論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Robust State Estimation of Power Systems under Cyber Attacks: Decomposition-based Approach
著者(和文)	AHMADINAJAFABADINAIME
Author(English)	Naime Ahmadinajafabadi
出典(和文)	学位:博士(学術), 学位授与機関:東京工業大学, 報告番号:甲第12481号, 授与年月日:2023年3月26日, 学位の種別:課程博士, 審査員:石井 秀明,三宅 美博,DEFAGO XAVIER,小野 功,小野 峻佑
Citation(English)	Degree:Doctor (Academic), Conferring organization: Tokyo Institute of Technology, Report number:甲第12481号, Conferred date:2023/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

Robust State Estimation of Power Systems under Cyber Attacks: Decomposition-based Approach

Naime Ahmadi
Department of Computer Science
Tokyo Institute of Technology

Supervisor
Hideaki Ishii

In partial fulfillment of the requirements for the degree of
Doctor of Philosophy

March, 2023

Abstract

Power grids are facing serious cyber-security issues due to the rapid development of the smart grid and increasingly integrated communication networks. State Estimation (SE) is one of the essential tasks to monitor and control the smart power grid. The impact of false data injection (FDI) attacks on static state estimation of power systems has been actively studied in the past decade.

This thesis studies the robust static state estimation under false data injection attacks targeting both the measurement vector and the regressor matrix which result in observation outliers and leverage points. The objective is to find how decomposing power systems to islands and implementing robust regression estimators affect the detection of random and coordinated attacks.

For decomposing the system to generate islands, we propose an algorithm for the on-line implementation of a robust static state estimator on large power systems. This algorithm increases the number of outliers and cyber-attacks that the estimator can resist while giving reliable estimates. In particular, the large power system is decomposed in several islands or subsystems and a highly robust regression estimator, namely the least trimmed squares estimator (LTS), is implemented on each island to detect bad data. Further, executing the estimators in parallel will greatly reduce the computation time of the robust static state estimator.

The introduced method is compared with two cycle detection graph-theory approaches, namely depth-first search (DFS) and minimum spanning tree (MST), which have been adapted here for power state estimation. Simulations on IEEE 14, 30, 57, 118, 145, and 300 bus systems show the superior performance of the proposed algorithm over the adapted DFS and MST. The algorithm could reduce significantly the number and size of cycles in the system. Furthermore, the number of detected outliers and attacks is maximized while the observability of the system is ensured. Attacks or outliers on both measurements and topology of the grid are detected as well.

We further compare the two methods namely, proposed and MST method by implementing different robust static state estimators such as the Huber M-estimation, the least absolute value (LAV), which are implemented for each island to detect the corrupted data. In particular, we focus on highly adversarial cases where the attacker can falsify both the measurement vector and the regressor matrix and attempts to manipulate the states to targeted values.

Extensive simulations on the IEEE bus systems show the superior performance of the proposed LTS with the proposed decomposition-based algorithm over other estimation and decomposition methods. The simulation results show also the limits of each robust method especially when the attacks are designed in a coordinated fashion. To this end, we analyze the structure of the system topology and measurements and perform extensive simulations using the IEEE 14 and 118 bus systems. Furthermore, we investigate robustness improvement when phasor measurement units (PMUs) are available and hybrid state estimation can be employed.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisor Professor Hideaki Ishii for the continuous support of my Ph.D. study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. There is no doubt that I could not have completed Ph.D. without his support. I also could not have imagined having a better advisor and mentor for my Ph.D. study.

I would like to thank Professor Yacine Chakhchoukh from the University of Idaho, USA, who has also supervised this study from the very start with his expert knowledge on power system state estimation. Without his precious support it would not have been possible to conduct this research.

I would like also to appreciate Professor Yoshihiro Miyake, Professor Xavier Défago, Professor Isao Ono, and Professor Shunsuke Ono, who kindly served as the examiners of my thesis committee. Thank you for reading my thesis and providing me with positive and constructive feedback.

Last but not the least, my warm and heartfelt thanks go to my family, my parents and brother for their tremendous support and hope they had given to me from thousand of kilometers distance. Without that hope, this thesis and Ph.D. would not have been possible. Thank you all for the strength you gave me. I love you all.

Contents

1 Introduction **1**

1.1 Background 1

1.2 Cyber Attacks in the Energy Sector 2

1.3 Classifying of Smart Grid Attacks 4

1.4 Smart Grid Security Requirements 6

1.5 False Data Detection Algorithms 9

1.5.1 Model-Based Detection Algorithms 9

1.5.2 Data-Driven Detection Algorithms 10

1.6 Static State Estimation and Security Problem 11

1.7 Contributions of the Thesis 13

1.8 Outline of the Thesis 17

2 Overview on Power System State Estimation **19**

2.1 Static State Estimation Problem 19

2.1.1 Power System Model 20

2.1.2 The Nonlinear and Linear Estimation Problems 22

2.1.3 The Jacobian Matrix 24

2.2 The Weighted Least Squares Estimator 25

2.3 Bad Data Detection 27

2.4 Model of False Data Injection Attacks 28

2.5 Robust State Estimation 29
2.5.1 Least Absolute Value (LAV) 29
2.5.2 Huber M-estimation 30
2.5.3 Least Trimmed Squares (LTS) 30

3 Decomposition-Based State Estimation and Attack Detection 32
3.1 Necessity for Decomposition 32
3.2 Cyber Security Criteria for Decomposing the System 33
3.3 General Approach: LTS with Decomposition 34
3.4 Detection of Cyclic Islands 36
3.5 Proposed Cycle Detection Algorithm 39
3.5.1 Planar Embedding of Power Systems 42
3.5.2 Planar Subgraphs 44
3.5.3 Face Detection in Planar Graphs 45

4 Analysis of the Decomposition-Based State Estimation 48
4.1 Decomposition into Islands 48
4.1.1 IEEE 14-Bus System Case 49
4.1.2 Numerical Performance and Scalability 50
4.2 LTS Estimators: Simulation Setting 58
4.3 LTS Estimators: Results and Comparisons 62

5 Targeted Coordinated Attacks on Decomposition-Based State Estimation 67
5.1 Three-Step SE Algorithm 67
5.2 Targeted Coordinated Attacks on Decomposition-Based SE 68
5.2.1 IEEE 14-Bus System: Decomposition and Its Resiliency . . 68
5.2.2 Two Classes of FDI Attacks Against the LTS 70
5.2.3 Resilience Analysis of the Two Decomposition Methods . . 74

5.2.4 Discussion on Detection of Random Errors and Attacks . . 77
5.3 Simulation 78
5.3.1 Simulation Setup for the IEEE 14-Bus System 78
5.3.2 Attacks on Measurements 79
5.3.3 Attacks on the Jacobian Matrix 81
5.3.4 Hybrid Estimation under Attacks on the Jacobian 86
5.3.5 IEEE 118-Bus system and Attacks on Its Jacobian 90

6 Conclusion 96

6.1 Summary 96
6.2 Future Directions 97

References 108

List of Figures

1.1 Classification of cyber-physical attacks based on how they are delivered. 4

1.2 Vulnerabilities of the smart grid to attacks involving false data injection [14]. 8

2.1 One-line diagram of 5-bus system 20

2.2 π-equivalent model of a transmission line 21

3.1 Radial and cycle islands in a sample power system. 34

3.2 Flowchart of the proposed cyclic island detection algorithm. . . . 39

3.3 Planar embedding of the IEEE 118-bus system by the STAC. . . . 43

3.4 Illustration of the cycle detection algorithm. 46

4.1 Decomposition of the IEEE 14-bus system: Original graph. 49

4.2 Decomposition of the IEEE 14-bus system faces in the (a) first subgraph $\mathcal{G}^{(1)}$ (b) second subgraph $\mathcal{G}^{(2)}$. 50

4.3 Decomposition of the IEEE 14-bus system using the (a) proposed method (b) MST method. 53

4.4 Decomposition of the IEEE 30-bus system using the (a) proposed method (b) MST method. 53

4.5 Decomposition of the IEEE 39-bus system using the (a) proposed method (b) MST method. 54

4.6 Decomposition of the IEEE 57-bus system using the (a) proposed method (b) MST method. 54

4.7 Decomposition of the IEEE 118-bus system using the (a) proposed method (b) MST method. 55

4.8 Decomposition of the IEEE 145-bus system using the (a) proposed method (b) MST method. 55

4.9 Decomposition of the IEEE 300-bus system using the (a) proposed method (b) MST method. 56

4.10 Boxplots of the breakdown points of the proposed method (P) versus the MST-based method (M) for the IEEE bus systems based on the reduced measurement configuration (see Table 4.2) for the estimation of phase angles. 56

4.11 Boxplots of the breakdown points of the proposed method (P) versus the MST-based method (M) for the IEEE bus systems based on the reduced measurement configuration (see Table 4.2) for the estimation of voltage magnitudes. 57

4.12 Average parallel computation times for SE: The proposed method (P) versus the MST-based method (M) for the IEEE bus systems based on the reduced measurement configuration (see Table 4.2). . 65

5.1 IEEE 14-bus system and the placement of measurements and attacks. 69

5.2 Average estimation errors under random attacks on measurements. 80

5.3 Average estimation errors under coordinated attacks on measurements. 81

5.4 Average estimation errors under attacks on the Jacobian matrix. . 82

5.5 Estimated phase angles of 14 buses by LTS-PFT (top) and LTS-MST (bottom) under attacks on the Jacobian matrix for $N_s = 4, 5$. 83

5.6 Estimated phase angles of 14 buses by LTS-PFT (top) and LTS-MST (bottom) under attacks on the Jacobian matrix for $N_s = 6, 8$. 84

5.7 The estimated probability of detection leverage point. 86

5.8 The estimated probability of false detection. 87

5.9 The true probability of detection of leverage points. 87

5.10 Average estimation errors with PMUs at bus 2 under coordinated attacks on the Jacobian matrix. 88

5.11 Average estimation errors with PMUs at buses 2 and 9 under coordinated attacks on the Jacobian matrix. 89

5.12 Average estimation errors with PMUs at buses 2, 6, and 9 under coordinated attacks on the Jacobian matrix. 89

5.13 IEEE 118-bus system decomposed by PFT-based method and attacked buses. 91

5.14 IEEE 118-bus system decomposed by MST-based method and attacked buses. 91

5.15 Estimated phase angles of 118 buses by LTS-PFT (top) and LTS-MST (bottom) under attacks on the Jacobian matrix for $N_s = 10$. 92

5.16 Average estimation errors under attacks on the Jacobian matrix for the IEEE 118-bus system. 93

5.17 The estimated probability of detection leverage points for the IEEE 118-bus system. 94

5.18 The estimated probability of false detection for the IEEE 118-bus system. 95

5.19 The true probability of detection of leverage points for the IEEE 118-bus system. 95

List of Tables

1.1 Timeline of the significant physical and cyber attacks on the energy sector. 3

1.2 Cyber attacks and the security attack category. 8

1.3 Summary of the advantages and disadvantages of FDIA detection algorithms. 10

4.1 Comparison of three algorithms for system decomposition. 51

4.2 Measurement configuration for the IEEE bus systems. 60

4.3 Monte Carlo SE detection probabilities and error norm averages with the proposed method, the MST-based method, and the largest normalized residual method for the IEEE 118-bus system. 63

5.1 Decomposition of the IEEE 14- and 118-bus system by two methods 70

5.2 Islands in both methods and active power measurements linked to buses 2 and 6 in each island 71

5.3 Islands obtained from PFT-based method and active power measurements linked to buses 2 and 6 in each island 72

5.4 Islands in MST-based method and active power measurements linked to buses 2 and 6 in each island 73

5.5 Attacked measurements in the IEEE 14-bus system simulations . 75

5.6 Attacked measurements in the IEEE 118-bus system simulations . 92

Chapter 1

Introduction

1.1 Background

In recent years, the power grids are undergoing major changes as a result of rapid increase in variable renewable energy sources. This is strongly motivated by the world-wide efforts towards decarbonization in response to the serious climate changes, which is causing more catastrophic weather occurrences. In order to make the power grid more efficient, reliable, and secure, the next generation system should turn to the so-called smart grid [66]. To build a fully automated, resilient, and self-healing smart grid, a number of advanced technologies including information and communication technologies (ICTs), automation, distributed control, wide area monitoring and control (WAMS and WAMC), smart metering, and so on have been implemented into the current electric grid [36; 62]. As a result of these changes, the current power grid can be seen as a major example of cyber-physical system (CPS) [35].

One the other hand, the vulnerability of the smart grid has significantly increased by the adoption of the ICT components, and various incidents of cyber attacks take place on a daily basis today [76]. As a result, numerous research studies have been carried out to improve the security of the smart grid by first analyzing the different sources of vulnerability and then offering appropriate and trustworthy solutions [86].

1.2 Cyber Attacks in the Energy Sector

Throughout the last decade, a number of cyber physical attacks have been reported in the energy sector. The first major attack dates back to 1982. Various levels of damages were caused by these attacks. While some have not been noticed at all, others brought about serious consequences in the forms of physical damages and explosions in facilities, economic losses at the order of million dollars, and life losses. The US Energy Department received 362 reports of power outages between 2011 and 2014 that are assessed to be connected to cyber physical attacks; 161 were claimed in 2013, compared to 31 in 2011 [82]. According to a report on the state of industrial cyber security from 2017 [3], 54% of the organizations polled (359 companies in 21 countries) claimed to have encountered cyber physical security issues in the previous year, and 21% stated to have had difficulties at the same time. Table 1.1 illustrates the major incidents reported in the energy sector [2; 26; 43; 71; 78].

These occurrences and their significant effects prompted governments all over the world to acknowledge these new dangers. In order to improve the critical infrastructures' cybersecurity, in the US, the White House issued Executive Order 13636 in 2013 [37]. The National Institute of Standards and Technology (NIST) published a three-volume report in 2014 to lay out the fundamental principles for the cyber security of the smart grid [1].

Table 1.1: Timeline of the significant physical and cyber attacks on the energy sector.

Year	Where	Attack	Type	Impact
1982	Russia (Soviet Union)	CIA manipulated gas pipeline control software	Code manipulation	3 kilotons TNT equivalent explosion that could be seen from the space
1999	Bellingham (USA)	Slowdown of SCADA system of gasoline pipeline	Code manipulation	A huge fireball that killed 3 people and injured many others
2003	Ohio (USA)	Slammer Worm penetrated the control system of the nuclear plant	Malware Injection	Parameter Display System was off for 5 hours
2007	Idaho (USA)	Aurora Attack manipulated a circuit breaker of a diesel generator	False data injection	Exploded generator
2008	Turkey	Attacks on control system of pipe line	False data injection	Oil explosion and 30k barrels are spelled in water
2012	Saudi Arabia & Qatar	Malware affected Aramco and RasGas	Malware Injection	Generation and delivery of energy has been affected
2015	Kiev (Ukraine)	Attack on the breakers sittings in 3 distribution companies	False data injection	Blackout affecting 225k customers for few hours
2017	Kiev (Ukraine)	Power grid	Malware Injection	Substation shutdowns, power outages
2019	Utah (USA)	Electric distribution utilities	Denial of service attack	Interrupted electrical systems
2021	Queensland (Australia)	Energy generators	Ransomware attack	Limiting damage
2022	Nordex (Germany)	Wind turbine farms	Ransomware attack	IT operational interruption, remote control

1.3 Classifying of Smart Grid Attacks

We can categorize of various cyber-physical attacks into four major classes based on how they are delivered [29; 58]. Figure 1.1 shows each attack and the details are addressed below.

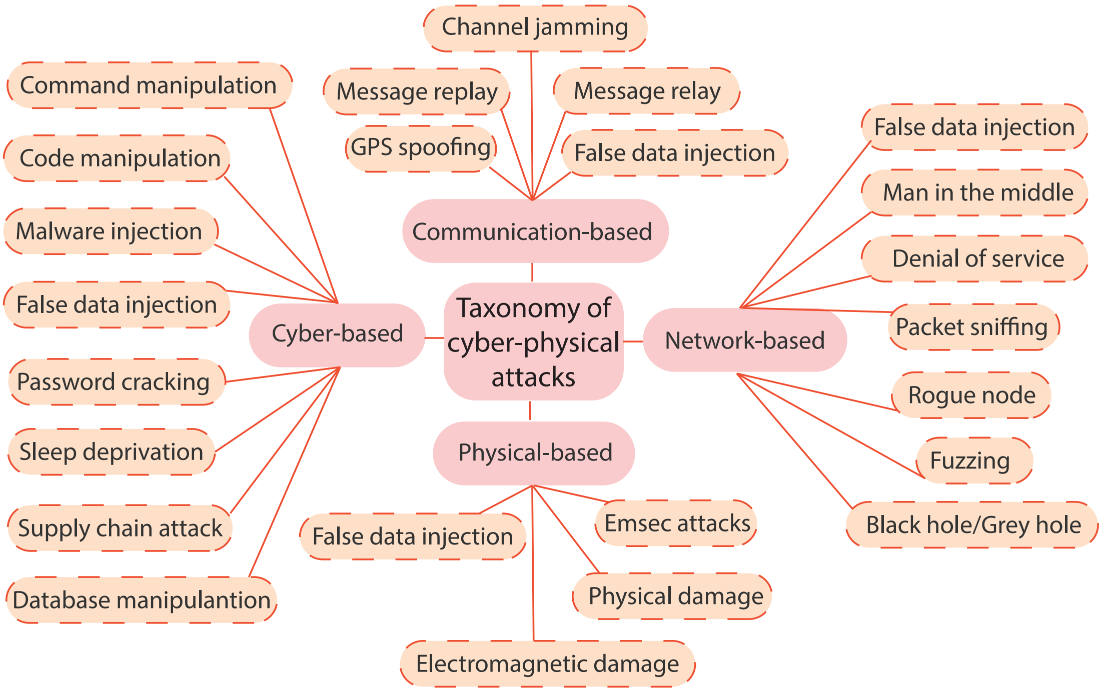


Figure 1.1: Classification of cyber-physical attacks based on how they are delivered.

- **Cyber-based attacks:** The system's cyber layer is used only to deliver cyber-based attacks.
  - **Code manipulation:** The attacker modifies the system's firmware or software to suit his or her purposes.
  - **Command manipulation:** The process of altering existing commands in the system without adding any new ones.
  - **Malware injection:** This attack happens frequently and involves

  injecting a virus or worm into the system.

  - **False data injection attacks (FDIA):** Change data without changing the system's code.
  - **Sleep deprivation:** Preventing devices from entering the low-power state and requiring them to continuously perform an action or receive, process, or transmit data. The sleep deprivation causes the devices to quickly exhaust themselves.

- **Network-based attacks:** Network-based attacks are built using virtual network access, which has no impact on the system's software, firmware, or physical communication link.

  - **Denial of service:** A large number of meaningless packets render the network unusable (main attack in this category).
  - **Black/grey hole:** Adversary completely or selectively discards packets from the network.
  - **False data injection attacks (FDIA):** The attacker can change the data contained within the network's packets.

- **Communication-based:** Attacks that use communication as their primary method of delivery and they do not involve any manipulation of the CPS virtual network; instead, they rely on a real, physical communication channel. These attacks may be created either by breaking the communication channel (channel gamming) or by sending messages that were false (FDIA).

  - **GPS spoofing:** Adversary imitates the GPS signal and inserts false data into it before sending it to the system.

  - **Message replay and relay attack:** Well-known attacks based on communication.

- **Physical-based attacks:** Physically harming the system.
  - **Electromagnetic damage:** Overvoltage or an electromagnetic pulse.
  - **FDIA:** Input of a particular device could be changed to produce false readings.
  - **Emission security (EmSec) attacks:** System emissions like heat, light, sound, or electromagnetic radiation.

When we examine the classification of cyber-physical attacks, we can see that the FDIA is a common trait among the various categories and it can be applied on all of the CPS's layers. Unlike other attack types, the FDIA may go undetected by the system according to the guidelines of NIST [1]. The numerous ways in which the smart grid may be exposed to FDIA are shown in Figure 1.2. The conclusion that can be drawn from these various layer-based FDIA is that as the technology develops, additional vulnerability spots may be created, which require further effort to secure the system [52].

1.4 Smart Grid Security Requirements

The National Institute of Standards and Technology (NIST) has defined three criteria for maintaining and protecting information in the smart grid: Confidentiality, Integrity, and Availability (CIA) [70]. Another important security criterion, according to [55], is accountability. Each criterion is described in detail below.

- **Confidentiality**

The confidentiality criterion requires safeguarding both personal privacy and proprietary information from unauthorized entities, individuals, or processes. For example, information sent between a customer and various entities such as meter control, metering usage, and billing information must be confidential and protected; otherwise, the customer's information could be manipulated, modified, or used for other malicious purposes.

- **Availability**

  The availability of information is defined as ensuring timely and reliable access to and use of information. It is regarded as the most important security criterion in smart grid because loss of availability means disruption of information access in a smart grid. For example, a loss of availability can disrupt the operation of the control system by preventing information from flowing through the network and thus denying the network's availability to control the system's operators.

- **Integrity**

  In the smart grid, integrity means safeguarding against unauthorized modification or destruction of data. Loss of integrity may cause the power management system to make incorrect decisions.

Table 1.2 lists the attacks that are preventing the CIA from operating in smart grids.

1.5 False Data Detection Algorithms

In order to detect FDIA in smart grids, several approaches have been developed [11; 50; 51; 56]. Despite the huge differences between these directions, two

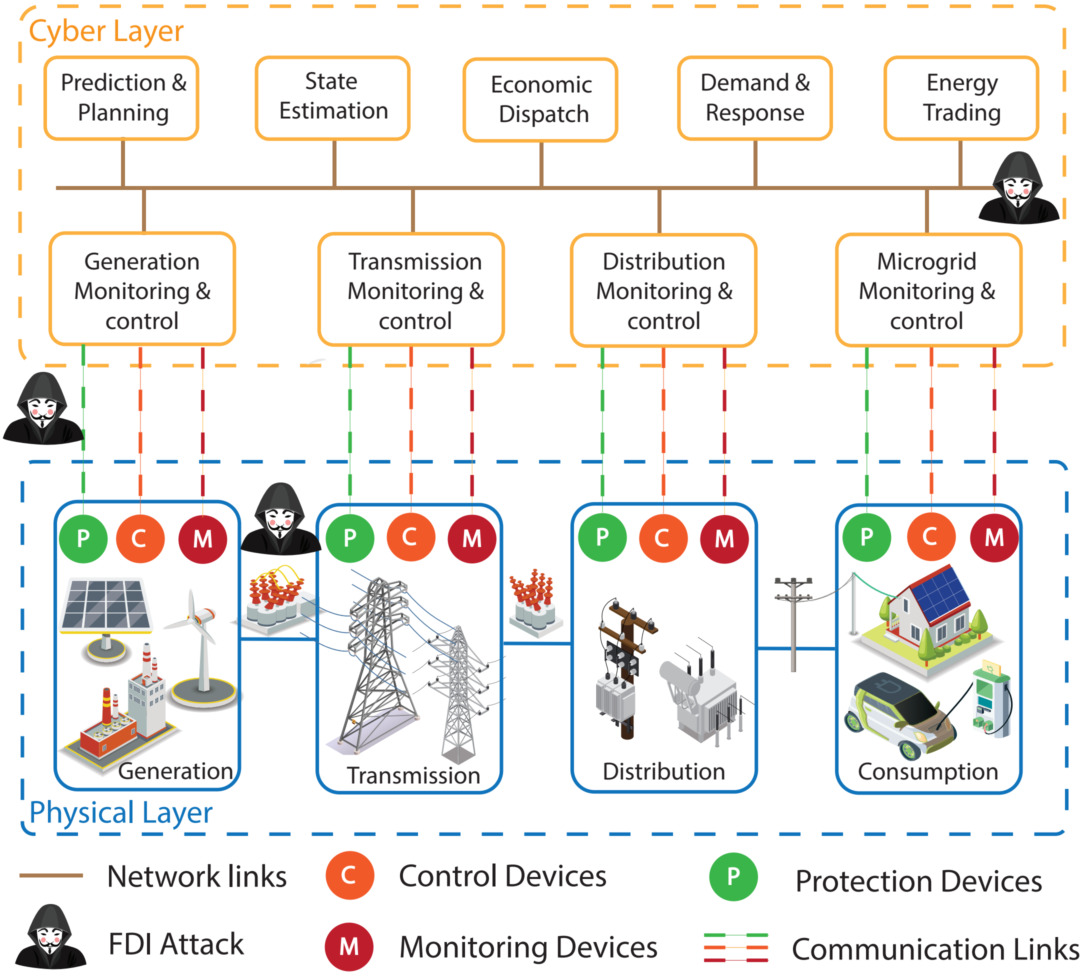


Figure 1.2: Vulnerabilities of the smart grid to attacks involving false data injection [14].

Table 1.2: Cyber attacks and the security attack category.

Attack Category	Security Requirements
False Data Injection	Integrity Availability
Man in the Middle	Integrity Confidentiality
Replay	Integrity Confidentiality
Denial of Service	Availability
Channel Jamming	Availability
Spoofing	Integrity Availability Confidentiality

main themes are model-based detection algorithms and data-driven detection algorithms.

1.5.1 Model-Based Detection Algorithms

Several FDIA detection techniques have been presented based on the system model (quasi-static or dynamic nature) [93]. The estimation-based detection could be categorized into three primary groups.

- **Estimation-based detection:** State estimate in power systems determines the states of the grid by using several sets of measurements taken throughout the entire power grid along with the system model and parameters.
  - **Static estimation methods:** Each estimation step in a static estimation is handled independently of the previous stage [65]. The main static state estimation-based FDIA detection method is based on the weighted least square.

- **Dynamic estimation methods:** However, due to stochastic changes in demand and generation, real-world power systems do not function in a steady state [93]. Dynamic state estimators, such the Kalman filter, were introduced to the power systems applications to address this issue [60].
- **Main detection tests:** Following the estimating processes, detection tests are the tools used to identify the FDIA [48]. These are basically comparisons of the estimated states with the actual measurements collected from the grid (Euclidean distance, largest normalized residual (LNR)).

1.5.2 Data-Driven Detection Algorithms

Data-driven detection algorithms are model-free, in contrast to model-based detection algorithms. As a result, neither the system's parameters nor models are utilized in the FDIA detection process [13; 19; 34]. Machine learning is one of these techniques which categorized into supervised learning [12; 44] and unsupervised learning [9]. On the other hand, data mining is the method of discovering patterns in large data sets and has been used in the context of attack detection in, e.g., [5; 69]. Also, principal component analysis (PCA) was employed in FDIA detection in [31].

To differentiate between the various FDIA detection algorithms in smart grid, Table 1.3 summarizes the benefits and drawbacks of each algorithm category.

For the safe and efficient operation of the power grid, the system is constantly monitored and operated at the control center. In practice, the operators use a static state estimator (SE), which provides the state of the grid [4] and permits the online security analysis. For this reason, we consider the static state estimation method in this dissertation.

Table 1.3: Summary of the advantages and disadvantages of FDIA detection algorithms.

Detection algorithm	Advantages	Disadvantages
Model-based	No training required No need for historical data set Reduced memory need	Need for system model Threshold selection Extensive computation Possible divergence
Data-driven	Independent of system and parameters Fast detection process Scalable	Need for extensive training

1.6 Static State Estimation and Security Problem

In order to evaluate the security of power systems, Fred Schweppe originally suggested the concept of the power system state estimation in the late 1960s [4]. State estimation (SE) is a mathematical procedure that processes redundant measurement data sets to remove measurement errors and estimate the most probable state of a power system. SE algorithms have been studied and improved for decades due to their critical role in reliable system monitoring.

The static SE gives the optimal state consisting of bus voltage phasors estimated from redundant measurements commonly provided by supervisory control and data acquisition (SCADA) units at remote terminal units and intelligent electronic devices, including active and reactive power flows and injections, and bus voltage magnitudes. More recently, the availability of phasor measurement units (PMUs) has enabled hybrid state estimation combining both PMUs and SCADA measurements in the observation set [42] to improve SE accuracy and performance. Placing a PMU at a bus can provide the voltage phasor at that bus, and the phasor currents on several or all lines incident to that bus [22].

Recently, the increase in cyber attack incidents has raised concerns for the problem of SE security [57; 77]. Under nominal operations, measurement errors could be present due to noise, equipment failures, and modeling errors and are detected by analyzing the residuals of the weighted least squares AC static SE [45; 53; 89; 91]. However, when an attacker launches malicious false data injection (FDI) attacks in the measurements with the knowledge on the system parameters and grid topology, the estimated states may be manipulated to targeted values without being detected as the residuals may remain small or unchanged [16; 49; 52; 87]. Recent works deal with FDI attack strategies which can be generated even if the attacker has only limited information such as data of a subnetwork [89] and limited PMU data [33]. In the literature, various FDI attack detection methods have been proposed; see the survey paper [67] and the references therein.

On the other hand, different FDI attack scenarios against the SE have been considered. One class of adversarial attacks known to be hard to detect is that of leverage point attacks, which target the entries in the Jacobian matrix of the regression model of SE, e.g., [7; 16; 17; 83; 91]. Such attacks can be generated by introducing changes in the network parameters and topology data stored at the system operators. Recently, it is shown in [54] that modifying network parameters can reduce the necessary number of FDI attacks. In the abovementioned works, it has been established that to obtain accurate state estimates under adversarial environments, robust estimation techniques (e.g., [61]) can be especially useful, including the least trimmed squares (LTS) [10; 16; 17; 20; 63; 83] and the robust Huber M-estimator [91]. Difficulties in SE when the data in the regressor model may contain uncertainties and the importance of robust methods have been recognized in the early works of [24; 63; 64] from the 1990s. In [17], it has been proposed to use multiple robust estimators in parallel to enhance the capability of attack detections.

In [24], robust estimation is used to detect bad measurements. The authors decomposed the IEEE 14-bus system into subsystems, or islands, for increasing the number of outliers that robust estimators can tolerate, which can be expressed in terms of breakdown points [61]. This approach enables robust SE algorithms such as least trimmed squares estimator (LTS) to execute on subsystems while ensuring the observability of the whole system [17]. To deal with large-scale systems, decomposition of the grid is found effective in [16; 63], where in each island the SE can be performed.

1.7 Contributions of the Thesis

For this reason, in our work [7; 8], we have developed a graph-based method to automatically decompose power systems and updating the decomposition data in real-time in a computationally efficient manner whenever the topologies change. We consider an estimation method that first decomposes the system into islands and then implements robust regression estimators at the island level as well as the system level. We can highlight the contributions of these thesis in three aspects:

- **Finding the cyclic island**

  The first objective is to extend the robust methods of [16; 24; 63] for their application to power systems of medium to large sizes. For small-scale systems, their decomposition is not a particularly challenging task and can be done manually. Our focus is on developing an algorithm for automatically finding islands and updating the decomposition data in real-time in a computationally efficient manner whenever the topologies change. This allows us to implement the detection of cyber-attacks online for real-life static SE.

  The main step in the decomposition of a given power network is to find islands containing loops or cycles. It turns out that for the robust state estimation techniques such as the LTS to perform well in the presence of attacks, it is essential to decompose the system into cyclic islands of smaller sizes. This is because in general, for smaller islands, the ratio of measurements that can be tolerated or resisted by the robust methods when attacked tends to be higher. Moreover, for state estimation, it suffices to have enough islands to cover the entire system. These aspects clearly depend on the number and the location of the measurements in the system, and we further discuss these issues in the thesis.

For finding cycles in a given graph, there are various established methods. These include the search and backtrack method [27; 81], the adjacency matrix method [72], methods using the minimum spanning trees (MST) [27; 39], and the cycle vector space method [79]. Note, however, that cycles in general simply refer to paths that are closed. Many of the methods above do not take account of the sizes of the cycles and hence may not be suitable for our purpose.

In this thesis, for finding the cyclic islands, we employ an alternative approach based on methods for detection of *faces* in planar graphs. In graph theoretic terms, faces refer to regions bounded by edges for a graph drawn on a plane. Hence, roughly speaking, faces correspond to islands of the smallest sizes in a graph while cycles may contain multiple faces. In comparison to algorithms for cycle detection, those for face detection require the additional information regarding the coordinates of the nodes. Such algorithms include those to detect polygons in a set of lines [38], computing overlays of two subdivisions [28], and the planar face traversal [73; 75].

However, these methods cannot be directly applied and there is another issue further adding computational complexity to the problem. Power systems have complex topologies and, in particular, have many intersections in their corresponding graphs [73]. Hence, in our proposed algorithm for cyclic island detection, we introduce several features to keep its complexity limited by not exhaustively searching for all faces in the system. Simulations show the effectiveness of the proposed algorithm for the larger IEEE systems with 118, 145, and 300 buses.

- **Decomposition and robust estimation in the presence of random attacks**

  We confirm the improvement of cyber-security obtained from the proposed decomposition and executing multiple LTS estimators with variable breakdown points for the different islands. In particular, we make extensive comparisons and with the case applying LTS to the decomposition obtained by a simpler cycle detection method. It is demonstrated that the number of measurement outliers detected increases. Different scenarios of measurement redundancy are considered. Moreover, the execution time is reduced thanks to the possibility of parallelizing the computation for detection on each island.

- **Decomposition and robust estimation in the presence of targeted coordinated attacks**

  We also consider the robust SE approach of [7; 16] against adversarial attacks especially when the attacks are more targeted and coordinated. The robust SE approach is based on two techniques: (i) Decomposition of the grid into islands and (ii) use of the LTS estimator at the island/subsystem level. The LTS is known as a particularly robust SE method; it ignores a fixed number of measurements corresponding to residuals with large magnitudes. In [7], we demonstrated the superiority of our PFT-based decomposition method[1] over other decomposition approaches. Comparisons were

[1] Throughout this thesis, the term "proposed algorithm" and "PFT-based decomposition"

made in terms of breakdown points for various IEEE systems with 14, 30, 57, 118, 145, and 300 buses.

Here, we aim to further improve our PFT-based robust SE method and expose its strength and limitations under FDI cyber-attacks of various degrees and placements. First, we analyze the properties of the decomposed grid from the viewpoint of the local state estimation executed at the islands. Its advantages are highlighted in comparison to islands obtained by a simpler graph-theoretic cycle detection based on the minimum spanning tree (MST) method. Then, through simulation studies, we will demonstrate the difference between the decomposition methods and the robust SE methods. The following two developments are critical in our study:

1. **Three steps SE algorithm**

   One is the enhanced version of the SE algorithm from [7; 16] consisting of three steps as follows: It first runs the LTS decentrally at each island level and then centrally at the entire system level; its robustness is enhanced by the residual analysis carried out as the third step.

2. **Construct adversarial coordinated FDI attacks against certain targeted buses in the system**

   Specifically, we attack the power injections at those targeted buses and their adjacent buses in both their measurements and the corresponding rows of the regressor matrix. By increasing the number of attack points, the attacker can eventually manipulate the state values of the targeted buses. In general, even by robust SE methods, the attacks on the regressor matrix are hard to resist and detect.

These techniques will be thoroughly tested by simulations on the IEEE 14-

are used interchangeably.

and 118-bus systems, and the impact of both randomly generated and targeted coordinated FDI attacks will be examined. For comparison reasons, we equip our algorithm with several robust SE schemes including the LTS, the Huber M-estimation, and the least absolute value (LAV). Furthermore, some of them as well as the conventional largest normalized residual (LNR) with a bad data detection (BDD) module will be implemented in a fully centralized fashion. Under three classes of attacks, we will demonstrate that our SE scheme clearly outperforms when equipped with the PFT-based decomposition in terms of accuracy on SE and attack detection probabilities especially when the regressor matrix is under coordinated attacks. We will moreover show that introducing PMUs can increase the SE performance.

1.8 Outline of the Thesis

This thesis is organized as follows.

In Chapter 2, we reviews static state estimation and bad data detection. We discuss the WLS is not reliable and analyzing its residuals does not guarantee their detection in the presence of attack. In fact, even one leverage point can go without detection and thus can greatly affect the estimation performance. Then, the robust estimation techniques are formulated.

In Chapter 3, our focus is on developing an algorithm for automatically finding islands and updating the decomposition data in real-time in a computationally efficient manner whenever the topologies change. We explain the decomposition criteria and also the decomposition methods of power systems. We develop the decomposition method which can implemented in the robust least trimmed squares estimator.

Chapter 4 analysis the random attacks on decomposition-based state estimation. We examine the effectiveness of the proposed approach through extensive simulations. For highlighting the advantage of our method, we apply our method for IEEE bus systems. Then the proposed decomposition method is compared to conventional algorithms. In the last part of this chapter, we perform state estimation by implementing the decomposition based least trimmed squares in the presence of FDI attacks.

Chapter 5 studies the targeted coordinated attacks on decomposition-based SE. We follow the approach of chapter 4 and demonstrate the effectiveness of the robust estimation method by analyzing it against a class of coordinated attacks targeting certain buses and their adjacent buses in the system. We discuss strength and limitations of our algorithm under FDI cyber-attacks of various degrees and placements.

Finally, Chapter 6 gives a summary for the results. Some interesting directions for the future research are also given in this chapter.

Chapter 2

Overview on Power System State Estimation

For the safe and efficient operation of the power grid, the system is constantly monitored and operated at the control center to keep the operating conditions normal and secure. In practice, the operators use a static state estimator (SE), which provides the state of the grid [4] and permits the online security analysis. It processes redundant measurements to provide an optimal estimate of the current operating state. The results of the state estimation are also used for contingency analysis, economic dispatch, optimal power flow, and security enhancement.

We begin this chapter by discussing static state estimation, weighted least squares, and bad data detection. The attack model is then explained, as well as why weighted least squares is insufficient for detecting the attack. We provide robust state estimation in the chapter's ending.

2.1 Static State Estimation Problem

State estimation uses three kinds of data as inputs:

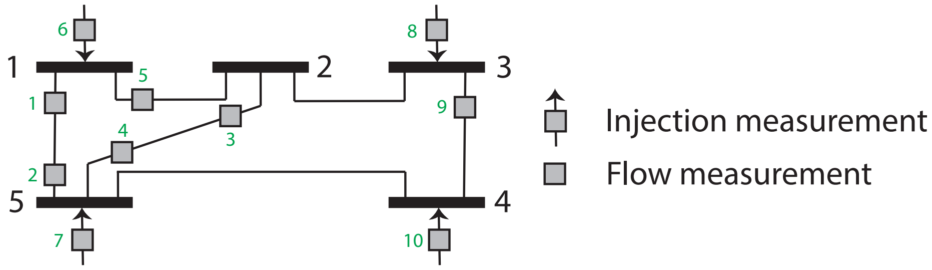


Figure 2.1: One-line diagram of 5-bus system

(i) The network topology data, consisting of the on/off status of power network switches and circuit breakers between buses.

(ii) The measurement data, including voltage magnitudes, power injections and flows.

(iii) The parameter data, including the branch admittance data and the variances of measurement noises.

The network topology and measurement data are communicated to the control center from SCADA units. After receiving the measurements and the topology, the system's observability is verified, and the weighted least squares (WLS) AC state estimator algorithm is executed to obtain the estimates of the state variables, which are the voltage magnitudes and phase angles at all buses of interest.

2.1.1 Power System Model

In this subsection, we outline the modeling of the power system, which forms the basis for state estimation. We consider the transmission system, which consists of N buses. A generator or synchronous condensor may inject power into a bus, and/or a load may draw power from it (a negative injection). Buses without any injected power are said to contain zero injection. Figure 2.1 shows a one-line diagram of a 5-bus system.

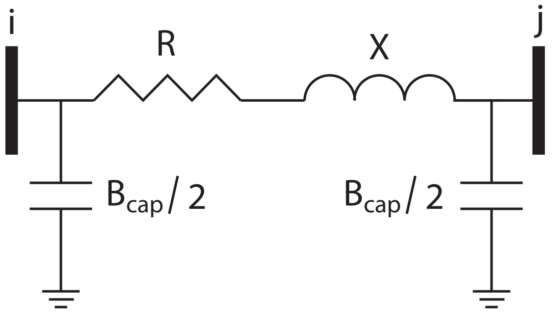


Figure 2.2: π-equivalent model of a transmission line

Transmission lines are typically represented by a π-equivalent model as shown in Figure 2.2, where the line connecting buses i and j is referred to as line (i, j). The impedance of a line, denoted by Z_{ij}, is equal to the complex sum of the line resistance, R_{ij}, and the line reactance, X_{ij}, yielding

$$Z_{ij} = R_{ij} + jX_{ij}. \tag{2.1}$$

The capacitance of the line, B_{cap}, is divided in half and treated as two discrete shunt capacitors - one at each end of the line. The inverse of the line impedance is given by

$$Y_{ij} = G_{ij} + jB_{ij}, \tag{2.2}$$

where Y_{ij} is the line admittance. The line conductance, G_{ij}, and the line susceptance, B_{ij}, are written as

$$G_{ij} = \frac{R_{ij}}{R_{ij}^2 + X_{ij}^2} \quad B_{ij} = \frac{-X_{ij}}{R_{ij}^2 + X_{ij}^2}. \tag{2.3}$$

The voltage at bus i is a complex quantity which can be expressed in polar form as $V_i \angle \theta_i$, where V_i is the magnitude and θ_i is the phase of the voltage at bus i. Both V_i and θ_i are the state variables of the system. The bus voltage magnitude, is often measured directly.

The real power flow from bus i to bus j on line (i, j) can be expressed as

$$P_{ij} = V_i^2 G_{ij} - V_i V_j \left(G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij}\right), \tag{2.4}$$

where δ_{ij} is equal to $\theta_i - \theta_j$. The reactive power flow on line (i, j) can be expressed as

$$Q_{ij} = V_i V_j \left(B_{ij} \cos \theta_{ij} - G_{ij} \sin \theta_{ij}\right) - V_i^2 \left(B_{ij} + B_{cap}\right). \tag{2.5}$$

The real power injected at bus i is equal to

$$P_i = \sum_j P_{ij}. \tag{2.6}$$

A similar expression for the reactive power injected at a bus i is

$$Q_i = \sum_j Q_{ij}. \tag{2.7}$$

2.1.2 The Nonlinear and Linear Estimation Problems

Based on the power system model above, we can formulate the state estimation problem. Here, the system measurements are expressed by the m-dimensional vector z, and the state variables by the $(2N - 1)$-dimensional vector x where one bus is taken as the phase angle reference. The overall system can be presented as

$$z = h(x) + e, \tag{2.8}$$

where $h(x)$ represents the set of equations (2.4) to (2.7) and e is an m-dimensional vector containing the measurement errors, which are assumed to follow the normal distribution with zero mean and covariance matrix R, i.e., $e \sim \mathcal{N}(0, R)$. Voltage magnitude measurements are also typically included in (2.8).

Since the power flow equations are nonlinear, determining the state of the power system is a nonlinear estimation problem. This is typically solved as a series of linearized problems by expanding (2.8) using a first-order Taylor series. Each step of the series is then expressed as

$$\Delta z = H(x)\Delta x, \tag{2.9}$$

where $H(x)$ is the measurement Jacobian matrix.

A standard simplification to (2.9) is called the decoupled model. The use of this model will be made in later sections; so it is now briefly described. The Jacobian matrix associated with the real and reactive power measurements can be partitioned into four submatrices as follows:

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} H_{P\theta} & H_{PV} \\ H_{Q\theta} & H_{QV} \end{bmatrix} \begin{bmatrix} \Delta\theta \\ \Delta V \end{bmatrix} \tag{2.10}$$

2.1.3 The Jacobian Matrix

Now we provide the details of the measurement Jacobian matrix H. Its structure is given as follows:

$$H = \begin{bmatrix} \frac{\partial P_{inj}}{\partial \theta} & \frac{\partial P_{inj}}{\partial V} \\ \frac{\partial P_{flow}}{\partial \theta} & \frac{\partial P_{flow}}{\partial V} \\ \frac{\partial Q_{inj}}{\partial \theta} & \frac{\partial Q_{inj}}{\partial V} \\ \frac{\partial Q_{flow}}{\partial \theta} & \frac{\partial Q_{flow}}{\partial V} \\ \frac{\partial I_{mag}}{\partial \theta} & \frac{\partial I_{mag}}{\partial V} \\ 0 & \frac{\partial V_{mag}}{\partial V} \end{bmatrix}. \tag{2.11}$$

The expressions for each partition are given below:

1. Elements corresponding to real power injection measurements:

$$\begin{aligned} \frac{\partial P_i}{\partial \theta_i} &= \sum_{j=1}^{N} V_i V_j \left(-G_{ij}\sin\theta_{ij} + B_{ij}\cos\theta_{ij}\right) - V_i^2 B_{ii} \\ \frac{\partial P_i}{\partial \theta_j} &= V_i V_j \left(G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}\right) \\ \frac{\partial P_i}{\partial V_i} &= \sum_{j=1}^{N} V_j \left(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}\right) + V_i G_{ii} \\ \frac{\partial P_i}{\partial V_j} &= V_i \left(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}\right) \end{aligned} \tag{2.12}$$

2. Elements corresponding to reactive power injection measurements:

$$
\begin{aligned}
\frac{\partial Q_i}{\partial \theta} &= \sum^{N} V_i V_j \left(G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij} \right) - V_i^2 G_{ii} \\
\frac{\partial Q_i}{\partial \theta_j} &= V_i V_j \left(-G_{ij} \cos \theta_{ij} - B_{ij} \sin \theta_{ij} \right) \\
\frac{\partial Q_i}{\partial V_i} &= \sum_{j=1}^{N} V_j \left(G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij} \right) - V_i B_{ii} \\
\frac{\partial Q_i}{\partial V_j} &= V_i \left(G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij} \right)
\end{aligned}
\tag{2.13}
$$

3. Elements corresponding to real power flow measurements:

$$
\frac{\partial V_i}{\partial V_i} = 1, \frac{\partial V_i}{\partial V_j} = 0, \frac{\partial V_i}{\partial \theta_i} = 0, \frac{\partial V_i}{\partial \theta_j} = 0 \tag{2.14}
$$

4. Elements corresponding to current magnitude measurements (ignoring the shunt admittance of the branch):

$$
\begin{aligned}
\frac{\partial I_{ij}}{\partial \theta_i} &= \frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} V_i V_j \sin \theta_{ij} \\
\frac{\partial I_{ij}}{\partial \theta_j} &= -\frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} V_i V_j \sin \theta_{ij} \\
\frac{\partial I_{ij}}{\partial V_i} &= \frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} \left(V_i - V_j \cos \theta_{ij} \right) \\
\frac{\partial I_{ij}}{\partial V_j} &= \frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} \left(V_j - V_i \cos \theta_{ij} \right)
\end{aligned}
\tag{2.15}
$$

2.2 The Weighted Least Squares Estimator

The weighted least squares estimator (WLS) forms the basis for most power system state estimator. First utilized for power system state estimation by Schweppe [74] in 1970, the WLS estimates the system state by minimizing the sum of the squared residuals. In matrix form, it is written as

$$\min_{x} J(x) = [z - h(x)]^T \left[R^{-1}\right] [z - h(x)], \tag{2.16}$$

where R denotes the $(m \times m)$ covariance matrix of measurement errors, assumed to be independent, and is equal to

$$R = \begin{bmatrix} \sigma_1^2 & & 0 \\ & \ddots & \\ 0 & & \sigma_m^2 \end{bmatrix}. \tag{2.17}$$

To execute the state estimation in real time, a simplified model based on linearization is commonly used [4].

The optimal estimate of the state can be computed by the iterations as

$$\hat{x}^{k+1} = \hat{x}^k + \Delta x^k, \tag{2.18}$$

where

$$\Delta x^k = \left[H^T R^{-1} H^T\right]^{-1} H^T R^{-1} \big(z - h(\hat{x}^k)\big), \tag{2.19}$$

and k is the index of the iteration. The matrix H is the Jacobian of the measurement function $h(\cdot)$ with respect to the state x. The state increment Δx^k is obtained by regressing $\big(z - h(\hat{x}^k)\big)$ on H. The algorithm terminates once the norm of Δx^k becomes smaller than a given threshold. Afterwards, bad data detection (BDD) is applied.

2.3 Bad Data Detection

The BDD module is essential to protect state estimation from effects of the outlier. The measurement data is checked to remove any abnormal values. After the state estimation process converges, the residuals are calculated as

$$r^k = z - h(\hat{x}^k). \tag{2.20}$$

If any entries of r^k are large in magnitude, the corresponding measurements are eliminated, and the SE is re-executed with the remaining data. The estimation and BDD are re-iterated until such large residuals do not appear.

The largest normalized residual (LNR) is employed in practice to remove bad measurements [4]. The LNR is based on computing the normalized residuals obtained from

$$r_i^N = \frac{|r_i|}{\sqrt{S_{ii}R_{ii}}}, \tag{2.21}$$

where r_i is the ith element of the residual r and S is the residual sensitivity matrix given by

$$S = I - H(H^T H)^{-1} H^T. \tag{2.22}$$

If the largest normalized residual is larger than a pre-determined threshold, e.g., $|r_i^N| > 3$, it is eliminated from the measurements in the next state estimation. The estimation is re-executed until no outlier is detected.

However, it is emphasized that in the presence of attacks, the WLS is not reliable, and analyzing its residuals as implemented in classical BDDs such as LNR does not guarantee their detection. In fact, even one leverage point can go without detection and thus can greatly affect the estimation performance. The

LNR was also shown to suffer from smearing effects when multiple gross errors are present. For more on the vulnerability of the LNR, see, e.g., [90].

2.4 Model of False Data Injection Attacks

The BDD is designed assuming that the outliers occur randomly. It is known to be vulnerable to outliers that are coordinated, which can be generated by malicious attackers. Here, we outline the class of attacks considered in this thesis.

The attacker is assumed to be capable of launching FDI attacks on SE inputs corresponding to a limited number of buses, including the measurement, topology, and parameter data. We consider the more adversarial scenario where the attacker has the information about elements in the regressor matrix H. In such a case, the following two classes of attacks are particularly effective:

(i) One consists of those against the measurements. The attacker may generate stealthy attacks of the form

$$z_c = z + Hc, \tag{2.23}$$

where c is a sparse vector with nonzero values at entries corresponding to the targeted buses [57]. The attack is stealthy in the sense that the residuals are not modified, and conventional detection schemes based on analyzing the residuals cannot detect the attacks.

(ii) The other consists of those against the regressor matrix. Such attacks are called leverage point attacks [59; 80], and the matrix is modified in the form

$$H_c = H + \delta H, \tag{2.24}$$

where δH contains nonzero columns corresponding to the targeted buses. If a column in H is multiplied by a chosen scalar in an attack, the attack will control the corresponding state, and the residuals will be kept unchanged. The attack becomes stealthy, and the estimated state will be manipulated and becomes the corrupted value targeted by the attacker. To generate such attacks, the attacker needs access to the line connections, parameters, and sensors adjacent to the targeted buses.

2.5 Robust State Estimation

Robust estimation theory provides a more secure alternative and has been considered for the detection of FDI attacks in the literature [16; 17; 18; 24; 59; 63; 83; 92]. Robust techniques can generate state estimates that are optimal beyond the strict assumptions of parametric models [61; 95]. This allows the data to depart from the exact parametric model while the estimators exploit the certain number of the measurements and resist a minority of outliers and cyber-attacks. Robust estimators are designed to reduce the influence of bad data on state estimation. One key feature of such estimators is to reduce the weights given to bad data. This is in contrast to the WLS, where large residuals have more influence on the objective function.

In this section, we summarize three robust estimators that we use in our simulation studies later. Here, the covariance matrix is taken to be $R = I$ without loss of generality.

2.5.1 Least Absolute Value (LAV)

This method minimizes the sum of the absolute values of the residuals:

$$J(x) = \sum_{i=1}^{m} |r_i|. \tag{2.25}$$

In the presence of leverage points (the outliers introduced in the Jacobian matrix H), however, the bad data rejection capability of the LAV estimator is known to be ineffective [4]. The state could be calculated using the dual-simplex algorithm [68].

2.5.2 Huber M-estimation

To reduce the influence of large residuals, the objective function for this method is chosen as a quadratic function and for small residuals as a linear function, i.e., it is quadratic-linear. More specifically, the Huber M-estimation minimizes the function

$$J(x) = \sum_{i=1}^{m} \rho(r_i), \tag{2.26}$$

where

$$\rho(r_i) = \begin{cases} \frac{r_i^2}{2} & \text{if } |r_i| \leq a, \\ a\big(|r_i| - \frac{a}{2}\big) & \text{otherwise.} \end{cases} \tag{2.27}$$

Note that this estimator is a generalization of WLS and LAV as these two methods can be obtained by changing the threshold parameter a. The state could be calculated using the iterative re-weighted least-squares algorithm (IRLS) [61].

2.5.3 Least Trimmed Squares (LTS)

In this thesis, among the robust methods, we mainly focus on the LTS estimator. It minimizes a trimmed percentage of the regression squared residuals [61]. We use the notation $\underline{r}$ to express the sorted version of the residual r in its entries from the smallest to the largest in magnitude as $\underline{r}_1^2 \leq \underline{r}_2^2 \leq \cdots \leq \underline{r}_m^2$. Then, the

LTS finds the estimate x that minimizes the cost function

$$J(x) = \sum_{i=1}^{m_T} \underline{r}_i^2, \tag{2.28}$$

where

$$m_T = \lfloor (1 - \alpha) m \rfloor + 1, \tag{2.29}$$

is the number of measurements used after trimming, α corresponds to the trimming fraction, and $\lfloor \cdot \rfloor$ is the floor function.

For any of these estimators, their capability when FDI attacks are present in the measurements and topology data can be represented by their (finite-sample) breakdown points [61]. This is the maximum fraction of outliers in the measurements that the estimator can resist while offering reliable estimates before breaking down. The LTS is known to be one of the most robust methods and, specifically, its maximum breakdown point can be expressed as

$$\epsilon_{\max,m} = \frac{1}{m} \left\lfloor \frac{s^*}{2} \right\rfloor, \tag{2.30}$$

where s^* is the minimum number of measurements whose removal makes at least one measurement critical for performing state estimation [24]. The challenging part for its calculation in the case of power systems is that when the system is large, the computation of s^* can be expensive as it involves combinatorial aspects. One solution to address this is decomposing the system into small islands, which we explain in the next chapter.

Chapter 3

Decomposition-Based State Estimation and Attack Detection

In this chapter, our focus is on developing an algorithm for automatically finding islands and updating the decomposition data in real-time in a computationally efficient manner whenever the topologies change. We first propose our criteria for decomposition, which is suitable for robust state estimation. Then we discuss how to use LTS with decomposition to improve cyber security. In the last part of this chapter, we propose our algorithm and introduce a few graph-related notions. The material of this chapter is based on [7].

3.1 Necessity for Decomposition

Our robust estimation approach is motivated by the study of [17; 24], where the power system is decomposed into subsystems, or islands, for increasing the number of outliers that can be tolerated. It is emphasized that decomposition allows the execution of the least trimmed squares estimator (LTS) on subsystems while ensuring the observability of the whole system. In particular, there are two main advantages of this approach as follows:

- **Increased outlier identification capability**

  In the power system, we might encounter buses with a low number of measurements and connections, which would impose a constraint on the breakdown point for the entire system. To keep the influence of such buses limited, it is effective to decompose the grid into several islands [7; 16; 24; 63]. In particular, finding small cycles is important for raising the cyber-security level of state estimation [7]. This is because the breakdown points for smaller islands are in general higher than those for larger islands.

- **Decreased computing time**

  For reducing the computation time, the state estimation in each island could be done in parallel. In addition, for smaller systems, the computation for estimation takes shorter time.

3.2 Cyber Security Criteria for Decomposing the System

Since the grid topology is very sparse in general, there could be a bus with a low number of measurements and connections. Such measurements with low redundancy would impose a constraint on the breakdown point for the state estimation of the entire system. Our approach is to decompose the system into several subsystems, or islands, and then apply robust estimators, following the methods proposed in [16; 24]. In this chapter, we provide the procedure of this approach.

Islands can be distinguished into two types, radial and cyclic. As illustrated in Fig. 3.1, a radial island is given by a subset of buses and related measure-

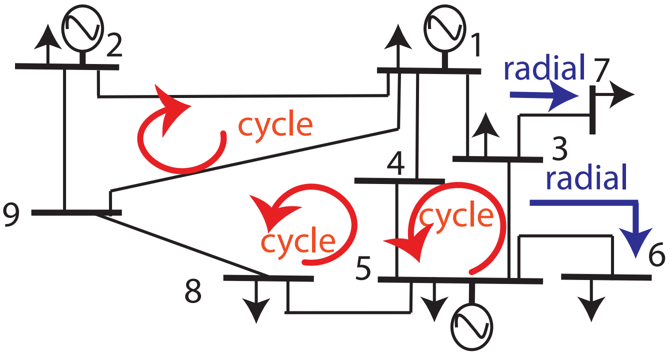


Figure 3.1: Radial and cycle islands in a sample power system.

ments between lines such that if one line is cut, the system is disconnected. An island is cyclic if it is not radial; such an island contains at least one loop. After decomposition, we can find the breakdown point for each island, and select different trimming percentages for the LTS depending on the available measurement redundancy available at each island.

When decomposing the system, it is important to keep the number of nodes in each island to be small. Such a decomposition would augment the number of outliers detected by the estimation, increasing the global breakdown point and moreover reducing the computation time when the estimators for the islands are executed in parallel. These advantages will be shown through simulations in Chapter 4.

3.3 General Approach: LTS with Decomposition

We first decompose the power system into radial and cyclic islands. Then for estimating the state at each island, injections at buses connected to adjacent islands are corrected by subtracting the power flows with neighboring islands.

In Fig. 3.1, for example the sets of buses $\{5, 6\}$ and $\{1, 3, 4, 5\}$ are radial and cyclic islands, respectively. For this cyclic island, the measurements are the power flows $P_{1,3}, P_{3,1}, P_{1,4}, P_{4,1}, P_{4,5}, P_{5,4}, P_{5,3}, P_{3,5}$ and the power injections $P_1^n, P_3^n, P_4^n, P_5^n$. For each island, the corrected power injections are computed after removing the power flows from cut-lines, i.e, $P_5^n = P_5 - P_{5,8} - P_{5,7} - P_{5,6}$ and $P_1^n = P_1 - P_{1,2} - P_{1,9}$. The covariances are adapted as well, e.g., $\sigma^2_{5_{\text{New}}} = \sigma_5^2 + \sigma_{5,8}^2 + \sigma_{5,7}^2 + \sigma_{5,6}^2$ and $\sigma^2_{1_{\text{New}}} = \sigma_1^2 + \sigma_{1,2}^2 + \sigma_{1,9}^2$.

The kth iteration state update $\delta x_i^k \in \mathbb{R}^{n_i}$ is obtained by regressing $\widehat{r}_i^k = z^{(i)} - h(\widehat{x}_i^k)$ on the matrix $H^{(i)}$ reflecting the topology of the ith island. It can be obtained from

$$\delta x_i^k = \arg\min_{\delta x} \sum_{j=1}^{\lfloor(1-\alpha_i)m_i\rfloor+1} \left(\underline{\widetilde{r}}_j^{(i)}(\delta x)\right)^2 \tag{3.1}$$

where $\widetilde{r}^{(i)}(\delta x) = \widehat{r}_i^k(j) - H_j^{(i)}\delta x$, $H^{(i)}$ is the regressor matrix corresponding to the ith island, $H_j^{(i)}$ is its jth row, m_i is the number of available measurements, and $\alpha_i \in (0,1)$ is the trimming percentage. Note that the notation $\underline{\widetilde{r}}_j^{(i)}(\delta x)$ in (3.1) indicates that its entries are the sorted version of $\widetilde{r}_j^{(i)}(\delta x)$ (similarly to $\underline{r}$ in (2.29)). Then, the residuals $|\widehat{r}_i^k(j) - H_j^{(i)}\delta x_i^k|$ larger than a given threshold τ are rejected. Finally, we detect the positions of the outliers in the ith island and store them. Hence, through this procedure, in each iteration, the state is estimated based on LTS, but among the resulting residuals, only those with large values are rejected. The number of detected outliers may be smaller than that determined by the trimming percentage.

The regression is re-evaluated by computing Δx_i^k to improve the efficiency after disregarding the detected outliers as

$$\Delta x_i^k = \arg\min_{\Delta x} \sum_{i=1}^{m_i^{\text{clean}}} \left(\widehat{r}_{i,\text{clean}}^k(j) - H_j^{(i,\text{clean})}\Delta x\right)^2, \tag{3.2}$$

where $m_i^{\text{clean}} = m_i - n_{\text{outlier}}^k$ and n_{outlier}^k is the number of detected outliers at the kth iteration. Removing the elements corresponding to outliers in $\widehat{r}_i^k$ gives $\widehat{r}_{i,\text{clean}}^k$. The state $\widehat{x}_i^{k+1}$ and residual $\widehat{r}_i^{k+1}$ are updated. The iterations are stopped once we have $\left\|\Delta x_i^k\right\| < \gamma$ with a small $\gamma > 0$. The set containing the detected outliers at the ith island is denoted by $\mathcal{J}_i = \cup_k \mathcal{J}_i^k$, where $\mathcal{J}_i^k$ contains the flagged outliers at the kth iteration. Then, the set containing all detected outliers in the system is obtained by $\mathcal{J} = \cup_i \mathcal{J}_i$.

Finally, the state estimate is performed for the entire system after removing all entries in the measurement and regressor matrix data corresponding to the detected outliers in $\mathcal{J}$ [16]. In this way, the accuracy level in estimation can be ensured while the computation load is limited as the WLS is simply run once. Note however that depending on the number and the specific entries of the outliers, the estimation at this stage may encounter problems due to lack of observability.

So far in our approach, the detected outliers by the LTS were removed. Another possible approach could be to correct those flagged measurements or leverage points which could enhance the observability of the system. The correction could be achieved by existing estimation algorithms such as an augmented state estimation for parameter correction [88] or exploiting past measurements and forecast a correction for isolated attacked measurements [11]. This is an interesting research direction to investigate in the future.

3.4 Detection of Cyclic Islands

In this section, we address the problem to decompose a given power system into islands and, in particular, to find cyclic islands. For a power system, the topology representing its power line structure may change over time. This can be due to opening and closing of lines for maintenance purposes or during the operation after faults or remedial action schemes. Since such a system may be large scale, for robust state estimation, it is important to develop automatic algorithms for decomposing it into islands with certain properties.

Here, we introduce a few graph related notions [30]. We treat the given power system as the undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with the set $\mathcal{V}$ of nodes corresponding to buses and the set $\mathcal{E}$ of edges corresponding to power lines. An edge $\{v_i, v_j\} \in \mathcal{E}$ indicates that buses v_i and v_j are connected by one or more power lines. Next, a *cycle* is a sequence of nodes $v_1, v_2, \ldots, v_\ell$ forming a path as $\{v_i, v_{i+1}\} \in \mathcal{E}$ for $i = 1, 2, \ldots, \ell - 1$, where only the start and the end nodes coincide as $v_1 = v_n$, and otherwise $v_i \neq v_j$ for $i \neq j$.

We now draw the graph $\mathcal{G}$ on a plane and obtain its *planar embedding.* The graph is said to be *planar* if it can be drawn without any intersections of edges. A *face* is a region bounded by edges in the planar embedding. In this context, a face can be identified as the corresponding cycle whose edges bound the region; it is clearly the minimal cycle containing the region. Note that faces are cycles, but the converse does not hold. Faces include the outer, infinitely large region as well. In a planar graph, the number of faces (including the outer face), denoted by $|\mathcal{F}|$, can be calculated using Euler's formula [30]

$$|\mathcal{F}| = 2 - |\mathcal{V}| + |\mathcal{E}|\,, \tag{3.3}$$

where $|\cdot|$ denotes the cardinality of a set.

We treat cycles and faces in a graph as islands. Clearly, there is no need to identify all cycles though it is desirable to find more faces. Moreover, approaches to find faces alone are not enough since graphs representing transmission systems may not be planer [73].

In what follows, we propose a graph decomposition algorithm for finding cycle islands with features suitable for robust state estimation. To this end, we would like to find cycles with the following three properties:

(i) Each node/edge in $\mathcal{G}$ belongs to one or more islands.

(ii) The number of nodes in each island is small.

(iii) The total number of islands is small.

Finding islands with small numbers of nodes is beneficial for robust state estimation as it increases their breakdown points and, in turn, the numbers of outliers that they can resist. Hence, to this end, we will later employ a face detection algorithm. The properties (ii) and (iii) above may appear contradicting since the total number of nodes is fixed. However, this is not necessarily the case since as indicated by (i), the islands may be overlapping if the system is not planar and each node/edge may belong to multiple islands. Hence, the problem is combinatorial and thus can be computationally intensive.

Typically, algorithms for finding cycles are based on those for finding spanning trees in a graph. For example, one may employ the depth-first search (DFS) [27; 81] and the minimum spanning tree (MST) search [27; 39]. While these methods are simple, they are based on blind search and thus are hard to direct, e.g., for finding small cycles. We will see later in simulations that these methods can result in detecting too many islands and include those that tend to be large.

In the MST method, for the given graph $\mathcal{G}$, we first find a set of edges $\mathcal{T} \subset \mathcal{E}$ forming a spanning tree. Then, by adding an edge that is not part of the spanning tree, we can find a cycle. A spanning tree has $|\mathcal{T}| = |\mathcal{V}| - 1$ edges. As an example, the IEEE 30-bus system has 41 edges, and any spanning tree of this system has $30 - 1 = 29$ edges. The number of edges that do not participate in the spanning tree is $41 - 29 = 12$. Thus, based on this method, we find that this system has

12 cycles and, in addition, it has 3 radial islands (in total 15 islands as shown in Table 5.6).

3.5 Proposed Cycle Detection Algorithm

The proposed algorithm is outlined in the flowchart in Fig. 3.2 and described more in detail below.

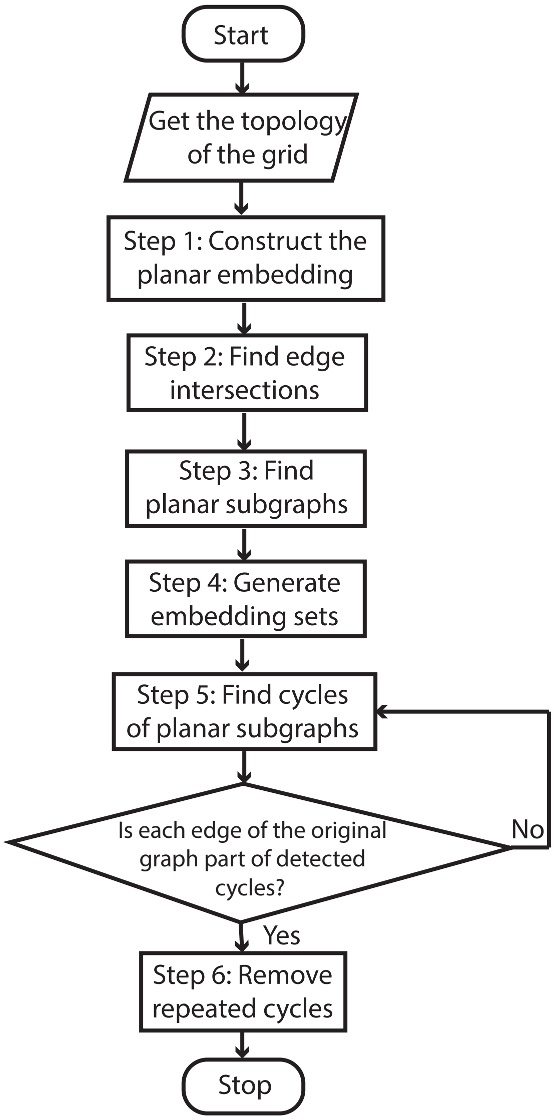

Start
Get the topology of the grid
Step 1: Construct the planar embedding
Step 2: Find edge intersections
Step 3: Find planar subgraphs
Step 4: Generate embedding sets
Step 5: Find cycles of planar subgraphs
Is each edge of the original graph part of detected cycles?
No
Yes
Step 6: Remove repeated cycles
Stop

Figure 3.2: Flowchart of the proposed cyclic island detection algorithm.

As mentioned above, the objective of our approach is to find small islands in small numbers. It thus is based on algorithms for finding faces for planer graphs [28; 73; 75]. However, power systems are in general not planar as they may have intersections in their edges. Hence, our algorithm starts with a preprocessing stage for finding planar subgraphs of the original graph.

More specifically, the algorithm can be outlined as follows: In Step 1, we find a planar embedding of the original graph. Then, in Step 2, we identify the edges intersections. Step 3 is for generating planar subgraphs by eliminating the intersections. Through Steps 4 and 5, we obtain the faces in the planar subgraphs. It terminates as soon as a sufficient number of cycles are found.

Proposed cyclic island detection algorithm

Input: Undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$

Output: Cycle islands in $\mathcal{G}$

1. (Construct the planar embedding) Determine the coordinates (x_i, y_i) of each node $i \in \mathcal{V}$ in the X-Y plane.

   (a) Use the Steady-State AC Network Visualization (STAC) [40] if $\mathcal{G}$ is given in MATPOWER format.

   (b) Remove parallel edges and radial islands.

   (c) If a subgraph is connected to the rest of the network by only one edge, remove the edge and carry out the remaining steps for the subgraphs individually. (Such an edge is present in the IEEE 300 bus system.)

2. (Find edge intersections) Find intersections of edges in the graph in the X-Y plane.

   (a) Construct the intersection matrix $S \in \{0, 1\}^{n_e \times n_e}$, where n_e is the number of edges.

(b) For each edge $e_i \in \mathcal{E}$, take edge $e_j \in \mathcal{E}$ with $i < j$ having end nodes different from those of e_i. If they intersect, then set $S(i,j) = 1$ and otherwise $S(i,j) = 0$. This matrix is upper triangular and is used for obtaining planar subgraphs of $\mathcal{G}$.

3. (Find planar subgraphs) From $\mathcal{G}$, generate a set of its planar subgraphs $\mathcal{G}^{(k)}$, $k = 1, \dots, n_p$, with $\mathcal{G}^{(k)} \neq \mathcal{G}^{(j)}$ if $k \neq j$ such that each edge of $\mathcal{G}$ is included in one or more subgraphs. The following steps are for keeping the size of n_p small.

   (a) Transform the intersection matrix S into a block-diagonal matrix by permuting its rows and columns.

   (b) Identify the diagonal blocks S_i in the intersection matrix S after the transformation.

   (c) For each block S_i in S, find a set of columns and rows such that removing them makes the remaining block zero. (By removing the edges corresponding to such columns and rows, we can eliminate all intersections in the part of the graph corresponding to the block.)

   (d) Find all such sets so that each edge remains in at least one of the sets. Let s_i be the number of such intersecting edges in block S_i.

   (e) Take one set per block for all blocks and remove the corresponding edges from the graph $\mathcal{G}$. This results in one planar subgraph. There are in total $n_p = \prod_i s_i$ such subgraphs.

4. (Generate embedding sets) For the planar subgraph $\mathcal{G}^{(k)}$ with $k = 1, \dots, n_p$, generate the embedding sets $\overline{\mathcal{E}}_i^{(k)}$ for each node $i \in \mathcal{V}$ in a clockwise manner:

   (a) Let $\overline{\mathcal{E}} \subset \mathcal{V} \times \mathcal{V}$ be the set consisting of directed edges $(i,j), (j,i)$ for each edge $\{i,j\} \in \mathcal{E}$.

(b) For node i, compute the angle of the edge $(i, j) \in \overline{\mathcal{E}}$ at node i with respect to the X-axis for each neighbor $j \in \mathcal{N}_i$ ($\mathcal{N}_i$ is the neighbor set of node i).

(c) Sort the directed edges (i, j) according to their angles in a descending order and define the ordered edge set $\overline{\mathcal{E}}_i^{(k)} \subset \overline{\mathcal{E}}$.

5. (Find faces of planar subgraphs) For each planar subgraph $\mathcal{G}^{(k)}$, $k = 1, \ldots, n_p$, find all faces (by using the planar face traversal algorithm [84]):

   (a) Take node $i_1 \in \mathcal{V}$.

   (b) Pick the first edge (i_j, i_{j+1}) in the embedding set $\overline{\mathcal{E}}_{i_j}^{(k)}$ according to the order. Then, go to node i_{j+1} and remove the edge from $\overline{\mathcal{E}}_{i_j}^{(k)}$.

   (c) Repeat Step b) until returning to the starting node i_1. At this point one face is found.

   (d) Stop if all embedding sets are empty. Otherwise, pick a node $i_1 \in \mathcal{V}$ whose embedding set is nonempty and go to Step b).

   (e) If each edge in the original graph $\mathcal{G}$ is included in one or more faces detected so far, then go to Step 6. Otherwise, go to Step b) and proceed with the next planar subgraph $\mathcal{G}^{(k+1)}$.

6. From all faces found so far, remove any that are repeated.

In what follows, we describe further details of the steps in the algorithm.

3.5.1 Planar Embedding of Power Systems

The first step in the algorithm is to construct a planar embedding of the graph $\mathcal{G}$. The planer embedding can be expressed by the coordinates (x_i, y_i) of each node $i \in \mathcal{V}$ in the X-Y plane. If a map of the system is available, such coordinates can easily be obtained. If not, we can employ graph plotting tools.

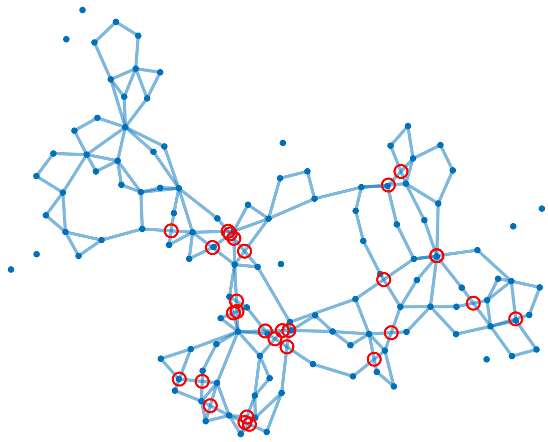


Figure 3.3: Planar embedding of the IEEE 118-bus system by the STAC.

For our proposed algorithm, we found that the graph plotting method provided by the Steady-State AC Network Visualization (STAC) [40] is suitable (also see, e.g., [85]). This tool is capable to directly take the power grid data from the MATPOWER [94] and obtain its planar embedding. Also, from the numerical software MATLAB, we can employ, for example, the *plot* function for graph objects, which is for non-planar graphs.

However, in general, the STAC performs better for larger systems in that the number of intersections is kept much smaller. For comparison, we applied these methods to the IEEE standard bus systems. For the 118, 145, and 300 bus systems, the STAC generated graphs with 29, 935, and 59 intersections, respectively; on the other hand, the MATLAB tool resulted in 50, 1205, and 129 intersections, respectively, which are much larger. Fig. 3.3 demonstrates the IEEE 118-bus system plotted by the STAC, where the red circles indicate the intersections.

3.5.2 Planar Subgraphs

In the algorithm, once the coordinates of the nodes in the planar embedding of the graph $\mathcal{G}$ are determined in Step 1, the intersections of the edges can be easily found as shown in Step 2. Then, in Step 3, we generate subgraphs $\mathcal{G}^{(k)} = (\mathcal{V}, \mathcal{E}^{(k)})$ of $\mathcal{G}$ which are planar with the edge sets satisfying $\mathcal{E}^{(k)} \subset \mathcal{E}$. These are obtained by removing some of the edges to eliminate intersections in such a way that the planar subgraphs differ from each other in their edge sets as $\mathcal{E}^{(k)} \neq \mathcal{E}^{(j)}$ if $k \neq j$ and the union of the edge sets form the original edge set as $\cup_k \mathcal{E}^{(k)} = \mathcal{E}$. Note that the intersection $\mathcal{E}^{(k)} \cap \mathcal{E}^{(j)}$ of two edge sets may be nonempty.

This may be systematically done by introducing the *intersection matrix* $S \in \{0,1\}^{n_e \times n_e}$ as follows: Here, n_e is the number of edges and S is upper triangular. First, index all edges in $\mathcal{E}$ from e_1 to e_{n_e}. We set $S(i,j) = 1$ if the two edges e_i and e_j with $i < j$ intersect with each other, and $S(i,j) = 0$ otherwise. Now, we determine the edges to be eliminated from the graph, and then remove the corresponding rows and columns from the intersection matrix S. We must remove sufficiently many edges so that after the removal of rows/edges, the remaining submatrix of S becomes 0. Then, the corresponding subgraph $\mathcal{G}^{(k)}$ becomes planar. To keep the number of subgraphs limited, we need not generate all possible subgraphs at this stage; the minimum requirement is that each edge appears at least in one subgraph.

In a)–e) of Step 3 , we outline a procedure to carry this out efficiently by first transforming the intersection matrix S into a block-diagonal matrix. Then, each diagonal block corresponds to a subset of edges that intersect with each other, but are independent of intersecting edges in other blocks. Consequently, we can systematically remove the edges according to the blocks to keep the number of islands minimal.

3.5.3 Face Detection in Planar Graphs

Finally, we must find the faces in each planar graph $\mathcal{G}^{(k)}$ of $\mathcal{G}$. In Step 4 of the algorithm, we first find orders among neighbors for the nodes in $\mathcal{G}^{(k)}$. More specifically, from the coordinates of the network, we obtain the angles between the edges for each node i. Based on these angles, we sort the edges in the clockwise order. This information will be stored in an ordered set, referred to as the *embedding set* of node i.

We introduce the notation for the embedding sets. For each planar graph $\mathcal{G}^{(k)} = (\mathcal{V}, \mathcal{E}^{(k)})$, we define its directional graph version $\overline{\mathcal{G}}^{(k)} = (\mathcal{V}, \overline{\mathcal{E}}^{(k)})$, where $\overline{\mathcal{E}}^{(k)} \subset \mathcal{V} \times \mathcal{V}$ is the set of directed edges consisting of two edges (i, j) and (j, i) for each undirected edge $\{i, j\}$ in $\mathcal{E}^{(k)}$. Now, partition $\overline{\mathcal{E}}^{(k)}$ into $\overline{\mathcal{E}}_i^{(k)}$ with $i \in \mathcal{V}$, where $\overline{\mathcal{E}}_i^{(k)} = \{(i, m) : m \in \mathcal{N}_i\} \subset \overline{\mathcal{E}}^{(k)}$ with the neighbor set $\mathcal{N}_i$ of node i. That is, we have $\overline{\mathcal{E}}^{(k)} = \cup_{i \in \mathcal{V}} \overline{\mathcal{E}}_i^{(k)}$ and $\overline{\mathcal{E}}_i^{(k)} \cap \overline{\mathcal{E}}_j^{(k)} = \emptyset$ if $i \neq j$. With some abuse of notation, each set $\overline{\mathcal{E}}_i^{(k)}$ in the partition is defined as an ordered set $\overline{\mathcal{E}}_i^{(k)} = \big((i, m_1), (i, m_2), \ldots, (i, m_{|\mathcal{N}_i|})\big)$, where the order follows that found from the coordinates of the buses above.

In our algorithm, after the embedding sets are obtained in Step 4 of algorithm, the planar face traversal algorithm [84] is applied in Step 5 to each planar graph $\mathcal{G}^{(k)}$. It essentially follows the traversing of the graph as in the DFS where at each node, the next node is chosen according to the order in the embedding set.

We explain the algorithm through an example graph in Fig. 3.4. As shown in the top of this figure, the original graph consists of four nodes and has an intersection between the edges (1,4) and (2,3). After detecting this intersection in the graph, we can obtain two planar graphs $\mathcal{G}^{(1)}$ by removing the edge (2,3) and $\mathcal{G}^{(2)}$ by removing (1,4). Next, we generate the embedding sets for the nodes in the planar graphs. In Fig. 3.4, the orders are indicated by the red arrows. For $\mathcal{G}^{(1)}$, the embedding sets are given by $\overline{\mathcal{E}}_1^{(1)} = ((1, 2), (1, 4), (1, 3))$, $\overline{\mathcal{E}}_2^{(1)} = ((2, 4), (2, 1))$,

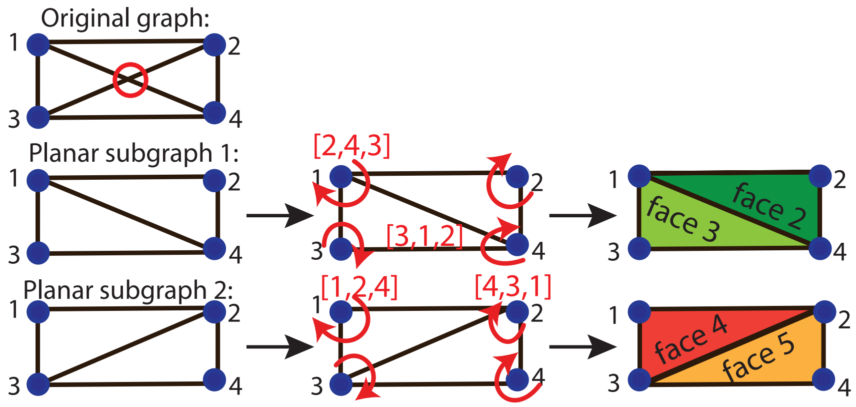


Figure 3.4: Illustration of the cycle detection algorithm.

$\overline{\mathcal{E}}_3^{(1)} = ((3,1),(3,4))$, and $\overline{\mathcal{E}}_4^{(1)} = ((4,3),(4,1),(4,2))$.

Now, the faces in $\mathcal{G}^{(1)}$ can be found by traversing the nodes. Starting from node 1, pick the edge $(1,2)$ as it is the first entry of $\overline{\mathcal{E}}_1^{(1)}$. Then, at node 2, we choose $(2,4)$ from $\overline{\mathcal{E}}_2^{(1)}$. Similarly, we go to node 4 and then node 3. This leads us back to the starting node 1. At this point, we found the face $(1,2,4,3)$, which is in fact the outer face. We remove the edges that have been selected from the nodes' embedding sets, e.g., $\overline{\mathcal{E}}_1^{(1)} = ((1,4),(1,3))$, $\overline{\mathcal{E}}_2^{(1)} = ((2,1))$, and so on. We continue this procedure until all embedding sets become empty. The process can be shown in terms of the chosen edges as follows:

$$\begin{array}{lll}
\text{Step 1: } (1,2) \to (2,4) \to (4,3) \to (3,1) & \Rightarrow & \text{Face 1: } (1,2,4,3) \\
\text{Step 2: } (1,4) \to (4,2) \to (2,1) & \Rightarrow & \text{Face 2: } (1,4,2) \\
\text{Step 3: } (1,3) \to (3,4) \to (4,1) & \Rightarrow & \text{Face 3: } (1,3,4)
\end{array}$$

We remove the face $(1,2,4,3)$ from the list since it is the union of the remaining faces, indicating that it is the outer face. Hence, we obtain the two faces (1,4,2) and (1,3,4). Then, we repeat this procedure for the second planar graph $\mathcal{G}^{(2)}$ and obtain the two faces (1,3,2) and (2,3,4).

Note that for the LTS to detect outliers in the measurements, it is enough that each edge appears at least in one cycle. Thus, the traversal procedure explained above can be terminated, e.g., if all edges which are part of cycles (i.e., not those in radial islands) are visited once (Steps 6 and 7). However, from the security viewpoint, there is a tradeoff between the number of islands and the chance of detecting attacked measurements. We show through simulations that favorable results can be obtained by looking for faces in subgraphs and then removing the repeating ones.

Chapter 4

Analysis of the Decomposition-Based State Estimation

In this section, we examine the effectiveness of the proposed approach through extensive simulations. To highlight the advantages of our proposed method, this section is divided into three parts. First, the proposed decomposition method is used to find cycles in the IEEE bus systems. In the second part, the proposed decomposition algorithm is compared to algorithms based on DFS and MST. In the last part, using these decompositions, we perform state estimation by implementing the LTS in the presence of FDI attacks. The material of this chapter is based on [7].

4.1 Decomposition into Islands

Here, we describe the decomposition procedure for a simple system and then show the scalability of our method.

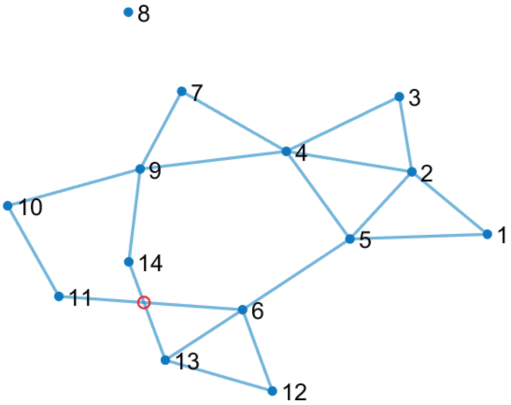
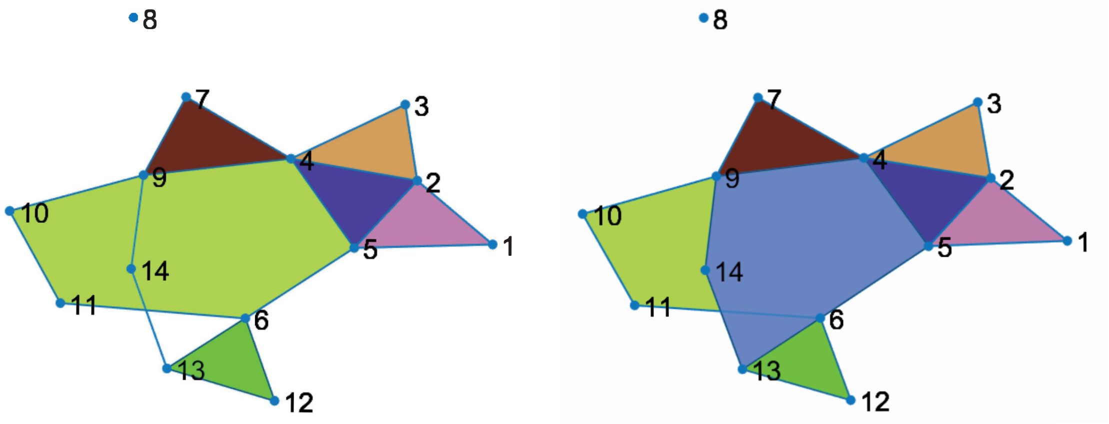


Figure 4.1: Decomposition of the IEEE 14-bus system: Original graph.

4.1.1 IEEE 14-Bus System Case

The decomposition procedure is illustrated using the IEEE 14-bus system. To this end, we first import the MATPOWER bus system from the database [94]. Then, we apply the algorithm in the previous chapter using the STAC [40], we obtain the coordinate of each bus in the grid (Step 1). Fig. 4.1 displays the result. Observe that this system has 14 vertices and 20 edges. There is one intersection marked by a red circle between edges (6,11) and (13,14) (Step 2). From this graph, we obtain two planar subgraphs $\mathcal{G}^{(1)}$ by removing the edge (13,14) and $\mathcal{G}^{(2)}$ by removing (6,11) (Step 3).

The results of cycle detection (Steps 4 and 5) are depicted in Fig. 4.2 for $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$, where the faces corresponding to cycle islands are plotted in different colors. The dot (labeled 8) indicates the bus not being part of any cycles and hence composes a radial island. From the results for $\mathcal{G}^{(1)}$, the detected cycles are (1,2,5), (2,4,5), (2,3,4), (4,5,6,11,10,9), (4,9,7), and (6,12,13). Then, from $\mathcal{G}^{(2)}$, we can find the remaining cycle (4,5,6,13,14,9). The IEEE 14-bus system is in fact planar, which can be numerically checked [41]. The discussion above using $\mathcal{G}^{(1)}$ and $\mathcal{G}^{(2)}$ is to illustrate our method. According to Euler's formula in (3.3), the number of cycles should be $2 - 14 + 20 = 8$. After removing the outer face,



(a)

(b)

Figure 4.2: Decomposition of the IEEE 14-bus system faces in the (a) first subgraph $\mathcal{G}^{(1)}$ (b) second subgraph $\mathcal{G}^{(2)}$.

we have seven cycles in total, as we found above.

4.1.2 Numerical Performance and Scalability

To confirm the scalability of the proposed decomposition algorithm for medium-to large-scale systems, we applied it to various IEEE bus systems with 14, 30, 57, 118, 145, and 300 buses. Moreover, we compared the proposed algorithm with other techniques such as the DFS- and MST-based methods discussed inprevious chapter. The results are summarized in Table 4.1. As we propose a decomposition algorithm for finding cycles with features suitable for robust state estimation, for each system, we present the following data: (i) simulation time, (ii) the number of islands, (iii) the average number of buses in each island, and (iv) the number of buses in the largest island. Moreover, for the results of the proposed approach, we show (v) the total number of blocks found in planar subgraphs in Step 3 of the proposed algorithm[1].

[1] All computation for the simulation was carried out using MATLAB on a Windows 10 64-bit operating system with Intel Core i5 processor of 2.6 GHz and 16 GB memory.

Table 4.1: Comparison of three algorithms for system decomposition. Data in each entry: (i) simulation time, (ii) the number of islands, (iii) the average number of buses in each island, (iv) the number of buses in the largest island, and (v) the number of blocks in the block-diagonal version of S.

IEEE bus systems		DFS-based	MST-based	Proposed
14 buses	(i)	0.05 sec	0.01 sec	0.05 sec
	(ii)	16 islands	8 islands	8 islands
	(iii)	7.87 buses per island	4.25 buses per island	3.62 buses per island
	(iv)	11 buses	8 buses	6 buses/1 block
30 buses	(i)	0.18 sec	0.02 sec	0.13 sec
	(ii)	68 islands	15 islands	15 islands
	(iii)	14.61 buses per island	4.26 buses per island	4.13 buses per island
	(iv)	21 buses	9 buses	8 buses/2 blocks
57 buses	(i)	7.29 sec	0.03 sec	1.24 sec
	(ii)	52584 islands	23 islands	23 islands
	(iii)	32.88 buses per island	8.95 buses per island	5.95 buses per island
	(iv)	53 buses	23 buses	15 buses/6 blocks
118 buses	(i)	–	0.06 sec	3.72 sec
	(ii)		71 islands	68 islands
	(iii)		6.49 buses per island	4.41 buses per island
	(iv)		20 buses	13 buses/22 blocks
145 buses	(i)	–	0.23 sec	63.02 sec
	(ii)		291 islands	258 islands
	(iii)		4.87 buses per island	4.07 buses per island
	(iv)		16 buses	16 buses/278 blocks
300 buses	(i)	–	0.42 sec	9.30 sec
	(ii)		197 islands	195 islands
	(iii)		5.05 buses per island	3.93 buses per island
	(iv)		32 buses	25 buses/41 blocks

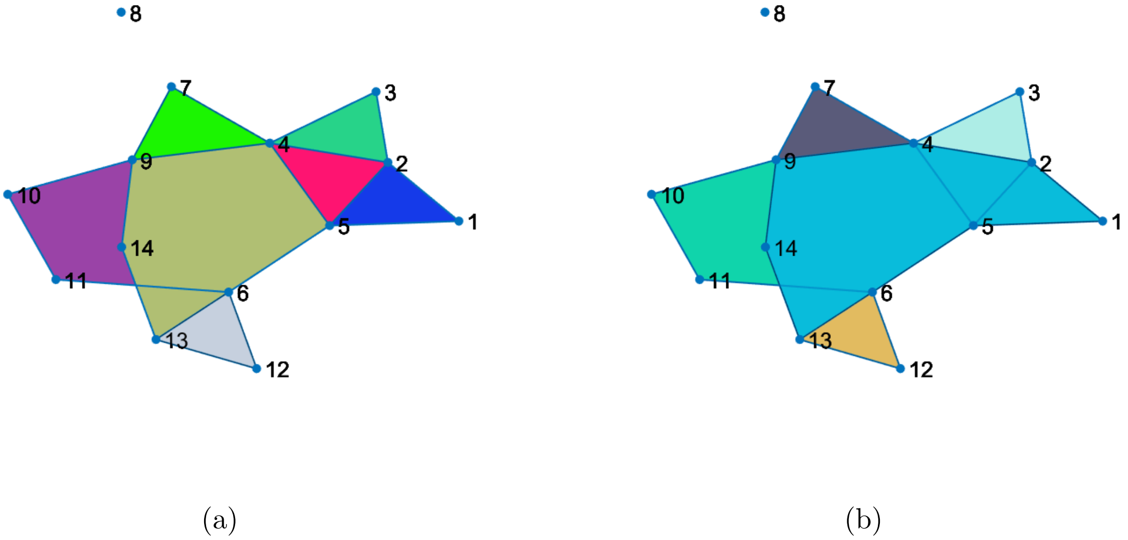
We observe that among the three methods, the proposed algorithm finds more cycles of smaller sizes. This can be seen by checking the average number of buses in each island and the number of buses in the largest island. It must be emphasized that this property was achieved by the use of face detection algorithms applied to the planar subgraphs in our algorithm. Moreover, this property is critical in the next stage of performing robust state estimation. While the MST-based [46] approach is the fastest in computation and is sometimes comparable with the proposed algorithm in other aspects, it was never better than the proposed algorithm in terms of the cycle sizes. On the other hand, the DFS solution finds many islands as expected, not being suitable for our purpose. However, we must note that the proposed method shows increase in computation time in comparison with the MST approach. This is due to its combinatorial nature in finding planar subgraphs.

For the IEEE bus systems with 14, 30, 57, 118, 145, and 300 buses, we depict the decomposition results of the proposed algorithm and the MST-based method in Figs. 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, and 4.9, respectively.

For the IEEE 118-bus system, from Fig. 4.7 and Table 4.1, we observe that the largest island found by the proposed approach consists of 13 buses. In comparison, the largest one found by the MST-based approach is the pink one with 20 buses, which in fact contains many smaller cycles.

As mentioned earlier, finding small cycles is important for raising the cyber-security levels of state estimation. This is because in robust state estimation techniques, breakdown points for smaller islands are in general higher than larger islands. Consequently, for the system as a whole, more outliers can be tolerated in the measurements in robustly performing state estimation. In this respect, the proposed algorithm is advantageous. We will further elaborate on these aspects.

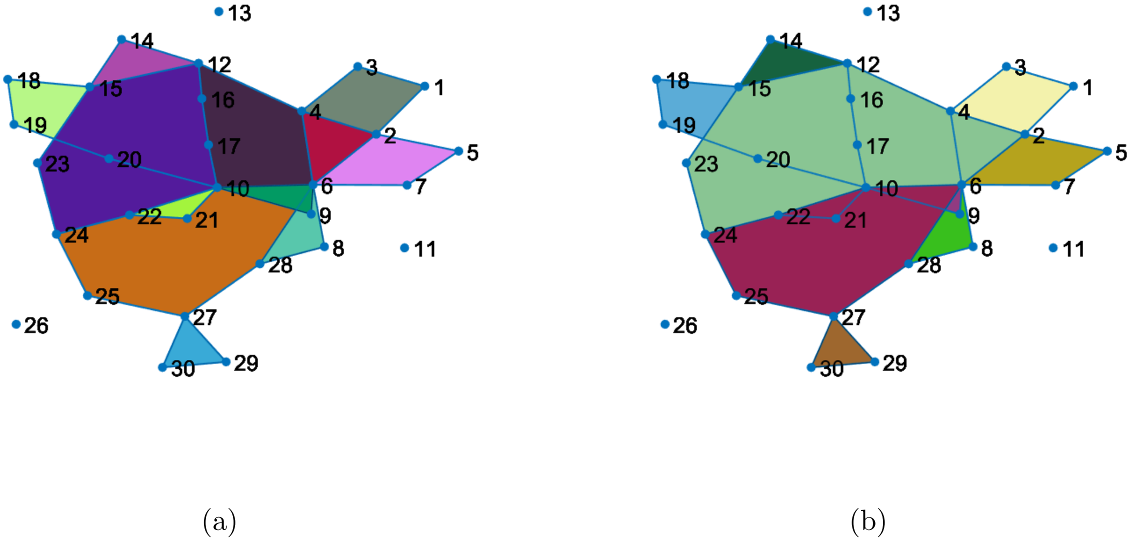
We emphasize that the maximum breakdown points of the proposed algorithm



(a)

(b)

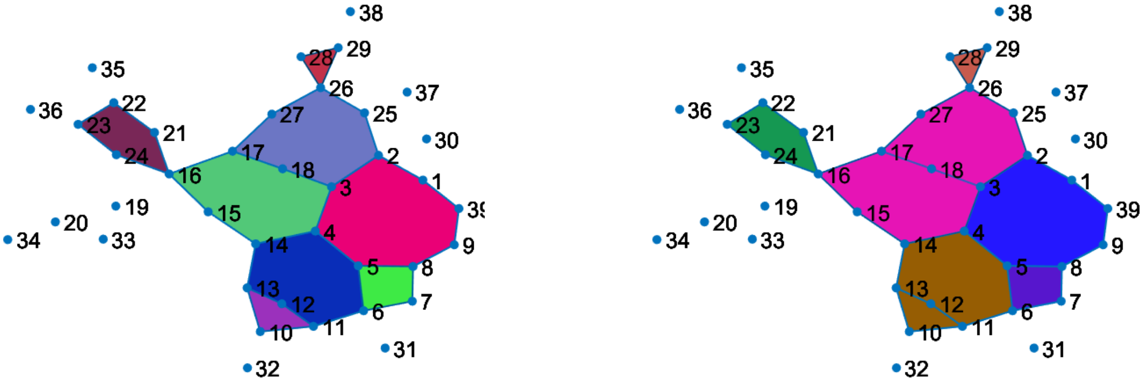
Figure 4.3: Decomposition of the IEEE 14-bus system using the (a) proposed method (b) MST method.



(a)

(b)

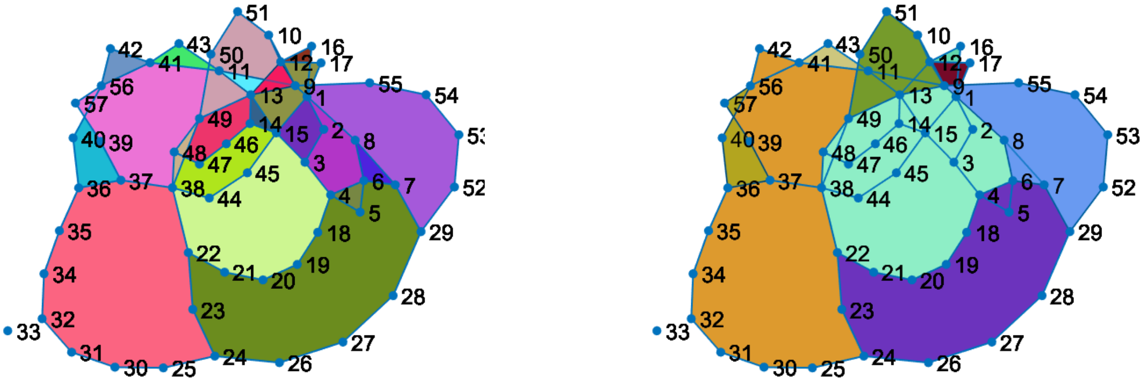
Figure 4.4: Decomposition of the IEEE 30-bus system using the (a) proposed method (b) MST method.



(a)

(b)

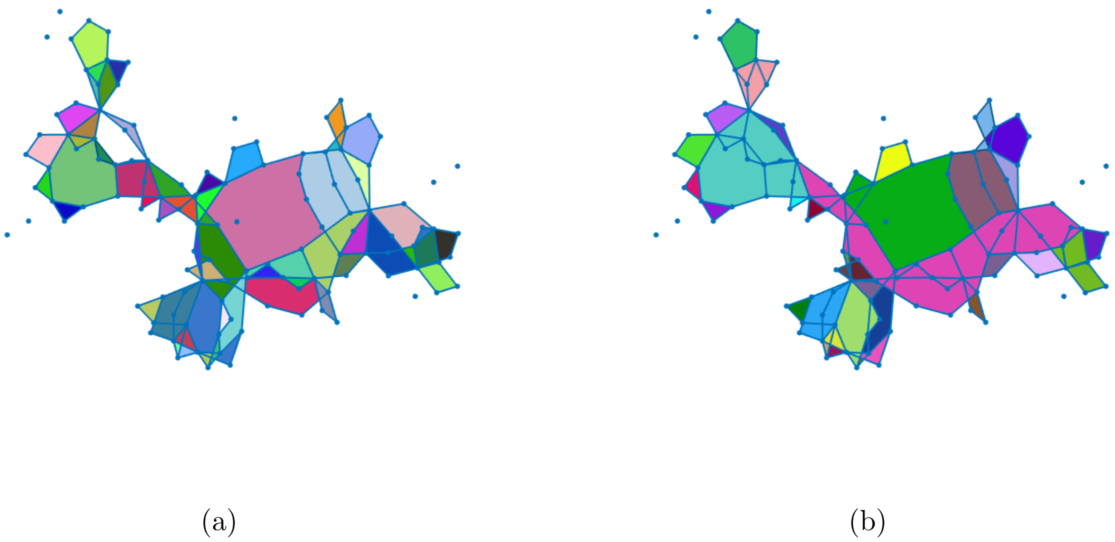
Figure 4.5: Decomposition of the IEEE 39-bus system using the (a) proposed method (b) MST method.



(a)

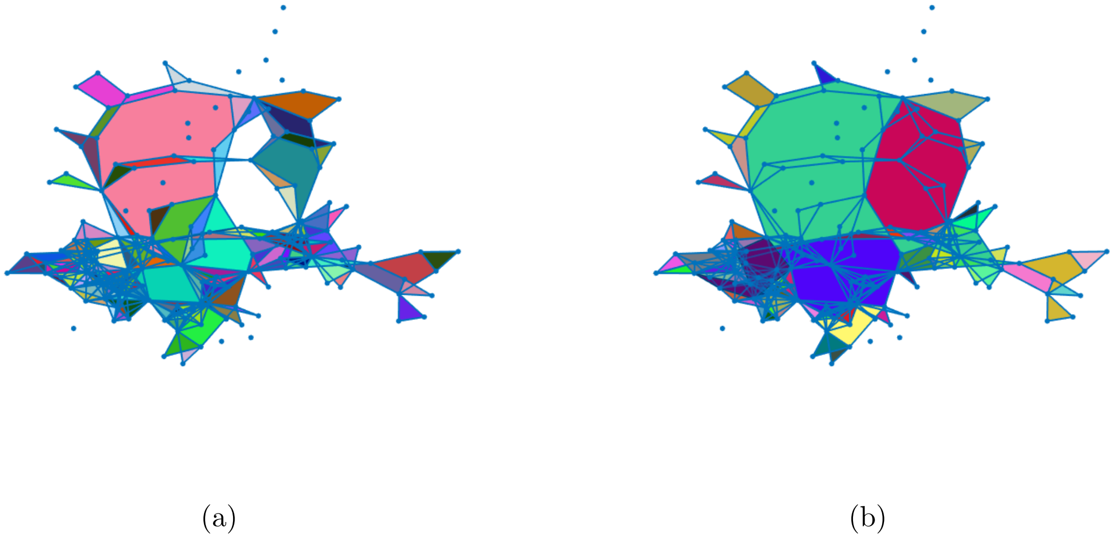
(b)

Figure 4.6: Decomposition of the IEEE 57-bus system using the (a) proposed method (b) MST method.


(a)

(b)

Figure 4.7: Decomposition of the IEEE 118-bus system using the (a) proposed method (b) MST method.


(a)

(b)

Figure 4.8: Decomposition of the IEEE 145-bus system using the (a) proposed method (b) MST method.

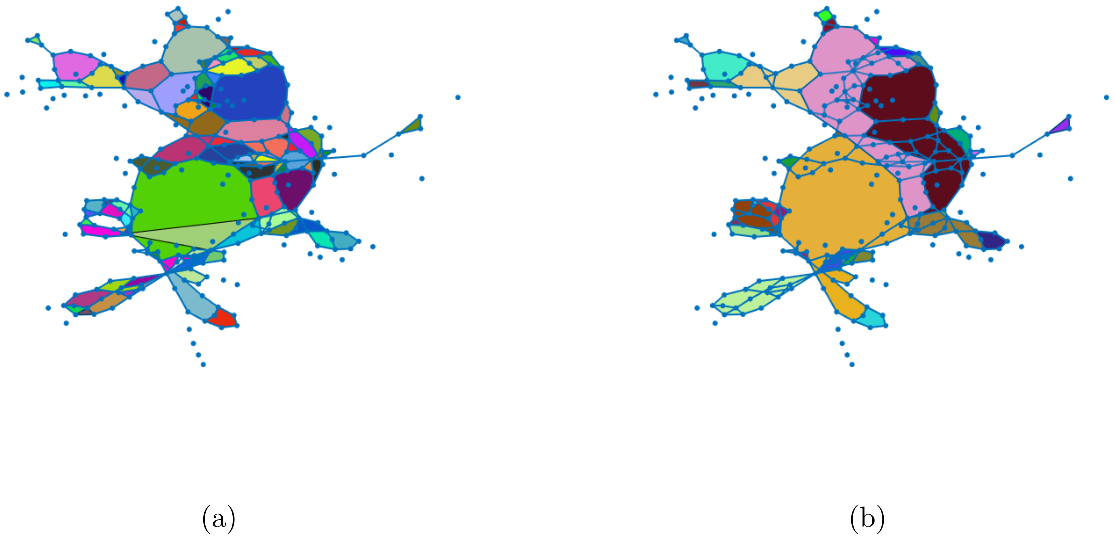


Figure 4.9: Decomposition of the IEEE 300-bus system using the (a) proposed method (b) MST method.

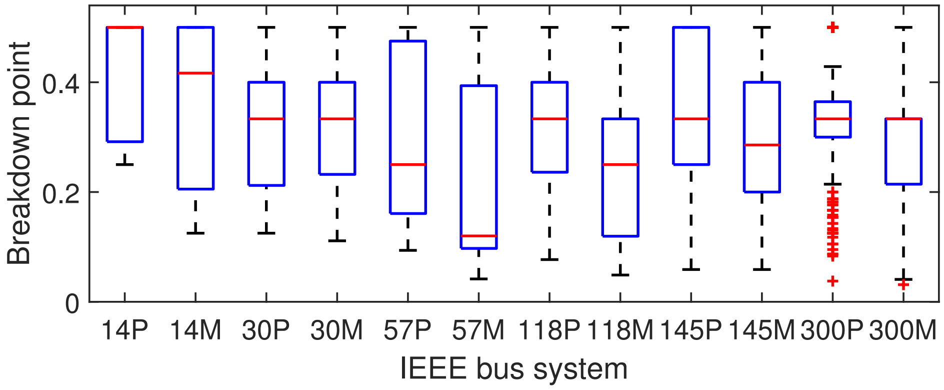


Figure 4.10: Boxplots of the breakdown points of the proposed method (P) versus the MST-based method (M) for the IEEE bus systems based on the reduced measurement configuration (see Table 4.2) for the estimation of phase angles.

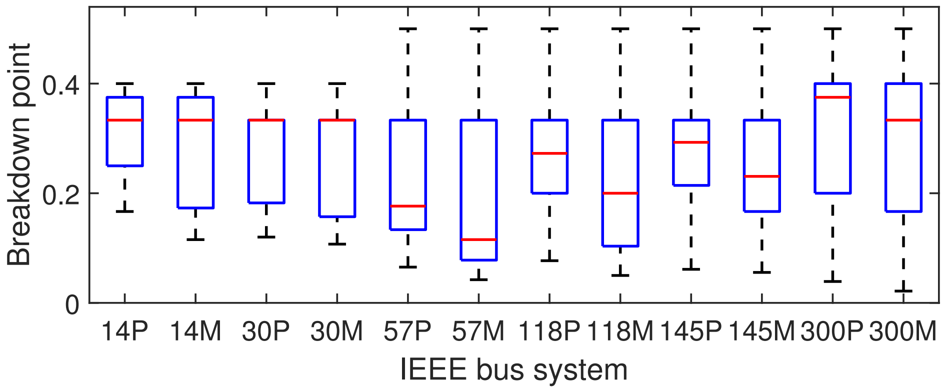


Figure 4.11: Boxplots of the breakdown points of the proposed method (P) versus the MST-based method (M) for the IEEE bus systems based on the reduced measurement configuration (see Table 4.2) for the estimation of voltage magnitudes.

are in general higher than those of the MST-based results. In Figs. 4.10 and 4.11 the theoretical maximum breakdown points of different IEEE systems are summarized for the reduced redundancy case in their measurements as presented in Table 4.2.

Here, we have decoupled the computation of the breakdown points corresponding to the estimation of phase angles in Fig. 4.10 and voltage magnitudes in Fig. 4.11. This helps to reduce the computational burden. The plots are boxplots based on the maximum breakdown points of all cycle islands for each case.

Note that real power measurements are related strongly to phase angle states and weakly to voltage magnitudes. Hence, the plot of Fig. 4.10 depicts the maximum breakdown points for the phase angle estimation obtained from real power injections and flows available at each island. Similarly, the plot of Fig. 4.11 shows the results for the voltage magnitude estimation using reactive power and voltage measurements in each island.

It must be noted that the calculation of maximum breakdown points is computationally expensive if an exhaustive search is executed to find s^*, the minimum number of measurements whose removal make at least one measurement critical for performing state estimation [24]. The challenging part for its calculation in the case of power systems is that when the system is large, the computation of s^* can be expensive as it involves combinatorial aspects. To solve this issue, one can employ the algorithm in [25] for accelerating the computation.

4.2 LTS Estimators: Simulation Setting

Now, we proceed to check the performance of the proposed algorithm using LTS for state estimation and outlier detection.

For this part, we use the IEEE 118-bus system and compare the results for two sets of measurements: one is the full redundancy case with 1098 measurements and the other is the more realistic case with 696 measurements taken from [15]. Here, we are considering adversarial environments where attackers may be targeting the power system, but the protection level of the measurements for security is assumed minimal in the sense that most of them are subject to false data injection; only those at radial subsystems are exceptional and are assumed to be safe from such attacks. Hence, the approach is to have higher redundancy in the number of measurements. It is clearly desirable to study the case with lower redundancy, and we plan to address such cases in our future works. The measurement configurations for the two cases are summarized in Table 4.2. The numbers of voltage measurements, active and reactive power injection measurements, and active and reactive power flow measurements are shown for the six IEEE bus system configurations. For the full measurement case, each bus of the system is assumed to have measurements for voltage magnitude and both active and reactive power injections; each line has measurements for two active and two reactive power flows at its ends. In these tables, we also provide the redundancy ratio, indicating the number of measurements divided by the number of state variables, as well as the number of branches in each system.

The state estimation program available in MATPOWER [94] was used and modified to introduce the LTS to the proposed approach. An algorithm for multivariate LTS estimator is provided in [6]. The program was adapted to the power systems context where the regressor matrix is sparse. High-performance computing may be applied to accelerate SSE for large power systems [23; 47] and could constitute a promising tool to speed up the execution of the proposed approach. The slack bus was considered at bus 69 where voltage magnitude was fixed to 1 p.u. and phase angle to zero. The system has been decomposed to 68 islands.

To compare the state estimation accuracy, the error in both voltage angles and magnitudes can be evaluated as follows:

$$x_I^M = \frac{1}{nM_c} \sum_{k=1}^{M_c} \left\| \widehat{x}^{[k]} - x_T \right\| , \tag{4.1}$$

where n and M_c are the numbers of buses and Monte Carlo runs, respectively. Here, we took $M_c = 100$. The state $\widehat{x}^{[k]}$ is the estimate from the kth run, and x_T is the true state (i.e., the power flow solution).

Through simulations, we analyze the detection performance of three robust methods to randomly generated outliers. Two of the robust methods are based on the LTS using graph decomposition by the proposed method and by the MST as discussed in the previous subsection. The third one is the conventional largest normalized residual method (LNR) [4], which is applied to the system without any decomposition. The outliers are introduced in the regressor matrix H (leverage points) and observation vector (observation outliers). For all the estimators including the LNR, if a residual is flagged as an outlier both its correspond-

Table 4.2: Measurement configuration for the IEEE bus systems. Results are shown in the format (reduced measurement case) / (full measurement case).

Type of measurements	14 bus	30 bus	57 bus
V_i	14 / 14	30 / 30	57 / 57
P_i	13 / 14	28 / 30	54 / 57
Q_i	13 / 14	28 / 30	54 / 57
P_{ij}	19 / 20	39 / 41	77 / 80
P_{ji}	0 / 20	0 / 41	0 / 80
Q_{ij}	19 / 20	39 / 41	77 / 80
Q_{ji}	0 / 20	0 / 41	0 / 80
Total number	78 / 122	164 / 254	319 / 491
Redundancy ratio	2.89 / 4.52	2.78 / 4.31	2.82 / 4.35
Number of branches	20	41	80

Type of measurements	118 bus	145 bus	300 bus
V_i	118 / 118	145 / 145	300 / 300
P_i	110 / 118	130 / 145	290 / 300
Q_i	110 / 118	130 / 145	290 / 300
P_{ij}	179 / 186	441 / 453	400 / 411
P_{ji}	0 / 186	0 / 453	0 / 411
Q_{ij}	179 / 186	441 / 453	400 / 411
Q_{ji}	0 / 186	0 / 453	0 / 411
Total number	696 / 1098	1287 / 2247	1680 / 2544
Redundancy ratio	2.96 / 4.67	4.45 / 7.78	2.80 / 4.25
Number of branches	186	453	411

ing measurement and row in the regressor matrix are rejected and considered as observation outlier or leverage point.

We now introduce some notations related to the performance indices. The numbers of the introduced leverage points and observation outliers are denoted by n_l and n_z, respectively; these numbers will be constant for all runs. For each run k, the number of detected leverage points truly present in the attack is denoted by $n^l_{T,k}$. Let $n^z_{T,k}$ be its observation outliers counterpart. The number of outliers detected which are neither generated leverage points nor observation outliers is $n_{F,k}$. The estimated probabilities of detection for leverage points and observation outliers are as follows:

$$P_l = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n^l_{T,k}}{n^l_{T,k}+n_{F,k}}, \quad P_z = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n^z_{T,k}}{n^z_{T,k}+n_{F,k}}. \tag{4.2}$$

The detection indices are also given by

$$d_l = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n^l_{T,k}}{n_l}, \quad d_z = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n^z_{T,k}}{n_z}. \tag{4.3}$$

The estimated probability of false detection is defined by

$$P_f = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n_{F,k}}{n^z_{T,k}+n^l_{T,k}+n_{F,k}}. \tag{4.4}$$

At each of the M_c runs, a set of quantities is randomly generated. Those are for the observation noise, the locations and magnitudes of leverage points and observation outliers. The IEEE 118-bus system has 9 radial islands, for which only 10 measurements are present; as the number is very limited, we assumed them to be free from attacks. Different scenarios of measurement redundancy are considered.

More in detail, each observation outlier is generated for a randomly chosen measurement i following a Gaussian $\mathcal{N}(8\sigma_i, \sigma_i^2)$, where σ_i is the standard deviation of the clean observation z_i. On the other hand, each leverage point is introduced by adding random elements generated from $\alpha\mathcal{U}(2, 12)$ to a randomly chosen row of H, where $\mathcal{U}$ is the uniform distribution and α is uniformly chosen as 1 or -1. The standard deviations of the SCADA measurements are 0.66% of the measured value plus a fixed value of 0.0017. The threshold τ for detecting outliers is set as 10 after some trials.

4.3 LTS Estimators: Results and Comparisons

We now present the simulation results for the three methods, where their performances are compared in terms of robust state estimation and detection of leverage points and observation outliers. In each Monte Carlo run, attacks were first determined for the entire system, affecting all islands containing the attacked portions in the measurement vectors and the regressor matrices.

We first examined the 118-bus system of moderate redundancy with 696 measurements and generated random attacks as explained above for 100 Monte Carlo simulations with 5 leverage points and 5 outlier measurements. The results for the three methods are displayed in Table 4.3 (a). In this case, all three methods remained observable. The proposed method and the MST-based method, which use LTS, performed well with relatively close values in their performance indices for detection probabilities and error norm averages. As expected, the conventional LNR, however, performed very poorly. The detection accuracy is low and the average number of measurements removed is very high. These indices show that LNR is unreliable. It is, however, interesting that the LNR performs well in the state estimation errors even under these conditions especially for voltage magnitude estimation. This could be because of to the high redundancy due to

Table 4.3: Monte Carlo SE detection probabilities and error norm averages with the proposed method, the MST-based method, and the largest normalized residual method for the IEEE 118-bus system.

(a) The more realistic case with 696 measurements under 5 leverage points and 5 output outliers.

Method	LTS Proposed	LTS MST	LNR
P_l	0.819	0.825	0.013
P_z	0.344	0.348	0.220
P_f	0.153	0.134	0.772
d_l	0.700	0.548	0.046
d_z	0.158	0.136	0.902
x_I^M(pu)	1.42×10^{-3}	1.53×10^{-3}	5.17×10^{-4}
x_I^M(deg)	0.754	0.995	1.067
# removed measurements	5.07	4.16	21.9

(b) The high redundancy case with 1098 measurements under 7 leverage points and 7 output outliers.

Method	LTS Proposed	LTS MST	LNR
P_l	0.958	0.754	0.011
P_z	0.795	0.588	0.234
P_f	0.036	0.224	0.770
d_l	0.769	0.717	0.033
d_z	0.261	0.213	0.979
x_I^M(pu)	2.15×10^{-3}	2.92×10^{-3}	4.75×10^{-4}
x_I^M(deg)	0.719	0.786	1.088
# removed measurements	9.53	11.1	31.4

the presence of voltage magnitudes at all buses of the system. Voltage magnitude measurements are not subject to leverage points since their entries are ones in the regressor matrix.

The difference between the two LTS-based methods became more evident as we increased the number of attacking points to 12 leverage points and 12 outlier measurements: In the MST-based method, LTS lost observability in some of the Monte Carlo runs and was unable to compute reliable state estimates. As discussed earlier, this occurred because the MST algorithm finds large-size islands in comparison with the proposed one. Such islands tend to have lower breakdown points, making them vulnerable to attacks, and hence become the weak points in the system. Issues with observability also occurred with the LNR. In contrast, the proposed algorithm stayed observable even under these numbers of attacks.

Next, we examined the same IEEE 118-bus system with full redundancy in the measurements. The results are shown in Table 4.3 (b). It is clear that the conventional robust technique (LNR) behaves badly. Overall, we can conclude from these results that the LTS with the proposed decomposition method provides the best detection for both outlier and leverage points. It is clearly demonstrated that the Monte Carlo average absolute errors in SE for voltage magnitudes and voltage phase angles remain smaller than the other two methods.

For comparison purpose, we ran the simulation using two conventional robust estimation methods, the M-estimator and the least absolute deviation (LAD). These methods were applied to the whole system for obtaining the estimates of voltage magnitudes and phases. Note that different from the three approaches using LTS and LNR considered so far, these methods do not detect the attacked measurements.

The average estimation performance (i.e., x_I^M) after running the simulations under the same Monte Carlo settings is the following. For the reduced measure-

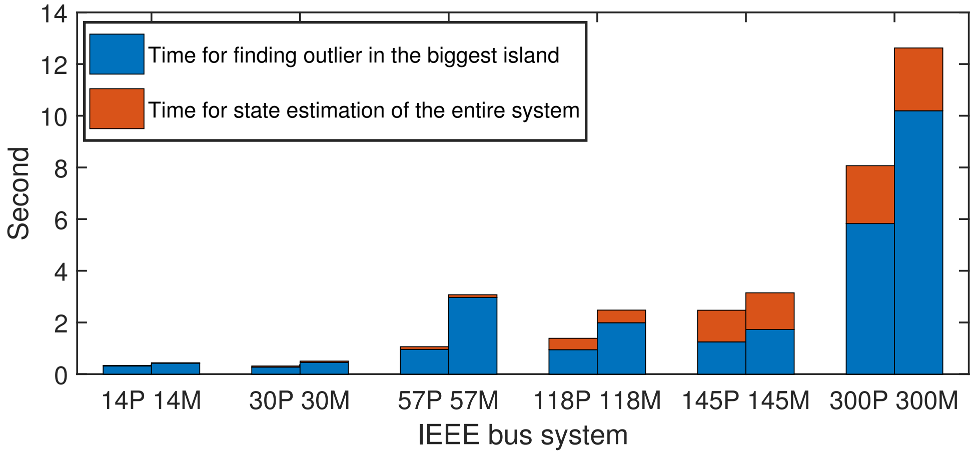


Figure 4.12: Average parallel computation times for SE: The proposed method (P) versus the MST-based method (M) for the IEEE bus systems based on the reduced measurement configuration (see Table 4.2).

ment case, the M-estimator resulted in 4.81 $\times 10^{-4}$ pu and 1.12 deg whereas the LAD yielded 1.91×10^{-3} pu and 1.06 deg. On the other hand, for the full measurement case, the M-estimator resulted in 6.19 $\times 10^{-4}$ pu and 1.04 deg whereas the LAD yielded 3.44 $\times 10^{-3}$ pu and 0.97 deg. In view of Table 4.3 (a) and (b), we observe that the estimation levels are similar to those from LNR or worse. This is due to the fact that both the M- and the LAD estimators are vulnerable to leverage points; this aspect is known in the literature [61].

Finally, we examined the average time of state estimation executed in parallel for the proposed decomposition method and the MST-based approach with LTS. Fig. 4.12 shows the average values in 100 Monte Carlo runs for the IEEE bus systems. For reducing the computation time, the state estimation in each island could be done in parallel. This figure shows the running times for the largest islands in the systems (plotted in blue) and the times for the whole state estimation after removing outliers (plotted in orange). The results indicate that the proposed decomposition algorithm is faster than the MST-based method. As the MST finds large size islands, the LTS-based state estimation takes time for those islands.

In the following chapter, we consider different FDI attack scenarios against the SE that manipulate states to a targeted value. We construct adversarial coordinated attacks against certain targeted buses in the system.

Chapter 5

Targeted Coordinated Attacks on Decomposition-Based State Estimation

In this chapter, we follow the approach of [7] and decompose the system into islands. We demonstrate the effectiveness of the robust estimation method by analyzing it against a class of coordinated attacks targeting certain buses and their adjacent buses in the system. Later, we extend our analysis to a larger-scale case with the IEEE 118-bus system. The material of this chapter is based on [8].

5.1 Three-Step SE Algorithm

To enhance robustness in static SE based on islanding and robust techniques in Chapters 3 and 4 (see also [7; 16]), we provide a modified version of the procedure. Specifically, we follow the three-step algorithm outlined as follows:

(i) As the first step, robust estimation is performed at each island. After its convergence, normalized residuals are calculated for the estimates. Then, the residuals larger than a specified threshold will be chosen as outliers and leverage points in each island.

(ii) In the second step, the corresponding outlier entries are removed from the measurement vector z and the regressor matrix H of the entire system. The SE for the entire system is then performed based on the WLS. Afterwards, the outliers and leverage points detected in the first step are put back, and we calculate the normalized residuals for the second time. The normalized residuals larger than a threshold are chosen as the final outliers and leverage points.

(iii) The third step is for ensuring the accuracy level of estimation and reducing unobservability. After removing detected outliers from the second step, we make the state estimate for the last time.

The difference from the original approach in Chapter 4 and [7; 16] lies in the second round of outlier detection and state estimate for the entire system in the second and third steps. This takes account of the chances that the residual-based outlier detections at the island level can be erroneous. To keep the number of false detections low, the choices of thresholds in these steps are important especially when the attacks are adversarial.

5.2 Targeted Coordinated Attacks on Decomposition-Based SE

5.2.1 IEEE 14-Bus System: Decomposition and Its Resiliency

In the power system, each bus is assumed to have measurements for voltage magnitude and both active and reactive power injections; each line has measurements

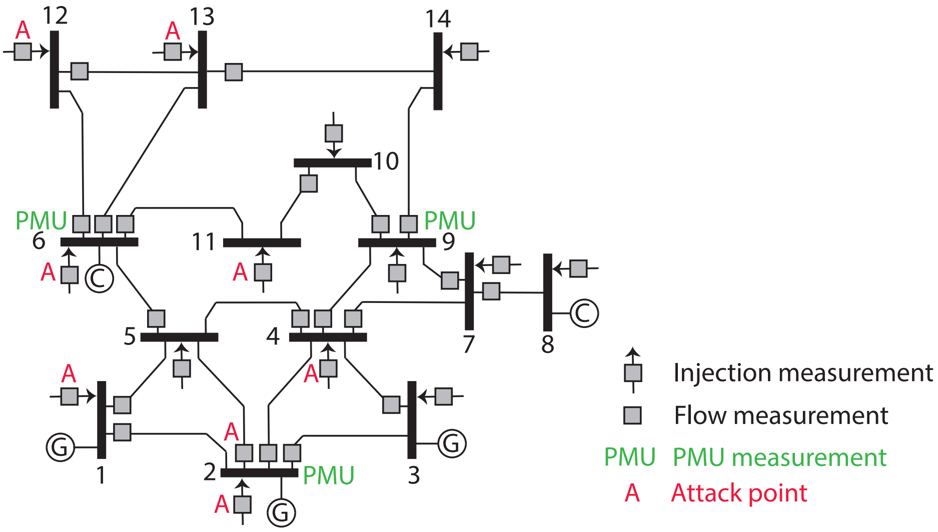


Figure 5.1: IEEE 14-bus system and the placement of measurements and attacks.

for one active and one reactive power flows at its ends. For the case of the IEEE 14-bus system, there are 27 states (excluding the phase angle of the slack bus) and 82 measurements in total.

First, we decompose the system based on the PFT-based and the MST-based methods. Table 5.1 gives the summary of the numbers of islands, the average number of buses in each island, the numbers of buses in the largest islands, and the computation times. We notice that the PFT-based method is capable to find islands of smaller sizes. The details of the decomposition are presented in Tables 5.2, 5.3, and 5.4[1]. The islands are denoted as I_i, $i = 1, \dots, 10$. Those common in both PFT- and MST-based methods are $I_1 = \{1,2,5\}$, $I_2 = \{2,3,4\}$, $I_3 = \{4,9,7\}$, and $I_4 = \{6,12,13\}$ (Table 5.2). The additional islands for the PFT-based method are $I_5 = \{2,4,5\}$, $I_6 = \{4,5,6,11,10,9\}$, and $I_7 = \{4,5,6,9,13,14\}$ (Table 5.3) while those for the MST-based method are $I_8 = \{1,2,4,5\}$, $I_9 = \{1,2,4,5,6,9,10,11\}$, and $I_{10} = \{1,2,4,5,6,9,13,14\}$ (Ta-

[1] Note that there is one radial island, $\{7,8\}$. This island is vulnerable to attacks due to the small number of measurements. Hence, it is assumed to be equipped with secure measurements and is not subject to attacks.

Table 5.1: Decomposition of the IEEE 14- and 118-bus system by two methods

	14-bus	
Decomposition method	PFT-based	MST-based
Number of islands	8	8
Average number of buses in each island	3.62	4.25
Number of buses in the largest island	6	8
Computation time (sec)	0.516	0.212
	118-bus	
Decomposition method	PFT-based	MST-based
Number of islands	68	71
Average number of buses in each island	4.41	6.49
Number of buses in the largest island	13	20
Computation time (sec)	4.36	0.09

ble 5.4). For these islands, their breakdown points for the LTS were calculated as shown in 5.2, 5.3, and 5.4. It was found that for this measurement configuration, each island can tolerate up to 2 attacks regardless of its size. This means that smaller islands have larger breakdown points, indicating the advantages of the PFT-based islands. In calculating the breakdown points, we took a decoupled approach to reduce the burden of computation. In particular, we considered only active power measurements for the phase angle estimation. It is known that reactive power and voltage magnitude measurements are only weakly linked to phase angles [4].

5.2.2 Two Classes of FDI Attacks Against the LTS

In our simulations using the LTS, in every island, we set the number of measurements discarded to be 2 in estimation against attacks. Under this setting, the LTS may produce false state estimations depending on the number of attacks and there are two scenarios:

(i) In an island, when the number of attacks is greater than the number of

Table 5.2: Islands in both methods and active power measurements linked to buses 2 and 6 in each island

	Islands in both methods			
Island indices	I_1	I_2	I_3	I_4
Buses	1,2,5	2,3,4	4,7,9	6,12,13
Breakdown point	1/3	1/3	1/3	1/3
# all active power meas.	6	6	6	6
# attacks to produce masked attacks	3	3	3	3
# attacks to produce targeted attacks	4	4	4	4
Active power measurements linked to bus 2				
P_{1-2}	1	0	0	0
P_{2-3}	0	1	0	0
P_{2-4}	0	1	0	0
$\underline{P_{2-5}}$	$\underline{\mathbf{1}}$	0	0	0
$\underline{P_1}$	$\underline{\mathbf{1}}$	0	0	0
$\underline{P_2}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$	0	0
P_3	0	1	0	0
$\underline{P_4}$	0	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$	0
P_5	1	0	0	0
Active power measurements linked to bus 6				
P_{5-6}	0	0	0	0
P_{6-11}	0	0	0	0
P_{6-12}	0	0	0	1
P_{6-13}	0	0	0	1
P_5	1	0	0	0
$\underline{P_6}$	0	0	0	$\underline{\mathbf{1}}$
$\underline{P_{11}}$	0	0	0	0
$\underline{P_{12}}$	0	0	0	$\underline{\mathbf{1}}$
$\underline{P_{13}}$	0	0	0	$\underline{\mathbf{1}}$

Table 5.3: Islands obtained from PFT-based method and active power measurements linked to buses 2 and 6 in each island

	Islands in PFT-based method		
Island indices	I_5	I_6	I_7
Buses	2,4,5	4,5,6, 9,10,11	4,5,6, 9,13,14
Breakdown point	1/3	1/6	1/6
# all active power meas.	6	12	12
# attacks to produce masked attacks	3	3	3
# attacks to produce targeted attacks	4	10	10
Active power measurements linked to bus 2			
P_{1-2}	0	0	0
P_{2-3}	0	0	0
P_{2-4}	1	0	0
$\underline{P_{2-5}}$	$\underline{\mathbf{1}}$	0	0
$\underline{P_1}$	0	0	0
$\underline{P_2}$	$\underline{\mathbf{1}}$	0	0
P_3	0	0	0
$\underline{P_4}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$
P_5	1	1	1
Active power measurements linked to bus 6			
P_{5-6}	0	1	1
P_{6-11}	0	1	0
P_{6-12}	0	0	0
P_{6-13}	0	0	1
P_5	1	1	1
$\underline{P_6}$	0	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$
$\underline{P_{11}}$	0	$\underline{\mathbf{1}}$	0
$\underline{P_{12}}$	0	0	0
$\underline{P_{13}}$	0	0	$\underline{\mathbf{1}}$

Table 5.4: Islands in MST-based method and active power measurements linked to buses 2 and 6 in each island

	Islands in MST-based method		
Island indices	I_8	I_9	I_{10}
Buses	1,2,4,5	1,2,4,5, 6,9,10,11	1,2,4,5, 6,9,13,14
Breakdown point	1/4	1/8	1/8
# all active power meas.	8	16	16
# attacks to produce masked attacks	3	3	3
# attacks to produce targeted attacks	6	14	14
Active power measurements linked to bus 2			
P_{1-2}	1	1	1
P_{2-3}	0	0	0
P_{2-4}	1	1	1
$\underline{P_{2-5}}$	0	0	0
$\underline{P_1}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$
$\underline{P_2}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$
P_3	0	0	0
$\underline{P_4}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$
P_5	1	1	1
Active power measurements linked to bus 6			
P_{5-6}	0	1	1
P_{6-11}	0	1	0
P_{6-12}	0	0	0
P_{6-13}	0	0	1
P_5	1	1	1
$\underline{P_6}$	0	$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$
$\underline{P_{11}}$	0	$\underline{\mathbf{1}}$	0
$\underline{P_{12}}$	0	0	0
$\underline{P_{13}}$	0	0	$\underline{\mathbf{1}}$

trimmed measurements (i.e., 2 in all islands), the local state estimate in that island may become inaccurate; such attacks are called *masked attacks*.

(ii) In an island, when the number of coordinated attacks is greater than or equal to the total number of measurements minus the number of trimmed measurements (given as m_T in (2.29)), the LTS might detect the remaining clean data as outlying. Such attacks can result in estimates at values chosen by the attacker, and hence can be much more harmful to the system. Such attacks are referred to as *targeted attacks* [16].

Tables 5.2, 5.3, and 5.4 indicates the number of FDIs necessary to create such attacks for each island.

5.2.3 Resilience Analysis of the Two Decomposition Methods

In the scenario considered here, the attacker aims to modify the phases of the target buses 2 and 6. Here, the attacks will be limited to FDIs against the active power injections at these buses and their neighboring buses. To this end, the attacker attempts to gain access to the active power measurements linked to these buses and then to inject false data there. In our experiment, we demonstrate the effects of attacks by gradually increasing the number of attack points, denoted by N_s, from 1 to 8. In particular, the order of the attacked buses (in their active power injections) is shown in Table 5.5. Note that when we say N_s attacks are made, measurements shown under 1 to N_s in the second row of this table will be under falsification. The attacker falsifies the measurements as well as the rows of the Jacobian matrix related to these attacked buses. By increasing the number of attacks, islands failing to generate accurate estimation will increase even by using the LTS.

At this point, we would like to discuss that when FDI attacks are launched

Table 5.5: Attacked measurements in the IEEE 14-bus system simulations

Number of attacks N_s	1	2	3	4	5	6	7	8
Measurements under falsification	P_2	P_6	P_1	P_4	P_{11}	P_{13}	P_{12}	P_5
Islands unable to estimate phase 2	–	–	–	I_8,I_9,I_{10}	I_8,I_9,I_{10}	I_8,I_9,I_{10}	I_8,I_9,I_{10}	I_1,I_5,I_8, I_9,I_{10}
Islands unable to estimate phase 6	–	–	–	–	–	–	I_4	I_4

on buses 2 and 6 and their neighbors, the islands from the PFT-based method have advantages over those from the MST-based method. To this end, we make a more careful inspection of the islands obtained from both methods. By the topology of the system shown in Fig. 5.1, we see that the two target buses have multiple neighboring buses. The neighbors of bus 2 are buses 1, 3, 4, and 5 while those of bus 6 are buses 5, 11, 12, and 13.

First, we notice that more MST-based islands contain bus 2 than the PFT-based ones, which may already indicate that attacking bus 2 can have more impact on MST-based state estimation. In fact, as shown in Tables 5.2, 5.3, and 5.4, among the seven PFT-based islands, only three of them contain bus 2. In contrast, among the seven MST-based islands, five of them have bus 2. On the other hand, the number of islands containing bus 6 are six for both decomposition cases; the attack impact for this case needs further analysis.

Second, there is a certain inclusion relation among the islands from the two methods. For example, the PFT-based island $I_5 = \{2, 4, 5\}$ is fully contained in the MST-based island $I_8 = \{1, 2, 4, 5\}$ as $I_5 \subset I_8$. Similarly, it holds $I_6 \subset I_9$ and $I_7 \subset I_{10}$. These relations indicate that in general, the impact of attacks can be greater on the MST-based islands than that on the PFT-based islands as they form a superset.

Third, among the PFT-based islands I_5, I_6, and I_7, the common buses can be found to be $I_5 \cap I_6 \cap I_7 = \{4, 5\}$ whereas among the MST-based islands I_8, I_9, and I_{10}, the common buses are $I_8 \cap I_9 \cap I_{10} = \{1, 2, 4, 5\}$. This indicates that targeting not only bus 2 but also bus 1 can be problematic in the local SE at MST-based islands. Having overlaps in the islands can create vulnerabilities because when buses contained in many islands are attacked, all of those islands can be affected in the SE performance.

Finally, among the PFT-based islands, bus 6 is contained in two islands, namely, I_6 and I_7. However, these islands do not contain bus 2. Hence, for PFT-based SE, the FDI attacks on the two target buses may have more independent effects. This is clearly different for MST-based SE, since the two islands I_9 and I_{10} contain both of the target buses 2 and 6; hence, attacking these buses may have more combined effects.

To make a more detailed analysis, from the attack pattern shown in Table 5.5, we can generate the lower part of Tables 5.2, 5.3, and 5.4, where the relations between active power measurements and their connections to islands are shown with entries 1 (linked) and 0 (not linked). Now, let's consider the case when the attacker attacks four measurements with N_4 and manipulates P_1, P_2, P_4, and P_6. From the table, we confirm that at least three of these measurements are linked to all three islands given by the MST-based method, i.e., I_8, I_9, and I_{10}. Consequently, the LTS may not be capable to make precise estimates of states or to correctly find the outliers because the number of trimmed measurements is set to 2. In Table 5.5, the third and fourth rows show the indices of the islands for which the numbers of attacks N_s exceed their breakdown points.

On the other hand, in all remaining islands, at most two measurements are linked. Islands I_1, I_2, and I_5 have three measurements linked to bus 2 which are not attacked and thus the chance of producing correct results is higher. We note that in our robust scheme, each state is estimated in multiple islands; even if some islands fail to make accurate estimation of some states, they may be recovered by other islands. This is the reason for adding the third step in our robust SE algorithm discussed in Section 5.1.

In conclusion, from the analysis and discussion so far, it is evident that the PFT-based islands should be more resilient compared to the MST-based ones in general but especially under attacks targeting certain buses. We will confirm this aspect through simulations in the next section.

5.2.4 Discussion on Detection of Random Errors and Attacks

How to distinguish between real events and FDI attacks is an important question in the context of ensuring a reliable and secure grid monitoring. Real events that can be potentially detected through our method include sensor failures, sensor noises, topology errors such as wrong states of circuit breakers and lines (open/close), and parameter errors. Sensor failures and noises occur sporadically in a limited number of sensors, mostly without much correlation. Such events can be detected by our method but may be difficult to be distinguished from attacks. If attack/failure detection continues over time at some sensors, they must be checked.

Opening lines in the system is a much more serious real event regardless of whether they are caused by faults and resulting protection actions, operator controls, or physical attacks. If one line is made open, measurements near this line will change at once. If it is a normal topology change or a fault, then the measurement changes will be consistent in the system, and this can be detected or known to the operator by other means. The proposed approach may not detect such changes by making one estimate run, partly because the least trimmed squares estimation depends on the majority of data. Moreover, under coordinated cyber-physical attacks that open a line and change all the measurements linked to this line in a consistent manner, detection would be difficult by any method using a single time snapshot. These attacks require extensive access and knowledge by the attacker and are known as stealthy attacks. These stealthy attacks could be detected, for example, by monitoring the time series in the measurements and state estimates or by securing specific sensors. For more on the subject of detection of random errors and attacks, we refer to the survey paper [67] and the references therein.

5.3 Simulation

In the simulations, we compare the performance of state estimation as well as detection of outliers in the measurement data for seven different schemes. First of all, as estimation algorithms, we employ the following four: The conventional LNR and the robust estimators using LTS, Huber M, and LAV. Four schemes are based on the robust algorithms applied to the decomposed islands obtained from the PFT- and MST-based methods; these are denoted LTS_{PFT}, LTS_{MST}, M_{PFT}, and LAV_{PST}. Further, for comparison purposes, three schemes apply the LNR, Huber M, and LAV to the entire system in a centralized fashion, without decomposition; these are denoted with the subscript C as LNR_{C}, M_{C}, and LAV_{C}.

5.3.1 Simulation Setup for the IEEE 14-Bus System

For the IEEE 14-bus system, we import the MATPOWER data from [94]. The slack bus is taken to be bus 1, whose voltage angle is fixed to zero. The error in each SCADA measurement follows the normal distribution with zero mean and standard deviation of 0.66% of the original value plus a fixed value of 0.0017. The LTS algorithm proposed in [6] is adapted to handle the sparsity in the AC SE.

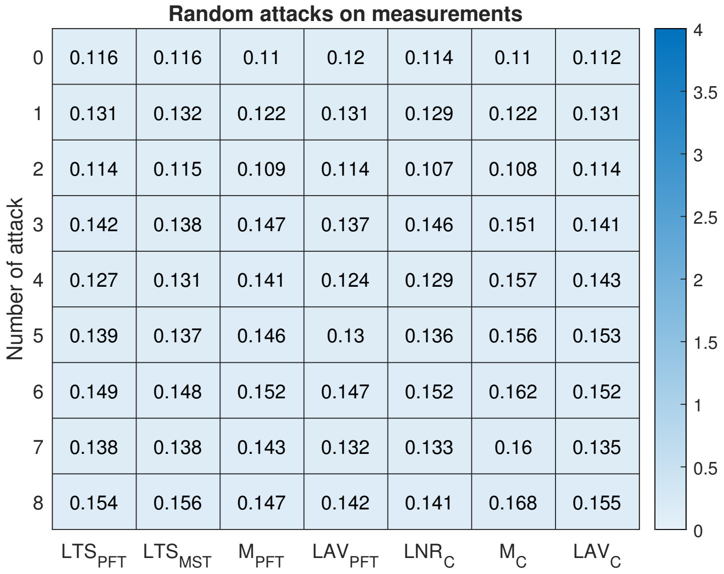
For the Huber M-estimator, the threshold parameter was taken as 1.345. For the detection of attacks, several thresholds are used. For the conventional $\mathrm{LNR}_{\mathrm{C}}$, the threshold is chosen to be 3 while for M_{C} and $\mathrm{LAV}_{\mathrm{C}}$, we have chosen the threshold to be 7. In the robust estimation schemes $\mathrm{LTS}_{\mathrm{PFT}}$, $\mathrm{LTS}_{\mathrm{MST}}$, $\mathrm{M}_{\mathrm{PFT}}$, and $\mathrm{LAV}_{\mathrm{PFT}}$, at each island, the threshold of 5 is used in the first step; then, in the second step, where we apply additional post-estimation processing to the whole system, we use the threshold of 7. These values were chosen after some trial runs so as to minimize the false alarm detection rates in the clean case (without attacks).

For each attack case, we make Monte Carlo simulations of 100 times ($M_c = 100$). To compare the estimation accuracy of the different schemes, we evaluate the average estimation error for voltage angles as $x_e = \frac{1}{n_b M_c} \sum_{k=1}^{M_c} \left\| \hat{x}^k - x_T \right\|$, where n_b is the number of buses, $\hat{x}^k$ is the estimate from the kth Monte Carlo run, and x_T is the true state (i.e., the power flow solution). As the base case under the described conditions, without any attacks, the LNR for the centralized scheme results in the average error 0.1142.

5.3.2 Attacks on Measurements

In this part, we apply two types of attacks on the measurements and compare the seven estimation schemes.

(a) First, we generate random attacks according to Table 5.5, where each attacked measurement is falsified by adding a uniformly random number between 20 to 60 percent of the original measurement value. Specifically, in the case when N_s points are attacked, the attack values are set as $\delta z_i = b_i z_i$ with $b_i \sim \mathcal{U}(0.2, 0.6)$ for $i = i_1, ..., i_{N_s}$, where i_j is the index of the jth attacked measurement in



Random attacks on measurements

Number of attack	LTS$_{PFT}$	LTS$_{MST}$	M$_{PFT}$	LAV$_{PFT}$	LNR$_{C}$	M$_{C}$	LAV$_{C}$
0	0.116	0.116	0.11	0.12	0.114	0.11	0.112
1	0.131	0.132	0.122	0.131	0.129	0.122	0.131
2	0.114	0.115	0.109	0.114	0.107	0.108	0.114
3	0.142	0.138	0.147	0.137	0.146	0.151	0.141
4	0.127	0.131	0.141	0.124	0.129	0.157	0.143
5	0.139	0.137	0.146	0.13	0.136	0.156	0.153
6	0.149	0.148	0.152	0.147	0.152	0.162	0.152
7	0.138	0.138	0.143	0.132	0.133	0.16	0.135
8	0.154	0.156	0.147	0.142	0.141	0.168	0.155

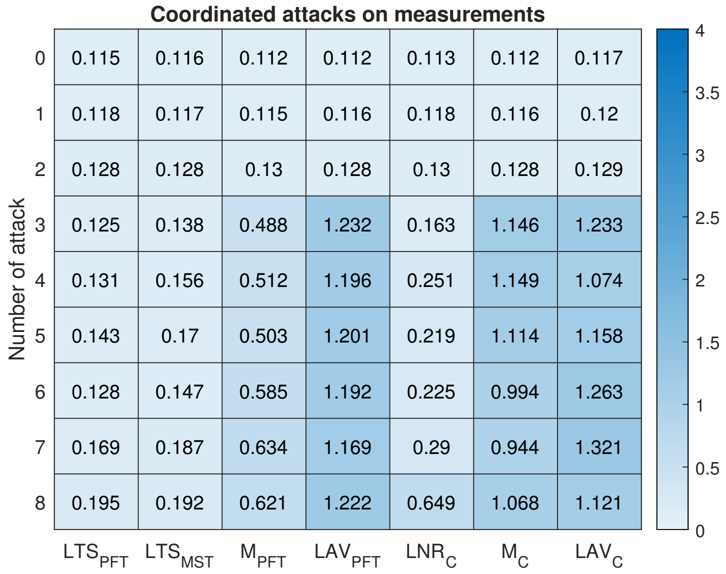
Figure 5.2: Average estimation errors under random attacks on measurements.

Table 5.5. Then, the attacked measurement vector z_c is generated as

$$z_{c,i} = \begin{cases} z_i + \delta z_i & \text{if } i = i_1, ..., i_{N_s}, \\ z_i & \text{otherwise.} \end{cases} \tag{5.1}$$

The results of the average estimation errors are shown in Fig. 5.2 in heatmap format. We observe that all schemes are capable to achieve good estimation at least up to seven attacks. It is notable that the centralized schemes perform quite well.

(b) As a more adversarial case, we consider measurement attacks in a more coordinated fashion. Specifically, the attack vector is set as $\delta z = Hc$, where c is a sparse vector with $c_i = 0.12$ rad for the entries corresponding to the phases of the targeted buses 2 and 6 and zero otherwise. Then, in the case when N_s points are attacked, the falsified measurements are generated by (5.1). The results of the average estimation errors are shown in Fig. 5.3. In this case, the two LTS-based schemes demonstrate to be the most robust, tolerating up to seven attacks. Other



Number of attack	LTS_{PFT}	LTS_{MST}	M_{PFT}	LAV_{PFT}	LNR_C	M_C	LAV_C
0	0.115	0.116	0.112	0.112	0.113	0.112	0.117
1	0.118	0.117	0.115	0.116	0.118	0.116	0.12
2	0.128	0.128	0.13	0.128	0.13	0.128	0.129
3	0.125	0.138	0.488	1.232	0.163	1.146	1.233
4	0.131	0.156	0.512	1.196	0.251	1.149	1.074
5	0.143	0.17	0.503	1.201	0.219	1.114	1.158
6	0.128	0.147	0.585	1.192	0.225	0.994	1.263
7	0.169	0.187	0.634	1.169	0.29	0.944	1.321
8	0.195	0.192	0.621	1.222	0.649	1.068	1.121

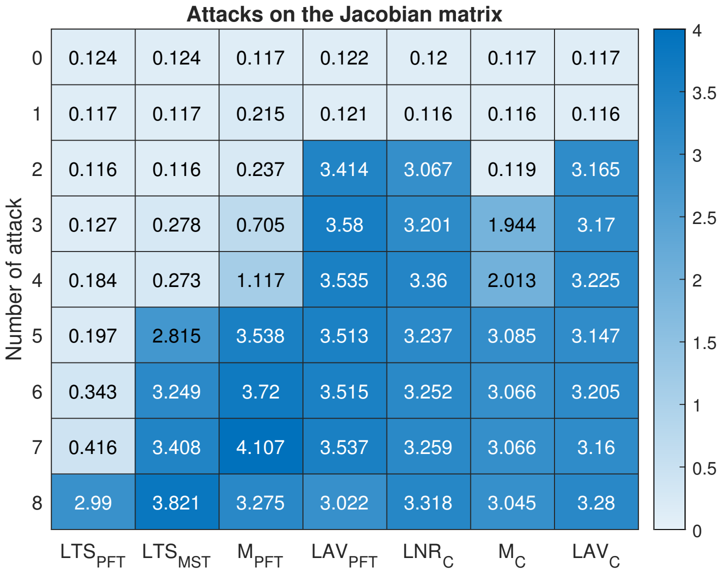
Figure 5.3: Average estimation errors under coordinated attacks on measurements.

methods quickly become unreliable. The Huber M and LAV for both centralized and decomposition-based schemes can handle only up to two attacks while the conventional centralized LNR manages up to three attacks.

5.3.3 Attacks on the Jacobian Matrix

Next, we examine the effects of attacks on the Jacobian matrix, resulting in leverage points. Here, we also follow the attack strategy in Table 5.5 and gradually increase the number N_s. To this end, the attack values on H are generated by first setting the matrix $\delta H \in R^{m\times n}$ as

$$[\delta H]_{i,j} = \begin{cases} (\eta - 1)[H]_{i,j} & \begin{array}{l}\text{if } j \text{ corresponds to phase} \\ \text{angle of bus 2 or 6,}\end{array} \\ 0 & \text{otherwise,} \end{cases}$$



Number of attack	LTS$_{PFT}$	LTS$_{MST}$	M$_{PFT}$	LAV$_{PFT}$	LNR$_{C}$	M$_{C}$	LAV$_{C}$
0	0.124	0.124	0.117	0.122	0.12	0.117	0.117
1	0.117	0.117	0.215	0.121	0.116	0.116	0.116
2	0.116	0.116	0.237	3.414	3.067	0.119	3.165
3	0.127	0.278	0.705	3.58	3.201	1.944	3.17
4	0.184	0.273	1.117	3.535	3.36	2.013	3.225
5	0.197	2.815	3.538	3.513	3.237	3.085	3.147
6	0.343	3.249	3.72	3.515	3.252	3.066	3.205
7	0.416	3.408	4.107	3.537	3.259	3.066	3.16
8	2.99	3.821	3.275	3.022	3.318	3.045	3.28

Figure 5.4: Average estimation errors under attacks on the Jacobian matrix.

for $i = 1, \ldots, m$ with $\eta = -3$. Then, the attacked Jacobian matrix H_c is set as

$$[H_c]_{i,j} = \begin{cases} [H]_{i,j} + [\delta H]_{i,j} & \text{if } i = i_1, \ldots, i_{N_s}, \\ [H]_{i,j} & \text{otherwise,} \end{cases}$$

for $j = 1, \ldots, n$. Under this attack, the estimated phases of the targeted buses 2 and 6 will become one third of the true estimate values. In the current setting, the true phase of bus 2 is -6.48 deg, and hence, after the modification by the intruder, it becomes $-6.48/\eta = 2.16$ deg.

Fig. 5.4 shows the average estimation errors for the seven estimation schemes. Under this attack scenario, we clearly see the advantage of LTS based on the PFT decomposition method. In particular, the difference from the LTS-MST method becomes more evident as we increase the number of attacks to more than four points. Figs. 5.5 and 5.6 show the phase angle estimations of all buses for LTS-PFT and LTS-MST in detail in box plots obtained from the Monte Carlo simulations. The green asterisks in the plots are the (true) power flow values.

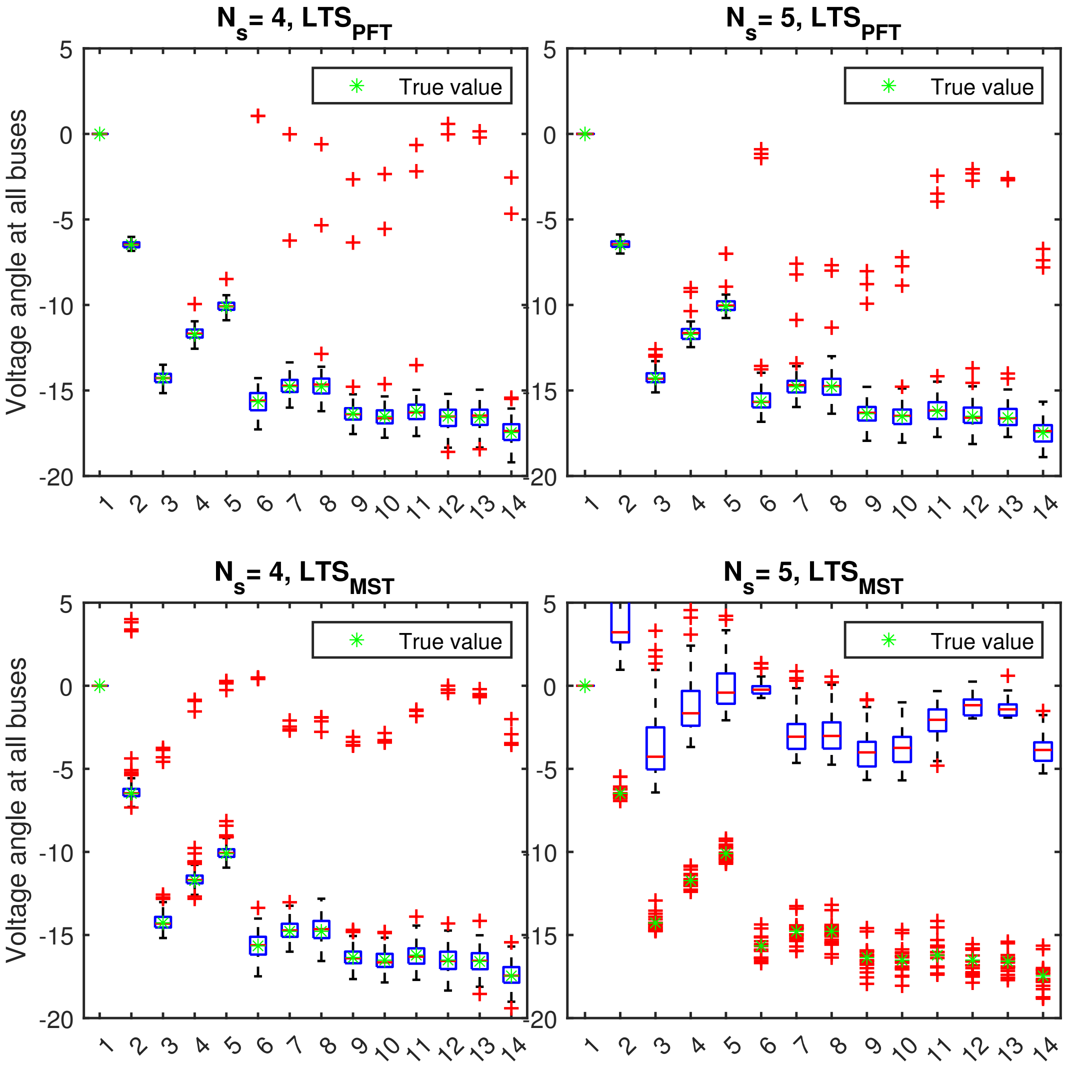


Figure 5.5: Estimated phase angles of 14 buses by LTS-PFT (top) and LTS-MST (bottom) under attacks on the Jacobian matrix for $N_s = 4, 5$.

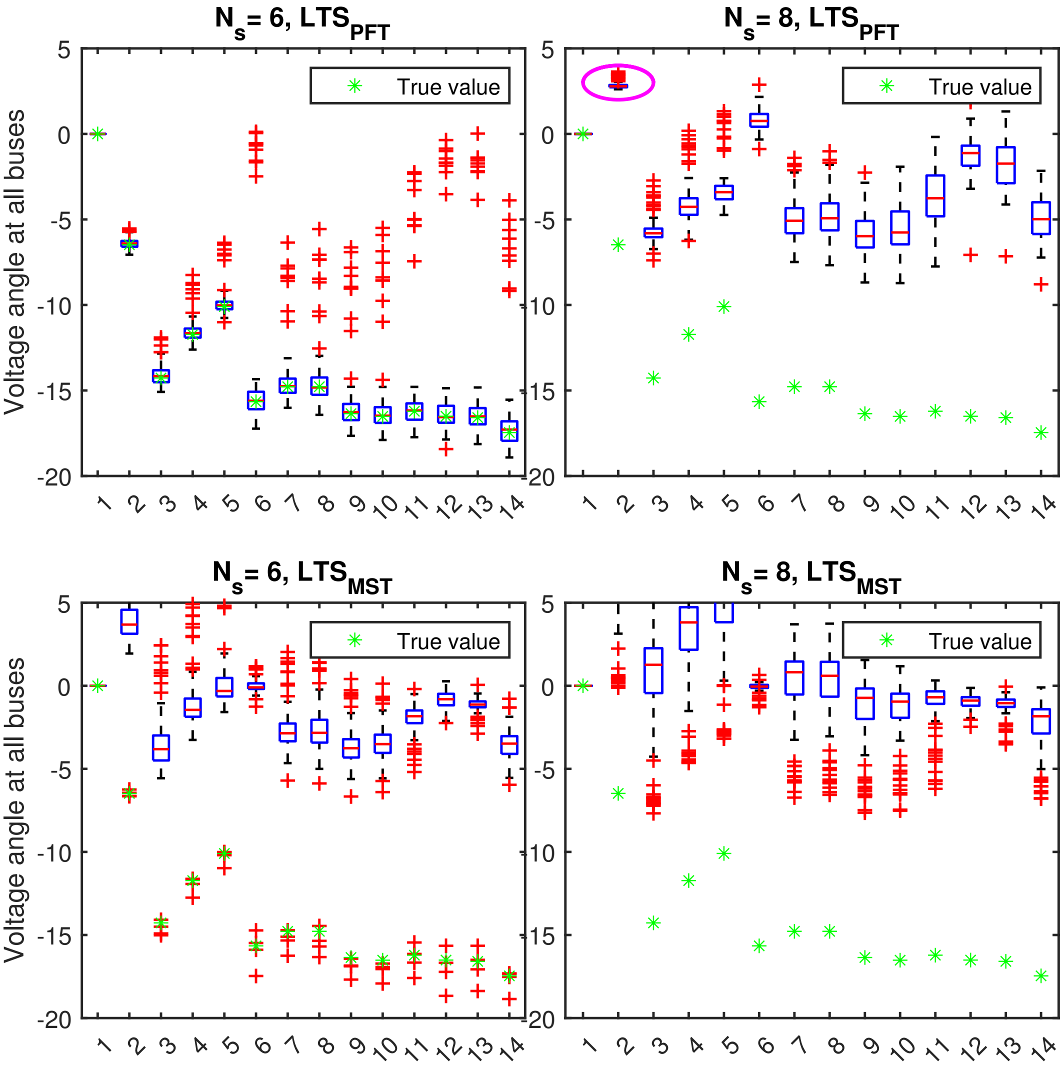
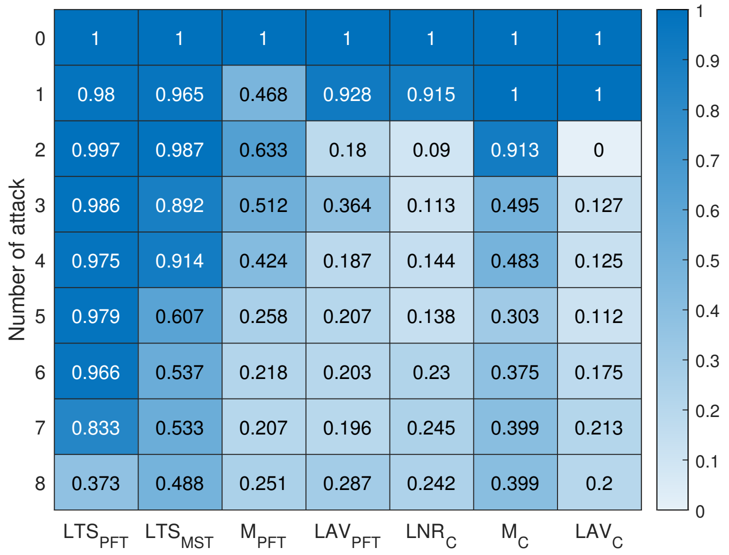


Figure 5.6: Estimated phase angles of 14 buses by LTS-PFT (top) and LTS-MST (bottom) under attacks on the Jacobian matrix for $N_s = 6, 8$.

When the number of attacks is $N_s = 4$, the difference between the two methods can be found in erroneous estimations in the MST-based results, indicated by the red pluses; this difference is not visible from the average estimation error data in Fig. 5.4. Here the attack points are P_1, P_2, P_4, and P_6, and these make the estimation of the large-sized islands I_8, I_9, and I_{10} for the MST-based method vulnerable as it goes beyond the breakdown points in these islands (see Table 5.4). As a consequence, the estimation in these islands fails to properly detect the attack points. In contrast, under the PFT-based method, all islands remain functional in estimation. Moreover, when we increase the attacks to five points, the MST-based method totally breaks down as shown in both Fig. 5.4 and Figs. 5.5. Finally, by increasing the attacks up to eight points for the PFT-based method, the phase angle at bus 2 moves to the targeted value of 2.16 deg (shown with a magenta circle in Fig. 5.6 for $\mathrm{LTS}_{\mathrm{PFT}}$ with $N_s = 8$). This occurs even though for some islands, the number of attacks may not be enough for realizing targeted attacks (as shown in Tables 5.2, 5.3, and 5.4). This is because the Jacobian matrix is sparse.

As demonstrated above, the LTS based on the PFT method well outperforms other estimation schemes, especially in comparison to the conventional $\mathrm{LNR}_{\mathrm{C}}$, which is popular in practice. We would like to highlight now that even when the estimation accuracy starts to degrade after the number of attacks goes beyond 4 or so, our approach can provide good performance in terms of detection of the attacked measurements. To show this, we introduce three performance measures as follows: (a) The estimated probability of leverage point detection given by $P_l = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n_{T,k}^l}{n_{T,k}^l+n_{F,k}}$, where $n_{T,k}^l$ is the number of detected leverage points truly present in the attack for each run k and $n_{F,k}$ is the number of falsely detected leverage points. (b) The estimated probability of false detection given by $P_f = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n_{F,k}}{n_{T,k}^l+n_{F,k}}$. (c) The true probability of leverage point detection



	LTS$_{PFT}$	LTS$_{MST}$	M$_{PFT}$	LAV$_{PFT}$	LNR$_{C}$	M$_{C}$	LAV$_{C}$
0	1	1	1	1	1	1	1
1	0.98	0.965	0.468	0.928	0.915	1	1
2	0.997	0.987	0.633	0.18	0.09	0.913	0
3	0.986	0.892	0.512	0.364	0.113	0.495	0.127
4	0.975	0.914	0.424	0.187	0.144	0.483	0.125
5	0.979	0.607	0.258	0.207	0.138	0.303	0.112
6	0.966	0.537	0.218	0.203	0.23	0.375	0.175
7	0.833	0.533	0.207	0.196	0.245	0.399	0.213
8	0.373	0.488	0.251	0.287	0.242	0.399	0.2

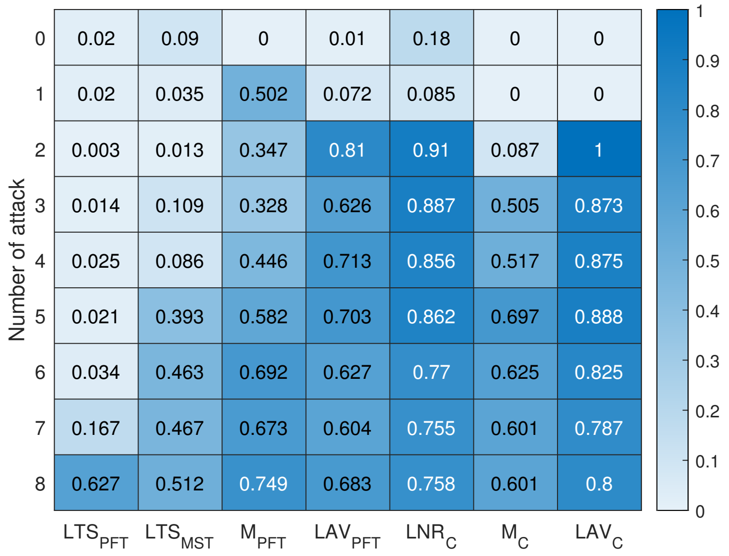
Figure 5.7: The estimated probability of detection leverage point.

$d_l = \frac{1}{M_c}\sum_{k=1}^{M_c}\frac{n^l_{T,k}}{n_l}$, where n_l is the number of the leverage points introduced.

The results for these three measures (a)–(c) are shown in Figs. 5.7, 5.8, and 5.9. In general, we observe that the LTS-PFT outperforms all other schemes in all three detection measures. In particular, the difference from the LTS-MST method becomes evident after N_s becomes larger than 5. Moreover, the measures for LTS-PFT indicate its high reliability in attack detection up to $N_s = 7$. Other schemes may be considered reliable in detecting only 1 leverage point except for M$_\text{C}$, which exhibits good performance when $N_s = 2$ also. In the robust statistics literature, it is known that the Huber M, LAV, and LNR are vulnerable to leverage points [32; 61; 90].

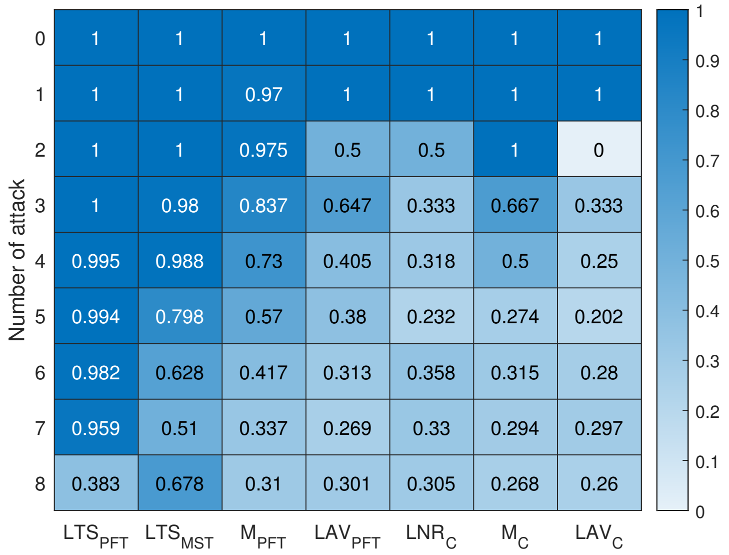
5.3.4 Hybrid Estimation under Attacks on the Jacobian

In this last part, we would like to see the effectiveness of introducing more measurements to the system and in particular use PMUs under attacks on the Jacobian as in the previous subsection. Following [21], we place PMUs at buses 2, 6,



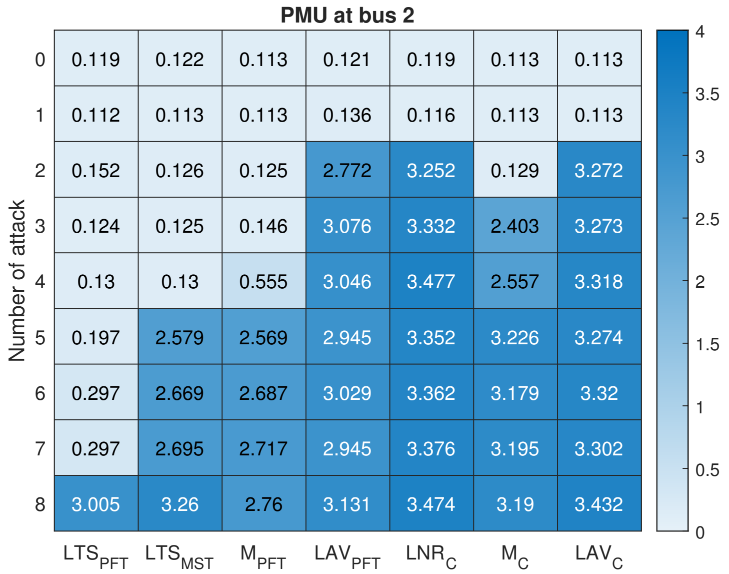
Number of attack	LTS$_{PFT}$	LTS$_{MST}$	M$_{PFT}$	LAV$_{PFT}$	LNR$_C$	M$_C$	LAV$_C$
0	0.02	0.09	0	0.01	0.18	0	0
1	0.02	0.035	0.502	0.072	0.085	0	0
2	0.003	0.013	0.347	0.81	0.91	0.087	1
3	0.014	0.109	0.328	0.626	0.887	0.505	0.873
4	0.025	0.086	0.446	0.713	0.856	0.517	0.875
5	0.021	0.393	0.582	0.703	0.862	0.697	0.888
6	0.034	0.463	0.692	0.627	0.77	0.625	0.825
7	0.167	0.467	0.673	0.604	0.755	0.601	0.787
8	0.627	0.512	0.749	0.683	0.758	0.601	0.8

Figure 5.8: The estimated probability of false detection.



Number of attack	LTS$_{PFT}$	LTS$_{MST}$	M$_{PFT}$	LAV$_{PFT}$	LNR$_C$	M$_C$	LAV$_C$
0	1	1	1	1	1	1	1
1	1	1	0.97	1	1	1	1
2	1	1	0.975	0.5	0.5	1	0
3	1	0.98	0.837	0.647	0.333	0.667	0.333
4	0.995	0.988	0.73	0.405	0.318	0.5	0.25
5	0.994	0.798	0.57	0.38	0.232	0.274	0.202
6	0.982	0.628	0.417	0.313	0.358	0.315	0.28
7	0.959	0.51	0.337	0.269	0.33	0.294	0.297
8	0.383	0.678	0.31	0.301	0.305	0.268	0.26

Figure 5.9: The true probability of detection of leverage points.



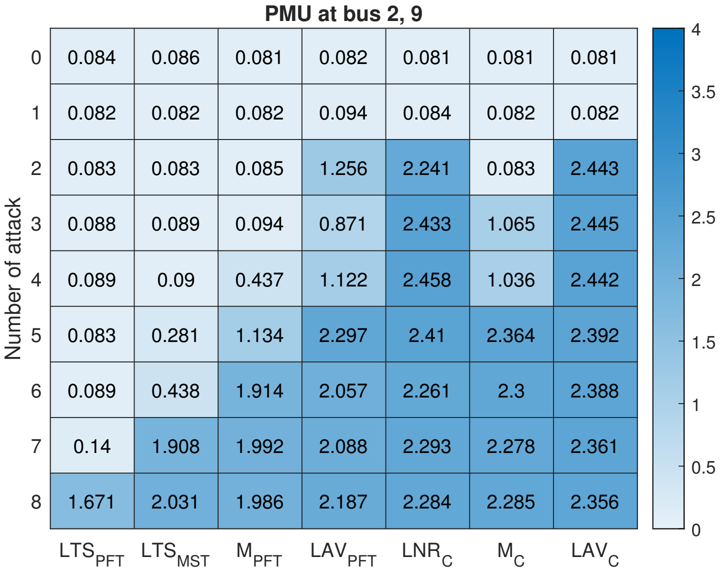
PMU at bus 2

Number of attack	LTS_{PFT}	LTS_{MST}	M_{PFT}	LAV_{PFT}	LNR_C	M_C	LAV_C
0	0.119	0.122	0.113	0.121	0.119	0.113	0.113
1	0.112	0.113	0.113	0.136	0.116	0.113	0.113
2	0.152	0.126	0.125	2.772	3.252	0.129	3.272
3	0.124	0.125	0.146	3.076	3.332	2.403	3.273
4	0.13	0.13	0.555	3.046	3.477	2.557	3.318
5	0.197	2.579	2.569	2.945	3.352	3.226	3.274
6	0.297	2.669	2.687	3.029	3.362	3.179	3.32
7	0.297	2.695	2.717	2.945	3.376	3.195	3.302
8	3.005	3.26	2.76	3.131	3.474	3.19	3.432

Figure 5.10: Average estimation errors with PMUs at bus 2 under coordinated attacks on the Jacobian matrix.

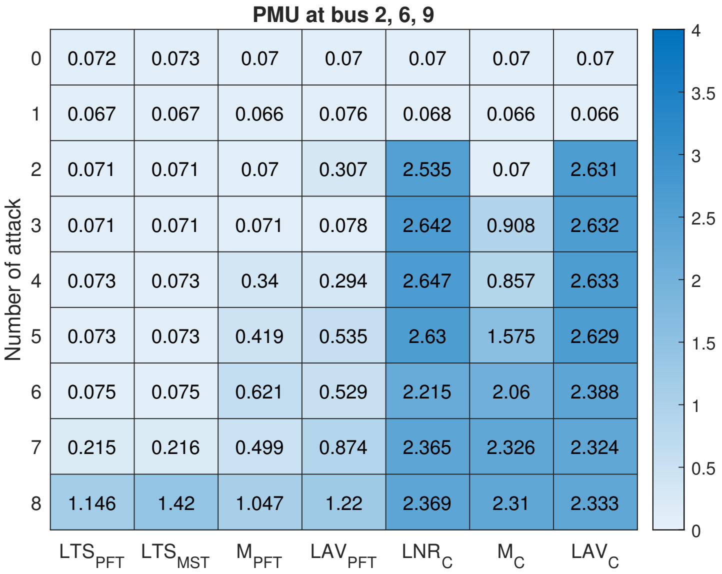
and 9 for phasor measurements. We use the errors from MATPOWER with the normal distribution of zero mean and standard deviation of 0.2 deg [94]. Here, PMUs are considered to be secure and will not be affected by FDI attacks.

It turns out that by increasing the number of PMUs, performance enhancement can be observed especially for the decomposition-based estimations. The average estimation errors in voltage angles are summarized in Figs. 5.10, 5.11, and 5.12 for three cases: (a) PMU at bus 2, (b) PMUs at buses 2 and 9, and (c) PMUs at buses 2, 6, and 9. Without any FDI attacks, the average errors are 0.108 for (a), 0.081 for (b), and 0.064 for (c). In comparison with the results in Fig. 5.4 without any PMU, we see that adding PMUs has immediate effects for all schemes except for the conventional LNR and LAV under centralized computation. Here, again, the LTS-PFT method performs best: While without PMU, it tolerated 4 attacks, adding one PMU does show a clear difference in the estimation accuracy. Moreover, with two PMUs, it increases the number of tolerable attack points to 7. It takes three PMUs for the performance of LTS-MST to become similar



Number of attack	LTS_{PFT}	LTS_{MST}	M_{PFT}	LAV_{PFT}	LNR_C	M_C	LAV_C
0	0.084	0.086	0.081	0.082	0.081	0.081	0.081
1	0.082	0.082	0.082	0.094	0.084	0.082	0.082
2	0.083	0.083	0.085	1.256	2.241	0.083	2.443
3	0.088	0.089	0.094	0.871	2.433	1.065	2.445
4	0.089	0.09	0.437	1.122	2.458	1.036	2.442
5	0.083	0.281	1.134	2.297	2.41	2.364	2.392
6	0.089	0.438	1.914	2.057	2.261	2.3	2.388
7	0.14	1.908	1.992	2.088	2.293	2.278	2.361
8	1.671	2.031	1.986	2.187	2.284	2.285	2.356

Figure 5.11: Average estimation errors with PMUs at buses 2 and 9 under coordinated attacks on the Jacobian matrix.



Number of attack	LTS_{PFT}	LTS_{MST}	M_{PFT}	LAV_{PFT}	LNR_C	M_C	LAV_C
0	0.072	0.073	0.07	0.07	0.07	0.07	0.07
1	0.067	0.067	0.066	0.076	0.068	0.066	0.066
2	0.071	0.071	0.07	0.307	2.535	0.07	2.631
3	0.071	0.071	0.071	0.078	2.642	0.908	2.632
4	0.073	0.073	0.34	0.294	2.647	0.857	2.633
5	0.073	0.073	0.419	0.535	2.63	1.575	2.629
6	0.075	0.075	0.621	0.529	2.215	2.06	2.388
7	0.215	0.216	0.499	0.874	2.365	2.326	2.324
8	1.146	1.42	1.047	1.22	2.369	2.31	2.333

Figure 5.12: Average estimation errors with PMUs at buses 2, 6, and 9 under coordinated attacks on the Jacobian matrix.

to that of LTS-PFT. We also computed the detection probabilities for the case with PMUs. Though we do not show the results, performance enhancement was evident as well.

5.3.5 IEEE 118-Bus system and Attacks on Its Jacobian

We now extend our study to the IEEE 118-bus system. Compared to the small-scale 14-bus case, the two decomposition methods result in quite different sets of islands. Some details about the island sizes and so on are shown in Table 5.1. In Figs. 5.13 and 5.14, the islands obtained by the PFT- and MST-based methods are, respectively, shown by different colors. Even at a glance, we see that in general, PFT-based islands are smaller in their sizes, which should help their robustness according to our discussion so far. The MST-based decomposition in Fig. 5.14 has a particularly large island indicated in pink. The attack scenario studied here centers around this island. Note that the measurement configuration is as explained in Section 5.2.1, and the total number of measurements is 726 for this system.

To this end, four target buses are selected to be buses 5, 19, 46, and 80. In Fig. 5.13, these buses are indicated by the red dots. They are far from each other and are clearly contained in different islands. However, notice in Fig. 5.14 that these buses are in fact all part of the largest island (in pink color). Attacks will be generated on these buses first and then on neighboring buses indicated by the yellow dots in Figs. 5.13 and 5.14. We demonstrate the effects of attacks by increasing the number N_s of attack points from 4 to 11 and following the order shown in Table 5.6.

The slack bus is taken to be bus 69, whose voltage angle is fixed to zero. For the detection of attacks, the thresholds are set to 10 for all steps and methods. These values were chosen after some trial runs so that in the clean case (without

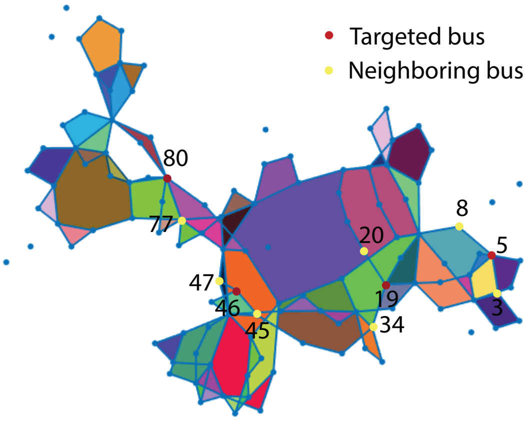


Figure 5.13: IEEE 118-bus system decomposed by PFT-based method and attacked buses.

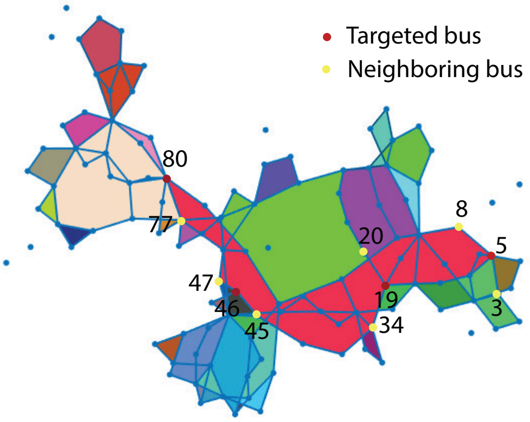


Figure 5.14: IEEE 118-bus system decomposed by MST-based method and attacked buses.

Table 5.6: Attacked measurements in the IEEE 118-bus system simulations

Number of attacks N_s	4	5	6	7	8	9	10	11
Measurements under falsification	$P_5, P_{19}, P_{46}, P_{80}$	P_3	P_{20}	P_{47}	P_{77}	P_8	P_{34}	P_{45}

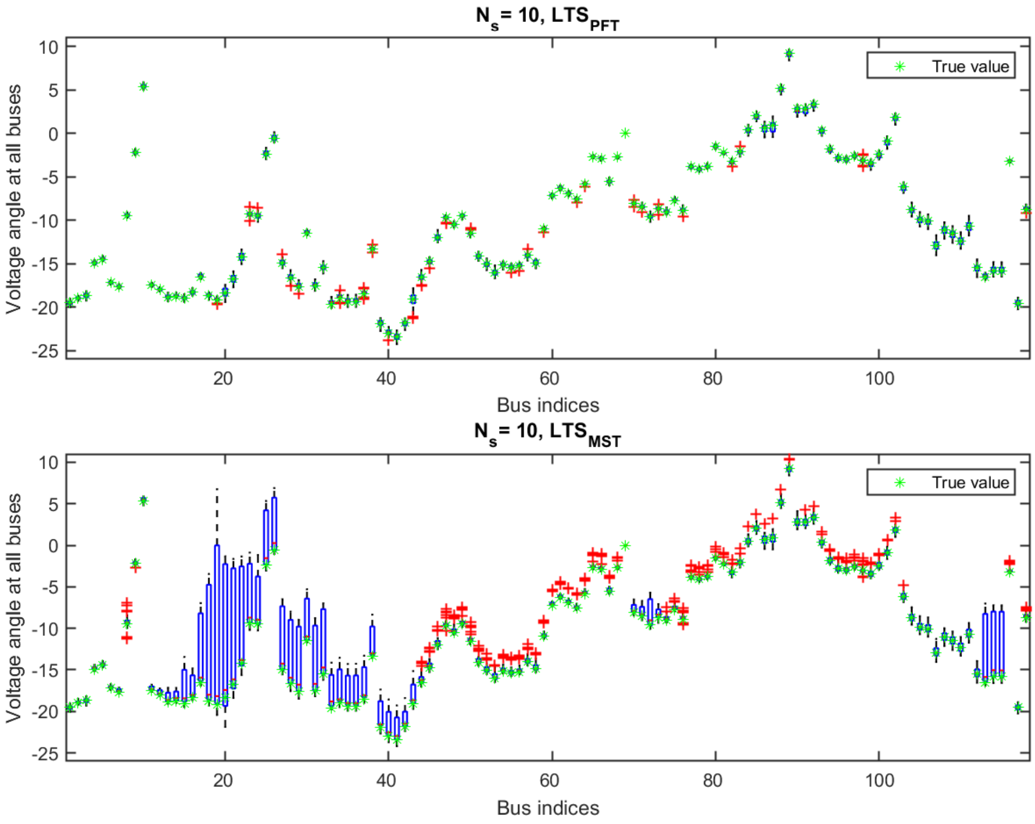
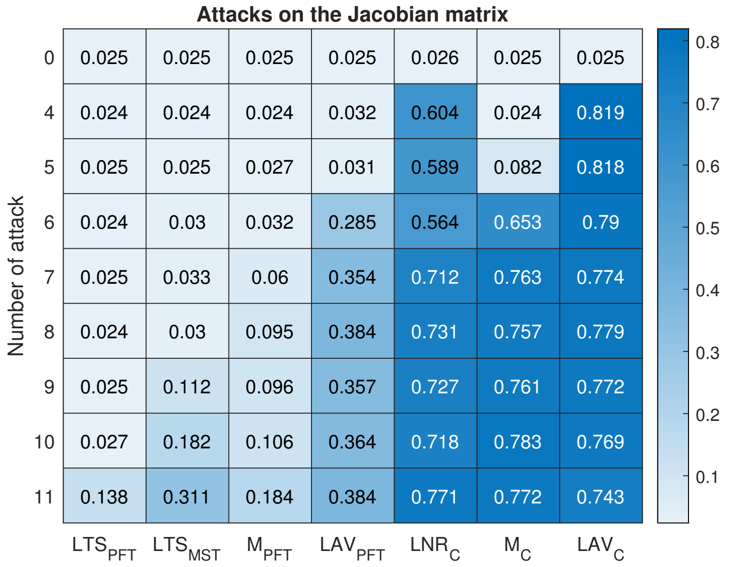


Figure 5.15: Estimated phase angles of 118 buses by LTS-PFT (top) and LTS-MST (bottom) under attacks on the Jacobian matrix for $N_s = 10$.



Number of attack	LTS_{PFT}	LTS_{MST}	M_{PFT}	LAV_{PFT}	LNR_C	M_C	LAV_C
0	0.025	0.025	0.025	0.025	0.026	0.025	0.025
4	0.024	0.024	0.024	0.032	0.604	0.024	0.819
5	0.025	0.025	0.027	0.031	0.589	0.082	0.818
6	0.024	0.03	0.032	0.285	0.564	0.653	0.79
7	0.025	0.033	0.06	0.354	0.712	0.763	0.774
8	0.024	0.03	0.095	0.384	0.731	0.757	0.779
9	0.025	0.112	0.096	0.357	0.727	0.761	0.772
10	0.027	0.182	0.106	0.364	0.718	0.783	0.769
11	0.138	0.311	0.184	0.384	0.771	0.772	0.743

Figure 5.16: Average estimation errors under attacks on the Jacobian matrix for the IEEE 118-bus system.

attacks), the false alarm detection rates are minimized. For each attack case, we make Monte Carlo simulations of 40 times ($M_c = 40$). Without any attacks, the LNR for the centralized scheme results in the average error 0.0241.

Fig. 5.15 shows the phase angle estimations of all buses for LTS-PFT (top) and LTS-MST (bottom) in box plots when $N_s = 10$ obtained from the Monte Carlo simulations. Obviously, the MST-based estimations vary more in their values and the error propagates much faster in the system (especially in the largest island). Fig. 5.16 shows the average estimation errors for the seven estimation schemes. We clearly see the advantage of the LTS-PFT method, especially over the LTS-MST method for $N_s = 9, 10$.

The results for estimated probabilities are shown in Figs. 5.17, 5.18, and 5.18. In general, we have the same pattern as that for the 14-bus system. We observe that the LTS-PFT outperforms all other schemes in all three detection measures. In particular, the difference from the LTS-MST method becomes evident after $N_s = 6$. Moreover, the measures for LTS-PFT indicate its high reliability up to

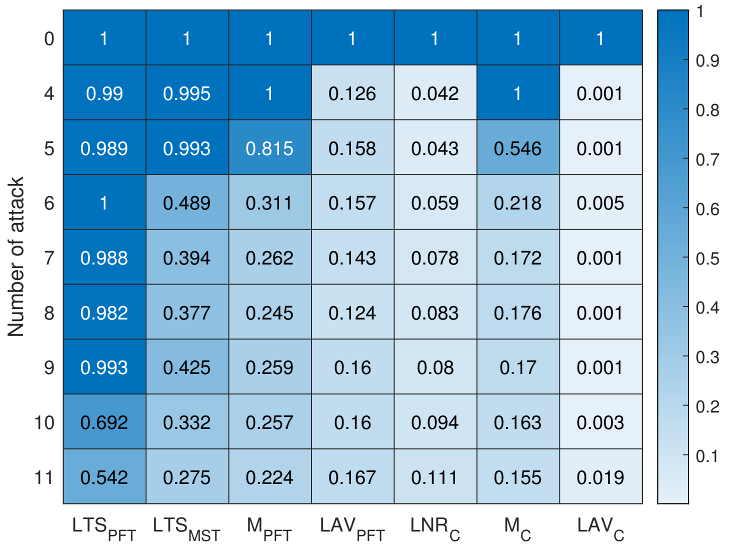
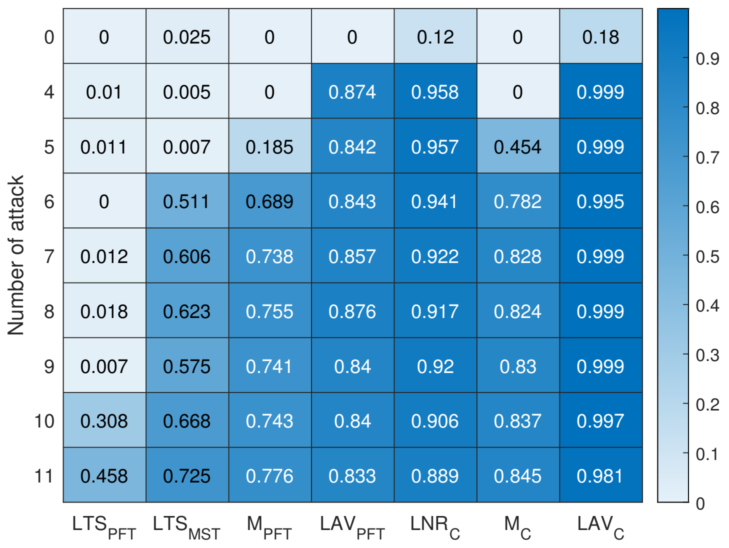


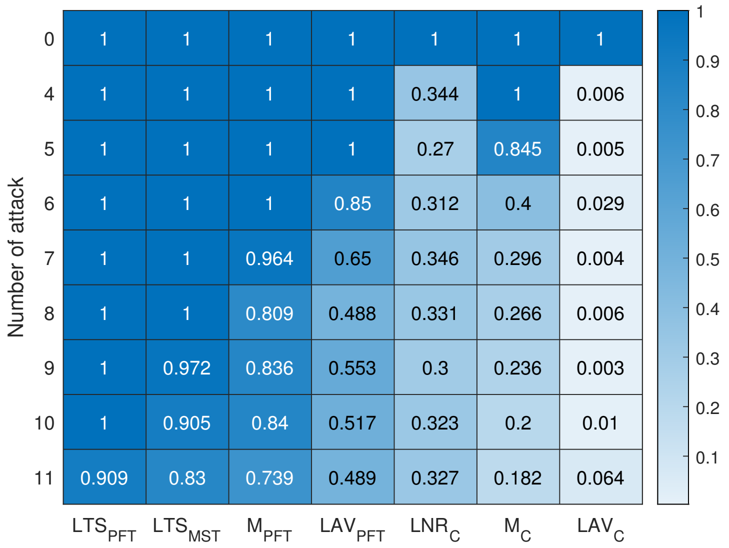
Figure 5.17: The estimated probability of detection leverage points for the IEEE 118-bus system.

$N_s = 10$. Other schemes may be considered unreliable after $N_s = 3$. Finally, we examined the average times of state estimation. For the LTS-PFT and LTS-MST methods, the running times for the SE at the largest islands (step 1 of Section 5.1, based on LTS executed in parallel) became 1.12 and 7.84 sec, respectively, whereas those for the SE of the whole system after removing outliers (steps 2 and 3, based on the common WLS) were 0.24 and 0.17 sec, respectively. The LTS-PFT method is faster since the islands are overall smaller than those of the LTS-MST.



Number of attack	LTS_{PFT}	LTS_{MST}	M_{PFT}	LAV_{PFT}	LNR_C	M_C	LAV_C
0	0	0.025	0	0	0.12	0	0.18
4	0.01	0.005	0	0.874	0.958	0	0.999
5	0.011	0.007	0.185	0.842	0.957	0.454	0.999
6	0	0.511	0.689	0.843	0.941	0.782	0.995
7	0.012	0.606	0.738	0.857	0.922	0.828	0.999
8	0.018	0.623	0.755	0.876	0.917	0.824	0.999
9	0.007	0.575	0.741	0.84	0.92	0.83	0.999
10	0.308	0.668	0.743	0.84	0.906	0.837	0.997
11	0.458	0.725	0.776	0.833	0.889	0.845	0.981

Figure 5.18: The estimated probability of false detection for the IEEE 118-bus system.



Number of attack	LTS_{PFT}	LTS_{MST}	M_{PFT}	LAV_{PFT}	LNR_C	M_C	LAV_C
0	1	1	1	1	1	1	1
4	1	1	1	1	0.344	1	0.006
5	1	1	1	1	0.27	0.845	0.005
6	1	1	1	0.85	0.312	0.4	0.029
7	1	1	0.964	0.65	0.346	0.296	0.004
8	1	1	0.809	0.488	0.331	0.266	0.006
9	1	0.972	0.836	0.553	0.3	0.236	0.003
10	1	0.905	0.84	0.517	0.323	0.2	0.01
11	0.909	0.83	0.739	0.489	0.327	0.182	0.064

Figure 5.19: The true probability of detection of leverage points for the IEEE 118-bus system.

Chapter 6

Conclusion

6.1 Summary

In this thesis, first we have considered an approach to enhance the cyber security of SSE for power systems. The proposed method systematically decomposes the system in a limited number of small islands. The main advantage of our approach lies in increasing the number of outliers that the state estimator can resist and detect. The implementation state estimation based on LTS on each island can be performed by computation in parallel. The effectiveness of the approach has been demonstrated via simulations using IEEE bus systems in comparison with other methods.

Second, we have considered robust techniques for static SE of power systems in the presence of FDI cyber-attacks on the measurement vectors and the Jacobian matrix. Our approach is to first apply the LTS at islands obtained from PFT-based decomposition and then execute state estimation for the entire system to verify the islands' detection results. We analyzed the PFT-based and MST-based decomposition methods and demonstrated the superior performance of the proposed method with the PFT-based method through extensive simulations on the IEEE 14- and 118-bus systems. Under coordinated attacks in the Jacobian matrix, the difference between the two decomposition methods has been shown in both state estimation and attack detection accuracies. For comparison, we have implemented other robust SE schemes and have further introduced PMUs providing more secure and accurate measurements.

6.2 Future Directions

The following is a list of some potential directions for future research based on the studies in this thesis:

1. **Consider more malicious attack**

   The type of attack considered in this study is a cyber attack. A new research focus would be on cyber physical attacks. It means that the attacker not only manipulates the physical system by opening or closing the targeted line's circuit breaker, but also penetrates the cyber layer and changes the neighboring measurement of the targeted line. Then, we use our algorithm to see if the mentioned attack is detectable. (manipulating measurement to see how far the attack can be detected.)

2. **Improve the robustness of the state estimation by taking account of the number of measurements and their locations in the time of cycle detections**

   In our research, we look at how to find islands in a given topology. Instead, we should consider islands base on where the measurements are placed. The challenge is to deal with additional layer of complexity in the computation.

References

[1] *Guidelines for Smart Grid Cybersecurity.* Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2014.

[2] *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Elect. Inf. Sharing Anal. Center, Washington, DC, USA, 2016.

[3] *Global Report: The State of Industrial Cybersecurity* 2017. Business Advantage Group Ltd., Orpington, U.K., 2017.

[4] A. Abur and A. G. Exposito. *Power System State Estimation: Theory and Implementation.* CRC Press, 2004.

[5] U. Adhikari, T. H. Morris, and S Pan. Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection. *IEEE Trans. Smart Grid*, 9(5):3928–3941, 2018.

[6] J. Agullo, C. Croux, and S. Van Aelst. The multivariate least-trimmed squares estimator. *J. Multivar. Anal.*, 99(3):311–338, 2008.

[7] N. Ahmadi, Y. Chakhchoukh, and H. Ishii. Power systems decomposition for robustifying state estimation under cyber attacks. *IEEE Trans. Power Syst.*, 36(3):1922–1933, 2021.

[8] N. Ahmadi, Y. Chakhchoukh, and H Ishii. Analysis of targeted coordinated attacks on decomposition-based robust state estimation. *IEEE Open Access Journal of Power and Energy*, to appear, 2023.

[9] S. Ahmed, Y. Lee, S. H. Hyun, and I. Koo. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Trans. Inf. Forensics Security*, 14(10):2765–2777, 2019.

[10] A. A. Aljabrine, A. A. Smadi, Y. Chakhchoukh, B. K. Johnson, and H. Lei. Resiliency improvement of an AC/DC power grid with embedded LCC-HVDC using robust power system state estimation. *Energies*, 14(14):7847, 2021.

[11] A. Ashok, M. Govindarasu, and V. Ajjarapu. Online detection of stealthy false data injection attacks in power system state estimation. *IEEE Trans. Smart Grid*, 9(3):1636–1646, 2016.

[12] M. Ashrafuzzaman, Y. Chakhchoukh, A. A. Jillepalli, P. T. Tosic, D. C. de Leon, F. T. Sheldon, and B. K. Johnson. Detecting stealthy false data injection attacks in power grids using deep learning. In *Proc. 14th Int. Wireless Comm. Mobile Comp. Conf. (IWCMC)*, pages 219–225, 2018.

[13] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. G. Shiva, and F. T. Sheldon. Detection of stealthy false data injection attacks in smart grid using ensemble-based security analytics. *Journal of Computers and Security*, 97, 2020.

[14] Designed by brgfx. Freepik [online]. Available: https://www.freepik.com/.

[15] E. Caro, A. Conejo, and R. Minguez. Power system state estimation considering measurement dependencies. *IEEE Trans. Power Syst.*, 4(24):1875–1885, 2009.

[16] Y. Chakhchoukh and H. Ishii. Coordinated cyber-attacks on the measurement function in hybrid state estimation. *IEEE Trans. Power Syst.*, 30(5):2487–2497, 2015.

[17] Y. Chakhchoukh and H. Ishii. Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations. *IEEE Trans. Power Syst.*, 31(6):4395–4405, 2016.

[18] Y. Chakhchoukh, H. Lei, and B. K. Johnson. Diagnosis of outliers and cyber attacks in dynamic PMU-based power state estimation. *IEEE Trans. Power Syst.*, 35(2):1188–1197, 2019.

[19] Y. Chakhchoukh, S. Liu, M. Sugiyama, and H. Ishii. Statistical outlier detection for diagnosis of cyber attacks in power state estimation. In *Proc. IEEE Power and Energy Society General Meeting*, pages 1–5, 2016.

[20] Y. Chakhchoukh, V. Vittal, G. T. Heydt, and H. Ishii. LTS-based robust hybrid SE integrating correlation. *IEEE Trans. Power Syst.*, 32(4):3127–3135, 2017.

[21] S. Chakrabarti and E. Kyriakides. Optimal placement of phasor measurement units for power system observability. *IEEE Trans. Power Syst.*, 23(3):1433–1440, 2008.

[22] J. Chen and A. Abur. Placement of PMUs to enable bad data detection in state estimation. *IEEE Trans. Power Syst.*, 21(4):1608–1615, 2006.

[23] Y. Chen, S. Jin, M. Rice, and Z. Huang. Parallel state estimation assessment with practical data. In *Proc. IEEE Power and Energy Society General Meeting*, pages 1–5, 2013.

[24] M. G. Cheniae, L. Mili, and P. J. Rousseeuw. Identification of multiple interacting bad data via power system decomposition. *IEEE Trans. Power Syst.*, 11(3):1555–1563, 1996.

[25] J. J. Cho, Y. Chen, and Y. Ding. Calculating the breakdown point of sparse linear models. *Technometrics*, 51(1):34–46, 2009.

[26] J. Condliffe. *Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks,*. MIT Technol. Rev., Cambridge, MA, USA, 2016.

[27] T. H. Cormen, C. E. Leiserson, R. Rivest, and C. Stein. *Introduction to Algorithms*. MIT Press, 2001.

[28] M. De Berg, M. Van Kreveld, M. Overmars, and O. Schwarzkopf. *Computational Geometry: Algorithms and Applications*. Springer, 1997.

[29] R. Deng, P. Zhuang, and H. Liang. Ccpa: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Trans. Smart Grid*, 8(5):2420–2430, 2017.

[30] R. Diestel. *Graph Theory*. Springer, 2000.

[31] Y. Ding and J. Liu. Real-time false data injection attack detection in energy Internet using online robust principal component analysis. In *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, pages 1–6, 2017.

[32] M. Dorier, G. Frigo, A. Abur, and M Paolone. Leverage point identification method for LAV-based state estimation. *IEEE Trans. on Instrum. Meas.*, 70(1008810):1–10, 2021.

[33] M. Du, G. Pierrou, X. Wang, and M. Kassouf. Targeted false data injection attacks against ac state estimation without network parameters. *IEEE Trans. Smart Grid*, 12(6):5349–5361, 2021.

[34] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z Han. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal*, 11(3):1644–1652, 2017.

[35] M. Faheem, S. B. H. Shah, R.A. Butt, B. Raza, M. Anwar, M. W. Ashraf, Md. A. Ngadi, and V.C. Gungor. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.*, 30:1–30, 2018.

[36] H. Farhangi. The path of the smart grid. *IEEE Power and Energy Mag.*, 8(1):18–28, 2010.

[37] Executive Office of the President. (Feb. 19, 2013). *Improving Critical Infrastructure Cybersecurity.* [online]. Available: https://bit.ly/2DRnTo5.

[38] A. Ferreira, M. J. Fonseca, and J. A. Jorge. Polygon detection from a set of lines. In *Proc. 12th EPCGI*, pages 159–162, 2003.

[39] H. N. Gabow, Z. Galil, T. Spencer, and R. E. Tarjan. Efficient algorithms for finding minimum spanning trees in undirected and directed graphs. *Combinatorica*, 6(2):109–122, 1986.

[40] A. Gaur. (2015) Steady-state ac network visualization in the browser [online]. Available: https://immersive.erc.monash.edu.au/stac/.

[41] D. Gleich. (2007) MATLAB BGL. [online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/10922-matlabbgl.

[42] M. Göl. A decentralization method for hybrid state estimators. *IEEE Trans. Power Syst.*, 33(2):2070–2077, 2018.

[43] T. L. Hardy. *Software and System Safety: Accidents, Incidents, and Lessons Learned.* Bloomington, IN, USA: AuthorHouse, 2012.

[44] Y. He, G. J. Mendis, and J. Wei. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans. Smart Grid*, 8(5):2505–2516, 2017.

[45] G. Hug and J. A. Giampapa. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Trans. Smart Grid*, 3(3):1362–1370, 2012.

[46] S. Iglin. (2009) grTheory: Graph Theory Toolbox. Available: https://www.mathworks.com/Matlabcentral/fileexchange/loadFile.do.

[47] S. Jin, Y. Chen, M. Rice, Y. Liu, and I. Gorton. A testbed for deploying distributed state estimation in power grid. In *Proc. IEEE Power and Energy Society General Meeting*, pages 1–7, 2012.

[48] H. Karimipour and V. Dinavahi. On false data injection attack against dynamic state estimation on smart power grids. In *Proc. IEEE Int. Conf. Smart Energy Grid Eng. (SEGE)*, pages 388–393, 2017.

[49] J. Kim and L. Tong. On topology attack of a smart grid: Undetectable attacks and countermeasures. *IEEE J. Sel. Areas Commun.*, 31(7):1294–1305, 2013.

[50] T. T. Kim and H. V. Poor. Strategic protection against data injection attacks on power grids. *IEEE Trans. Smart Grid*, 2(2):326–333, 2011.

[51] T. T. Kim and H. V. Poor. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Trans. Smart Grid*, 5(3):1216–1227, 2014.

[52] O. Kosut, L. Jia, and J. Thomas. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid*, 2(4):645–658, 2011.

[53] J. Liang, L. Sankar, and O Kosut. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Trans. Power Syst.*, 31(5):3864–3872, 2015.

[54] C. Liu, H. Liang, and T. Chen. Network parameter coordinated false data injection attacks against power system AC state estimation. *IEEE Trans. Smart Grid*, 12(2):1626–1639, 2021.

[55] J. Liu, Y. Xiao, and J Gao. Achieving accountability in smart grid. *IEEE Systems Journal*, 8(2):493–508, 2014.

[56] X. Liu and Z. Li. False data attacks against AC state estimation with incomplete network information. *IEEE Trans. Smart Grid*, 8(5):2239–2248, 2016.

[57] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Trans. Information and System Security*, 14(1):1–33, 2011.

[58] G. Loukas. *Cyber-Physical Attacks: A Growing Invisible Threat.* Butterworth-Heinemann, Oxford, U.K., 2015.

[59] A. Majumdar and B. C. Pal. Bad data detection in the context of leverage point attacks in modern power networks. *IEEE Trans. Smart Grid*, 9(3):2042–2054, 2018.

[60] K. Manandhar, X. Cao, F. Hu, and Y Liu. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control Netw. Syst.*, 1(4):370–379, 2014.

[61] R. A. Maronna, R. D. Martin, and V. J. Yohai. *Robust Statistics: Theory and Methods*. Wiley, 2006.

[62] S. Massoud Amin and B. F. Wollenberg. Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Mag.*, 3(5):34–41, 2005.

[63] L. Mili, M. G. Cheniae, and P. J. Rousseeuw. Robust state estimation of electric power systems. *IEEE Trans. Circuits Syst. I*, 41(5):349–358, 1994.

[64] L. Mili, V. Phaniraj, and P. J. Rousseeuw. Least median of squares estimation in power systems. *IEEE Trans. Power Syst.*, 6(2):511–523, 1991.

[65] A. Monticelli. Electric power system state estimation. *Proc. IEEE*, 88(2):262–282, 2000.

[66] K. Moslehi and R. Kumar. A reliability perspective of the smart grid. *IEEE Trans. Smart Grid*, 1(1):57–64, 2010.

[67] A. S. Musleh, G. Chen, and Z. Y. Dong. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid*, 11(3):2218–2234, 2020.

[68] J. Nocedal and S. J. Wright. *Numerical Optimization*. Springer, 2006.

[69] S. Pan, T. Morris, and U Adhikari. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Trans. Smart Grid*, 6(6):3104–3113, 2015.

[70] S. G. I. Panel. Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements, and Vol. 2, privacy and the smart grid, National Institute of Standards and Technology (NIST). *Interagency Rep*, 7628, 2010.

[71] T. Reed. *At the Abyss: An Insider's History of the Cold War.* Novato, CA, USA: Presidio Press, 2015.

[72] R. L. Rivest and J. Vuillemin. On recognizing graph properties from adjacency matrices. *Theoret. Comput. Sci.*, 3(3):371–384, 1976.

[73] S. Schneider and I. F. Sbalzarini. (2015) Finding faces in a planar embedding of a graph [online]. Available: https://mosaic.mpicbg.de/docs/Schneider2015.pdf.

[74] F. C. Schweppe and J. Wildes. Power system static state estimation, part i: Exact model. *IEEE Trans. Power Appar. Syst.*, PAS-89:120–125, 1970.

[75] J. Siek, L.-Q. Lee, and A. Lumsdaine. *The Boost Graph Library: User Guide and Reference Manual.* Addison-Wesley, 2002.

[76] G. Simard. *IEEE Grid Vision 2050.* IEEE PES, Piscataway, NJ, USA, 2013.

[77] C. C. Sun, A. Hahn, and C. C. Liu. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.*, 99:45–56, 2018.

[78] M. Swearingen, S. Brunasso, J. Weiss, and D. Huber. *What You Need to Know (and Don't) About the AURORA Vulnerability, PowerMag.* Bloomington, IN, USA: AuthorHouse, 2013.

[79] M. M. Sysło. An efficient cycle vector space algorithm for listing all cycles of a planar graph. *SIAM J. Computing*, 10(4):797–808, 1981.

[80] S. Tan, W. Z. Song, M. Stewart, and L. Long. LPAttack: Leverage point attacks against state estimation in smart grid. In *IEEE Global Communications Conference*, pages 643–648, 2014.

[81] R. Tarjan. Depth-first search and linear graph algorithms. *SIAM J. Computing*, 1(2):146–160, 1972.

[82] S. Toppa. (Mar. 2015). *The National Power Grid Is Under Almost Continuous Attack Report Says* [online]. Available: https://bit.ly/1FH246I.

[83] Y. Weng, R. Negi, Q. Liu, and Ilić M. D. Robust state-estimation procedure using a least trimmed squares pre-processor. In *Proc. IEEE PES Innovative Smart Grid Technol.*, pages 1–6, 2011.

[84] A. Windsor. (2015) Planar face traversal, boost c++ libraries [online]. Available: https://www.boost.org/doc/libs/1 36 0/ boost/graph/planar face traversal.html.

[85] M. Yao, D. Molzahn, and J. Mathieu. An optimal power-flow approach to improve power system voltage stability using demand response. *IEEE Trans. Contr. Network Syst.*, 6(3):1015–1025, 2019.

[86] X. Yu and Y Xue. Smart grids: A cyber–physical systems perspective. *Proc. IEEE*, 104(5):1058–1070, 2016.

[87] Y. Yuan, Z. Li, and K. Ren. Modeling load redistribution attacks in power systems. *IEEE Trans. Smart Grid*, 2(2):382–390, 2011.

[88] P. Zarco and A. G. Exposito. Power system parameter estimation: A survey. *IEEE Trans. Power Syst.*, 15(1):216–222, 2000.

[89] J. Zhang, Z. Chu, L. Sankar, and O. Kosut. Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? *IEEE Trans. Power Syst.*, 33(5):4775–4786, 2018.

[90] J. Zhao and L. Mili. Vulnerability of the largest normalized residual statistical test to leverage points. *IEEE Trans. Power Syst.*, 33(4):4643–4646, 2018.

[91] J. Zhao, L. Mili, and M. Wang. A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. *IEEE Trans. Power Syst.*, 33(5):4868–4877, 2018.

[92] J. Zhao, G. Zhang, and R. A. Jabr. Robust detection of cyber attacks on state estimators using phasor measurements. *IEEE Trans. Power Syst.*, 32(3):2468–2470, 2016.

[93] J. Zhao *et al.* Power system dynamic state estimation: Motivations, definitions, methodologies, and future work. *IEEE Trans. Power Syst.*, 4(34):3188–3198, 2019.

[94] R. D. Zimmerman and Murillo-Sánchez. (2019) Pmatpower, ver. 6.0. [online]. Available: https://matpower.org.

[95] A. M. Zoubir, V. Koivunen, Y. Chakhchoukh, and M. Muma. Robust estimation in signal processing: A tutorial-style treatment of fundamental concepts. *IEEE Signal Proc. Magazine*, 29(4):61–80, 2012.