.

2.5.1 On the Measurement of Electric Current and Energy

Setting of Our Model

The settings described by Definition 1 also apply here. In addition, the electric current and the voltage are measured at the MPs as well, at time $t_1, t_2, \cdots, t_m$. The tree model used in this section is depicted by Figure 1.3b.

We also use the following notations to represent the tree model. Let $\bar{n}$ denote the number of layers of the tree, then the layer number ranges from 0 to $\bar{n}-1$. Let α_i denote the transformer parameter of the DT located at layer i, $0 \le i \le \bar{n}-2$.

For any $0 \le i \le m, 1 \le j \le n$, $s(i)$ denotes the measurement of the energy supply of the whole grid in time interval $[t_{i-1}, t_i]$; $d_j(i)$ denotes the measurement of the energy consumption of the user at the leaf node labeled as j at time interval $[t_{i-1}, t_i]$; $I_v^{in}(i)$ denotes the input current to node v at time t_i; $I_{u\to v}(i)$ denotes the electric current flowing from node u to node v at time t_i; $R_{u\to v}$ denotes the resistance of the tree edge from node u to node v; $\mathcal{T}_{u\to v}(i)$ denotes the amount of power theft along the tree edge from node u to node v at time interval $[t_{i-1}, t_i]$; $\tilde{I}_v^{in}(i), \tilde{I}_{u\to v}(i)$ respectively denote the measurements of $I_v^{in}(i), I_{u\to v}(i)$; $\hat{R}_{u\to v}$ denotes the estimation of $R_{u\to v}$.

Assumptions and Objective

We assume $m \ge n$. We assume the measurement of $I_v^{in}(i)$ $(1 \le i \le m)$ for each leaf v of the tree is not tampered with. That is to say, $I_v^{in}(i) = \tilde{I}_v^{in}(i)$. We assume that there is no unknown link secretly introduced. Given the measurements $s(i), d_j(i)$ for all

$1 \le i \le m, 1 \le j \le n$, and measurements $\tilde{I}_v^{in}(i)$ $(1 \le i \le m)$ for any leaf node v, our objective is to estimate the transmission resistance $R_{u\to v}$ for any transmission link $u \to v$ in the tree.

Formulation

We extend the formulation in [20] to a multi-layer tree topology as follows.

First, we have the measurement $\tilde{I}_v^{in}(i)$ for any node v locating at the $(\bar{n}-1)$th layer at time t_i. Then we can estimate the electric current at the entry of any node u at the $(\bar{n}-2)$th layer at time t_i by

$$I_u^{in}(i) = \frac{1}{\alpha_{\bar{n}-2}} \times \sum_{v \in \textbf{Children}(u)} I_{u\to v}(i) \tag{2.19}$$

$$\approx \frac{1}{\alpha_{\bar{n}-2}} \times \sum_{v \in \textbf{Children}(u)} \tilde{I}_{u\to v}(i) \tag{2.20}$$

For any $v \in \textbf{Children}(u)$, v is locating at the $(\bar{n}-1)$th layer of the tree and hence the measurement $\tilde{I}_v^{in}(i)$ is available at time t_i. Thus this estimation (2.20) is computable. Then we can propagate such computation layer by layer from bottom to top to estimate the electric current at the entry of any node at any intermediate layer of the tree.

For any link $u \to v$ in the tree, with the estimation (or measurements) of instantaneous transmission current of the link $u \to v$ at the start and end of the interval $[t_{i-1}, t_i]$, $\tilde{I}_{u\to v}(i-1)$ and $\tilde{I}_{u\to v}(i)$, we estimate the instantaneous current of this link at each moment of the time interval $[t_{i-1}, t_i]$ by linear approximation

$$\hat{I}_{u\to v}(t) = \tilde{I}_{u\to v}(i-1) + \zeta_{u\to v}(i)(t - t_{i-1}), \qquad t_{i-1} \le t \le t_i, \tag{2.21}$$

where $\zeta_{u\to v}(i) = \frac{\tilde{I}_{u\to v}(i) - \tilde{I}_{u\to v}(i-1)}{t_i - t_{i-1}}$ is the slope of electric current at the time interval $[t_{i-1}, t_i]$. The amount of estimated technical losses of the link $u \to v$ at time interval $[t_{i-1}, t_i]$ is

$$\hat{L}_{u\to v}(i) = \int_{t_{i-1}}^{t_i} \hat{I}_{u\to v}(t)^2 R_{u\to v} dt, \tag{2.22}$$

Using Equation (2.21), Equation (2.22) can be re-written as

$$\begin{aligned} \hat{L}_{u\to v}(i) &= \frac{1}{\zeta_{u\to v}(i)} \int_{\tilde{I}_{u\to v}(i-1)}^{\tilde{I}_{u\to v}(i)} \hat{I}_{u\to v}(t)^2 R_{u\to v} d\hat{I}_{u\to v}(t) \\ &= \frac{R_{u\to v}}{3\zeta_{u\to v}(i)} [\tilde{I}_{u\to v}(i)^3 - \tilde{I}_{u\to v}(i-1)^3] \end{aligned}$$

Then at any time $t_i (1 \le i \le m)$, we have the following equation

$$\begin{aligned} s(i) - \sum_{j=1}^{n} d_j(i) &= \sum_{(u,v)\in E} \hat{L}_{u\to v}(i) + \sum_{(u,v)\in E} \mathcal{T}_{u\to v}(i) + L_0 \\ &= \sum_{(u,v)\in E} \frac{R_{u\to v}}{3\zeta_{u\to v}(i)} [\tilde{I}_{u\to v}(i)^3 - \tilde{I}_{u\to v}(i-1)^3] + \sum_{(u,v)\in E} \mathcal{T}_{u\to v}(i) + L_0 \end{aligned}$$

where E denotes the set of edges of the tree; $(u, v) \in E$ denotes that there is a link from the node u to node v; $L_0 \in \mathbb{R}$ is the amount of time-independent non-ohmic technical losses in a time interval. Then we have the linear system same as in section 2.4.2.

$$Y = Hx + T,$$

where $R_{u\to v}$ for each transmission link (u, v) in the tree is a component of the unknown vector x and the last entry of x is the amount of time-independent non-ohmic technical losses in a time interval; the last column of H contains all ones, and the entry of H locating at the ith row and at the column corresponding to the link (u, v) is set to $\frac{\tilde{I}_{u\to v}(i)^3 - \tilde{I}_{u\to v}(i-1)^3}{3\zeta_{u\to v}(i)}$. Similarly, we estimate x by solving the optimization problem (2.13).

2.5.2 On the Measurement of Electric Current and Voltage

Setting of Our Model

The settings described by Definition 1 also apply here. In addition, the electric current and the voltage are measured at the MPs as well, at time $t_1, t_2, \cdots, t_m$. The tree model used in this section is depicted by Figure 1.3c.

We also use the following notations to represent the tree model. Let $\bar{n}$ denote the number of layers, then the layer number ranges from 0 to $\bar{n} - 1$. Let α_i denote the transformer parameter of the DT located at layer i, $0 \le i \le \bar{n} - 2$. Let v_{kj} denote the j^{th} node (from left to right) at the k^{th} layer, with $\mathbf{Parent}(v_{kj})$ denoting the parent of the node v_{kj} and $\mathbf{Children}(v_{kj})$ denoting the set of children of the node v_{kj}.

We regularly measure the instantaneous electric current and voltage at the entries of the root and the leaves of the tree at time $t = t_1, \cdots, t_{m-1}, t_m$. $V_0^{in}(i)$ denotes the voltage at the entry of the root node at time t_i; $V_{k,j}^{in}(i)$ denotes the voltage at the entry of the node v_{kj} at time t_i; $V_{v_{lr}\to v_{kj}}^{out}(i)$ denotes the voltage at the exit of the node v_{lr} directed towards node v_{kj} at time t_i; $I_0^{in}(i)$ denotes the input current to the root node at time t_i; $I_{k,j}^{in}(i)$ denotes the input current to node v_{kj} at time t_i; $I_{v_{lr}\to v_{kj}}^{out}(i)$ denotes the output current of node v_{lr} to node v_{kj} at time t_i; $R_{v_{lr}\to v_{kj}}$ denotes the resistance of the tree edge between node v_{lr} and node v_{kj}; $\mathbf{path}(x, y)$ denotes the set of edges that are on the path from x to y; $V_0^{in}(i)$, $V_{k,j}^{in}(i)$, $V_{v_{lr}\to v_{kj}}^{out}(i)$, $I_0^{in}(i)$, $I_{k,j}^{in}(i)$, and $I_{v_{lr}\to v_{kj}}^{out}(i)$ represent the true values before tampering; $\tilde{V}_0^{in}(i)$, $\tilde{V}_{k,j}^{in}(i)$, $\tilde{V}_{v_{lr}\to v_{kj}}^{out}(i)$, $\tilde{I}_0^{in}(i)$, $\tilde{I}_{k,j}^{in}(i)$, and $\tilde{I}_{v_{lr}\to v_{kj}}^{out}(i)$ respectively denote the measurements of $V_0^{in}(i)$, $V_{k,j}^{in}(i)$, $V_{v_{lr}\to v_{kj}}^{out}(i)$, $I_0^{in}(i)$, $I_{k,j}^{in}(i)$, and $I_{v_{lr}\to v_{kj}}^{out}(i)$; $\hat{R}_{v_{lr}\to v_{kj}}$ denotes the estimation of $R_{v_{lr}\to v_{kj}}$.

Assumptions and Objective

We assume $m \ge n$. We assume the measurement of $I_{k,j}^{in}(i)$ for all v_{kj} in the tree and all $1 \le i \le m$ are not tampered with. That is to say, $I_{k,j}^{in}(i) = \tilde{I}_{k,j}^{in}(i)$. We assume that there is no unknown link secretly introduced. Given the measurements $\tilde{V}_0^{in}(i)$, for all $1 \le i \le m$,

and the measurements $\tilde{V}^{in}_{k,j}(i)$, $\tilde{I}^{in}_{k,j}(i)$ for any leaf node v_{kj} for all $1 \le i \le m$, our objective is to estimate the transmission resistance $R_{v_{lr}\to v_{kj}}$ for any transmission link $v_{lr} \to v_{kj}$ in the tree.

Formulation

We propose a novel formulation to estimate the resistance of each link in a multi-layer tree topology as follows.

Along the leftmost path (the yellow path in Figure 2.2) at the tree, we have the following equations at time t_i:

$$\alpha_0 V_0(i) - I^{in}_{11}(i) R_{v_{01}\to v_{11}} = V^{in}_{11}(i), \tag{2.23}$$
$$\alpha_1 V^{in}_{11}(i) - I^{in}_{21}(i) R_{v_{11}\to v_{21}} = V^{in}_{21}(i), \tag{2.24}$$
$$\alpha_2 V^{in}_{21}(i) - I^{in}_{31}(i) R_{v_{21}\to v_{31}} = V^{in}_{31}(i), \tag{2.25}$$
$$\vdots \qquad\qquad \vdots$$
$$\alpha_{\bar{n}-2} V^{in}_{\bar{n}-2}(i) - I^{in}_{\bar{n}-1,1}(i) R_{v_{\bar{n}-2,1}\to v_{\bar{n}-1,1}} = V^{in}_{\bar{n}-1,1}(i). \tag{2.26}$$

Substitute the left hand side of (2.23) for $V^{in}_{11}(i)$ into (2.24), we can get

$$\alpha_1\alpha_0 V_0(i) - \alpha_1 I^{in}_{11}(i) R_{v_{01}\to v_{11}} - I^{in}_{21}(i) R_{v_{11}\to v_{21}} = V^{in}_{21}(i). \tag{2.27}$$

Substitute the left hand side of (2.27) for $V^{in}_{21}(i)$ into (2.25), we can get

$$\alpha_2\alpha_1\alpha_0 V_0(i) - \alpha_2\alpha_1 I^{in}_{11}(i) R_{v_{01}\to v_{11}} - \alpha_2 I^{in}_{21}(i) R_{v_{11}\to v_{21}} - I^{in}_{31}(i) R_{v_{21}\to v_{31}} = V^{in}_{31}(i). \tag{2.28}$$

We proceed such substitution inductively and we eventually get

$$(\prod_{j=0}^{\bar{n}-2} \alpha_j) V_0(i) - \sum_{k=1}^{\bar{n}-1} (\prod_{j=k}^{\bar{n}-2} \alpha_j) I^{in}_{k,1}(i) R_{v_{k-1,1}\to v_{k,1}} = V_{\bar{n}-1,1}(i). \tag{2.29}$$

Thus we have the following linear system about $R_{v_{0,1}\to v_{1,1}}, R_{v_{1,1}\to v_{2,1}}, \ldots, R_{v_{n-1,1}\to v_{n,1}}$:

$$\begin{bmatrix} (\prod_{j=1}^{\bar{n}-2} \alpha_j) I^{in}_{1,1}(1) & \ldots & \alpha_{\bar{n}-2} I^{in}_{\bar{n}-2,1}(1) & I^{in}_{\bar{n}-1,1}(1) \\ (\prod_{j=1}^{\bar{n}-2} \alpha_j) I^{in}_{1,1}(2) & \ldots & \alpha_{\bar{n}-2} I^{in}_{\bar{n}-2,1}(2) & I^{in}_{\bar{n}-1,1}(2) \\ \ldots & & & \\ (\prod_{j=1}^{\bar{n}-2} \alpha_j) I^{in}_{1,1}(m) & \ldots & \alpha_{\bar{n}-2} I^{in}_{\bar{n}-2,1}(m) & I^{in}_{\bar{n}-1,1}(m) \end{bmatrix} \begin{bmatrix} R_{v_{0,1}\to v_{1,1}} \\ R_{v_{1,1}\to v_{2,1}} \\ \ldots \\ R_{v_{\bar{n}-2,1}\to v_{\bar{n}-1,1}} \end{bmatrix}$$
$$= \begin{bmatrix} (\prod_{j=0}^{\bar{n}-2} a_j) V_0(1) - V_{\bar{n}-1,1}(1) \\ (\prod_{j=0}^{\bar{n}-2} a_j) V_0(2) - V_{\bar{n}-1,1}(2) \\ \ldots \\ (\prod_{j=0}^{\bar{n}-2} a_j) V_0(m) - V_{\bar{n}-1,1}(m) \end{bmatrix} \tag{2.30}$$

If we let

$$A := \begin{bmatrix} (\prod_{j=1}^{\bar{n}-2} \alpha_j)\tilde{I}^{in}_{1,1}(1) & \dots & \alpha_{\bar{n}-2}\tilde{I}^{in}_{\bar{n}-2,1}(1) & \tilde{I}^{in}_{\bar{n}-1,1}(1) \\ (\prod_{j=1}^{\bar{n}-2} \alpha_j)\tilde{I}^{in}_{1,1}(2) & \dots & \alpha_{\bar{n}-2}\tilde{I}^{in}_{\bar{n}-2,1}(2) & \tilde{I}^{in}_{\bar{n}-1,1}(2) \\ \dots & & & \\ (\prod_{j=1}^{\bar{n}-2} \alpha_j)\tilde{I}^{in}_{1,1}(m) & \dots & \alpha_{\bar{n}-2}\tilde{I}^{in}_{\bar{n}-2,1}(m) & \tilde{I}^{in}_{\bar{n}-1,1}(m) \end{bmatrix}, b := \begin{bmatrix} (\prod_{j=0}^{\bar{n}-2} a_j)\tilde{V}_0(1) - \tilde{V}_{\bar{n}-1,1}(1) \\ (\prod_{j=0}^{\bar{n}-2} a_j)\tilde{V}_0(2) - \tilde{V}_{\bar{n}-1,1}(2) \\ \dots \\ (\prod_{j=0}^{\bar{n}-2} a_j)\tilde{V}_0(m) - \tilde{V}_{\bar{n}-1,1}(m) \end{bmatrix},$$

and

$$x := \begin{bmatrix} R_{v_{0,1}\to v_{1,1}} \\ R_{v_{1,1}\to v_{2,1}} \\ \dots \\ R_{v_{n-1,1}\to v_{n,1}} \end{bmatrix},$$

then the resulting linear system $Ax \approx b$ is normally over-determined due to the measurement noise. Hence we use the minimizer of the following optimization problem

$$\min_{x\geq 0} \|Ax - b\|_1 \tag{2.31}$$

to be the estimator of the resistance of each link on the yellow path in Figure 2.2. The resistance of the links on any other path can be estimated in a similar way. The numerical results of solving Problem (2.31) are shown in Section 5.3.2.

2.6 A Big Picture

Figure 2.4 shows the big map of our theft detection procedure. Our method depends on the measurement of the electric currents that flows to each customer. If the electric currents measured by the smart meters satisfy the law of conservation (2.3), then we proceed to state S_t (of Figure 2.4). Otherwise we go to both state S_3 for the estimation of the tampering ratios and state S_4 for the recovery of electric currents. After the recovery, if we measure the voltages (at the root and the leaves), we can go to state S_8 to estimate the resistance of each link in the power grid by solving 2.31; otherwise we go to state S_9 to estimate the resistance of each link by solving 2.13 . After we estimate the resistances, we can go to state S_{11} to estimate the time series of electricity theft. If we find the estimated tampering ratio of some user is much greater than one and the amount of estimated theft is very large at some time, then this is a strong evidence of the existence of power theft.

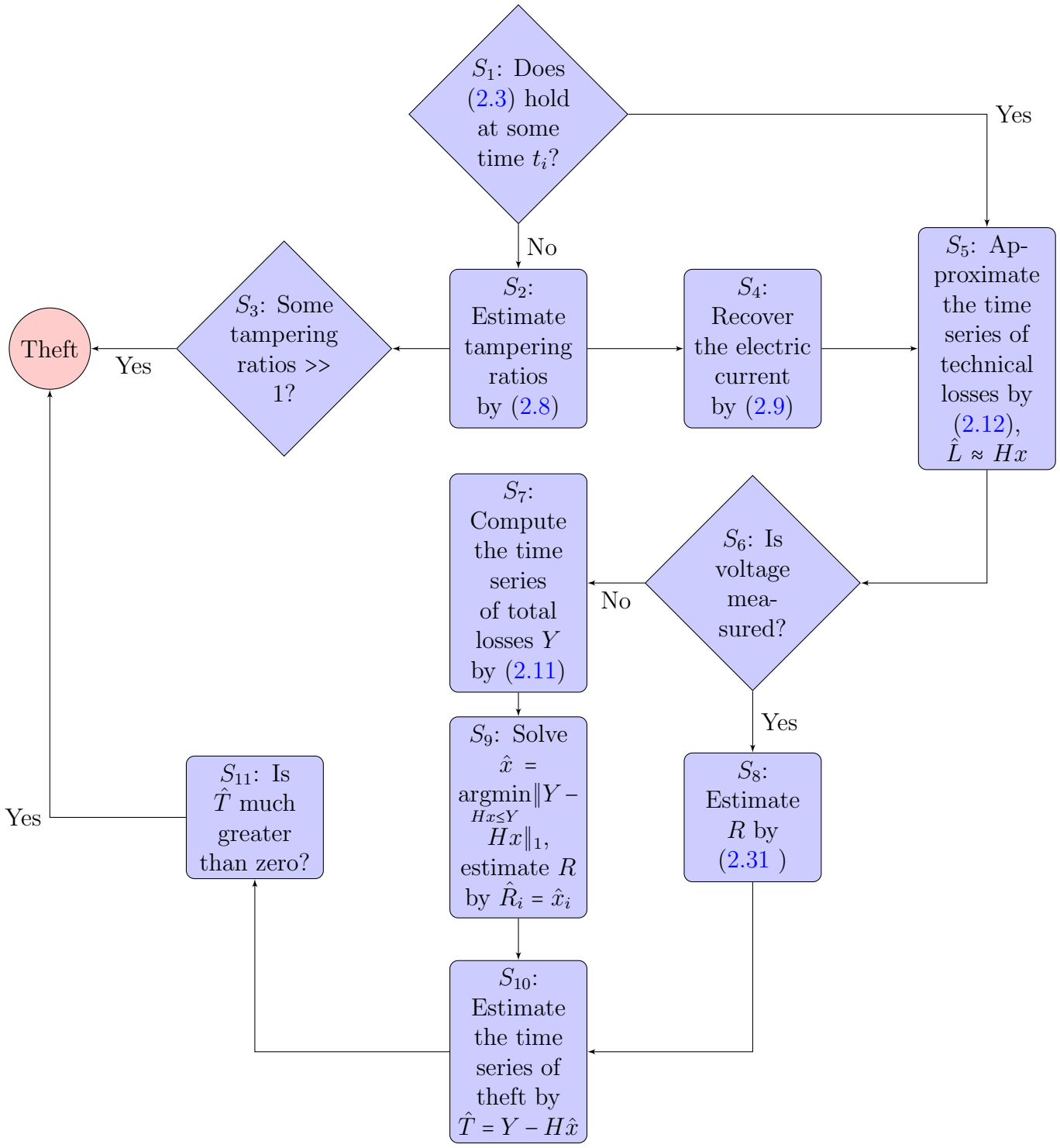


Figure 2.4: BigMap
$S_1, S_2, \cdots, S_{11}$ respectively denote the 11 states in the flow-chart.

Chapter 3

ℓ_1 Minimization in Non-negative Space

In Section 3.1 we review the formulation and the KKT conditions of a linear program. In Section 3.2, we analyze under what conditions the optimization problem $\min_{x \geq 0} \|y - Ax\|_1$ can give an exact reconstruction of the true underlying value x^*, assuming the observation $y \in \mathbb{R}^m$ is $Ax^* + e$, where e is a sparse noise vector. In Section 3.3, we argue that by adding additional feasible constraint $Y \geq Hx$, which appears in the formulation of Problem (2.13)

$$\begin{aligned} \underset{x \in \mathbb{R}^n}{\text{minimize}} \quad & \|Y - Hx\|_1, \\ \text{subject to} \quad & Hx \leq Y, x \geq 0. \end{aligned}$$

introduced previously, we can reduce the effect of outliers to the estimation of the resistance of each link. In Section 3.4, we propose a hyperplane separation algorithm that can potentially detect the time-varying theft in different scenarios described previously in Chapter 2.

3.1 Linear Programming and ℓ_1 Minimization

3.1.1 Linear Program

A linear program can be stated in the following form [4]

$$\begin{aligned} \min_{x \in \mathbb{R}^n} \quad & c^\top x, \\ \text{subject to} \quad & A_{\text{ineq}} x \leq b_{\text{ineq}}, \\ & A_{\text{eq}} x = b_{\text{eq}}, \end{aligned} \tag{3.1}$$

where $A_{\text{eq}} \in \mathbb{R}^{m_1 \times n}$, $A_{\text{ineq}} \in \mathbb{R}^{m_2 \times n}$ are two matrices, $c \in \mathbb{R}^n$, $b_{\text{eq}} \in \mathbb{R}^{m_1}$, $b_{\text{ineq}} \in \mathbb{R}^{m_2}$ are vectors, $x \in \mathbb{R}^n$ is an unknown vector. The term $c^\top x$ is the objective function. The

equality $A_{\text{eq}}x = b_{\text{eq}}$ and inequality $A_{\text{ineq}}x \leq b_{\text{ineq}}$ are the linear constraints. The objective of a linear program is to find an x that minimizes the objective function over the linear constraints. Generally, there is no closed form solution to Problem (3.1). Fortunately, as a convex optimization problem, a linear program can be solved efficiently by many effective numerical methods such as simplex methods and interior point methods.

Given a matrix $A \in \mathbb{R}^{m\times n}$ and a vector $b \in \mathbb{R}^m$, if $\text{rank}(A) < n$, then the linear system (about the unknown variable x)

$$Ax = b \tag{P}$$

is under-determined and it can have infinitely many solution. In the pursuit of simplicity, ℓ_1 regularization is often imposed to choose a sparse solution of equation (P). That is, we want to solve the following optimization problem [4]

$$\begin{aligned} \underset{x}{\text{minimize}} \quad & \|x\|_1 \\ \text{subject to} \quad & Ax = b \end{aligned} \tag{3.2}$$

This problem can be equivalently expressed as a linear programming problem. We define $\rho = |x|$, in other words, $\rho_i = |x_i|$, where ρ_i and x_i respectively denote the ith coordinate of ρ and x. Then ρ and x satisfy the constraint $-\rho \leq x \leq \rho$. In addition, $\|x\|_1 = e^\top \rho$, where e is a vector of ones. Therefore Problem (3.2) can be equivalently written as

$$\begin{aligned} \underset{x}{\text{minimize}} \quad & e^\top \rho, \\ \text{subject to} \quad & Ax = b, \\ & x - \rho \leq 0, \\ & -x - \rho \leq 0. \end{aligned}$$

which is in the form of a linear program.

3.1.2 KKT Conditions

A general optimization problem is typically formulated as below [4]

$$\begin{aligned} \min_{x\in\mathbb{R}^n} \quad & f(x), \\ \text{subject to} \quad & h_i(x) \leq 0, \quad i = 1, 2, \ldots, m, \\ & l_j(x) = 0, \quad j = 1, 2, \ldots, r, \end{aligned} \tag{3.3}$$

where f, h_i, l_j are all differentiable function. The Karush-Kuhn-Tucker(KKT) conditions of the above optimization problem in general form are [4]

$$\begin{aligned} \nabla f(x) + \sum_{i=1}^{m} u_i \nabla h_i(x) + \sum_{j=1}^{r} v_j \nabla l_j(x) &= 0, \\ u_i h_i(x) &= 0, \forall i, \\ h_i(x) &\leq 0, \forall i, \\ l_j(x) &= 0, \forall j, \\ u_i &\geq 0, \forall i, \end{aligned}$$

where $\nabla f(x)$, $\nabla h_i(x)$, $\nabla l_i(x)$ respectively denote the derivative of $f(x), h_i(x), l_i(x)$; u_i and v_i are called Lagrangian multiplier. The KKT conditions of (3.1) can be written as

$$\begin{aligned} c + A_{\text{ineq}}^{\top} u + A_{\text{eq}}^{\top} v &= 0, \\ \mathbf{diag}(u)(A_{\text{ineq}} x - b_{\text{ineq}}) &= 0, \\ A_{\text{ineq}} x &\leq b_{\text{ineq}}, \\ A_{\text{eq}} x &= b_{\text{eq}}, \\ u &\geq 0, \end{aligned}$$

where $\mathbf{diag}(u)$ is a diagonal matrix whose diagonal contains the entries of u.

3.2 Exact Reconstruction Based on Sparsity

In this section, we introduce an ℓ_1 minimization problem on which our theft detection framework heavily relies. Given a non-negative over-determined matrix $A \in \mathbb{R}^{m \times n}$, assume we have a non-negative vector $f \in \mathbb{R}^n$ and a sparse vector $e \in \mathbb{R}^m$ that has at most S non-zero entries, put $y := Af + e$. In this scenario, both A and y are known, f and e are unknown. We consider whether we can recover f from A and y. We estimate f by solving the following ℓ_1 minimization problem in the non-negative space

$$\begin{aligned} &\min && \|y - Ax\|_1, \\ &\text{subject to} && x \geq 0. \end{aligned} \tag{3.4}$$

We hope that the minimizer of Problem (3.4) is f. We show that under suitable conditions of the coefficient matrix A, the unknown non-negative input vector f is the unique solution to Problem (3.4). In the following subsections 3.2.1 and 3.2.2, the symbols f and e share the same meaning as we have just defined here.

The theft detection framework introduced in Chapter 2 solves four different optimization problems (2.5), (2.8), (2.13), (2.31) according to different sets of available measurements. Among these four formulations, Problem (2.5), (2.8) and (2.31) can be cast into the

same form (3.4). In different scenarios, f has different physical meanings while e means the difference between the measured values (of some electrical quantity) and the corresponding real values. This motivates us to investigate under what conditions of the coefficient matrix A the minimizer of Problem (3.4) gives an exact recovery of the real answer f.

Our analysis in this section is based on the work of [6] by Candes and Tao. The problem considered in [6] is $y = Af+e$ where f and A are not necessarily non-negative. They estimate f by solving an ℓ_1 minimization problem without the non-negativity constraint of x:

$$\min \quad \|y - Ax\|_1. \tag{3.5}$$

[8] and [30] consider the following problem

$$\begin{aligned} &\min && \|y - Ax\|_1, \\ &\text{subject to} && Ax \le y, \end{aligned} \tag{3.6}$$

which has an additional non-negativity constraint $Ax \le y$ compared to Problem (3.5). However, this is not the non-negativity that we are interested in. In our case, we are interested in putting the non-negativity constraint on x, i.e., $x \ge 0$.

In subsection 3.2.1 we first review the paper [6] and illustrate the motivation of our extension to their work. In subsection 3.2.2 we introduce how we extend the results in [6]. We use the following notations in the following sections. J_1, J_2 denote the following two two sets of integer indices

$$J_1 = \{1, 2, \ldots, n\}, J_2 = \{n+1, n+2, \ldots, m\}. \tag{3.7}$$

Given a matrix $F \in \mathbb{R}^{m\times n}$, a vector $c \in \mathbb{R}^m$, two sets $T \subset J_1 \cup J_2$ and $T' \subseteq J_1$, F_T denotes the sub-matrix of F with column indices $j \in T$; $F_{T',:}$ denotes the sub-matrix of F with row indices $i \in T'$; $F_{T',T}$ denotes the sub-matrix of F with row indices $i \in T'$ and column indices $j \in T$; F_j denotes the jth column of F; c_T denotes the sub-vector of c with row indices $j \in T$; c_i denotes the ith entry of c; $\mathbf{sgn}(x)$ denotes the vector whose entries are -1, 1, 0 corresponding to the negative entries, positive entries, zero entries of x respectively.

3.2.1 Decoding by Linear Programming

We first provide the definitions of several norms that will appear in the following contexts. The ℓ_1-norm $\|\cdot\|_1$ of a vector $v \in \mathbb{R}^n$ is defined to be [29]

$$\|v\|_1 = \sqrt{\sum_{i=1}^{n} |v_i|}. \tag{3.8}$$

The ℓ_2-norm $\|\cdot\|$ of a vector $v \in \mathbb{R}^n$ is defined to be [29]

$$\|v\| = \sqrt{\sum_{i=1}^{n} v_i^2}. \tag{3.9}$$

The ℓ_1-norm $\|\cdot\|_1$ of a matrix $M \in \mathbb{R}^{m\times n}$ is defined to be [29]

$$\|M\|_1 = \max_{1\le j\le n} \sum_{i=1}^{m} |M_{ij}|. \tag{3.10}$$

Then we review the following definitions introduced in [6].

Definition 2 *Let F be the matrix with finite collection of vectors $(F_j)_{j\in J} \in \mathbb{R}^m$ as columns. For every integer $1 \le S \le |J|$, the $S-$restricted isometry constant $\delta_S(F)$ with respect to F is the smallest number such that F_T obeys*

$$(1-\delta_S(F))\|c\|^2 \le \|F_T c\|^2 \le (1+\delta_S(F))\|c\|^2$$

for all subsets $T \subset J$ of cardinality at most S, and all real vectors c supported on T. Similarly, the $S, S'-$restricted orthogonal constants $\theta_{S,S'}(F)$ with respect to F for $S+S' \le |J|$ is the smallest number such that

$$|c^\top F_T^\top F_{T'} c'| \le \theta_{S,S'}(F)\|c\|\|c'\|$$

holds for all disjoint $T, T' \subset J$ of cardinality $|T| \le S$ and $|T'| \le S'$, and all real coefficients $(c_j)_{j\in T}$, $(c'_j)_{j\in T'}$.

The numbers δ_S and θ_S measures how close the columns of the matrix F corresponding to the non-zero entries of the vector c behave like an orthonormal system. Candes et al point out in [6] that δ_S and $\theta_{S,S'}$ are clearly non-decreasing in S, S'. Candes et al construct a matrix F such that $FA = 0$ and multiply F on both sides of $y = Af + e$ to obtain [6]

$$\tilde{y} := Fy = F(Af + e) = Fe.$$

Note that recovering f is equivalent to recovering e. Since y and F are known, $\tilde{y}$ can be computed. Let $d = y - Af$, then $Fd = F(y - Af) = \tilde{y} - FAf = \tilde{y}$. Therefore Problem (3.5) is equivalently written as [6]

$$\begin{aligned} &\min && \|d\|_1 \\ &\text{subject to} && Fd = \tilde{y} \end{aligned} \tag{3.11}$$

In [8] and [30], correspondingly, Problem (3.6) is equivalently written as

$$\begin{aligned} &\min && \|d\|_1, \\ &\text{subject to} && Fd = \tilde{y},\ d \ge 0. \end{aligned} \tag{3.12}$$

The following main result is provided in [6]:

Theorem 1 *Suppose that $S \ge 1$ is such that $\delta_S + \theta_S + \theta_{S,2S} < 1$, and let c be a real vector supported on a set $T \subset J$ obeying $|T| \le S$. Put $\tilde{y} := Fc$. Then c is the unique minimizer to*

$$\begin{aligned} &\min_d && \|d\|_1 \\ &\text{subject to} && Fd = \tilde{y} \end{aligned}$$

The companion result of Theorem 1 is as follows [6].

Theorem 2 *Suppose F is such that $FA = 0$ and let $S \geq 1$ be a number obeying the hypothesis of Theorem 1. Set $y = Af + e$, where e is a real vector supported on a set of size at most S. Then f is the unique minimizer to*

$$\min_{g} \quad \|y - Ag\|_1$$

The condition $\delta_S + \theta_S + \theta_{S,2S} < 1$ of Theorem 1 on S and F requires the vector c to be sufficiently sparse. Theorem 1 actually says that if c is sparse enough such that the condition $\delta_S + \theta_S + \theta_{S,2S} < 1$ holds, then c is the unique minimizer to the optimization problem mentioned in Theorem 1. The proof of Theorem 1 relies on the following two important lemmas in [6].

Lemma 1 *Given $F \in \mathbb{R}^{m\times n}$, let $S, S' \geq 1$ be such that $\delta_S(F) < 1$, and c be a real vector supported on $T \subset J_1$ such that $|T| < S$. Then there exists a vector $w \in \mathbb{R}^m$ such that $F_j^\top w = c_j$ for all $j \in T$. Furthermore, there is an exceptional set $E \subset J_1$ which is disjoint from T, of size at most*

$$|E| \leq S',$$

and with the properties

$$|F_j^\top w| \leq \frac{\theta_{S,S'}(F)}{(1-\delta_S(F))\sqrt{S}}\|c\|, \forall j \notin T \cup E$$

and

$$\|F_E^\top w\| \leq \frac{\theta_S(F)}{1-\delta_S(F)}\|c\|$$

In addition, $\|w\| \leq K\|c\|$ for some constant $K \geq 0$ only depending upon δ_S.

The detailed proof of this lemma can be found in the paper [6] . The main idea is that, if we set $w \in \mathbb{R}^m$ to be the vector

$$w := F_T(F_T^\top F_T)^{-1}c_T,$$

then it can be verified that w satisfies all the conditions above.

Lemma 2 *Given $F \in \mathbb{R}^{m\times n}$, let $S \geq 1$ be such that $\delta_S(F) + \theta_{S,2S}(F) < 1$, and c be a real vector supported on $T \subset J$ obeying $|T| \leq S$. Then there exits a vector w such that $F_j^\top w = c_j$ for all $j \in T$. Furthermore, w satisfies that*

$$|F_j^\top w| \leq \frac{\theta_S(F)}{(1-\delta_S(F)-\theta_{S,2S}(F))\sqrt{S}}\|c\|$$

for all $j \notin T$.

The detailed proof of this lemma can be found in the paper [6].

3.2.2 Non-negativity

The non-negativity constraint of x is not considered in [6] . In each scenario of our theft detection framework, f is non-negative. Hence we impose the non-negativity constraint and solve Problem (3.4) to find the minimizer. We investigate under what conditions of A the minimizer of Problem (3.4) provides the exact reconstruction of f.

Given two vectors $f \in \mathbb{R}^n, c \in \mathbb{R}^m$, we define the following two sets

$$Z := \{i : f_i = 0, i \in J_1\}, \backslash Z := \{i : f_i \neq 0, i \in J_1\}, \tag{3.13}$$

$$T := \{i : c_i \neq 0, i \in J_1 \cup J_2\}, \backslash T := \{i : c_i = 0, i \in J_1 \cup J_2\}. \tag{3.14}$$

Then we have the following equalities

$$Z \cup \backslash Z = J_1 \tag{3.15}$$

$$T \cup \backslash T = J_1 \cup J_2 \tag{3.16}$$

Let K be the size of the set Z, M be the size of the set T. For simplicity, we rearrange the entries of f and c such that $f_1 = f_2 = \ldots = f_K = 0, c_1 \neq 0, \ldots, c_M \neq 0$, in other words, $Z = \{1, 2, \ldots, K\}, T = \{1, 2, \ldots, M\}$. Thus f and c can be written as

$$f = \begin{bmatrix} f_Z \\ f_{\backslash Z} \end{bmatrix}, c = \begin{bmatrix} c_T \\ c_{\backslash T} \end{bmatrix}.$$

We also rearrange the columns and rows of A such that the columns of A correspond to f and the rows of A correspond to c.

We construct a matrix $H \in n \times m$ such that

$$HA = I, \tag{3.17}$$

where I is an n by n identity matrix. Namely, H is a left inverse of A. A can have many different left inverses. For example, if we set $H := (A^\top A)^{-1} A^\top$, then $HA = (A^\top A)^{-1} A^\top A = I$. Using $HA = I$, $d = y - Af$ and $f \geq 0$, we can get $Hd = H(y - Af) = Hy - f \leq Hy$. Let $\bar{y} := Hy$. Then Problem (3.4) can be equivalently written as

$$\begin{aligned} \min \quad & \|d\|_1 \\ \text{subject to} \quad & Hd \leq \bar{y} \\ & Fd = \tilde{y} \end{aligned} \tag{3.18}$$

Compared to Problem (3.11), Problem (3.18) has one more constraint $Hd \leq \bar{y}$. Imposing the constraint $Hd \leq \bar{y}$ may sacrifice the sparsity of the optimal solution of Problem (3.18). In other words, the minimizer of Problem (3.18) may be less sparse than the minimizer of Problem (3.11). This motivates us to explore whether imposing the constraint $Hd \leq \bar{y}$ requires fewer zero entries in the real underlying solution for exact reconstruction.

From $HA = I$ and $H = \begin{bmatrix} H_Z \\ H_{\setminus Z} \end{bmatrix}$, we require that

$$H_{Z,:}A = \begin{bmatrix} I_{Z,Z} & 0 \end{bmatrix}.$$

For any subset $\mathcal{R} \subseteq Z$, we define the value $\mathcal{K}(\mathcal{R}) \in \mathbb{R}$ with respect to $\mathcal{R}$ by

$$\mathcal{K}(\mathcal{R}) := \begin{cases} 0 & \text{If } \mathcal{R} = \varnothing \\ \|A_{\mathcal{R},:}(A_{\setminus T,:}^\top A_{\setminus T,:})^{-1} A_{\setminus T,:}^\top\|_1 & \text{Otherwise} \end{cases} \tag{3.19}$$

where $\|\cdot\|_1$ is the ℓ_1-norm of a matrix. Before we introduce our main result Theorem 3, we first provide the following lemma, which is used to prove Theorem 3.

Lemma 3 *Let $S \geq 1$ be such that $c \in \mathbb{R}^m$ is a real vector supported on $T \subset J$ obeying $|T| \leq S$. Given a matrix $A \in \mathbb{R}^{m\times n}$, where the sub-matrix $A_{\setminus T,:}$ of A has full rank, suppose F is such that $FA = 0$. Let $f \in \mathbb{R}^n$ be a non-negative real vector supported on $\setminus Z$ with exactly K zero entries. Let $y = Af + c$. If there is a subset $\mathcal{R} \subset T$ of size κ such that $\kappa \leq K$, $\mathcal{K}(\mathcal{R}) < 1$ and*

$$0 < \frac{\theta_{S-\kappa}(F)}{1 - \delta_{S-\kappa}(F) - \theta_{S-\kappa,2S-2\kappa}(F)} < \frac{1 - \mathcal{K}(\mathcal{R})}{1 + \mathcal{K}(\mathcal{R})}, \tag{3.20}$$

where $\mathcal{K}(\mathcal{R})$ is defined as (3.19), then there exists a real vector β, a non-negative real vector $\alpha \in \mathbb{R}^n$ and a left inverse H of A (i.e., $HA = I$) such that $\alpha \geq 0$, $\alpha_{\setminus Z} = 0$ and

$$\begin{aligned} H_j^\top \alpha + F_j^\top \beta &= -\,\boldsymbol{sgn}(c_j) && \text{if } j \in T, \\ \left|H_j^\top \alpha + F_j^\top \beta\right| &< 1 && \text{if } j \notin T. \end{aligned} \tag{3.21}$$

Proof: Let K be the size of the set Z, M be the size of the set T. Without loss of generality, we rearrange the columns and rows of A, the entries of c and f such that

$$\begin{aligned} \mathcal{R} &= \{1, 2, \cdots, \kappa\}, \\ Z &= \{1, 2, \cdots, K\}, \\ T &= \{1, 2, \cdots, M\}. \end{aligned}$$

The rearrangement keeps the columns of A corresponding to f and the rows of A corresponding to c. Let $\mathcal{C} := \{1, \cdots, \kappa\}$ and thus $\mathcal{C} = \mathcal{R}$. We define c' by

$$c_i' = \begin{cases} 0 & i \in \mathcal{R} \\ c_i & \text{Otherwise} \end{cases}$$

Let $T\setminus\mathcal{R}$ denote the set $\{i : i \in T, i \notin \mathcal{R}\}$. Then c' is supported on $T\setminus\mathcal{R}$ and the size of the support of c' is at most $S - \kappa$. Using (3.20), we can show that $\frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F)-\theta_{S-\kappa,2S-2\kappa}(F)} < 1$ and hence $\theta_{S-\kappa}(F) + \delta_{S-\kappa}(F) + \theta_{S-\kappa,2S-2\kappa}(F) < 1$. Then it follows that

$$\begin{aligned} \delta_{S-\kappa}(F) + \theta_{S-\kappa,2S-2\kappa}(F) &< \theta_{S-\kappa}(F) + \delta_{S-\kappa}(F) + \theta_{S-\kappa,2S-2\kappa}(F) \\ &< 1. \end{aligned}$$

By Lemma 2, there exits a vector β such that the following two conditions hold:

$$F_{T\backslash\mathcal{R}}^{\top}\beta = -\mathbf{sgn}(c'_{T\backslash\mathcal{R}}), \tag{3.22a}$$

$$|\beta^{\top}F_j| < \frac{\theta_{S-K}(F)}{1-\delta_{S-K}(F)-\theta_{S-K,2S-2K}(F)}, \forall j \notin T\backslash\mathcal{R}. \tag{3.22b}$$

Then we define $\alpha \in \mathbb{R}^n$ by specifying each entry of α to be

$$\alpha_i = \begin{cases} \frac{1}{\epsilon}|\mathbf{sgn}(c_i) + \beta^{\top}F_i| & i \in \mathcal{C}, \\ 0 & \text{Otherwise}, \end{cases} \tag{3.23}$$

for some sufficiently large $\epsilon > 0$ (we will discuss how large this ϵ should be later). Thus we have $\alpha \geq 0$ and $\alpha_{\backslash\mathcal{C}} = 0$, where $\backslash\mathcal{C} = \{i : i \notin \mathcal{C}, i \in J_1\}$. Since $\backslash Z$ is a subset of $\backslash\mathcal{C}$, we have $\alpha_{\backslash\mathcal{Z}} = 0$. Then for any $j \notin T$, we have

$$\begin{aligned}
&\left|\alpha_{\mathcal{C}}^{\top}\cdot\epsilon\cdot\mathbf{diag}(\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:}(A_{\backslash T,:}^{\top}A_{\backslash T,:})^{-1}A_{j,:}^{\top}\right| \\
\leq &\sum_{i\in\mathcal{R}}|(\mathbf{sgn}(c_i)+\beta^{\top}F_i)|\cdot\left|A_{i,:}(A_{\backslash T,:}^{\top}A_{\backslash T,:})^{-1}A_{j,:}^{\top}\right| && \text{(using (3.23) and } \mathcal{R}=\mathcal{C}) \\
\leq &\left(1+\frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F)-\theta_{S-\kappa,2S-2\kappa}(F)}\right)\left\|A_{\mathcal{R},:}(A_{\backslash T,:}^{\top}A_{\backslash T,:})^{-1}A_{j,:}^{\top}\right\|_1 && \text{(using (3.22}b\text{))} \\
\leq &\left(1+\frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F)-\theta_{S-\kappa,2S-2\kappa}(F)}\right)\mathcal{K}(\mathcal{R}) && \text{(using (3.19))} \\
< &\left(1+\frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}\right)\mathcal{K}(\mathcal{R}) && \text{(using (3.20))}
\end{aligned}$$

Since the above inequality strictly holds independent of ϵ, there must exist a sufficiently large $\epsilon \in \mathbb{R}$ such that each entry α_i of α is sufficiently small (according to (3.23)) and

$$\begin{aligned}
&\left|\alpha_{\mathcal{C}}^{\top}\cdot\epsilon\cdot\mathbf{diag}(\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:}(A_{\backslash T,:}^{\top}A_{\backslash T,:})^{-1}A_{j,:}^{\top}\right| + \left|\alpha_{\mathcal{C}}^{\top}\begin{bmatrix} I_{\mathcal{C},\mathcal{C}} & 0 \end{bmatrix}(A_{\backslash T,:}^{\top}A_{\backslash T,:})^{-1}A_{j,:}^{\top}\right| \\
<&\left(1+\frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}\right)\mathcal{K}(\mathcal{R})
\end{aligned} \tag{3.24}$$

for any $j \in \backslash T$. We set $H_{\mathcal{C},:}$ to be

$$H_{\mathcal{C},:} = \begin{bmatrix} \epsilon\cdot\mathbf{diag}(\text{-}\mathbf{sgn}(c_{\mathcal{R}})) & 0_{\kappa\times(M-\kappa)} & B \end{bmatrix}, \tag{3.25}$$

where $0_{\kappa\times(M-\kappa)}$ denotes the κ by $(M-\kappa)$ zero matrix, $B \in \mathbb{R}^{\kappa\times(m-M)}$ is defined as

$$B = \left(\begin{bmatrix} I_{\mathcal{C},\mathcal{C}} & 0_{\kappa,n-\kappa} \end{bmatrix} + \epsilon\cdot\mathbf{diag}(\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:}\right)(A_{\backslash T,:}^{\top}A_{\backslash T,:})^{-1}A_{\backslash T,:}^{\top}. \tag{3.26}$$

Then we can show that

$$
\begin{aligned}
H_{\mathcal{C},:}A &= \begin{bmatrix} \epsilon \cdot \mathbf{diag}(-\mathbf{sgn}(c_{\mathcal{R}})) & 0 & B \end{bmatrix} \begin{bmatrix} A_{\mathcal{R},:} \\ A_{T\backslash\mathcal{R},:} \\ A_{\backslash T,:} \end{bmatrix} \\
&= \epsilon \cdot \mathbf{diag}(-\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:} + BA_{\backslash T,:} \\
&= \epsilon \cdot \mathbf{diag}(-\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:} + \left(\begin{bmatrix} I_{\mathcal{C},\mathcal{C}} & 0 \end{bmatrix} + \epsilon \cdot \mathbf{diag}(\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:} \right) (A_{\backslash T,:}^{\top} A_{\backslash T,:})^{-1} (A_{\backslash T,:}^{\top} A_{\backslash T,:}) \\
&= \epsilon \cdot \mathbf{diag}(-\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:} + \begin{bmatrix} I_{\mathcal{C},\mathcal{C}} & 0 \end{bmatrix} + \epsilon \cdot \mathbf{diag}(\mathbf{sgn}(c_{\mathcal{R}}))A_{\mathcal{R},:} \\
&= \begin{bmatrix} I_{\mathcal{C},\mathcal{C}} & 0 \end{bmatrix}.
\end{aligned}
$$

If $j \in \mathcal{R}$, then we have

$$
\begin{aligned}
\alpha^{\top} H_j + \beta^{\top} F_j &= \alpha_{\mathcal{C}}^{\top} H_{\mathcal{C},j} + \beta^{\top} F_j \\
&= -\alpha_j \cdot \epsilon \cdot \mathbf{sgn}(c_j) + \beta^{\top} F_j && \text{(using (3.25) and } \mathcal{R} = \mathcal{C}) \\
&= -|\mathbf{sgn}(c_j) + \beta^{\top} F_j| \mathbf{sgn}(c_j) + \beta^{\top} F_j && \text{(using (3.23))} \\
&= \begin{cases} -(1 + \beta^{\top} F_j) + \beta^{\top} F_j & \text{if } \mathbf{sgn}(c_j) = 1 \\ \\ (1 - \beta^{\top} F_j) + \beta^{\top} F_j & \text{if } \mathbf{sgn}(c_j) = -1 \end{cases} && \text{(using (3.22}b\text{))} \\
&= \begin{cases} -1 & \text{if } \mathbf{sgn}(c_j) = 1 \\ \\ 1 & \text{if } \mathbf{sgn}(c_j) = -1 \end{cases} \\
&= -\mathbf{sgn}(c_j) && .
\end{aligned}
$$

If $j \in T\backslash\mathcal{R}$, then we have

$$
\begin{aligned}
\alpha^{\top} H_j + \beta^{\top} F_j &= \alpha_{\mathcal{C}}^{\top} H_{\mathcal{C},j} + \beta^{\top} F_j && \text{(using (3.23))} \\
&= \beta^{\top} F_j && \text{(using (3.26))} \\
&= -\mathbf{sgn}(c'_j) && \text{(using (3.22}a\text{))} \\
&= -\mathbf{sgn}(c_j).
\end{aligned}
$$

If $j \notin T$, then we have

$$
\begin{aligned}
&|\alpha^\top H_j + \beta^\top F_j| \\
\leq &|\alpha_{\mathcal{C}}^\top H_{\mathcal{C},j}| + |\beta^\top F_j| \\
= &|\alpha_{\mathcal{C}}^\top B_{j-M}| + |\beta^\top F_j| && \text{(using (3.25))} \\
\leq &\left|\alpha_{\mathcal{C}}^\top \cdot \epsilon \cdot \mathbf{diag}(\mathbf{sgn}(c_{\mathcal{R}})) A_{\mathcal{R},:} (A_{\setminus T,:}^\top A_{\setminus T,:})^{-1} A_{j,:}^\top\right| + \\
&\left|\alpha_{\mathcal{C}}^\top \begin{bmatrix} I_{\mathcal{C},\mathcal{C}} & 0 \end{bmatrix} (A_{\setminus T,:}^\top A_{\setminus T,:})^{-1} A_{j,:}^\top\right| + |\beta^\top F_j| && \text{(using (3.26))} \\
< &\left(1 + \frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}\right)\mathcal{K}(\mathcal{R}) + \frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F) - \theta_{S-\kappa,2S-2\kappa}(F)} && \text{(using (3.22b), (3.24))} \\
< &\mathcal{K}(\mathcal{R}) + \frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}(1+\mathcal{K}(\mathcal{R})) \\
= &1.
\end{aligned}
$$

Summing up all the three cases ($j \in \mathcal{R}$, $j \in T \setminus \mathcal{R}$, $j \notin T$) above, we have

$$
\begin{aligned}
\alpha^\top H_j + \beta^\top F_j &= -\mathbf{sgn}(c_j), && j \in T, \\
|\alpha^\top H_j + \beta^\top F_j| &< 1, && j \notin T.
\end{aligned}
$$

□

Now we present our main result Theorem 3, which shows under what conditions Problem (3.18) gives an exact reconstruction.

Theorem 3 *Let $S \geq 1$ be such that $c \in \mathbb{R}^m$ is a real vector supported on $T \subset J$ obeying $|T| \leq S$. Given a matrix $A \in \mathbb{R}^{m\times n}$, where the sub-matrix $A_{\setminus T,:}$ of A has full rank, suppose F is such that $FA = 0$. Let $f \in \mathbb{R}^n$ be a non-negative real vector supported on $\setminus Z$ with exactly K zero entries. Let $y = Af + c$. Assume $\delta_S(F) < 1$. If there is a subset $\mathcal{R} \subset T$ of size κ such that $\kappa \leq K$, $\mathcal{K}(\mathcal{R}) < 1$ and*

$$
0 < \frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F) - \theta_{S-\kappa,2S-2\kappa}(F)} < \frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}, \tag{3.28}
$$

where $\mathcal{K}(\mathcal{R})$ is defined as (3.19), then there exists a left inverse of A (i.e., $HA = I$) such that c is the unique minimizer to the optimization problem

$$
\begin{aligned}
&\textit{min} && \|d\|_1 \\
&\textit{subject to} && Fd = b_1 \\
& && Hd \leq b_2
\end{aligned} \tag{3.29}
$$

where $b_1 := Fy, b_2 := Hy$.

Proof: According to Lemma 3, we can find a real vector β, a real non-negative vector $\alpha \in \mathbb{R}^n$ and a left inverse H of A (i.e., $HA = I$) such that $\alpha \geq 0$, $\alpha_{\setminus Z} = 0$, and

$$\alpha^\top H_j + \beta^\top F_j = -\mathbf{sgn}(c_j), \qquad \forall j \in T, \tag{3.30a}$$
$$|\alpha^\top H_j + \beta^\top F_j| < 1, \qquad \forall j \notin T. \tag{3.30b}$$

By the definition of b_1, b_2, we have $b_2 = Hy = H(Af+c) = f+Hc \geq Hc$, $Fc = F(y-Af) = Fy = b_1$ and hence c is feasible to Problem (3.29). The definition of Z implies that $(b_2)_i = (Hc)_i$ if and only if $i \in Z$. If $\hat{d}$ is a minimizer of Problem (3.29), then $\hat{d}$ is feasible to Problem (3.29) and $\|\hat{d}\|_1 \leq \|c\|_1$. Hence we have $F\hat{d} = b_1 = Fc$ and $H\hat{d} \leq b_2$. By the property of α that $\alpha_{\setminus Z} = 0$, we have $\alpha_i = 0$ if $(Hc - b_2)_i \neq 0$. As a result $\alpha^\top(Hc - b_2) = 0$. By the non-negativity of α, we can imply that $\alpha^\top H\hat{d} \leq \alpha^\top b_2$. Using the information above, we can compute that

$$\begin{aligned}
\|\hat{d}\|_1 &= \sum_{j\in T} |c_j + \hat{d}_j - c_j| + \sum_{j\notin T} |\hat{d}_j| \\
&\geq \sum_{j\in T} \mathbf{sgn}(c_j)(c_j + \hat{d}_j - c_j) + \sum_{j\notin T} \hat{d}_j(-\alpha^\top H_j - \beta^\top F_j) && \text{(using (3.30}b\text{))} \\
&= \sum_{j\in T} \mathbf{sgn}(c_j)c_j + \sum_{j\in T} \mathbf{sgn}(c_j)(\hat{d}_j - c_j) - \sum_{j\notin T} \hat{d}_j(\alpha^\top H_j + \beta^\top F_j) \\
&= \sum_{j\in T} |c_j| + \sum_{j\in T} (-\alpha^\top H_j - \beta^\top F_j)(\hat{d}_j - c_j) - \sum_{j\notin T} \hat{d}_j(\alpha^\top H_j + \beta^\top F_j) && \text{(using (3.30}a\text{))} \\
&= \sum_{j\in T} |c_j| + \alpha^\top\Big(\sum_{j\in T} c_j H_j - \sum_{j\in J_1\cup J_2} \hat{d}_j H_j\Big) + \beta^\top\Big(\sum_{j\in T} c_j F_j - \sum_{j\in J_1\cup J_2} \hat{d}_j F_j\Big) && \text{(using (3.14), (3.16))} \\
&= \sum_{j\in T} |c_j| + \alpha^\top\Big(\sum_{j\in J_1\cup J_2} c_j H_j - \sum_{j\in J_1\cup J_2} \hat{d}_j H_j\Big) + \\
&\quad \beta^\top\Big(\sum_{j\in J_1\cup J_2} c_j F_j - \sum_{j\in J_1\cup J_2} \hat{d}_j F_j\Big) && \text{(using } c \text{ supported on } T\text{)} \\
&= \sum_{j\in T} |c_j| + \alpha^\top(Hc - H\hat{d}) + \beta^\top(Fc - F\hat{d}) && \text{(using (3.7))} \\
&\geq \sum_{j\in T} |c_j| + \alpha^\top(Hc - b_2) && \text{(using } \alpha^\top H\hat{d} \leq \alpha^\top b_2, Fc = F\hat{d}\text{)} \\
&= \|c\|_1 && \text{(using } \alpha^\top(Hc - b_2) = 0\text{).}
\end{aligned}$$

Thus $\|\hat{d}\|_1 = \|c\|_1$, and therefore the all the inequalities in the above computation must be equality. Since $|\alpha^\top H_j + \beta^\top F_j| < 1$ strictly holds whenever $j \notin T$, if we want the inequality $\sum_{j\notin T} |\hat{d}_j| \geq \sum_{j\notin T} \hat{d}_j(-\alpha^\top H_j - \beta^\top F_j)$ to appear as an equality, we must have $\hat{d}_j = 0$ whenever $j \notin T$. In other words, $\hat{d}_j = c_j = 0$ if $j \notin T$. Then it follows that

$$\begin{aligned}
& F_T\hat{d}_T = F\hat{d} = b_1 = F_T c_T \\
\Longrightarrow\quad & F_T(\hat{d}_T - c_T) = 0.
\end{aligned}$$

Noting that we have the hypothesis $\delta_S(F) < 1$, if $\hat{d}_T - c_T \neq 0$, then we can imply that $\|\hat{d}_T - c_T\| > 0$ and moreover $0 = \|F_T(\hat{d}_T - c_T)\| \geq (1 - \delta_S(F))\|\hat{d}_T - c_T\| > 0$, contradiction. Therefore we must have $\hat{d}_T = c_T$. Finally, $\hat{d}$ can be concluded to be identical to c. □

When $\mathcal{R} = \varnothing$, we have $\kappa = 0, \mathcal{K}(\mathcal{R}) = 0$ and thus the condition $\frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F)-\theta_{S-\kappa,2S-2\kappa}(F)} < \frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}$ becomes $\frac{\theta_S(F)}{1-\delta_S(F)-\theta_{S,2S}(F)} < \frac{1-0}{1+0} = 1$. Consequently Theorem 3 is identical to Theorem 1 in this case. When $\kappa > 0$, we have $\theta_{S-\kappa}(F) \le \theta_S(F)$, $\delta_{S-\kappa}(F) \le \delta_S(F)$ as well as $\theta_{S-\kappa,2S-2\kappa}(F) \le \theta_{S,2S}(F)$ according to Definition 2, therefore we have $\frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F)-\theta_{S-\kappa,2S-2\kappa}(F)} \le \frac{\theta_S(F)}{1-\delta_S(F)-\theta_{S,2S}(F)}$. If $\frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}$ is close to 1 but $\frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F)-\theta_{S-\kappa,2S-2\kappa}(F)}$ is much smaller than $\frac{\theta_S(F)}{1-\delta_S(F)-\theta_{S,2S}(F)}$, then the condition $\frac{\theta_{S-\kappa}(F)}{1-\delta_{S-\kappa}(F)-\theta_{S-\kappa,2S-2\kappa}(F)} < \frac{1-\mathcal{K}(\mathcal{R})}{1+\mathcal{K}(\mathcal{R})}$ (on F and S) of Theorem 3 is weaker than the condition $\delta_S(F) + \theta_S(F) + \theta_{S,2S}(F) < 1$ of Theorem 1.

Theorem 3 actually says that if we have one more constraint $Hx \le b_2$ for Problem (3.11) mentioned in Theorem 1, then a weaker condition on the sparsity of c may guarantee c to be the unique solution to Problem (3.29). The companion result of Theorem 1 and Theorem 3 is as follows.

Theorem 4 *Suppose F is such that $FA = 0$ and let $S \ge 1$ be a number obeying the hypothesis of Theorem 1 or the hypothesis of Theorem 3. Set $y = Af + e$, where e is a real vector supported on a set of size at most S. Then f is the unique minimizer to*

$$\min_{g \ge 0} \quad \|y - Ag\|_1$$

3.3 Robustness to Outliers

In this section, we analyze the advantage of the formulation of Problem (2.13) in Section 2.4 compared to least squares estimation without the constraint $Y \ge Ax$. If the given data points (x_1, y_1), (x_2, y_2), ..., (x_n, y_n), (x_{n+1}, y_{n+1}), ..., (x_m, y_m), where $x_i \in \mathbb{R}^n, y_i \in \mathbb{R}$ for all $1 \le i \le m$, are lying above and close to the hyperplane $y = \bar{\alpha}^\top x + b$ with $\bar{\alpha} \in \mathbb{R}^n$ and $b \in \mathbb{R}$, then we use the following estimator

$$(\hat{\alpha}, \hat{b}) := \underset{\alpha \in \mathbb{R}^n, b \in \mathbb{R}}{\operatorname{argmin}} \ \mathbb{1}_m^\top (Y - X\alpha - b \cdot \mathbb{1}_m) \text{ s.t. } Y \ge X\alpha + b \cdot \mathbb{1}_m, \tag{3.31}$$

where $X = \begin{bmatrix} x_1^\top \\ \vdots \\ x_m^\top \end{bmatrix} \in \mathbb{R}^{m \times n}$, $Y = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} \in \mathbb{R}^m$, and $y = \hat{\alpha}^\top x + \hat{b}$ to estimate the hyperplane $y = \bar{\alpha}^\top x + b$. Given sufficient number of observations of the points lying around the hyperplane, the least squares estimation is very sensitive to the points far from the hyperplane, namely outliers. By imposing the constraint that each point is located above the estimated hyperplane, our estimation is less sensitive to the outliers.

The theorem that we present in this section relies on the definition of convex hull. We first provide the the definition of convex hull as follows.

Definition 3 *Let $v_1, \ldots, v_k \in \mathbb{R}^n$, the convex hull of $\{v_1, \ldots, v_k\}$ denoted* $\boldsymbol{conv}(v_1, \ldots, v_k)$ *is the set defined as*

$$\boldsymbol{conv}(v_1, \ldots, v_k) = \{\sum_{i=1}^{k} \lambda_i v_i : \sum_{i=1}^{k} \lambda_i = 1, \lambda_1, \ldots, \lambda_k \geq 0\},$$

Then we provide the theorem which shows that the estimator (3.31) is less sensitive to the outliers and the estimator provides an exact reconstruction of the hyperplane under some conditions.

Theorem 5 *Given m data points $(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)$ where $x_i \in \mathbb{R}^n$, $y_i \in \mathbb{R}$, $i = 1, \ldots, m$, and $m > n$, suppose there exists a subset $T = \{l_1, l_2, \ldots, l_{n+1}\}$ of $J = \{1, 2, \ldots, m\}$ such that*

$$\begin{aligned} y_i &= \bar{\alpha}^\top x_i + b, \qquad i \in T, \\ y_i &> \bar{\alpha}^\top x_i + b, \qquad i \notin T, \end{aligned}$$

in addition, assume $(x_{l_1}, 1), (x_{l_2}, 1), \ldots, (x_{l_n}, 1), (x_{l_{n+1}}, 1)$ are linearly independent, and

$$\{x_i : i \notin T\} \subseteq \boldsymbol{conv}(x_{l_1}, x_{l_2}, \ldots, x_{l_{n+1}}),$$

then it follows that

$$\bar{\alpha} = \hat{\alpha} := \underset{\alpha}{argmin}\ \mathbb{1}_m^\top (Y - X\alpha - b \cdot \mathbb{1}_m) \ \ s.t.\ \ Y \geq X\alpha + b \cdot \mathbb{1}_m,$$

where $Y = [y_1\ y_2\ \ldots\ y_m]^\top \in \mathbb{R}^m$, $X = [x_1\ x_2\ \ldots\ x_m]^\top \in \mathbb{R}^{m \times n}$ and $\mathbb{1}_m$ is an m by 1 vector with each entry to be 1.

Proof: Without loss of generality, suppose $l_i = i$, $i = 1, \ldots, n+1$. We first define two sets

$$\begin{aligned} S_1 &= \{j : \hat{\alpha}^\top x_j + b > y_j, 1 \leq j \leq n+1, j \in \mathbb{Z}\}, \\ S_2 &= \{j : \hat{\alpha}^\top x_j + b = y_j, 1 \leq j \leq n+1, j \in \mathbb{Z}\}, \end{aligned}$$

When $1 \leq i \leq n+1$, it follows that

$$\begin{aligned} \bar{\alpha}^\top x_i + b &= y_i, \\ \hat{\alpha}^\top x_i + b &\leq y_i, \end{aligned}$$

and hence

$$\bar{\alpha}^\top x_i \geq \hat{\alpha}^\top x_i.$$

When $n+2 \leq i \leq m$, x_i can be written as

$$x_i = \sum_{k=1}^{n+1} t_k^{(i)} x_k,$$

where $t_1^{(i)}, t_2^{(i)}, \ldots, t_{n+1}^{(i)} \geq 0$ and $\sum_{k=1}^{n+1} t_k^{(i)} = 1$. Thus it follows that

$$\begin{aligned}
\bar{\alpha}^\top x_i &= \bar{\alpha}^\top \sum_{k=1}^{n+1} t_k^{(i)} x_k = \sum_{k=1}^{n+1} t_k^{(i)} \bar{\alpha}^\top x_k = \sum_{k=1}^{n+1} t_k^{(i)} (y_k - b), \\
\hat{\alpha}^\top x_i &= \hat{\alpha}^\top \sum_{k=1}^{n+1} t_k^{(i)} x_k = \sum_{k=1}^{n+1} t_k^{(i)} \hat{\alpha}^\top x_k \leq \sum_{k \in S_1} t_k^{(i)} (y_k - b) + \sum_{k \in S_2} t_k^{(i)} (y_k - b) = \sum_{k=1}^{n+1} t_k^{(i)} (y_k - b),
\end{aligned}$$

and hence

$$\bar{\alpha}^\top x_i \geq \hat{\alpha}^\top x_i.$$

Hence, we have

$$\bar{\alpha}^\top x_i \geq \hat{\alpha}^\top x_i, \forall 1 \leq i \leq m.$$

If $S_1 \neq \varnothing$, then the following strict inequality,

$$\bar{\alpha}^\top x_i > \hat{\alpha}^\top x_i, \forall i \in S_1,$$

suggests that $\hat{\alpha}$ cannot be the minimizer, contradiction. Thus $S_1 = \varnothing$. Since $(x_1, 1)$, $(x_2, 1)$, $\ldots$, $(x_{n+1}, 1)$ are linear independent, the solution (of (α, b)) to the linear system

$$\alpha^\top x_i + b = y_i, \forall 1 \leq i \leq n+1$$

is unique. Hence $\bar{\alpha} = \hat{\alpha}$ □

We note that, $\{x_i : i \notin T\} \subseteq \mathbf{conv}(x_{l_1}, x_{l_2}, \ldots, x_{l_{n+1}})$ is a very strong condition. It implies that $x_{l_1}, x_{l_2}, \ldots, x_{l_{n+1}}$ can represent any other data point and they form a good representative of the entire data set. Theorem 5 says, if a good representative of the whole data set fortunately locates at the underlying hyperplane $\bar{\alpha}^\top x + b = y$, then the estimation of the underlying hyperplane by the above minimization objective can be immune to any number of outliers.

The theft detection framework introduced in Chaper 2 estimates the resistance of each link by solving Problem (2.13) in Section 2.4. Theorem 5 is related to Problem (2.13). The resistance of each link decides the underlying hyperplane. The measurements obtained when no theft occurs corresponds to the data points that is close to the underlying hyperplanes while the measurements obtained when a large amount of theft occurs corresponds to the outliers. Theorem 5 provides a condition under which Problem (2.13) gives an exact recovery of the resistance of each link. Theorem 5 also shows the advantage of the optimization formulation (2.13) over the previous method. The previous method proposed in [20] estimates the resistance of each link by by the least squares estimation, which is very sensitive to outliers. Even though we have a sufficient number of the measurements that are obtained when the power theft is tiny, the least squares estimation may still give an incorrect estimation far from the real values if several measurements are obtained when the power theft is large. Theorem 5 shows that the minimizer to Problem (2.13) is immune to the measurements that are obtained when large power theft occurs provided that there is a sufficient number of the measurements that are collected when the power theft is tiny. The proof of Theorem 5 is as follows.

3.4 Hyperplane Separation By ℓ_1 Minimization

Before we introduce the problem, we first provide a definition as follows:

Definition 4 *Given $\alpha, \beta \in \mathbb{R}^n$, $b_1, b_2 \in \mathbb{R}$, two hyperplanes $y = \alpha^\top x + b_1$ and $y = \beta^\top x + b_2$ are said to be **separated** in non-negative space if the set $\{x > 0 : \alpha^\top x + b_1 = \beta^\top x + b_2\}$ is an empty set.*

In this section, we consider the following problem. If we have a sequence of non-negative data points lying in several unknown hyperplanes separated in non-negative space, how can we find the underlying hyperplanes? To answer the question above, we propose Algorithm 1 to partition the input data points into several hyperplanes. In Algorithm 1, the function **size**(A) returns the dimension of the matrix A, **zeros**$(n, 1)$ produces an n-dimensional zero vector, **countNonZeros**(b) returns the number of non-zero entries in b.

Given a sequence of m non-negative data points $(x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m)$, where $x_1, x_2, \cdots, x_m \in \mathbb{R}^n$, $y_1, y_2, \cdots, y_m \in \mathbb{R}$, we construct $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$ as follows:

$$A = \begin{bmatrix} x_1^\top \\ x_2^\top \\ \vdots \\ x_m^\top \end{bmatrix}, b = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}.$$

Then we pass A and b to Algorithm 1. Among the hyperplanes higher than all remaining data points, Algorithm 1 recursively looks for the hyperplane closest to all remaining data points by minimizing the total distance of all the data points from the target hyperplane while the inequality constraint that any point is not higher than the target hyperplane is imposed to the minimization. After such a target hyperplane is found, the points close this hyperplane are removed. Then Algorithm 1 proceeds to the next iteration to find the next target hyperplane. The iterations halt when the rank of the remaining matrix is less than the number of columns n. Since estimating the rank of a matrix is computationally expensive, we use the number of remaining entries in b as an indicator to tell the whether the remaining matrix is full rank. If the number of remaining entries in b is less than n, then the corresponding remaining rows in A are less than n and hence A becomes rank deficient .

Algorithm 1 is used to solve the theft detection problems in different scenarios as described in Section 2.2, 2.3, 2.4, 2.5. Since the formulation of these problems are the same, we only use the estimation of tampering ratio as a case study to explain how Algorithm 1 is related and helpful to our theft detection problems. Recall that if the tampering ratio of each user is a constant, then we solve Problem (2.8) to estimate the tampering ratio of each user. However, if the tampering ratio of each user is time-varying, then formulation (2.8) is not applicable. Instead, we pass the (X, b) defined in formulation (2.8) (as (A, b)) to Algorithm 1 and estimate the time-varying tampering ratios.

Here we provide an example where the formulation (2.8) is not applicable to the time-varying tampering ratios. For simplicity, the topology we use in this example is the single-layer tree as described in Figure 2.1, and the distribution transformer at the root is connected to only two users (leaves), user 1 and user 2. We suppose the distribution parameter is one. I^{in} denotes the instantaneous electric current that flows to the distribution transformer. I_1, I_2 respectively stand for the instantaneous electric currents that flow to user 1 and user 2. If we obtain the following data points (I_1, I_2, I^{in}) from measurements, (2.64, 17.36, 20), (16.41, 3.59, 20), (2.37, 14.10, 20), (13.15, 5.48, 20), (5.07, 9.95, 20), (9.62, 6.92, 20), (3.53, 8.24, 20), (9.86, 5.07, 20), then the input measurement data I^{in} and I^{out} are

$$I^{out} = \begin{bmatrix} 2.64 & 17.36 \\ 16.41 & 3.59 \\ 2.37 & 14.10 \\ 13.15 & 5.48 \\ 5.07 & 9.95 \\ 9.62 & 6.92 \\ 3.53 & 8.24 \\ 9.86 & 5.07 \end{bmatrix}, I^{in} = \begin{bmatrix} 20 \\ 20 \\ 20 \\ 20 \\ 20 \\ 20 \\ 20 \\ 20 \end{bmatrix},$$

Suppose the measurement of I_1 is always accurate but the measurement of I_2 is lower than the real values. Then the real tampering ratios of these users are summarized as follows

$$\beta = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1.25 & 1.25 & 1.5 & 1.5 & 1.9984 & 1.9984 \end{bmatrix},$$

where each column of β corresponds to the tampering ratios of two users at each time, the first row and the second row correspond to the tampering ratios of user 1 and user 2 respectively at different times.

Given $A = I^{in}, b = I^{out}$ as input, the optimal solution of Problem (2.8) is

$$\hat{\beta} = \begin{bmatrix} 1 & 1 \end{bmatrix}^\top,$$

which fails to recover the original current due to the time-varying β in this case. Given $A = I^{in}, b = I^{out}, \epsilon = 0.01$ as input, the output of Algorithm 1 is

$$\hat{\beta} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1.25 & 1.5 & 1.9984 \end{bmatrix},$$

which shows Algorithm 1 is able to recognize the change of β at different times in this case. This is a heuristic algorithm which does not guarantee the success of recognition all the time. The effectiveness of Algorithm 1 can be found from more numerical results shown in Section 5.2.2, 5.2.3.

$[w, S]$:= **planeSepr**(A, b, ϵ):
input : A matrix $A \in \mathbb{R}^{m \times n}$, a vector $b \in \mathbb{R}^m$ and a threshold $\epsilon \in \mathbb{R}$
output: A weight vector $w \in \mathbb{R}^n$ and a set S of n-dimensional vectors

$[m, n]$:=**size**(A);
w := **zeros**$(n, 1)$;
$S := \varnothing$;
while countNonZeros$(b) \geq$ n **do**
    $\hat{\beta} := \underset{\beta: A\beta \leq b, \beta \geq 0}{\operatorname{argmin}} \|A\beta - b\|_1$;
    $S := S \cup \{\hat{\beta}\}$;
    for $i \in \{i : |A(i,:)\beta - b_i| < \epsilon\}$ **do**
        $A(i,:) := 0$;
        $b_i := 0$;
        $w_i := w_i + 1$;
    end
end
return $[w, S]$;

Algorithm 1: Hyperplane Separation Algorithm

Chapter 4

Clustering and Anomaly Detection

In Chapter 2, we analyze the electricity theft in the form of tampering with the smart meter. In this chapter, we tackle the theft in another form, tapping into a power line from a point ahead of the energy meter (as indicated in Figure 4.1). Figure 4.1 shows an example of how an unknown transmission link is introduced. In this case, the energy consumption data recorded by the smart meter of User 2 (as depicted in Figure 4.1) is much less than his real consumption and thus highly likely to demonstrate some abnormal patterns compared to the normal users. We do not have a formal definition for "normal pattern" and "abnormal pattern". However, their difference can be easily judged by the human eyes. The subplots on the first three rows of Figure 4.2 show the patterns of normal users while Figure 4.3 shows the synthetically generated patterns of abnormal users. This visualization shows that a normal user's plot is smooth and natural while the thief's plot is sharp.

The introduction of an unknown link breaks the conservation of energy and the conservation of the flows of electric currents. Hence the prior knowledge of the physical laws in electricity and the knowledge of the connection topology are not applicable. We assume that the usage data of a thief who illegally draws the energy by a direct hooking from a line indicates an anomaly pattern compared to the normal users (who are not stealing energy). Let n denote the number of users. All users' data are collected in the same period. For user i $(1 \leq i \leq n)$, we have the vector $x_i \in \mathbb{R}^m$ that records the time-series usage data of this user in m equal-sized contiguous time intervals. Then we run the clustering algorithms on these n vectors to partition them. A desired algorithm is expected to put the vectors corresponding to the thieves into one group and the other vectors into the other group. (Note: the unknown users are not considered in the scope of this thesis. Clustering is applied to potentially detect whether a known user introduce an unknown link to steal energy.)

Clustering is a fundamental and useful tool in data mining that groups data according to their similarities. However, the clustering problem is not well defined. Under different assumptions and criteria, different clustering algorithms may produce dramatically differ-

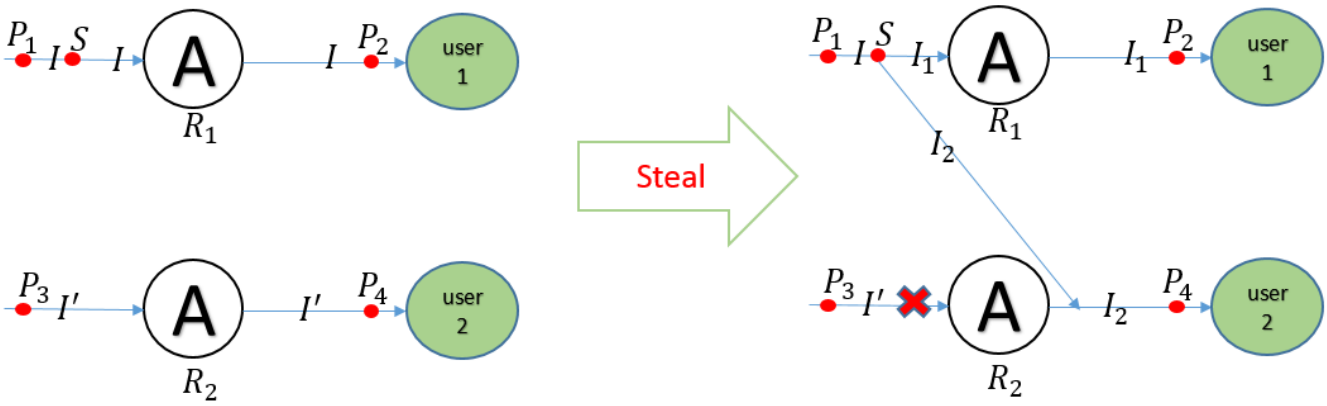


Figure 4.1: *The circle* ***A*** *represents a smart meter. User 2 directly draw the energy from the point S, which is ahead of the smart meter of user 1. User 2 could also draw the energy from the point P_3, which is ahead his own smart meter. Thus the power does not flow through the smart meter located at the entry of user 2, which is supposed to record the energy consumption of user 2.*

ent results. In Section 4.1 and 4.2, we first introduce the K-means algorithm [10] and spectral clustering [28], which are two popular and effective clustering techniques in data mining. Then in Section 4.3 and 4.4 we propose a clustering method that bi-partitions the data according to their difference along their maximum variance direction and a hierarchical clustering method which bi-partitions the data recursively until the variance inside a group is sufficiently low.

4.1 K-Means

The goal of K-Means is to partition the data points into K groups such that the sum of dissimilarities inside each group is minimized [10]. Each input sample is indexed by an integer $i \in \{1, 2, \ldots, N\}$. We assign each sample to a group and we denote the assignment of the ith sample (the sample labeled by i) by $C(i)$. Corresponding to K groups, the value of $C(i)$ is in the range of $\{1, 2, \ldots, K\}$. Given the input samples (feature vectors) $x_1, x_2, \ldots, x_n \in \mathbb{R}^m$, the objective of K-means is to minimize the following objective function

$$f(C) := \sum_{k=1}^{K} \sum_{C(i)=k} \sum_{C(j)=k} d(x_i, x_j),$$

where $d(x_i, x_j)$ denotes the dissimilarity between x_i and x_j. A standard dissimilarity measure is squared Euclidean distance [10]:

$$d(x_i, x_j) = (x_i - x_j)^\top (x_i - x_j) = \|x_i - x_j\|_2^2.$$

We want to to solve the following optimization problem

$$\underset{C}{\text{minimize}}\ f(C) := \sum_{k=1}^{K} \sum_{C(i)=k} \sum_{C(j)=k} \|x_i - x_j\|_2^2, \tag{4.1}$$

which is known to be NP-hard. Let $\bar{x}_k$ be the mean vector, which can be obtained from dividing the sum of all vectors in this cluster by the number of vectors in this cluster, associated with the kth cluster. Let N_k be the size of the kth cluster. Then we can extract the mean vector of each group and write the objective function $f(C)$ alternatively as

$$\begin{aligned} f(C) &= \sum_{k=1}^{K} \sum_{C(i)=k} \sum_{C(j)=k} \|x_i - x_j\|_2^2 \\ &= 2\sum_{k=1}^{K} N_k \sum_{C(i)=k} \|x_i - \bar{x}_k\|_2^2. \end{aligned}$$

And thus Problem (4.1) can be equivalently written as

$$\underset{C}{\text{minimize}} \sum_{k=1}^{K} N_k \sum_{C(i)=k} \|x_i - \bar{x}_k\|_2^2. \tag{4.2}$$

input : m vectors $x_1, x_2, \ldots, x_n \in \mathbb{R}^m$, an integer K
output: An assignment C partitions $x_1, x_2, \ldots, x_m$ into group $1, 2, \ldots, K$

Initialize C randomly;
while not convergent yet **do**
  for *i=1 to k* **do**
    $\bar{x}_k \leftarrow \frac{1}{N_k} \sum_{C(i)=k} x_i$
  end
  for *i=1 to m* **do**
    $C(i) \leftarrow \underset{1 \le k \le K}{\text{argmin}} \|x_i - \bar{x}_k\|^2$
  end
end
Return C;

Algorithm 2: K-means Algorithm

A local optimizer of Problem (4.2) can be effectively solved by an iterative descent algorithm as shown in Algorithm 2 [10]. In order to partition the data points into two groups, we just need to simply choose the parameter $K = 2$.

4.2 Spectral Clustering

In this section, we introduce another clustering method called spectral clustering which adopts a different objective from K-means to group data points.

4.2.1 Graph Laplacian

The radial basis function kernel (RBF kernel) on two input vectors x and y with respect to parameter σ is defined as [7]

$$K_{\text{RBF}}(x, y) = \exp(\frac{(x-y)^\top (x-y)}{2\sigma^2}).$$

The parameter σ is typically set to be the variance of input data points. Given the input samples $x_1, x_2, \ldots, x_n \in \mathbb{R}^m$, we define the similarity matrix $W \in \mathbb{R}^{n \times n}$ by

$$W_{ij} = K_{\text{RBF}}(x_i, x_j),$$

where W_{ij} denotes the entry located at the ith row and the jth column of W. Then we define a diagonal matrix G by

$$G_{ii} = \sum_{j=1}^{n} W_{ij},$$

where G_{ii} denotes the ith diagonal entry of G. Finally, the graph Laplacian [28] is defined by

$$L = G - W.$$

4.2.2 Ratio Cut

We represent the dissimilarity $S(A, B)$ between set A and set B by $S(A, B) = \sum_{x \in A} \sum_{y \in B} K_{\text{RBF}}(x, y)$ [28]. Then the ratio cut [28] between two sets A, B is defined as follows

$$\text{RatioCut}(A, B) = \frac{1}{2}\left[\frac{S(A, B)}{|A|} + \frac{S(A, B)}{|B|}\right],$$

where $|A|$ and $|B|$ denote the size of set A and B.

If we want to partition the input data points into two groups, A and $\bar{A}$, then our objective is to maximize $\text{RatioCut}(A, \bar{A})$. Intuitively, this objective aims at maximizing the dissimilarity between two groups, while this dissimilarity is normalized by the size of one group to prevent the dominance of either. Given the input data points $x_1, x_2, \ldots, x_n \in \mathbb{R}^m$, we define the vector $f \in \mathbb{R}^n$ with respect to the two-group partition A and $\bar{A}$ by

$$f_i = \begin{cases} \sqrt{|\bar{A}|/|A|} & \text{if } x_i \in A, \\ -\sqrt{|A|/|\bar{A}|} & \text{if } x_i \in \bar{A}, \end{cases} \tag{4.3}$$

where f_i is the ith entry of f. It can be shown that maximizing $\text{RatioCut}(A, \bar{A})$ can be relaxed to the following optimization problem

$$\begin{aligned} \underset{f \in \mathbb{R}^n}{\text{maximize}} \quad & f^\top L f, \\ \text{subject to} \quad & f^\top f = 1, \\ & e^\top f = 0. \end{aligned} \tag{4.4}$$

The optimal solution $\hat{f}$ to Problem (4.4) is the second non-principle eigenvector of L [28]. Each entry of $\hat{f}$ corresponds to one input data point. According to (4.3), the sign of $\hat{f}_i$ decides which group the ith sample is assigned to. That is, if $f_i > 0$, then the ith sample is assigned to group A and otherwise to group $\bar{A}$.

4.3 Bi-partition along the Principle Component

In the two-group spectral clustering, the second non-principle eigenvector is used as an indicator of partition. Motivated by the power of eigenvector, we propose a "one-dimension bi-partition along principle eigenvector"(1DBPE) method which also uses the principle eigenvector. Different from spectral clustering, we use the principle eigenvector of the covariance matrix of input data points, which is shown to be the direction of maximum variance in feature space.

Before we introduce our 1D bi-partition method, we assume that a sorting method $[sortArray\ rank]$:=**sort**$(array)$ is given. The routine **sort**$(array)$ takes an a list of unsorted real numbers $array$ as input. It outputs a list $sortArray$ of sorted numbers and a list $rank$ of ranks of each number from $array$. For example, if the input is $array = [4, 8, 9, 2, 5]$, and we run the routine $[sortArray\ rank]$:=**sort**$([4, 8, 9, 2, 5])$, then the output is $sortArray = [2, 4, 5, 8, 9]$ and $rank = [2, 4, 5, 1, 3]$.

We look for a direction to project the input data points such that the variance of the projections is maximized. Given n input data points $x_1, x_2, \ldots, x_n \in \mathbb{R}^m$, we include all data points into a $m \times n$ matrix

$$X = \begin{bmatrix} x_1 & x_2 & \ldots & x_n \end{bmatrix}.$$

In other words, the ith column of X is x_i, $1 \le i \le n$. Then we define the column mean $\bar{x}$ of X by

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i.$$

We also define $\bar{X} = \begin{bmatrix} \bar{x} & \bar{x} & \ldots & \bar{x} \end{bmatrix} \in \mathbb{R}^{m \times n}$. Then the n-by-n covariance matrix of X is defined as

$$V = (X - \bar{X})(X - \bar{X})^\top.$$

In order the catch the main difference between two column groups of data, we attempt to compute the direction ω of feature space along which the variance of data is maximum. The variance of data along the direction ω in the feature space is

$$\mathbf{VAR}(\omega^\top X) = \omega^\top (X - \bar{X})(X - \bar{X})^\top \omega = \omega^\top V \omega$$

Since we only care about the direction, ω can be scaled to be a unit vector and the constraint $\omega^\top \omega = 1$ is imposed. Thus we want to solve the following optimization problem

$$\begin{aligned} \max_{\omega} \quad & f(\omega) := \omega^\top V \omega \\ \text{subject to} \quad & \omega^\top \omega = 1 \end{aligned} \tag{4.5}$$

It can be shown that the solution to the optimization problem 4.5 is the eigenvector of V corresponding to its largest eigenvalue [11], which is also named the principle eigenvector of V. The projection of the columns of the matrix X to the direction ω is $\omega\omega^\top X$, where

$[I, L]$=**oneD-Bipartition**(X):
input : A m by n matrix X, where each of the n columns corresponds to a sample and each sample has m features
output: An indicator vector I that shows which group each data point is assigned to, and a list L of the projection of the input data points to their principle eigenvector

u :=**principleEigenVector**(X);
$L := u^\top X$;
$[sortL\ rank]$:=**sort**(L);
n :=**size**$(sortL)$;
$cut := -1$;
$minSoFar := +Inf$;
for $i = 1$ *to* $n - 1$ **do**
  $sumVar(i) :=$ **VAR**$(sortL(1:i))$ + **VAR**$(sortL(i+1:n))$;
  if $(sumVar(i) < minSoFar$ **then**
    $minSoFar := sumVar(i)$;
    $cut := i$;
  end
end
$I(rank(1:cut)) = 1$;
$I(rank(cut+1:n)) = 2$;
Return $[I, L]$;

Algorithm 3: 1D Bipartition

$\omega\omega^\top$ is a projection matrix since $(\omega\omega^\top)(\omega\omega^\top) = \omega\omega^\top$. Thus the projection of the ith column x_i of X is $(\omega^\top x_i)\omega$ for all $1 \le i \le n$ and each column of X is projected to be a multiple of ω. Then we sort the numbers $\omega^\top x_1$, $\omega^\top x_2$, ..., $\omega^\top x_n$. After the numbers are sorted, we want to partition the numbers into two groups such that the sum of variance inside two groups are minimized. The algorithm of 1D bi-partition is summarized in Algorithm 3.

Our bipartition algorithm can be simply summarized in two steps:

1. Project the data points onto the direction ω along which the variance maximized;
2. Partition the projections $\omega^\top X$ of data on ω, which is a one-dimensional list, into two groups such that the sum of variance in two groups are minimized.

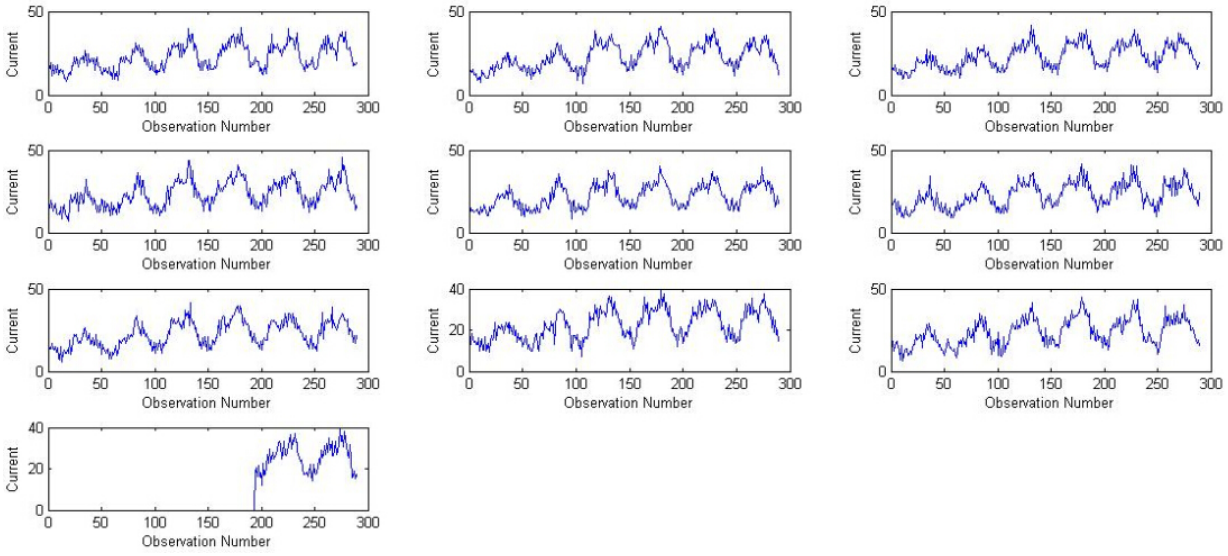


Figure 4.2: *The instantaneous current of each user is observed every half an hour. We have 289 observations for each user. The X-axis of each subplot represents the observation number from 0 to 288, the Y-axis represents the instantaneous current at each observation. In this figure, the first 9 users are normal users while the 10th one(the one in the first column and the fourth row) is the thief.*

4.4 Hierarchical Clustering —An Extension of 1D Bi-partition along Principle Component

In order to separate the normal users and the thieves, we expect to run clustering algorithms to partition the data points into two groups, one group corresponding to the normal users and the other corresponding to the thieves. Clustering algorithms group data points according to their similarities and similar data points are partitioned into the same group. Although the normal users share much similarity, there may be huge diversity among the thieves. As a result, the thieves may not be partitioned into the same group by the above clustering algorithms. Thus partitioning the data points into two groups may not be enough to separate normal users and thieves. While the clustering methods introduced previously requires the number of groups to be explicitly provided, it is not easy to determine how many groups that the data points should be partitioned into in advance. With respect to such a drawback of the above methods, we extend our bi-partition routine to a multi-group clustering method, which does not need the the number of groups as an input and figures out the number of groups automatically. In our multi-group clustering algorithm, we recursively project data to its maximum variance direction,and partition the resulted one-dimensional list into two groups by minimizing the sum of variance of two groups. The data points are then bi-partitioned the same as how their projections are partitioned. The recursion halts until the list of 1D projection has a sufficiently small variance. Since

the bi-partition recursively proceeds and the clustering results demonstrate a hierarchical structure of binary tree, we call it hierarchical clustering. The details of this algorithm are shown in Algorithm 4.

$[I,\ Z] =$ **HierachyClustering**(X, Y, σ):
input : A m by n matrix X, where each of the n columns corresponds to a sample and each sample has m features
output: An indicator vector I that shows which group each data point is assigned to

$[m\ n]$:=**size**(X);
I =: Y×**ones**$(n, 1)$;
$[\hat{I}\ L]$ =: **oneD-Bipartition**(X);
if $\sqrt{\boldsymbol{VAR}(L)} < \sigma$ **then**
  Return $[I,\ Y + 1]$;
end
$[I(\mathbf{find}(\hat{I} == 1))\ Y]$ = **HierachyClustering**$(X(:, \mathbf{find}(\hat{I} == 1)), Y, \sigma)$;
$[I(\mathbf{find}(\hat{I} == 2))\ Y]$ = **HierachyClustering**$(X(:, \mathbf{find}(\hat{I} == 2)), Y, \sigma)$;
Return $[I,\ Y]$;

Algorithm 4: Hierachy Clustering

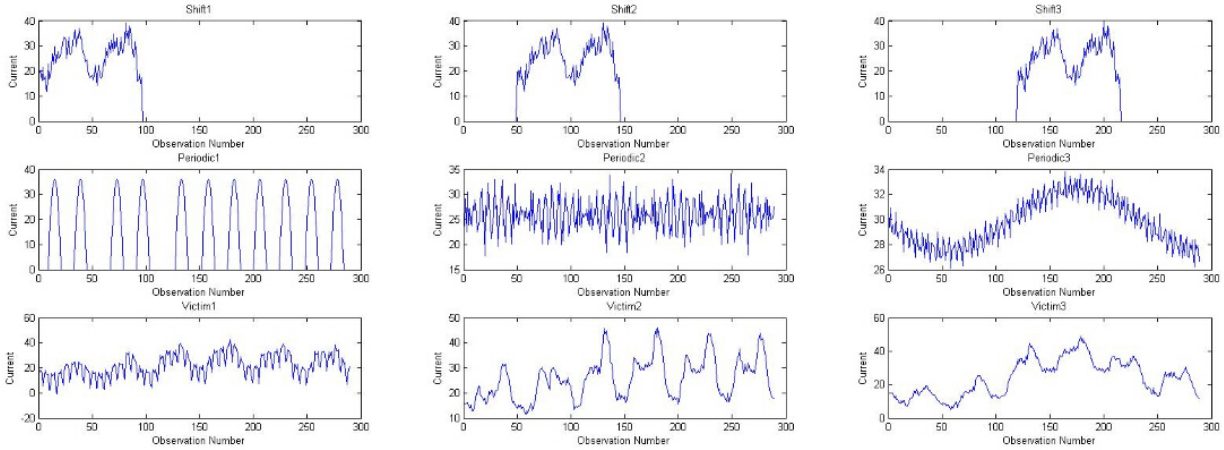


Figure 4.3: ***Shift1***, ***Shift2*** *and* ***Shift3*** *are obtained by shifting the theft pattern appearing in figure 4.2 to different phases;* ***Periodic1***, ***Periodic2*** *and* ***Periodic3*** *are designed to simulate periodic theft patterns;* ***Victim1***, ***Victim2*** *and* ***Victim3*** *are generated by adding periodic theft to normal user pattern.*

Chapter 5

Numerical Results

In this chapter, we show the numerical results of the theft detection methods introduced and proposed at Chapter 2 and 4. Section 5.1 describes the data set that we use. Section 5.2 describes the simulation of the time-invariant tampering as well as the time-varying tampering and shows the numerical results of the methods proposed in Section 2.3 and 3.4. Section 5.3 shows the numerical results of the methods introduced at Section 2.4.1 and proposed at Section 2.4.2 and 2.5.2. Section 5.4 describes the simulation of the anomaly in the time-series measurements of electric currents and shows the numerical results of the clustering methods introduced and proposed in Chapter 4.

5.1 Description of the Data

We employ the data set used in [20] for testing. We name this data set **Nikovski2013**. **Nikovski2013** contains the demand profiles of ten users, where the first nine users are honest (not stealing energy) and the tenth user is stealing energy. All these ten users are attached to the same distribution transformer. The time span of the data collection of **Nikovski2013** was 144 hours and the measurements of instantaneous electric currents and energy were made every 30 minutes. The theft only occurred in the last 24 hours, that is, no theft occurred at the first 120 hours. Figure 4.2 shows the plots of electric currents of the 10 users of **Nikovski2013**. **Nikovski2013** also provides the simulated resistance of each link from the DT (at the root) to each user (at the leaf) for evaluation [20]. The major limitation of **Nikovski2013** is the low ratio of thieves to honest users. In practice, a higher percentage of users could be stealing energy. In the following sections, scenarios with more thieves are simulated .

5.2 Estimation of Tampering Ratio

The objective of this section is to estimate the tampering ratio of each user. This section shows the numerical results of the methods in Section 2.3 and 3.4.

5.2.1 Constant Tampering Ratio

In the following tests, we use 14 users for testing, where the first nine users are all the nine honest users directly from **Nikovski2013**, and users 10~14 are additionally simulated thieves based on **Nikovski2013**. We describe how users 10~14 are simulated as follows.

We denote the time-series real electric currents that flow to all users by the matrix $I \in \mathbb{R}^{288\times 14}$, where the ith row $I(i,:)$ of I corresponds to the electric currents flowing to all users at the ith time, the jth column $I(:,j)$ of I corresponds to the real electric currents flowing to User j at different times. The first nine columns of I are directly from **Nikovski2013**. The last five columns of I are simulated as follows. The real current flowing to the 10th user is simulated to be the mean of the currents flowing to the first 9 users. For $i = 11, 12, 13, 14$, the real currents flowing to the ith user is simulated to be

$$I(:,i) = \frac{2}{10} I(:, 1:10)\gamma + f, \gamma \in \mathbb{R}^{10}, f \in \mathbb{R}^{288},$$

where the coordinates γ_j $(1 \le j \le 10)$ of γ are independently drawn from a uniform distribution $\mathbf{Unif}(0,1)$, $f \in \mathbb{R}^{288}$ is drawn from a multi-variate Gaussian distribution. The realizations of γ and f for different users are independent.

The measurements of the electric currents that flow to the first nine users are simulated to be their real electric currents plus small Gaussian noises. As for users 10~14, we use $0.2{\cdot}I(:,10)$, $0.6{\cdot}I(:,11)$, $0.4{\cdot}I(:,12)$, $0.68932{\cdot}I(:,13)$, $0.4814789{\cdot}I(:,14)$ as the measurements of $I(:,10)$, $I(:,11)$, $I(:,12)$, $I(:,13)$, $I(:,14)$ respectively.

Recall that we estimate the tampering ratios by solving Problem (2.8). In fact, the minimizer of Problem (2.8) contains the estimation of the multiplicative inverse of the tampering ratio of each user. For convenience, we define the **recovery parameter** of a user to be the multiplicative inverse of the tampering ratio of this user. That is to say, the minimizer of Problem (2.8) contains the estimation of the recovery parameter of each user. According to the simulation above, the vector $\beta \in \mathbb{R}^{14}$ that includes the real recovery parameters of all the 14 users is

$$\beta = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 5 & 1.667 & 2.5 & 1.6969 & 2.0769 \end{bmatrix}^{\mathsf{T}}.$$

Then we conduct the following 5 tests. In the first test, we only use the first 10 users, the measured input current is the sum of the real currents of the first 10 users; in the second test, we only use the first 11 users, the measured input current is the sum of the

	Tst1 Est.	Tst2 Est.	Tst3 Est.	Tst4 Est.	Tst5 Est.	Real RP.
User 1	1.0121	1.0072	1.0062	1.0000	1.0000	1.0000
User 2	1.0065	1.0059	1.0053	1.0094	1.0000	1.0000
User 3	1.0064	1.0051	1.0000	1.0085	1.0000	1.0000
User 4	1.0000	1.0000	1.0000	1.0001	1.0000	1.0000
User 5	1.004	1.0015	1.0026	1.0000	1.0000	1.0000
User 6	1.0031	1.0000	1.0082	1.0073	1.0000	1.0000
User 7	1.0000	1.0014	1.0000	1.0000	1.0000	1.0000
User 8	1.0081	1.0083	1.0000	1.0046	1.0000	1.0000
User 9	1.0000	1.0012	1.0082	1.0099	1.0031	1.0000
User 10	4.8102	4.8813	4.9282	4.8626	4.9432	5.0000
User 11	NA	1.6427	1.6191	1.6761	1.6301	1.667
User 12	NA	NA	2.4870	2.3922	2.5587	2.5
User 13	NA	NA	NA	1.7376	1.6680	1.6969
User 14	NA	NA	NA	NA	2.1121	2.0769

Table 5.1: Constant Tampering Ratio

The column "Tst1 Est." records the estimation of recovery parameter in the first test, "Tst2 Est." records the second and so forth. RP is short for the term recovery parameter and the column "Real RP." lists the real values of the recovery parameters.

real currents of the first 11 users plus a small Gaussian noise; in the third test, we only use the first 12 users, the measured input current is the sum of the real currents of the first 12 users plus a small Gaussian noise; in the fourth test, we only use the first 13 users, the measured input current is the sum of the real currents of the first 13 users plus a small Gaussian noise; in the fifth test, we use all the 14 users, the measured input current is the sum of the real currents of all the 14 users plus a small Gaussian noise.

Using the measurements of the instantaneous currents at the entry of the DT and at the entry of each user, our objective is to estimate the tampering ratio of each user. The estimation results of the recovery parameter (the multiplicative inverse of the tampering ratio) of each user in these 5 tests are displayed in Table 5.1. The column "Tst1 Est." records the estimation of the recovery parameters in the first test, "Tst2 Est." records the estimation in the second test and so forth. The column "Real Val" lists the real value of the recovery parameter of each user. As we can see from the table, the estimated values are very close to the real values. These results show that ℓ_1 minimization is immune to slight white noise of measurement and estimates the recovery parameters accurately.

In the following two subsections, keeping the real electric currents the same as in this subsection, we generate time-varying tampering ratios.

5.2.2 Discrete Time-varying Tampering Ratio

The simulation of the real electric currents flowing to the 14 users in Subsection 5.2.1 still apply in this subsection. Instead of simulating constant tampering ratios, we simulate discrete time-varying tampering ratios. We generate a sequence of m numbers, $a_i = 3sin(i), i = 1, 2, \ldots, m$, which are used to decide the change of tampering ratios. We simulate time-varying tampering ratios for the currents flowing to users 10, 12 and 14. The measured currents flowing to user 10 are simulated to be $0.2{\cdot}I(i, 10)$, $0.25{\cdot}I(i, 10)$ and $0.3{\cdot}I(i, 10)$ respectively when $|a_i| \leq 1, 1 < |a_i| \leq 2$, and $2 < |a_i| \leq 3$; the measured currents flowing to user 12 are simulated to be $0.9{\cdot}I(i, 12)$, $0.7{\cdot}I(i, 12)$, and $0.83{\cdot}I(i, 12)$ respectively when $|a_i| \leq 1, 1 < |a_i| \leq 2$, and $2 < |a_i| \leq 3$; the measured currents flowing to user 14 are simulated to be $0.64{\cdot}I(i, 14)$, $0.59{\cdot}I(i, 14)$, and $0.74{\cdot}I(i, 14)$ respectively when $|a_i| \leq 1, 1 < |a_i| \leq 2$, and $2 < |a_i| \leq 3$, where i ranges from 1 to m. The measured currents of other users are the same as in Subsection 5.2.1. The measured input current is the sum of the real currents of all the 14 users plus a small Gaussian noise.

Using the measurements of the instantaneous currents at the entry of the DT and at the entry of each user, our objective is to estimate the tampering ratio of each user. With respect to the above simulation of discrete time-varying tampering ratios, Table 5.2 shows the estimation of the recovery parameters by solving the optimization problem (2.8), while Table 5.3 lists the estimation results by the time-varying recovery method (Algorithm 1). The formulation of Problem (2.8) assumes that the tampering ratio of each user is constant and thus it only gives a single estimation of the tampering ratio for each user, which is closest to the lowest real tampering ratio (of each user) during the horizon. The time-varying recovery method catches the changes of the tampering ratios and provides a sequence of estimations, which are all very close to the real recovery parameters during the horizon.

5.2.3 Continuous Time-varying Tampering Ratio

The simulation of the real electric currents flowing to the 14 users in Subsection 5.2.1 still apply in this subsection. In this part, we simulate continuous time-varying tampering ratios. We generate a sequence of m numbers, $c_i = 0.8 \times |sin(2i + 5)|, i = 1, 2, \ldots, m$, which determines the fluctuation of tampering ratios. We simulate a continuous time-varying tampering ratio for the current flowing to user 14. The measurements of the current $I(i, 14)$ flowing to user 14 is simulated to be $c_i \cdot I(i, 14)$. As a result, the tampering ratio of user 14 is simulated to be a continuous function of time. The measured currents of other users are the same as in Subsection 5.2.1.

Using the measurements of the instantaneous currents at the entry of the DT and at the entry of each user, our objective is to estimate the tampering ratio of each user. With respect to the simulation of continuous time-varying tampering ratios, Table 5.2 lists the estimation results of the recovery parameters by solving the optimization problem

	Discrete Variance		Cont. Variance	
Users	Est. RP	Real RP.	Est. RP	Real RP
User 1	1.0644	1.0000	1.0117	1.0000
User 2	1.0000	1.0000	1.0000	1.0000
User 3	1.1025	1.0000	1.0506	1.0000
User 4	1.0229	1.0000	1.0129	1.0000
User 5	1.0448	1.0000	1.0000	1.0000
User 6	1.0000	1.0000	1.1015	1.0000
User 7	1.1952	1.0000	1.0634	1.0000
User 8	1.2198	1.0000	1.0288	1.0000
User 9	1.0000	1.0000	1.000	1.0000
User 10	1.8430	3.3333,4,5	2.7384	2.9412
User 11	1.7981	1.6667	3.5825	3.5714
User 12	1.1367	1.2048, 1.4286, 1.1111	4.0082	4.0000
User 13	1.5372	1.4507	3.0825	3.2258
User 14	1.3514	1.3514, 1.6949, 1.5625	1.0000	$0.3sin(\frac{2t+5}{24}) + 0.6, 1 \leq t \leq m.$

Table 5.2: Estimation of Recovery Parameter by Time-invariant Method
RP is short for the term ***recovery parameter****. The column "Discrete Variance" corresponds to the case when the simulated tampering ratio changes with time discretely. "Cont. Variance" corresponds to the case when the simulated tampering ratio changes with time continuously.*

User	1st Est.	2nd Est.	3rd Est.	4th Est.	5th Est.	6th Est.	7th Est.	Real RP
1	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.000
2	1.0000	1.0000	1.0006	1.0077	1.0000	1.0000	1.0000	1.000
3	1.0000	1.0000	1.0189	1.0131	1.0014	1.0000	1.0000	1.000
4	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.000
5	1.0000	1.0095	1.0034	1.0000	1.0000	1.0000	1.0000	1.000
6	1.0000	1.0000	1.0017	1.0000	1.0017	1.0000	1.000	1.0000
7	1.0000	1.0000	1.0006	1.0093	1.0004	1.0000	1.0000	1.000
8	1.0000	1.0023	1.0000	1.0000	1.0000	1.0000	1.0000	1.000
9	1.0000	1.0017	1.0013	1.0024	1.0000	1.0000	1.0000	1.000
10	3.3333	4.0106	4.0157	3.9618	4.0136	4.000	5.000	3.3333,4,5
11	1.6667	1.7053	1.7087	1.6766	1.6657	1.6667	1.6667	1.6667
12	1.2048	1.3349	1.3775	1.3811	1.4180	1.4286	1.1111	1.20,1.43,1.11
13	1.4507	1.4699	1.4589	1.4798	1.4575	1.4507	1.4507	1.4507
14	1.3514	1.6255	1.5376	1.5465	1.6665	1.6949	1.5625	1.35,1.69,1.56

Table 5.3: Estimation of Recovery Parameters by Time-varying Method
RP is short for the term ***recovery parameter****. This table provides the estimation results of recovery parameters by Algorithm 1 when the simulated tampering ratios change with time discretely.*

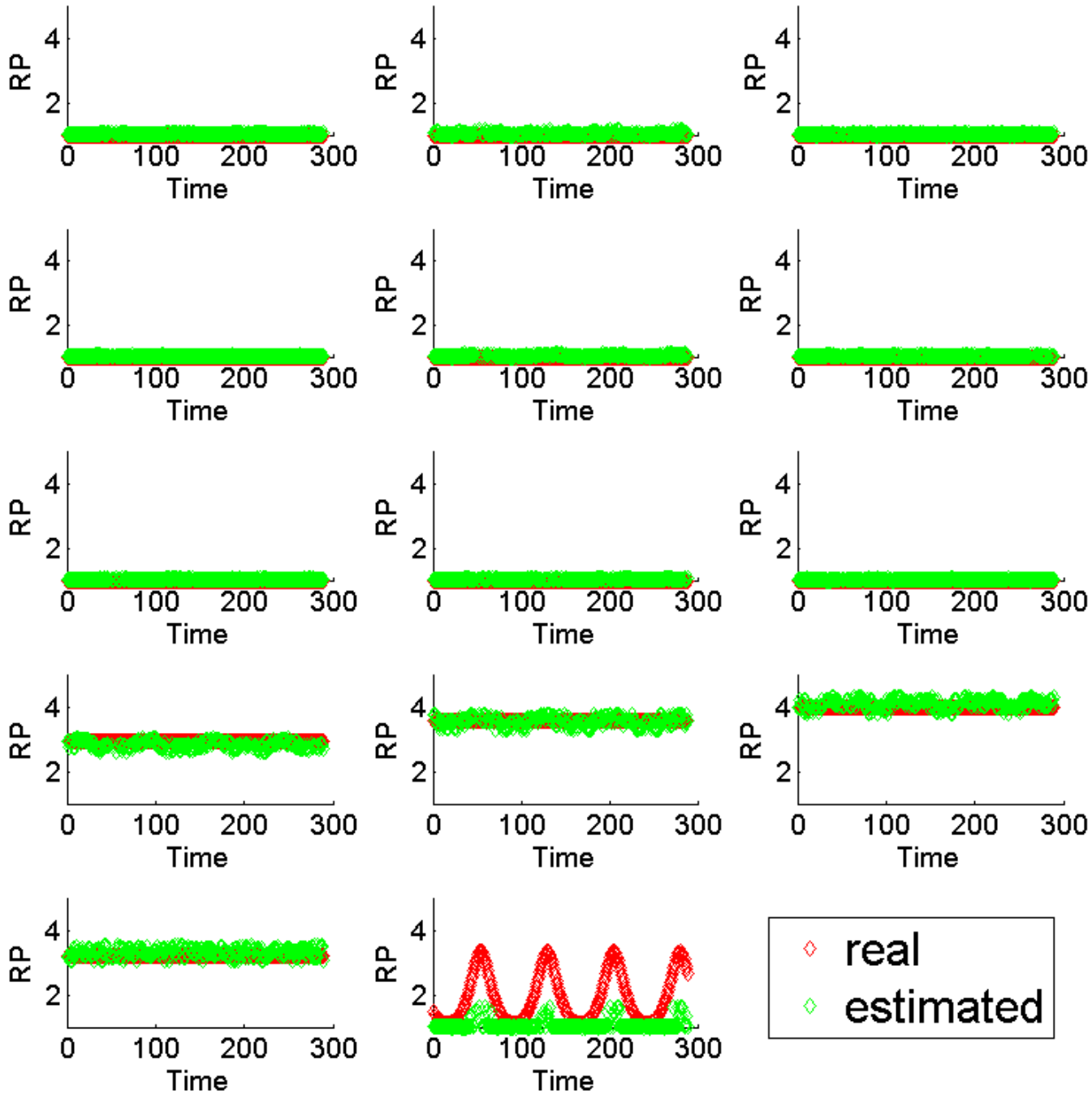


Figure 5.1: Continuous Time-varying Recovery of Electric Current

The X-axis and Y-axis of each diagram respectively represent the time and the recovery parameter(RP). The red plots shows the real value of the recovery parameter of each user. The green plots shows the estimation of recovery parameters by the dynamic recovery method.

(2.8), while Figure 5.1 shows the estimation results by the time-varying recovery method (Algorithm 1). The solution to Problem (2.8) estimates the recovery parameter of user 14 to be a constant one, which does not reflect the fact that the recovery parameter of user 14 varies continuously between 1 and 3.33. The time-varying recovery method can recognize the trend of the continuous change of the recovery parameter of user 14. An unsatisfactory indication from Figure 5.1 is that it is a bit away from an accurate estimation of all the tampering ratios during the horizon, which is probably due to the insufficient number of the measurements with respect to each single tampering ratio during the horizon and the large range of the changes of the tampering ratios. However, a continuous change of the recovery parameter in the form of a sine function $0.8 \times |sin(2x+5)|$ is unlikely in practice. The fact that, in such extreme conditions, the time-varying recovery method can still recognize the pattern of change is an acceptable performance.

5.3 Estimation of The Resistance

The objective of this section is to estimate the resistance of each link in the smart distribution network. This section shows the numerical results of the methods in Section 2.4.1, 2.4.2 and 2.5.2.

5.3.1 Estimation Based on Electric Current and Energy

In this part, we use the data of the first 9 users from the data set **Nikovski2013**. We define the **Theft Frequency** to be the ratio of the number of time intervals in which power theft occurs to the total number of time intervals (when energy is measured). We define the **Theft Ratio** to be the ratio of the mean of power theft to the ohmic losses in each time interval. Given a sequence of real values $R_1, R_2, \ldots, R_m$ of the resistance of the links and the estimation values $\hat{R}_1, \hat{R}_2, \ldots, \hat{R}_m$ of $R_1, R_2, \ldots, R_m$, we define the **Relative Estimation Error of Resistance** to be

$$\sqrt{\sum_{i=1}^{m} \frac{(\hat{R}_i - R_i)^2}{R_i^2}}.$$

Given the real amount of energy theft $\mathcal{T}_i$ and the estimation of energy theft $\hat{\mathcal{T}}_i$ at the ith time interval, we define the **Estimation Error of Theft** in the ith interval to be

$$(\hat{\mathcal{T}}_i - \mathcal{T}_i)^2$$

Given the theft frequency κ and the theft ratio q, we simulate the power theft to appear in each time interval with probability κ; if theft occurs in a time interval, we simulate the theft amount to be q times the ohmic losses in this time interval plus some Gaussian noise.

Resistance (Ω)	Estimation		Real Val
	Before Recovery	After Recovery	
R_1	0.3869	0.3869	0.3869
R_2	0.4613	0.4613	0.4613
R_3	0.4613	0.4613	0.4613
R_4	0.5152	0.5152	0.5152
R_5	0.3288	0.3288	0.3288
R_6	0.4192	0.4192	0.4192
R_7	0.3894	0.3895	0.3894
R_8	0.3369	0.3370	0.3369
R_9	0.5149	0.5134	0.5149
R_{10}	2.3386	**0.4731**	0.4677
R_{11}	0.1703	**0.1055**	0.1022
R_{12}	0.5054	**0.1991**	0.2022
R_{13}	0.2922	**0.1773**	0.1722
R_{14}	0.4605	**0.2200**	0.2217

Table 5.4: Estimation of Resistance Using Measurement of Voltage 1

Resistance (Ω)	Estimation			Real Val
	Before Recovery	Time-invariant	Time-varying	
R_1	0.3701	0.3736	0.3941	0.3869
R_2	0.4207	0.4751	0.4681	0.4613
R_3	0.4003	0.3842	**0.4135**	0.4126
R_4	0.4848	0.5168	0.5232	0.5152
R_5	0.3173	0.3237	0.3350	0.3288
R_6	0.3964	0.4314	0.4260	0.4192
R_7	0.3653	0.3337	**0.3935**	0.3894
R_8	0.3215	0.2832	**0.3435**	0.3369
R_9	0.4914	0.5289	0.5195	0.5149
R_{10}	1.0532	0.8933	**0.4742**	0.4677
R_{11}	0.2292	0.1836	0.1888	0.1837
R_{12}	0.2187	**0.2133**	0.1657	0.2041
R_{13}	0.3869	0.2666	0.2784	0.2691
R_{14}	0.2382	0.2806	**0.1863**	0.1876

Table 5.5: Estimation of Resistance Using Measurement of Voltage 2

The column of "Time-invariant" corresponds to the estimation of resistance after the recovery by solving Problem (2.8). The column of "Time-varying" corresponds to the estimation of resistance after the recovery by the time-varying recovery method

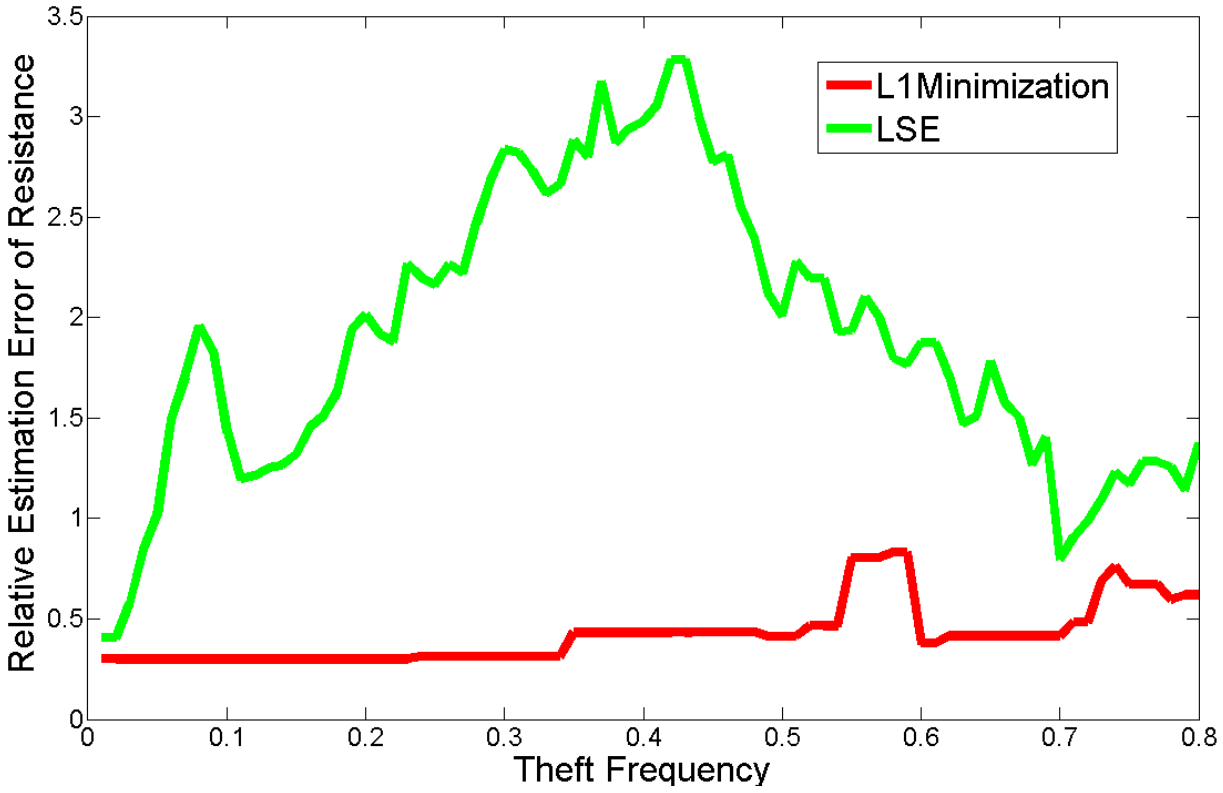


Figure 5.2: *The X-axis of this figure represents the theft frequency while the Y-axis stands for the relative estimation error of resistance. The green plot is the result of least squares estimation while the red plot is the result of ℓ_1 minimization. As we can see, the estimation error of ℓ_1 minimization is less than the estimation error of least squares estimation overall. In addition, the estimation error of ℓ_1 minimization is more robust than least squares estimation with the increase of theft frequency.*

Figure 5.2 shows the comparison between ℓ_1 minimization and least squares estimation in estimating the resistance of the links with the increase of theft frequency. The estimation errors of these two methods are very close when the theft frequency is close to zero. With the increase of theft frequency, the error of least squares method dramatically increases but the error of ℓ_1 minimization method only increases slightly. After the theft frequency crosses over 0.4, the estimation error of least squares estimation falls back while the estimation error of ℓ_1 minimization still increases slightly. The estimation error of least squares estimation is greater than ℓ_1 minimization overall.

Figure 5.3 shows that comparison between ℓ_1 minimization and least squares estimation in estimating the resistance of the links with the increase of theft ratio. The estimation errors of least squares estimation is smaller than ℓ_1 minimization when the theft ratio is lower then 0.03. After the theft ratio crosses over 0.04, the estimation error of least squares estimation becomes greater than ℓ_1 minimization. With the increase of theft ratio, the estimation error of least squares method dramatically increases but the estimation error of ℓ_1 minimization method is almost not changed. Here is the reason for the robustness of ℓ_1 minimization compared to ℓ_2 minimization: if the locations of the non-zero entries of the residual are fixed, then the optimality conditions (the KKT conditions) for the ℓ_1 minimization problem are not changed with the increase of the size of residual; for ℓ_2 minimization, the optimality conditions depend on the size of the residual and thus the solution may change significantly with the increase of the size of the residual.

When the theft ratio is 0.08 and the theft frequency is 0.4, the red plot and the green plot of Figure 5.4 respectively record the error in estimating the amount of energy theft in each time interval by ℓ_1 minimization and least squares estimation. Figure 5.4 shows that ℓ_1 minimization has better accuracy in estimating the amount of energy theft in each time interval than least squares estimation.

The above results show that the accuracy of the estimation by ℓ_1 minimization is robust while the accuracy of least squares estimation is very sensitive to the increase of theft ratio or theft frequency. The reason is, since the non-negativity constraint has already enforced the estimated resistance in a correct range, some bad samples (collected when theft occurs) cannot affect the estimation much. Least squares estimation selects a hyperplane in the middle of the data points. If there are several bad data points that are far away from and on the same side of the correct hyperplane, least squares estimation needs to compromise to these bad points and thus the estimation is seriously mislead to the wrong side.

5.3.2 Estimation based on Voltage and Electric Current

Simulation in Single-layer Tree Topology

The simulation of the real electric currents flowing to the 14 users in Subsection 5.2.1 still apply in this subsection.

All the 14 users are attached to a single DT. We denote the resistance of the link between the DT and the ith user by R_i, for $i = 1, 2, \cdots, 14$. The resistance of the links

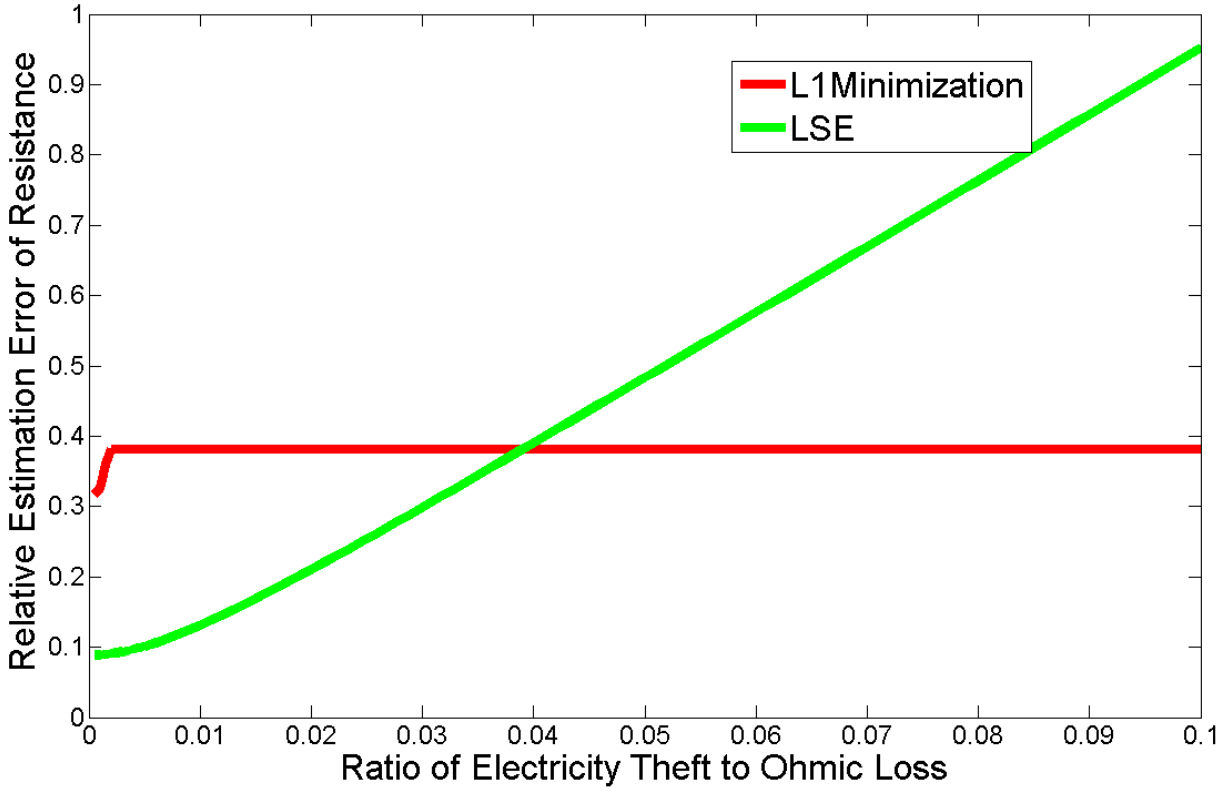


Figure 5.3: *The X-axis of this figure stands for the theft rate while the Y-axis corresponds to the relative estimation error of resistance. The green plot is the result by the least squares estimation while the red plot is the result of ℓ_1 minimization. As we can see, the estimation error of least squares estimation increases rapidly with the increase of theft rate while the estimation error of ℓ_1 minimization is robust against the increase of theft ratio.*

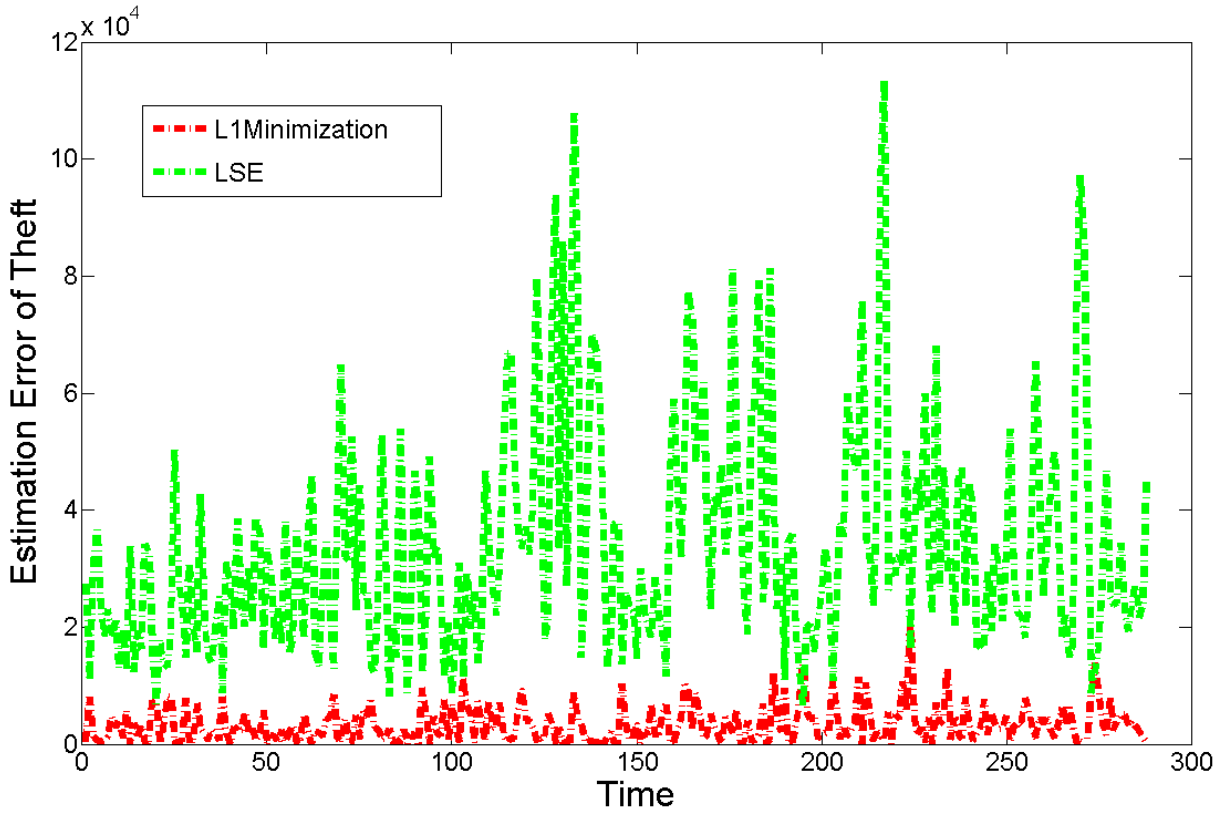


Figure 5.4: *The X-axis of this figure represents the time interval number while the Y-axis stands for the estimation error of theft in a time interval. The green plot is the result of least squares estimation while the red plot is the result of the ℓ_1 minimization. As we can see, the estimation error of ℓ_1 minimization is smaller than least squares estimation overall.*

between DT and the first 10 users are directly from **Nikovski2013**. For $i = 11, 12, 13, 14$, the resistance of the line between DT and the ith user is generated to be

$$R_i = \frac{2}{10}\begin{bmatrix} R_1 & R_2 & \dots & R_{10} \end{bmatrix}\sigma, \sigma \in \mathbb{R}^{10},$$

where the coordinates σ_j $(1 \le j \le 10)$ are independently drawn from a uniform distribution $\mathbf{Unif}(0, 1)$. The realizations of σ for different users are independent. The DT parameter is set to be $\frac{1}{20}$. The voltage potentials measured at the entry of the DT and at the entry of each user are simulated respectively to be 5,000 Volts and 250 Volts plus a small Gaussian noise.

In the following discussion, if method 1 and method 2 respectively estimate the resistance R to be $\hat{R}$ and $\tilde{R}$, with $\tilde{R}$ being closer to R than that of $\hat{R}$, then we say that method 2 (compared to method 1) improves the accuracy of estimation by

$$\frac{\left|\hat{R} - R\right| - \left|\tilde{R} - R\right|}{R}.$$

We conduct the following two tests. In the first test, we use the simulated measurements of electric currents from Subsection 5.2.1. We recover the incorrect measurements by solving Problem (2.8) and Table 5.4 shows the estimation of resistance before and after the recovery of incorrect measurements. Since the first nine users are not tampering with the meters, there is not much difference between the accuracy of the estimation of $R_1, \cdots, R_9$ before and after the recovery. However, the accuracy of the estimation of $R_{10}, \cdots, R_{14}$ is improved significantly by at least 50% after the recovery.

In the second test, we use the simulated measurements of electric currents from Subsection 5.2.2. We recover the incorrect measurements by two different recovery methods (solving Problem (2.8) and running Algorithm 1), and Table 5.5 shows the estimation of resistance before and after the recovery of incorrect measurements. As indicated in Table 5.5, the accuracy of the estimation of $R_1, \cdots, R_9$ before the recovery is affected by the time-varying tampering ratios of Users 10, 12, 14 even though the first nine users are not tampering with the smart meters. As for the estimation of R_2 and R_4, both recovery methods improves the accuracy by at least 5%; as for the estimation of R_{11} and R_{13}, both recovery methods improves the accuracy by at least 20%; as for the estimation of R_{10} and R_{14}, the recovery method by solving Problem (2.8) does not show significant improvement while the time-varying recovery method increases the accuracy by at least 25%; as for the estimation of the other resistance, both recovery methods do no show significant improvement.

Simulation in Multi-layer Tree Topology

The topology we use for simulation is shown in Figure 5.5. The nodes $v_{0,1}, v_{1,1}, v_{1,2}$, $v_{2,1}$, $v_{2,2}$, $v_{2,3}$, $v_{2,4}$ decrease the voltage and distribute the energy to users, which are represented by the nodes $v_{3,1}$, $v_{3,2}$, $v_{3,3}$, $v_{3,4}$, $v_{3,5}$, $v_{3,6}$, $v_{3,7}$, $v_{3,8}$. The real electric currents that flow to

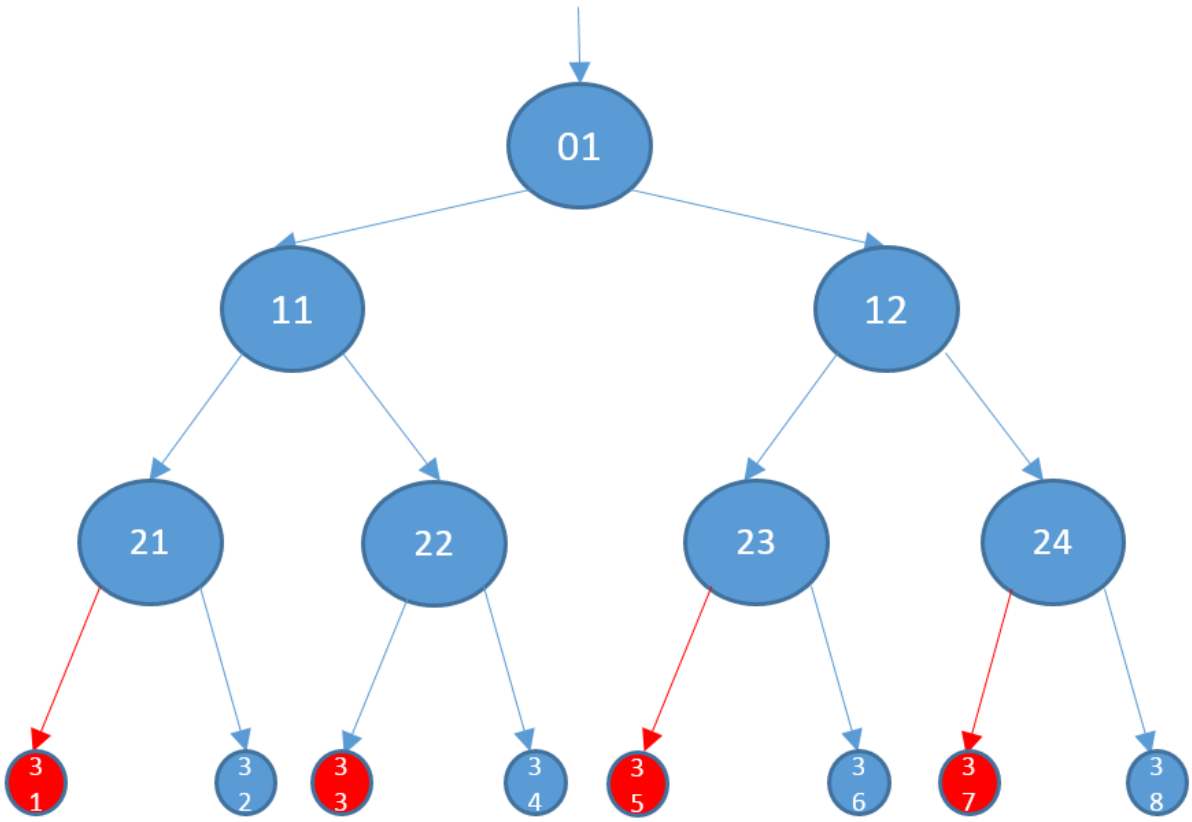


Figure 5.5: Topology for the Simulation in Section 4.4

Resistance	Estimation	Real Val
$R_{v_{0,1}\to v_{1,1}}$	0.1957	0.1957
$R_{v_{0,1}\to v_{1,2}}$	0.2069	0.2076
$R_{v_{1,1}\to v_{2,1}}$	21.8860	21.7003
$R_{v_{1,1}\to v_{2,2}}$	27.0417	27.1434
$R_{v_{1,2}\to v_{2,3}}$	20.1511	19.7573
$R_{v_{1,2}\to v_{2,4}}$	18.4532	18.2867
$R_{v_{2,1}\to v_{3,1}}$	0.2185	0.2185
$R_{v_{2,1}\to v_{3,2}}$	0.1815	0.1815
$R_{v_{2,2}\to v_{3,3}}$	0.2359	0.2359
$R_{v_{2,2}\to v_{3,4}}$	0.2418	0.2418
$R_{v_{2,3}\to v_{3,5}}$	0.2148	0.2148
$R_{v_{2,3}\to v_{3,6}}$	0.1789	0.1789
$R_{v_{2,4}\to v_{3,7}}$	0.1806	0.1806
$R_{v_{2,4}\to v_{3,8}}$	0.2296	0.2296

Table 5.6: Estimation of Transmission Resistance Using Measurement of Voltage 3

Resistance	Estimation		Real Val
	Before Recovery	After Recovery	
$R_{v_{0,1}\to v_{1,1}}$	0.1957	0.1957	0.1957
$R_{v_{0,1}\to v_{1,2}}$	0.2069	0.2069	0.2069
$R_{v_{1,1}\to v_{2,1}}$	22.2054	22.2054	21.8860
$R_{v_{1,1}\to v_{2,2}}$	27.3867	27.3867	27.0417
$R_{v_{1,2}\to v_{2,3}}$	20.2986	20.2986	20.1511
$R_{v_{1,2}\to v_{2,4}}$	18.7835	18.7835	18.4532
$R_{v_{2,1}\to v_{3,1}}$	0.5202	0.2185	0.2185
$R_{v_{2,1}\to v_{3,2}}$	0.1815	0.1815	0.1815
$R_{v_{2,2}\to v_{3,3}}$	0.6427	0.2359	0.2359
$R_{v_{2,2}\to v_{3,4}}$	0.2417	0.2418	0.2418
$R_{v_{2,3}\to v_{3,5}}$	0.3181	0.2147	0.2148
$R_{v_{2,3}\to v_{3,6}}$	0.1789	0.1789	0.1789
$R_{v_{2,4}\to v_{3,7}}$	0.3909	0.1806	0.1806
$R_{v_{2,4}\to v_{3,8}}$	0.2296	0.2296	0.2296

Table 5.7: Estimation of Transmission Resistance Using Measurement of Voltage 4

the users located at the leaves are directly from **Nikovski2013**. The real resistance of each link is simulated in the same way as described in the part of **Simulation in Single-layer Tree Topology**. Electric current and voltage are measured only at the entry of the DT $v_{0,1}$ and the entries of all users. The measurement of voltage at the entry of each user is simulated to be 240 Volts plus a small Gaussian noise.

In the first test, we do not simulate any user who is tampering with the smart meter. The measurement of the electric current flowing to each user is simulated to its real value plus a small Gaussian noise. The results of estimations are shown in Table 5.6. The result shows that our estimations are not affected much by the the noise of measurement and very close to the real values.

In the second test, the red users in the Figure 5.5, $v_{3,1}, v_{3,3}, v_{3,5}, v_{3,7}$ are simulated to be tampering with the smart meters. The measurements of the electric currents flowing through the red links are respectively simulated to be 0.42, 0.367, 0.675 and 0.462 times of their real values. Table 5.7 shows the estimation of resistance before and after the recovery of incorrect measurements. As for the estimation of $R_{v_{2,1}\to v_{3,1}}$, $R_{v_{2,2}\to v_{3,3}}$, $R_{v_{2,3}\to v_{3,5}}$ and $R_{v_{2,4}\to v_{3,7}}$, the estimation accuracy is improved by at least 50% after the recovery; as for the estimation of other resistance, the estimation accuracy is not significantly improved after the recovery.

5.4 Clustering

5.4.1 Test 1—Different Electric Current Patterns of Power Theft

In this subsection, we use 18 users in total for testing. The first nine users that we use for this section are all the nine honest users directly from the **Nikovski2013** data set. In addition to the honest users from **Nikovski2013**, we simulate 9 more users who are stealing energy by directly tapping a line. The simulated measurements of the electric currents flowing to these 9 thieves are shown in Figure 4.3. We call these 9 different theft patterns (of electric currents) in Figure 4.3 **Shift1**, **Shift2**, **Shift3**, **Periodic1**, **Periodic2**, **Periodic 3**, **Victim1**, **Victim2**, and **Victim3**. We run 9 tests and in each of the nine tests we use one of the these nine simulated thieves as user 10. For user i $(1 \le i \le 10)$, we have the vector $x_i \in \mathbb{R}^{288}$ that records the time-series measurements of electric current flowing to user i at 288 different moments. In each of these 9 tests, we apply 3 clustering algorithms K-means, spectral clustering and 1DBPE to partition the 10 vectors corresponding to the 10 users into two groups. The clustering results are shown in Table 5.8. As Table 5.8 indicates, all the clustering algorithms can figure out which one of the ten vectors of the measured electric currents shows an anomaly.

10th User	K-means		Spectral Clustering		1DBPE	
	Group1	Group2	Group1	Group2	Group1	Group2
Shift1	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Shift2	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Shift3	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Periodic1	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Periodic2	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Periodic3	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Victim1	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Victim2	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10
Victim3	Users 1~9	User 10	Users 1~9	User 10	Users 1~9	User 10

Table 5.8: Accuracy of Three Clustering Methods for Alternative Theft Patterns

Algorithm	Partition Results in Group1	Partition Results in Group2
K-means	Users 1~9 and users 14~18	Users 10~13
Spectral Clustering	Users 1~9 and users 13~18	Users 10~12
1DBPE	Users 1~9 and users 14~18	Users 10~13

Table 5.9: Accuracy of Three Clustering Methods for Standard Data Set

5.4.2 Test 2—An Explore of Clustering Accuracy VS Many Thieves

In the simulation of the last section, we have only one thieve and all of those 3 clustering algorithms can figure out whose measured currents shows anomaly compared to others . We are interested in how the clustering result changes with the increase of the number of abnormal users.

This section studies the relationship between the accuracy of clustering and the number of thieves. We maintain the first 9 honest users. We include all the 9 theft patterns in Figure 4.3 into our test. That is to say, there are 9 honest users and 9 abnormal users in this test, where users 1~9 are honest and users 10~18 are abnormal. Table 5.9 shows the results of clustering.

Unfortunately, the honest users and the abnormal users cannot be perfectly separated. The honest users share large similarities but the theft patterns are diverse. The common objective of all these clustering algorithms is to minimize the dissimilarities between different groups or maximize the similarities inside each group. Under such objective, it is unlikely for these clustering algorithms to put all these theft patterns in the same group since there is a huge diversity among them. Consequently, some theft patterns are partitioned into the same group as the honest users. For example, in the result (Table 5.9) of this test, users 14~18 (thieves) are assigned to the same group (group1) as users 1~9 (the honest users). In this situation, we may want to proceed one more step of bi-partition in group 1 to separate users 1~ 9 and users 14~18. This motivates us to apply the hierarchical

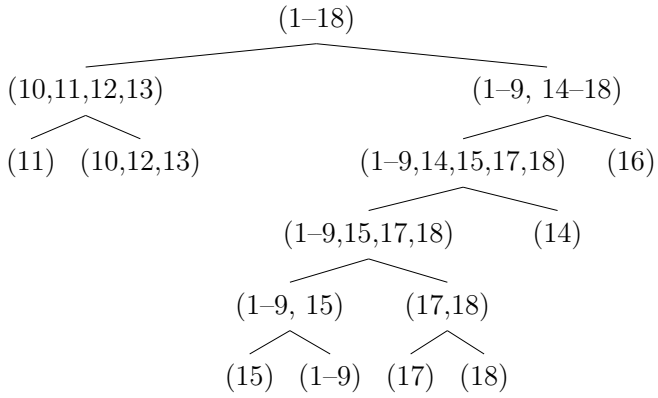


Figure 5.6: Recursion Tree

	Results of Hierarchy Clustering
Group1	User 11
Group2	User 10,12,13
Group3	User 16
Group4	Users 1~9
Group5	User 18
Group6	User 17
Group7	User 14
Group8	User 15

Table 5.10: Partition Results of Hierarchy Clustering

clustering, which bi-partitions the data points recursively until the dissimilarity inside a group is low enough.

To better illustrate the working process of the hierarchical clustering, we show the recursion tree of clustering in Figure 5.6. At the first step of clustering, 18 users are divided into two groups, the first group contains users 10~13, the second group contains users 1~9, 14~18. So the normal users 1~9 and thieves are assigned to the same group in the first step. With the proceeding of recursion, thieves are gradually excluded from the group of normal users. Finally, at the base level (leaf node), normal users 1~9 are in the

# Users	Members of Majority Group	Size of Second Majority	# Groups
30	Users 1~9	3	19
40	Users 1~9	3	28
50	Users 1~9	4	32
60	Users 1~9	4	38

Table 5.11: Hierarchy Clustering VS Number of Theives

same group with no thieves involved.

5.4.3 Test 3—An Explore of Clustering Accuracy VS Number of Thieves

In this subsection, we directly use the first 9 honest users from **Nikovski2013** and generate at most 51 thieves. The measurements of the electric currents flowing to the 51 thieves are generated from a linear combination of the 9 vectors in Figure 4.3. The coefficients of the linear combination are absolute values of a series of numbers drawn from Gaussian distribution. Consequently there are only 15% normal users in the worst case. To explore whether the accuracy of hierarchy clustering is affected by number of thieves, we include 21,31,41,51 thieves into our tests in turn.

The results of hierarchical clustering with 21, 31, 41, 51 thieves are summarized in Table 5.11. Table 5.11 shows the members of the majority group, the size of the second majority group, and the total number of groups partitioned by hierarchical clustering with the increase of thieves. The result tells that the hierarchical clustering constantly includes the normal users into the majority group while any other thieve is excluded from the majority group. The number of groups(partitioned by hierarchy clustering) increases with the number of thieves. Other than the majority group, any other group has only very few members. So the hierarchy clustering can recognize the normal users as the majority group even though the percentage of normal users is as low as 18%.

Chapter 6

Conclusion

In this thesis, we deal with mainly two types of theft: tampering with a smart meter and tapping a line. For the theft in the form of tampering with the smart meters, we propose a theft detection framework based on the knowledge of the tree topology of the electricity grid, which can potentially locate the source of theft and estimate the resistance of each link in the grid using the measurements of electric current, voltage and energy, where the measurement points are only set at the root distribution transformer and at the entries of all customers. When the theft in the form of tapping a line happens, the secretly introduced links prevent us from using the knowledge of the tree topology of the grid and thus our theft detection framework cannot locate the unknown illegal links. In this situation, we apply clustering algorithms to analyze the anomalies in the usage data of all customers. We propose a hierarchical clustering named 1DBPE which recursively bi-partitions the data along the principle eigenvector and separate the usage data of normal users and abnormal users.

On the numerical side of this thesis, we test our theft detection framework and our clustering algorithm 1DBPE on the computer simulation based on real data. Our numerical results show that

- Our theft detection framework can effectively locate the tampering and accurately estimate the tampering ratio of each user within a range of measurement noises when the tampering ratios are constant;
- Our theft detection framework can recognize the time-varying tampering but the exact recovery of the real electric currents is not guaranteed when the tampering ratios change with time;
- Our theft detection framework can accurately estimate the resistance of each link as long as the measurements (or the estimations) of the electric currents are accurate and hence the severe lossy links can be accurately located;

- Given a suitable threshold of variance, our clustering algorithm 1DBPE can automatically decide the number of groups that the data are partitioned into, and separate the usage data of normal users from the abnormal users.

On the theoretical side of this thesis, we observe that our estimation of path loss rates, estimation of tampering ratios and estimation of transmission resistance share the same formulation $\min_{x \geq 0} \|Y - Ax\|_{\ell_1}$. We give a novel proof to show that under some suitable conditions, the ℓ_1 minimization problem has a unique minimizer and the unique minimizer is equal to the real underlying solution.

References

[1] *http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf*.

[2] *https://www.bchydro.com/safety-outages/keeping-communities-safe/electricity-theft.html*.

[3] Vijay Arya and Balakrishnan Narayanaswamy. Loss localisation in smart distribution networks. In *Sixth International Conference on Communication Systems and Networks (COMSNETS), IEEE, 2014*, pages 1–8. IEEE, 2014.

[4] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[5] Rasmus Bro and Sijmen De Jong. A fast non-negativity-constrained least squares algorithm. *Journal of chemometrics*, 11(5):393–401, 1997.

[6] Emmanuel J Candes and Terence Tao. Decoding by linear programming. *Information Theory, IEEE Transactions on*, 51(12):4203–4215, 2005.

[7] Jianlin Cheng, Arlo Randall, and Pierre Baldi. Prediction of protein stability changes for single-site mutations using support vector machines. *Proteins: Structure, Function, and Bioinformatics*, 62(4):1125–1132, 2006.

[8] David L Donoho and Jared Tanner. Sparse nonnegative solution of underdetermined linear equations by linear programming. *Proceedings of the National Academy of Sciences of the United States of America*, 102(27):9446–9451, 2005.

[9] Michel Goossens, Frank Mittelbach, and Alexander Samarin. *The LaTeX Companion*. Addison-Wesley, Reading, Massachusetts, 1994.

[10] Trevor Hastie, Robert Tibshirani, and Jerome Friedman. *The Elements of Statistical Learning*. Springer Series in Statistics. Springer New York Inc., New York, NY, USA, 2001.

[11] Ian Jolliffe. *Principal component analysis*. Wiley Online Library.

[12] Petr Kadurek, Jos Blom, JFG Cobben, and Wil L Kling. Theft detection and smart metering practices and expectations in the netherlands. In *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, pages 1–6. IEEE, 2010.

[13] Peter Kelly-Detwiler. Electricity theft: A bigger issue than you think. *http://www.forbes.com*, 2013.

[14] Donald Knuth. *The TEXbook*. Addison-Wesley, Reading, Massachusetts, 1986.

[15] Tony R. Kuphaldt. Lessons in electric circuits, Volume II AC. *ibiblio, http://www.ibiblio.org/kuphaldt/electricCircuits/AC/AC.pdf*, 2007. Sixth Edition.

[16] Leslie Lamport. *LATEX — A Document Preparation System*. Addison-Wesley, Reading, Massachusetts, second edition, 1994.

[17] Yuan-Liang Lo, Shih-Che Huang, and Chan-Nan Lu. Non-technical loss detection using smart distribution network measurement data. In *Innovative Smart Grid Technologies-Asia (ISGT Asia), 2012 IEEE*, pages 1–5. IEEE, 2012.

[18] Michael Merritt and Yin Zhang. Interior-point gradient method for large-scale totally nonnegative least squares problems. *Journal of optimization theory and applications*, 126(1):191–202, 2005.

[19] Reid Miller. Analysis of weather, time, and mandatory time-of-use pricing effects on aggregate residential electricity demand. *UWspace*, 2015.

[20] Daniel Nikolaev Nikovski, Zhenhua Wang, Alan Esenther, Hongbo Sun, Keisuke Sugiura, Toru Muso, and Kaoru Tsuru. Smart meter data analysis for power theft detection. In *Machine Learning and Data Mining in Pattern Recognition*, pages 379–389. Springer, 2013.

[21] AH Nizar, ZY Dong, and Y Wang. Power utility nontechnical loss analysis with extreme learning machine method. *Power Systems, IEEE Transactions on*, 23(3):946–955, 2008.

[22] LLC Northeast Group. World loses $89.3 billion to electricity theft annually, $58.7 billion in emerging markets. *http://www.prnewswire.com/news-releases*, 2014.

[23] Kalil T Swain Oldham. *The Doctrine of Description: Gustav Kirchhoff, Classical Physics, and the" purpose of All Science" in 19th-century Germany*. ProQuest, 2008.

[24] Sergio Salinas, Ming Li, and Pan Li. Privacy-preserving energy theft detection in smart grids. In *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on*, pages 605–613. IEEE, 2012.

[25] Lindsay I Smith. A tutorial on principal components analysis. 2002.

[26] Staff Report. *Assessment of Demand Response and Advanced Metering*. Federal Energy Regulatory Commission, December 2012.

[27] Lloyd N Trefethen and David Bau III. *Numerical linear algebra*, volume 50. Siam, 1997.

[28] Ulrike Von Luxburg. A tutorial on spectral clustering. *Statistics and computing*, 17(4):395–416, 2007.

[29] Stephen J. Wright and Jorge Nocedal. *Numerical optimization*. Springer New York, second edition, 2006.

[30] Yin Zhang. A simple proof for recoverability of l1-minimization (ii): the nonnegativity case. *Rice University CAAM technical report TR05-10*, 2005.