Vulnerability Analysis of Power System State Estimation

Data and Topology-Driven Attacks

Ammara Gul

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

ROYAL HOLLOWAY UNIVERSITY OF LONDON

2020

Vulnerability Analysis of Power System State Estimation

School of Mathematics and Information Security
Royal Holloway, University of London

To my Parents, my husband Junaid, and my children Bareera & Badar.

Declaration of Authorship

I, Ammara Gul, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

(Ammara Gul)

Date:

Summary

State estimation is a significant tool for a system's control and monitoring purposes. It is a process of estimating the actual state of the system. It has been extensively used in electrical power networks. Transformation of power systems to largely distributed smart grids provides the ability to deal with networks that are more complex and to enhance robustness. On the other side, for a smart grid to be robust, its information infrastructure must be reliable in case of failures and attacks. This thesis contributes to the characterisation of information flows and error propagation within state estimators (centralised and hierarchical) in the face of different (yet novel) attacks.

For a couple of decades, state estimation has gained much attention and several state estimators have been proposed so far including centralized, hierarchical and distributed. However, as far as resilience and robustness against attacks are concerned, conventional state estimation has remained the centre of interest. While future generation smart grid is mostly distributed, decentralised structures are high in demand to retain system robustness. We particularly propose data and topology related (novel) attacks for centralised state and then extend them to hierarchical case determining the necessary and sufficient conditions for the adversary to attack.

We instigate a constrained swapping attack mechanism which will be realistic even with the communication channel (for measurements) being authenticated and integrity-protected such as those recommended by the ISO/IEC 62351 standard. We show that measurement re-ordering is sufficient to provoke errors in state estimation or prevent it to converge. We define security metrics to quantify the importance of sparse and minimum magnitude re-ordering attacks, assuming partial knowledge available. In addition, we translate re-ordering attacks on hierarchical state estimation and study fault propagation in intermediate and top-level state estimate because of attack on bottom level region.

Among deliberate attacks on state estimation, data-driven malicious activities e.g., false data attacks are extensively explored than the other main cause i.e., topology related attacks. Hence, we consider types of attacks including single and double topology modifications and study the impacts on state estimators of induced double line faults. Possible effects range from state forcing to divergence while determining optimal conditions for attackers (with partial system knowledge). Moreover, as topology processing is conventionally performed before state estimation, attacker has a good chance to stealthily induce and possibly revert topology changes within a single scan cycle. We exploit the abstraction that all measurements arrive instantly and synchronously to be processed by state estimator. We therefore give an adversary model by formulating an optimisation problem that minimises attack cost and determines the impacts in form of denial of service

attacks up to loss of observability and study recoverability.

Both the use of renewable energy and demand management require more frequent controlled topology changes compared to arising from faults/maintenance. Topology processing is hence an integral part of state estimation. We expand topology processing algorithm for better understanding of vulnerabilities with respect to an attacker. Therefore, we propose topology modifications that can cause impacts including state forcing and propose an approach to determine optimum cost attacks for adversaries with limited system knowledge.

List of Publications

- Gul, A. and Wolthusen, S.: 'Measurement Re-Ordering Attacks on Power System State Estimation' in *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017 IEEE PES*, and pp. 26-29 (DOI: 10.1109/ISGTEurope.2017.8260145).
- Gul, A. and Wolthusen, S.: 'A Review on Attacks and their Countermeasures in Power System State Estimation' in *Smart Micro-Grid Systems Security and Privacy (SMGSP 2017)*.
- Gul, A. and Wolthusen, S.: 'Error Propagation after Re-ordering Attacks in Hierarchical State Estimation' in *Twelfth IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Virginia, USA, March 2018*.
- Gul, A. and Wolthusen, S.: 'In-Cycle Sequential Topology Faults and Attacks: Effects on State Estimation' in *Thirteenth International Critical Infrastructures Conference (CRITIS), Lithuania, 2018*.
- Gul, A. and Wolthusen, S.: 'State Estimation under Undetectable Single and Double Line Failures' in *Innovative Smart Grid Technologies Conference (ISGT-North America), 2019*.
- Gul, A., Baiocco, A. and Wolthusen, S.: 'State Forcing under Dynamic Topology Faults and Attacks' (in process)

Acknowledgments

The research in this thesis would not have been possible to complete without the encouragement of many people. It is a delight to acknowledge all those who have supported me over the last four years.

I am sincerely and heartily grateful to Professor Stephen D. Wolthusen, my PhD supervisor, for his endless support, guidance, motivation, patience and immense knowledge throughout my PhD study and related research. His guidance helped me throughout the time spent in performing the research for and writing up of this thesis. I could not have imagined having a better supervisor for my PhD study.

I cannot find words to express my heartily thanks to my soul mate, my best friend, and my husband, Junaid, for his constant love, support and understanding before and during my study of PhD degree. He is always been the one for me to lean on at all times.

I owe thanks to my lovely daughter, Bareera who is the pride and joy of my life. Having her during my PhD gave me strength and helped me to be more efficient and my young boy, Badar, apple of my eye, who taught me to become more responsible.

I wholeheartedly thank my father, Gul Muhammad who is the key motivation behind this PhD and who always believed in me, supported me in every decision I made and every step I took to ensure that I reach where I want to be. He is the one who always wanted me to study abroad regardless of all the family and society norms.

I am really grateful to my friend Dr. Sundas Khan who have always been on my side throughout my journey.

I would particularly like to thank Dr. Alessio Baiocco who joined in for the last journal submission to provide numerical results for State Forcing Attack which is an integral part of the thesis.

I profoundly appreciate my colleague, Mr Shao for presenting my work on my behalf at CRITIS2018.

I would like to show my gratitude to my siblings: Bilal, Zubair, Rahila and Umair who always played their role throughout.

I am very grateful to my mother Qamar Sultana, my mother-in-law Shaista Bano, my father-in-law Mohammed Younus and all my relatives and friends.

Finally, I owe sincere and earnest thankfulness to Allah who gave me the blessing to have such amazing people in my life and for giving me the strength to do my PhD.

Contents

List of Figures

List of Tables

List of Theorems

List of Definitions

List of Algorithms

Chapter 1

Introduction

Conventionally, power systems have been following a unidirectional flow of energy from generation through transmission and distribution to the loads. The downside of having no real-time information on (load) parameters along with other issues (including rapidly increase in demand) calls for a more distributed system. To deal with such drawbacks, the idea of smart grid emerged with a concept of automated real-time monitoring and control, so that the system is more resilient and robust to failures/attacks. Regardless of how better is the smart grid, existing power networks cannot be completely replaced but both work side by side adding new technology i.e., smart devices to the system now.

In recent decades, an adequate amount of study has been done dealing with bad data and robustness issues of power system state estimators. However, most of the state estimators (introduced) so far are not taking into account the level of integration involved in recent grid environment i.e., penetration of renewables, mobile loads and high precision measurement devices etc. Such situations demand a dynamic system able to cope with unanticipated scenarios e.g., load changes and topology faults including others.

Moreover, reviewing most of the influential works on attacks and mitigation schemes on state estimation along with their limitations can be a crucial task. It can be a helpful survey for an interested individual to follow the path of theoretical advancements in this area.

State estimation depends on remote sensors (for measurements) and topology processing for its reliable operation. Sequentially, it has a crucial role in Energy Management system (EMS) operating the grid and carrying out contingency analysis [4]. Measurements can both be faulty and attacked on sensors or communication network. Several attacks have been presented ranging from the measurement manipulation [61] to delays in communication channels by Baiocco et al. [9]. False data injection is, however, may not be quite a realistic assumption and that the future grid is equipped with the security of measurements and communication channels, at least being authenticated and integrity protected as provided e.g. by the ISO/IEC 62351 standard. This feature should be investigated for possible advanced attacks i.e., measurement re-ordering including others, both on centralised and decentralised state estimation cases (hierarchical).

In addition, attacks on topology have become a vital aspect to consider besides the well-known data-related attacks. Induced single and multiple line faults would be interesting to explore. Topology processing can either be performed before (conventionally) or alongside state estimation (generalised). In an ideal world, state estimation should take a few seconds for its one scan but rather, a scan cycle is taking a few minutes until recently. In all respect, an adversary can make changes to the topology within this time window and remain unobservable by maintaining the topology to be the same before and after measurement taking process.

Network topology processing is itself a complex algorithm consisting of further sub-tasks to be performed in a certain order. To launch an attack on topology algorithm, understanding the information flow from one phase to other is critical. State forcing can be one of the possible impacts of addressing the vulnerability in topology processing algorithm.

1.1 Research Questions

In this section, we first give justifications/motivations and then state the corresponding research questions.

- Unlike the work mentioned before, most of attacks, however, rely on the assumption that arbitrary values may be injected by an adversary. *We argue that this assumption is quite strong* and that instead, it is of considerable interest to study cases where measurements and communication channels are protected, at least using authentication and integrity protection as provided e.g. by the ISO/IEC 62351 standard. **RQ1** *Can a feasible measurement re-ordering (swapping) attack be modelled in centralized state estimation assuming certain security protocols?*
- In addition to the same security measures in place, it would be interesting to see the error propagation after a swapping attack in a decentralised structure. **RQ2** *and translated to hierarchical (decentralized) case with reference to swapping in one of the sub-areas?*
- Looking into line-faults, it is compelling to see how an attacker can fool Transmission System Operators (TSO)/ Distribution System Operators (DSO) into believing that a topology change has occurred, while no such change has taken place. **RQ3** *Can targeted single-line and double-line attacks be made possible against state estimation and constructed to determine optimal attack strategies for such attacks?*
- Moreover, with transient topology changes in today's grid, it is of considerable interest to study a type of topology attack within a single measurement poll. **RQ4** *How the transient topology changes affect state estimation particularly if occurred during a single scan cycle and what is the possible trade-off between the reverse-nature sequential topology attack and its overall impact?*
- Finally, a type of state forcing attack which is initiated by topology processing is quite appealing to examine. **RQ5** *Can different phases of topology processing algorithm be explicitly demonstrated and vulnerability be spotted in respect of attacker to launch a possible state forcing topology attack?*

After giving the motivation statements and the follow-up questions, we put forward our research proposal as:
An investigation of State Estimation robustness in the face of both data and topology-driven attacks in a decentralized configuration focused on state forcing.

1.2 Main Contributions

In this thesis, we address the general problem of attack models with regards to the updated security and safety protocols in power system state estimation. As noted above, the research described in this thesis makes contributions in two specific areas within this field: data-related attacks and topology-related attacks. We enlist the main contributions as follows:

- We propose a measurement swapping attack model and critically examine the assumptions/constraints for instantiating this model, including all those previously presented for various attacks. We offer a greedy algorithm to find a re-ordering attack along with the optimization tools. This analysis reveals several practical issues with existing models including the consideration of strong assumptions against weak detection methods. We translate the measurement re-ordering attack to a three-level hierarchical infrastructure (which was already developed by Baiocco et al. in [10]) while considering the region and level-wise division and information flow.

- Topology processing and risks involved in its manipulation is an area of huge practical importance. We propose algorithmic visualisations of all the steps involved in topology processing. Understanding the vulnerability and novelty, we offer both general and induced topology faults along with the necessary and sufficient criteria for the attacker to force a certain system state. Optimization tools are used to achieve optimal attacks.

- We initiate a novel topology attack scenario as *In-cycle Topology modifications* to exploit the time interval before the next state estimation roll defining the limitations of such attack. Time constrained optimization problem is formulated to get the optimal sequential attack.

1.3 List of Publications

- Gul, A. and Wolthusen, S.: 'Measurement Re-Ordering Attacks on Power System State Estimation' in *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017 IEEE PES*, and pp. 26-29 (DOI: 10.1109/ISGTEurope.2017.8260145).
- Gul, A. and Wolthusen, S.: 'A Review on Attacks and their Countermeasures in Power System State Estimation' in *Smart Micro-Grid Systems Security and Privacy (SMGSP 2017).*
- Gul, A. and Wolthusen, S.: 'Error Propagation after Re-ordering Attacks in Hierarchical State Estimation' in *Twelfth IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Virginia, USA, March 2018.*
- Gul, A. and Wolthusen, S.: 'In-Cycle Sequential Topology Faults and Attacks: Effects on State Estimation' in *Thirteenth International Critical Infrastructures Conference (CRITIS), Lithuania, 2018.*
- Gul, A. and Wolthusen, S.: 'State Estimation under Undetectable Single and Double Line Failures' in *Innovative Smart Grid Technologies Conference (ISGT-North America), 2019.*

- Gul, A., Baiocco, A. and Wolthusen, S.: ‘State Forcing under Dynamic Topology Faults and Attacks’ (under review)

1.4 Structure of the Dissertation

The remainder of this thesis is divided into three parts:

- Part I contributes an introductory review. It consists of following two chapters.
  - Chapter 2 provides background material and covers the following topics: *an overview of power system state estimation techniques, topology processing principles, bad data detection (identification) and optimal (and continuous) power flow*.
  - Chapter 3 provides a state of art for the following topics: *state estimation, topology detection and identification, error propagation due to attacks (data and topology), Phasor Measurement Units (PMUs)* and a discussion of the shortcomings of existing state estimation, bad data detection and attack regimes.
- Part II is comprised of attacks on centralised and decentralised state estimation. This part is the author’s (my) original contribution.
  - Chapter 4 introduces a mathematical model for measurement re-ordering attack. It considers modern security measures in designing an attack model to address identified shortcomings in existing schemes. Further, it provides a detailed analysis of how re-ordering attack can be translated on hierarchical state estimation. In particular, it describes the impact of message swapping in a region of lower level on the regions of upper level(s).
  - Chapter 5 provides a detailed specification and analysis of topology attacks including *single-line, double-line and in-cycle failures*. Least cost attacks can be formulated by solving a constrained optimization problem. In addition, induced double-line faults can be designed in a way to avoid detection however causing the desirable bias. Also, it introduces in-cycle topology attacks which gives an overview of a scan cycle of the measurement taking process.
  - Chapter 6 describes in detail the algorithm of topology processing, and also gives the pseudo-codes of each of the sub-processes. Moreover, it identifies the vulnerability by formulating a state forcing attack on topology processing.
- Part III concludes the thesis by summarising the main contributions including the model limitations as well as highlighting possible areas for future work. This part of the thesis consists of a single chapter.

Chapter 2

Background

This chapter provides the background material on Power grid necessary for the remainder of the thesis. It is concerned with introducing real-time network model, network topology processing, WLS state estimator and observability analysis. It also introduces multi-area state estimation including hierarchical and distributed state estimation.

A power grid has several main elements e.g., power plant, transformer, transmission line, substation, distribution line and the distribution transformer among others. Usually, the number of elements in an actual grid varies a lot, e.g., medium-scale system model with buses on the order of 10000 and large-scale on the order of 22000 buses [74]. In general, neither grid models nor grid data are publicly available [65] however, there are various European and British grid models that are available e.g., French, Polish, Iceland and British grids respectively. For instance, Iceland network data which represents electricity transmission network of Iceland consists of 118 nodes, 206 branches and 35 generators. British grid data (GB network) represents detailed model of electricity transmission network of Great Britian (GB) which consists of 2224 nodes, 3207 branches and 394 generators [1].

The definitions of some of the elements are as follows:

- A *generating plant* is an installation that produces electric current for commercial sale.
- A *transmission line* is a pair of electrical conductors carrying an electrical signal from one place to another.
- A *Substation* transforms voltage from high to low, or the reverse, or perform any of several other important functions.
- A *transformer* is a passive electrical device that transfers electrical energy from one electrical circuit to another, or multiple circuits.

2.1 Real-Time Power Network Model

All the elements of the power grid are connected through a communication network called Smart Grid Communication Network (SGCN). SGCN is expected to carry various types of traffic that require different quality of services (QoSs) in terms of bandwidth, latency and reliability [72]. The following Table 2.1 provides typical bandwidths and delays required by different traffic types.

Figure 2.1 illustrates the conceptual reference diagram for smart grid information networks [15]. It consists of six domains such as bulk generation, transmission,

Traffic Types	Descriptions	Bandwidth	Latency
Meter Reads	Meters report energy consumption (e.g., the 15min interval reads are usually transferred every 4h)	upto 10kbps	$2 - 10$s
Demand Response (DR)	Utilities to communicate with customer device to allow customers to reduce or shift their power use during peaks	Low	0.008s
Connects and Disconnects	To connect/disconnect customers to/from the grid	Low	0.010s
Synchrophasor	The major primary measurement technologies deployed for WASA	A few 100kbps	0.008s
Substation SCADA	Periodical polling by the master to IEDs inside substation	$10 - 30$kbps	0.008s
Inter-substation communications	Emerging applications such as DER might need GOOSE communication outside substation	-	0.010s
Substation Surveillance	video site surveillance	A few Mbps	0.004s
FLIR for distribution grid	To control protection/restoration circuits	$10 - 30$kbps	0.004s
Protection for microgrids	To report to faults, isolate them and ensure that loads are not affected	-	$100ms - 10s$

Table 2.1: QoS requirements of some types of traffic in SGCN [72]

distribution, customer, operations, service providers and market. Generation stations which generate electricity and send to the transmission line. The transmission system that carries the power from generating centres to load centres through multiple substations. This network is typically operated by a Regional Transmission Operator or Independent System Operator (RTO/ISO) whose primary responsibility is to maintain stability on the electric grid by balancing generation with load across the transmission network. The distribution domain is the electrical interconnection between the transmission domain, the customer domain and the metering points for consumption, distributed storage, and distributed generation which may be arranged in a variety of structures, including radial, looped or meshed. Customer domain is the domain where electricity is consumed. Operations domain is responsible for the smooth operation of the power system.

A real-time power system model is a mixture of static data from network and snapshots of real-time measurements (phasor measurements). Static network data is related to the parameters while real-time measurements including analogue measurements and switch statuses. A real-time model is a mathematical representation

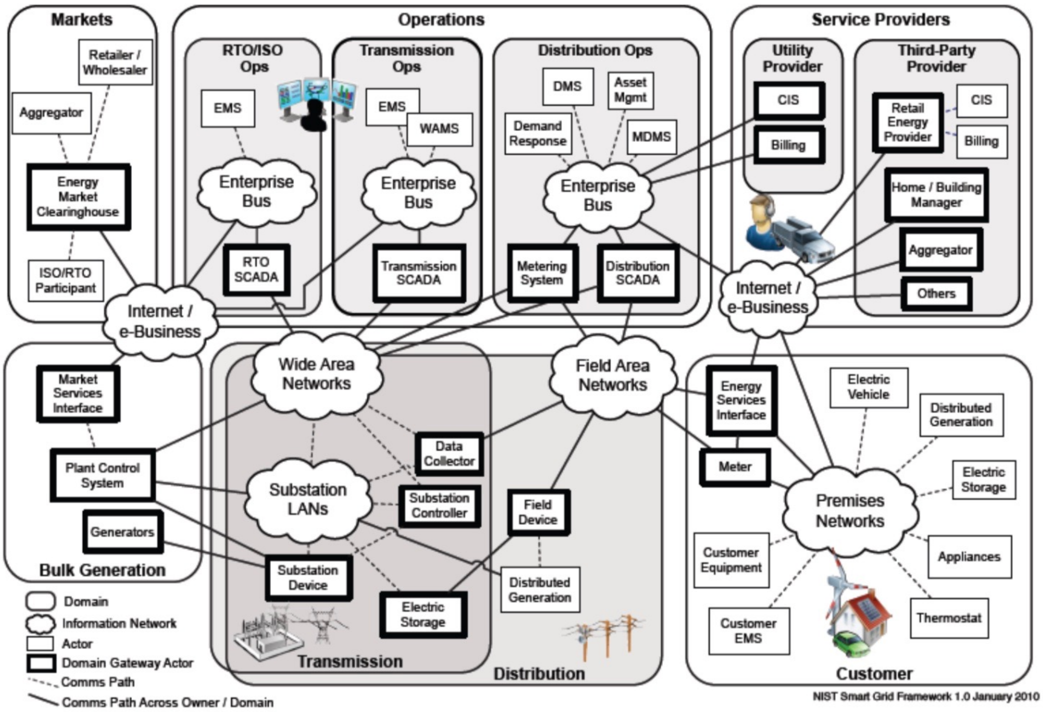

Figure 2.1: Reference Model for Power Network [15]

of the current conditions in a power network extracted at intervals from state estimation results [70]. Real-time modelling is a six-step procedure that a power network usually follows:

- data gathering
- network topology processing
- observability analysis
- state estimation
- processing of bad data and
- identification of network model.

Step 1) is data or measurement gathering assumes a bus-section/switching-device model. Steps 2) and 3) assume that the given switch status is true. Step 4) assumes the parameters to be correct as well. Step 5) processes bad data considering them as faults in analogue measurements.

Note that the above procedure does not include any security-related processes e.g., attack or malicious activities. In addition, the topic of observability analysis is not described in detail here (For details please see [16]).

As far as typical measurement size is concerned, it is 10-16 bits. As seen in Fig. 2.2 energy storage technology can be present at different locations in the power grid where electricity is generated, transported, consumed, and held in reserve (back-up). Based on the location, these storage systems can be large-scale (GW), medium-sized (MW) or micro, local (kW). The capabilities of different type energy storage systems [24] are given below:

- The bulk energy storage has capacity in GW e.g Thermal storage, Pumped hydro.
- The grid storage systems has capacity in MW e.g super capacitors, flywheel.
- The end-user storage systems has capacity in kW e.g Li-ion batteries.

The energy storage systems maintain a real-time balance between generation and load (matching supply to demand). Information processing in a power system involves primary analysis at the power plants and substations and then the secondary analysis by integrating the primary processing from throughout the network [43]. These monitoring and control functions can be summarised as supervisory control and data acquisition (SCADA). This system controls and monitors the parameters (voltage, current etc) of electric grid from a central control location through a software installed on computers which have processing capability of 2-3 Ghz. Moreover, as far as security protection capabilities are concerned, a power grid has a mixture of several protections which can be summarized and compared as follows [23]:

- **Risk management** involves machine learning and adaptive relaying etc.
- **Situational awareness and asset discovery** involves cyber and physical based anomaly detection and asset management etc.
- **Automated orchestration** involves threat informed defences and mitigation sharing etc.
- **Endpoint Protection** involves trusted systems and device fingerprints etc.
- **Boundary Protection** involves zero trust architecture and command register etc.
- **Identity-based networking** involves virtual secure enclave etc.

2.1.1 Conventional State Estimation

State estimation relies on data gathering and topology processing and the protective features that they may or may not have. The basic IEEE C37.118 and the basic IEC 61850-90-5 are the two well-known communication frameworks for synchrophasor technology [50].

2.1.1.1 IEEE C37.118

IEEE C37.118 is the improved version of IEEE 1344 which was the first available synchrophasor communication standard. It defines methods for evaluation of synchrophasor measurements, time synchronization, application of time-tags and format of messages exchanged over the network.

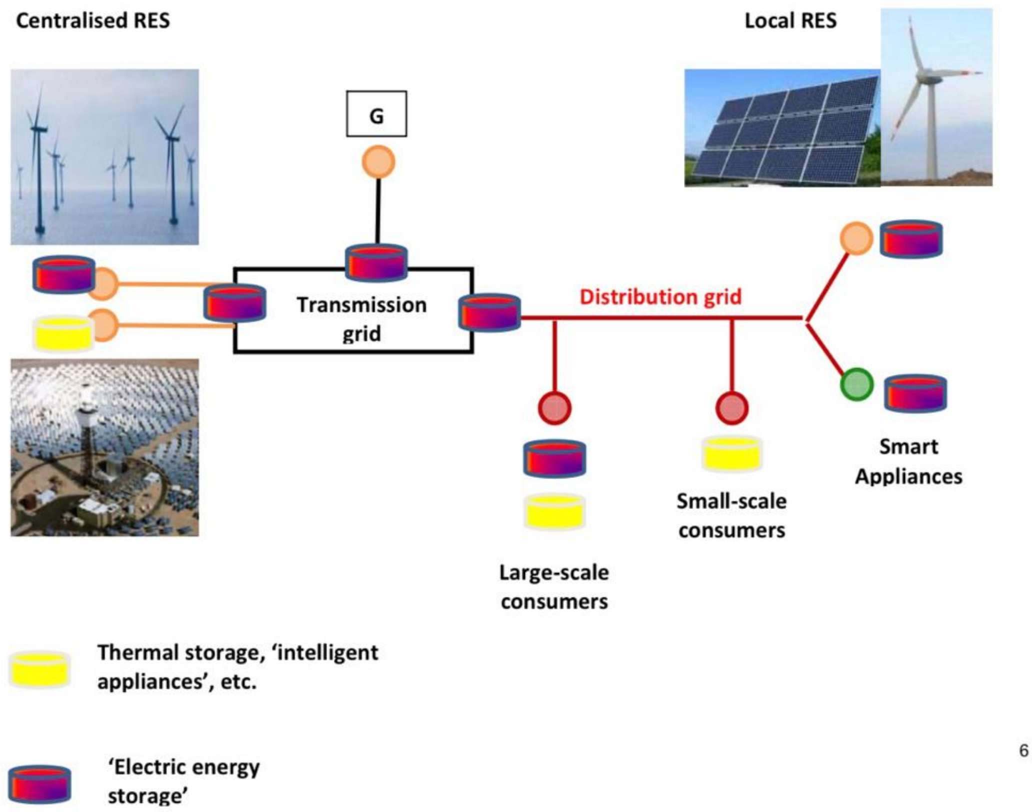

Figure 2.2: Storage capabilities of various parts of the system

Due to no encryption, eavesdropping on IEEE C37.118 traffic could reveal useful information to an attacker e.g., name and current state of substation, location of devices (PMUs, breakers etc), communication configurations etc. An attacker may launch authentication or access attack to get unauthorized access to information. Such an attack could be launched on a physical device or network traffic (by inspecting packet content). With no authentication process in IEEE C37.118, it is possible that a device assumes data is received from genuine sender but it may indeed generated by an intruder.

In addition, Man-in-the-middle MITM attack on the configuration message of IEEE C37.118 could permanently leave a receiver unable to decode upcoming data messages. Another common attack in communication system is Denial of Service (DoS) which targets availability and IEEE C37.118 is vulnerable to DoS/availability attacks.

The communication overhead indirectly reflects the maximum size of data that can be included in a single packet. It is also a factor determining how much additional channel bandwidth is required due to overhead information. High communication overhead for synchrophasor applications which involve high data transmission rates significantly increases the channel bandwidth requirement. Note that the communication overhead for IEEE C37.118 is significantly high. IEEE C37.118

data messages are very compact in size due to reporting configuration/decoding information separately in infrequent configuration message, resulting in much lower bandwidth requirement.

2.1.1.2 IEC 61850-90-5

IEC 61850-90-5 is derived from IEC 61850 which was initially proposed for substation automation. IEC 61850 is a complete communication system that addresses modeling of power system components, abstraction of services and communication protocols and methods.

IEC 61850-90-5 is protected against unauthorized access attacks as security credentials are only known to authorized devices (assuming that communicating devices are secure). Re-ordering attack stores network traffic between communicating peers and replays it to the receiver to hide real time status of the sender (e.g., power system). The outdated replayed packets will leave receiver unintentionally performing wrong decisions. Replay/reflection attacks could be launched on both, unencrypted (e.g., IEEE C37.118) as well as encrypted (e.g., IEC 61850-90-5) traffic.

Furthermore, IEC 61850-90-5 based communication is protected against MITM attacks due to encryption. As far as DoS are concerned, IEC 61850-90-5 is vulnerable to DoS/availability attacks. However, it could be mitigated to some degree in IEC 61850- 90-5 communication.

The overhead is relatively low for IEC 61850-90-5. It has high bandwidth requirement because of the fact that IEC 61850-90-5 has large packet size due to metadata and carrying complete decoding information in each packet.

2.1.2 Node Capabilities

In the traditional grid like in 1980s, the measurement cycle (e.g, voltage, current, phase are collected and) was measured in minutes. State estimation was done on the order of once every couple of minutes. In such scenario, node capabilities stopped really mattering. In other words in a conventional grid where you did not have PMUs or the need to co-ordinate (and then run state estimation frequently), the requirements were just very different. This was developed in the early 1970s and at that time, state estimation calculations were still demanding on the system running the state estimator, and communication requirements had to be satisfied over slow links. Now (with aggressive use of PMUs), communication and computational requirements went up several orders of magnitude.

2.1.2.1 SCADA node

Supervisory control is a general term for a high-level of overall control of many individual controllers or multiple control loops. It gives the operations supervisor an overview of the plant process and permits integration of operation between low-level controllers [4]. Whereas, Data acquisition is the process of sampling signals by measuring a physical property of the real world in the form of signals and converting it from analog waveform into digital numeric values so that it can be processed by computing machines. Following are the minimum system requirements to host SCADA [2]:

- 1.5 GHz processor; recommended: 2.4 GHz multi-core processor
- 1 GB RAM; recommended: 4GB RAM
- Windows 7 or higher (not Embedded Compact)
- Microsoft .NET 4.0 Framework

2.1.2.2 EMS node

An energy management system (EMS) is a system of computer-aided tools used by operators of electric grids to monitor, control, and optimize the performance of the generation or transmission system. Also, it can be used in small scale systems like microgrids.

2.1.2.3 Sensor node

Recently, the difference came when you have a network full of PMUs. In case of PMUs, there are some requirements like reliable timestamps and they have the capability to send these messages either by IEEE C37 or IEC 61850 protocol. The choice of the protocol matters because the communication overhead you are producing depends on the protocol [50]. For example, if I sent you a message that is cyrptographically protected, on the sender side, no problem but if the receiver has to do the decryption and verification not for just one sensor but thousands of them. As currently utilities are putting PMUs quite aggressively in their network mainly because of the cost (as the cost of PMUs has gone down may be by the factor between 20-50). In other words, you can put PMUs in a lot more places inside your network therefore getting a precise state estimate. But the flip side is that now all these sensors will now produce a much greater volume of traffic of values that need to be processed and fed into state estimator. In a European network, these measurements will come in up to every $1/50$th of a second (20ms) because it is fairly common to take these measurements at a maximum speed of the grid frequency i.e., 50 Hz. You can take them less frequently but that will be a kind or worst case estimate i.e, every PMU generates messages of the order of few hundreds of bytes (in size) and does that every 20ms that means the recipient will now have 20ms to receive and process this message feeded into the state estimator and now you multiply that with however many units you have. Even so, that is not much of a concern when you have e.g., 20-25 PMUs spread throughout the network but when you multiply that with a 1000 or 5000, then you are certainly talking about an awful lot of messages that need to be processed. Certainly, the EMS that is running state estimator, the pressure isn't so much coming from running the state estimation algorithm but also the pressure of handling the measurements.

2.1.3 Storage Capabilities

Actually, for the state estimator, a relatively limited time horizon is needed and no need to retain a huge amount of history. As far as storage capabilities are concerned, we only need a sliding time window to retain messages and not storage upto even day(s), say for example to detect re-ordering attacks, we will be interested in keeping the packet history in a certain window while no need to retain of what happened yesterday.

2.1.4 Processing Capabilities

As per processing capabilities, state estimation algorithm has the influence of the size of the measurement matrix, the more PMUs you have, the larger the matrix. Therefore, computationally more complex in addition to the topology processing and all that worst case scenario every 20ms.

Real-time power network modelling in conventional state estimation has two components i.e., 1. processing of topological data (switching device statuses) and 2. processing of analogue data (power flow, power injection, voltage measurements etc.). The first phase involves the processing of switch-status data using a bus-section/ switching-device network model. In a conventional setting, the next tasks including state estimation consider system topology to be known.

2.1.5 Generalised State Estimation

There is no definite dividing line between logical and analogue data processing in generalised state estimation. Rather, it often estimates some parts of topology and even network parameters. In the case of topology faults, this type of precise switch status modelling helps bad data analysis to detect/identify errors.

This case also includes measurements on zero impedance branches and switches due to the parts of the network model being at the physical level. These new measurements are called pseudo-measurements and the additional state variables will be augmented with the conventional state vector. Pseudo-measurements will be added in both the cases of switch status being open or closed but will be ignored if it is unknown. *There can be conditions where wrong switch status affects state estimation results.* In such situations, it is more desirable to consider that status as unknown.

2.2 Topology Processing

A network topology processor (NTP) is the pre-requisite in state estimation. It is responsible for the first stage of data processing and to determine the connectivity and the location of the metering devices in the system. The main function of an NTP is to transform the bus-section/switching device model to bus/branch model and to allocate metering devices to the parts of the new model. Topology processing can be performed either by a *conventional method* or *generalized method*. Conventional topology processing is performed before other functions like state estimation and bad data analysis. On the other hand, generalized topology processing can be considered as an on-line approach that sends the topology information in parallel with the other measurement data for state estimation [70]. Generalised topology processing involves one task in addition to the basic functions of conventional one i.e., to identify extended islands. This will help to represent the open switching devices in the database more explicitly. This way, suspected and unknown statuses can be identified and help in processing bad data.

Converting raw analogue measurements into appropriate units is the first task of the network topology processor. Next task includes simple tests and checks i.e. verifying operating limits, validating non-zero flows in open switches and non-zero voltage differences across closed switching devices. Assuming that the switching data is correct, initially, a bus-section/switching-device model is considered and data is gathered for topology processing. Then the state estimator assumes the topology to be correct and carry on with estimating the states and detecting/identifying bad data. Recently, there is quite a number of papers addressing topology processing with distinct perspectives including [55] where the authors studied topology processing in distribution systems and [34] where the topology processing itself is explicitly described.

2.3 State Estimation

State Estimation is the core function in the control centre of the power systems. State estimator evaluates the most likely state of the system by filtering and processing the measurements from the RTUs installed in the system via transmission lines, In this section, two well-known methods to solve the state estimation problem will be discussed briefly, which are Weighted Least Square (WLS) Method and Weighted Least Absolute Value (WLAV) Method. Other methods are stated in Section 3.1.

2.3.1 Weighted Least Square (WLS) State Estimation

The well-known WLS approximation involves solving a non-linear set of equations relating measurements and state variables (voltage magnitudes and phase angles) by minimizing the summation of squares of residuals. Consider the non-linear measurement model as,

$$\mathbf{z} = h(\mathbf{x}) + \mathbf{e} \tag{2.1}$$

where z is the vector of measurements (m vector), x is the state vector (n vector, and $m > n$), $h(.)$ is usually a non-linear function relating measurements to the states and $\mathbf{e}$ is the vector of measurement errors having zero mean and known co-variance, which is denoted by $\mathbf{R}$. The errors are assumed to be independent, therefore, $\mathbf{R}$ is a diagonal matrix.

$$Cov(\mathbf{e}) = \mathbf{R} = diag\{\sigma_1^2, \sigma_2^2, \cdots, \sigma_m^2\} \tag{2.2}$$

Now, the objective function will be given as

$$J(\mathbf{x}) = \sum_{i=1}^{m} (\mathbf{z}_i - h_i(\mathbf{x}))^2 / \mathbf{R}_{ii} = [\mathbf{z} - h(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z} - h(\mathbf{x})] \tag{2.3}$$

which is to be minimized and the first-order optimality condition is

$$g(\mathbf{x}) = \frac{\partial J(\mathbf{x})}{\partial \mathbf{x}} = -\mathbf{H}^T(\mathbf{x}) \mathbf{R}^{-1} [\mathbf{z} - h(\mathbf{x})] = 0 \tag{2.4}$$

Where $\mathbf{H}(\mathbf{x}) = \partial h(\mathbf{x}) / \partial \mathbf{x}$. After expanding $g(\mathbf{x})$ with Taylor series and writing the relation of $k+1$ iteration in terms of k^{th} iteration

$$\mathbf{x}^{k+1} = \mathbf{x}^k - \mathbf{G}(\mathbf{x}^k)^{-1} g(\mathbf{x}^k) \tag{2.5}$$

Where $\mathbf{G}(\mathbf{x})$ is the Gain matrix

$$\mathbf{G}(\mathbf{x}^k) = \frac{\partial g(\mathbf{x}^k)}{\partial \mathbf{x}} = \mathbf{H}^T(\mathbf{x}^k)\mathbf{R}^{-1}\mathbf{H}(\mathbf{x}^k) \tag{2.6}$$

With the help of the above three equations, the normal equation to solve the state estimation problem will be

$$\mathbf{G}(\mathbf{x}^k)\Delta\mathbf{x}^{k+1} = \mathbf{H}^T(\mathbf{x}^k)\mathbf{R}^{-1}(\mathbf{z} - h(\mathbf{x}^k)) \tag{2.7}$$

Where $\Delta\mathbf{x}^{k+1} = \mathbf{x}^{k+1} - \mathbf{x}^k$.

We can summarize this method by a simple algorithm.

- Initialize the state vector $\mathbf{x}^k$ for $k = 0$ and get the measurement function $h(\mathbf{x})$.
- Calculate the Jacobian $\mathbf{H}(\mathbf{x})$ and the gain matrix $\mathbf{G}(\mathbf{x})$ from Eq. (2.3).
- Determine the right-hand side of normal Eq. (2.4) and solve it for $\Delta\mathbf{x}^k$
- Check for convergence, $\mid \Delta\mathbf{x}^k \mid \leq \epsilon$.
- If not converged, update $\mathbf{x}^{k+1} = \mathbf{x}^k + \Delta\mathbf{x}^k$ and get a new $h(\mathbf{x})$ and repeat the above procedure.

It is assumed that now the reader has a rigorous view of the state estimation. Before going into the details of the procedures, some definitions are worth mentioning:

Definition 2.1 (Energy Management System (EMS) [68])
An energy management system is usually a collection of computer-aided tools used by operators of electric facilities to monitor, control, and optimize the performance of the generation and/or transmission system. Different computer aided tools are implemented from short time control modules to scheduling or commitment of power production units on a day/week basis.

Definition 2.2 (Supervisory Control And Data Acquisition (SCADA))
Supervisory Control And Data Acquisition (SCADA) is a system for remote monitoring and control that operates with coded signals over communication channels (using typically one communication channel per remote station).

Definition 2.3 (Remote Terminal Units (RTUs))
Remote Terminal Units (RTUs) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.

Definition 2.4 (Intelligent Electronic Devices (IEDs))
Intelligent Electronic Devices (IEDs) are the devices incorporating one or more processors with the capability to receive or send data/control signals from or to an external source (e.g., electronic multi-function meters, digital relays, controllers) [33].

Definition 2.5 (Phasor Measurement Units (PMUs))
Phasor Measurement Units (PMUs) are the devices that measure voltage and current magnitudes using a global positioning system (GPS) reference source for synchronization with an accuracy of 1μ second. The resultant time-tagged phasors can be transmitted to a local or remote receiver at rates up to 60 samples per second [33].

For giving more transparency, the network model and the method to construct $h(\mathbf{x}^k)$ and $\mathbf{H}(\mathbf{x}^k)$ is as follows:

2.3.1.1 Network Model

We can model the entire power network if we start from the line data information. First, by writing the nodal equations for each bus from Kirchhoff's current law being applied on each bus. Net current injection and net voltage phasors are denoted by $\mathbf{I}$ and $\mathbf{V}$ respectively and nodal equations will become

$$\mathbf{I} = \begin{bmatrix} i_1 \\ \vdots \\ i_N \end{bmatrix} = \begin{bmatrix} Y_{11} & \cdots & Y_{1N} \\ \vdots & \ldots & \vdots \\ Y_{N1} & \cdots & Y_{NN} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_N \end{bmatrix} = \mathbf{Y}\bar{\mathbf{V}} \tag{2.8}$$

where i_k and v_k is the current injection and voltage phasor at bus k respectively. Each element of the admittance matrix $\mathbf{Y}$ is denoted by Y_{km}. In general, bus admittance matrix is complex i.e., it is of the form $\mathbf{G} + j\mathbf{B}$.

Each entry of Y can be derived from scratch by using one branch at a time by these equations,

$$\begin{aligned} Y_{kk} &= Y_{kk} + y_{km}/|a|^2 \\ Y_{km} &= Y_{km} - y_{km}/a* \\ Y_{mk} &= Y_{mk} - y_{km}/a \\ Y_{mm} &= Y_{mm} + y_{km} \end{aligned} \tag{2.9}$$

where y_{km} is the line series admittance of the branch (k,m) and a is off-nominal tap ratio which is considered as complex.

2.3.1.2 The measurement function $h(x^k)$

The measured quantities include real and reactive power injection P_i and Q_i at each bus i, real and reactive power flow P_{ij} and Q_{ij} and the line current flow I_{ij} from every bus i to bus j. They are related to the state variables as

$$P_i = V_i \sum_{i \neq j} V_j (G_{ij} cos\theta_{ij} + B_{ij} sin\theta_{ij}) \tag{2.10}$$

$$Q_i = V_i \sum_{i \neq j} V_j (G_{ij} sin\theta_{ij} + B_{ij} cos\theta_{ij}) \tag{2.11}$$

$$P_{ij} = V_i^2 (g_{si} + g_{ij}) - V_i V_j (g_{ij} cos\theta_{ij} + b_{ij} sin\theta_{ij}) \tag{2.12}$$

$$Q_{ij} = -V_i^2 (b_{si} + b_{ij}) - V_i V_j (g_{ij} sin\theta_{ij} - b_{ij} cos\theta_{ij}) \tag{2.13}$$

$$I_{ij} = \sqrt{P_{ij}^2 + Q_{ij}^2 / V_i} \tag{2.14}$$

Where in the above relations, V_i is the voltage magnitude at bus i,
θ_i is the phase angle at bus i, $\theta_{ij} = \theta_i - \theta_j$,
$G_{ij} + jB_{ij}$ is the ijth element of the admittance matrix,
$g_{ij} + jb_{ij}$ is the admittance of the series branch between buses i and j
and $g_{sj} + jb_{sj}$ is the admittance of the shunt branch at bus i.

2.3.1.3 The measurement Jacobian H

The Jacobian matrix **H** can be written as

$$\mathbf{H} = \begin{bmatrix} \frac{\partial P_{inj}}{\partial \theta} & \frac{\partial P_{inj}}{\partial V} \\ \frac{\partial P_{flow}}{\partial \theta} & \frac{\partial P_{flow}}{\partial V} \\ \frac{\partial Q_{inj}}{\partial \theta} & \frac{\partial Q_{inj}}{\partial V} \\ \frac{\partial Q_{flow}}{\partial \theta} & \frac{\partial Q_{flow}}{\partial V} \\ \frac{\partial I_{mag}}{\partial \theta} & \frac{\partial I_{mag}}{\partial V} \\ 0 & \frac{\partial V_{mag}}{\partial V} \end{bmatrix} \tag{2.15}$$

Where in each block

- the expressions corresponding to P_i (real power injection):

$$\frac{\partial P_i}{\partial \theta_i} = \sum_{j=1}^{N} V_i V_j (-G_{ij} sin\theta_{ij} + B_{ij} cos\theta_{ij}) - V_i^2 B_{ii} \tag{2.16}$$

$$\frac{\partial P_i}{\partial \theta_j} = V_i V_j (G_{ij} sin\theta_{ij} - B_{ij} cos\theta_{ij}) \tag{2.17}$$

$$\frac{\partial P_i}{\partial V_i} = \sum_{j=1}^{N} V_j (G_{ij} cos\theta_{ij} + B_{ij} sin\theta_{ij}) + V_i G_{ii} \tag{2.18}$$

$$\frac{\partial P_i}{\partial V_j} = V_i (G_{ij} cos\theta_{ij} + B_{ij} sin\theta_{ij}) \tag{2.19}$$

- the expressions corresponding to Q_i (reactive power injection):

$$\frac{\partial Q_i}{\partial \theta_i} = \sum_{j=1}^{N} V_i V_j (G_{ij} cos\theta_{ij} + B_{ij} sin\theta_{ij}) - V_i^2 G_{ii} \tag{2.20}$$

$$\frac{\partial Q_i}{\partial \theta_j} = V_i V_j (-G_{ij} cos\theta_{ij} - B_{ij} sin\theta_{ij}) \tag{2.21}$$

$$\frac{\partial Q_i}{\partial V_i} = \sum_{j=1}^{N} V_j (G_{ij} sin\theta_{ij} - B_{ij} cos\theta_{ij}) - V_i B_{ii} \tag{2.22}$$

$$\frac{\partial Q_i}{\partial V_j} = V_i (G_{ij} sin\theta_{ij} - B_{ij} cos\theta_{ij}) \tag{2.23}$$

- the expressions corresponding to P_{ij} (real power flow):

$$\frac{\partial P_{ij}}{\partial \theta_i} = V_i V_j (g_{ij} sin\theta_{ij} - b_{ij} cos\theta_{ij}) \tag{2.24}$$

$$\frac{\partial P_{ij}}{\partial \theta_j} = -V_i V_j (g_{ij} sin\theta_{ij} - b_{ij} cos\theta_{ij}) \tag{2.25}$$

$$\frac{\partial P_{ij}}{\partial V_i} = -V_j (g_{ij} cos\theta_{ij} + b_{ij} sin\theta_{ij}) + 2(g_{ij} + g_{si}) V_i \tag{2.26}$$

$$\frac{\partial P_{ij}}{\partial V_j} = -V_i (g_{ij} cos\theta_{ij} + b_{ij} sin\theta_{ij}) \tag{2.27}$$

- the expressions corresponding to Q_{ij} (reactive power flow):

$$\frac{\partial Q_{ij}}{\partial \theta_i} = -V_i V_j (g_{ij} cos\theta_{ij} + b_{ij} sin\theta_{ij}) \tag{2.28}$$

$$\frac{\partial Q_{ij}}{\partial \theta_j} = V_i V_j (g_{ij} cos\theta_{ij} + b_{ij} sin\theta_{ij}) \tag{2.29}$$

$$\frac{\partial Q_{ij}}{\partial V_i} = -V_j (g_{ij} sin\theta_{ij} - b_{ij} cos\theta_{ij}) - 2(b_{ij} + b_{si}) V_i \tag{2.30}$$

$$\frac{\partial Q_{ij}}{\partial V_j} = -V_i (g_{ij} sin\theta_{ij} - b_{ij} cos\theta_{ij}) \tag{2.31}$$

- the expressions corresponding to V_i (voltage magnitude):

$$\frac{\partial V_i}{\partial V_i} = 1, \quad \frac{\partial V_i}{\partial V_j} = 0 \tag{2.32}$$

$$\frac{\partial V_i}{\partial \theta_i} = 0, \quad \frac{\partial V_i}{\partial \theta_j} = 0 \tag{2.33}$$

- the expressions corresponding to I_{ij} (current magnitude)

$$\frac{\partial I_{ij}}{\partial \theta_i} = \frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} V_i V_j sin\theta_{ij} \tag{2.34}$$

$$\frac{\partial I_{ij}}{\partial \theta_j} = -\frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} V_i V_j sin\theta_{ij} \tag{2.35}$$

$$\frac{\partial I_{ij}}{\partial V_i} = \frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} (V_i - V_j cos\theta_{ij}) \tag{2.36}$$

$$\frac{\partial I_{ij}}{\partial V_j} = \frac{g_{ij}^2 + b_{ij}^2}{I_{ij}} (V_j - V_i cos\theta_{ij}) \tag{2.37}$$

Example 1 Consider a 3-bus power system shown in Fig. 2.3. The network data are presented in the table below. □

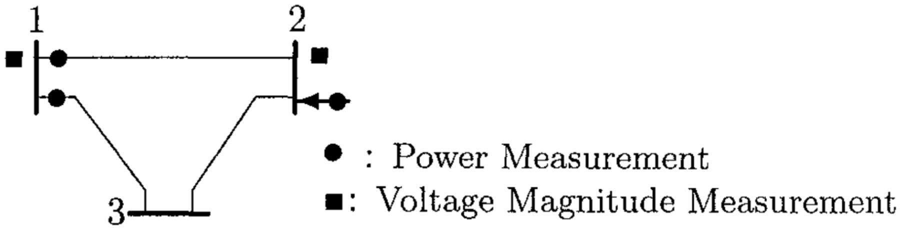

Figure 2.3: one-line diagram and measurement configuration of a 3-bus power system [4]

Line (from bus)	Line (to bus)	Resistance $R(pu)$	Reactance $X(pu)$	Total Susceptance $2b_s(pu)$
1	2	p_{12}	0.888	0.008
1	3	p_{13}	1.173	0.008
2	3	p_2	-0.501	0.010

The system is monitored by 8 measurements and hence $m = 8$ in Equation 2.3.1. Measurement values and their associated error standard deviations $\sqrt{R_{ii}} = \sigma_i$, are given as:

Measurement, i	Type	Value (pu)	$\sqrt{R_{ii}}$
1	p_{12}	0.888	0.008
2	p_{13}	1.173	0.008
3	p_2	-0.501	0.010
4	q_{12}	0.568	0.008
5	q_{13}	0.663	0.008
6	q_2	-0.286	0.010
7	V_1	1.006	0.004
8	V_2	0.968	0.004

The state vector $\mathbf{x}$ will have 5 elements in this case $(n = 5)$,

$$\mathbf{x} = [\theta_2, \theta_3, V_1, V_2, V_3] \tag{2.38}$$

$\theta_1 = 0$ is chosen as the arbitrary reference angle. Assume flat start conditions, where the state vector is equal to:

$$\mathbf{x}^0 = \begin{array}{c} \theta_2 \\ \theta_3 \\ V_1 \\ V_2 \\ V_3 \end{array} \begin{bmatrix} 0 \\ 0 \\ 1.0 \\ 1.0 \\ 1.0 \end{bmatrix}$$

Then, the measurement Jacobian can be evaluated as follows, using the expression already given above:

$$\mathbf{H}(x)^0 = \begin{array}{r} \partial p_{12} \\ \partial p_{13} \\ \partial p_2 \\ \partial q_{12} \\ \partial q_{13} \\ \partial q_2 \\ \partial V_1 \\ \partial V_2 \end{array} \left[\begin{array}{cc|ccc} -30.0 & & 10.0 & -10.0 & \\ & -17.2 & 6.9 & & -6.9 \\ 40.9 & -10.9 & -10.0 & 14.1 & -4.1 \\ \hline 10.0 & & 30.0 & -30.0 & \\ & 6.9 & 17.2 & & -17.2 \\ -14.1 & 4.1 & -30.0 & 40.9 & -10.9 \\ & & 1.0 & & \\ & & & 1.0 & \end{array}\right]$$

Note that the dimension of **H** is 8×5, and it is a sparse matrix. Its sparsity becomes more pronounced for large scale systems where the number of nonzeros per row stays fairly constant, irrespective of the system size. Next, Gain matrix $\mathbf{G}(x)_0$ will be obtained as follows:

$$\mathbf{G}(x)^0 = \; 10^7 \left[\begin{array}{cc|ccc} 3.4392 & -0.5068 & 0.0137 & & -0.0137 \\ -0.5068 & 0.6758 & -0.0137 & 0.0137 & 0.0000 \\ \hline 0.0137 & -0.0137 & 3.1075 & -2.9324 & -0.1689 \\ & 0.0137 & -2.9324 & 3.4455 & -0.5068 \\ -0.0137 & 0.000 & -0.1689 & -0.5068 & 0.6758 \end{array}\right]$$

Gain matrix is 5×5, symmetric and less sparse than the corresponding Jacobian $\mathbf{H}_0$. Its eignvalues can be computed as

$$\mathbf{x}^0 = 10^7 \begin{bmatrix} 3.5293 \\ 6.2254 \\ 0.5857 \\ 0.9992 \\ 0.0042 \end{bmatrix}$$

confirming that it is positive definite. Cholesky decomposition of the gain matrix $\mathbf{G}(x^0)$ is given as follows:

$$\mathbf{G}(x^0) = \mathbf{L}\mathbf{L}^T$$

where:

$$\mathbf{L} = 10^3 \begin{bmatrix} 5.8645 & 0 & 0 & 0 & 0 \\ -0.8643 & 2.4517 & 0 & 0 & 0 \\ 0.0234 & -0.0476 & 5.5743 & 0 & 0 \\ -0.000 & 0.0559 & -5.2600 & 2.6045 & 0 \\ -0.0234 & -0.0082 & -0.03030 & -2.5579 & 0.3503 \end{bmatrix}$$

Triangular factors of **G** are not unique and their sparsity depends heavily on the way the decomposition is carried out. Consider the iterative solution of the WLS state estimation problem for the system and applying the algorithm described in section 2.3.1, the state vector can be solved iteratively. The convergence criteria will be chosen as $10^{-}4$ for the state variable updates. Starting from the flat start, and using the jacobian and gain matrices as above, the solution is obtained in 3

iterations. The convergence summary for the objective function $J(x^k)$ and the state updates Δx^k are given in the below table.

Iterations, k	1	2	3
$\Delta\theta_2^k$	$-2.10e-2$	$-6.00e-4$	$-0.02e-5$
$\Delta\theta_3^k$	$-4.52e-2$	$-2.70e-3$	$2.81e-6$
ΔV_1^k	$3.00e-4$	$-1.09e-4$	$-1.65e-6$
ΔV_2^k	$-2.57e-2$	$-1.06e-4$	$-1.63e-6$
ΔV_3^k	$-5.72e-2$	$1.15e-3$	$1.87e-6$
Objective function, $J(x^k)$	$49,123$	59.6	8.6

The algorithm converges to the following state estimation solution:

Bus i	$\hat{\mathbf{V}}_i$ (pu)	$\hat{\theta}_i$ (degrees)
1	0.9996	0.0000
2	0.9742	-1.2475
3	0.9439	-2.7457

Finally, we can also compute the estimated measurements and their residual vector given by:

$$\mathbf{r} = \mathbf{z} - h(\mathbf{x})$$

These values are shown below:

Measurement No. i	Type	Measured Value (pu)	Estimated Value (pu)	Residual (pu)
1	p_{12}	0.888	0.8930	-0.0050
2	p_{13}	1.173	1.1711	0.0019
3	p_2	-0.501	-0.4959	-0.0051
4	q_{12}	0.568	0.5588	0.0092
5	q_{13}	0.663	0.6677	-0.0047
6	q_2	-0.286	-0.2977	0.0117
7	V_1	1.006	0.9996	-0.0064
8	V_2	0.968	0.9742	-0.0062

The gain matrix $\mathbf{G}$ evaluated in the 3rd iteration is given by:

$$\mathbf{G}(x)^3 = \ 10^7 \left[\begin{array}{cc|ccc} 3.2086 & -0.4472 & -0.0698 & & -0.0 \\ -0.5068 & 0.6758 & -0.0137 & 0.0137 & 0.0000 \\ \hline -0.0698 & -0.0451 & 3.2011 & -2.8862 & -0.2160 \\ -0.0314 & 0.0045 & -2.8862 & 3.3105 & -0.4760 \\ 0.0038 & 0.000 & -0.2160 & -0.4760 & 0.6684 \end{array}\right]$$

Note that this matrix is not very different from the initial $G(x^0)$ matrix evaluated as a flat start. While there are exceptions, in general, the gain matrix elements do not change significantly during the iterative solution procedure.

2.3.2 Weighted Least Absolute Value (WLAV) State Estimation

The very famous and comparable alternative to WLS estimation is the approach of WLAV estimation. The problem in WLAV estimation can be framed as a Linear Programming (LP) problem, which is then solvable by utilizing one of the well known LP solution methods. LP based solution methodologies for WLAV estimation problems were first proposed in 1978. In this section, first of all, we formulate the LAV estimation problem, then we demonstrate how it can be seen as an LP problem and in the end, two eminent strategies, namely simplex and interior point methods are briefly explained. Consider the linear regression model given below [4]:

$$\mathbf{z}_i = \mathbf{A}_i^T\mathbf{x} + \mathbf{e}_i \tag{2.39}$$

where $\mathbf{z}_i$ is the vector of measurements, which is linearly dependant on $\mathbf{x}$, which is the state vector which is to be determined, A, set of vectors and the measurement error $\mathbf{e}$. Now, the least absolute value estimate (LAV) $\hat{\mathbf{x}}$ for the unknown state vector $\mathbf{x}$ is given by the following minimization problem

$$\begin{aligned} &\text{Minimize} \quad \mathbf{c}^T \mid \mathbf{r} \mid \\ &\text{Subject to} \quad \mathbf{z} - \mathbf{A}\mathbf{x} = \mathbf{r} \end{aligned} \tag{2.40}$$

Where $\mathbf{c} \in R^m$ is a vector with all entries as 1 and $\mathbf{r} \in R^m$ is the vector of measurement residuals.

In a simple one dimensional case, a sample median is considered as the LAV estimate.

2.3.2.1 LAV Problem as an LP Problem

The LAV problem given in Eqs. (2.35) and (2.36) can be seen as a linear programming LP problem. Therefore, first, we will formulate the LAV problem as an LP problem and then solve it using one of the well-established techniques of LP methods.

Let ξ_i is defined such that,

$$\mid r_i \mid \leq \xi_i, \quad 1 \leq i \leq m$$

and if we introduce two slack variables l_i and k_i, and replace the above inequality by

$$r_i - l_i = -\xi_i$$

$$r_i + k_i = \xi_i$$

Let us now consider 4 new variables x_i^u, x_i^v, u_i and v_i such that

$$x_i = x_i^u - x_i^v$$

$$r_r = u_i - v_i$$

$$u_i = \frac{1}{2}l_i$$

$$v_i = \frac{1}{2}k_i$$

and Eq. (2.35) can be rewritten as

$$\mathbf{z}_i = \{\sum_{j=1}^{n}[A_{ij}x_j^u - A_{ij}x_j^v]\} + u_i - v_i, \quad 1 \le i \le m \tag{2.41}$$

Note that the term $\mid r_i \mid$ in the objective function in Eq. (2.36) can be replaced by ξ_i in terms of new variables [4]

$$\xi_i = u_i + v_i \tag{2.42}$$

Then, the optimization problem in Eq. (2.36) can be formulated as the following linear programming problem

$$\begin{aligned} &\text{Minimize} \quad \sum_{i=1}^{m}[u_i + v_i] \\ &\text{Subject to} \quad \sum_{j=1}^{n} A_{ij}(u_i + v_j) = -u_i + v_i + z_i, \ \ 1 \le j \le m \end{aligned} \tag{2.43}$$

$$x_j^u, x_j^v \geqslant 0, \ \ 1 \le j \le n \tag{2.44}$$

$$u_i, v_i \geqslant 0, \ \ 1 \le i \le m \tag{2.45}$$

2.3.3 Kalman Filter for State Estimation

In wide-area control applications, dynamic state estimation is important. Along with system states, other variables need to be accurately and precisely estimated for reliable operation of a power system. These variables can be rotor angle and speed among others. For such cases, Kalman Filter (both extended and unscented one) is widely used. An Ensemble Kalman Filter is proposed for power distribution system state estimation which uses previous estimates to enhance the accuracy of the present ones [22]. Based on Extended and Unscented Kalman filters, a new filter is introduced to improve the performance of dynamic power system state estimation [18].

2.3.3.1 Extended Kalman Filter (EKF) Algorithm

EKF is a recursive state estimation algorithm for non-linear systems. This method involves a minimization problem of squared error covariance between real and estimated states. A general non-linear state and measurement equations are as follows (please see [89] for the complete process)

$$\begin{aligned} \mathbf{x}_{k+1} =& f_k(\mathbf{x}_k, \mathbf{u}_k, w_k) \\ \mathbf{y}_{k+1} =& h_{k+1}(\mathbf{x}_{k+1}, \mathbf{v}_{k+1}) \\ \mathbf{w}_k \sim& (0, \mathbf{Q}_k) \\ \mathbf{v}_k \sim& (0, \mathbf{R}_k) \end{aligned} \tag{2.46}$$

where $\mathbf{x}_{k+1}$ be the state vector, $\mathbf{u}_k$ be the input vector, f be the non-linear function, $\mathbf{y}_{k+1}$ be the output vector, $\mathbf{w_k}$, $\mathbf{v_k}$ be the (state and measurement) noise and $\mathbf{Q_k}$, $\mathbf{R_k}$ be the respective covariances. Usually EKF regime has two main steps: time update equations and measurement equations.

A non-linear system solution by EKF has the following stages:

1. Filter initialization
2. Partial derivative matrices of system equations
3. Time update
4. partial derivative matrices of output equations
5. Measurement update

The above steps of EKF can be seen as:

- The filter initialization is as follows

$$\hat{\mathbf{x}}_0^+ = E(\mathbf{x}_0) \tag{2.47}$$

$$P_0^+ = E[(\mathbf{x}_0 - \hat{\mathbf{x}}_0^+)(\mathbf{x}_0 - \hat{\mathbf{x}}_0^+)^T] \tag{2.48}$$

  where $\hat{\mathbf{x}}_{k+1}$ is a priori state estimate at step $k+1$ given knowledge of the process prior to this step, $\hat{\mathbf{x}}_{k+1}^+$ is a posteriori state estimate at step $k+1$ given measurement $\mathbf{y}_{k+1}$,$\mathbf{P}_{k+1}^-$ and $\mathbf{P}_{k+1}^+$ is the a-priori and a-posteriori estimate error covariance, $\mathbf{F}_k$ is the Jacobian matrix of f with respect to X, and $\mathbf{K}_{k+1}$ is the Kalman gain that minimizes the error covariance. For $k = 1, 2, 3, \cdots, n$ the following stages are performed.

- Partial derivative matrices of system equations are the following:

$$\mathbf{F}_k = \left.\frac{\partial f_k}{\partial X}\right|_{\hat{\mathbf{x}}_k^+} \tag{2.49}$$

$$\mathbf{L}_k = \left.\frac{\partial f_k}{\partial \mathbf{w}}\right|_{\hat{\mathbf{x}}_k^+} \tag{2.50}$$

- Time update equations are as follows:

$$\mathbf{P}_{k+1}^- = \mathbf{F}_k \mathbf{P}_k^+ \mathbf{F}_k^T + \mathbf{L}_k \mathbf{Q}_k \mathbf{L}_k^T \tag{2.51}$$

$$\hat{\mathbf{x}}_{k+1}^- = f_k(\hat{\mathbf{x}}_k^+, \mathbf{u}_k, 0) \tag{2.52}$$

- Partial derivative matrices of output equations can be obtained as follows:

$$\mathbf{H}_{k+1} = \left.\frac{\partial h_{k+1}}{\partial X}\right|_{\hat{\mathbf{x}}_{k+1}^-} \tag{2.53}$$

$$\mathbf{M}_{k+1} = \left.\frac{\partial h_{k+1}}{\partial \mathbf{v}}\right|_{\hat{\mathbf{x}}_{k+1}^-} \tag{2.54}$$

- Finally, the measurement update equations are as follows:

$$\mathbf{K}_{k+1} = \mathbf{P}_{k+1}^- \mathbf{H}_{k+1}^T (\mathbf{H}_{k+1} \mathbf{P}_{k+1}^- \mathbf{H}_{k+1}^T + \mathbf{M}_{k+1} \mathbf{R}_{k+1} \mathbf{M}_{k+1}^T)^{-1} \tag{2.55}$$

$$\hat{\mathbf{x}}_{k+1}^+ = \hat{\mathbf{x}}_{k+1}^- + K_{k+1}[\mathbf{y}_{k+1} - h_{k+1}(\hat{\mathbf{x}}_{k+1}^- 0)] \tag{2.56}$$

$$\mathbf{P}_{k+1}^+ = (\mathbf{I} - \mathbf{K}_{k+1} \mathbf{H}_{k+1}) \mathbf{P}_{k+1}^- \tag{2.57}$$

EKF expand Taylor series up to first order and therefore the system state equations become linear. It is computationally cheap but in some instances, it cannot capture the real non-linearity of the system and therefore, estimated states come out complete different than the real states. The ultimate solution to this is the use of UKF which has the ability to approximate the states' mean and covariance up to third order.

2.3.3.2 Unscented Kalman Filter (UKF) Algorithm

UKF generates the mean and covariance of states of the system through non-linear equations up to third order. Consider the system and measurement equations, UKF approach will be as follows: (the whole procedure of this approach is given in [48] and a similar one in [83])

UKF has the following main steps:

1. Filter initialization
2. Derivation of Sigma points
3. Time update
4. *a priori* state estimate
5. *a priori* estimate for error covariance matrix
6. Measurement update
7. Measurement prediction
8. Measurement covariance prediction
9. Cross covariance
10. Measurement update

- Filter initialization is as follows:

$$\hat{\mathbf{x}}_0^+ = E(\mathbf{x}_0) \tag{2.58}$$

$$\mathbf{P}_0^+ = E[(\mathbf{x}_0 - \hat{\mathbf{x}}_0^+)(\mathbf{x}_0 - \hat{\mathbf{x}}_0^+)^T] \tag{2.59}$$

- Sigma points can be derived using the following equations:

$$\hat{\mathbf{x}}_{k-1}^{(i)} = \hat{\mathbf{x}}_{k-1}^{-} + \tilde{\mathbf{x}}^{(i)} \qquad i = 1, 2, \ldots, 2n \tag{2.60}$$

$$\tilde{\mathbf{x}}^{(i)} = \left(\sqrt{n\mathbf{P}_{k-1}^{+}}\right)_i^T \qquad i = 1, 2, \ldots, n \tag{2.61}$$

$$\tilde{\mathbf{x}}^{(n+i)} = -\left(\sqrt{n\mathbf{P}_{k-1}^{+}}\right)_i^T \qquad i = 1, 2, \ldots, n \tag{2.62}$$

where n is the total states the system have and $\sqrt{n\mathbf{P}}$ is the matrix square root. Subscript i denotes the ith row of the matrix.

- Time update as a $2n$ vector $\hat{\mathbf{x}}_k^i$ can be obtained from:

$$\hat{\mathbf{x}}_k^{(i)} = f(\hat{\mathbf{x}}_{k-1}^{(i)}, \mathbf{u}_k, t_k) \tag{2.63}$$

- *a priori* state estimate can be derived by sing the above equation and is as follows:

$$\hat{\mathbf{x}}_k^{-} = \frac{1}{2n}\sum_{i=1}^{2n}\hat{\mathbf{x}}_k^{(i)} \tag{2.64}$$

- *a priori* state estimate of error covariance is determined from:

$$\mathbf{P}_k^{-} = \frac{1}{2n}\sum_{i=1}^{2n}(\hat{\mathbf{x}}_k^{(i)} - \hat{\mathbf{x}}_k^{-})(\hat{\mathbf{x}}_k^{(i)} - \hat{\mathbf{x}}_k^{-})^T + \mathbf{Q}_{k-1} \tag{2.65}$$

- Measurement update steps are as follows:

$$\hat{\mathbf{x}}_k^{(i)} = \hat{\mathbf{x}}_k^{-} + \tilde{\mathbf{x}}^{(i)} \qquad i = 1, 2, \ldots., 2n \tag{2.66}$$

$$\tilde{\mathbf{x}}^{(i)} = (\sqrt{n\mathbf{P}_k^{-}})_i^T \qquad i = 1, 2, \ldots., n \tag{2.67}$$

$$\tilde{\mathbf{x}}^{(n+i)} = -(\sqrt{n\mathbf{P}_k^{-}})_i^T \qquad i = 1, 2, \ldots .n \tag{2.68}$$

- Sigma points $\hat{\mathbf{x}}$ transformed to $\hat{\mathbf{y}}$ by an output equation

$$\hat{\mathbf{y}}_k^{(i)} = h(\hat{\mathbf{x}}_k^{(i)}, t_k) \tag{2.69}$$

- Measurement prediction at k time step is determined as follows:

$$\hat{\mathbf{y}}_k = \frac{1}{2n}\sum_{i=1}^{2n}\hat{\mathbf{y}}_k^{(i)} \tag{2.70}$$

- Measurement covariance prediction is calculated as follows:

$$\mathbf{P}_{\mathbf{y}} = \frac{1}{2n}\sum_{i=1}^{2n}(\hat{\mathbf{y}}_k^{(i)} - \hat{\mathbf{y}}_k)(\hat{\mathbf{y}}_k^{(i)} - \hat{\mathbf{y}}_k)^T + \mathbf{R}_k \tag{2.71}$$

- Cross covariance is obtained as follows:

$$\mathbf{P}_{\mathbf{xy}} = \frac{1}{2n}\sum_{i=1}^{2n}(\hat{\mathbf{x}}_k^{(i)} - \hat{\mathbf{x}}_k^{-})(\hat{\mathbf{y}}_k^{(i)} - \hat{\mathbf{y}}_k)^T \tag{2.72}$$

- Finally, measurement update is performed as follows:

$$\mathbf{K}_k = \mathbf{P}_{\mathbf{xy}}\mathbf{P}_{\mathbf{y}}{}^{-1} \tag{2.73}$$

$$\hat{\mathbf{x}}_k^{+} = \hat{\mathbf{x}}_k^{-} + \mathbf{K}_k(\mathbf{y}_k - \hat{\mathbf{y}}_k) \tag{2.74}$$

$$\mathbf{P}_k^{+} = \mathbf{P}_k^{-} - \mathbf{K}_k\mathbf{P}_y\mathbf{K}_k^T \tag{2.75}$$

UKF can approximate mean and covariance of system states up to third-order as compared to EKF which is first order approximation. In presence of noise, UKF is able to represent the system with higher-order non-linearity in contrast to EKF but the former is computationally more complex.

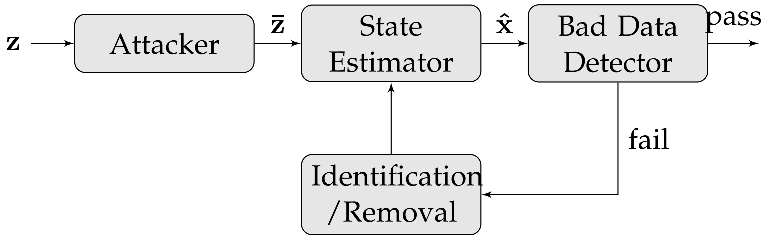

Figure 2.4: State estimation model with attacker and bad data detection test [52]

2.4 Observability Analysis

State estimation makes use of the available measurements in the system to estimate the state of the system. The system observability analysis will check if a unique state estimate can be obtained with the given set of measurements (and locations) [16]. Such analysis can be performed both on-line or off-line. When off line, it is carried out during the primary stage of state estimation where it can be checked if the measurements are adequate enough. If not, further meters may have to be added (at certain places) to cope with the observability issue. On the other hand, if online, observability analysis is usually performed prior to state estimation to ensure that the estimator has the required set of measurements. Occasionally, topology or meter faults may prevent estimator from convergence, therefore, state can be estimated using various observable islands.

Observability of a system is obtained from the network topology along with the set of measurements and their locations i.e., it needs graph theoretical knowledge to understand basic formulation of observability analysis. Without loss of generality it is carried out on linearised model the methods includes fully coupled or decoupled measurement equations (for details, see [4]).

2.5 Bad Data Analysis

This section includes basic arguments on bad data detection and identification theory.

2.5.1 Bad Data Detection

State estimation algorithms fit measurements made on the system to a mathematical model in order to provide a reliable data base for other monitoring, security assessment and control functions [44]. Usually, such algorithms are able to deal with measurement, parameter and structural errors. A few of bad data is obvious can be detected and removed before state estimation by simple outlier approach i.e., negative voltage magnitudes, measurements with several orders of of magnitude larger or smaller than expected values or large differences between incoming and leaving currents at connection node within a substation, as stated in [4]. Fig. 2.4 shows how a simple bad data detection algorithm works. Detection and identification methods to deal with bad data highly depend on the SE technique however, the most widely used is WLS estimator among others (reported in section 2.3). Depending upon various factors, bad data may arise in several ways. They can be categorised into single or multiple bad data. Further, multiple bad data are classified as (as mentioned in [8]):

- **Multiple non-interacting** bad data which has weakly correlated measurement residuals.
- **Multiple interacting and non-conforming** bad data with strongly correlated measurement residuals.
- **Multiple interacting and conforming** bad data with strongly correlated measurement residuals.

There are several bad data detection methods, however the most common ones are described below:

2.5.1.1 Largest Normalized Residual Test (LNRT)

It has been seen that the Largest Normalized Residual Test (LNRT) works quite well for single/multiple non-interacting bad data [4]. The residues vector is defined by:

$$\mathbf{r}(\mathbf{x}) = \mathbf{z} - h(\mathbf{x}) \tag{2.76}$$

normalize the residue is necessary to calculate the residues covariance matrix, defined by the equation:

$$\Omega = \mathbf{R}(\mathbf{x}) - \mathbf{H}(\mathbf{x}).\mathbf{G}^{-1}(\mathbf{x}).\mathbf{H}^t(\mathbf{x}) \tag{2.77}$$

Thus, the normalized residue is calculated by:

$$r_i^N(\mathbf{x}) = \frac{r_i(\mathbf{x})}{\sqrt{\Omega}_{ii}(x)} \tag{2.78}$$

where $\Omega_{ii}(\mathbf{x})$ is the ith diagonal element of the residues covariance matrix.

We assume measurements errors e_i to be independent random variables having zero mean and known variance i.e., presenting normal distribution. Also, it is proved that the elements of the normalized residues are standard normal distributed i.e.,

$$r_i^N \sim N(0,1) \tag{2.79}$$

Thus, the bad data detection test is as follows:

- If $|r_N| < \beta$, with $i = 1, ..., m$, bad data exist
- If all $|r_N| \geq \beta$, with $i = 1, \cdots, m$, there is no bad data

Usually, β is assumed to be 3.

2.5.1.2 Hypothesis Testing

A bad datum can be detected, and eventually removed, if it is not critical or, in other words, its removal does not make the system unobservable. The detection of bad data or structural errors can be viewed as an hypothesis testing problem with two hypothesis H_0 and H_1, where

- H_0 denotes the case with no bad data
- H_1 denotes that H_0 is not true.

(For more detail about the traditional bad data detection please refers to [4]).

- **The** $J(x)$ **Test**: Consider a random variable $J(x)$ and its observation $J(\bar{x})$ as provided by state estimator. Then, this observation must be checked if it belongs to the hypothesized χ^2 distribution or not. In addition, measurement error/noise is also checked for normal distribution $N(0, \sigma_j^2)$. Hypothesis test can be performed by:

  - If $J(\hat{x}) \leq C$, accept H_0;
  - If $J(\hat{x}) > C$, accept H_1.

  where C is the constant to be determined. If α is the significance level of the test, C is

  $$C = \chi^2_{m-n,1-\alpha}$$

  i.e., when H_0 is true, the probability of $J(\hat{x}) > C$ is α and

  $$\int_0^C f(t)dt = 1 - \alpha \quad \text{with } f(t) = \frac{t^{\frac{\nu}{2}-1} e^{-\frac{t}{2}}}{2^{\frac{\nu}{2}} \Gamma(\frac{\nu}{2})}$$

  where $f(t)$ is the probability density function of the χ^2_ν distribution, where $\nu = m - n$ degrees of freedom and Γ is the Gamma function.

2.6 Decentralised State Estimation

With the evolution of smart grid environment, power systems are now more connected and there exists thousands of substations under one network. All of these call for a Multi-area/decentralised state estimation in which, whole network is decomposed into certain number of sub-systems to make state estimation more peaceful. There are further two categories on the basis of levels:

- *Single-level distributed state estimation:* It is also known as distributed state estimation (DSE) in which the whole network is decomposed into a number of overlapping or non-overlapping areas. Each sub-area estimates its own state using the locally available measurements then either share the estimated states with neighbouring areas and without any central entity, state of the whole system is determined (fully DSE) or the local estimates are sent to the central coordinator to determine the state of the entire network (DSE).

- *Multi-level distributed state estimation:* It is called hierarchical state estimation (HSE) in which whole system is divided into certain regions to make the state estimation less complicated. This way, firstly, at the bottom level, the states are being determined for each area separately and send over to the upper level as measurement set and finally, at the upper most level, the system state is determined and pass on to the lower levels for the functions like contingency analysis.

2.6.1 Distributed and Fully Distributed State Estimation

The difference between the distributed and fully distributed lies in the obligation of central entity in distributed whereas no such requisite for fully distributed state estimation. The relevant state of the art can be found in section 3.1. Let us consider a power system having n buses, which is decomposed into s non-overlapping regions (areas) S_i having n_i buses each connected by tie-lines. Each area is regulated by its own local control centre and credited for its own local state and connected to the system control centre via communication channels. We assume (without loss of generality) the global reference bus to be contained in region S_1.

The non-linear multi-area measurement model is framed as

$$\mathbf{z}_i = f_i(\mathbf{x}_i) + \mathbf{e}_i, \quad i = 1, \cdots, r \tag{2.80}$$

where
$\mathbf{z}_i$ $m_i \times 1$ local measurement vector of region S_i;
$\mathbf{x}_i$ $2n_i \times 1$ local state vector (Voltage magnitudes and phasors) of region S_i;
$\mathbf{x}$ $2n \times 1$ state vector for the entire system;
$\mathbf{e}_i$ corresponding Gaussian measurement noise with covariance matrix as $\mathbf{R}_i$.

The measurement vector includes (but not limited to) voltage magnitudes V_l and real and reactive power injections $P_l,\ Q_l$ for every bus and real and reactive power flows $P_{lm},\ Q_{lm}$ for each branch $l - m$. If l is the border bus of the region S_i then the injections become boundary injections and flow become tie-line flows. The state estimation for each region can be written as a minimization WLS problem

$$\begin{aligned} &\text{Minimize} \quad J = r_i^T \mathbf{R}_i^{-1} r_i \\ &\text{Subject to} \quad \mathbf{r}_i = \mathbf{z}_i - f_i(\mathbf{x}_i), \ \ 1 \leq i \leq l \end{aligned} \tag{2.81}$$

where J is the objective function and $\mathbf{W}_i = \mathbf{R}_i^{-1}$ is the weighting matrix. First optimality condition gives the iterative procedure for every region

$$[\mathbf{F}_i^T \mathbf{W}_i \mathbf{F}_i] \Delta x^{i+1} = \mathbf{F}_i^T \mathbf{W}_i [\mathbf{z} - f_i] \tag{2.82}$$

where $\mathbf{F}_i = \partial f_i / \partial x_i$ is the Jacobian matrix and $\mathbf{G}_i = \mathbf{F}_i^T \mathbf{W}_i \mathbf{F}_i$ is the gain matrix.

Once local state estimation is prosecuted, the estimates from every region are sent to the central coordinator along with the boundary measurements for the coordination step. If the need for the coordinator is alleviated, regions can also compute the system state by exchanging the necessary information with neighbouring regions and then that distributed system is called fully distributed state estimation.

2.6.2 Hierarchical State Estimation

The conventional or centralized state estimation which is currently in use worldwide can be followed by a multi-area hierarchical procedure in which local state estimators processes all the raw measurements available locally, hence transferring only a manageable data set to its immediate higher level. This process continues until the highest level where the state for the whole system is evaluated and conveyed to the lower levels for other crucial tasks for example bad data processing [33]. Firstly, a general multi-area hierarchical state estimation is proposed. Let us consider a k-level case with the assumption that each area will perform its own state estimation with its own measurement set along with the information coming from lower level if its not the lowest level itself. A multi-level state estimation can be expressed as:

$$\begin{aligned} \mathbf{y}_{0,j_1} &= f_{1,j_1}(\mathbf{y}_{1,j_1}) + \mathbf{e}_{1,j_1}, \quad j_1 = 1, \cdots, r_1 \\ \mathbf{y}_{0,b_1} &= f_{1,b_1}(\mathbf{y}_1) + \mathbf{e}_{1,b_1} \end{aligned} \tag{2.83}$$

$$\begin{aligned} \mathbf{y}_{1,j_2} &= f_{2,j_2}(\mathbf{y}_{2,j_2}) + \mathbf{e}_{2,j_2}, \quad j_2 = 1, \cdots, r_2 \\ \mathbf{y}_{1,b_2} &= f_{2,b_2}(\mathbf{y}_2) + \mathbf{e}_{2,b_2} \end{aligned} \tag{2.84}$$

$$\vdots$$

$$\mathbf{y}_{0,b_1} = f_{1,b_1}(\mathbf{y}_1) + \mathbf{e}_{1,b_1} \tag{2.85}$$

where
$\mathbf{y}_{0,j_1}$ local measurement vector in S_{j1} at level 1;
$\mathbf{y}_{0,b_1}$ border measurement vector at level 1;
$\mathbf{y}_{1,j_2}$ local measurement vector in S_{j2} at level 2;
$\mathbf{y}_{1,b_2}$ border measurement vector at level 2;
$\mathbf{y}_k$ state vector of over all system;
f_l corresponding non-linear measurement functions for each level l;
$\mathbf{e}_l$ corresponding Gaussian measurement noise vector.

Now, let us formulate each level

2.6.2.1 Level 1 Multi-area State Estimation:

For level 1, each area S_j estimates its own state $\tilde{\mathbf{y}}_{1j}$ by solving the corresponding Normal Equations iteratively

$$\begin{aligned} [\mathbf{F}_{1,j_1}^T \mathbf{R}_{1,j_1}^{-1} \mathbf{F}_{1,j_1}] \Delta\tilde{\mathbf{y}}_{1,j_1} &= \mathbf{F}_{1,j_1}^T \mathbf{R}_{1,j_1}^{-1} [\mathbf{y}_{0,j_1} - f_{1,j_1}(\mathbf{y}_{1,j_1}(k))] \\ [\mathbf{F}_{1,b_1}^T \mathbf{R}_{1,b_1}^{-1} \mathbf{F}_{1,b_1}] \Delta\tilde{\mathbf{y}}_{1,j_1} &= \mathbf{F}_{1,b_1}^T \mathbf{R}_{1,b_1}^{-1} [\mathbf{y}_{0,b_1} - f_{1,b_1}(\mathbf{y}_{1,j_1}(k))] \end{aligned} \tag{2.86}$$

where the inputs at this level include the measurement vectors $\mathbf{y}_{0,j_1}$ and $\mathbf{y}_{0,b_1}$ and the Jacobian matrices, $\mathbf{F}_{1,j1}$ and $\mathbf{F}_{1,b1}$ and the gain matrices $\mathbf{R}_{1,j_1}$ and $\mathbf{R}_{1,b_1}$. Note that the Jacobian matrices are updated at every iteration.

2.6.2.2 Level i Multi-area State Estimation:

The following two equations must be solved for each intermediate level hierarchically from the lower levels. Using the estimate $\tilde{\mathbf{y}}_{i-1,j_{i-1}}$ from the level $l-1$ as the measurements in a distributed approach, $\tilde{\mathbf{y}}_{i,j_i}$ can be obtained from [10]

$$\begin{aligned}
&[\mathbf{F}^T_{i,j_{i-1}}\mathbf{G}_{i-1,j_{i-1}}\mathbf{F}_{i,j_{i-1}}]\Delta\tilde{\mathbf{y}}_{i-1,j_{i-1}}(k) = \mathbf{F}^T_{i,j_{i-1}}\mathbf{G}_{i-1,j_{i-1}}[\tilde{\mathbf{y}}_{i-1,j_{i-1}} - f_{i,j_{i-1}}(\mathbf{y}_i(k))]\\
&[\mathbf{F}^T_{i,b_i}\mathbf{G}_{i-1,b_{i-1}}\mathbf{F}_{i,b_i}]\Delta\tilde{\mathbf{y}}_{i-1}(k) = \mathbf{F}^T_{1,b_1}\mathbf{G}_{i-1,b_{i-1}}[\tilde{\mathbf{y}}_{i-1} - f_i(\mathbf{y}_i(k))]
\end{aligned} \tag{2.87}$$

Based on the estimates from level i and $i+1$, the Jacobian matrices are revised.

2.6.2.3 Level l Multi-area State Estimation:

Using the vector $\tilde{\mathbf{y}}_{l_1}$ supplied by the lower level $l-1$ as the measurement vector, the system state can be estimated by iteratively solving the following equations

$$\begin{aligned}
&[\mathbf{F}^T_{l,j_{l-1}}\mathbf{G}_{l-1,j_{l-1}}\mathbf{F}_{l,j_{l-1}}]\Delta\tilde{\mathbf{y}}_{l-1,j_{l-1}}(k) = \mathbf{F}^T_{l,j_{l-1}}\mathbf{G}_{l-1,j_{l-1}}[\tilde{\mathbf{y}}_{l-1,j_{l-1}} - f_{l,j_{l-1}}(\mathbf{y}_l(k))]\\
&[\mathbf{F}^T_{l,b_l}\mathbf{G}_{l-1,b_{l-1}}\mathbf{F}_{l,b_l}]\Delta\tilde{\mathbf{y}}_{l-1}(k) = \mathbf{F}^T_{1,b_1}\mathbf{G}_{l-1,b_{l-1}}[\tilde{\mathbf{y}}_{l-1} - f_l(\mathbf{y}_l(k))]
\end{aligned} \tag{2.88}$$

Now, Let us simplify the multi-level approach to two level for better understanding. Then the *two-level model* can be explained as

$$\begin{aligned}
\mathbf{y}_{0,j} &= f_{1,j}(\mathbf{y}_{1,j}) + \mathbf{e}_{1,j}, \quad j = 1,2\\
\mathbf{y}_{0,b} &= f_{1,b}(\mathbf{y}_{1,b}) + \mathbf{e}_{1,b}\\
\mathbf{y}_1 &= f_2(\mathbf{x}) + \mathbf{e}_2
\end{aligned} \tag{2.89}$$

where, the measurement vectors $\mathbf{y}_{0,j}$ and $\mathbf{y}_{0,b}$, the state vectors $\mathbf{y}_{1,j}$ and $\mathbf{y}_{b,j}$ and the non-linear measurement functions $f_{1,j}$ and $f_{1,b}$ are as described earlier. For making the process more simpler, lets assume that there are no border variables and the measurement functions are linear as well. Now, more simplified version of two-level can be seen as

$$\begin{aligned}
\mathbf{y}_{0j} &= \mathbf{F}_{1j}\mathbf{y}_{1j} + \mathbf{e}_{1j}, \quad j = 1,2\\
\mathbf{y}_1 &= \mathbf{F}_2\mathbf{x} + \mathbf{e}_2
\end{aligned} \tag{2.90}$$

where $\mathbf{F}_{1j}$ and $\mathbf{F}_2$ are the Jacobian matrices of the corresponding measurement functions. For each area, the state estimator carries out iterative solution algorithm (given in section 2.2) and determines the local state vector along with another iterative process among the two levels [10]:

- *Level 1:* The inputs at the first level are $\mathbf{y}_{1j}$ for area $j = 1,2$ (assuming two areas) and the weighting matrix $\mathbf{R}^{-1}_{1j}$. The output is the local state vector $\hat{\mathbf{y}}_{1j}$ for each area, Normal equations to be solved by each area iteratively are

$$[\mathbf{F}^T_{1j}\mathbf{R}^{-1}_{1j}\mathbf{F}^T_{1j}]\hat{\mathbf{y}}_{1j} = \mathbf{F}^T_{1j}\mathbf{R}^{-1}_{1j}\mathbf{y}_{0j} \tag{2.91}$$

- *Level 2:* The inputs of this level are state vectors of level-1 $\hat{\mathbf{y}}_1$ and the gain matrices $\mathbf{G}_{1j} = \mathbf{F}^T_{1j}\mathbf{R}^{-1}_{1j}\mathbf{F}^T_{1j}$ as the weighting matrix. The output $\hat{\mathbf{x}}$ is the state of the entire system when solving the following Normal equations for the second level

$$[\mathbf{F}_2^T \mathbf{G}_1^{-1} \mathbf{F}_2^T]\hat{\mathbf{x}} = \mathbf{F}_2^T \mathbf{G}_1^{-1} \hat{\mathbf{y}}_1 \tag{2.92}$$

where $\mathbf{y}_1$ and $\mathbf{G}_1$ can be found by juxtaposing the corresponding $\mathbf{y}_{1j}$ an $\mathbf{G}_{1j}$ respectively.

Chapter 3

Literature Review

In this chapter, our main focus is to review some of the well-known previous work on the type and characteristics of attack schemes on power system state estimation. However, mitigation is out of our scope. Furthermore, we will develop an argument for the choice of our stated research questions by motivating from existing gaps.

We start with an overview of centralized and decentralized state estimation and the commonly used methods for estimating the states. State estimation particularly in power systems was first introduced by Schweppe [80] and attracted adequate number of research groups. Along with state estimation, bad data analysis remain an integral part of discussion throughout.

Bad data analysis includes the methods for detecting bad data independent of its cause. A volume of theoretical work is to design an attack such as it can avoid detection from these methods. Such attacks are undetectable or stealth attacks and the criterion on which they work is the stealth condition. There is another category where attacker deliberately maximizes the detection probability to harm the system that is known as detectable attacks.

In addition, there are other attacks not directly related to bad data detection but affect system topology by opening/closing switches or circuit breakers. Such attacks are topology-related attacks. They include line failures, induced topology faults and even (switch) status tempering physically. To cope with topology errors, methods including phasor measurements are well explored. Synchrophasor traffic has varying levels of latency requirements, ranging from 20 ms to 200 ms depending on the applications [46]. The required bandwidth is a few hundreds of kbps and it is determined by the number of phasor measurement units, word length, number of samples, and frequency [46].

In the last section, a discussion on centralized and distributed state estimation is presented. It also includes various multi-area and/or multi-level state estimation theories developed until now and analyse their shortcomings.

However, the assumptions made by several authors are mostly for ideal case scenario far away from reality. Also, the imposed conditions are generally not implementable at operational level. Therefore, there is no existing work that can answer the raised research questions satisfactorily.

3.1 Power System State Estimation

State estimator determines the most likely state of the system by filtering and processing the measurements from metering devices e.g., Remote Terminal units (RTUs) installed in the system via transmission lines. There are two familiar methods to

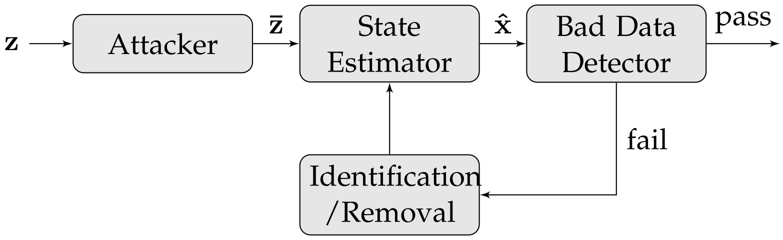

Figure 3.1: State estimation model with attacker and detection test [52]

solve the state estimation problem i.e., Weighted Least Square (WLS) Method and Weighted Least Absolute Value (WLAV) Method. Other methods include the Least Median of Squares (LMS), the Least Trimmed Squares (LTS) and Generalised Maximumlikelihood (GM) estimator. The Least Median of Squares (LMS) estimator minimizes a certain ordered squared residual and is considered as a min-max bias robust estimator [57] while Least Trimmed Squares (LTS) estimator minimizes the sum of the smallest ordered squared residuals up to a certain rank. Generalized Maximum likelihood (GM) estimator was introduced to increase the robustness of SE, i.e., [94], where normalized residuals (r_n) are used through a convex score functions in formulating the objective function.

Although, WLAV is robust and stable in the face of bad data but it has some major downsides, i.e., it requires time consuming Linear Programming (LP) method, inclusion of auxiliary variables reduces convergence pace while minimizing and unreliable in presence of leverage points (i.e., ill-conditionality may occur). Hence, WLS (although not overly efficient in the presence of bad data) is considered as the most commonly used method to solve SE problems. For more details on WLAV, please see [5]. The WLS problem is explained in chapter 2 and reported extensively in [70].

Along with centralised state estimation, decentralised state estimation is getting much attention as well. An approach that leads to the development of a fully distributed state estimator, named the SuperCalibrator (SC) is described in [66] which is a three-phase state estimator that operates at the substation level and requires at least one PMU at each substation. The computed substation state estimate is transferred to the control centre where the overall system state is synthesized from the substation states [66]. A distributed state estimation method is proposed that takes the PMU installation locations as alternative points of the partition, and takes the scale of sub-zone, the number of real-time measurement, and the DG configuration position as the partition criteria, and then conducts distributed state estimation [19].

A multi-area (fully distributed) state estimator is proposed where each subsystem independently conducts its state estimation according to the local measurements, and only limited information of consensus variables and boundary-bus state variables is shared among adjacent regions, while the system-level global optimal solution can be obtained within several iterations [90]. Merging the high speed of Modified Moving Horizon Estimation (mMHE), the accuracy of Moving Horizon Estimation (MHE), and the advantage of Partitioned Moving Horizon Estimation (PMHE) to implement the MHE in a distributed way, a distributed state estimation method named the modified PMHE (mPMHE) is proposed [18]. Authors in [91] presented a fully distributed state estimation algorithm for wide-area monitoring in power systems with the differences from existing methods are; the condition of local observability of all the control areas being no longer needed and that the topology changes are also incorporated. In addition, another fully distributed state estimation approach is proposed using matrix splitting methods [67].

Naziri and Kerrari presented a robust hierarchical state estimation algorithm that make use of the combination of data from PMUs and RTUs for a better estimation [71]. A relatively new hierarchical multi-area power system state estimation method is proposed which is based on exchanging the sensitivity functions of local state estimators instead of exchanging boundary measurements or state estimates [42].

Numerical stability refers to the impact of an incorrect/false input on the execution algorithm, therefore for a sound state estimation, the estimators must be numerically stable (although it is not the case always especially while using WLS state estimator [11]).

Bad data analysis is the ability of the state estimator to reject the bad measurements. For example, if there exist some faulty meter or the bad data induced by an attacker, Eq. (2.1) will become

$$\mathbf{z} = h(\mathbf{x}) + \mathbf{e} + \mathbf{a} \tag{3.1}$$

where $\mathbf{a}$ denotes, the induced bias and its detection/identification is known as bad data analysis. Few of the bad data detection methods are stated in chapter 2.3. Other than that, to enhance the robustness of a power system state estimator to topology errors, bad critical measurements, multiple non-interacting, or interacting bad data (BD), [94] presents a new robust bad data detection method by exploiting the temporal correlation and the statistical consistency of measurements.

There are various ways that an attacker injects false data i.e., either by compromising some meter measurements by physical means or by hacking or manipulating transmission line(s). We divide the attack regimes into two categories i.e., data-related and topology-related attacks and presented a survey [38]. A new classification of attacks against the cyber-physical security of smart grids is also proposed [31]. There are surveys in literature for both types of attacks and mitigation schemes. Authors in [30] provided a survey that comprehensively overviews the literature on FDI attacks, their impacts and defence against them. Moreover, a revised version of a comprehensive overview of different security aspects of smart grid e.g., attack and defence schemes is presented [32]. Recently, another survey on state estimation techniques and challenges in smart distribution systems is published [26]. Considering advanced metering infrastructure, a review of cyber-physical attacks and counter defence is given [87]. Another comprehensive survey of vulnerabilities, threats, challenges and solutions of power grid is given by [79].

3.2 Data-attack Strategies

This section is devoted to the study of data-related attacks on state estimation. The reason why we included these is to educate the reader about the surrounding research and how our contribution covers some of the previous gaps. In addition, this chapter is designed to help the reader understanding most of the related types of attacks to get the understanding of any discrepancies/gaps if present.

The symbols in some of the works have been slightly adjusted to keep notational harmony. As a reference point, we follow the formulation of [70] which we used in chapter 2 as well. Throughout this section, the common features upon which it relies are as follows: 1). model under consideration is steady state linearised DC state estimation model and the category of attacks considered is data driven attacks unless otherwise specified. We define two attack classes upon which the following work lie; injection and non-injection attacks. Injection attacks cover false data injection in meters (section 3.2.1), data injection on SCADA systems (section 3.2.3), false data injection in limited number of meters (section 3.2.4), injection involving just one control centre (section 3.2.5), attacks include multiple adversaries (section 3.2.9) and attacks that are detectable in nature (section 3.2.7). Non-injection attacks include delay attacks (section 3.2.6), jamming or suppression of measurements (section 3.2.8).

Soon after the pioneering work of false data injection attacks by Liu et al., Bobba et al. proposed a notable protection scheme for such attacks stated in section 3.2.2.

3.2.1 Origin of False Data Injection Attacks

Substations are generally provided with metering devices whether the conventional RTUs or the smart IEDs. Meter readings can be manipulated physically or the computers in which all the data is saved can be hacked. Then, the resulting bad data can initialize cascading failures if not detected/identified in finite time. There are various methods to cope with bad data e.g., shown in [70]. Usually, these techniques use *Largest Normalized Residual Test (LNRT)* as stated in section 2.5.1.1.

In a novel approach proposed by Liu et al., to orchestrate a type of coordinated attack that can thwart the conventional detection schemes by dodging the system operators. Such attacks are called *false data injection (FDI) attacks* or stealthy/hidden attacks [61].

3.2.1.1 Description

A power network is considered with m meters providing m measurements. There are n state variables associated with them by a measurement function h as given in section 2.3.1.2. Firstly, it is proved that if the attack vector can be designed by combining linearly the columns of the Jacobian matrix $\mathbf{H}$ (already defined in section II) or $\mathbf{a} = \mathbf{Hc}$, it can evade the detection scheme (provided earlier). On this basis, Liu et al. examined two *attack goals* [61]: 1) *Random False Data Injection Attacks*: The attacker intends to find any attack vector satisfying the above condition. 2) *Targeted False Data Injection Attacks*: The attacker attempts to determine a specific attack vector to force certain state variables to be fallacious. It can be deduced that while former are easier to perform, the latter are more damaging. Under targeted FDI attacks, further two cases are observed: unconstrained case: in which attacks are designed to manipulate certain state variable irrespective of their impact on others and constrained case: in which attacks are performed to compromise certain variable while keeping others unaffected. Two logical attack scenarios are taken into account: In *Scenario I: Limited access to meters*, the attacker is constrained to attack only a particular set of measurements mainly due to the higher physical security. In *Scenario II: Limited resources available to compromise measurements*, the attacker is restricted to some specific number of readings to attack due to the finite resources. These attacks are also extended to the notion of generalized false data injection attacks. These are the kind of attacks which can further increase the impact by exploiting measurement errors typically tolerated in state estimation. Simulations proved their capability of launching more strong attacks than the false data injection attacks. However, these attacks are restricted by real world constraints and therefore not very threatening at the moment.

3.2.1.2 Discussion

- Attacker is assumed to have the knowledge of the system topology or the Jacobian matrix $\mathbf{H}$ [61]. It is an open question for future research to orchestrate false data injection attacks with partial topology knowledge or even with no knowledge of $\mathbf{H}$, for example, GPS spoofing in [82], delay and jitter attacks in [9] and measurement jamming in [29] among others.

- For theoretical observation, a linear model state estimation is presented in [61] while simulations to verify the possibility of the attacks are shown on non-linear models based on SCADA/EMS test bed. Therefore, modelling non-linear state estimator for false data injection attacks can be explored.

- Also, the simulations tested each scenario for only 10^3 times on a random basis leaving some space unexplored [61]. The optimal solution to which measurements to be manipulated is almost unknown. Following this, there are multiple papers like [54] where a low complexity attack strategy is proposed and in [76] where security indices are proposed to find the optimal attack.

3.2.2 Immunity by Protecting Critical Measurements

While Liu et al. presented the stealthy attack strategies from the attacker's point of view and demonstrated what the attacker require to perform an attack without being detected, Bobba et al. looked at the problem from the system operator's perspective. Bobba et al. in [14], demonstrated a practical scheme instead of providing new algorithms for detection. It is proved that after *protecting a particular set of measurements* (equal to the number of state variables), the system can be made immune to false data injection. On this basis, it is quite useful to protect the whole system only by protecting a small set. An alternative can be independent verification of certain carefully chosen state variables or it is also possible for the operator to get benefited from both by using them side by side.

3.2.2.1 Description

The mathematical model to determine the measurements to be protected is as follows [14]: Let M be the set of measurement indices and $I_{\bar{m}}$ denote the indices of protected measurements while I_m denoting its complement. Similarly, let V be the set of indices of state variables and $I_{\bar{v}}$ denote the indices of independently verified state variables while its complement is I_v. For any stealthy attack vector $\mathbf{a}_i = \mathbf{H}\mathbf{c}_i$, if $i \in I_{\bar{m}}$ or $i \in I_{\bar{v}}$, $\mathbf{a}_i = 0$ which implies that attacker cannot find such stealthy attack vector $\mathbf{a}$. It is now clear that the system operator have to protect the minimum $I_{\bar{m}}$ or $I_{\bar{v}}$ in order to make the system secure. The problem now is to find identify the optimal $I_{\bar{m}}$ and $I_{\bar{v}}$. Two approaches are used:

Approach I Brute-Force Search: This attempt to determine $I_{\bar{m}}$ and $I_{\bar{v}}$ is a straight forward brute-force approach. Let $p =\mid I_{\bar{m}} \mid$ or $q =\mid I_{\bar{v}} \mid$ where $0 \leq p \leq m$ and $0 \leq q \leq n$. System operators need to search from $\binom{m}{p} * \binom{n}{q}$ combinations for their choice of p and q to find the optimal sets such that after protecting, no stealthy attack is possible.

Approach II Protecting Basic Measurements: A set of basic measurements in state estimation is a minimum set of measurements which make the system observable [14]. It is evident that cardinality of such set must be n. In this approach, basic measurements are made protected by defining an equivalent mapping by which all measurements are identified either as basic or as redundant. Some adaptations of these methods with some modifications can be seen in [76].

3.2.2.2 Discussion

- Note that, the set of basic measurements is equal in number to the state variables i.e, n. To make the system resilient in case of attacks, protecting such a large set is very unlikely due to cost and time constraints [76]. Being an active research area, numerous researchers approach this problem with the construction of greedy algorithms by [54] where a subset of measurements is made to be attack proof and [12] where a low complexity sub-optimal algorithm is proposed to protect a certain estimates.

- [92] identified the threat to state estimation in power grids and formulated the problem of attack-resilient state estimation exploiting consistency among sensor measurements and develop several algorithms for attack-resilient state estimation accordingly.

3.2.3 Minimum Cost Stealth Attacks

In [76], it is proved that *stealthy attacks can be launched on SCADA systems* and two security indices α_k and β_k are formulated defining sparse attacks and small magnitude attacks respectively. Hence, in [25] the security index α_k quantifying the minimum measurements to be modified in performing the successful attacks (or minimum cost attacks) is computed.

3.2.3.1 Description

The research considered by Dan and Sandberg [25] is threefold, firstly, a security index α_k for minimum cost attack is computed. It is the least number of measurements that need to be manipulated to perform a specific attack. Then, a partitioning of the set of measurements is defined in such a way that a cluster of measurements is available to attacker at the unit cost. This can be the case when attack is performed from a substation and technically, all of its measurements can be attacked at once. Finally, protection schemes are devised utilizing the same cluster strategy. Two approaches are defined for this purpose:

1. *Perfect protection*: is the set of protected measurements P such that no stealthy attack is possible. It has further two categories, i.e, protecting stealthy meter attacks and protecting RTUs from attacks. The cost of perfectly securing all measurements from attacks is quite expensive, and cost is equal to $n = \mid P \mid$. Whereas, we can find a dominating set of RTUs such that no RTU is vulnerable to stealthy attack with the cost much less than n.

2. *Non-perfect protection*: is the set of maximal secured measurements such that stealthy attacks can be minimum. For this purpose, two possible metrics are inspected i.e, maximal minimum attack cost and maximal average attack cost [25]. For the former, the operator intends to maximize the minimum attack cost for all the measurements that can possibly be attacked and for the later one, the operator aims to maximize the average minimum cost for the likely attackable measurements. For both, simple greedy algorithms that aim to find the optimal solution can be leveraged.

3.2.3.2 Discussion

- Perfect protection against stealthy meter attacks is quite difficult to attain as it requires at least n measurements to be protected (same as provided by [14]) while for the security against RTU attacks, *Dominating Set Augmentation Algorithm(DSA)* is used with initiating the set of protected measurements P with a minimal dominating set rather than a flat start. One research question might be giving a flat start to see the efficiency of the algorithm.

- For non-perfection protection, high-level redundancy is required by both greedy algorithms to reach the optimal solution. Results are quite favourable but no argument on the convergence time is made. Resilience and time limitations of greedy algorithms by lowering the redundancy might be tested in future.

3.2.4 Sparse Attacks Corrupting Two Injection Meters

A discrepancy in [61] is rectified as the scheme did not answer which measurements to be compromised. In [36] by Giani et al., a resilient algorithm is proposed to determine (≤ 5) sparse attacks involving only two power meters and arbitrary line meters. Precisely $3, 4$ *and* 5 *sparse attacks* can be devised when all lines are metered.

3.2.4.1 Description

Failures occur in the power system mainly because of either some faulty component/meter or due to some malicious activity that leaves the system unobservable, and these unobservable stealthy attacks need coordination to evade detection. Here, in [36] low-sparsity stealthy attack is under consideration that requires coordination of at most five meters. Stealthy attacks involving large number of meters are uncertain because of the level of coordination required to perform them. An effective algorithm is proposed by Giani et al. in [36] to determine all the possible unobservable attacks that require only two injection meters and arbitrary line meters to be manipulated with $O(n^2m)$ computational complexity with n buses and m line meters. In the specific situations when there are meters on each line, canonical forms for 3, 4 and 5 sparse unobservable attacks can be derived by the algorithms from graph theory requiring complexity of $O(n^2)$ to determine the possibility of these canonical forms.

As far as the detection of stealthy unobservable attacks (not compulsory to be sparse) are concerned, utilizing the known-secure PMUs is proposed [36]. Location of PMUs is identified by buses at which PMUs must be installed to thwart the stealthy attacks. Problem of determining the minimal sufficient PMUs is NP-hard, therefore it is verified that by placing $p+1$ known secure PMUs, system can be protected from P unobservable attacks. An efficient algorithm to find this placement has complexity of $O(n^2p)$.

3.2.4.2 Discussion

- Although PMUs are considered to be the most reliable source of data base as they use GPS to provide synchronous measurements. Here, known secure PMUs are assumed to ignore any fault occurred in PMUs or in GPS that provide the time-stamped signals. For example, GPS spoofing attacks in [82] can cause extensive damage to the power systems hence, unfolding numerous future research questions.

- Another yet interesting question is to explore the applicability of these models on decentralised state estimation.

3.2.5 Stealth Attacks Involving Exactly One Control Centre

False data injection attacks are also possible in decentralised state estimation structure [35]. Ognjen and Gyorgy in [85] presented five attack strategies for *distributed state estimation* (DSE) provided the attacker require the knowledge of the system topology. Further, an attack involving a single control centre is considered in DSE that seems to be successful in either divergence or the erroneous convergence of the system. A similar approach [86] in which attacker aims to compromise the infrastructure of a single control centre.

3.2.5.1 Description

The work [86] is an equivalent version of the previous work of Vukovic and Dan in [85]. Additionally, stealthy attacks on the fully distributed state estimation is being considered for the first time. In the former, stealthy attack that requires the corruption of a single control centre is examined whereas in this paper, authors focussed on the manipulation of the communication infrastructure of a single control centre. Byzantine consensus problem is considered as a baseline in which there are processors that have to consent on a single value even if an error is reported by a processor. In this work, regions act as processors but attack is different. Therefore, resulting in a successful *denial of service* attack i.e, this attack can blind the system operators of the individual area. First singular vector (FSV) attacks and uniform rotation (UR) attacks are applied, and it is verified that even small FSV attacks can cause the desired damage when the state estimation converges with a minimum of 10% error.

Also, an efficient and novel mitigation scheme that not only support convergence but also let the attack to be localized. Starting with the token assumption that every region uses to express their beliefs. Empirical frequency (of token visits) is evaluated for every region. A high empirical frequency determine the likely corrupted region. Exploiting Markov chain to model this random walk of a global observer, the belief consensus localization algorithm (BCL) for regional operators is proposed. Any compromised region is identified and after isolating the infected region, state estimation is re-run until convergence.

3.2.5.2 Discussion

- Although the attacker is not assumed tz have access to all entries of H rather it knows the estimate of the previous iteration which is helpful in launching the attack. The subject of the future work is to study the impacts while alleviating this requisite.
- Numerical results proved the argument of both the attack performance and their diminution. However, it can be seen that smaller weak attacks can not be detected in polynomial time that can make the convergence fallacious as can be observed in the first part of [86]. Hence, a fair research might examine this in future.

3.2.6 Random and Structured Delay Attacks

It is assumed that installing PMUs is the most genuine solution to stealthy attacks. But Shepard and Humphreys, in [82], introduced *GPS spoofing attacks* that has the ability to change the measurement of PMUs just by delaying the signal for some μs. In the last decade, civil GPS spoofing is becoming a serious threat to smart grids which are heavily relied on PMUs. On the argument of GPS spoofing attacks, Baiocco et al. defined *random and structured delay* attacks in HSE [9]. In these kind of attacks, adversary do not require the complete knowledge of the topology, and with very few trivial assumptions, severe impacts in form of ill-conditionality of the Jacobian matrix or instability of power systems can be observed.

3.2.6.1 Description

On hierarchical state estimation, Baiocco et.al in [9] exploited delay and jitter attacks considered with their possible applicability on CSE and DSE as well with very low constraints. Three-level hierarchy is proposed where, either top-down or bottom-up synchro-upgrade procedure is followed. In either case, estimated states of every level has to pass on to the next in a synchronous manner so that the whole system state can be evaluated in time upon which contingency analysis heavily rely.

With the introduction of delay between the levels, stealthy attacks are possible. Two types of attacks are examined, 1) Random delay (jitter) and 2) Structured delay (jitter). It can be observed that while random delay/jitter attacks are easier to perform, the structured have more adverse impacts. These attacks produce strong outcomes in the form of ill-conditionality of the Jacobian matrix or instability of the power system. Majority of the above mentioned stealthy attacks need to be coordinated to avoid detection. For this purpose, system topology or Jacobian **H** in addition to the manipulated measurements or state variables is assumed to be known to the attacker. Surprisingly, to launch delay or jitter attacks, its not necessary for the attacker to have the in-depth knowledge of the topology.

3.2.6.2 Discussion

- Random delays require no prior knowledge of the system (in depth) and therefore are less effective than structured delays with the assumption of known Jacobian **H**. One might examine impacts of small structured delay attacks with partial or no knowledge of **H** for future study.

- An active research area for further research might be on the mitigation policies for the delay and jitter attacks (for both random and structured). In addition, these attacks might be explored in fully distributed state estimation.

- [81] studied load frequency control of a one area power system under denial-of-service attacks where the time delay of the communication channels is taken into account.

3.2.7 Subspace Methods for Data Attacks

Major part of previous work on the security of power system state estimation focus on stealthy attacks that avoid bad data detection tests. To our knowledge, *data framing attacks* by Kim et al. is the first piece of work towards detectable attacks that proves to be successful despite detection by misleading the error identifier [52]. *Subspace methods* for constructing data framing attacks have recently been formulated in [53] while assuming that the attacker is only capable of manipulating a subset of the measurement vector without the detailed knowledge of H or the system parameters.

3.2.7.1 Description

The research by Kim et al. in [53] is twofold: firstly, unobservable data attacks are designed with the help of subspace methods with only partial measurements and secondly, subspace information, is used to orchestrate data framing attacks with the similar requirement of partial measurements.

All information that an attacker require is the subspace of H i.e, $R(H)$. Two algorithms are proposed to perform successful data-driven attacks: 1) Attack with full measurements and 2) Attack with partial measurements. Due to similarity, we will discuss the latter while interested readers are advised to see [53] for details. Algorithm for data attacks with partial measurements is as follows:

- *Step 1) Subspace Estimation:* Based on the available measurements, estimate the basis matrix U of $R(\mathbf{H})$ (subspace of **H**).

- *Step 2) Null Space Estimation:* Calculate the null space of the matrix obtained by removing from basis matrix the rows corresponding to the critical set C just to ensure the non-attack positions.

- *Step 3) Attack:* Corrupt the data from C by corresponding values of $\alpha.U$ where α being a scalar.

The subspace related data framing attacks exploit the bad data detection and removal techniques. Particularly, the attacker maximizes the residual of the framed measurements to trigger the false alarm purposely hence misguiding the system operator. After removing such data, despite of the consistency with the model, existing false measurements result in spurious estimates. Algorithm for data framing attack with partial measurements executes the same way as for unobservable data attacks given above (for details see [53]).

3.2.7.2 Discussion

- Majority of literature in countermeasures focus on protecting certain number of measurements to made the system un-attackable while assuming that the adversary has the knowledge of **H** or the system parameters. This paper opens many questions to rescale the mitigation and protection measures.
- On the other hand, it is revealed that today's power systems are not secure under these orthodox bad data detection and identification techniques. More work on bad data monitoring mechanism is required.

3.2.8 Detectable Jamming Attacks

Deka et al. in [27], later discovered that cardinality of the *detectable framing attacks* (introduced in previous subsection) can be reduced to more than 50% of the stealthy attacks by controlling the presence of certain protected measurements. Furthermore, the authors maximize the attack impact by the inclusion of *measurement jamming* into the detectable attacks [29].

3.2.8.1 Description

False data injection attacks are considered as unobservable when they remain undetected while testing through traditional schemes. All of the above mentioned work in section 4 verifies adequate success of these stealthy/hidden attacks (with some assumptions) and their corresponding counter measures. But the concept of data framing detectable attacks in [52] have pressed the power security researchers. On this basis, [27] is the first known work (to our best knowledge) to examine the detectable false data injection attacks by Deka et al.. Following this, the authors present detectable jamming attacks by adding measurement jamming into it [29] to maximize the impact.

Earlier, it is proved by the same authors that the cardinality of detectable attacks can be reduced to more than half of that of stealthy attacks (or atleast half) [27]. In addition to performing detectable attacks, the adversary here is capable of jamming/blocking some measurements/communication in the network. Compared to bad data injection, jamming is less cost-intensive (can also be observed from section 4.6) and therefore its cost varies from 0 to the maximum of P_d (where P_d be the cost of detectable attack without jamming). This way, jamming cost is partitioned into two regions to obtain the optimal attack by graph-theoretic means. One of the essential findings in this work is the ability of attacker to apply jamming only if the jamming cost is less than half of that of injection cost [29]. Since, determining the optimal detectable jamming attack is NP-hard, a polynomial time approximation is obtained to verify the results.

3.2.8.2 Discussion

- [29] is one of the the most recent works (to our best knowledge) in this mention and protection against such attacks might be devised in near future to overcome the potential threats by detectable jamming attacks.

- In the perspective of an adversary, designing optimal detectable jamming attack must be the next task. In addition, data jamming in decentralised state estimation can be one of the areas of further study.

3.2.9 Data Injection Attacks with Multiple Adversaries

Till the end of 2015, almost all of the ongoing research focussed on investigating a kind of false data injection attacks involving a single attacker and examining the attack impacts on the security of the grid. Along with this, countermeasures are also proposed to cope with the mentioned class of attacks. Interestingly, no work on the notion of *multiple adversaries* is seen until Sanjab and Saad studied the impact of two attackers simultaneously [77].

3.2.9.1 Description

Following the above mentioned proposition for multiple attackers, the authors in [78] constructed two models from game theory relied on linearised/DC state estimation while considering centralized case. Successful attacks can manipulate the price and hence have financial benefits causing loss for the grid operators.

In the *first* model, Stackelberg game paradigm is used in which defender or the system operator act as a leader and the attackers as its followers. Thus, a non-cooperative game is played between the defender and the attackers noting that in this game, leader can predict the adversary's actions prior to playing its defence strategy (e.g., selecting the measurements to protect). Solution to this game is studied where defender needs to minimize the attack impacts and in parallel attacker chooses its strategy to maximize the trade off between benefits and attack cost. The only difference in the *second* game which is Nash equilibrium model (see reference [78] for details) is that now the defender can not anticipate the actions of adversaries and hence play to meet its certain objective regarding defence. In both of the mentioned paradigms, two situations can be observed: 1) The attackers can cancel the effect of each other resulting in no manipulation and hence no need to defend and 2) The attackers can help each other achieving their targets and therefore can be destructive for the grid.

3.2.9.2 Discussion

- Recently in Dec. 2015, Ukraine's power plant has been hacked so badly that the control centre operators have to manually operate the breakers for so many days following the attack. It is reported that the hack involved multiple adversaries [93].

- After this attack, it is also shown that the grids in the US are more vulnerable to these attacks as they have more automated breakers than Ukraine had. All of this call for more strategic defence of our power grids.

- Later, Pilz et. al in [75] proposed a class of false data injection attacks that are based on modifying forecasted demand data and studied its impacts on system's parameters. Monitoring approaches are demonstrated that the control centre may employ to deal with such attacks. A game-theoretic method is used to support the utility company's decision-making process for the allocation of their defence resources [75].

3.3 Topology Detection and Identification

The topology state such as status of circuit breaker and switches along with the primary topology graph can be regarded as binary data. Such data is used by a topology processor to estimate the current topology prior to state estimation, which then determines the most likely system state that is essential for taking control decisions and contingency analysis.

In this section, we review some of the previous works on topology (change) detection and identification. So far, there are mainly three types of methods to detect/identify topology changes, namely (1) numerical (analytical) methods, (2) rule-based, and (3) synchrophasor methods. Analytical methods are the ones where data is verified along with the state estimation using network graph. Rule-based methods make use of control centre information to verify the changes in switch position [62] and synchrophasor methods are the ones which depend on Phasor Measurement Unit (PMU) for their deployment.

Each of the above methods allow topology change detection, but has different drawbacks. For instance, in numerical methods, converged state estimation is desired to detect/identify changes in topology— however, the very topology errors sought may result in a failure of the state estimator to converge [62]. On the other hand, rule-based methods may have problems detecting topology errors when the measurements used for validation process include bad data. Finally, the use of synchrophasor measurements to validate switch positions is attractive, but at present difficult to achieve given limited installation of synchrophasors; even then it is unlikely to see deployment of such devices at each bus which also may be vulnerable e.g. to spoofing attacks [82].

One of the pioneering works in this regard is by Clements and Davis [21] as they developed a method for detecting topology errors in electric power networks by providing a geometric interpretation of the measurement residuals caused by such errors. Hines et al. [45] elaborated topological and electrical structure of the power grid while proposing a graph theoretic method for generating random networks similar to the power grid to better notice topology changes. Monitoring of power system topology in real-time is achieved currently by observing the circuit breaker's (CB) operation and statuses by using Regional Transmission Units (RTUs) of SCADA system. However, changes such as trip conditions, etc. cannot be determined solely by this SCADA approach. Kezunovic proposed a solution based on a new CB Monitor (CBM) which would be permanently connected to the substation CBs [49]. This CBM scheme can be extended to the system level, but deployment cost cannot be ignored.

In [62], Lu et. al proposed a rule-based topology error/change detection method in which all analogue data are screened before applying the heuristic rules to detect the errors. Lefebrve et al. [58] proposed a pre-processing method for detecting and identifying topology errors and bad measurements before a state estimation solution. Similarly, a pre-estimation algorithm depending on PMU measurements examines the change for each new received set of data in order to locate anomalies and apply countermeasures [73]. Another approach is to take the status of switching devices as new state variables estimated together with usual ones while considering three state variables for one switch status [55].

Steady state simulations of power system with changes in topology are shown in [3] by collecting all the possible topologies as a result of isolation of transmission lines from the system. Placing PMUs at strategic points can help quickly detecting topology changes caused by events such as lines going down or large voltage drops [88]. A quick change algorithm is proposed to be applied on the data provided by high-speed PMUs to detect the change-point that corresponds to the system topology change instant [47]. A systematic bus selection scheme is presented for the minimum required PMUs. Taking into account the load dynamics and measurement error, the topology detection algorithm is constructed based on data from synchrophasors [17]. [7] proposed that the minimal difference between measured and calculated voltage angle or magnitude indicates the actual topology and hence a method based on multiple synchrophasors is devised.

3.4 Topology attack Schemes

Bad data errors (attacks) and their detection/mitigation is a widely researched area in power system state estimation, with a large body of work emerging since study of bad data injection was proposed in work by Liu et al. in [61]. However, substantially less attention has been paid to the other main cause of the faults namely topology errors. However, topology attacks is getting much attention these days. Therefore, in this section, we aim to provide most of the (existing) considerable literatures on topology related faults and attacks.

3.4.1 Man-in-the-Middle (MiM) Topology Attack

Most of the previously studied area involving topology errors discussed general faults, their impacts, detection and identification methods. To the best of our knowledge, Kim and Tong are the first ones to examine a type of undetectable topology attacks.

3.4.1.1 Description

This paper proposed a form of "man-in-the-middle" (MiM) attack on the topology of a power grid [51]. It studied two main attack regimes depending on the set of information I available to attacker.

First is *the global information regime* in which the attacker can ideally observe all meter and network data before altering few of them. Although such scenario is unrealistic, it is stated just as a base case to analyse the worst case attack by giving the attacker extra power. A necessary and sufficient condition is presented algebraically that, having the controlled meters known, an undetectable attack exists that can launch targeted topology attack by misleading the control centre. This condition provides the methods to check grid vulnerability to such attacks in addition to giving a defence insight on which meters to protect first.

A more realistic scenario is *the local information regime* where the adversary can only observe a certain number of meters which are in the local information set I_{local}. Similar to the first technique, some particular conditions are proposed for such attacks to exist. Another interesting finding was providing the conditions when such attacks cannot be made undetectable. Such conditions give insights for defence mechanisms and therefore it is shown that, by protecting certain meters, system can be made such that no topology attack could go undetected.

3.4.1.2 Discussion

- Jinsub and Tong proposed the attack on DC framework. As demonstrated earlier, DC models for state estimation exaggerates the effects of such MiM undetectable topology faults while AC model limits the impact. Also, the Global attack regime has too strong assumptions to be practically applicable.

3.4.2 Hidden Topology Attack Using One Breaker

A coordinated cyber-attack on meter readings and breaker statuses is proposed that can lead to incorrect state estimation subsequently destabilize the grid [28].

3.4.2.1 Description

This model focuses on stealthy/hidden attacks that basically depends on topology changes (change in breaker statuses). Particularly, attacker changes the statuses of a few operational breakers from 1 (closed) to 0 (open), as well as jams (blocks the communication) of flow measurements on a subset of transmission lines in the grid [28]. However, the attacker does not compromise any meter measurement to some arbitrary value. These attacks are termed as 'breaker-jammer' attacks by the authors. This attack framework can be generalised to any grid with meters for measuring line flows and injections. The optimal stealthy attack is obtained using a novel graph-colouring analysis.

The attacker is assumed to be agnostic i.e., having no system knowledge yet capable of changing a few statuses along with blocking the corresponding measurements to make the hidden attack possible. One of the main results was the existence of optimal topology based attacks involving just one breaker.

3.4.2.2 Discussion

- Another related regime is proposed by Liu et al. [60] where outages of some lines can be masked by injecting false data into a set of measurements and therefore the residual in the line outage detection is increased such that the line outage cannot be detected by phasor measurement unit data.

- Recently, a similar approach is proposed by [20], where the term *masking* (the measurements) is used instead of jamming which results in wrong topology information being sent to the control centre.

3.4.3 Recovery following a Joint Cyber and Physical Topology Attack

A cyber-physical attack cause obstruction in information flow along with physical tampering to the breaker's status(es). Information recovery after such attack is the main focus of this work [84]. Methods of power grid state estimation after a joint cyber and physical attack are developed and resilience to various topologies and different kinds of attacks is studied.

3.4.3.1 Description

The commonly used linearised Direct-Current (DC) power flow model is considered. The modified version of the control network model that includes PMUs and Phasor Data Concentrator (PDC) is examined. A zone is defined as a set of buses (nodes), power lines (edges), PMUs and an associated PDC. Attack analysis is performed for an adversary that disconnects lines within a zone (physical attack) and obstructs the flow of information from the PMUs within the zone to the control center (cyber attack) [84]. For instance, a cyber attack can be launched by making the associated PDC disable or by attacking the communication line between the PMUs and corresponding PDC. As a consequence, the phase angle and the line status (of the missing lines) become unavailable. Main objective here is the recovery of phase angle and detection of the missing transmission lines.

Particularly, by applying matrix algebra and graph theory techniques to the region outside the attacked zone, methods to retrieve missing state variable and line information (of the attacked zone) are developed. In addition, depending on the zone structure, necessary and sufficient conditions to guarantee the recovery are presented. It is proved that if there exists a matching between the inside and outside nodes of the attacked zone that covers the inside nodes (V_H, then the phase angles of the nodes in the attacked zone are recoverable by solving a set of linear equations of size $|V_H|$ [84]. As far as recovery of disconnected lines are concerned, it is shown that if H is acyclic, missing lines can be detected solving size $|E_H|$ set of linear equations. However, if H is planar, missing lines can be detected solving a Linear Programming (LP) problem.

3.4.3.2 Discussion

- Illustrations shown in this work include base line 14 and 30-bus systems therefore leaving the large scale application for further research. In addition, limited PMUs or PMUs on selected buses can make the approach more promising.

- A similar attack regime where adversary aims to provide data that paints a completely safe picture for the grid which is consistent with the net load change, while at the same time disguising large line overloads, a fundamentally dangerous situation that may lead to a cascading failure [13].

- On the other hand, there are methods proposed to distinguish cyber attacks from physical faults. A data-driven approach is provided where labelled data are projected in a new low-dimensional subspace using Principal Component Analysis (PCA) [6].

Last decade seems to be quite devoted in the study of attacks (both state and topology) and their mitigations on power system state estimation. In this chapter, we examined the most convincing of them. The reason behind including recovery study section 3.4.3 in the literature review chapter is to make the reader aware of the level of damage a cyber-physical attack can cause and also the cost of recovery after that. In addition, it is relevant to our ongoing work as well.

A general observation can be: *such type of attacks are a genuine threat to the power grids*. Two essential reviews after analysing above significant papers are: 1) Almost all of the above mentioned attacks proved their success against the weaker bad data detection test that relies on residuals (i.e, residual method). 2) Most of the work considered the traditional WLS method for state estimation rather than using some better and advanced methods like Kalman Filter. Therefore, interactions with models other than WLS and residual method is an uncovered and open research question.

Most of the work previewed in this chapter supported our motivation in terms of research questions already stated. Particularly, data attacks guided us towards swapping attacks whereas topology attacks took us to in-cycle line failures. In other words, by specifically examining the assumptions and parameter choices, we come across the idea to design such new type of attacks.

Chapter 4

Reordering Attacks

A number of attacks have been proposed ranging from bad data injection as may be achievable by direct manipulation of sensors to indirect attacks such as manipulating the signal timing proposed by Shepard and Humphreys [82], jamming of signals proposed by Deka et al. [27] or delays in communication channels proposed by Baiocco et al. [9]. Unlike the work mentioned before, most of attacks, however, rely on the assumption that arbitrary values may be injected by an adversary. *We argue that this assumption is quite strong* and that instead, it is of considerable interest to study cases where measurements and communication channels are protected, at least using authentication and integrity protection as provided e.g. by the ISO/IEC 62351 standard. This offers a more realistic adversary model compared to that introduced by Liu et al. [61]. In other words, in FDI attacks, measurements are compromised but here only the time-stamp is compromised. Note that the study of countermeasures against proposed measurement re-ordering is our ongoing work which based on detection probability.

In Fig. 4.1, communication between the N (remote) sensors (could be meters apart) and the state estimator is shown where the communication network is authenticated and integrity protected. Measurement data packets generated by the sensors respectively are conveyed to the state estimator for processing in a certain defined order.

In particular, this chapter provides swapping attack impacts (both theoretical and numerical) for both the conventional and hierarchical state estimation.

4.1 Attack Model for Conventional State Estimation

Our aim, here, is to highlight the vulnerabilities in the existing communication infrastructure by introducing a novel attack relying solely on re-ordering of the measurement vector which result in spurious estimates. ISO/IEC 62351 supports message authentication and integrity protection but not time-stamped authentication of messages that means, a MITM attack who is re-ordering just the time-stamps. We formulate targeted re-ordering attack considering two scenarios for this: 1) swapping the measurements by the previous plausible vector. In the first scenario, we are assuming some attacker that is manipulating the communication network. In other words, the attack is about to re-order the time-stamps of the measurement vectors and not swapping the measurement vectors themselves hence avoiding the standards. 2) manipulating sensor readings in a constrained way such that it looks like swapping the measurements by some scalar multiple of previous measurement vector. For example, sensors usually do not give a true value but the true values need to be calibrated. The scaling factor in this scenario can be built in the calibra-

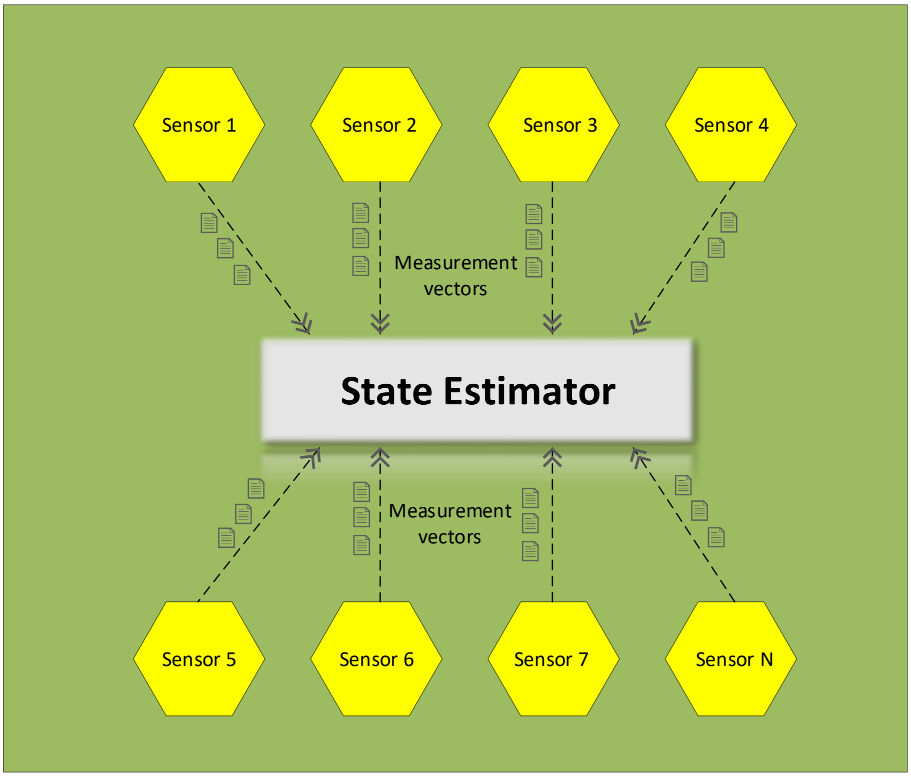

Figure 4.1: Communication network from sensors to estimator

tion phase. Therefore, these attacks can be named as calibration attacks. It is worth noting that *we assume that the preceding and present measurement vectors are known to the attacker*. For both the scenarios, we prove validity of our attacks through the simulation results.

The developments in the notion of attacks and their countermeasures flourished much in the last decade. But as far as mitigation/protection is concerned, the majority of the work focused on integrity protection as one of the possible countermeasures. The attack we are proposing is novel in the sense that it can be launched successfully despite of these modern restrictions. In chapter 2, a continuous model for state estimation is presented, however, to study attacks and their impacts, discrete approximation of the model is widely used [4] and from now onward we will also follow discrete time approximation model.

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{4.1}$$

where $\mathbf{H} \in \mathcal{R}^{m \times n}$ is a constant Jacobian matrix. Then the estimation problem can be solved by

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z} \tag{4.2}$$

The active power flows can be estimated by the phase angle estimate $\hat{\mathbf{x}}$

$$\hat{\mathbf{z}} = \mathbf{H}\hat{\mathbf{x}} = \mathbf{H}(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z} := \mathbf{K}\mathbf{z} \tag{4.3}$$

where $\mathbf{K}$ is the hat matrix. Bad data detection system identify faulty sensors and bad data by calculating the measurement residue which is defined as

$$\mathbf{r} := \mathbf{z} - \hat{\mathbf{z}} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} = (\mathbf{I} - \mathbf{K})\mathbf{z} \tag{4.4}$$

If the residue $\mathbf{r}$ is larger than the threshold τ, then an alarm is triggered and bad measurements $\mathbf{z}_i$ are identified and removed.

In case of False Data Injection (FDI), $\mathbf{a}$ generally denotes the attack vector that shows the amount of change to the original measurement vector [61].

$$\mathbf{a} = \mathbf{Hc} \tag{4.5}$$

where $\mathbf{c}$ is a vector denotes the magnitude of change and is bounded by some stealthy condition. *A necessary condition for a stealthy FDI attack is that the bad data detection alarm is not triggered if* $\mathbf{a}$ *lies in the null-space of* $\mathbf{I} - \mathbf{K}$. Whereas, in jamming or delay attacks, there is no attack vector to be added, rather adversary just drop/block or jitter the measurements irrespective of whether they are secure/protected. Similarly, **re-ordering** of the measurement vector is introduced where the goal of the adversary is to misguide the system operators about the type and strength of attack while keeping itself in the communication network. In other words, it is like a man-in-the-middle attack on communication network e.g., in Fig. 4.2 where adversary can re-order the time-stamps of the data packets transmitting from substation to the control center via SCADA. Once, the re-ordering attack launched successfully, manipulated information will flow from substation to the control center (can be seen in figure 4.2) where critical decisions will be made depending upon the false data. Therefore, the objective of the attack is to be successful in state forcing or convergence with errors while being in-noticed by the model-based bad data detection. There may be more sophisticated detection criteria, of course, but these apply mostly to determining whether measurement devices (vector entries) are compromised, and that does not apply here. Other models rely on redundancy among measurements to determine compromise, but for a network-based attack this does not match very well.

Now, $\mathbf{z}^*$ is the new measurement vector obtained after swapping/ re-ordering the measurements

$$\mathbf{z}^* = \mathbf{z} + \mathbf{a} \tag{4.6}$$

where $\mathbf{a}$ is the swapping attack vector. This attack is less recourse intensive as it does not require modification or bad data injection into the sensors rather tampering the transmission lines would be enough. After re-ordering, the system model is

$$\mathbf{z}^* = \mathbf{Hx}^* + \mathbf{e} \tag{4.7}$$

where and $\mathbf{x}^*$ is the corresponding state vector which can be determined by

$$\mathbf{x}^* = (\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z}^* \tag{4.8}$$

where $\mathbf{H}$ is the Jacobian matrix. As, the final result of the state estimate from the above set of normal equations involves matrix multiplication with $\mathbf{z}^*$, therefore even the swapping of just 2 readings will change the whole state vector. We assume that all data is subjected to outlier removal which is usually a residue test to

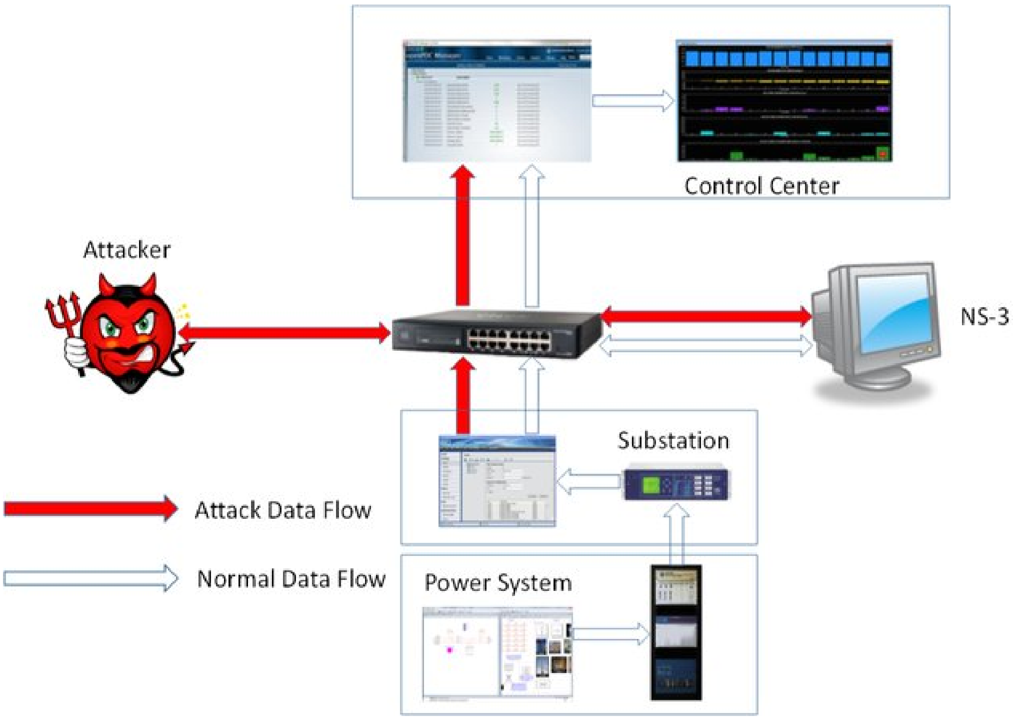

Figure 4.2: Man-in-the-Middle attack on communication network [59]

filter bad data (see section 2.5). We have to show that the attack proposed below will not be affected by this removal while satisfying stealth condition. To make the swapping attack successful, attacker has to know the previous plausible measurement vector (either partial or full). As in [76], Sandberg et al., defined two security indices for sparse attacks as well as for small magnitude attacks. The first security index α_k in [76] is for sparse attacks i.e. the adversary can get the least/minimum cost attack by solving this and the second security index β_k help the attacker to find the small magnitude false data injection attacks to avoid detection tests. The aim of the attacker here is to maximize the impact P of swapping i.e, in terms of convergence time and MSE while keeping the measurement re-ordering to the minimum. Such that, when there is no attack, $P = 0$ and in the presence of attack, $P > 0$. This optimization problem can be formulated as

$$\max_{\mathbf{a}_i} \; P \quad s.t. \quad \| \mathbf{a}_i \| \leq \mu \tag{4.9}$$

where $\mu > 0$ is the desired bound on the size of attack. As defined, $P = \infty$ means that the state estimator does not converge. For a feasible attack, P must be some definite number greater than 0.

The two scenarios defined in section I are as follows:

4.1.1 Scenario I

Here, we consider the re-ordering of measurement with some measurement vector from the plausible preceding data sets. By plausible we mean that the difference between the corresponding estimates is bounded i.e.,

$$|\ \mathbf{x}^{new} - \mathbf{x}^{old}\ | < \mu \tag{4.10}$$

where μ is some scalar. In other words, attacker is not free to choose any previous data set for swapping attack but only the one satisfying the above condition. Here, we are assuming that a particular set of measurements is secured such that they are integrity protected but not encrypted. By integrity protection we mean, protection of content and processes against injection. Assumptions regarding knowledge that attacker has, include: 1) Order ($m \times n$)of Jacobian matrix $\mathbf{H}$, 2) Arrangement in which the measurements are placed in $\mathbf{H}$ and 3) Set of protected measurements is also known to the adversary.

Once the data set to be used in the attack is chosen, the man-in-the-middle attacker now has to select which readings to swap between the two measurement vectors, and which not i.e restricted swapping. This means the attacker can launch minimum cost/sparse attacks with carefully chosen minimum possible swapping. For this purpose, we define a measure to quantify the hardness to perform sparse swapping attacks.

$$\begin{aligned} \text{minimize} \quad & \|\mathbf{a}\|_0 \\ \text{subject to} \quad & |\mathbf{z}_i^{new} - \mathbf{z}_i^{old}| < \epsilon \\ & \frac{1}{n}\Sigma_n(\mathbf{x}_i^{new} - \mathbf{x}_i^{old})^2 \geq c \end{aligned} \tag{4.11}$$

where ϵ is an upper bound on all the measurement swappings and $c \neq 0$ is a scalar to ensure a non-zero attack vector. In our particular case, we (attacker) choose $\epsilon = 3$ which is the highest difference between any two respective measurements and $c = 0.01$ as to avoid zero s.t., the optimization problem will not yield zero vector as the optimal attack vector. Note that we found the above chosen values for ϵ and c by experimental evaluation. We did the experiments by setting $\epsilon =$ from 1 to 20 with 1 as increment and c from 0.001 to 1 with 0.01 as increment respectively. To analyse the sensitivity for the choice of ϵ and c respectively, if we choose ϵ to be < 3, it will decrease the attack impact but if we choose it to be > 3, the attack impact will remain the same. On the other hand, any c which is < 0.01 but > 0 will have no effect but if e.g., $c = 2$, it is quite likely that we miss the optimal attack vector.

Zero norm of a vector $\mathbf{v}$ is $\|\mathbf{v}_i\|_0$ is the number of non-zero entries in $\mathbf{v}_i$, solution to (4.11) is the minimum number of swapping required to make the attack successful and a meter i with higher metric will be considered more secure means the adversary need to swap several measurements to make the swapping attack hidden. Note that In Eq. (4.11), we optimize over all re-ordering that lie under a threshold and its solution is $|\mathbf{a}^*|$ that can be used to construct sparse attack. The first constraint is to limit the attacker to manipulate relatively closer measurements where ϵ is some arbitrary number. Whereas, the other constraint is to bound the impact (mean squared error) to a certain value to guarantee erroneous convergence. If we look at the sensitivity study of both of the parameters, by changing the values of parameter, one at a time, we come to know that as the value for ϵ goes down, size of attack decreases same goes for c with respect to the impact. Note that MSE is a convex function hence global minimum can be achieved. The sparse attack vector can be seen as

$$\mathbf{a} = \begin{cases} \mathbf{z}_i^{new} - \mathbf{z}_i^{old} & : \mathbf{z}_i \notin S_m \\ 0 & : otherwise \end{cases} \tag{4.12}$$

where S_m denotes the set of secured measurements.

```
Algorithm 4.1: Re-ordering Attack for scenario I
   Input: $M_{old} = \{\mathbf{z}_1, \cdots \mathbf{z}_m\}$
   Output: $M_{new}$
   Data: $hole \leftarrow hole\ in\ array\ M_{new}$
   $\mathbf{z}_i \leftarrow measurement,\ i = 1, \cdots m$
1  for t = 1 to length(M) do
2      $\mathbf{z}_t \leftarrow M[t]$
3      $hole = t$
4      $M_{new}[hole] = \mathbf{z}_t$ while hole > 0 do
5          if $|\mathbf{z}_{i(new)} - \mathbf{z}_{i(old)}| < \epsilon$ then
6              $\mathbf{z}_{i(new)} = \mathbf{z}_{i(old)}$
7      else
8  return $M_{new}$
9  $\mathbf{z} = M_{new}$
10 Solve $\mathbf{z} = h(\mathbf{x}) + \mathbf{e}$
11 Solve Equation 4.2 for $\mathbf{x}$
12 Calculate Mean Square Error (MSE)
```

We now combine the intuitions attained for the above scenario and propose Algorithm 4.1 to design a successful re-ordering attack. Step 1 is the input for the adversary about the knowledge of some previous plausible measurement vector M_{old}. From steps 2-6, our attacker which is in fact a man-in-the-middle receive all data packets from the sensors and construct M_{new}. Steps $7-8$ are the conditions for measurement swapping, after which, attacker successfully swap it to the measurement vector M_{new} ready to use for state estimation. The following arguments for the pre-condition prove its correctness: 1) The sufficient condition for the swapping attack to be not affected by the traditional bad data detection is $\epsilon < \tau$ and 2) For FDI attacks, $\mathbf{a}$ is defined to have a non-zero entry corresponding to the attacked measurements and zero for the non-attacked ones. Similarly, for the re-ordering attack vector, as, for the swapped data packet, there will be corresponding non-zero entries in $\mathbf{a}$ while with no swapping, will get $\mathbf{a} = 0$. Therefore, a necessary condition for a swapping attack is same as that for stealth FDI attacks, i.e., the bad data detection alarm is not triggered if $\mathbf{a}$ lies in the null-space of $\mathbf{I} - \mathbf{K}$.

To prove the attainability of optimum to the above optimization problem, we need to state a few lemmas from [63]:

Lemma 4.1 (Existence of infimum)
Consider the following minimization problem

$$\begin{aligned} &\textit{minimize} && f(x, y) \\ &\textit{subject to} && (x, y) \in \Omega \end{aligned} \tag{4.13}$$

where f is a given function bounded from below over a feasible region Ω. Let $y = g(x)$ be a given function and consider a restriction of Eq. (4.8):

$$\begin{aligned} &\textit{minimize} \quad h(x) := f(x, g(x)) \\ &\textit{subject to} \quad x \in \bar{\Omega}, \quad (x, g(x)) \in \Omega \end{aligned} \tag{4.14}$$

where $\bar{\Omega}$ is some subset of $\mathcal{R}^n$. Suppose that $\inf(4.9) \leq \inf(4.8)$ *and the objective function of the problem* (4.9) *attains its infimum. Then* $\inf(4.9) = \inf(4.8)$ *and the infimum of* (4.8) *is also attainable.*

Lemma 4.2 (Existence of infimum and lower bound)
If

$$\begin{aligned} &\textit{minimize} \quad f(x, y_0) := \frac{1}{2}x^T Q x + q^T x + (r_0 + r^T x)y_0 + \lambda y_0^2 \\ &\textit{subject to} \quad \|x\|_0 \leq y_0, \quad Ax + a y_0 \leq c \end{aligned} \tag{4.15}$$

is bounded below over a feasible region, then its optimal solution is attainable.

Proof is omitted here (please see details in [63]). Applying above lemmas to our optimization problem, it can be seen as:

Theorem 4.3 (Existence of optimum re-ordering attack)
If the objective function in

$$\begin{aligned} &\min && \| \mathbf{a} \|_0 \\ &\textit{subject to} && |\mathbf{z}^{new} - \mathbf{z}^{old}| \leq \epsilon \\ & && \frac{1}{n}\Sigma_n(\mathbf{x}_i^{new} - \mathbf{x}_i^{old})^2 \geq c \end{aligned} \tag{4.16}$$

is bounded from below, the optimum is attainable.

PROOF Let us begin from the objective function and the definition of 0-norm,

$$\| \mathbf{a} \|_0 = \| \mathbf{z}^{new} - \mathbf{z}^{old} \|_0 = \lim_{p \to 0} \sum_{k=1}^{n} |\mathbf{z}_k^{new} - \mathbf{z}_k^{old}|^p \tag{4.17}$$

expanding the term on right hand side,

$$\| \mathbf{z}^{new} - \mathbf{z}^{old} \|_0 = \lim_{p \to 0} [|\mathbf{z}_1^{new} - \mathbf{z}_1^{old}|^p + |\mathbf{z}_2^{new} - \mathbf{z}_2^{old}|^p + \cdots + |\mathbf{z}_n^{new} - \mathbf{z}_n^{old}|^p] \tag{4.18}$$

where the number of terms inside square brackets are n. As we are looking for the sparsest possible re-ordering attack, w.l.g, we can assume that at least one of those n terms is non-zero which leads to

$$\| \mathbf{z}^{new} - \mathbf{z}^{old} \|_0 = \lim_{p \to 0} [|\mathbf{z}_1^{new} - \mathbf{z}_1^{old}|^p + |0|^p + \cdots + |0|^p] \tag{4.19}$$

where we assume $\mathbf{z}_1^{new} - \mathbf{z}_1^{old}$ is the only non-zero entry,

$$\| \mathbf{z}^{new} - \mathbf{z}^{old} \|_0 = |\mathbf{z}_1^{new} - \mathbf{z}_1^{old}|^0 + |0|^0 + \cdots + |0|^0] \tag{4.20}$$

which leads to

$$\| \mathbf{z}^{new} - \mathbf{z}^{old} \|_0 = [|\mathbf{z}_1^{new} - \mathbf{z}_1^{old}|^0 + |0|^0 + \cdots + |0|^0] \tag{4.21}$$

and a sum of absolute values is always ≥ 0 which leads to

$$\| \mathbf{a} \|_0 = \| \mathbf{z}^{new} - \mathbf{z}^{old} \|_0 = [|\mathbf{z}_1^{new} - \mathbf{z}_1^{old}|^0 + |0|^0 + \cdots + |0|^0] \geq 0 \tag{4.22}$$

and it is showed that the objective function is bounded below hence, optimum to this problem is attainable. ■

4.1.2 Scenario II

For this case, the model is same as for scenario I with an additional constraint of a scalar multiple. This attack can be regarded as a constrained injection or a very specific case of injection. Here, to make the attack more effective, the adversary swap the measurements with a scalar multiple of one of the previous plausible data sets. The security metric defined in Eq. (4.7) is appropriate to measure the minimum possible sparsity pattern of the attack vector regardless of whether the magnitude is high or low. However, it is also possible that some attack vector may satisfy the sparsity criteria but instead due to large magnitude, be caught in detection. Therefore, another metric to keep the magnitudes of the swapping attack vector as low as possible while making the attack successful is required.

$$\begin{aligned} \text{minimize} \quad & \|\mathbf{a}\|_1 \\ \text{subject to} \quad & |\mathbf{z}^{new} - \mathbf{z}^{old}| \leq \epsilon \\ & \frac{1}{n}\Sigma_n(\mathbf{x}_i^{new} - \mathbf{x}_i^{old})^2 \geq c \end{aligned} \tag{4.23}$$

where the 1-norm of a vector **v** is $\|v_i\|_1 := \sum \mid v_i \mid$ and ϵ is a predefined scalar which will limit the attacker to swap relatively closer measurements and c is a scalar to ensure a non-zero attack vector each time.

The above problem is a convex optimization problem and can be re-cast into a linear program. The solution of the re-scaled problem can be used to obtain optimal attack vector $\mathbf{a}^*$ to achieve its goal of swapping and remaining unnoticed at the same time.

The proof of existence of its solution is similar to that of scenario I as here in scenario II, by definition of 1-norm, the objective function can be easily proved as bounded from below and hence the optimal solution is attainable in this scenario as well.

The corresponding small magnitude swapping attack vector obtained after solving the problem (4.18)

$$\mathbf{a} = \begin{cases} \mathbf{z}_i^{new} - d.\mathbf{z}_i^{old} & : \mathbf{z}_i \notin S_m \\ 0 & : otherwise \end{cases} \tag{4.24}$$

where d is an arbitrary scalar, "." represents element-wise scalar multiplication and S_m is the set of protected measurements as already defined.

4.1.3 Results

Before going into the detail of simulation results, it should be recalled that to perform re-ordering attacks, the attacker does not require the topology/subspace knowledge of the system unlike already proposed attack strategies. In this section, we discuss the performance of the above mentioned model in constructing the re-ordering attacks in both scenarios by simulations on IEEE 14 and 30-bus systems. It is worth mentioning here that for both scenarios discussed the following two conditions hold: firstly, without any re-ordering, it only takes 4 iterations till convergence and secondly, measurement re-ordering attack is performed after each complete round of WLS. The technique used to estimate the state is WLS and MATPOWER is used for loading the data for AC model.

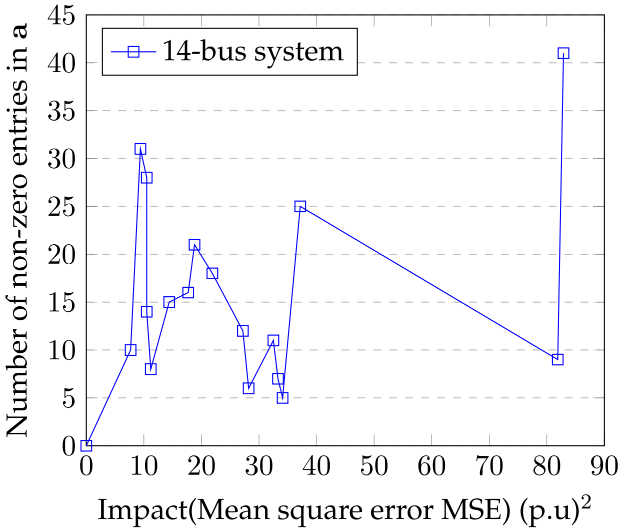

Figure 4.3: Optimum attack vector for Scenario I case I

Mean square error (MSE) versus re-ordering attack vector's sparsity for scenario I, is illustrated in Figs. 4.3 and 4.4 for 14 and 30-bus systems respectively. Several plausible measurement vector samples have been re-ordered and the sparsity and the mean squared error is shown. It can be seen in Fig. 4.3 that the sparsest attack vector $\mathbf{a}^*$ is $\|\mathbf{a}\|_0 = 5$ with the corresponding impact of $MSE = 34.1$. While in Fig. 4.4, the optimum attack vector has $\|\mathbf{a}\|_0 = 11$ with respective impact of 20.9 as MSE.

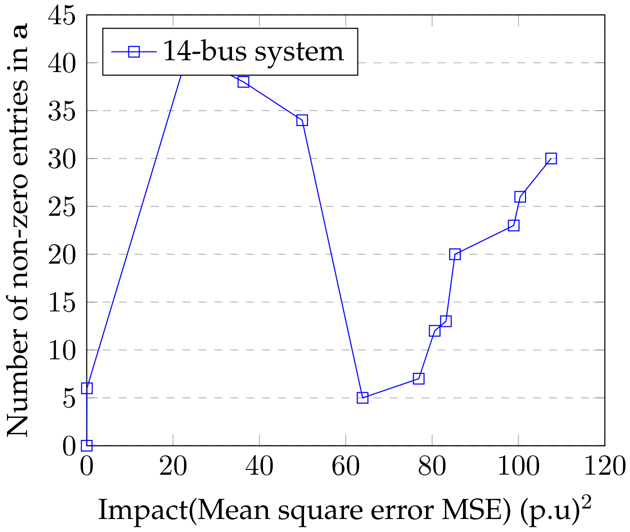

Figure 4.5: Optimum Attack vector for Scenario II case I

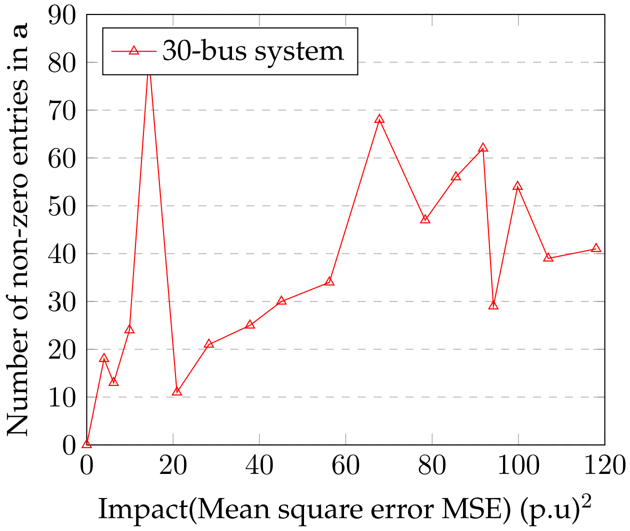

Figure 4.4: Optimum Attack vector for Scenario I case I

Similarly, MSE versus sparsity of re-ordering attack vector for scenario II, is illustrated in Figs. 4.5 and 4.6 for 14 and 30-bus systems respectively. Several plausible measurement vector samples have been re-ordered and the sparsity and the mean squared error is shown. It can be seen in Fig. 4.5 that the sparsest attack vector $\mathbf{a}^*$ is $\|\mathbf{a}\|_0 = 5$ with the corresponding impact of $MSE = 63.9$. While in Fig. 4.6, the optimum attack vector has $\|\mathbf{a}\|_0 = 8$ with respective impact of 10.9 as MSE.

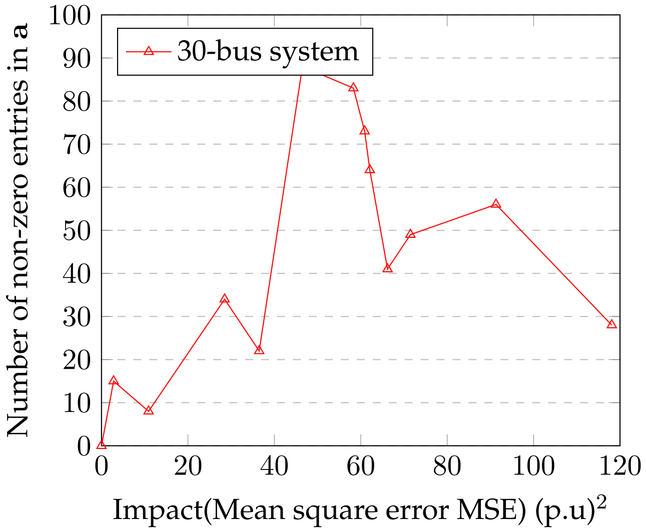

Figure 4.6: Optimum Attack vector for Scenario II case I

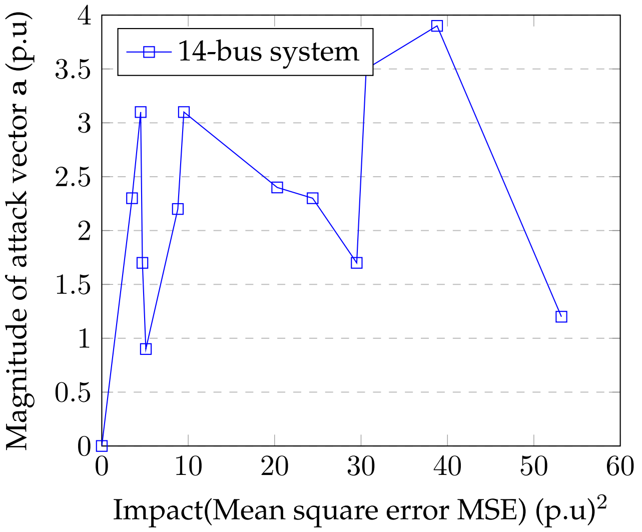

Figure 4.7: Optimum Attack vector for Scenario I case II

Mean square error (MSE) versus re-ordering attack vector's magnitude for scenario I, is illustrated in Figs. 4.7 and 4.8 for 14 and 30-bus systems respectively. Several plausible measurement vector samples have been re-ordered and the sparsity and the mean squared error is shown. It can be seen in Fig. 4.7 that the smallest attack vector $\mathbf{a}^*$ has magnitude $\|\mathbf{a}\|_1 = 0.9$ with the corresponding impact of $MSE = 5.1$. While in Fig. 4.8, the optimum attack vector's magnitude as $\|\mathbf{a}\|_1 = 4.2$ with respective impact of 33.75 as MSE. Mean square error (MSE) versus magnitude of re-ordering attack vector for scenario II, is illustrated in Figs. 4.9 and 4.10 for 14 and 30-bus systems respectively. Several plausible measurement vector samples have been re-ordered and the sparsity and the mean squared error

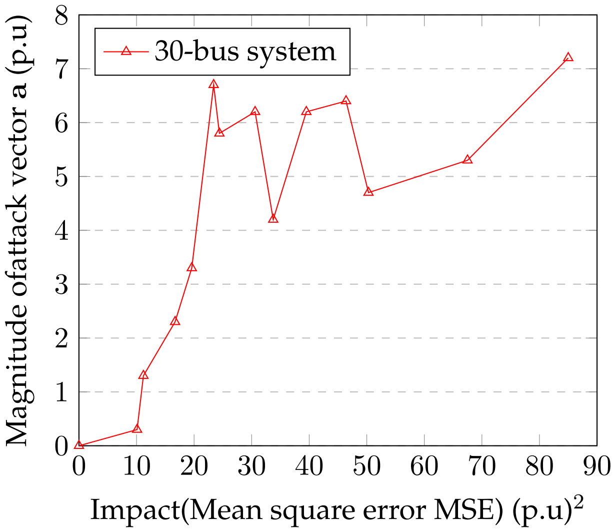

Figure 4.8: Optimum Attack vector for Scenario I case II

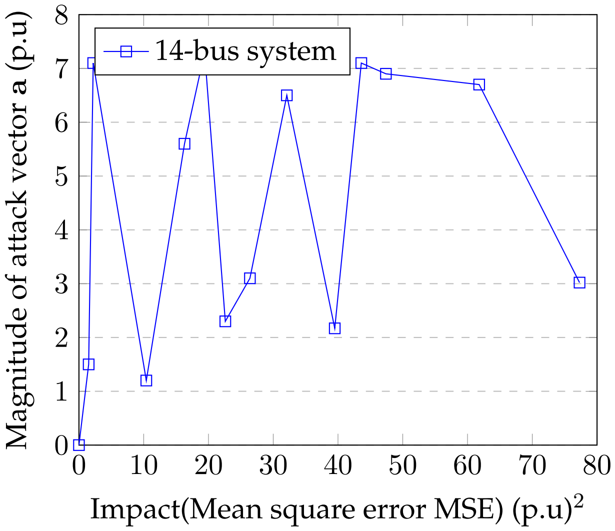

Figure 4.9: Optimum Attack vector for Scenario II case II

is shown. It can be seen in Fig. 4.9 that the optimum attack vector $\mathbf{a}^*$ has a magnitude of $\|\mathbf{a}\|_0 = 1.2$ with the corresponding impact of $MSE = 10.4$. While in Fig. 4.10, the optimum attack vector has $\|\mathbf{a}\|_1 = 1.2$ magnitude with respective impact of 16.5 as MSE.

After examining all of the above simulation results, we can infer that these swapping attacks are most appropriate even when a part of the system is integrity- and confidentiality-protected. Another aspect is that for power systems, as an attacker we did achieve the error in both scenarios with very low measurement reordering (cost) e.g., in Figs. 4.5 and Fig. 4.10.

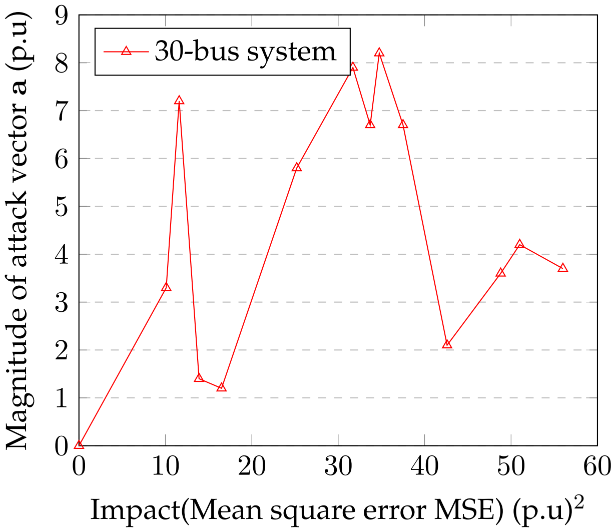

Figure 4.10: Optimum Attack vector for Scenario II case II

4.2 Propagation of Error in HSE after Re-ordering Attacks

False data and related attacks are well studied in conventional state estimation, but analysing the attack on hierarchical state estimation is not quite common. To the best of our knowledge, measurement swapping is not yet studied in hierarchical structure. Although false data attacks and delay/jamming attacks on HSE is explored by [9].

Therefore, our next task is to analyse the impacts of measurement swapping on hierarchical structure where the goal of measurement swapping on HSE is to create disruption in the control centre [39]. To attain this, we consider that the attacker is capable of re-ordering the measurement set $\mathbf{y}^0$ of only one partition $S^0 \in S$ in the lower level l_1 of hierarchy where S is the set of all partitions. As a result, the untrue state variables are being transmitted to the partitions at upper levels at the beginning of each iteration of HSE. Note that the Hierarchical formulation used here was proposed by Baiocco and Wolthusen in [10].

A structured re-ordering attack is considered while assuming the internal knowledge of the partitions to launch the re-ordering attack in a way that maximizes its effect. The knowledge required for the success of the re-ordering attack includes some previous plausible measurement set $\mathbf{y}_{old}$ of the targeted partition. The main objective of the attack is to have a desired/false local state estimate that propagate to higher levels to produce certain estimate $\mathbf{x}$.

The scheme we are following for the attack is a three level hierarchical structure with the following constraints:

- Once the attack is launched on a single partition of level l_1, the data exchange between the upper two levels i.e, l_2 and l_3 would still remain normal. That means there is no further attack on upper levels.
- The network configuration, i.e, the sub area partitioning at level l_2 and l_2 is not permitted to change over a course of full top-down synchro-upgrade

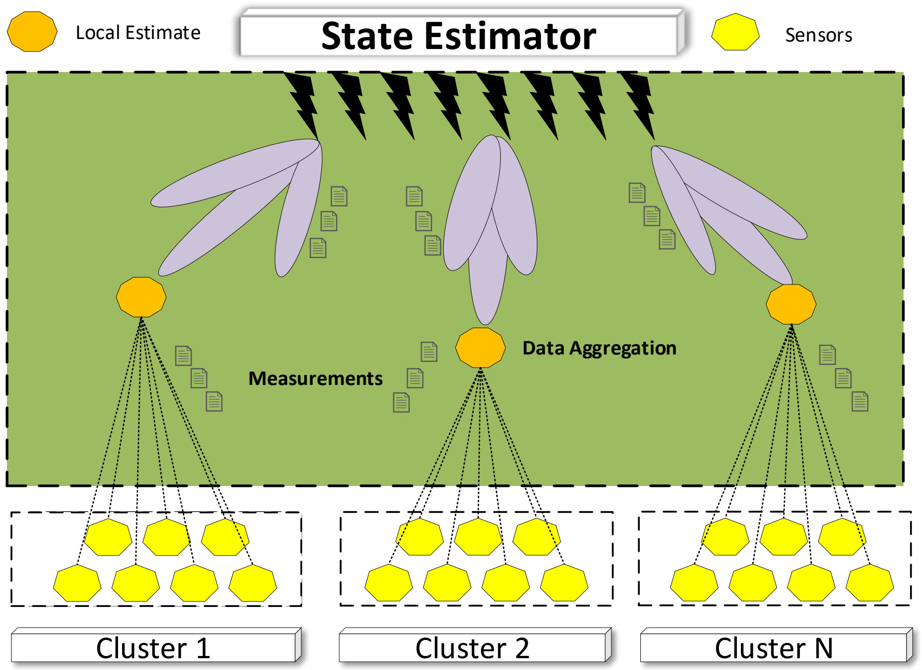

Figure 4.11: Communication network from sensors to estimator in hierarchical state estimation [64]

(This constraint is usually not required by HSE [10].

After the attack, the flow equations of the first level would be like

$$[\mathbf{F}_{1j}^T \mathbf{R}_{1j}^{-1} \mathbf{F}_{1j}^T]\hat{y}_{1j}^* = \mathbf{F}_{1j}^T \mathbf{R}_{1j}^{-1} \mathbf{y}_{0j}^* \tag{4.25}$$

where $\mathbf{y}_{0j}^*$ is the swapped measurement vector of one of the sub-areas at level one. The inputs at the second level $\mathbf{y}_{1j}^*$ for area $j = 1, 2$ are the false estimates from the first level and then

$$[\mathbf{F}_{2j}^T \mathbf{R}_{2j}^{-1} \mathbf{F}_{2j}^T]\hat{\mathbf{y}}_{2j}^* = \mathbf{F}_{2j}^T \mathbf{R}_{2j}^{-1} \mathbf{y}_{1j}^* \tag{4.26}$$

and finally, the output $\hat{\mathbf{x}}^*$ is the state of the entire system when solving the following Normal equations for the third level

$$[\mathbf{F}_3^T \mathbf{G}_2^{-1} \mathbf{F}_3^T]\hat{\mathbf{x}}^* = \mathbf{F}_3^T \mathbf{G}_2^{-1} \hat{\mathbf{y}}_2^* \tag{4.27}$$

where $\mathbf{y}_2^*$ and $\mathbf{G}_2$ are as defined earlier in section 2.6.2.

In case of False Data Injection (FDI), $\mathbf{a}$ generally denotes the attack vector that shows the amount of change to the original measurement vector [61].

$$\mathbf{a} = \mathbf{F}\mathbf{c}$$

where $\mathbf{c}$ is a vector denotes the magnitude of change and is bounded by some stealthy condition. Jamming or delay attacks can be seen as a sub-class of reordering as they resend the previous data with some time interval. Also, attacks performed by replaying or blocking the measurement vector can be considered a special case of re-ordering with a time constraint on them. The common aspect among all of the above is that there is no attack vector to be added, rather adversary just drop/block or jitter the measurements irrespective of whether they are secure/protected or not by hacking the communication infrastructure. Therefore, a general term, **re-ordering** of the measurement vector is introduced where the adversary swap the true measurement vector with the previously plausible (true) vector.

In this case, time horizon is critical for the attacker and it determines the strength of the attack. Being realist, we assume that the attacker has the measurement information from the present till some particular limited point in time. Within these time instances, the attacker can choose the measurement vector to be swapped the present one while avoiding detection. In other words, an attack that is successful in state forcing or non-convergence while being in-noticed by the model-based bad data detection. There may be more sophisticated detection criteria, of course, but these apply mostly to determining whether measurement devices (vector entries) are compromised, and that does not apply here. Other models rely on redundancy among measurements to determine compromise, but for a network-based attack this does not match very well.

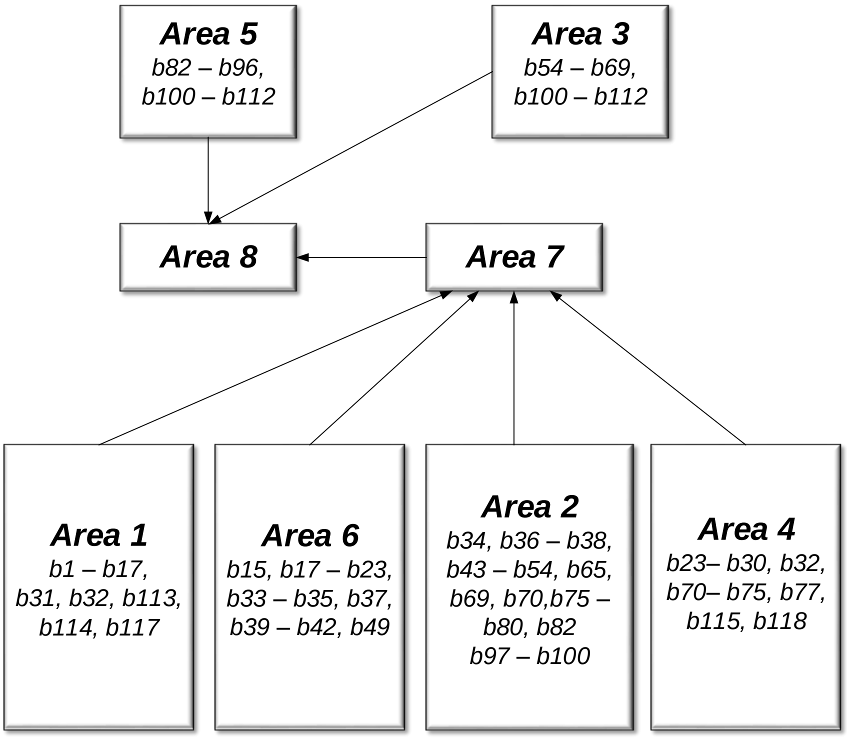

Figure 4.12: Bus-bars distribution of 118-bus system

4.2.1 Re-ordering Attack Cost and Attack Impact

We quantify the minimum attack cost as the attacking cost where attacker needs to put the least effort to get the maximum Mean Square Error (MSE) and denote it by Γ_y. All the regions in the power grid can be secured in one of the three ways, i.e. non tamper proof authentication ($S_{ntp} \subseteq S_m$), tamper-proof authentication ($S_{tp} \subseteq S_m$) or protected. Non-tamper proof authentication is of Bump-in-the-Wire (BITW) type device authentication or a Remote Terminal Unit (RTU) with a non tamper-proof authentication module. The regions with this type of authentication are only susceptible to attacks by some physical access to the region from where the data is originated. Tamper-proof authentication is not susceptible to attacks in any case. Other cases of protection are also possible by guards or video surveillance and generally this type is also not vulnerable to attacks. But realistically, all regions of the power grid can not be made protected by all means and there must be at least one region that is vulnerable ($S_{m'}$). If the region where the measurement vector to be attacked is located is protected and uses non tamper-proof authentication or tamper-proof authentication then the measurement is not vulnerable and we define $\Gamma_y = \infty$. Otherwise, for a measurement y, we define Γ_y as

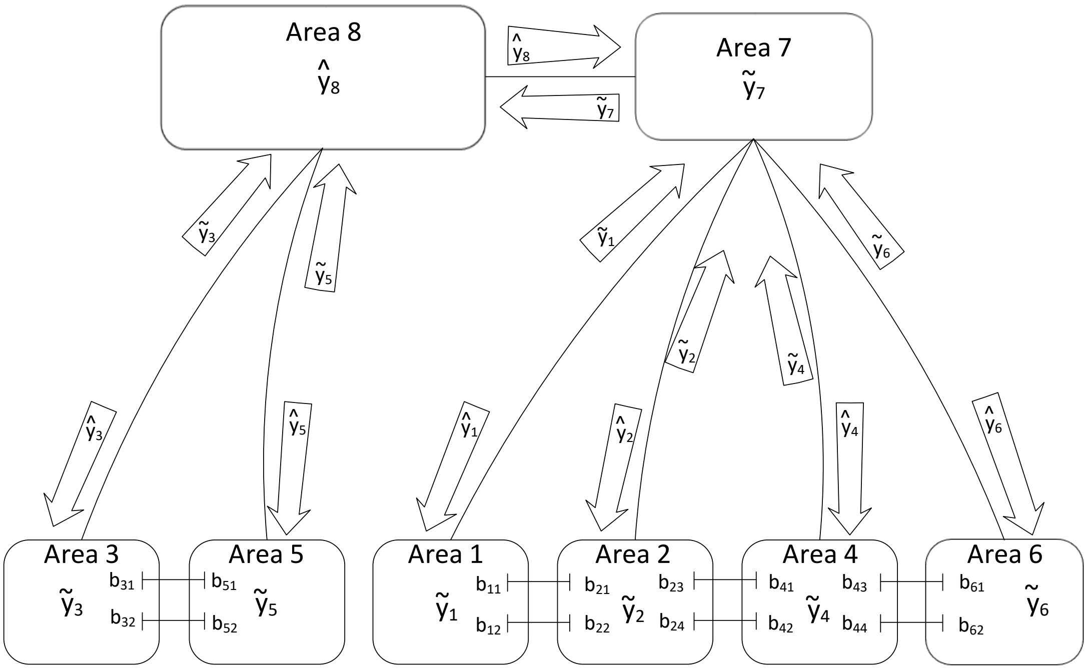

Figure 4.13: Information flow in Hierarchical State Estimation

$$\begin{aligned} &\min\ \|a\| \\ &\text{s.t. } \hat{y}^{new} - \hat{y}^{old} \leq \varepsilon \end{aligned} \tag{4.28}$$

and when $a(y) \neq 0$ it implies $|S(m')| \neq 0$, such that $S = S(m) \cup S(m')$ where S_m denotes authenticated areas/regions and $S_{m'}$ denotes the vulnerable areas s.t. $S = S(m) \cup S(m')$.

Similar to the one in re-ordering attacks on conventional state estimation, this optimization problem is convex and can be proved on the same lines to be attainable to the optimum value. Therefore, the proof is omitted here.

In addition, we assume that the attacker is free to choose the set from plausible measurements in a particular time frame to be used for re-ordering attack. As a result of this freedom and the attack cost (Γ_y) mentioned above, we quantify the maximum attack impact as the attacker's outcome and denote it by $\mathcal{I}_y$

$$\begin{aligned} &\mathcal{I}_y = \max \;\; I = \sqrt{\sum (\tilde{\mathbf{y}}^{new} - \tilde{\mathbf{y}}^{old})^2} \\ &\text{s.t.} \;\;\; t^{new} - t^{old} \geqslant \epsilon \end{aligned} \tag{4.29}$$

where t denotes the time slot among the available time frames to the attacker and ϵ is the pre-defined threshold to limit the attacker's choice. Superscripts "old" and "new" denotes the measurement used in the swapping and the measurement to be swapped respectively.

Theorem 4.4 (Existence of optimum attack in hierarchical structure) *Consider the following optimization problem*

$$\begin{aligned} &max \;\; \sqrt{\sum (\tilde{\mathbf{y}}^{new} - \tilde{\mathbf{y}}^{old})^2} \\ &s.t. \;\;\; t^{new} - t^{old} \geqslant \epsilon \end{aligned} \tag{4.30}$$

its optimum solution is attainable if the objective function is bounded below.

Proof First, we transform the optimization problem into standard form as

$$\begin{aligned} &\min \;\; -\sqrt{\sum (\tilde{\mathbf{y}}^{new} - \tilde{\mathbf{y}}^{old})^2} \\ &\text{s.t.} \;\;\; t^{old} - t^{new} \leq \epsilon \end{aligned} \tag{4.31}$$

The objective function can be then written as

$$f = \sqrt{(-1)^2}\sqrt{\sum (\tilde{\mathbf{y}}^{new} - \tilde{\mathbf{y}}^{old})^2} \tag{4.32}$$

or

$$f = \sqrt{(-1)^2 \sum (\tilde{\mathbf{y}}^{new} - \tilde{\mathbf{y}}^{old})^2} \tag{4.33}$$

which is

$$f = \sqrt{\sum (\tilde{\mathbf{y}}^{new} - \tilde{\mathbf{y}}^{old})^2} \tag{4.34}$$

w.l.g., at least one term inside square root on right hand side will be non-zero in case of attack, therefore

$$f = \sqrt{\sum (\tilde{\mathbf{y}}^{new} - \tilde{\mathbf{y}}^{old})^2} \geq 0 \tag{4.35}$$

and it is proved that the objective function is bounded from below. Hence optimum of this problem is attainable. ■

4.2.2 Numerical Results

Before going into the detail of simulation results, it should be recalled that to perform re-ordering attacks, the attacker requires the topology/subspace knowledge of the system and it is assumed that the topology is not changing or it is static in the duration of the attack. In this section, we discuss the performance of the above mentioned model in constructing the re-ordering attacks on each region of a hierarchical state estimation by simulations on IEEE 118-bus systems. We divide the 118-bus system into 6 sub-areas/regions and additionally there is an intermediate level between the top and bottom layers (shown in Fig. 4.12). Since the presented hierarchical model is two-way synchro-upgrade model as shown in Fig. 4.13, i.e., at first, from lower level to the top-most and then the way back to the bottom levels again, it is very interesting to see the error propagation after the proposed attack. The attacker is free to choose the particular data set from a certain time frame i.e, attacker has a limited amount previous data knowledge. The technique used to estimate the state is WLS and MATPOWER is used for loading the data for AC model.

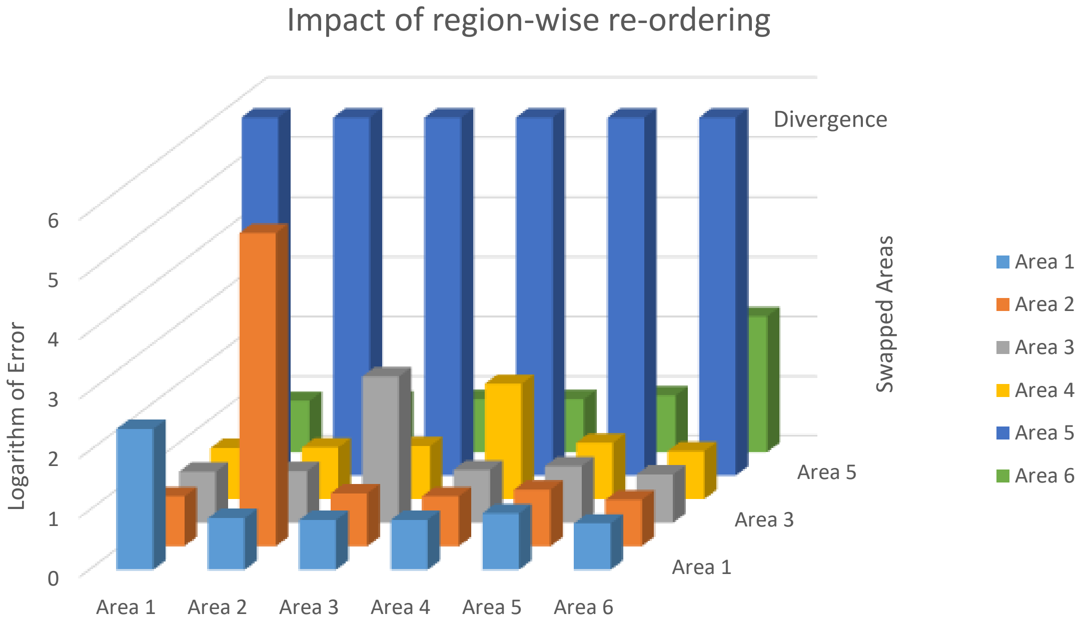

Figure 4.14: Effect of re-ordering at lower level of HSE

Mean square error (MSE) after performing least cost re-ordering attack of described earlier, is illustrated in Fig. 4.14 for 118-bus system. Figure denotes the logarithm (base 10) of MSE for one complete round of WLS state estimation i.e., from the lower layer to the top (Fig. 4.14) and all the way down detailing how that error propagates from the lower level to the top and back again. We can clearly see that in the end of a complete round after re-ordering attack, all areas are affected no matter what the intensity is and which area is re-ordered individually. The important point to notice is the epidemic property of the attack and it shows the error propagation from one infected area at lower level to all the areas at lower level.

The plot illustrates how a single area from lower level hierarchy influence all the areas at lower level such that the attacker can choose for the cheapest and the most vulnerable area to perform the attack. An obvious observation is that the error is maximum for the areas from where the attack originates. In the given partitioning of 118-bus system, area-5 seems to be the most vulnerable as the system diverges when the input data is re-ordered. It is worth noting here that the partitioning of 118-bus system for the re-ordering is a particular one and other cases may exist.

4.3 Countermeasures of Re-ordering Attacks

Generally, the process of estimating the states is based on data gathering, observability analysis and topology processing i.e., to check if there are enough measurements in the power grid to determine its state to provides protection, monitoring and control. Hence, IEEE C37.118 (details in section 2.1.1.1) and IEC 61850-90-5 (details in section 2.1.1.2) emerged as two well known communication frameworks for data transmission in the grid.

Furthermore, protocols like IEEE C37.118 and IEC 618-90-5 have built-in commands to accept messages only up to a certain time interval i.e., each of them have their particular time limits for measurement acceptance. While IEEE C37.118 is susceptible to timing related attacks, IEC 618-90-5 has a definite acceptable range (in context of time) for measurement reporting [50].

The study on countermeasures for the proposed re-ordering attacks (for both conventional and hierarchical infrastructure) is one of our ongoing works. However, to prove the effectiveness of these attacks, a discussion on potential countermeasures is desirable. As analysed in the previous sections 4.1 and 4.2 , there exist control system's protocols that are not robust against measurement re-ordering attack.

Two of the possible countermeasures are timestamp based and Cryptographic nonce based methods (as shown in Fig. 4.15, packets are transmitted from sensor to the control centre using timestamp or cryptographic nonce) which are as follows:

4.3.1 Timestamp Based Countermeasure

In timestamp based countermeasure, synchronized and secured time clocks can be used such that swapping attacks can be prevented. A typical timestamp based scheme via digital signature $\mathcal{E}_k(M||t)$, t is time stamp, M is the message or data, k is the key and $\mathcal{E}$ represents encryption.

is a mechanism where we transmit the signature along with the data packet and the timestamp. The control center check the timestamps to ensure them to be in an acceptable range of current time.

In case of PMU for example, the demand for additional processing and communication overhead will increase due to the addition of time stamp value in the packet size, and encryption and decryption functions at both ends may be expensive. Secondly, it may add little delay in communication due to additional time to encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ each packet before sending and after receiving respectively. The other main issue is trusted time source to ensure the freshness of each packet i.e., synchronization of nodes with the trusted time source will be required.

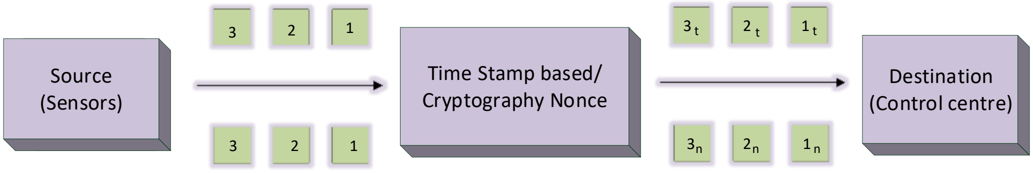

Figure 4.15: Timestamp based and Cryptography based order validation

4.3.2 Using Cryptographic nonce

We can also deploy cryptographic encryption to detect if somebody has sent these measurements before by keeping history of measurements. A typical symmetric encryption using cryptographic nonce is such that, for each data packet M from sensors, attach a nonce n Encrypt the hash with the public key $\mathcal{E}_k(M||n)$ and then transmit the signature along with the data packet and the nonce.

Using cryptographic nonce can prevent message swapping but the calculations are expensive and not constant time, i.e. it differs for each system along with the requirement of additional storage. Also, reporting delay caused by encryption and decryption must be incorporated.

The nonce requires some level of persistence, since it only works if uniqueness is guaranteed and checked. Also, if the man in the middle can interrupt the sender, get the nonce, and keep the sender from sending it, the man in the middle attack could still be successful.

4.4 Conclusion

The measurement re-ordering attack as described in section 4.1.1 is made to work even if some parts of power system are integrity protected. Key observation is that currently in our power grid, the measurements are not authenticated time-stamped to detect such re-ordering and such authentication for detection purposes is adequately expensive to implement at least till near future. But, even assuming time-stamped authentication, which is offered by ISO/IEC 62351 but not widely deployed at present, re-ordering attacks may still succeed when combined with message spoofing. This implies that as long as there are old components in our power network, there can be a chance of these kind of attacks. But, in ten years time, cryptographically time-stamped authentication can be made possible leaving the re-ordering attack less effective.

We have introduced a new attack on power systems termed as *re-ordering attacks*, where the adversary uses swapping as a tool to change the order of data while not injecting or modifying any data. Due to targeted re-ordering, it become very difficult for the system operator to detect the source of the error. Two cases for the attacker depending upon the nature of swapping are discussed, and it is demonstrated that, in all of the described cases, we can be successful in achieving malicious goals i.e. state estimation converges for both cases but with an adequate error and even divergence. The significance of the presented attack lies in its applicability despite modern protections.

We proposed an attack termed as *re-ordering attacks* on hierarchical state estimation as well that we introduced earlier where the adversary uses swapping of data sets as a tool to swap the order of data with some previous data set while not injecting or modifying any data. The present work relied on the fact that not all parts of the grid can be made tamper/non-tamper proof authenticated over night. Therefore, a targeted re-ordering attack on the most vulnerable region of the system is studied that can provide desirable propagation of error all over the system and not just the attacked area. Moreover, it can be clearly seen that such an attacker can force the estimate of a authenticated region by launching an intelligent attack in less protected region.

Chapter 5

Topology Related Attacks

The deployment of PMUs allows topology change detection schemes that are substantially faster and more accurate than existing approaches [88, 7]. The major issue related to this advancement is the cost of these advanced devices. Due to this constraint, there are still thousands of branches with no PMUs, thereby leaving room for the attackers. Even if it is possible to have PMUs at every line, these devices are themselves possible to attack such as by targeting the all-important time reference signal obtained typically from GNSS satellite configurations. As PMUs generally rely on un-authenticated civilian signals such as the NAVSTAR (GPS) C/A code, spoofing or denial of service (DoS) is easily and inexpensively achieved [82].

5.1 General Line Failures

An undetectable topology fault (attack) is a line failure deliberately induced by attacker by changing a single switch/breaker status (e.g. via SCADA or in a physical attack) to create misconceptions among system operators while suppressing the resulting alert or response to polling requests. Alternatively, an attacker may seek to fool a TSO/DSO system operator into believing that a topology change has occurred, while no such change has taken place; this is again possible to achieve through network-based attacks on the monitoring system whose realisation are beyond the scope of our work. Un-planned topology errors may also arise from natural causes such as lightning strikes, earthquakes, high winds, ice formation, or flooding. Here, however, we are focusing only on deliberate topology attacks.

To understand the power grid behaviour upon these changes, we need to estate some facts. Liu. et al. proposed undetectable data attacks on state estimation and the undetectability condition is:

Theorem 5.1 (Stealth Condition for False Data Injection Attack [61])
Suppose the original measurements $\mathbf{z}$ *can pass the bad measurement detection. The malicious measurements* $\bar{\mathbf{z}} = \mathbf{z} + \mathbf{a}$ *can pass the bad measurement detection if* $\mathbf{a}$ *lies in a column space of* $\mathbf{H}$ *i.e.,* $\mathbf{a} \in Col(\mathbf{H})$.

PROOF Since $\mathbf{z}$ can pass the detection, we have $\| \; \mathbf{z} - \hat{H}\mathbf{x} \; \| \leq \tau$, where τ is the detection threshold. $\hat{\mathbf{x}}_{bad}$, the vector of estimated state variables obtained from $\mathbf{z}_a$, can be represented as $\hat{\mathbf{x}} + c$. If $\mathbf{a} = \mathbf{Hc}$, i.e., a is a linear combination of the column vectors $h1, \cdots, hn$ of $\mathbf{H}$, then the resulting L2-norm of the measurement residual is

$$\begin{aligned} \| \; \mathbf{z}_a - \mathbf{H}\hat{x}_{bad} \; \| &= \| \; \mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c}) \; \| \\ &= \| \; \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{Hc}) \; \| \\ &= \| \; \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \; \| \leq \tau \end{aligned} \tag{5.1}$$

Thus, the L_2-norm of the measurement residual of $\mathbf{z_a}$ is less than the threshold τ. This means that $\mathbf{z}_a$ can also pass the bad measurement direction. ■

For a topology attack $\bar{\mathcal{G}}$, the above undetectability condition will be:

Theorem 5.2 (Stealth Condition for Topology Attack)
Suppose the original measurement set $(\mathbf{z};\mathbf{s})$ can pass the bad measurement detection. The malicious measurements $\bar{\mathbf{z}} = \mathbf{z} + \mathbf{a}$ can pass the bad measurement detection if $\bar{\mathbf{z}}$ lies in a column space of $\hat{\mathbf{H}}$ where s denotes the topological data and $\hat{\mathbf{H}}$ is the measurement matrix after topology attack $\bar{\mathcal{G}}$ [51].

5.1.1 Attack Model

In this section, we aim to review the adversary model for topology change in power grid state estimation. The attacker intends to change the current topology $\mathcal{G}$ to a desired topology $\bar{\mathcal{G}} = (\mathcal{V}, \bar{\mathcal{E}})$. We are only considering line faults, therefore, the number of vertices $\mathcal{V}$ (bus-bars) will remain the same during the attack but the number of edges $\mathcal{E}$ (transmission lines) will become $\bar{\mathcal{E}}$ where $\bar{\mathcal{E}} \subset \mathcal{E}$. The lines that are not common in $\mathcal{E}$ and $\bar{\mathcal{E}}$ are called *attacked lines* and the buses with which target lines are connected are called *attacked buses*.

To launch the topology attack, the attacker needs to change the topology and send over the false topology $\bar{\mathcal{G}}$ to the control center by commencing e.g., a man-in-the-middle attack initially. This way, the attacker obstructs the input data $(\mathbf{s}, \mathbf{z})$ from RTUs, alters the desired information and send the revised data $(\bar{\mathbf{s}}, \bar{\mathbf{z}})$ to the control center. Prior to the attack, a very small fraction of the input data $(\mathbf{s}, \mathbf{z})$ is assumed to be known to the attacker. Such a restricted access to the system parameters and information is the key point in this work. In our ongoing work, we seek to efficiently recover the missing information after such dominant attacks and hence the impact of such attacks.

The attack model to alter the topology from $\mathcal{G}$ to $\bar{\mathcal{G}}$ is as follows:

$$\begin{aligned} \bar{\mathbf{z}} &= \mathbf{z} + \mathbf{a}, \quad \mathbf{a} \in \mathcal{A} \\ \bar{\mathbf{s}} &= \mathbf{s} + \mathbf{b}, \quad \mathbf{b} \in \{0, 1\} \end{aligned} \tag{5.2}$$

where $\bar{\mathbf{z}}$ is the new measurement vector, $\mathbf{a}$ is the attack vector to be added up, $\mathcal{A}$ is the attack vector subspace for all the feasible attacks and $\mathbf{b}$ is the binary vector to be added up in the network topology data $\mathbf{s}$. Here, the term feasible is related to sparsity and low magnitude of the attack vectors. Therefore, $\mathbf{a}$ is any attack vector in $\mathcal{A}$ that satisfies the sparsity and low magnitude criteria as in [37].

The combination of data and topology attacks will allow it to be undetectable as otherwise, if there is only the topology that the attacker can modify, it can easily be caught in detection through the data of the missing lines. We assume the noiseless case to begin with and leaving the noisy measurement case for future research.

We assume that it is not possible for the attacker to modify more than a couple of switch/breaker statuses to launch undetectable topology attacks and similarly for the data attack to alter the measurement vector due to the access/cost constraints for the attacker. Therefore, the attack vector $\mathbf{a}$ is usually sparse, which shows the validity of the attack as if the attacker has access to a desired substation to drop the line(s), she can also modify a handful of measurements to satisfy the undetectability condition by hacking/tampering with communication to the control centre.

Even if the system is robust against single line failures, the proposed approach ascertains the success of adversary by keeping the fault undetected. In addition, *double-line faults* are also proposed focusing on concurrent failure of two lines.

5.1.2 Least Cost Topology Attack

Definition 5.1 (Cut-Set)
A cut-set is the set of edges between the two parts of a bipartition of the vertices in a graph. So if a graph has n vertices, there are $2^{n-1} - 1$ ways to partition those vertices into two non-empty subsets.

Let $\mathcal{E}' \subset \mathcal{E}$ be the cut-set of all such edges (1-cuts) in a graph. We call such edges as critical edges. In power engineering terms, a critical edge is a transmission line between a pair of buses whose removal leave the system disconnected. Once topology changes in a power system, operator needs to check whether this change violate the pre-conditions of the topology algorithm. If yes, then the best possibility is to re-run the whole state estimation with the changed topology. Note that we are only considering single/double line faults here.

We are considering the power network as a graph connecting bus bars ($\mathcal{V}$) through transmission lines ($\mathcal{E}$). The resulting sub-graph obtained after the single line failure (removal of one edge) must satisfy the following necessary but not sufficient condition in order to keep the power grid well operating:

- The resulting sub-graph should be connected.

In the perspective of attacker, the system operator must be unaware of the attack i.e, the attack must be undetectable. Following the condition of undetectability in the beginning of section 5.1, the attacker needs to choose the lines according to available resources to give a desired impact. To make such undetectable attacks possible, attackers need to modify a few entries of the measurement vector as well to justify the changed topology. Otherwise, the meter readings would not match the topology that operators think as true and the operators could simply reject the data and go for contingency analysis.

We initiate the terms critical attack size p^* and system robustness $n_\infty(p)$ for an attack size p. Critical attacks can be seen as DoS attacks or an attack in which at least one critical line is involved, and by size we mean the total cost of all the modifications it require to launch such attack i.e.,

$$\mathbf{p} = \beta\mathbf{a} + \gamma\mathbf{b}, \quad \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \{0,1\}^d \tag{5.3}$$

where β and γ are the coefficients which are used to give weights to the respective attack vectors according to the effort/cost required by the attacker to get the least cost attack and $\mathbf{a}$ and $\mathbf{b}$ are as already defined. When considering single line failure, we assume the the false data injection to $\mathbf{a}$ to suppress the line failure will be $\mathbf{a} = [a_1, a_2, 0, \cdots, 0]$ and $\mathbf{b} = [1, 0, \cdots, 0]$. Similarly, we assume that when double line failure

The metric for system robustness $n_\infty(\mathbf{p})$ should ideally be 1. But, for a critical attack $\mathbf{p} = \mathbf{p}^*$, this metric is $n_\infty(\mathbf{p}^*) = 0$ which means a complete breakdown of the system. For all the other attack scenarios, the system robustness is greater than zero but less 1 and so is here where the reason of limiting the system robustness $n_\infty(\mathbf{p})$ to a particular attack is to increase the impact of the attack. The optimal attack $\mathbf{a}^*$ can be determined by solving a convex optimization problem as

$$\begin{aligned} &\text{minimize} && ||\mathbf{p}|| \\ &\text{subject to} && |\mathbf{a}| = |\bar{\mathbf{z}} - \mathbf{z}| \leq \eta \end{aligned} \tag{5.4}$$

where $||.||$ of any vector $\mathbf{v}$ is the sum of the squares of entries in $\mathbf{v}_i$, p is the cost of the attack as already defined and η is the maximum resources the attacker has. In other words, η is a combination of number of modifications the attacker can make and the maximum acceptable magnitude.

Following the lemmas 4.1 and 4.2, we now show that the optimization problem (5.4) has an optimal solution. For that, considering $\mathbf{a} = \{a_1, a_2, \cdots, a_n\}$ and $\mathbf{b} = \{b_1, b_2, \cdots, b_n\}$ we can rewrite

$$||\mathbf{p}|| = ||\beta\mathbf{a} + \gamma\mathbf{b}|| \tag{5.5}$$

as

$$||\mathbf{p}|| = ||\beta \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} + \gamma \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} || \tag{5.6}$$

$$||\mathbf{p}|| = || \begin{bmatrix} \beta a_1 \\ \beta a_2 \\ \vdots \\ \beta a_n \end{bmatrix} + \begin{bmatrix} \gamma b_1 \\ \gamma b_2 \\ \vdots \\ \gamma b_n \end{bmatrix} || \tag{5.7}$$

$$||\mathbf{p}|| = || \begin{bmatrix} \beta a_1 + \gamma b_1 \\ \beta a_2 + \gamma b_2 \\ \vdots \\ \beta a_n + \gamma b_n \end{bmatrix} || \tag{5.8}$$

$$||\mathbf{p}|| = (\beta a_1 + \gamma b_1)^2 + (\beta a_2 + \gamma b_2)^2 \cdots (\beta a_n + \gamma b_n)^2 \tag{5.9}$$

Applying Lemma 4.2 to our optimization problem (5.4), it becomes

Theorem 5.3 (Existence of optimum topology attack)
If

$$\begin{aligned} &\textit{minimize} && ||\mathbf{p}|| = (\beta a_1 + \gamma b_1)^2 + (\beta a_2 + \gamma b_2)^2 \cdots + (\beta a_n + \gamma b_n)^2 \\ &\textit{subject to} && |\mathbf{a}| \leq \eta \end{aligned} \tag{5.10}$$

is bounded below over a feasible region, then its optimal solution is attainable.

Proof We will start by expanding $\mathbf{a}$ as

$$|\mathbf{a}| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2} \tag{5.11}$$

where $|\mathbf{a}| \leq \eta$,

$$a_1^2 + a_2 + \cdots + a_n^2 \leq \eta^2 = \zeta \tag{5.12}$$

where $\zeta = \eta^2$. We are only considering single and double line faults here and $\mathbf{b}$ represents the topology changes, therefore either $\mathbf{b} = (1, 0, \cdots, 0)$ or $\mathbf{b} = (1, 1, \cdots, 0)$ making Eq. (5.9) as

$$f = \|\mathbf{p}\| = (\beta a_1 + \gamma)^2 + \beta a_2^2 + \cdots + \beta a_n^2 \tag{5.13}$$

or

$$f = (\beta a_1 + \gamma)^2 + (\beta a_2 + \gamma)^2 + \beta a_3^2 + \cdots + \beta a_n^2 \tag{5.14}$$

w.l.g, we are considering the double line failure, as follows

$$f = \beta^2 a_1^2 + \gamma^2 + 2\beta\gamma a_1 + \beta^2 a_2^2 + \gamma^2 + \beta\gamma a_2 + \beta a_3^2 + \cdots + \beta a_n^2 \tag{5.15}$$

$$f = \beta^2 (a_1^2 + a_2^2 + \cdots + a_n^2) + 2\gamma^2 + 2\beta\gamma(a_1 + a_2) \tag{5.16}$$

It is obviously,

$$\beta^2 (a_1^2 + a_2^2 + \cdots + a_n^2) + 2\gamma^2 + 2\beta\gamma(a_1 + a_2) \geq (a_1^2 + a_2^2 + \cdots + a_n^2) \tag{5.17}$$

Arbitrarily assuming $\beta = \gamma = 1$

$$(a_1^2 + a_2^2 + \cdots + a_n^2) + 2 + 2(a_1 + a_2) \geq (a_1^2 + a_2^2 + \cdots + a_n^2) = \nu \tag{5.18}$$

and finally, we can show that the objective function is bounded from below to a number ν which is the size of the measurement manipulations from the attacker.

$$(a_1^2 + a_2^2 + \cdots + a_n^2) + 2 + 2(a_1 + a_2) \geq \nu \tag{5.19}$$

as the function f is bounded below, it is proved that the optimum is attainable. ■

The theorem about existence of infimum can be validated in Figure 5.1.

Example 2 Observe that the attacker can solve the above optimization problem (5.4) with only a fraction of the entire measurement vector information. For example, for 14-bus system as in Fig. 5.2, if the attacker want to initialize a single-line fault, with the parameters as $\beta = \gamma = 1$, the cost (number of modifications required) will be 3 if the targeted line is non-critical and the value of the metric is higher if the line to be attacked is the critical line due to the presence of additional protection that system operators have deployed to secure that line. □

5.2 Results

Before going into the detail of simulation results, it should be recalled that as an adversary, we consider undetectable (single/double line) topology attacks considering the conventional centralised state estimation. The technique used to estimate the state is WLS and MATPOWER is used for loading the data for IEEE 118 and 300 test beds. Note that without any topology error 118-bus system takes 5 iterations to convergence and for 300, convergence needs 14 iterations. As the attacker desires an undetectable topology change, the number of iterations in this case remains the same.

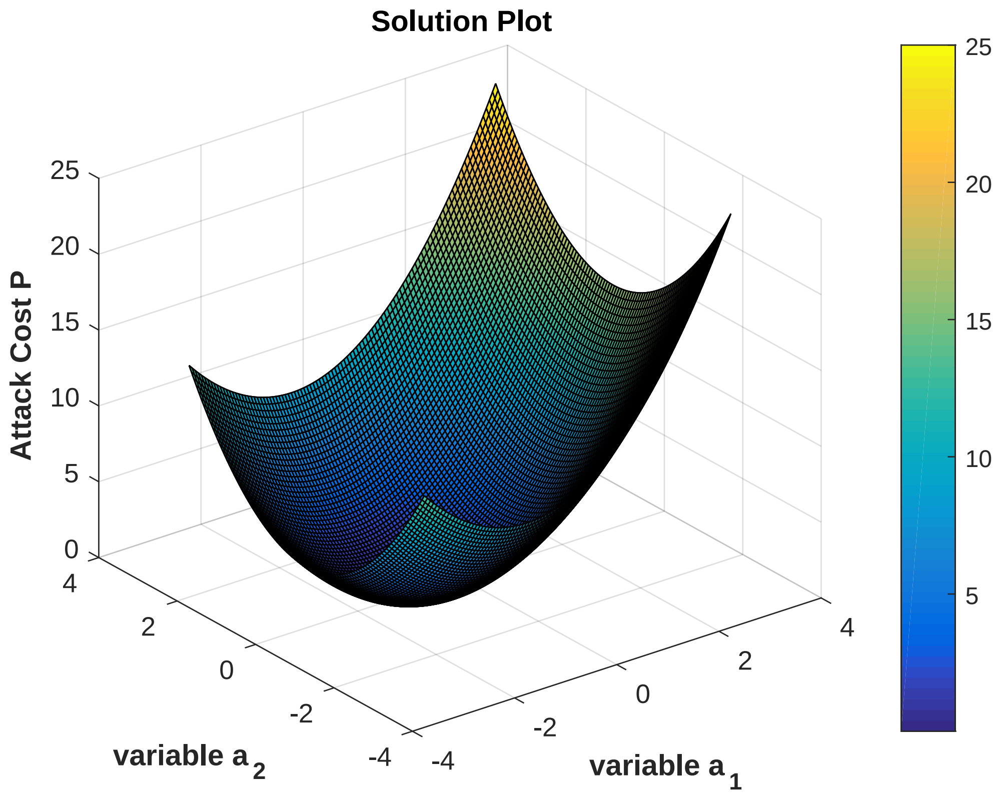

Figure 5.1: Solution plot for a single line failure (axis have scalars therefore, no units)

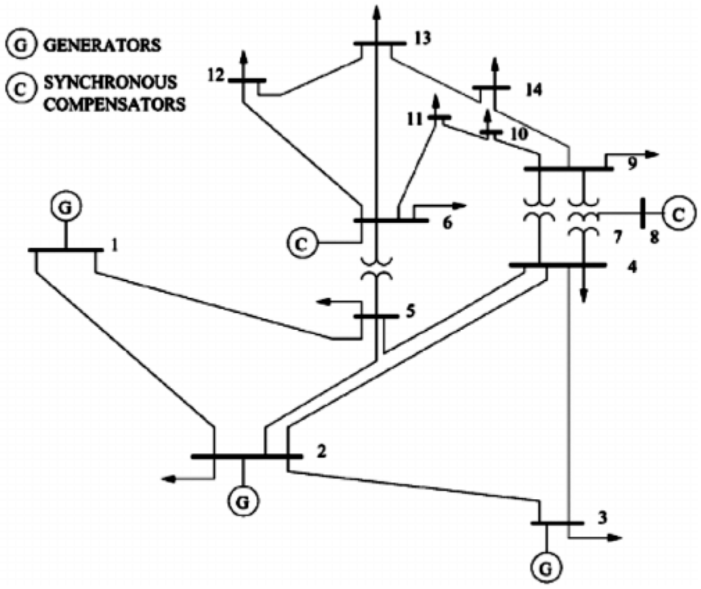

Figure 5.2: Single-line diagram of 14-bus system

Table 5.1: Single-line faults in 118 and 300-bus system

Test case	Failed line	Criticality	Error (MSE)
118-bus system	$5-6$	non-critical	0.5
	$86-87$	critical	∞
	$77-78$	non-critical	0.44
300-bus system	$20-27$	non-critical	0.92
	$108-31$	critical	∞
	$243-244$	non-critical	0.27

Table 5.2: Double-line faults in 118 and 300-bus system

Test case	Failed lines	Criticality	Error (MSE)
118-bus system	$1-3,\ 4-5$	non-critical	74.2
	$56-57,\ 50-57$	1 critical	∞
	$9-10,\ 86-87$	both critical	∞
300-bus system	$12-21,\ 25-26$	non-critical	297
	$119-75,\ 95-1$	both critical	∞
	$254-39,\ 35-72$	1-critical	∞

We repeat the process N times for single-line fault whereas $\binom{N}{2}$ times for double-line faults, where N is the total number of lines in each system. Results show that the base case i.e., single line fault has a negligible effect unless it is critical line. After N simulations for each bus system, we got a set of critical lines i.e, for 118-bus system, 11 lines are critical and for 300-bus system, they are 69. Note that the single line failure is only considered as a base case while double-line faults are our main focus.

For double-line faults, all the three cases are considered, 1) when both lines are non-critical, 2) when both are critical and 3) when one line among the double-line failure is critical. Generally, system operators are aware about the critical lines in the system and usually put more effort to secure those lines/locations. We assume that the attacker has knowledge about the criticality of the attacked line. For the first case, the attacker achieves state forcing while for the other two cases, divergence of the state estimation is guaranteed.

In tables 5.1 and 5.2, we made a comparison of the mean square error (MSE) of the state vectors before and after single and double topology faults, respectively. It is illustrated that our proposed attack scheme works for all cases of double-line failures while as expected, the single-line faults are effective only if the targeted line is critical. For the simulations, we made 3 random lines and 3 random pairs of lines fail for both types of attacks and the test cases, respectively. In both tables, the term ∞ denotes divergence of the power system state estimation after the respective failure. The least cost topology attack would depend on how powerful is the protection of the desired location and therefore, also on the criticality of underlying lines.

5.3 In-Cycle sequential Topology Attacks

With a dynamic power grid that we have today, it is fair to expect frequent topology changes. The expertise of power engineers rely on the smooth and steady operation of the grid despite these recurrent changes in topology. Deployment of Phasor Measurement Units (PMUs) is allowing topology change detection schemes to be more accurate and significantly faster [58], [88]. Hundreds of PMUs are being deployed round the globe to increase the redundancy in measurement vector and help getting topology changes detected, therefore contributing to more secure power grid. Due to the cost constraint, there are still thousands of branches with no PMUs leaving room for the attackers. Even if it is possible to have PMUs at every line, there is still a potential chance for the attacker such as by aiming at GPS, a time reference signal upon which generally all PMUs rely. Spoofing of such signals is very common and inexpensive source to create confusion about the correct signals in the control centre.

In general, the PMU reporting rate ranges between $10 - 60$ samples per second evenly aligned to hour (min and sec). Higher reporting rates of $100 - 240$ samples per second are allowed and available with advance PMU devices.

Details of the undetectable single/multiple topology attack and the related possibilities for the attacker to create misconception among the operators can be found in [41]. Here, we are introducing a novel **sequential topology attack** that goes undetected due to its reverse nature. In addition, in both of our works i.e., the previous and the present one, we consider these faults as a result of deliberately induced error. However, such errors can also emerge due to some natural reasons for example thunderstorms, earthquakes, floods, or even high winds that are not under the scope of this work.

5.3.1 Adversary Model

In this section, we intend to analyse the attack model for transient topology changes in a single scan cycle. There are usually two scenarios when SCADA systems transmit the measurement data collected from sensors i.e., I) the devices will sent a message if something interesting/unusual happens and II) SCADA systems need to complete its scan/poll cycle despite of some changes. Theoretically, former is correct as protocols allow one to perform it but such a synchronization is relatively uncommon. Contrarily, later is common traditionally which is a deterministic real-time behaviour where every deadline is maintained within a certain time period.

As an attacker, we are considering the most widely used behaviour of SCADA systems where SCADA take a definite amount of time after coming back to the same sensor. In fact some sensors are slightly slower or faster compared to others. In other words, there must be an interval between each time the measurements being integrated leaving a possibility for the attacker. As long as the attacker maintains operation(s) within that frame of single scan cycle while keeping itself hidden, the attack can be made successful.

The attacker aims to change the current topology $\mathcal{G}$ to a desired topology $\bar{\mathcal{G}} = (\mathcal{V}; \bar{\mathcal{E}})$ and then reverses that change before the completion of the scan cycle such that the final topology $\bar{\bar{\mathcal{G}}} = (\mathcal{V}; \bar{\bar{\mathcal{E}}})$ would be same as it was in the start i.e., $\bar{\bar{\mathcal{G}}} = \mathcal{G}$. This attack only involves line faults, therefore, the number of vertices $\mathcal{V}$ (bus-bars)

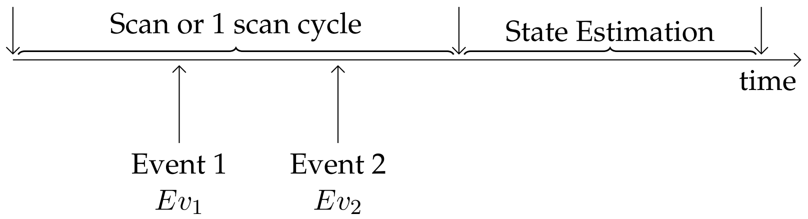

Figure 5.3: Sequential topology attack model

will remain the same during the attack but the number of edges $\mathcal{E}$ (transmission lines) will become $\bar{\mathcal{E}}$ or $\bar{\bar{\mathcal{E}}}$ where $\mathcal{E} \subset \bar{\mathcal{E}}$, $\mathcal{E} = \bar{\bar{\mathcal{E}}}$. The lines that are not common between $\mathcal{E}$ and $\bar{\mathcal{E}}$ and between $\bar{\mathcal{E}}$ and $\bar{\bar{\mathcal{E}}}$ are called attacked lines in the first and second attack intervals respectively. Similarly, all the buses with which target/attacked lines are connected are called attacked buses.

As a prerequisite, the attacker must have the knowledge of few of the time windows in between two scan cycles where the success probability is maximum. In the beginning of a particular scan cycle, the attacker closes already open circuit breakers/switches. The corresponding measurements from the relative sensor changes themselves due to the change in topology. Before the end of the same cycle, the attacker switch the statuses back to its original (open) position such that the topology now $\bar{\bar{\mathcal{E}}}$ is same as was before the manipulation i.e., $\bar{\bar{\mathcal{E}}} = \mathcal{E}$.

To launch such a sequential or a two-stage attack, the attacker at first, needs to change the status of a single breaker from $0 \rightarrow 1$ and then within the scan of measurements, the attacker needs to reverse that change i.e., $1 \rightarrow 0$.

$$\begin{aligned} \bar{\mathbf{s}} &= \mathbf{s} + \mathbf{b}_1, \quad \mathbf{b}_2 \in \{0,1\} \\ \bar{\bar{\mathbf{s}}} &= \bar{\mathbf{s}} + \mathbf{b}_2, \quad \mathbf{b}_2 \in \{0,1\} \end{aligned} \tag{5.20}$$

where $\mathbf{b}_1$ and $\mathbf{b}_2$ are the topology changes at first and second stage of the sequential attack respectively. The attacker is limited in resources in terms of time availability and therefore, the necessary but not sufficient condition for the attacker about time limitation will be

$$\bar{\mathbf{s}}_t - \bar{\bar{\mathbf{s}}}_{t+1} \leq \mathbf{T}, \quad \bar{\mathbf{s}} \in \bar{\mathcal{G}}, \bar{\bar{\mathbf{s}}} \in \bar{\bar{\mathcal{G}}} \tag{5.21}$$

where $\bar{\bar{\mathbf{s}}} - \bar{\mathbf{s}}$ is the length of the attack. This constraint limit the attacker such that he must launch and complete the attack before the next scan cycle starts. There is no proper attack vector in both stages of this attack as the amount of topology change induced by the attacker is reversed inside the same scan cycle. It is important to mention that the above model can be seen as a more realistic extension of [61] where Liu et al. introduced a as an amount of change in the true measurement data. The difference here is of the resources available to the attacker along with very low detection probability and the similarity is the ultimate data fault caused by the attacker.

The measurement vector can be seen as a collection of measurements at three instants, 1) before attack, 2) after first attack and 3) after second sequential attack

$$\mathbf{z}^* = \begin{bmatrix}1\\1\\\vdots\\1\\0\\0\\0\\\vdots\\0\end{bmatrix} \cdot \mathbf{z}' + \begin{bmatrix}0\\\vdots\\0\\1\\\vdots\\1\\0\\\vdots\\0\end{bmatrix} \cdot \mathbf{z}'' + \begin{bmatrix}0\\0\\0\\\vdots\\0\\1\\1\\\vdots\\1\end{bmatrix} \cdot \mathbf{z}''' \tag{5.22}$$

where $\mathbf{z}^* = z' + z'' + z'''$ is the manipulated measurement vector when looking at it cumulatively. In other words, $\mathbf{z}'$ and $\mathbf{z}'''$ are the sets of true value of measurement vectors for the interval before and after the attack respectively. Whereas, z'' is the set of manipulated measurement vector and hence the attack vector can be taken as,

$$\mathbf{a} = \mathbf{z} - \mathbf{z}^* \tag{5.23}$$

Although, the attack vector $\mathbf{a}$ consists of the difference between the whole vectors e.g., $\mathbf{z}$ and $\mathbf{z}^*$ but in fact the attacker is not supposed to manipulate each entry of $\mathbf{z}$ but only the section of z'' measurements.

System states can be determined by $\mathbf{z} = \mathbf{Hx} + \mathbf{e}$ as

$$\hat{\mathbf{x}}^* = \text{argmin}(\mathbf{z}^* - \hat{H}\mathbf{x})^t\mathbf{R}^{-1}(\mathbf{z}^* - \hat{H}\mathbf{x}) \tag{5.24}$$

where $\hat{\mathbf{x}}^*$ is the false state.

The success of the attack lies on how bad is its influence on the measurements in between such sequential change and then how the compromised measurements impact the state estimation process. If the topology before the scan cycle would not match the topology after it, the operators could simply reject the corresponding data and go for contingency analysis. However, even if it not a sequential attack, the first attack alone can cause damage to the system but here, the adversary is aiming for its desired impact or at most DoS attack.

The least cost attack can be seen as the one with optimizing the cost function such as

$$\begin{aligned} \min \ \mathcal{C} \ &= \quad \parallel \mathbf{z} - \mathbf{z}^* \parallel_1 \\ \text{subject to} \quad & \quad \bar{\mathrm{s}} - \bar{\bar{\mathrm{s}}} \le \mathbf{T}, \end{aligned} \tag{5.25}$$

where $\mathbf{z}$ and $\mathbf{z}^*$ are the manipulated and true measurements respectively. $\| \cdot \|_1$ is the magnitude of a vector. Eq. (5.25) is a an optimization problem with an objective function minimizing the cost of the proposed topology attack by finding the optimum attack vector. The cost $\mathcal{C}$ depends on the total number of measurements between the two stages of the attack i.e., $\bar{\mathrm{s}}$ and $\bar{\bar{\mathrm{s}}}$.

Solutions to such convex optimization problems usually exist and their existence can be proved using Lemma 4.2 as follows:

Theorem 5.4 (Existence of optimum sequential topology attack)
If the objective function in

$$\begin{aligned} \min\ \mathcal{C} \quad = \quad & \parallel \mathbf{z} - \mathbf{z}^* \parallel_1 \\ \textit{subject to} \quad & \bar{\mathrm{s}} - \bar{\bar{\mathrm{s}}} \leq \mathbf{T}, \end{aligned} \tag{5.26}$$

is bounded from below, the optimum is attainable.

PROOF Let us begin from the objective function,

$$\parallel \mathbf{z} - \mathbf{z}^* \parallel = \parallel (\mathbf{z}_1 - z') + (\mathbf{z}_2 - z'') + (\mathbf{z}_3 - z''') \parallel \tag{5.27}$$

where $\mathbf{z}$ is a cumulative vector of the three sections $\mathbf{z}_1$, $\mathbf{z}_2$ and $\mathbf{z}_3$. The first and the last term on right hand side will be zero because these are the measurements taken before the attacked launched and after the completion of the attack respectively.

$$\parallel \mathbf{z} - \mathbf{z}^* \parallel = \parallel (\mathbf{z}_2 - z'')) \parallel \tag{5.28}$$

and

$$\parallel (\mathbf{z}_2 - z'')) \parallel = \Sigma_{i=1}^{n} |\mathbf{z}_{2i} - z_i''| \tag{5.29}$$

and a sum of absolute values is always ≥ 0 which leads to

$$\parallel \mathbf{z} - \mathbf{z}^* = \parallel (\mathbf{z}_2 - z'')) \parallel = \Sigma_{i=1}^{n} |\mathbf{z}_{2i} - z_i''| \geq 0 \tag{5.30}$$

and it is showed that the objective function is bounded below hence, optimum to this problem can be attained. ■

5.3.2 Results and Discussions

We note that we seek to consider undetectable topology attacks on conventional centralised state estimation. In this section, we discuss the performance of the above mentioned state estimation model as a result of sequential topology errors by simulations on IEEE 14 and 30-bus systems. The technique used to estimate the state is WLS and MATPOWER is used for loading the data for AC model. Note that, without any topology attack both systems take 4 iterations to converge.

Our sequential attack is composed of two stages to be completed in a single scan cycle. It is worth mentioning here that we consider the same transmission line in both stages i.e., first stage of attack is opening a line while the second stage is closing the same line. Table 5.3 shows that there is always an impact no matter which line is under attack. After N simulations for each bus system, where N is the total number of lines in a system we notice that our attack model remain successful whether it is about the error in estimated states or delayed convergence.

In above table, the first and second columns are for the considered test systems and the attacked lines respectively. We test all the lines of both systems but only showing few of them in table chosen randomly. We make a comparison between a single topology attack (base case) and the proposed one. *Single LF* column represents a single line failure as a result of an undetectable attack whereas *Sequential LF* column shows the proposed attack where the attacker opens and closes the breaker sequentially during measurement taking process. The mean-square error (MSE)

Table 5.3: Sequential faults in 14 and 30-bus system

Test case	Failed line	Convergence (iterations)		Error (MSE)	
		Single LF	Sequential LF	Single LF	Sequential LF
14-bus system	$1-2$	4 iterations	4 iterations	83.19	3.455
	$2-3$	4 iterations	5 iterations	0.0003	0.6424
	$5-8$	4 iterations	7 iterations	0.0013	0.4731
	$3-14$	4 iterations	5 iterations	0.0001	0.287
30-bus system	$1-2$	4 iterations	5 iterations	0.0001	6.159
	$2-4$	diverge	6 iterations	∞	108.12
	$4-12$	4 iterations	4 iterations	0.0001	6.53
	$24-25$	diverge	6 iterations	∞	6.16

between two vectors is simply a squared Euclidean distance between them, normalized by the length of the vectors. It can be seen for the two transmission lines in 30-bus system, i.e., $2-4$ and $24-25$ that the system diverge due to singularities after removing these lines. Even for such critical lines (a transmission line between a pair of buses whose removal leave the system disconnected), the proposed attack (Sequential LF) outperforms the single LF by forcing the state estimator and not just breaking down the system. It is mainly due to the fact that the proposed method can avoid detection because the topology state of the system remains the same before and after the measurement process. Last part of table 5.3 illustrates that the proposed model works better than the basic one in almost every respect and shows even better results for the larger grid.

5.4 Countermeasures for Topology-Related Attacks

As described in section 5.1.1, to launch the topology attack, the attacker needs to change the topology and send over the false topology $\bar{\mathcal{G}}$ to the control centre by commencing e.g., a man-in-the-middle attack initially as discussed in section 5.1.1. We are currently working on the respective countermeasures for topology-related attacks.

There can be multiple solutions for this type of attack but Edge addition and anomaly detection are the two techniques we are proposing for potential mitigation.

5.4.1 Edge Addition

Unlike single line failures for which control centres are capable to deal with, multiple line faults are crucial to prevent. Adding edges (transmission lines) can overcome the effects of multiple line failures by giving redundant measurements i.e., Fig. 5.4 shows a base model for edge addition. For a network like power grid, deployment cost is one of the potential constraints among others. Edge addition can be formulated as an optimization problem giving optimum edges as solution with an upper-bound on cost.

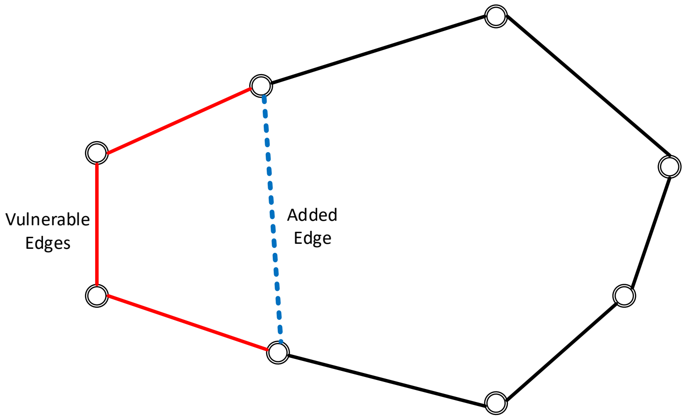

Figure 5.4: Edge addition as a countermeasure to topology failures

Measurement redundancy allows the control centre to help compensate the missing information on system parameters. In addition, redundancy might be a viable solution where there is a high requirement of reliability and successful multi-faults attack might have a substantial impact that it justifies the cost of having additional transmission lines (edges). For environments where redundancy is not a potential solution because it is prohibiting costly to implement, the proposed solution might be wild. allows the control centre to help compensate the missing information on system parameters.

5.4.2 Anomaly Detection

Another possibility of a potential mitigation scheme might be a solution to anomaly detection algorithm. Here, anomaly is termed as any topology fault (line failure), irrespective of its source/cause and is a type of screening process using measurement pattern or trustworthiness metric. Whenever network topology is attacked i.e., a switch/breaker status is manipulated, the corresponding measurements show abnormal/different behaviour. This variation in the measurement pattern can be used to detect anomaly. Once the infected packet from a sensor is detected, the control centre might take actions to normalize the state.

In addition, a trustworthiness metric can be used to quantify the reliability of a certain measurement packet with a limitation of real time required to analyse each packet. The metric works by analysing potential transient instability in the network and prevents controller from this attack. We can assume the value of metric as 1 for absolute trustworthy and 0 for unreliable packet respectively. To assess each packet for reliability might be computationally expensive.

5.5 Conclusion

Modern power networks are likely to experience more rapid and dynamic topology changes, but require accurate state estimation even more so as they would operate closer to safety margins and need rely on techniques such as demand response and management. We have sought to study the effects of multiple-line failures and the resulting topology changes when these are induced by adversaries also capable of suppressing alerts on the occurrence of such induced faults and have given a cost criterion for attackers to choose the lines to target efficiently based on only incomplete information about power networks. We have demonstrated the efficiency and success of this class of attacks also against the common IEEE 118 and 300 bus test systems.

The frequent topology changes make our grid more vulnerable to topology attacks where the operator can think of the attack as the usual unplanned change. We propose a transient topology attack involving sequential failures during a single scan cycle. This way, the state of the topology remains same in the beginning and the end of the process of collecting measurements therefore, making the attack adequately undetectable. Finally, an optimization problem for the least cost attack is formulated.

Chapter 6

State Forcing Topology Attacks

The static arrangement of power system components e.g., transmission lines, busbars, etc. is referred to as *connectivity* and the status of switches/circuit breakers determine the dynamic structure of the network know as topology. Connectivity is considered to be fixed over a certain period of time but topology changes are quite frequent.

6.1 Topology Processing

Converting raw analogue measurements into appropriate units is the first task of the network topology processor. Next task includes simple tests and checks i.e., verifying operating limits, validating non-zero flows in open switches and non-zero voltage differences across closed switching devices. Assuming that the

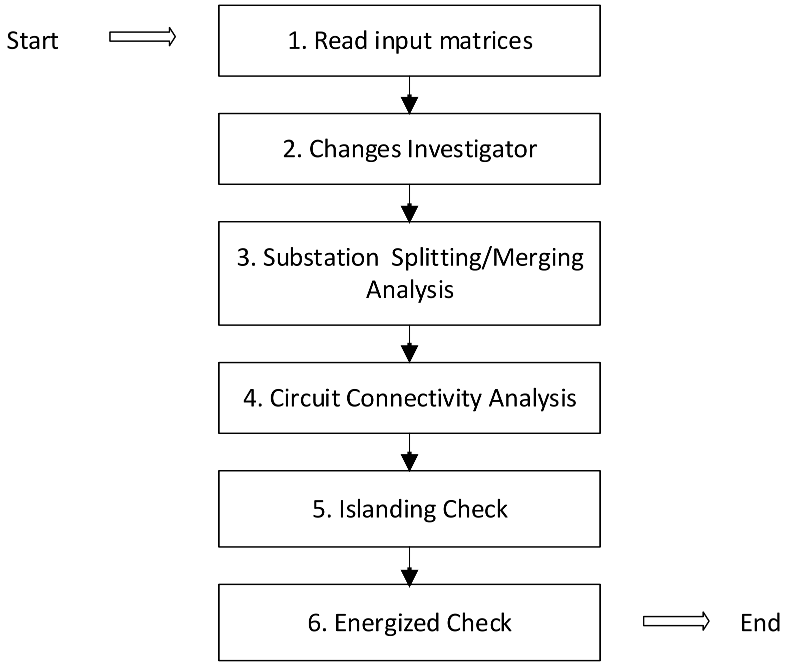

Figure 6.1: Flowchart showing topology processing Algorithm [34]

switching data is correct, initially, a bus-section/switching-device model is considered and data is gathered for topology processing. Then the state estimator assumes the topology to be correct and carry on with estimating the states and detecting/identifying bad data.

One of the classical works on topology processing was documented e.g. by Monticelli [70]. In this section, we explicitly explain the topology processing algorithm following [34]. The reason of choosing later one to replicate is is mostly to understand the data structures and control flows so as to identify attack vectors.

Fig. 6.1 shows the 6-step procedure for topology processing. Step 1 is responsible for reading the input matrix which has all the switching devices data. This primary step does not need an algorithm as it is just about collecting the input data. The next 5 phases can be seen in the algorithms from 1 to 5.

Each switch should be listed with one of the following four types

- Type 1: Switches which are located on a line directly connected to a generator.
- Type 2: Switches which are located on a line connecting two different substations.
- Type 3: Switches which are located within a substation.
- Type 4: Switches which are located on a shunt element, i.e. loads or capacitor banks.

Algorithm 6.1: Changes Investigator Algorithm

```
   Input: $S = \{s_1, \cdots s_m\}$ where $s_m \in (0, 1)$
   Output: $S_{new}$
1  for m = 1 to size(S) do
2      if $s^n_{m(new)} \neq s^n_{m(old)}$ then
3          Determine Breaker type of $s_m$ if $s^n_m$ is of type 3 then
4              Save $m$ and $n$ and call Algorithm 2
5              else if $s^n_i$ is of type 2 then
6                  Save $m$ and $n$ and go to line 13
7                  else
8                      go to line 13
9          else
10             Call Algorithm 3
11 return $S_{new}$
```

The next phase is to investigate the changes in the network. As shown in Algorithm 1, the NTP compares the current snapshot of the breaker and switch statuses with the previous one. It identifies any change in the status of the switches within a substation or on the line connecting two substations. All other changes will be left unsaved as breakers and switches elsewhere have no role in connections of circuit.

The output of algorithm 1 will be S_{new} i.e., the set of revised statuses which is to be used as input for algorithm 2 which is a substation splitting/merging algo-

Algorithm 6.2: Substation Splitting/merging Algorithm

```
Input: $S_{new} = \{s_1, \cdots s_m\}$ where $s_m \in (0,1)$
for any breaker of type 3 do
    while $s^n_{m(new)} \neq s^n_{m(old)}$ do
        Determine all such breakers and circuits
        if Any breaker with $s^n_m = 0$ is left then
            Start a new list with one of $m$ and $n$ are connected
            Save all such $n$ that are located through closed path in $L$
        else
            Call Algorithm 3
```

rithm. It runs only when there is a change of status within the substation. Then, the program identifies and saves all the substations with updated status information.

Algorithm 6.3: Circuit Connectivity Analysis

```
Input: $S_{new} = \{s_1, \cdots s_m\}$ where $s_m \in (0,1)$
$\mathcal{E} = \{e_1, \cdots e_t\}$
for $t = 1$ to size($\mathcal{E}$) do
    if $e_t = 0$ in Algorithm 2 then
        The line is disconnected
        else if Any type 2 breaker with $s_i$ being changed and Corresponding
          $s_i = 0$ then
            The line is disconnected
Call Algorithm 4
```

Connectivity analysis (Algorithm 3) has two steps: first is performed during the splitting/merging analysis to report if a circuit under investigation is open/ disconnected. Second step is carried out on all the switches on the lines connecting two substations. The engine checks if the status is open, it reports the corresponding line to be a disconnected one and vice versa.

Next step is islanding check (Algorithm 6.4) which is quite similar to the changes investigator phase. All mutually connected substations are added in a list and if there are more than one lists, that means there are more than one islands in the network [34].

In the last phase of topology processing, energization check (Algorithm 5) is performed. This is done by checking the switches on the shunt elements i.e., loads or capacitors.

6.2 Attack Model

Topology errors can occur as a result of false manufacturing data/line length or environmental conditions including others. The impact of such errors could be unreliable SE results or correct data being filtered out as bad due to inconsistencies with network parameters. A part from this, these errors can also be adversary based, where attack is formulated in such a way to damage the system.

Algorithm 6.4: Islanding Check

```
   Input: $S_{new} = \{s_1, \cdots s_m\}$ where $s_i \in (0, 1)$
   $\mathcal{E} = \{e_1, \cdots s_n\}$
   Data: $L$ be the List of substations initially singleton i.e., $L = \{l_1\}$ and $M$ be
         the set of all substations
1  for $t = 1$ to length $M$ do
2      if $\exists$ a mutually connected $l_i$ then
3          Include $l_i$ into $L$
4          and update $L$ else if Any $l_i$ still not investigated then
5              Prepare for investigation if $l_i \in L$ then
6                  Call Algorithm 5
7              else
8                  Go to line 2
9  return $L$
```

Algorithm 6.5: Energized Check

```
   Input: List of Substations from Algorithm 4 $L = \{l_1, \cdots s_m\}$
   Data: $L$ be the List of substations initially singleton i.e., $L = \{l_1\}$ and $M$ be
         the set of all substations
1  for $t = 1$ to length $M$ do
2      if $\exists$ a mutually connected $l_i$ then
3          Include $l_i$ into $L$
4          and update $L$ else if Any $l_i$ still not investigated then
5              Prepare for investigation if $l_i \in L$ then
6                  Call Algorithm 5
7              else
8                  Go to line 2
9  return $L$
```

There are two ways for SCADA to transmit the sensor data to the control centre i.e., it responds to any interesting change that happens or it takes its time to complete the poll cycle despite of any change. Former is theoretically correct but later is commonly practised. As an adversary, we are considering two cases to induce targeted errors, i.e., *in-cycle* and *inter-cycle*. In-cycle attack is a type of topology attack in which the attacker is limited to one scan cycle (see details in [40]). On the other hand, inter-cycle attacks are the ones which are not limited to a single cycle for their launch or impact. Few examples of topology attacks include single/double topology failures along with their impacts among others [41].

As an attacker, we have the following goals to be achieved for state estimation:

- Non-Convergence of state estimator
- Adequate errors in state estimation results
- Forcing the state estimator for a certain state

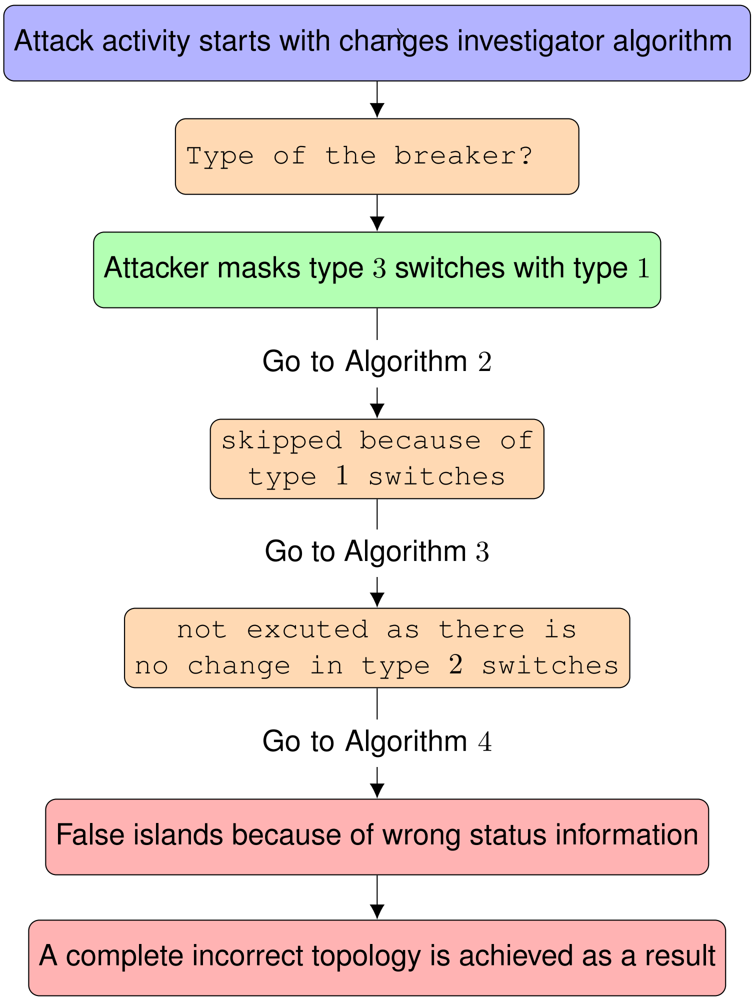
Attack activity starts with changes investigator algorithm
Type of the breaker?
Attacker masks type 3 switches with type 1
Go to Algorithm 2
skipped because of type 1 switches
Go to Algorithm 3
not excuted as there is no change in type 2 switches
Go to Algorithm 4
False islands because of wrong status information
A complete incorrect topology is achieved as a result

Figure 6.2: Erroneous State estimation due to tampered topology

By following the step-by-step topology processor algorithm (in section 6.1), the objectives stated above can be achieved by exploiting the vulnerability in sub-algorithm (Algorithm 6.1). Then, we will show how the goals are attained by propagating the error from the start.

6.2.0.1 Non-convergence

The attacker can push the state estimator to non-convergence by sending the wrong status information that will make the network topology invalid.

6.2.0.2 Error bounds

Generally, there is a certain threshold on the SE error tolerance. But sometimes, the errors become significant and make the system operators take crucial decisions.It can be the one, where the attacker make you believe that there is a certain topology which is false.

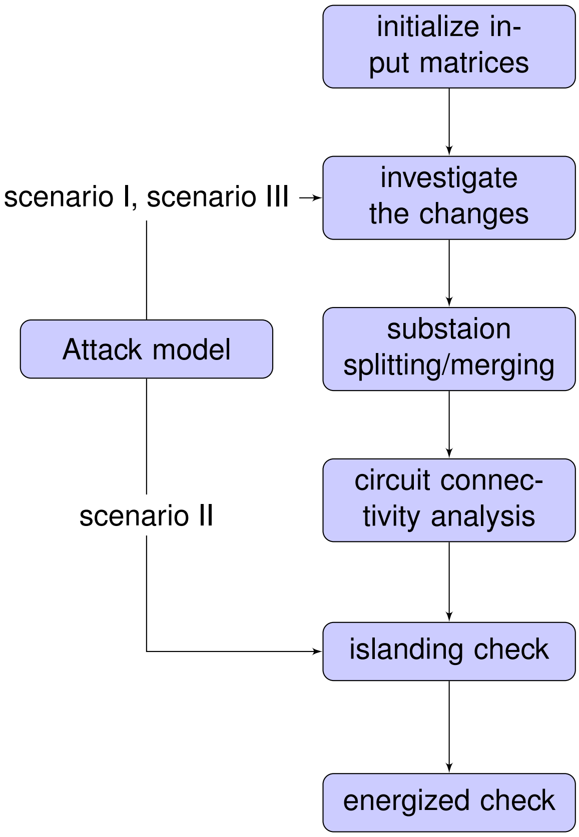

Figure 6.3: Target algorithms of attack in different scenarios

Fig. 6.3 shows the details of which algorithm to manipulate for each of scenarios I, II and III respectively. In other words, for scenario I (non-convergence) type attack, attacker will mask the true topology change with a false one in algorithm 6.1 and for scenario II type attack, attacker will manipulate the true list of connected substations hence resulting a different topology (algorithm 6.4). Finally, scenario III type attacks are similar to launch as scenario I (i.e., on algorithm 6.1), except for the type of attack.

6.2.0.3 State Forcing

Here, we aim to review the adversary model for topology changes that result in a particular state in state estimation. The adversary needs to manipulate the breakers status that effect the adjacent network such as to force a certain state.

In state forcing scenario, the attacker needs to compromise certain circuit breakers while keeping the resources to the minimum. Resources here include the access to breakers and number of attacked breakers. Such attack involve the changes in statuses that are non-linear in nature and hence attacker needs to approximate a highly non-linear function.

To approximate such a function, most widely used techniques are Weighted Least Square (WLS) method, Weighted Least Absolute Value (WLAV) method and

Kalman Filter. Relatively low complexity and the ability to provide a quality estimate are the main advantages of Kalman filter over the other two. However, for a non-linear approximation, unscented Kalman filter could be a suitable choice.

The attacker will perform its own state estimation of the non-linear dynamic system based on the information set $\mathcal{I}$. Attacker has access to all the data on $\mathcal{I}$ which includes the placement information of critical and non-critical switches and also a subset of the topology graph. For a non-zero topology attack, the problem of discrete-time, dynamical system will become

$$\bar{\mathbf{x}}_{k+1} = f(\mathbf{x}_k, \mathbf{v}_k) \tag{6.1}$$

$$\bar{\mathbf{y}}_k = h(\mathbf{x}_k, \mathbf{n}_k) + \mathbf{a}_k \tag{6.2}$$

$\bar{\mathbf{x}}_{k+1}$ is the desired state, $\bar{\mathbf{y}}_{\mathbf{k}}$ is the false measurement input after the topology is being changed and $\mathbf{a}$ is the change in topology.

These attacks are formulated as the ones defined in [61]. Particularly, an attack vector $\mathbf{a}$ belongs to this category if

$$\mathbf{a}_k = h(\mathbf{x}_k + \mathbf{c}_k, \mathbf{n}_k) - h(\mathbf{x}_k, \mathbf{n}_k) \tag{6.3}$$

for some $\mathbf{c}_k$. Adversary changes the topology in a way that the true state $\mathbf{x}_k$ and the false state $\mathbf{x}_k + \mathbf{c}_k$ are both valid network states. Hence, the control centre believe $\mathbf{x}_k + \mathbf{c}_k$ to be the true one. As, the arbitrary vector $\mathbf{c}_{\mathbf{k}}$ can be scaled according to the topology changes that attacker made, the desired state can be attained while fulfilling the stealth condition

$$\mathbf{a}_k = h(\mathbf{c}_k, \mathbf{n}_k) \tag{6.4}$$

Attacks in this regime have the following constraints, which are:

- Attacks are unobservable under the condition (6.4).
- Attacker must have the access (either physical or cyber) to change the switching device(s) status(es)
- Attacker is limited in resources i.e the placement and magnitude of changes
- The desired states which the attacker needs to force are

$$\mathbf{x}_k^{target} = \{\mathbf{x}_k^1, \cdots, \mathbf{x}_k^t\}$$

- The information $\mathcal{I}_a$ available to the attacker is considered to be the optimal information set.

Therefore, this attack is defined as the smallest l-sparse vector s.t

$$\begin{array}{ll} \min & |\mathbf{a}_k| \\ \text{subject to} & \parallel \mathbf{y}_k - \bar{\mathbf{y}_k} \parallel_1 \leq \alpha \end{array} \tag{6.5}$$

Assuming the optimization run is faster than the change in topology, the solution set is the least switch statuses that needs to be modified. Constraint in (6.5) is to ensure the changes in topology are limited. This condition along with the above will help finding out the modifications but it will still work even if the information set is incomplete. Any Kalman Filter method will be able to approximate the function even if a single status is unknown. Particularly, UKF can approximate without major constraints unlike other approximation techniques.

The above optimization problem is convex and the convexity can be proved by the positive-definiteness of its Hessian matrix $\mathbf{y}^t\mathbf{H}\mathbf{y}$. Existence of its solution can be seen by the theorem below:

Theorem 6.1 (Existence of optimum state forcing attack)
If the objective function in

$$\begin{array}{ll} \min & |\mathbf{a}_k| \\ \textit{subject to} & \| \mathbf{y}_k - \bar{\mathbf{y}_k} \|_1 \leq \alpha \end{array} \tag{6.6}$$

is bounded from below, the problem has an optimal solution.

Proof Its proof is quite straight forward as $|\mathbf{a}| \geq 0$. ■

It seems that **a** depends on **H** but results show that it only depends on the topology of the system [56]. For that reason, topology attacks [40] are the best choice for the attacker.

Note that the system can be considered as unobservable if there are insufficient measurements including breaker and switch statuses due to some system error. Un-observability caused by attacker is different in a sense that for former case, the control centre knows exactly about the discrepancies and how they are going to impact the state. On the other hand, if the system is unobservable due to some malicious activity, the control centre would have no idea about the missing network information and their impact on system state.

Example 3 (Convergence to a false value) The attack can result the state estimator to converge to a false value by launching attack on **Changes Investigator Phase** where the physical location of the breaker is to be determined. The attacker will mask the true switch location with a false one. Then, **Splitting and Merging** will have the impact as the switches located within the substation are wrongly considered as the ones connected to a generator(s). In the end, when **Island-ing** occurs, produced islands in form of a list of substations are incorrect. Hence, the wrong breaker type results in a complete different topology. Consequently, state estimator gives the inaccurate estimates. □

Example 4 (Non-convergence) The attack can result the state estimator to non-convergence by launching attack on **Energized Islands Check** phase where the engine is checking for the energized islands. Attacker will mask the true energized substations as de-energized and therefore cause non-convergence. □

Example 5 Forced Convergence to a desired value Consider the IEEE 30-bus test system, shown in Fig. 6.4. Take $\mathcal{I} = \{(12,16),(14,15)\}$ as the information set that means the attacker has the ability to read and modify statuses on these branches. When attacker changes the statuses from $1-0$ or $0-1$, the measurement data on the branches $(12,16)$, $(16,17)$, $(12,13)$, $(4,12)$, $(12,14)$, $(12,15)$, $(15,18)$, and $(15,23)$

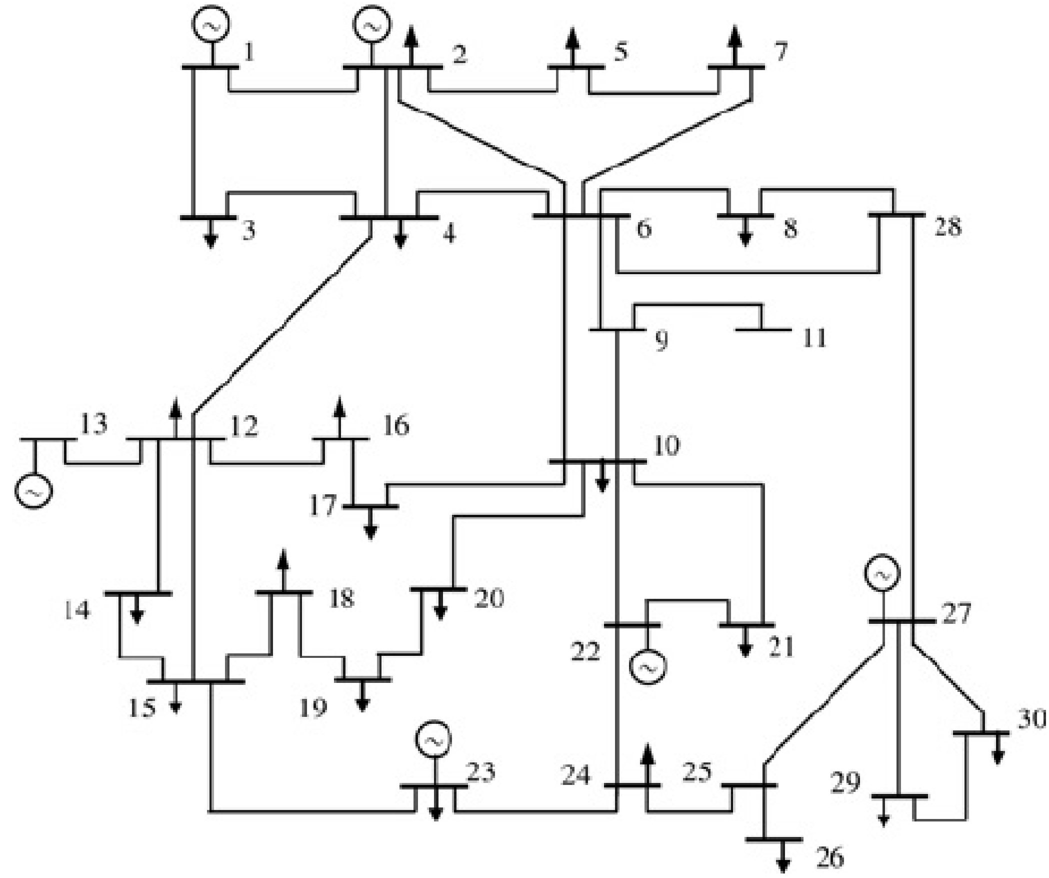

Figure 6.4: Bus-bars distribution in 30-bus system

will change. In other words, the data on adjacent buses/branches to the attacked branch will be affected. This new set of measurements would be sent over to control centre for state estimation via SCADA systems. Therefore, as an attacker, we can force the state variables x_k^{12}, x_k^{14} and x_k^{15} by modifying the data in the information set. In other words, attacker can choose which branches to add in its I depending upon its desired state.

6.3 Countermeasures for State Forcing Topology Attacks

The proposed attack in section 6.2.0.3 makes the state estimator think that the actual topology is something different which forces an error in the true state. While the focus here is to propose state forcing topology attacks, we are also currently in the process of producing a manuscript discussing the potential solutions which detect the state forcing topology attack and also prevents it.

Having topology knowledge is a prerequisite for state estimation. The countermeasure needs to be in a way in which we can then conclusively ensure that the topology information is as close to the real topology as possible. Therefore, any countermeasure must deal with the ways in which we can reduce the error or closes the gap between the estimated and the real topology. A fast and better way of detecting topology might be a potential countermeasure with a constraint on the available time for detection. In addition, a way of preventing fake topology updates might be another countermeasure by topology validation for each state estimation cycle. Both the topology detection and prevention techniques might be efficient but computationally complex as to validate each and topology update while staying in the state estimation poll is crucial.

6.4 Conclusions

Faults in power system state estimation can be induced maliciously by various manners. False data injection or manipulation both in sensor measurements or in communication network is widely known approach. Launching attack prior to these processes e.g., in topology processing phase is relatively new.

We proposed a type of state forcing attack which is initiated in topology processing phase and propagate through the state estimation while assuming that the attacker has certain topology knowledge i.e., about switch statuses. For a successful state forcing attack, the attacker needs to manipulate some of the switches information in the topology processing phase such that the desired system state can be achieved. Furthermore, we formulated an optimization problem for optimum state forcing attack.

Chapter 7

Analysis and Discussions

In this chapter, we will summarize our research first, followed by key contributions, directions for future work and then adoption of thesis findings will be discussed.

7.1 Summary

We introduced adversary models for power system state estimators, considering measurement data and topology being attacked. The models enabled us to analyse the vulnerabilities and hence impacts of such malicious approaches on power system. It also enabled us to propose certain criteria to make such schemes undetectable by system based detection.

We emphasised on measurement swapping (which is a novel approach to the best our knowledge) as a source of attack while considering a power network that is equipped with security protocols. As compared to existing work on *Replay Attacks (RAs)* e.g., in [69], repetition of measurement vectors is used as an attack while assuming that attacker has access to the sensors and can monitor them, our approach does not have such limitations on knowledge, access and time. As an attacker, we found out that such an attack can be made possible even with relatively less strong assumptions.

Moreover, we translated swapping attack to multi-level hierarchical state estimation which is novel to the best of our knowledge and demonstrated how error propagates from regions of lower/intermediate levels to upper and vice versa.

In addition, we found out that topology related attacks are comparatively less explored and therefore, we studied two types of topology attacks/failures: i.e., *line faults* and *in-cycle topology attacks*. We introduced a type of sequential faults that can be made unnoticed by system operators due to their reverse nature. We termed them as in-cycle topology attacks which are novel to the best of our knowledge because the attacker exploits the available time window between two scan cycles to launch the attack. A scan cycle is the time SCADA takes to collect a single round of measurement taking process for state estimation.

Topology processing has vital role in reliable state estimation and in turn to a smooth power system operation. Hence, we elaborated each of the steps involved in topology processing (which is relatively new in comprehensiveness that we provided) and found vulnerabilities for the attacker. We considered State forcing as a consequence of undetectable topology faults while supposing that the attacker is restricted for certain location and magnitude of the possible change.

7.2 Key Contributions

- We showed that measurement re-ordering is adequate to cause misconceptions in state estimation or avert convergence. We defined two security metrics to ensure sparsity and to limit the attack magnitude respectively assuming only the restricted knowledge available to the attacker. Also, we examined three level system where there is an intermediate level between bottom and top layer which act as a coordinator for local state estimation and input data for the top layer (final state of the system). We also examined the effect of a single compromised (measurement vector of) sub-area other sub-areas. Thus, we successfully answered our first research question from section 1.1 in this chapter.

- In context of line faults, we considered line outages and termed them as single and double line failures. We combined data modification of the attacked lines along with line failures to ensure the attack's undetectability while attacker is assumed to have limited knowledge of system's parameters. Therefore, the second research question from section 1.1 is answered.

- We showed that the condition of undetectability is coming from the fact that the topology state in the beginning and end of the measurement taking process remains the same. Also, we formulated an optimization problem to achieve optimum topology attack. By this, we managed to answer our third research question from section 1.1.

- We demonstrated how a desired state can be forced by creating misconception among the system operators about an adversary who is capable of making undetectable topology changes. As compared to already known state forcing attacks, the proposed one is novel in the sense of the cause i.e., topology faults. Finally, we approached our last research question as introduced in section 1.1.

7.3 Directions for Future Work

It is obvious from the chapters above that the research carried out in this dissertation can not be considered concluded. It is certainly because the research area of emerging smart grid is quite vast and there is adequate amount of work to be done to cope with the advancement.

- An investigation on how to provide practical feasibility of the proposed attacks by analysing the vulnerabilities in current IEEE standards for synchrophasors etc. is quite interesting to analyse.

- An implementation of measurement re-ordering model by giving weights to certain parameters depending upon the criticality of the measurements is one of the future works. Similarly, an analysis on how we can translate such attacks in a hierarchical or full distributed setting will be preferable to make the future grid more resilient.

- A study of countermeasures for measurement re-ordering is helpful by proposing a timestamp based and cryptography based method that guarantees prevention to make the power system robust against attacks.
- One of the reasonable mitigation techniques, we are working on, is edge addition and anomaly detection to force all the topology attacks to be detected using a certain criteria.
- We are also currently in the process of producing possible mitigation technique against state forcing topology attacks which detects and also prevents them. It based on detecting fake links by analysing transient instability in the network and prevents controller from this attack.

7.4 Adoption of Thesis Findings

C37.118-2005 is one of the IEEE standards for synchrophasors for power system. According to which synchrophasor measurements shall be tagged with the Universal Time Coordinated (UTC) time corresponding to the time of measurement. Synchrophasor estimates shall be made and transmitted as data packets at a rate that is an integer number of times per second. The PMU supports data reporting and the reporting rate depends on the frequency of the system i.e, for a 50 Hz system, reporting rate varies from 10-25 data packets per second and for 60hz system, it varies from 10-30 data packets per second.

To launch measurement re-ordering in the above case, consider that MitM would have knowledge about information flow from PMUs and attacker re-order the data packets, hence causing the system operator to make actions depending on the wrong packet. Multiple packet swapping is also possible on the same lines. Therefore, it is advised that standards of this kind are vulnerable to proposed attacks and for long term, the standards should be modified.

IEC 62351 is an industry standard aimed at improving security in automation systems in the power system domain. It contains provisions to ensure the integrity, authenticity and confidentiality for different protocols used in power systems. Furthermore, it provides end-end encryption. With all of these in place, in-cycle topology attack is possible as the messages during this attacks will be integrity and confidentiality protected and authenticated. End-to-end encryption comes from the fact the topology before and after a single scan cycle is same. Hence, to make industry standards more robust against these type of attacks, modifications will be required.

Bibliography

[1] Power System Test Cases. In *https://pandapower.readthedocs.io/en/v1.3.0/networks/*$power_system_test_cases.html, pp.\ 1--1$.

[2] *SCADA Data Gateway. In* https://www.trianglemicroworks.com/products/scada-data-gateway/system-requirements *(2020), pp. 1–1.*

[3] Abidin, A., Nagi, F., Ramasamy, A., and Abidin, I. *Steady State Simulation of Power Systems with Change in Topology.* International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering 7 *(2013), 1046–1049.*

[4] Abur, A., and Exposito, A. Power System State Estimation: Theory and Implementation. *CRC Press, Mar. 2004.* *doi:10.1007/978-0-387-75462-8-24.*

[5] Ahmed, M. Power System State Estimation. *Technology and Engineering. Artech House, Jan. 2013.* *doi:10.1007/978-3-642-28920-05.*

[6] Anwar, A., Mahmood, A., and Shah, Z. *A Data-Driven Approach to Distinguish Cyber-Attacks from Physical Faults in a Smart Grid. In* Proceedings of the 24th ACM International on Conference on Information and Knowledge Management *(Melbourne, Oct. 2015), ACM, pp. 1811–1814.* *doi:10.1145/2806416.2806648.*

[7] Arghandeh, R., Gahr, M., Meier, A., Cavraro, G., Ruh, M., and Andersson, G. *Topology Detection in Microgrids with Micro-Synchrophasors.* *doi:arXiv:1502.06938.*

[8] Baiocco, A. Power Network State Estimation Security for Centralized and Hierarchical Estimators: From Bad Data Injections to Estimator Stability. *Ph.D. thesis, 2 2017.*

[9] Baiocco, A., Foglietta, C., and Wolthusen, S. *Delay and Jitter Attacks on Hierarchical State Estimation. In* Proceedings of 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm) *(Miami, FL, Nov. 2015), IEEE, pp. 485–490.* *doi:10.1109/SmartGridComm.2015.7436347.*

[10] Baiocco, A., and Wolthusen, S. *Dynamic forced partitioning of robust hierarchical state estimators for power networks. In* Proceedings of 2014 IEEE Innovative Smart Grid Technologies (ISGT 2014) *(Washington DC, USA, May 2014), IEEE.* *doi:10.1109/ISGT.2014.6816475.*

[11] BAIOCCO, A., AND WOLTHUSEN, S. *Stability of Power Network State Estimation under Attack. In* Proceedings of 2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA) *(Kuala Lumpur, May 2014), IEEE, pp. 441–446.* `doi:10.1109/ISGT-Asia.2014.6873832`.

[12] BI, S., AND ZHANG, Y. *Defending mechanisms against false data injection attacks in the power system state estimation. In* GLOBECOM workshops 2011 IEEE *(Dec. 2011), IEEE.* `doi:10.1109/GLOCOMW.2011.6162362`.

[13] BIENSTOCK, D., AND ESCOBAR, M. *Computing undetectable attacks on power grids.* ACM SIGMETRICS Performance Evaluation Review archive 45 *(Sept. 2017), 115–118.* `doi:10.1145/3152042.3152077`.

[14] BOBBA, R., ROGERS, K., WANG, Q., KHURANA, H., NAHRSTEDT, K., AND OVERBYE, T. *Detecting false data injection attacks on DC state estimation. In* Proceedings of First Workshop on Secure Control Systems (SCS 2010) *(Stockholm, Sweden, Apr. 2010).* `doi:10.1109/59.801884`.

[15] BRYSON, J. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 .* Office of the National Coordinator for Smart Grid Interoperability Engineering Laboratory *(Feb. 2012).*

[16] CASTILLO, E., CONEJO, A., AND SOLARES, C. *Observability analysis in state estimation: a unified numerical approach.* IEEE Transactions on Power Systems 21 *(May 2006), 877–886.* `doi:10.1109/TPWRS.2006.873418`.

[17] CAVRARO, G., ARGHANDEH, R., POOLLA, K., AND MEIER, A. *Data-Driven Approach for Distribtion Network Topology Detection. In* Proceedings of IEEE PES GM 201 *(Apr. 2015), IEEE Press.* `doi:10.1109/PESGM.2015.7286490`.

[18] CHEN, T., FOO, Y., LING, K., AND CHEN, X. *Distributed State Estimation Using a Modified Partitioned Moving Horizon Strategy for Power Systems.* Sensors 17 *(Oct. 2017), 1–21.* `doi:10.3390/s17102310`.

[19] CHEN, Y., KONG, X., YONG, C., MA, X., AND YU, L. *Distributed State Estimation for Distribution Network with Phasor Measurement Units Information.* Energy Procedia 158 *(Feb. 2019), 4129–4134.* `doi:10.1016/j.egypro.2019.01.820`.

[20] CHUNG, H., LI, W., YUEN, C., CHUNG, W., ZHANG, Y., AND WEN, C. *Local Cyber-Physical Attack for Masking Line Outage and Topology Attack in Smart Grid.* IEEE Transactions on Smart Grid 10 *(2019), 4577 – 4588.* `doi:10.1109/TSG.2018.2865316`.

[21] CLEMENTS, K., AND DAVE, P. *On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures.* IEEE Transactions on Power Systems 3 *(1988), 1748 –1753.* `doi:10.1109/59.192991`.

[22] COME CARQUEX, C. R., AND BHATTACHARYA, K. *State Estimation in Power Systems Based on Ensemble Kalman Filtering.* IEEE Transactions on Power Systems 33 *(Nov. 2018), 6600–6610.* `doi:10.1109/TPWRS.2018.2847289`.

[23] COUNCIL, N. R. Terrorism and the Electric Power Delivery System. *The National Academies Press, Washington, DC, 2012.* `doi:10.17226/12050.`

[24] DAIGLE, P. *All-Electronic Power and Energy Meters .*

[25] DAN, G., AND SANDBERG, H. *Stealth Attacks and Protection Schemes for State Estimators in Power Systems. In* Proceedings of the 2010 first IEEE Smart Grid Communication *(Gaithersburg, MD, Oct. 2010), pp. 214–219.* `doi:10.1109/SMARTGRID.2010.5622046.`

[26] DEHGHANPOUR, K., WANG, Z., WANG, J., YUAN, Y., AND BU, F. *A Survey on State Estimation Techniques and Challenges in Smart Distribution Systems.* IEEE Transactions on Smart Grid 10 *(Mar. 2019), 2312–2322.* `doi:10.1109/TSG.2018.2870600.`

[27] DEKA, D., BALDICK, R., AND VISHWANATH, S. *Data Attack on Power Grid: Leveraging Detection. In* 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) *(Feb. 2015), IEEE.* `doi:10.1109/ISGT.2015.7131822.`

[28] DEKA, D., BALDICK, R., AND VISHWANATH, S. *One breaker is enough: Hidden topology attacks on power grids. In* Proceedings of the Power and Energy Society General Meeting, 2015 IEEE *(July 2015), IEEE Press, pp. 1–5.* `doi:10.1109/PESGM.2015.7286568.`

[29] DEKA, D., BALDICK, R., AND VISHWANATH, S. *Optimal Data Attack on Power Grid: Leveraging Detection and Measurement Jamming. In* Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm) *(Miami, FL, Nov. 2015), IEEE , pp. 392–397.* `doi:10.1109/SmartGridComm.2015.7436332.`

[30] DENG, R., XIAO, G., LU, R., LIANG, H., AND VASILAKOS, A. *False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey.* IEEE Transactions on Industrial Informatics 13 *(Apr. 2017), 411–423.* `doi:10.1109/TII.2016.2614396.`

[31] ELBEZ, G., KELLER, H., AND HAGENMEYER, V. *A New Classification of Attacks against the Cyber-Physical Security of Smart Grids. In* Proceedings of the 13th International Conference on Availability, Reliability and Security *(Hamburg, Germany, Aug. 2018), ACM .* `doi:10.1145/3230833.3234689.`

[32] ELMRABET, Z., KAABOUCH, N., ELGHAZI, H., AND ELGHAZI, H. *Cybersecurity in smart grid: Survey and challenges.* Computers & Electrical Engineering 67 *(Apr. 2018), 469–482.* `doi:10.1016/j.compeleceng.2018.01.015.`

[33] EXPOSITO, A., ABUR, A., JAEN, A., AND QUILES, C. *A Multi Level State Estimation Paradigm for Smart Grids.* Proceedings of the IEEE 99 *(Apr. 2011), 952 – 976.* `doi:10.1109/JPROC.2011.2107490.`

[34] FARROKHABADI, M., AND VANFRETTI, L. *An efficient automated topology processor for state estimation of power transmission networks.* Electric Power Systems Research 106 *(Jan. 2014), 188–202.* `doi:10.1016/j.epsr.2013.08.014`.

[35] FENG, Y., BAIOCCO, A., FOGLIETTA, C., PANZIERI, S., AND WOLTHUSEN, S. *Malicious False Data Injection in Heirarchical Electric Power Grid State Estimation Systems. In* 4th International Conference on Future Energy Systems (ACM e-Energy '13) *(May 2013), ACM.* `doi:10.1145/2487166.2487187`.

[36] GIANI, A., BITAR, E., GARCIA, M., MCQUEEN, M., KHARGONEKAR, P., AND POOLLA, K. *Smart grid data integrity attacks: characterizations and countermeasures. In* International Conference on Smart Grid Communications (SmartGridComm) *(Oct. 2011), IEEE.* `doi:10.1109/SmartGridComm.2011.6102324`.

[37] GUL, A., AND WOLTHUSEN, S. *Measurement Re-Ordering Attacks on Power System State Estimation. In* Proceedings of 7th IEEE International Conference on Innovative Smart Grid Technologies, Europe *(2017), IEEE.* `doi:10.1109/ISGTEurope.2017.8260145`.

[38] GUL, A., AND WOLTHUSEN, S. *A Review on Attacks and Their Countermeasures in Power System State Estimation.* Smart Micro-Grid Systems Security and Privacy, Advances in Information Security 71 *(Aug. 2018).* `doi:10.1007/978-3-319-91427-5_2`.

[39] GUL, A., AND WOLTHUSEN, S. *Error Propagation after Re-ordering Attacks in Hierarchical State Estimation. In* Twelfth IFIP WG 11.10 International Conference on Critical Infrastructure Protection *(Mar. 2018), Springer.* `doi:10.1007/978-3-030-04537-1_4`.

[40] GUL, A., AND WOLTHUSEN, S. *In-Cycle Sequential Topology Faults and Attacks: Effects on State Estimation. In* Lecture Notes in Computer Science (LNCS) *(Dec. 2018), vol. 11260, Springer Cham, pp. 17–28.* `doi:10.1007/978-3-030-05849-4_2`.

[41] GUL, A., AND WOLTHUSEN, S. *State Estimation under Undetectable Single and Double Line Failures. In* 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) *(Feb. 2019), IEEE.* `doi:10.1109/ISGT.2019.8791666`.

[42] GUO, Y., TONG, L., WU, W., SUN, H., AND ZHANG, B. *Hierarchical Multi-Area State Estimation via Sensitivity Function Exchanges.* IEEE Transactions on Power Systems 32 *(Jan. 2017), 442–453.* `doi:10.1109/TPWRS.2016.2537836`.

[43] HANDSCHIN, E. *Electrical Network Control .* Control Systems, Robotics, And Automation 18.

[44] HANDSCHIN, E., SCHWEPPE, F., KOHLAS, J., AND FIECHTER, A. *Bad Data Analysis for Power System State Estimation.* IEEE Transactions on Power Apparatus and Systems 94 *(Apr. 1975), 329–337.* `doi:10.1109/T-PAS.1975.31858`.

[45] HINES, P., BLUMSACK, S., SANCHEZ, E. C., AND BARROWS, C. *Topological and Electrical Structure of Power Grids. In* Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS),2010 *(Jan. 2010), IEEE, pp. 1–10.* `doi:10.1109/HICSS.2010.398`.

[46] HO, Q.-D., AND LE-NGOC, T. *Smart Grid Communications Networks: Wireless Technologies, Protocols, Issues, and Standards1, 2013.*

[47] JIANG, X. Real-Time Power System Topology Change Detection and Identification. *Ph.D. thesis, University of Illinois, Urbana-Champaign, 2013.*

[48] JULIER, S., AND UHLMANN, J. *Unscented Filtering and nonlinear Estimation.* Proceedings of the IEEE (Volume: 92 , Issue: 3 , Mar 2004) 92 *(Mar. 2004), 401–422.* `doi:10.1109/JPROC.2003.823141`.

[49] KEZUNOVIC, M. *Monitoring of Power System Topology in Real-Time. In* Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS),2010 *(Kauai, Hawaii, Jan. 2006), IEEE, pp. 1–10.* `doi:10.1109/HICSS.2006.355`.

[50] KHAN, R., MCLAUGHLIN, K., LAVERTY, D., AND SEZER, S. *Analysis of IEEE C37.118 and IEC 61850-90-5 SynchrophasorCommunication Frameworks. In* Proceedings of Power and Energy Society General Meeting(PESGM) *(2016), IEEE, pp. 1–1.* `doi:10.1109/PESGM.2016.7741343`.

[51] KIM, J., AND TONG, L. *Detection and identification of topology errors in electric power systems.* IEEE Journal on Selected Areas in Communications 31 *(2013), 1294 –1305.* `doi:10.1109/JSAC.2013.130712`.

[52] KIM, J., TONG, L., AND THOMAS, R. *Data Framing Attack on State Estimation.* IEEE Journal on Selected Areas in Communications 32 *(July 2014), 1460–1470.* `doi:10.1109/JSAC.2014.2332032`.

[53] KIM, J., TONG, L., AND THOMAS, R. *Subspace Methods for Data Attack on State Estimation: A Data Driven Approach. In* IEEE Transactions on Signal Processing *(Mar. 2015), IEEE.* `doi:10.1109/TSP.2014.2385670`.

[54] KIM, T., AND POOR, V. *Strategic Protection Against Data Injection Attacks on Power Grids.* IEEE Transactions on Smart Grid 2 *(June 2011), 326–333.* `doi:10.1109/TSG.2011.2119336`.

[55] KORRES, G., AND MANOSAKIS, N. *A state estimation algorithm for monitoring topology changes in distribution systems. In* Proceedings of Power and Energy Society General Meeting, 2012 IEEE *(July 2012), IEEE Press.* `doi:10.1109/PESGM.2012.6345126`.

[56] KOSUT, O., JIA, L., THOMAS, R., AND TONG, L. *Malicious Data Attacks on the Smart Grid.* IEEE Transactions on Smart Grid 2 *(Dec. 2011), 645–658.* `doi:10.1109/TSG.2011.2163807`.

[57] LAMINE MILI, M. C. . P. R. *Robust state estimation of electric power systems.* IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 41 *(May 1994), 349–358.* *doi:10.1109/81.296336.*

[58] LEFEBVRE, S., AND PREVOST, J. *Topology Error Detection and Identification in Network Analysis .* Electrical Power and Energy Systems 28 *(Dec. 2005), 293–305.* *doi:10.1016/j.ijepes.2005.12.006.*

[59] LIU, R., VELLAITHURAI, C., BISWAS, S., GAMAGE, T., AND SRIVASTAVA, A. *Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid.* IEEE Transactions on Smart Grid 6 *(Sept. 2015).* *doi:10.1109/TSG.2015.2432013.*

[60] LIU, X., LI, Z., LIU, X., AND LI, Z. *Masking Transmission Line Outages via False Data Injection Attacks.* IEEE Transactions on Information Forensics and Security 11 *(July 2016), 1592–1602.* *doi:10.1109/TIFS.2016.2542061.*

[61] LIU, Y., NING, P., AND REITER, M. *False data injection attacks against state estimation in electric power grids. In* Proceedings of 16th ACM conference on Computer and communications security *(NY, USA, Nov. 2009), pp. 21–32.* *doi:10.1145/1653662.1653666.*

[62] LU, C., TENG, J., AND CHANG, B. *Power System Network Topology Error Detection. In* IEE Proceedings - Generation, Transmission and Distribution *(Nov. 1994), vol. 141, IET, pp. 623–629.* *doi:10.1049/ip-gtd:19941482.*

[63] LUO, Z., AND ZHANG, S. *On extensions of the frank-wolfe theorems.* Computational Optimization and Applications 13*, 1 (Apr 1999), 87–110.* *doi:10.1023/A:1008652705980.*

[64] LYU, L., CHEN, C., ZHU, S., AND GUAN, X. *5G Enabled Co-design of Energy-Efficient Transmission and Estimation for Industrial IoT Systems. In* IEEE Transactions on Industrial Informatics *(Jan. 2018), IEEE, pp. 1–1.* *doi:10.1109/TII.2018.2799685.*

[65] MEDJROUBI, W., MÜLLER, U. P., SCHARF, M., MATKE, C., AND KLEINHANS, D. *Open Data in Power Grid Modelling: New Approaches Towards Transparent Grid Models .* Energy Reports 3 *(Nov. 2017), 14 – 21.* *doi:10.1016/j.egyr.2016.12.001.*

[66] MELIOPOULOS, A., COKKINIDES, G., HEDRINGTON, C., AND CONRAD, T. *The supercalibrator — A fully distributed state estimator. In* IEEE PES General Meeting *(July 2010), IEEE.* *doi:10.1109/PES.2010.5589997.*

[67] MINOT, A., AND LI, N. *A fully distributed state estimation using matrix splitting methods. In* 2015 American Control Conference (ACC) *(IL, USA, July 2015), IEEE .* *doi:10.1109/ACC.2015.7171105.*

[68] MO, H. Handbook of Research on Artificial Immune Systems and Natural Computing: Applying Complex Adaptive Technologies. *, Apr. 2009.* *doi:10.4018/978-1-60566-310-4.*

[69] MO, Y., AND SINOPOLI, B. *Secure Control against Replay Attacks. In* 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton) *(Jan. 2010), IEEE.* `doi:10.1109/ALLERTON.2009.5394956`.

[70] MONTICELLII, A. State Estimation in Electric Power System: A generalized approach. *Business and Economics. Springer Science and Business Media, May 1999.* `doi:10.1007/978-3-642-03552-4-6`.

[71] NAZIRI, I., AND KARRARI, M. *Hierarchical robust state estimation in power system using phasor measurement units. In* Proceedings of the ISGT 2011 *(Anaheim, CA, USA, Jan. 2011), IEEE .* `doi:10.1109/ISGT.2011.5759141`.

[72] OBAIDAT, M., ANPALANGAN, A., AND WOUNGANG, I. Handbook of Green Information and Communication Systems. *Elsevier Science and Technology, Nov. 2012.*

[73] PIGNATI, M., ZANNI, L., SARRI, S., CHERKAOUI, R., BOUDEC, J., AND PAOLONE, M. *A pre-estimation filtering process of bad data for linear power systems state estimators using PMUs. In* 2014 Power Systems Computation Conference *(Aug. 2014), IEEE.* `doi:10.1109/PSCC.2014.7038329`.

[74] PILATTE, N., ARISTIDOU, P., AND HUG, G. *TDNetGen: An open-source, parametrizable, large-scale, transmission and distribution test system. In* IEEE Systems Journal *(Mar. 2019), vol. 13, IEEE, pp. 729–737.* `doi:10.1109/JSYST.2017.2772914`.

[75] PILZ, M., NAEINI, F., GRAMMONT, K., SMAGGHE, C., DAVIS, M., NEBEL, J., ALFAGIH, L., AND PFLUEGEL, E. *Security attacks on smart grid scheduling and their defences: a game-theoretic approach.* International Journal of Information Security *(Aug. 2019), 1–17.* `doi:10.1007/s10207-019-00460-z`.

[76] SANDBERG, H., TEIXEIRA, A., AND JOHANSSON, K. *On Security Indices for State Estimators in Power Networks. In* Preprints of the First Workshop on Secure Control Systems CPSWEEK 2010 *(Stockholm, 2010).*

[77] SANJAB, A., AND SAAD, W. *Smart Grid Data Injection Attacks: To Defend or Not? In* Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm) *(Miami, FL, Nov. 2015), IEEE , pp. 380–385.* `doi:10.1109/SmartGridComm.2015.7436330`.

[78] SANJAB, A., AND SAAD, W. *Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective. No. 99, IEEE.* `doi:10.1109/TSG.2016.2550218`.

[79] SANJAB, A., SAAD, W., GÜVENÇ, I., SARWAT, A., AND BISWAS, S. *Smart grid security: Threats, challenges, and solutions.* ArXiv abs/1606.06992 *(2016).*

[80] SCHWEPPE, F., AND WILDES, J. *Power System Static-State Estimation Part I-III.* IEEE Transactions on Power Apparatus and Systems PAS-89 *(Jan. 1970), 120–135.* `doi:10.1109/TPAS.1970.292680`.

[81] SHEN, Y., FEI, M., AND DU, D. *Cyber security study for power systems under denial of service attacks.* Transactions of the Institute of Measurement and Control 41 *(June 2019), 1600–1614.* *doi:10.1177/0142331217709528.*

[82] SHEPARD, D., HUMPHREYS, T., AND FANSLER, A. *Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks. In* Proceedings of 6th Annual IFIP WG 11.10 International Conference on Critical Infrastructure Preotection 2012 *(2012).*

[83] SIMON, D. Optimal state estimation: Kalman, H infinity, and nonlinear approaches. *John Wiley & Sons, 2006.*

[84] SOLTAN, S., YANNAKAKIS, M., AND ZUSSMAN, G. *Power Grid State Estimation Following a Joint Cyber and Physical Attack.* IEEE Transactions on Control of Network Systems PP *(2016), 1–1.* *doi:10.1109/TCNS.2016.2620807.*

[85] VUKOVIC, O., AND DAN, G. *On the Security of Distributed Power System State Estimation under Targeted Attacks. In* SAC ’13 Proceedings of the 28th Annual ACM Symposium on Applied Computing *(Mar. 2013), ACM.* *doi:10.1145/2480362.2480490.*

[86] VUKOVIC, O., AND DAN, G. *Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks.* IEEE Journal on Selected Area Communication *(July 2014).* *doi:10.1109/JSAC.2014.2332106.*

[87] WEI, L., RONDON, L., MOGHADASI, A., AND SARWATI, A. *Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid. In* 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D) *(CO, USA, Apr. 2018), IEEE .* *doi:10.1109/TDC.2018.8440552.*

[88] WEIL, S., BENT, R., CASLETON, E., AND LAWRENCE, E. *Identification of Topology Changes in Power Grids using Phasor Measurements.* Applied Stochastic Models in Business and Industry 30 *(Nov. 2014), 740–752.* *doi:10.1002/asmb.2082.*

[89] WELCH, G., AND BISHOP, G. *An Introduction to the Kalman Filter.* Technical Report *(2006).*

[90] XIA, S., ZHANG, Q., JING, J., DING, Z., YU, J., CHEN, B., AND WU, H. *Distributed State Estimation of Multi-Region Power System Based on Consensus Theory.* Energies 2019 12 *(Mar. 2019), 1–16.* *doi:10.3390/en12050900.*

[91] XIE, L., CHOI, D., KAR, S., AND POOR, V. *Fully Distributed State Estimation for Wide-Area Monitoring Systems.* IEEE Transactions on smart grid 3 *(May 2012), 1154–1169.* *doi:10.1109/TSG.2012.2197764.*

[92] XIONG, K., AND NING, P. *Cost-efficient and attack-resilient approaches for state estimation in power grids. In* Proceedings of the 30th Annual ACM Symposium on Applied Computing *(Salamanca, Apr. 2015), ACM, pp. 2192–2197.* *doi:10.1145/2695664.2695937.*

[93] ZETTER, K. *Inside the Cunning, Unprecedented Hack of Ukrain's Power Grid.* Critical Infrastructures *(Mar. 2016).*

[94] ZHAO, J., ZHANG, G., SCALA, M., AND WANG, Z. *Enhanced Robustness of State Estimator to Bad Data Processing Through Multi-innovation Analysis .* IEEE Transactions on Industrial Informatics 13 *(Aug. 2017), 1610–1619.* `doi:10.1109/TII.2016.2626782`*.*