Cyber-Physical Security of Power Distribution Systems

by

Abdelrahman Ayad

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

Waterloo, Ontario, Canada, 2019

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

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

Abstract

Smart grids have been witnessing continuous and rapid radical developments in the recent years. With the aim towards a more sustainable energy system, the share of distributed generation resources is ever-increasing and transforming the traditional operations of the power grids. Along with these allocated resources, an ensemble of smart measurement devices, multiple communication layers, sophisticated distributed control techniques and interconnection of system equipment represent the pillars that support the modernization of these power networks. This progress has undoubtedly enabled a more efficient and accurate operation of the power networks. At the same time, it has created vulnerability points and challenges that endanger the safety and security of the smart grids operation. The cyber-physical security of smart grids has consequently become a priority and a major challenge to ensure a reliable and safe operation of the power grid. The resiliency of the grid depends on our ability to design smart grid that can withstand threats and be able to mitigate against different attack scenarios. Cyber-physical security is currently an active area of research, and threats that target critical operation components have been classified and investigated in the literature. However, many of the research efforts have focused on the threats on the transmission level, with the intention of extending the protection, detection and mitigation strategies to the distribution level. Nevertheless, many of the performed analysis is not suitable for Power Distribution Systems (PDS) due to the inherently different characteristics of these systems.

This thesis first investigates and addresses the stealthy False Data Injection (FDI) attacks on the PDS, which target the Distribution Systems Optimal Power Flow (DSOPF) and are not detectable by traditional Bad Data Detection (BDD) methods. The attacks formulation is based on the Branch Current State Estimation (BCSE), which allows separation of the phases, thus full analysis on the unbalanced three-phase system is performed. In specific, it is shown how an adversary, having access to system measurements and topology, is able to maximize the system losses. By launching FDI attacks that target the Distribution Systems State Estimation (DSSE), the adversary constructs the attack vectors that drive the objective function in the opposite direction of optimality. Optimal attack strategy effects is investigated. The results demonstrate the increase in system losses after corrupting the measurements.

Second, a machine learning technique is proposed as a protection measure against the cyber-physical threats to detect the FDI attacks. Although FDI vectors cannot be detected by conventional BDD techniques, exploiting the historical data enables a more thorough analysis and a better detection advantage of anomalies in the measurements. Recurrent Neural Networks (RNN) is applied on the stream of data measurements to

identify any anomaly, which represents a compromised measurement, by analyzing multiple points across the measurement vector and multiple time steps. The temporal correlation of data points is the basis of identifying attack vectors. The results of the RNN model indicate an overall strong ability to detect the stealthy attacks.

Acknowledgements

I would like first to extend my genuine gratitude and appreciation for my supervisor Prof. Ehab El-Saadany, who firstly gave me the opportunity to join his group and secondly for his continuous support throughout the last two years. He always encouraged me in every step I took with his grand clear vision.

I would like also to sincerely thank Dr. Hany Farag, for all his guidance, patience and advice during these two years. He was always available whenever I needed help.

My heartiest appreciation goes to Dr. Amr Youssef, for offering me the valuable time and rich guidance. His dedication always inspired me to work harder on my research.

I am honored that this dissertation has been examined by Dr. Tarek Abdel-Galil and Dr. Ramadan El-Shatshat. I owe respect and thanks to them for their time and insight.

I am truly fortunate that I have been accompanied by Mohsen Khalaf (and Mizo) during my masters program. I will be always grateful for all the endless memories, countless laughter moments and one true everlasting bond!

To the companions of the journey, I would like to thank Michael, Hamouda, Mohannad, Khaled, Ahmed, and all friends I have met in Waterloo. You guys made my stay feels more like home.

To my friends in Egypt, who always sheer, encourage and push me forward. Basto, Masry, Omar, Ronty, and Sharkawi. Brothers for life, wherever we are.

I want to give special thanks to Mary Ann Offer, Peter Westort, Bob, and Tom, for always being my family. I always had the best holidays at Oshkosh.

I cannot describe my feelings to my mother and my sister. Without their sacrifices, love, and affection I would not have been able to accomplish this research abroad. They are my source of endless motivation, which never fails to pick me up in the most difficult moments. My mothers single mission has been keeping me and my sister successful and happy. For that I will always be in debt to her.

Dedication

إلي أمي
إلي أمنية
إلي روح أبي

It is forbidden not to smile
at problems, not to fight for
what you want, leave everything
for fear, not to make
true your dreams.
- Pablo Neruda.

Table of Contents

List of Tables

List of Figures

Glossary

ADNs Active Distribution Networks. 8

AI Artificial Intelligence. 3, 30

ANN Artificial Neural Networks. 30, 41

BCSE Branch Current State Estimation. iii, viii, 2, 3, 5, 9, 13, 14, 31, 36, 38, 52

BDD Bad Data Detection. iii, 2–5, 14, 26, 28–30, 32–34, 36, 37, 46, 50, 52

BFM Branch Flow Model. ix, 5, 17, 18

BPL Backpropagation Learning Algorithm. 43

BPTT Backpropagation Through Time. ix, 43–45

DERs Distributed Energy Resources. 6, 23, 27, 29, 53

DG Distributed Generation. 1, 7, 8, 17, 23

DMS Distribution Management System. xii, 9

DoS Denial of Service. 25, 26

DSOPF Distribution Systems Optimal Power Flow. iii, xii, 2–4, 9, 16–18, 20, 21, 30–32, 34–37, 39, 52, 53

DSSE Distribution Systems State Estimation. iii, viii, xii, 2–5, 7, 9, 10, 13, 27–31, 34, 37, 46, 52, 53

FDI False Data Injection. iii, ix, xi, xiii, 2–5, 26, 28–34, 36–38, 41, 45, 47, 48, 50, 52, 53

IESO Independent Electricity System Operator. 45, 46

LRT Load Ratio Transformer. 3, 27

ML Machine Learning. 3–5, 10, 30, 31, 41, 52

OPF Optimal Power Flow. viii, 2, 5, 15–20, 39

ORPF Optimal Reactive Power Flow. 16

PDS Power Distribution Systems. iii, viii, ix, xi, xii, 1–7, 9, 10, 16–18, 20, 23, 25–30, 32, 34, 36, 38, 41, 53

PMU Phasor Measurement Unit. 1, 25, 28, 34

PV Photovoltaic. 27, 29

RNN Recurrent Neural Networks. iii, iv, ix, xi–xiii, 3, 4, 41–53

ROC Receiver Operating Characteristic. xiii, 49, 50

RTU Remote Terminal Unit. 34

SDP Semi Definite Programming. 5, 17, 20, 21, 31, 36, 39, 52

SE State Estimation. 2, 5, 9–11, 14, 15, 26, 28–30, 33

SVM Support Vector Machines. 30

VVC Volt-Var Control. viii, 1–3, 6–8, 20, 23, 27–29, 52

WLS Weight Least Squares. 9–12

Chapter 1

Introduction

1.1 Problem Description and Motivation

Recent advancements in power systems have rendered smart grids a more than ever sophisticated complex system. System operators are currently facing, more than ever,different challenges to maintain a reliable and safe operation of the overall power systems, which include generation, transmission and distribution levels. Concerning Power Distribution Systems (PDS), the main driving force for change is the large scale integration of Distributed Generation (DG) units, including renewable energy resources, with the aim of a more sustainable and greener energy systems [3]. In the aim of achieving these aspirations, many transformations have been recently occurring, among these are: Introduction of communication in control and monitoring and the implementation of distributed Volt-Var Control (VVC) strategies [4], usage of digital field meters and Phasor Measurement Units (PMUs) [5], increasing number of microgrids [6], high share of renewable energy sources [3]. A direct consequence of these changes is the creation of new challenges and vulnerabilities for the modern grid. One of the most critical vulnerability is the cyber-physical security [7, 8, 9]. The cyber-physical security aspect of the smart grid has become of utmost importance for power system operators as it keeps the entirety of energy systems in a safe and secure state against a myriad of threats. The consequences of malicious attacks range from economical effects, to partial malfunctioning of equipment and sub-systems, all the way to cascading failures and shut-down of entire power systems [10, 11]. These attacks can target both the cyber part, which consists of the communication and software layer, or the physical part, which consists of the electrical power devices and equipment [12].

Although the PDS represents a major component of the modern smart grid, much of

the research in the area of cyber-physical security is focused on transmission systems [13]. Due to the inherent fundamental differences between transmission systems and the PDS including but not limited to system topology, unbalanced phases, number of measurement devices, and the high number of nodes, many of the assumptions made for attacks formulation and detection do not hold for PDS. Accordingly, two main operations are considered in this work for analysis of cyber-physical security on PDS: Optimal Power Flow (OPF) and State Estimation (SE).

The OPF lies in the heart of grid control, as operators seek to optimize various objectives, such as voltage regulation, loss minimization and system configuration, constrained by the electrical laws and grid operation limits. The nonlinear nature of the OPF problem makes it difficult to obtain accurate results, especially for Distribution Systems Optimal Power Flow (DSOPF), as many of the OPF approaches formulated for studies on the transmission level are not suitable for PDS characterized with high R/X ratio and radial topologies [14]. The same logic holds for the Distribution Systems State Estimation (DSSE) process, where the approach differs based on the nature and topology of the system [15, 16]. For example, in radial distribution systems, the Branch Current State Estimation (BCSE) model is found to be more suitable than node voltages [17], as its computation efficiency allows better convergence based on the branch power flow model. In addition, the analysis of the state estimation BDD is usually implemented on the DC power flow, a linear version of the AC power flow. This simplification is acceptable for the transmission level studies, but it does not suit PDS. For the state estimation procedure, voltage magnitudes and angles are usually chosen as system states. Accordingly, Liu *et al.* started investigating stealthy False Data Injection (FDI) attacks using the DC power flow. Authors also investigated FDI on AC power flow models [18], but again the investigation was on the transmission level systems. Concerning PDS, many authors became interested in analyzing different threats against distribution networks operations. Recently, Deng *et al.* [19] were among the first to investigate the FDI attacks on the PDS level. The analysis of attacks was based on the assumption of a single phase system, with local attacks and without consideration of VVC devices, such as line voltage regulators or shunt capacitors. This attack model is considered as part of the physical security for three reasons: i) The literature considers these attacks as cyber-physical threats as they often formulation, detection and mitigation of attacks happen in the joint space of cyber-physical space [20, 21] ii) The majority of FDI attacks corrupts the sent power measurements (information in cyber-space), but also can take place by physically compromising a meter or sensor that sends the data [8]. iii) The effects of the attacks is extended to the Volt-Var control equipment, (In this thesis only the shunt capacitors are considered), and their KVAR injected values changed as a result of the attack. Therefore the attacks affected the physical infrastructure of the system under

study. On the other hand, a positive outcome of the grid modernization and digitization, is the sheer availability of data, powered by the integration of information networks with the smart grid . This data permits a better insight for monitoring and control of the grid using data driven approaches such as Artificial Intelligence (AI) or Machine Learning (ML) techniques [22, 23, 24]. Among the many applications of ML, securing the power grid is certainly an ambitious goal [25]. Many authors have already utilized these approaches for detection and mitigation of cyber-physical attacks [26, 27].

1.2 Research Objectives

The scope of this thesis is to develop accurate modelling of cyber-physical threats against the PDS. Since most of the previous research work concerning cyber-physical security, and especially FDI attacks, focuses on the transmission systems [28], there is still a demanding necessity to build cyber-physical security models specifically tailored for PDS systems. These systems require the detailed modelling of the unbalanced 3-phases, and the inclusion of VVC devices such as Load Ratio Transformer (LRT) or shunt capacitors. The objective is to evaluate the impacts of stealthy affects targeting a critical operation such as the DSOPF. Also, a detection technique based on ML is proposed to defend against stealthy attacks. The approach utilizes the available historical data in the attacks identification. The two main objectives of this thesis can be listed as follows:

1. *Optimal stealthy attacks strategy on PDS*: In order to accurately assess the consequences of cyber-physical threats, the first step is to construct a full model of the PDS DSSE. For this reason, a three phases DSSE based on the BCSE approach has been modeled. Stealthy FDI attacks have been constructed to bypass the BDD, and incur maximal damage on the DSOPF.The damage is represented by the deviation in the objective function, such as increase in the power losses. The attacks are analyzed on a three-phases, radial and unbalanced distribution system.

2. *Detection of FDI attacks on the power flow measurements*: A data driven ML approach, using RNN is adopted to detect the anomalies in the power flow measurements. The model aims to capture the temporal correlation of the data features, as well as the state of the measurements at each time step. The RNN is trained to detect stealthy attacks that bypass the traditional BDD.

1.3 Thesis outline

The remainder of this thesis is organized into five chapters as follows:

- **Chapter 2** presents the background and literature review for the work in this thesis. A general overview of modern PDS is given, including the process of DSOPF, as well as the different techniques for DSSE. The requirements for cyber-physical security of smart grids are listed, with focus on the threats and defense mechanisms that are most relevant to the PDS. An overview of ML techniques is given, as defense and mitigation measures for cyber-physical security in the power systems.

- **Chapter 3** presents the case study of stealthy FDI attacks against the DSOPF. An optimal attack strategy is first developed. The attack vectors are formulated and injected into the power flow measurements to bypass the BDD of the DSSE, and incorporated into the DSOPF. Results of the attacks are validate on the IEEE-34 unbalanced radial system.

- **Chapter 4** proposes the usage of ML to detect the stealthy FDI attacks. The RNN model is derived and built to capture the temporal correlations between the data points of the measurements vector. The model is trained using real world data, and the performance of the model is statistically evaluated.

- **Chapter 5** presents the thesis summary, contributions, and suggestions for future research.

Chapter 2

Literature Review and Background

This chapter reviews the related work in literature and provides the necessary background for the rest of the thesis. The first section presents the modern PDS and their main features. The second section reviews the different DSSE algorithms and the mathematical formulation of the State Estimation (SE) process. Also, the derivation of the BCSE as the used method to estimate the sates of the studied system is presented. An overview is also given over the Bad Data Detection as an approach to identify and eliminate bad measurements. The third section presents the Optimal Power Flow formulation and techniques used in PDS. The Branch Flow Model is presented as well as the convex relaxation based on Semi Definite Programming. The fourth section presents the main challenges for cyber-physical security in the PDS. Further, requirements for the cyber-physical security are reviewed, as well as the main threats that endanger the integrity of these requirements. A special focus is given for the stealthy FDI attacks and protection techniques against them. The last section reviews the research done on ML which concerns the power systems cyber-physical security.

2.1 Power Distribution Systems (PDS)

The traditional power systems have been witnessing radical transformation in their infrastructures. The modernization of the overall integrated complex system, renders it into a smart grid. The waves of change reaches all the stages and levels of energy systems, starting from power generation, to transmission systems, all the way down to Power Distribution Systems (PDS). Distribution systems operators have had a, complex but limited, set of processes required to maintain a reliable and safe operation. The new era of smart

grid brings however more challenges and initiatives to improve the quality of power systems. Concerning the PDS, several functions and characteristics are desired to be included and improved such as [29, 30]: Increased share of Distributed Energy Resources (DERs) to harness the power of renewable energy, Efficient Volt-Var Control (VVC) for different configuration of distribution networks, integration of microgrids to increase reliability and distribution flexibility, and enhancement of the PDS against cyber-physical security risks to ensure a robust protection and security against malicious threats. Figure 2.1 shows the current main areas of research necessary to modernize the PDS. PDS inherently differ

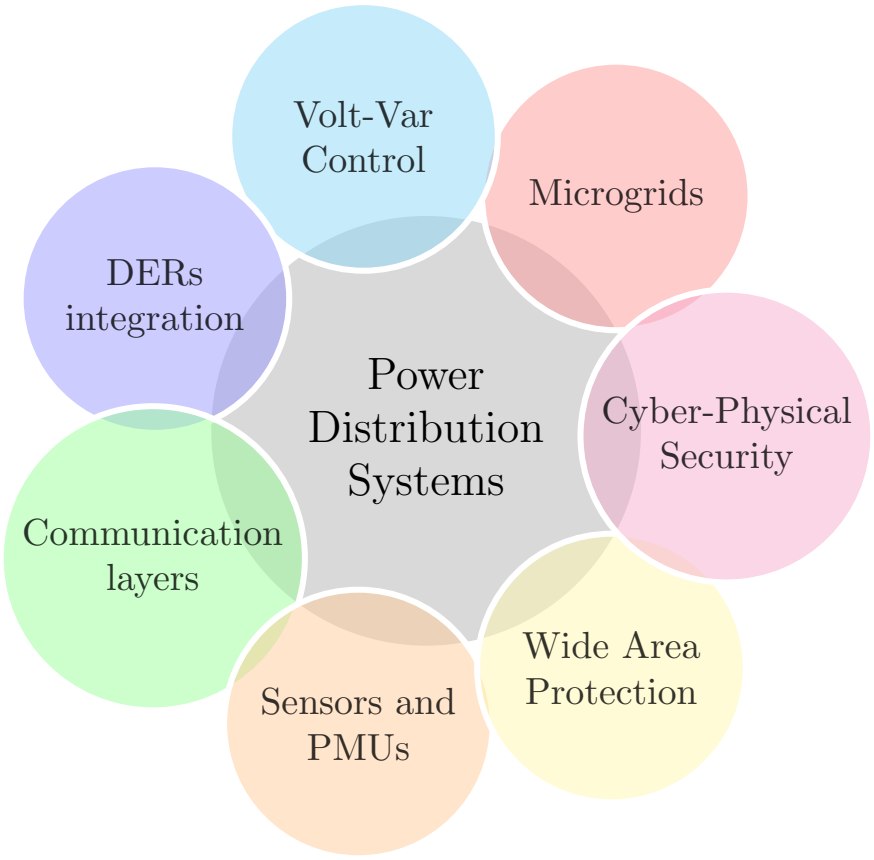

Figure 2.1: Current PDS active research areas and interests

in their infrastructure from the transmission systems. These differences should be considered in the different analyses in the distribution systems operation - such as and not

limited to DSSE - to achieve accurate results. The main distinctive features of PDS can be summarized as follows [15]:

1. **System topologies:** Distribution networks have distinctively radial configurations, which allows a cheap and simple operation. Modern distribution networks witness rapid integration of DGs, which render the power flow bi-directional instead of the traditional unidirectional flow.

2. **Phases imbalance:** Distribution loads are not necessarily symmetrical in nature, which results in an unbalance between the three phases. The increasing share of DG units integrated into the distribution networks have further heightened the level of imbalance. Consequently, a single-phase equivalent representation, which assumes a phases-balanced system, is not an appropriate approximation for DSSE, and the full three-phases model is to be considered.

3. **Number of measurement devices:** The number of measurements data is deficient in PDS to ensure system observability [16]. In order to overcome this problem, pseudo-measurements are utilized. Pseudo-measurements are obtained from historical data at specific nodes, and are defined as Gaussian distributions.

4. R/X **ratio:** PDS cables are characterized by a high R/X ratio. This high ratio prevents certain relaxations and simplifications which are routinely exercises in Transmission level systems. An example of these simplifications is the usage of the linear DC power flow instead of nonlinear AC power flow.

5. **High number of nodes:** Due to the large networks structure, PDS have a high number of nodes. This results in a curse of dimensionality, where the computation burden significantly increases for any calculation on these networks.

6. **Network model uncertainty:** In contrast with the assumption of full knowledge of lines parameters, there is a high uncertainty in the network model, which negatively affects any process such as the DSSE [15].

2.1.1 Volt-Var Control (VVC) in PDS

The task of Volt/Var regulation is considered of highest importance in the distribution systems. The system operator aims to maintain the voltage level along the feeders within the specified limits at all times. This task has become more complicated due to the increased number of DGs, which significantly change the voltage profile [31, 32]. This section

provides a survey of various VVC schemes in Active Distribution Networks (ADNs). The control schemes are classified based on the used communication structure, as it will help categorize the cyber security risks in later sections. These schemes do not require remote measurements and they only depend on measurements at Points of Common Coupling (PCC). Due to their autonomous control structure, these methods require limited coordination and are generally more robust against communication-caused problems [33, 34]. However, they do not achieve optimal performance because of the limitations of communication with different systems components [35]. The communication based schemes can be categorized into: i) Centralized, ii) Distributed and iii) Decentralized. This classification will help in the assessment and classification of cyber-physical threats and attacks that target VVC schemes.

- **Centralized Control:** In centralized VVC schemes, one central controller is responsible for computing a global solution and sends control commands to all Intelligent Electronic Devices (IEDs). The centralized control scheme is more efficient the local scheme and requires smaller safety margins to remote measurements. In the same time, it is dependable on more communication links and does not adapt to changing operation needs [36]. Multiple authors have addressed the problem of DGs integration in distribution network based on centralized control scheme. In[37], coordinated voltage control algorithms are proposed to mitigate voltage rise problems and optimize usage of distributed energy resources. An efficient dispatch of load tap changers and shunt capacitors is proposed in [38].

- **Decentralized Control:** The decentralized control scheme aims to partition the power network into multiple sub-networks (zones), which communicate with each other [39, 40] to achieve VVC in the network. This allows running the voltage regulation problem in each sub-network area, rendering the optimization problem easier to tackle. In [41], the authors achieved voltage regulation through a distributed algorithm based on the ϵ decomposition of the sensitivity matrix. The control action is coordinated by communication between the areas to achieve optimal generation of the DGs.

- **Distributed Control:** The distributed control scheme establishes communication between each IEDs and neighboring nodes. The distributed control, along with the decentralized control, schemes are largely viewed as better approaches in the modern ADNs [42, 43]. The distributed control schemes allows a more efficient integration of distributed energy resources. However these benefits comes with the cost of adding vulnerable points to distribution networks.

2.2 Distribution Systems State Estimation (DSSE)

As a main part of the DMS, Distribution systems operators utilize the SE process in order to acquire knowledge of the system state variables such as voltage nodes or branch currents.

Figure 2.2 shows the SE process as a perquisite for all major processes such as DSOPF. The SE is a widely used technique for estimating the states in the power system networks.

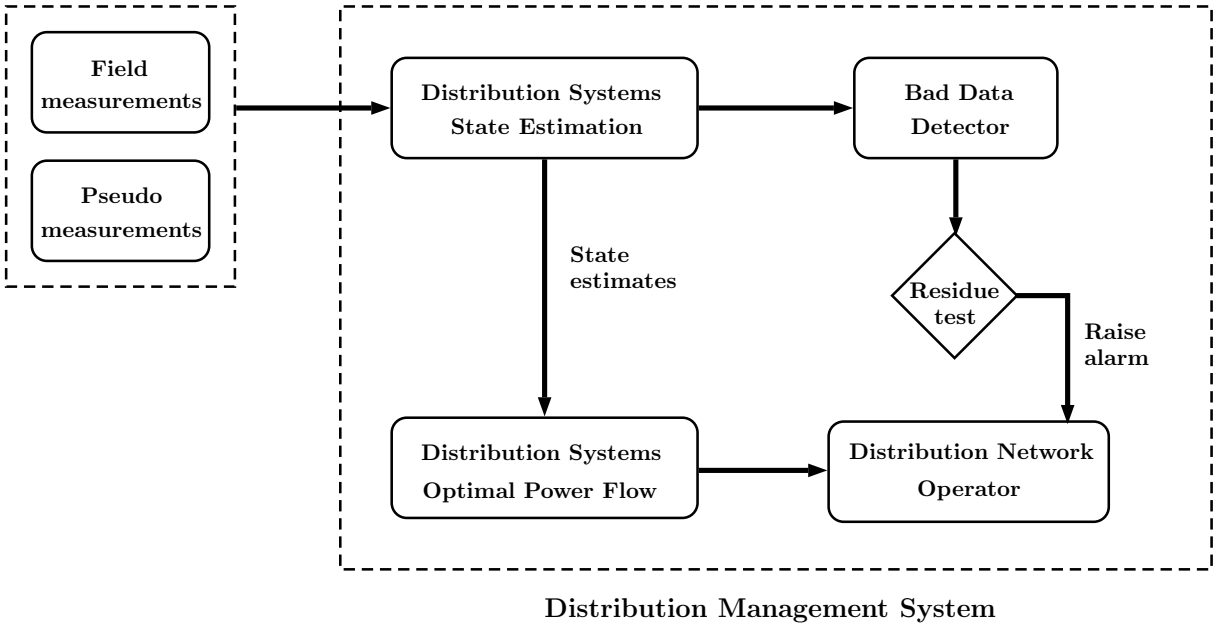

Figure 2.2: DSSE process in the DMS

The process of SE is critical to a reliable operation of the power systems as it ensures accurate representation of the system states given the uncertainty and errors of received measurements from various field devices. The majority of the implemented techniques for SE, however, are geared towards transmission systems and do not always suit the distribution systems[44], [17]. In the realm of PDS, this process is commonly referred to as DSSE, and different algorithms are implemented for this process. This section presents the mathematical formulation of the Weight Least Squares (WLS) algorithm, as it is the most common algorithm for DSSE. Based on the WLS method, the BCSE model is derived as the chosen model to implement the DSSE in this thesis. The Performance of the BCSE is evaluated on the IEEE-34 unbalanced radial bus system. As a direct result of the distinctive features of PDS, presented in the previous section, many dedicated research work

have developed specific techniques of SE, commonly referred to as Distribution Systems State Estimation (DSSE) tailored to fit the specific needs of distribution networks. The first class of DSSE algorithms are based on the WLS. System states can be voltage nodes [45, 46], or branch currents [47, 48]. Another approach is based on load adjustments, where the modeling of the loads is dependent on the customers profile curves [49]. Authors in [50, 51] adopted the iterative Gauss-Seidel load flow algorithm to adjust bus loads. Another category of DSSE focuses on the robustness of the process against any bad data or corrupted measurements. Machine Learning techniques have been employed in [52] to adjust weights based on confidence in their validity. Authors in [53] utilized the concept of leverage measurements to reduce measurements with high residuals. The modern PDS can be divided into zones and sub-networks, and distributed monitoring and control techniques are applied to all the sub-networks. The distributive process reduces the stress on a centralized control center to handle huge amounts of data with accuracy and speed. To that end, algorithms of distributed DSSE have been proposed for multi-area State Estimation [54, 55]. These processes can be done in parallel or in sequence [55]. Another well-known class of DSSE is Dynamic based State Estimation. In this types of DSSE, recursive estimations are based on consecutive snapshots measurements. The most common technique utilized for this approach is the iterated Kalman Filter method [56, 57]. Figure 2.3 summarizes the classification of different DSSE algorithms.

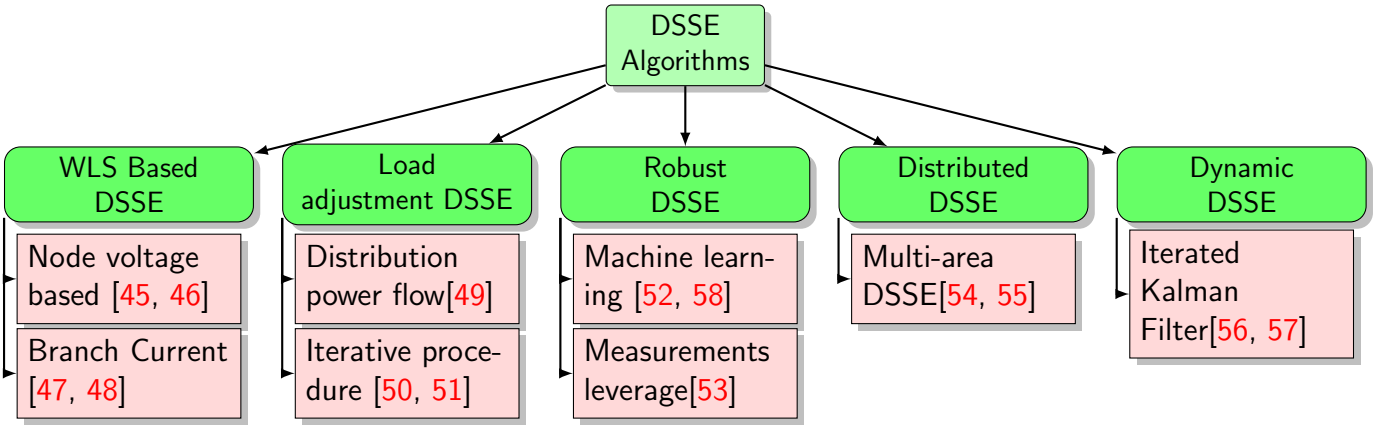

Figure 2.3: DSSE algorithms

2.2.1 Mathematical Formulation

This section reviews the general mathematical derivation of the SE process in details, and presents the WLS algorithm. Distribution systems operators collect field measurements and process them in order to infer the system states. The measurements vector consist of line active and reactive power flow measurements, bus active and reactive power injections, bus voltages magnitudes and angles. The measurement function $h(x)$ maps the system sates to the measurements vector z:

$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} h_1(x_1, x_2, \cdots, x_n) \\ h_2(x_1, x_2, \cdots, x_n) \\ \vdots \\ h_m(x_1, x_2, \cdots, x_n) \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix} = h(x) + e \tag{2.1}$$

where

z : power flow measurements vector $\in \mathbb{R}^m$

x : system states variables vector $\in \mathbb{R}^n$

$h(x)$: nonlinear measurement function that maps the states to the measurements

e : measurements error vector $\in \mathbb{R}^m$

The errors in this model represent the limited accuracy of readings, a malfunctioning meter or uncertainty of pseudo-measurement. Measurements errors are modeled as white Gaussian noise with zero mean and standard deviation σ. Typical choice of states x are voltage nodes magnitudes and angles, and branch currents. The measurement function $h(x)$ depends on the network model used. In this work, the three phases PI model is considered [59]. The model of the lines between the sending node V_s and receiving node V_r is shown in Figure 2.4: For a phase subscript $\phi \in \{a, b, c\}$, I_{s_ϕ} is the current from sending end, I_ϕ is the branch current, I_{r_ϕ} is the current at the receiving node end, and I_{y_ϕ} is the current flowing through the ground.

2.2.2 Weight Least Squares

The WLS method is the most common used method for state estimation, due to its high robustness and low computation cost. The standard approach of the WLS aims to minimize the weighted squares of the difference between the estimated measurements and the actual measurements [59]. The difference is referred to as the residual r and is represented as:

$$r = z - h(x) \tag{2.2}$$

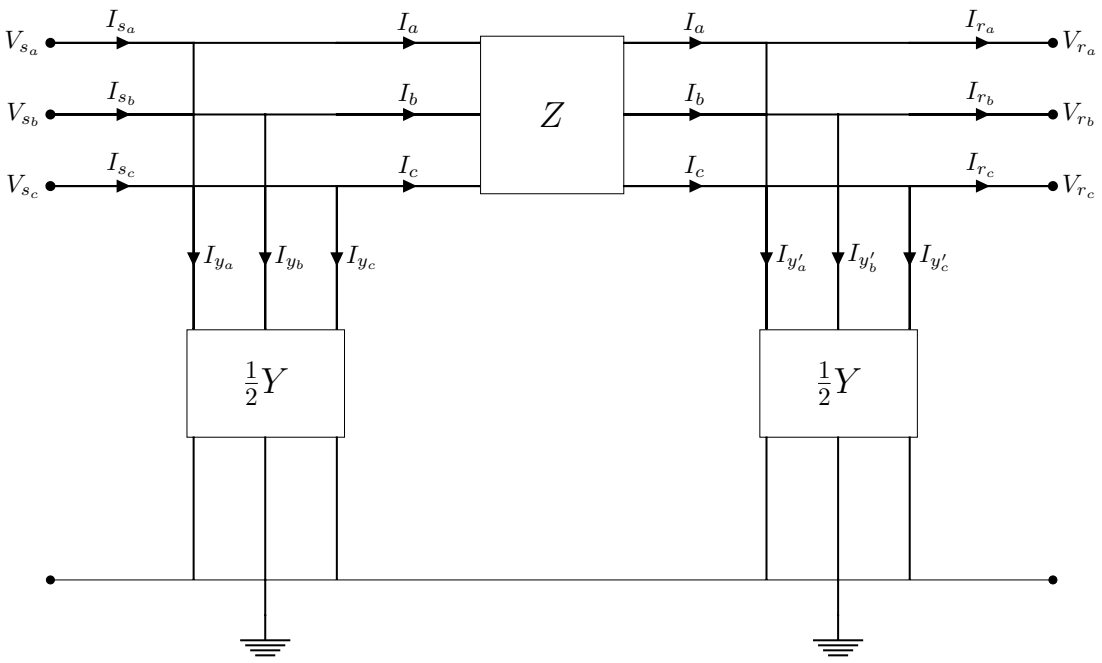

Figure 2.4: Three phases PI model

The WLS minimization objective function is defined as:

$$\underset{x}{\text{minimize}} \; J(x) = \sum_{i}^{m} \frac{(z_i - h(x))^2}{\sigma_i^2} = [z - h(x)]^\intercal \, W^{-1} \, [z - h(x)] \tag{2.3}$$

where σ_i^2 is the variance of meter (measurement) i, and W is a weighting diagonal matrix whose elements are the variance of meters errors, i.e., $W = diag\{\sigma_1^2, \sigma_2^2, \cdots, \sigma_m^2\}$. The first-order optimality condition is then applied to find the minimum:

$$g(x) = \frac{\partial J(x)}{\partial x} = -H^\intercal(x) W^{-1} [z - h(x)] \tag{2.4}$$

where $H(x)$ is the Jacobian matrix defined as:

$$H(x) = \frac{\partial h(x)}{\partial x} \tag{2.5}$$

A Taylor expansion is applied to Equation 2.4 around the variable x^k:

$$g(x) = g(x^k) + G(x^k)(x - x^k) + \cdots = 0 \tag{2.6}$$

where $G(x)$ is the Gain matrix and obtained by:

$$G(x^k) = \frac{\partial g(x)}{\partial x} = H^\intercal(x^k) W H(x^k) \tag{2.7}$$

The Gain matrix is usually sparse, positive definite and symmetric. Applying an iterative method such as the Gauss-Newton minimization method results in:

$$x^{k+1} = x^k - \left[G(x^k)\right]^{-1} \cdot g(x^k) \tag{2.8}$$

where k is the iteration index, x^k is the solution vector at iteration k. The solution is found by iteratively solving Equation (2.8) until a satisfactory accuracy is reached, usually implemented by pre-setting a threshold for accuracy or a maximum number of iterations.

2.2.3 Branch Current State Estimation

The BCSE model is used for DSSE, as it is more accurate and is more efficient for the state estimation iterative procedure in radial systems [60]. In addition, the usage of BCSE allows the decoupling of the phases in the unbalanced systems.

For distribution radial feeders branch currents for phase ϕ are defined as:

$$I_l^\phi = I_{re}^\phi + jI_{im}^\phi \tag{2.9}$$

where I_{re}^ϕ, I_{im}^ϕ, are the real and imaginary components of the branch currents, respectively, Branch currents are determined from the real and reactive power flow measurements for each phase as follows:

$$I_{re}^\phi(V_s) + jI_{im}^\phi(V_s) = \left(\frac{P^{m,\phi} + jQ^{m,\phi}}{V_s^\phi}\right)^* \tag{2.10}$$

where $P^{m,\phi}$, $Q^{m,\phi}$ are the real and reactive power measurements, respectively, with the superscript m denoting a measurement quantity, and V_s^ϕ is the node voltage. The measurement function of the equivalent current measurements is represented by:

$$h_{re}^\phi(I_{re}^\phi) + jh_{im}^\phi(I_{im}^\phi) = I_{re}^\phi + jI_{im}^\phi \tag{2.11}$$

In addition to the power flow measurements, branch current measurements are also mapped by:

$$h_c^{\phi}(I^{\Phi}) = \sqrt{I_{re}^{\phi^2} + jI_{im}^{\phi^2}} \tag{2.12}$$

where $h_{re}^{\phi}(I_{re}^{\phi}) + jh_{im}^{\phi}(I_{im}^{\phi})$ is the branch current magnitude measurement function. The minimization problem for the BCSE can be formatted for each phase ϕ by:

$$\underset{I}{\text{minimize}} \;\; J(I) = \sum_{i}^{ms} \frac{(I_{re_i}^{m,\phi} - h_{re}(I_{re_i}))^2 + (I_{im_i}^{m,\phi} - h_{im}(I_{im_i}))^2}{\sigma_i^2} + \sum_{i}^{mc} \frac{(I_{c_i}^{m,\phi} - h_c(I_{c_i}))^2}{\sigma_i^2} \tag{2.13}$$

where ms, and mc denote the number of power measurements and branch current magnitude measurements, respectively. The first summation reflects the optimization of the power measurements, and the second summation of the current measurements. The first summation has a linear solution of the form:

$$h_{re}^{\phi}(I_{re}^{\phi}) = A(I_{re}^{\phi}) \tag{2.14}$$

$$h_{im}^{\phi}(I_{im}^{\phi}) = A(I_{im}^{\phi}) \tag{2.15}$$

where A is a constant matrix with the entries equal -1 or 1. To validate the accuracy of the BCSE, a model is built to estimate the voltage magnitudes and angles of the IEEE-34 radial system. The results are compared to the voltage profile reported in [61]. Figure 2.5 depicts the absolute percentage error in the voltage magnitudes of the three phases for each node. The maximum error does not pass the 0.9% mark. Figures 2.6 and 2.7 show the comparison between the voltage magnitudes (in p.u.) and the voltage angles (in degrees), respectively. The results confirm the accuracy of the BCSE for estimating the node voltages for all the nodes.

2.2.4 Bad Data Detection

The process of SE may include bad measurements that results in unreliable predictions of the system state. Several reasons contribute to bad measurements such as meter malfunctioning, or intentional malicious attacks. Several, statistical based, techniques have been developed to identify and eliminate bad measurements [62, 63]. The core defense mechanism is based on the Bad Data Detection (BDD) approach, which is a statistical approach that compares the residual difference between the measurements vector and the estimated measurements vector resulting from the SE process. A common approach based on the residuals in the Largest Normalized Residual Test (LNRT) [59]. This test is used

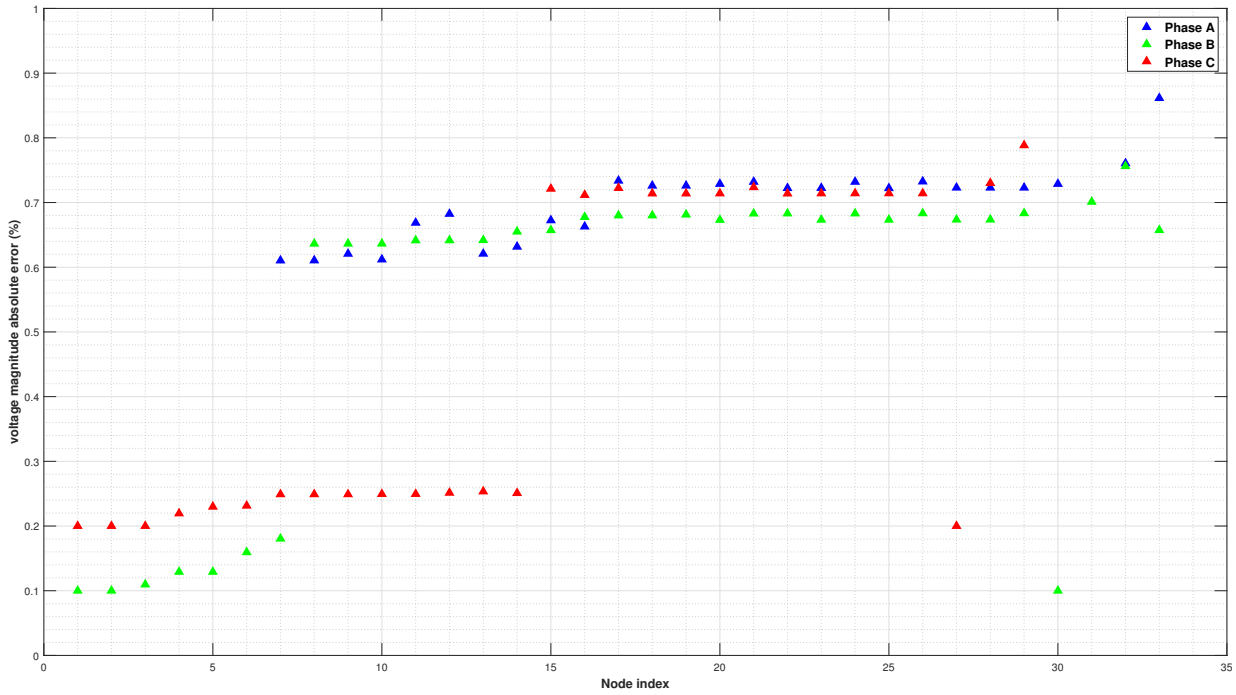

Figure 2.5: BCSE magnitudes errors

to detect and remove bad measurements, as follows: i) Compute the residual according to (2.2), ii) find the largest residual and compare it to a pre-defined threshold, and remove this measurement if the residual exceeds the threshold, iii) re-iterate the SE process again.

2.3 Optimal Power Flow (OPF)

The OPF processes in power systems encompasses optimization problems that aims to optimize certain operation objectives using numerical analysis. The OPF has been introduced by Carpentier which was formulated as an extension to economic load dispatch to minimize the total cost of electricity generation while keeping the electrical system within the prescribed operation limits [64]. Over the period of more than five decades, OPF has been a research focus and has become a mature operation utilized by system operators.

The OPF can be constructed in different variants based on the objective of the system operator, and the nature of the modeled power system. For example, Security constrained OPF includes the power system contingency constraints [65, 66]. A commonly used version

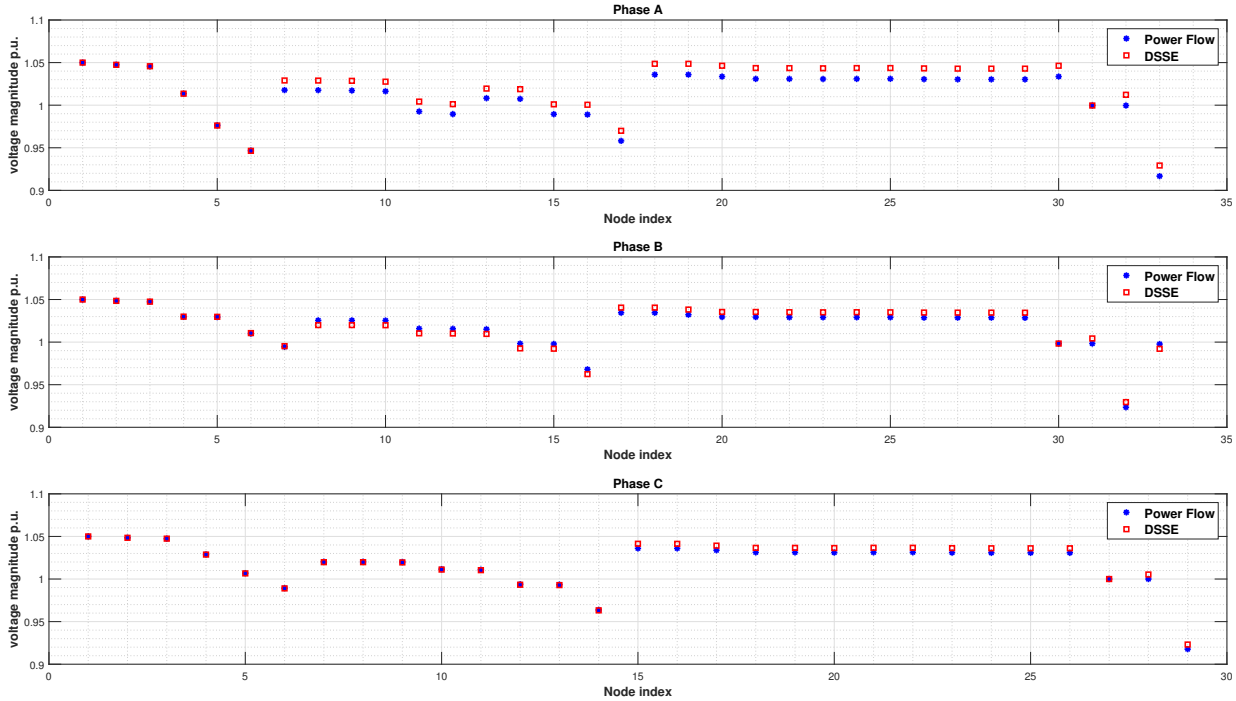

Figure 2.6: Voltage magnitudes comparison

of the OPF is the DCOPF, which is a Linear Programming optimization problem [67, 68]. The application of the OPF determines the objective function as it can be applied to minimize operation costs, optimize capacitor placement, or optimizes nodal pricing of power. Equality constraints of the optimization problem include the power balances of the system at each node, while the inequality constraints include the control variable limits, voltage magnitude limits, thermal limits, bound on voltage angles, and operating limits on power flows.

A subset of OPF formulations has been tailored to better suit the nature of the PDS, and is known as Distribution Systems Optimal Power Flow (DSOPF) [69, 70, 71]. Optimal Reactive Power Flow (ORPF), also referred to as reactive power dispatch or VAR control aims to minimize the losses in distribution networks. In ORPF, the real power generation is calculated beforehand [72]. In addition to the classical OPF formulation, the vector of control variables includes the effects of phase-shifting and load tap change transformers, shunt capacitors operations, which are often represented by integer variables for tap changes, and binary variables for ON/OFF switching of shunt capacitors [73].

The DSOPF is inherently a non-convex problem, because of the non-convex and non-

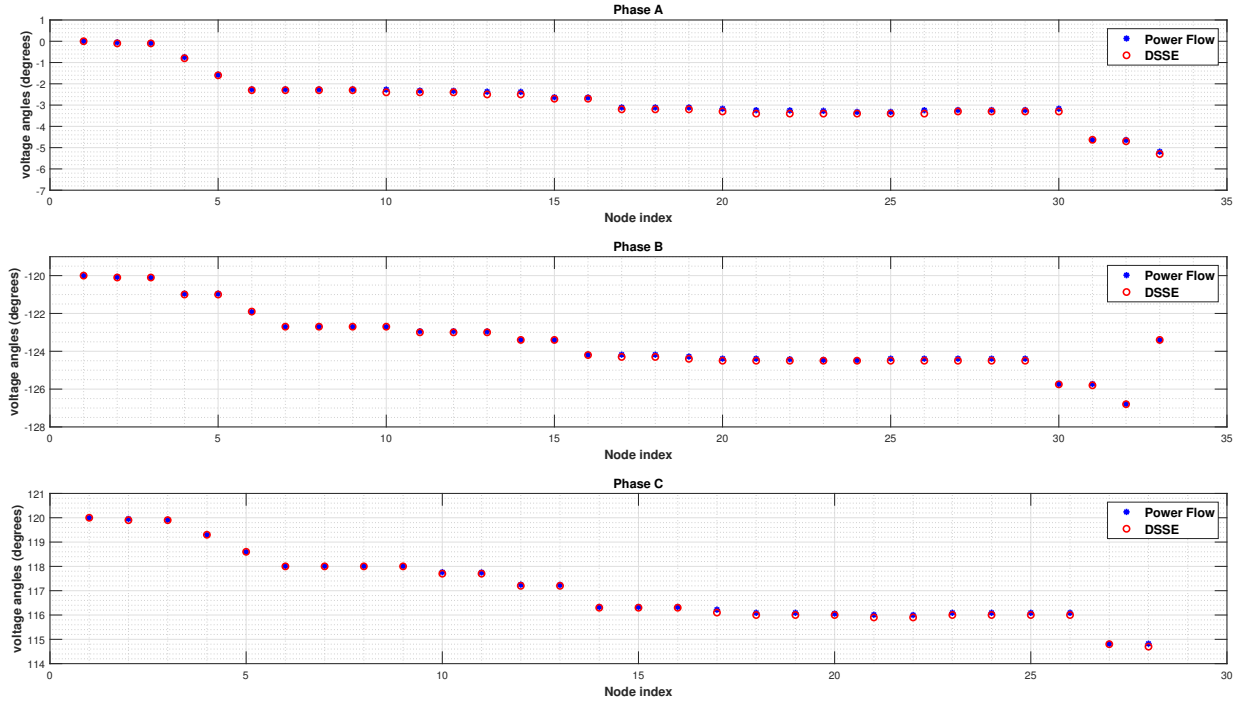

Figure 2.7: Angles comparison

linear constraints, which makes reaching an accurate optimal solution a non-trivial task. In order to overcome the nonlinear and non-convex constraints, there are usually three approaches [74]: i) linearize power flow constraints, ii) look for local optima, or iii) convex relaxations of the power flow constraints. Since convex problems guarantee finding global minimum, convex DSOPF (or OPF in general) determines absolute lower or upper bound of control effort. In addition, as PDS, are usually radial in nature, it is more efficient to utilize Branch Flow Model for the power flows. In [75], authors utilize a Semi Definite Programming (SDP) convex relaxation for OPF in radial distribution networks and prove the exactness of the approach.

2.3.1 OPF Formulation

The OPF is an optimization problem that seeks to optimize a particular objective function in the power systems operations. System operators depend on the OPF to minimize operations costs, limit voltage deviations, ensure system supply security, and optimally allocate DG resources in across the smart grid. The standard representation of an OPF is

as follows:

$$\underset{x}{\text{minimize}} \quad f(x) \tag{2.16a}$$

$$\text{subject to} \quad g(x) = 0, \tag{2.16b}$$

$$h(x) \leq 0 \tag{2.16c}$$

where

$f(x)$ is the objective function
$g(x)$ is the set of equality constraints
$h(x)$ is the set of inequality constraints

The objective function expresses the quantity to be optimized, the equality and constraints represent the physical laws such as power balance and kirchoff's laws, and the inequality constraints define bounds of operations and contingency constraints on voltages and power flows. The two sets of constraints have to be obeyed while solving the OPF problem.

2.3.2 Branch Flow Model (BFM)

The Branch Flow Model (BFM) is considered in this thesis to model the DSOPF, as it is most suitable for the PDS, which are usually radial in nature [76]. For a radial system with a set of N buses indexed by $i = 1, 2, ..., n$, and E distribution lines connecting these buses, the power flow equations can be formulated as follows [73]:

$$s_j = (S_{ij} - z_{ij}|I_{ij}|^2) - \sum_{(j,k)\in E} S_{jk}, \qquad \forall (i,j) \in E \tag{2.17}$$

$$V_i - V_j = z_{ij} I_{ij}, \qquad \forall (i,j) \in E \tag{2.18}$$

$$S_{ij} = V_i I_{ij}^*, \qquad \forall (i,j) \in E \tag{2.19}$$

where

$s_j = p_j + p_j$: complex net load on bus j (net load is defined as the consumption minus generation),
$S_{ij} = P_{ij} + jQ_{ij}$: complex power flow from bus i to bus j,
$z_{ij} = r_{ij} + jx_{ij}$: impedance on line (i, j),
I_{ij} : complex current from bus i to bus j,
V_i : complex voltage on bus i

Equation (2.17) defines the power balance at each bus j, Equation (2.18) is Ohm's law on each line (i, j), and Equation (2.19) defines the complex power on each line (i, j). The following variables are introduced for notational simplicity: $v_i = V_i^2$ and $l_{ij} = I_{ij}^2$. From Equations (2.17) and (2.18), we get:

$$V_j = V_i - z_{ij}\frac{S_{ij}^*}{V_i^*} \tag{2.20}$$

and by taking the square of the magnitude:

$$v_j = v_i + |z_{ij}|^2 l_{ij} - (z_{ij}S_{ij}^* + z_{ij}^* S_{ij}) \tag{2.21}$$

Separating Equations (2.17) and (2.19) into active and reactive power terms yields:

$$p_j = (P_{ij} - r_{ij}l_{ij}) - \sum_{(j,k)\in E} P_{jk} \tag{2.22}$$

$$q_j = (Q_{ij} - x_{ij}l_{ij}) - \sum_{(j,k)\in E} Q_{jk} \tag{2.23}$$

$$v_j = v_i - 2(r_{ij}P_{ij} + x_{ij}Q_{ij}) + (r_{ij}^2 + x_{ij}^2)l_{ij} \tag{2.24}$$

$$l_{ij} = \frac{P_{ij}^2 + Q_{ij}^2}{v_i} \tag{2.25}$$

The set of Equations (2.22)-(2.25) were first introduced in [73] to model radial systems, and they represent a relaxed branch flow model of Equations (2.17)-(2.19). The former set of Equations represent in the variables (P, Q, l, v) represent a subset of the original modelling variables (S, I, V), without the current and voltage phasor angles. According to [77], there is a one-to-one correspondence between Equations (2.17)-(2.19) and Equations (2.22)-(2.25) in radial networks, and it is therefore possible to compute, effectively, the phasors angles based on the latter set of Equations. To construct the OPF problem, we add the following constraints to the branch flow model (Equations (2.22)-(2.25)):

$$\underline{p_i} \leq (p_i) \leq \bar{p_i} \quad i = 1, 2, ..., n \tag{2.26}$$

$$\underline{q_i} \leq (q_i) \leq \bar{q_i} \quad i = 1, 2, ..., n \tag{2.27}$$

which represent the lower and upper bounds on active and reactive power, and

$$\underline{v_i} \leq (v_i) \leq \bar{v_i} \quad i = 1, 2, ..., n \tag{2.28}$$

which represents the lower and upper bounds of bus voltage magnitudes.

2.3.3 Semi Definite Programming Optimal Power Flow

The OPF is an integral part of the distribution systems operations, and is used to efficiently optimize the operation of the distribution network. For the PDS, the complexity of DSOPF arises from the 3-phases, unbalanced radial configuration of the networks. Several approaches are used to obtain the most accurate representation and reduce the required computation. Approaches usually attempt to either linearize the constraints, find local optima, or relax the constraints into convex constraints [78]. The convex relaxation approach consists of transforming a non-convex problem into a convex-problem, so one global minimum is to be found. Figure 2.8 shows the convex relaxation of non-convex function.

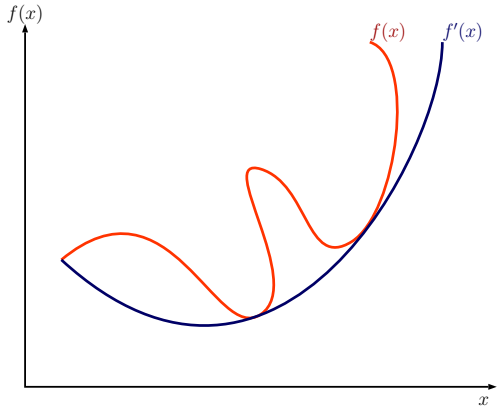

Figure 2.8: Convex relaxation of a non-convex function

Concerning the DSOPF, there is growing interest in convex relaxations on OPF [79, 78]. Many of the research assumes a single-phase model, based on the assumption that multi-phases networks can be rendered into equivalent single-phase network [80]. one approach of convex relaxation is the transformation of the DSOPF into a convex Semi Definite Programming (SDP) problem. Authors in [75] proposed an SDP convex relaxation and a linear approximation of power flow, and proved that the former is exact *iff* the latter is exact as well. This work has been applied to multi-phase radial networks, and is applicable for VVC and demand response. The three main concerns in regard to the OPF convex relaxations in general [75]: i) Feasibility of global optimal solution through convex relaxations, ii) Efficient convex relaxation computations, and iii) Numerical stability. In this work, the convex relaxations based on SDP is chosen for its numerical stability [81].

A SDP optimization problem has the standard form:

$$\text{minimize} \quad C \bullet X \tag{2.29a}$$

$$\text{subject to} \quad A_i \bullet X = b_i, \ \forall i = 1, \cdots, m, \tag{2.29b}$$

$$X \succeq 0, \tag{2.29c}$$

where $X \in S_+^n$, and S_+^n denotes the set of positive semidefinite symmetric $n \times n$ matrices, and C is also symmetric. Constraint (2.29c) denotes X is a positive semidefinite symmetric matrix. The objective function is a linear function of the matrix X, and there are m linear equality constraints, denoted by constraint (2.29b). With the SDP formulation, a wide variety of optimization problems can be solved efficiently, in theory and in practice [82]. The DSOPF can be cast as SDP problem as follows:

$$\text{minimize} \quad \sum_i C_i(s_i) \tag{2.30a}$$

$$\text{subject to} \quad \sum_{j:k}(S_{ij} - z_{ij} l_{ij}) + s_j + y_j v_j = \sum_{j:k} diag(S_{jk})^{\Phi_j}, \tag{2.30b}$$

$$v_j = v_i^{\Phi_{ij}} - (S_{ij} z_{ij}^H + S_{ij}^H z_{ij}) + z_{ij} l_{ij} z_{ij}^H), \tag{2.30c}$$

$$\underline{v_i} \leq diag(v_i) \leq \bar{v_i}, \tag{2.30d}$$

$$\underline{v_0} = V_0^{ref} (V_0^{ref})^H, \tag{2.30e}$$

$$\begin{bmatrix} v_i^{\Phi_{ij}} & S_{ij} \\ S_{ij}^H & l_{ij} \end{bmatrix} \succeq 0 \tag{2.30f}$$

where $C_i(s_i)$ denotes the power losses at bus i, and s_i is the branch power injection. The reactive power of the shunt capacitors is represented by relaxing their output as continuous variables and constraining the real part of s_i to zero, V_i denotes the voltage at node i, while I_{ij} denotes the branch current between nodes i and j. Control variables are defined by: $v_i = V_i V^H$, $l_{ij} = I_{ij} I_{ij}^H$, and $S_{ij} = V_i^{\Phi_{ij}} I_{ij}^H$, with the superscript H indicating the Hermitian transpose, and superscript Φ as phase index. Constraint (2.30b) describes the power flow balance equation, Kirchoff's voltage law is described by (2.30c), lower and Upper voltage bounds are enforced by (2.30d), while the source voltage node is enforced by (2.30e), and (2.30f) is the positive semi-definite constraint.

2.3.4 Load Models

Power consumption for loads is dependent on voltage and frequency and therefore it is crucial to capture an accurate behaviour of the load for the critical operations in power

systems such as the power flow analysis and state monitoring. Considering the static loads model, (i.e., time independent), loads characteristics can be defined as [83]:

$$P = p(V, f) \tag{2.31}$$

$$Q = q(V, f) \tag{2.32}$$

where P and Q are the active and reactive power, V is the voltage magnitude, and f is the frequency. Most commonly used is the exponential load model, where loads are classified as constant power, constant current, and constant power loads. In constant power model, loads power do not vary with the change in voltage magnitude, and consequently the voltage and the current are allowed to change to hold the power constant. This load is the most common model in transmission systems. In constant current models, the power varies directly with the voltage magnitude. Distribution systems voltage drop calculations typically model loads as current sinks. In constant impedance model, the power varies with the square of voltage magnitude. This model is utilized for certain voltage unbalance analysis and motor starting calculations. The exponential load model is defined mathematically by:

$$P = P_0 \left(\frac{V}{V_0} \right)^{\alpha}, \tag{2.33}$$

$$Q = Q_0 \left(\frac{V}{V_0} \right)^{\beta} \tag{2.34}$$

where P_0 and Q_0 define the active and reactive power consumption at the rated voltage V_0. For Constant impedance loads $\alpha = \beta = 2$, for constant current loads $\alpha = \beta = 1$, and for constant power loads $\alpha = \beta = 0$. The sensitivity of load power to voltage is derived by taking the derivative of the power with respect to voltage change [83]:

$$\frac{dP}{dV} = \alpha P_0 \left(\frac{V}{V_0} \right)^{\alpha - 1} \frac{1}{V_0} \tag{2.35}$$

This sensitivity analysis is widely used for voltage stability calculations. By arrangement of (2.35), and setting $V_0 = V$ we get:

$$\frac{dP/P_0}{dV/V_0} = \alpha \tag{2.36}$$

Thus, the normalized sensitivity of power is equal to the corresponding load exponent [83]. By taking the inverse we get:

$$\frac{dV/V_0}{dP/P_0} = \frac{1}{\alpha} \tag{2.37}$$

Equation (2.37) implicates that the change in voltage based on power variation will be most sensitive for lower α values. Therefore, voltage values of constant power loads will be of higher sensitivity, then constant current, and finally constant impedance.

2.4 Cyber-Physical Security

The cyber-physical security of the power systems is considered one of the most critical challenges to the overall modern grid. The Power Distribution Systems (PDS) are witnessing an increasing penetration of Distributed Energy Resources (DERs) that add new layers of challenges to goal of operating the power networks securely and reliably. With the incorporation of communication into the power networks, a wide range of vulnerability points are created [20]. The motivations behind launching cyber-physical attacks include, but not limited to, financial motives (e.g., energy theft), terrorism and system corruption (e.g., cascading failures of energy systems) [84]. The cyber-physical security aspect affects nearly all the critical operations of monitoring, control and protection for the power systems. Thus, it is of the utmost importance to consider the various threats while designing the modern smart grid. As an integral part of the smart grid, The PDS has its share of risks, especially with the recent developments on the distribution level. The new upgrades to the PDS include large shares of DGs which contribute to a bi-directional power flow, new schemes of VVC which are based on communication and coordination between different control equipment, and the addition of smart meters and measurement devices that send sensitive data over multiple communication networks. Table 2.1 summarizes the classification of the cyber-physical challenges that face the modern PDS.

Table 2.1: Risks due to modernization of distribution networks

Conventional Power Distribution Systems	Modern Power Distribution Systems	Possible cyber-physical security threats
Unidirectional flow	Bidirectional power flow	[85, 86]
Local and simple centralized Volt-Var Control	Sophisticated strategies	[87, 88]
Non-existing distributed generation	Large share of Distributed Generators (DGs) renewable energy resources and Microgrids	[89, 90]
Minimum level of communication	Sophisticated communication networks over several layers	[91, 9, 8]
Local measurements units	Smart sensors, digital meters and PMUs	[92, 11, 93]

2.4.1 Cyber-Physical Security Requirements

There are different technical and also regulatory challenges for the security in the recent distribution system [94, 95] include: 1) the complexity and scale of future power distribution systems, 2) traditional communication vulnerabilities, 3) new communication requirements 4) trustworthy between all participation parties, 5) legacy devices, 6) heterogeneous technologies and protocols, 7) proprietary systems, and 8) users privacy. To overcome all the pre-mentioned challenges, many security properties are required by the power distribution systems i.e., availability, confidentiality, integrity, authentication, authorization. These requirements can be defined as:

1. **Availability:** Requires that the data must be available to the authorized parties when there is a need for this data without any security compromise [96, 97, 98, 99]. It assures that all network resources (e.g., data, bandwidth, equipment, servers) are always available at all nodes for the authorized parties [100, 7, 101]. The importance of the availability of data has been from the fact that the cyber layer of the distribution system, and in power system in general, manages the continuous power flow in the physical layer. Therefore, any data shortage may drive the the power system operators to make wrong decisions.

2. **Confidentiality:** Means that data is disclosed only to authorized individuals or systems [100, 7, 96, 97, 98, 99]. Critical data in power system distribution e.g., meter data should be confidential. Meter data is critical because it provides information about the usage patterns for individual appliances, which can reveal personal activities through non-intrusive appliance monitoring. For this purpose, the meter data should be protected such that only intended parties can access. Price information and control commands are not critical as long as it is public knowledge [20].

3. **Integrity:** Is the assurance that the accuracy and consistency of data is maintained. No unauthorized modifications, destruction or losses of data go without being detected [100, 7, 101, 96, 97, 98, 99]. Integrity of price information, meter data, control commands, and software used in power system substations are critical. For instance, negative prices injected by an attacker can cause an electricity utilization spike as numerous devices would simultaneously turn on to take advantage of the low price. The impact of attacking the integrity of meter data and control commands is mostly limited to revenue loss. However, integrity of software is critical since compromised software or malware can control any device and component in the power system [20].

4. **Authorization:** Also known as access control as it makes sure that the access rights of every entity in the substation are defined for the purposes of access control [100]. On one hand, authorization distinguishes between valid and invalid users for all other security objectives, e.g., confidentiality, integrity, etc. On the other hand of access control, it restricts the ability to issue commands to the plant control system. Violation of authorization may cause safety issues [12].

5. **Authentication:** Identity verification of a communication system practitioner and linking this identity to a system-internal principal (e.g., valid user account) by which this user is known to the system. In other words, the validation that communicating parties are who they claim they are, and that messages supposedly sent by them are indeed sent by them [100]. Most other security objectives, most notably authorization, distinguish between legitimate and illegitimate users based on authentication [12]

2.4.2 Threats Analysis

Common cyber-physical attack models

In order to equip the PDS, and the whole of smart grids for that matter, against cyber-physical threats, a thorough analysis of the network architecture and the different interconnection links is of utmost necessity. The most commonly threats and attack models in literature include:

- **Man in the middle attacks:** By getting access to a communication channel, an adversary alters metering devices and thus compromising the availability and integrity of power system data. Conditions and impacts of such attacks is presented in [102], and data framing attack is proposed in [103]. The replay attack is another form of man in the middle attack that can incur catastrophic negative impacts [104].

- **Rogue Devices:** If an attacker gets physical access to field devices such as sensors or PMUs, they can replace the device with a rogue one that sends corrupted signals, or falsely acknowledges the performance of specific operation [105, 5].

- **Denial of Service (DoS):** DoS attacks target the availability security objective, by attempting to corrupt, delay or block critical communication links by flooding the communication with a bogus traffic [8]. Different communication layers in the power systems are found to be susceptible to DoS attacks [7]: (i) Channel Jamming can

occur on the Physical layer, with effects ranging from delayed delivery of messages to complete denial of service [106], (ii) MAC layer, as attackers can modify MAC parameters, leading to a spoofing attack. An Intrusion detection method is proposed in [107] to detect threats on an IEC61850 automated substation. (iii) Network and transport layers targeted attacks can severely affect performance of end to end communication. For example, [108] investigated the vulnerability of real hardware and software to DoS attacks.

- **False Data Injection (FDI):** The FDI attacks result from injecting (corrupting) measurements data, with the goal of initiating wrong control actions. A well known FDI model are attacks that target the SE process and bypasses the BDD, first introduced by Liu *et al.* [109]. Several assumptions, conditions and scenarios have been studied to launch successful attacks such as the usage of AC power flow model [18], attacks on PDS [19], attacks with incomplete information [110], attacks against Automatic Generation Control Systems [111], and attacks targeting electricity markets [112]. Counter-measures techniques of attacks detection and mitigation have been investigated in [113, 114, 115]. Further analysis of the FDI attacks is presented in chapter 3.

It is important to assess the possible threats and their impacts on the cyber-physical requirements when designing modern power systems. Table 2.2 categories the different attack models that threaten the distribution networks [9], [5], and the impacts on the cyber-physical security requirements stated in the previous section.

Table 2.2: Classification of cyber-physical attacks

Attack model	Cyber	Physical	Attack target
Denial of Service (DoS)	✓	✓	Availability
Eavesdropping	✓		Confidentiality
False Data Injection (FDI)	✓	✓	Integrity
Malicious software patching	✓	✓	Authentication
Man in the middle	✓	✓	Integrity, Confidentiality
Rogue devices		✓	Integrity, Confidentiality
Unauthorized access		✓	Authorization, Confidentiality
Wireless scrambling	✓		Integrity

2.4.3 Cyber-physical attacks on PDS

The problem of Volt-Var optimization under malicious attacks has been investigated by Majumdar *et al.* in [116]. The authors have investigated mitigation techniques against the attacks on VVC that target the DSSE, and presented two formulations for mitigation. The first solution depends on the local controller set-point, where it proposes the usage of DERs power generation instead of attacked measurements. The second solution is to use the historical data to build a density function of the attacked state. Isozaki *et al.* [87] investigated the impact of cyber attacks on voltage regulation in distribution systems, in the presence of Photovoltaic (PV) systems and the usage of communication based sensors. The authors demonstrate that voltage regulations can occur if measurements are falsified, and a detection algorithm is presented to limit the damage of attacks, especially in the case of limited number of attacked sensors. The attacker falsifies measurement data to cause irregular tap changes in the LRTs, thus causing voltage violation at feeder nodes. Two possible attack scenarios are considered: Suppressing tap changes at the LRT, or Inducing tap changes at the LRT. Both scenarios may lead to under-voltage (over-voltage) at some nodes, based on the load profile at each node. In order to achieve the most efficient attack, the attacker aim is to maximize the voltage variation, constrained by lower and upper limits of voltage values. The proposed algorithm is composed of four steps [87]: (1) Checking whether a measurement value V_i falls within admissible range of upper and lower limit values for voltage at node i. (2) Checking of nodes voltage order. In the case of no power injections through PVs, then node voltages values are smaller than those upstream. This step is ignored in the presence of operating PVs. (3) Checking voltage Variation rate. If a tap change did not occur in the previous time step $(k-1)$, then the difference, at node i, between $V_i(k)$ and $V_i(k-1)$ is lower than a time-varying upper bound. (4) Checking lower bound on voltage differences, which is achieved by checking that the difference between maximum and minimum voltage values at a given node is bigger than a time- varying lower bound. The results in [87] show that falsification of measurements can be detected in the case of limited number of attacked nodes, while voltage violation can result due to larger number of attacks. Also, attacks that target PV output power have been investigated. Teixeira *et al.* [88] addressed stealthy attacks that target integrated VVC measurements. Considering $\mathbb{C}_{\mathbb{F}}$, a subset of capacitor bank configuration $\mathbb{C}$ that satisfy all operational constraints in system state $\mathbf{x}$, the optimal configuration for cost is minimization is found as:

$$C(\mathbf{x}) = \underset{C \in \mathbb{C}_{\mathbb{F}}(\mathbf{x})}{\arg\min}\ V(\mathbf{x}, C) \tag{2.38}$$

The attacker objective is to maximize adverse impact without being detected. Therefore, under the assumption of access only to voltage measurements, a $\mathbb{C}_k$ stealth attacks can be

defined as [88]: an attack vector $\mathbf{a}$ is a $\mathbb{C}_k$ stealthy attack *iff* there exists $\Delta\mathbf{y} \in \mathbb{C}^n$ such that

$$\begin{cases} \mathbf{a} = H_v(C_k)\Delta\mathbf{y} \\ 0 = H_S(C_k)\Delta\mathbf{y}. \end{cases} \tag{2.39}$$

Where H_v and H_S are matrices derived from system topology. Moreover, the authors present a game-theoretic framework to limit the adversary action space. The operator strategically bases countermeasures to detect and mitigate possible action strategies adopted by the adversary. Results reveal damages that occur from data manipulation while the operator continues to apply normal system configuration. Evaluating VVC on IEEE-13 node feeder, using GridLab-D [117]. For a stealthy attack of adding and subtracting 50 volts at two distinct nodes, respectively, the VVC was able to bring the voltages from 2450 volts to 2350 volts, although the actual desired level is 2300 volts. Deng *et al.* incorporated FDI attacks that bypass BDD in DSSE for PDS [19]. Although multiple FDI attacks schemes have been proposed and analyzed in several occasions [18, 118, 119], however the FDI was based on an attack model that assumes a strong condition of having access to the states in the system. This strong condition may be valid and practical in transmission systems, however it is not the case in Distribution systems due to difference in topologies and properties of the two systems. Nodal voltage phasors values, used as system states, cannot be easily obtained in the Distribution systems due to the limiting availability of PMUs. To tackle this challenge, the authors propose constructing local FDI attacks, based on approximate states obtained from local measurements. Using the voltage and phase angles as system states, approximation of voltage magnitude and phase angle at node j, V_j and θ_j are given by [19]:

$$\begin{cases} V_j \approx V_i - (P_{ij}r_{ij} + Q_{ij}x_{ij}) \quad \forall j \in \mathbb{N} \\ \theta_j \approx P_{ij}x_{ij} - Q_{ij}r_{ij} \quad \forall\{i,j\} \in \mathbb{L} \end{cases} \tag{2.40}$$

where P_{ij}, Q_{ij} and r_{ij}, x_{ij} are the active and reactive power flow, line resistance and reactance between nodes i and j, respectively, while $\mathbb{N}, \mathbb{L}$ are the set of nodes and set of lines respectively. Based on these approximations, approximations of nodal voltages and phase angles are obtained from local meter measurements. The information are used to launch a local FDI attack. It is worth mentioning that the authors did not consider VVC in their model. Also, the strong condition stated by the authors is valid for using nodal voltage based SE. Table 2.3 summarizes some of the work done concerning attacks that target VVC in PDS, and comments on the assumptions made in each work and the considered model.

Table 2.3: Summary of Volt/Var attacks on PDS

Attack type	Contribution	Approach/Solution	Remarks
Falsifying voltage measurements with PV injection nodes [87]	Mitigation algorithm	Sequential check of nodal voltage according to pre-set criteria	Does not consider BDD in SE
Data Integrity attacks [88]	Attack algorithm	Stealthy attacks by corruption set of measurements	Assumption of full system topology knowledge
FDI against approximated DSSE [19]	Attack algorithm	Local FDI attacks based on low cost approximate states	Nodal voltage based DSSE on balanced system, no consideration of VVC equipment
Attacks against leverage measurements [120]	Detection algorithm	Identification and separation of leverage measurements using Diagnostic Robust Generalized Potentials (DRGP)	Statistical method applied on transmission and distribution systems
Malicious attacks on DERs [116]	Mitigation algorithm	Probabilistic VVC optimization strategy and Forecast aided approaches	Backup solution based on local measurements

2.4.4 Detection of FDI Attacks

The literature classifies methods of protection against FDI attacks into protection-based approaches and detection-based approaches. Protection-based approaches depend on protecting measurements of certain sensors from being attacked [121]. The realization of these approaches depends on the determination of minimal set of measurements needed for protection. Drawbacks of these approaches include the drop of measurements redundancy and the unguaranteed effectiveness under all operating conditions [122]. Detection-based approaches, however, use Bayesian framework to detect the attack [123]. The objective of these methods is to detect any anomaly, or abnormal data points in the system state or measurements. One general drawback of these methods is the inability of detecting anomalies that fit the historical distribution of the data [122]. Much attention has been drawn to the problem of detecting FDI attacks, especially when attackers are able to construct undetectable attacks that bypass the BDD within the power system state estimators [124]. Several previous works have pointed to the consequences and implications of FDI on the grid [125] . The authors in [126] reviewed the theoretical basis of FDI attacks and their defense strategies in modern systems. In [127], graphical methods are used to detect attacks by using tree-pruning based approximation algorithm. The authors in [122] proposed a statistical method based on tracking the dynamics of measurements and using probability distributions derived from measurements variation to detect the attacks. Another approach for anomaly detection is based on complementing bad data detection methods with independent data such as historical and forecast data to detect data anomalies [128].

2.5 Machine learning for Cyber-Physical Security

Driven by the huge amount of currently available data in many fields, the applicability of Machine Learning (ML) techniques has been rising in popularity. ML techniques have been used to model complex systems with high accuracy in different fields, including power systems, with a wide range of applications. The ability to extract features from raw data is an extremely valuable asset and alternative to tackle previously extremely demanding computation problems. Many recent advancements in power systems researchers have been attributed to the usage of AI and ML techniques. Deep neural networks have been used in energy dis-aggregation to estimate each appliance consumption from the overall home's electrical consumption [129]. Also, adaptive neural networks has been used to detect FDI attacks on the sensors of an unmanned aerial vehicles [130]. In [131], Support Vector Machines (SVM) have been implemented to detect stealthy attacks in the smart grid. Authors in [132] utilized ML in order to detect deception assaults in communications networks. The approach employs SVM to learn the decision boundaries that separates compromised from non-compromised data points. In [133], authors complemented an interval SE based defense mechanism with deep learning to improve load forecasting. The distinctive addition in [133] is the independence of the ML model on the system topology and attack type. Stealthy FDI attacks, which cannot be detected using conventional BDD methods, were detected using two ML approaches in [134]. Historical data were projected to low-dimensional space to prove the feasibility of attacks data separation. Both supervised and unsupervised methods were applied to detect the stealthy attacks. Wang *et al.* employed a Margin Setting Algorithm (MSA) to mitigate FDI attacks [135]. The experimental results were compared to other ML techniques such as SVM and Artificial Neural Networks (ANN). In order to identify any hacked meters in the smart grid, the authors in [136] proposed an AI technique that protects the power systems against FDI attacks. The AI technique detected the attacks vectors on the condition that the cumulative injection error surpassed a pre-specified threshold. Wilson *et al.* proposed a stacked auto-encoder framework against SCADA attacks [137]. The approach enhanced automation of unsupervised machine learning models, which reduces human intervention in defining the models.

2.6 Conclusion

This chapter presented an overview of the PDS and the main features that characterize radial systems. The critical operations such as DSSE and DSOPF were introduced to

build the model in the subsequent chapters. Unlike the conventionally used approaches to analyze different attacks scenarios, the BCSE based DSSE and the SDP based DSOPF model accurately the radial distribution systems, and includes the unbalanced 3-phases of the system. A general overview was of the cyber-physical threats was also presented, with a specific focus on the FDI attacks. Finally, different ML approaches were reviewed to demonstrate the potential of these techniques to tackle detection problems of cyber-physical attacks.

Chapter 3

False Data Injection On Optimal Power Flow

The critical problem of cyber-physical security presents itself in many forms for the Power Distribution Systems. In this chapter a special focus is given to the stealthy False Data Injection attacks, which cannot be detected by traditional Bad Data Detection techniques. The attack vectors are injected to corrupt the measurements, which leads to deceiving states perceived by the system operators. Optimal attacks strategy is formulated based on incorporating the attack vectors into the Distribution Systems Optimal Power Flow. The effects of the attacks are assessed based on the increase in the objective function, voltage profile deviation, and the changes in the shunt capacitors reactive power injection.

3.1 False Data Injection (FDI)

The FDI attacks are among the well known cyber-physical threats against smart grids. Liu *et al.* [109] showed that attackers, equipped with a prior knowledge of the network topology, are able to manipulate the measurements by inserting attack vectors that are undetected by the residue test of the state estimation techniques. Let $z \in \mathbb{R}^m$ be the original measurement vector than can pass the bad measurement detection, where m is the total number of measurements. For an attack vector $a \in \mathbb{R}^m$, the compromised measurement data is presented as:

$$z_a = z + a \tag{3.1}$$

If a is constructed as a linear combination of the column vectors of H (i.e., $a = Hc$), then z_a can pass the bad data detection. The obtained state variables estimated from

compromised data z_a are referred to as $\hat{x}_{comp}$, and can be represented as $\hat{x}_{comp} = \hat{x} + c$, where c is a non-zero vector $\in \mathbb{R}^n$. Since original measurements z can pass the bad data detection, then

$$\begin{aligned} \|z_a - H\hat{x}_{comp}\| &= \|z + a - H(\hat{x} + c)\| \\ &= \|z - H\hat{x} + (a - Hc)\| \\ &= \|z - H\hat{x}\| \leq \tau \end{aligned} \tag{3.2}$$

Thus, the L_2-norm of z_a, which is less than threshold τ can bypass the BDD. The results from [109] have triggered an important alarm to the necessity of revisiting the techniques used to defend against possible cyber-physical attacks in the power networks, as conventional SE approaches might fail to detect stealthy FDI that are constructed with prior knowledge of the network topology. The work presented in [109] was based on the DC power flow model, which is a lineraized version of the AC power flow. However the FDI attack strategy is valid for the nonlinear AC version and is given by[18]:

$$a = h(\hat{x} + c) - h(\hat{x}) \tag{3.3}$$

where a is the structured attack vector to be added to the measurements. The attacker is able alter the states by intelligently manipulating specific measurements while keeping the residue norm unchanged in order not to raise the BDD alarm as follows:

$$\begin{aligned} \|z_a - h(\hat{x}_{comp})\| &= \|z + a - h(\hat{x} + c)\| \\ &= \|z - h(\hat{x})\| \leq \tau \end{aligned} \tag{3.4}$$

Based on (3.4), the attacker must consider the output value of the measurement function $h(x)$ to successfully launch a stealthy attack. The vector c corresponds to the alteration in the state variables from the attack vector α on the measurements. The attacker is constrained by the following conditions in order to successfully launch a hidden attack:

1. The attack vector c has non-zero entries only for load buses,
2. The attacks are launched on buses which are not constant current loads, as it can be easily verified if the current values are altered
3. Injection of non-load buses cannot be altered . To achieve a load distribution attack (i.e., where the net change in the system remains zero), the attacker will consider the nodal balance for each non-load bus j [18]:

$$P_{inj_j} = V_j \sum_n V_n(G_{jn}\cos(\theta_{jn}) + B_{jn}\sin(\theta_{ji})) \tag{3.5}$$

$$Q_{inj_j} = V_j \sum_n V_n (G_{jn} \sin(\theta_{jn}) - B_{jn} \cos(\theta_{ji}) \tag{3.6}$$

where $G_{jn} + B_{jn}$ is the (j, n) entry of the complex bus admittance matrix and $\theta_{jn} = \theta_j - \theta_n$ is the angle difference between bus j and n. The attacker must constrain the attack vectors to these conditions in order to keep the attack undetected by the BDD and not violate the electrical physical laws of the system.

3.2 Optimal Attacks Strategy

In order to maximize the losses on the system, the adversary, equipped with FDI stealthy formulation, is able to incorporate the attack vectors formulated in the previous section into the DSOPF. The optimal attack formulation is derived through an optimization problem that mimics the features of the original DSOPF that the system operator utilizes. The attack strategy flowchart is shown in Figure 3.1, detailing the work done by the attacker to construct the attack vectors, to be injected in the measurements received by the DSSE process. The first (left) part of the flowchart is shows the steps done by the attacker, while the second (right) part is the normal DSOPF operations run by the PDS operator. For the attacker, the first step is getting access to the measurements sent from different meters and sensors devices such as Remote Terminal Units (RTUs) or PMUs [138, 139]. Second, the adversary gets an estimate of the network by deploying an DSSE to get accurate state estimates. The third step consists of running a modified DSOPF problem, which has similar constraints to the operator's DSOPF, but with a modified objective function, which maximizes the losses of the PDS operator. The derivation of this problem is explained in the next section. After running the optimization problem, the solution point represents the maximum losses of the system given the system parameters and constraints. The arguments of the optimal solution represent the values of the variables that lead to this solution. The gap between the resulting arguments and the arguments from the uncompromised DSOPF represent the values of injection to be added to the measurements, according to the process presented in section 3.1. These vectors can be injected into the measurements data received from the meters without triggering the BDD alarm. Since the vectors are synthesized from the modified DSOPF, they represent the optimal attack vectors to be added to the measurements. The now corrupted measurements are passed to the PDS system operator, as they run the normal DSOPF.

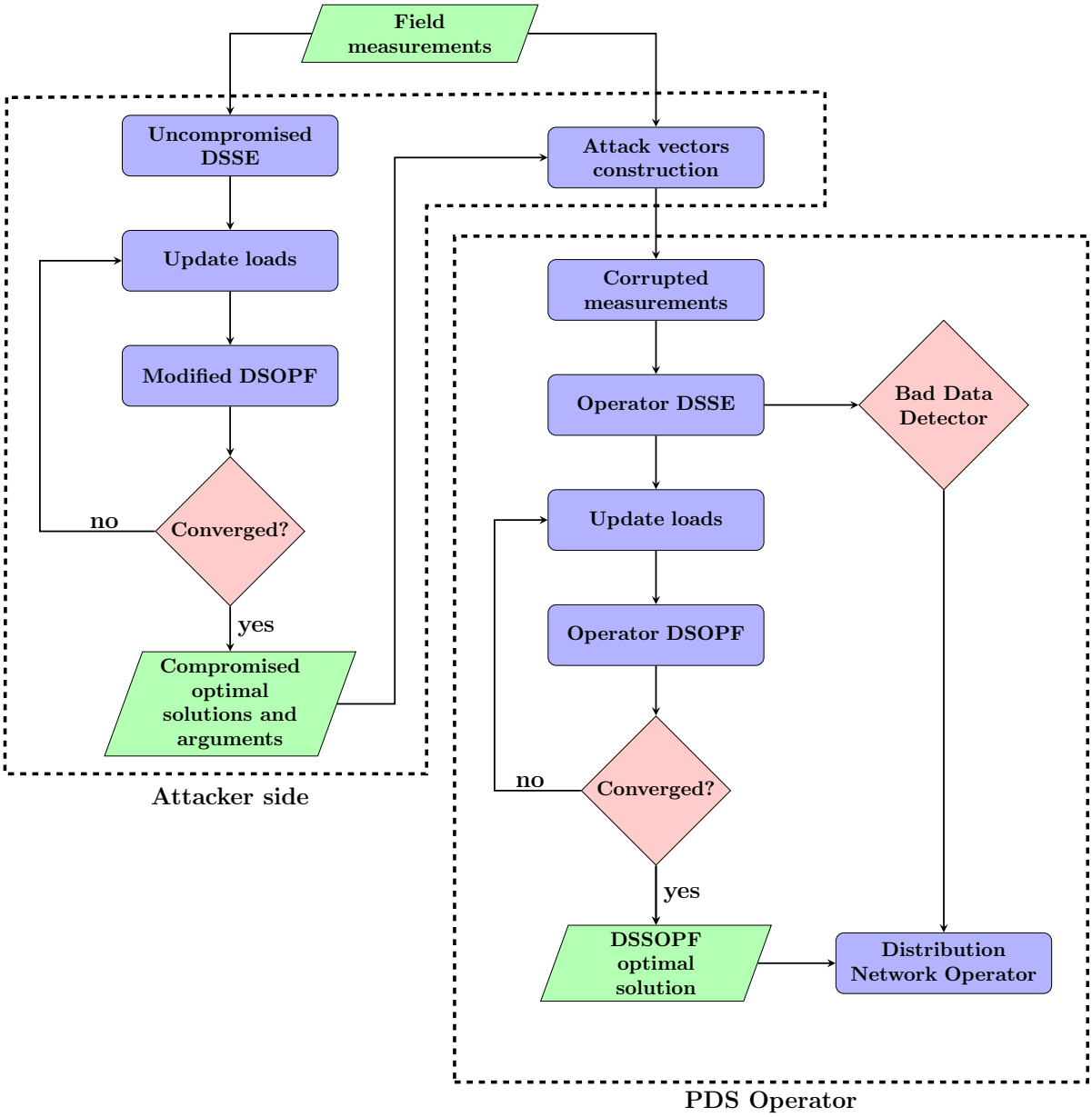

Figure 3.1: Optimal attacks on DSOPF Flow Chart

3.3 Attack Vectors Construction

The core attacks strategy is based on the running a modified DSOPF that resembles the PDS operator optimization problem, but outputs the highest losses for the given optimization problem. In order to achieve this objective, the attacker incorporates the FDI attacks construction strategy as part of the optimization problem constraints. Based on the SDP optimization methodology. The adversary ultimate objective is to manipulate the measurement vector z to change the i^{th} entry in attack vector c by using (3.3), with $c_i = 0$ if the i^{th} state is not changed. The attacker runs the DSOPF with the objective of maximizing the losses, instead of minimizing it, as follows:

$$\text{maximize} \quad \sum_i C_i(s_i) \tag{3.7a}$$

$$\text{subject to} \quad \text{(2.30b),(2.30c),(2.30d),(2.30e) (2.30f),} \tag{3.7b}$$

$$\|diag(z_a - h(\hat{x}_{bad}))\| \leq \tau, \tag{3.7c}$$

$$\underline{s}_{a_{ij}} \leq s_{a_{ij}} \leq \bar{s}_{a_{ij}} \tag{3.7d}$$

where $\underline{s}_{a_{ij}}$, $\bar{s}_{a_{ij}}$ are the lower and upper bounds of power injections after alterations of measurements using (3.3) of pre-specified limits by the attacker, inspired by the AC attacks formulation [18]. Constraint (3.7c) is added to ensure that the altered measurements bypass the BDD according to (3.4). Note that this DSOPF, run by the attacker, is similar to the original problem with a different objective function, and is used to determine the deviation in current variables I_{ij} to be injected for maximum losses in the DSOPF. The affected currents represent the sub-graph of measurements needed to be changed to hide the attack. The choice of the BCSE allows to add the linear measurement function as a convex constraint implicit in constraint (3.7c) as part of the DSOPF problem.

3.4 Attacks Analysis

The case study is based on the IEEE-34 radial bus system. The system loads are modeled based on the exponential load model, and the substation voltage is set at 1.05 p.u. It is assumed that measurements taken in the system are active and reactive power flows on all branches. Lower and upper bounds of voltage are defined at 0.9 and 1.1 p.u. Shunt capacitors, C_1 and C_2 are placed at nodes 844 and 848, respectively, as the original system configuration in [61]. No pseudo measurements are considered during the analysis and attacks construction. The SDP convex optimization problem of the DSOPF problem is

implemented using the CVX toolbox [140]. First, the attack vectors are constructed as per the previous section, and added to the measurements of each phase. Figure 3.2 and Figure 3.3 depict the DSSE normalized residuals without and with attacks for the branch currents magnitudes and phases vectors of the three phases. 300 scenarios are generated to validate that the norm does not trigger the BDD alarm. Second, the voltage profile

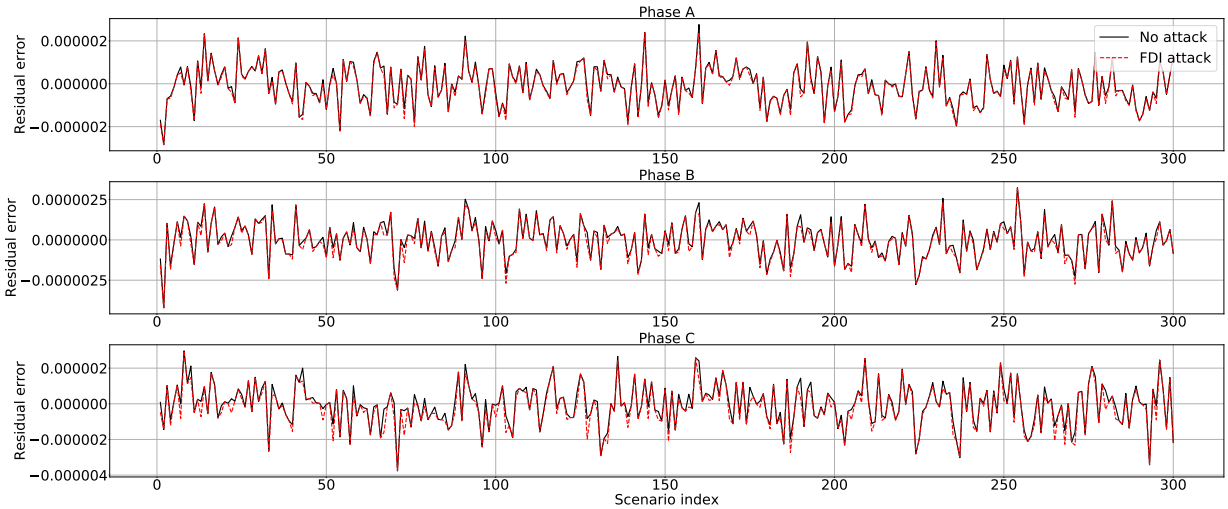

Figure 3.2: Norm of normalized residual error of Branch current magnitudes vectors of each phase

is analyzed after the attack vectors are injected to the measurements. Figure 3.4 shows the voltage profile of the three phases for the system nodes resulting from the original and compromised DSOPF. The voltage nodes remained within permissible range, however the losses increase from 187.07 KW obtained form the original DSOPF to 218.43 KW, an increase of approximately 17% in power losses. The voltage deviations are a direct result from the FDI attacks, but no there is no formal mechanism of detecting such attacks from observing the voltage profile. In addition, reactive power injection from the shunt capacitors C_1 and C_2 increased from 140 KVAR and 150 KVAR to 180 KVAR and 160 KVAR respectively. Thus, it is shown that the stealthy attacks kept the voltage profile within the regulation limits, and no physical damage is observed. However, the effects of the attacks is evident in the increase of both the power losses and the reactive power injection of the shunt capacitors.

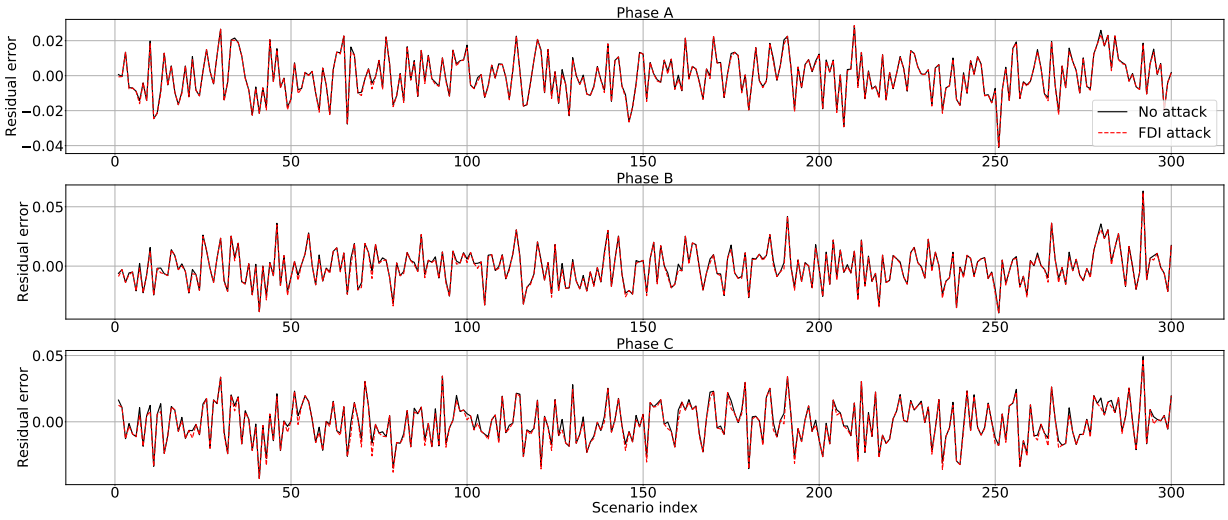

Figure 3.3: Norm of normalized residual error of Branch current phases vectors of each phase

3.4.1 Effects of load types

As PDS loads cannot be always treated as constant power, it is necessary to consider the load type in determining the currents. Figure 3.5 depicts the difference in node voltages due to the same attack for the same conditions for phase A. The loads are modeled based on the exponential load model described in section 2.3. Configuration O is the standard IEEE-34 load configuration [61], which is a mixture of constant impedance, constant current and constant power loads, configuration P is all constant power loads, and configuration Z is all constant impedance loads. It it seen that the constant impedance loads present the highest sensitivity of voltage variations due to the power measurements alterations. This analysis demonstrates that the attack effects are highly dependant on the system configuration and load types. Thus, voltage deviation from measurements manipulation depends on the load type of the attacked node.

3.5 Conclusion

This chapter presented a detailed analysis of the FDI attacks on the IEEE-34 3-phases unbalanced radial distribution system. The stealthy FDI attacks are based on the BCSE, which separates the 3-phases, which allows to target the measurements of each phase

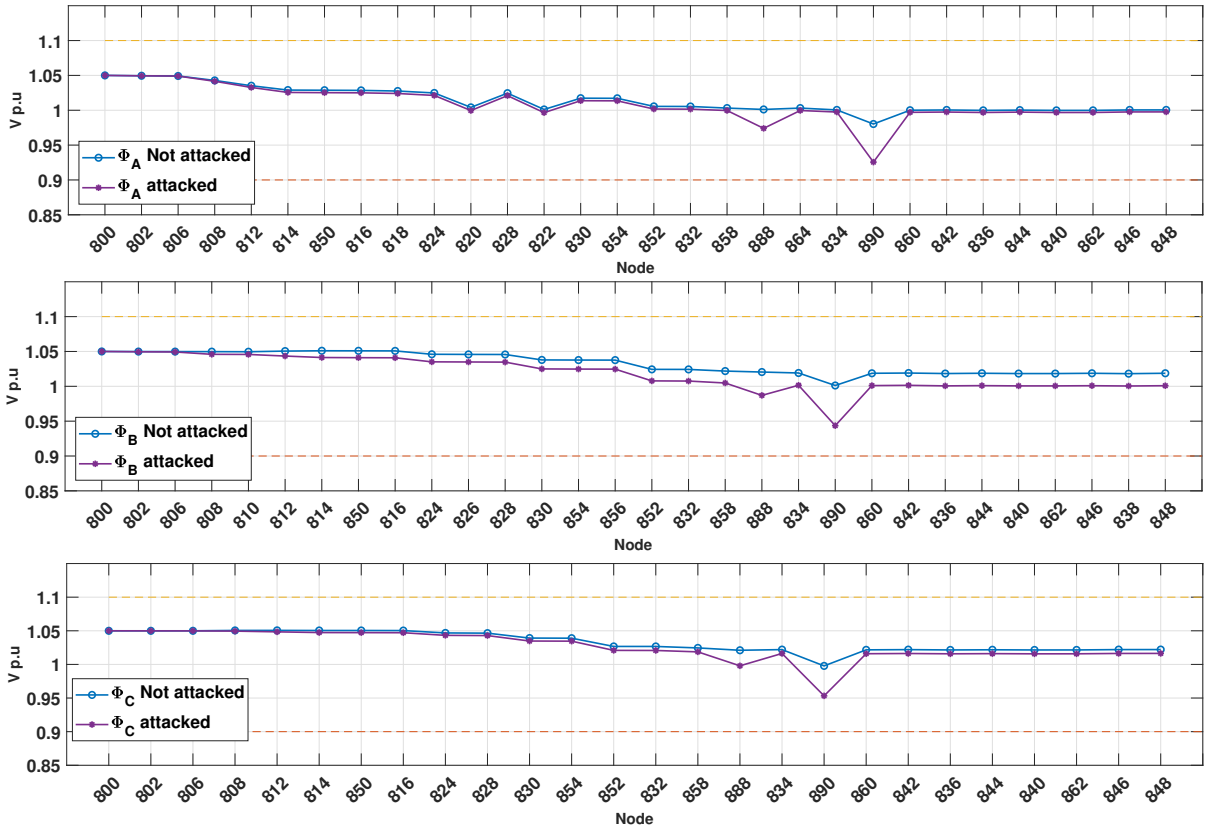

Figure 3.4: Voltage profile of phases A, B, and C of the IEEE-34 Bus system based on the original and compromised DSOPF

individually. A maximum attack strategy is derived to target the DSOPF, which is modeled using the SDP model to accurately represent the OPF problem of radial systems. The attacks strategy is based on an optimization problem that mimics the DSOPF, however with a modified objective function and added constraints to guarantee the stealthiness of the attacks. The attacks compromised the optimal solution of the power losses, by manipulating optimization problem control variables, while keeping the voltage profile within limits. Different load models were considered in the case study to analyze the effect of attacks on each load type.

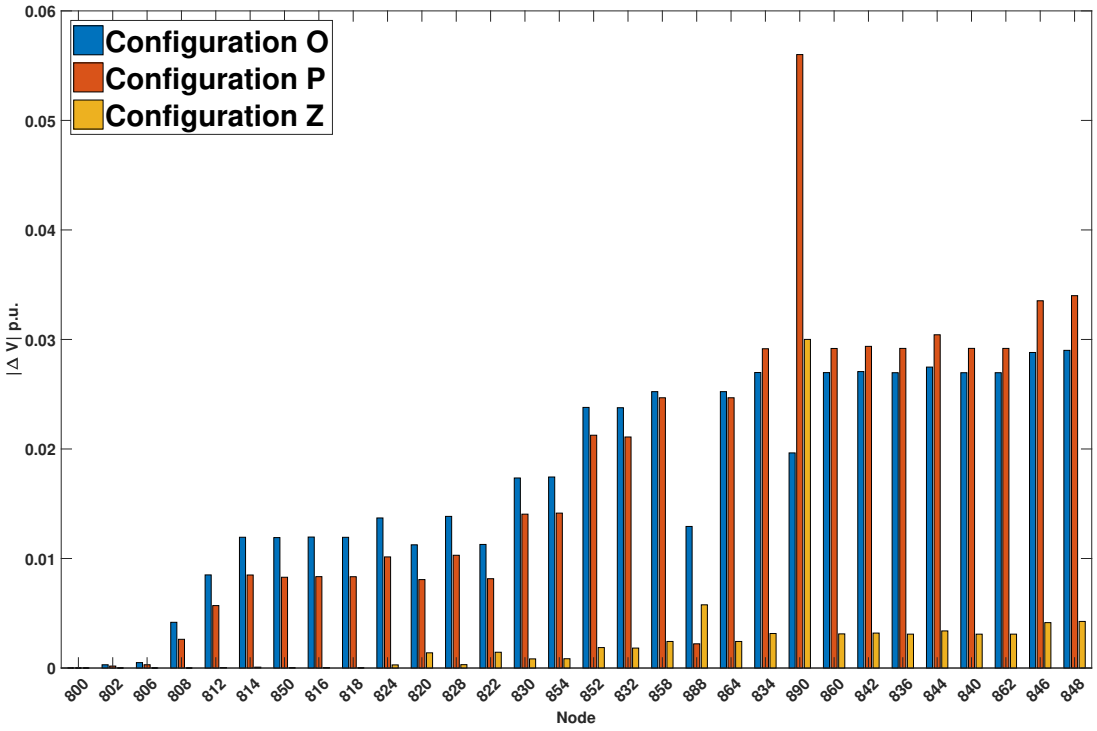

Figure 3.5: Change in voltage nodes (absolute values) due to compromised DSOPF for different system loads configurations.

Chapter 4

Attacks detection using Recurrent Neural Networks

This chapter discusses the usage of machine learning techniques for stealthy attacks detection in the framework of PDS. The objective is to develop a ML model capable of detecting anomalies in the measurements data vectors and flag them as possible FDI attacks. The RNN model is first derived to fit the described problems. Then, the model is trained on real power flow measurements and statistically evaluated on unseen testing data. The work in this chapter has been published in [141].

4.1 Recurrent Neural Networks

Unlike regular Artificial Neural Networks (ANN) which assume inputs (outputs) are independent from each other, RNN are a special type of neural networks, that make use of sequential information to predict the output [142]. Sequential data might contain temporal correlation between inputs at time t and inputs at time $t-1, t-2, \cdots$. By using information of previously calculated outputs, RNN is capable of constructing a memory, which is to be used in computing the output. RNN can be utilized as a sequence classifier. For an observation sequence $\in \mathbb{R}^l$, $\{\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_l}\}$ and corresponding labels $\in \mathbb{R}^l$, $\{y_1, y_2, ..., y_l\}$, the objective is develop a learning function that maps (labels) the feature to its corresponding label, i.e., $f : \mathbf{x} \rightarrow y$. RNN models dynamic systems, by sending feedback signals, so that subsequent outputs depend on computed output. This can be mathematically modeled as [1]:

$$\mathbf{h}_t = f(\mathbf{h}_{t-1}, \mathbf{x}_t) \tag{4.1}$$

where $\mathbf{h}_t$ is the hidden state, $\mathbf{h}_{t-1}$ is the previous hidden state, and $\mathbf{x}_t$ is the current feature observed, and f is a nonlinear mapping function. Equation (4.1) captures the essence of RNN and what differentiates it from regular neural networks. The hidden state $\mathbf{h}_t$ is used as a memory to capture sequence information. Figure 4.1 shows the unfolding of RNN in time of the computation. $\mathbf{x}_t$ denotes the input at time t, while the hidden state $\mathbf{h}_t$ represents the memory of the network, and it depends on the previous hidden state and current input. The output of the network at time t is z_t. The memory concept of the RNN gives it great advantages in storing information about the time sequence.

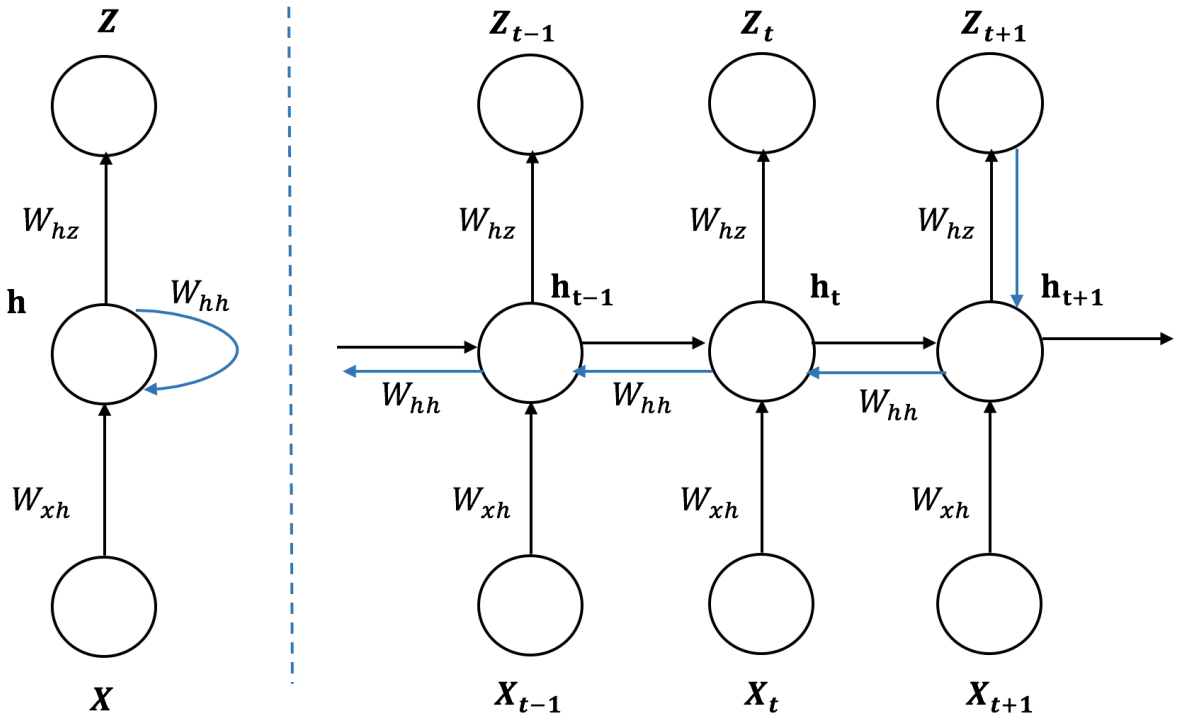

Figure 4.1: Left: Recursive Description of RNN. Right: Corresponding Extended RNN model for time sequence [1]

4.2 Backpropagation Through Time (BPTT)

Conventional Neural Networks use the Backpropagation Learning Algorithm (BPL) to train the network by adjusting the weights of the network. The BPL is based on the gradient descent technique, used to minimize the network cumulative error. The Backpropagation Through Time (BPTT) Algorithm is an extension of the BPL over a time sequence where the gradient at each output depends on calculations of current as well as previous steps. BPTT has been developed by many authors independently as in [143] and [144]. Derivation of the BPTT is summarized as follows [1]: Starting with the RNN model described in Figure 4.1, parameters are assumed to be the same across the whole sequence in each time step. This assumption is used to simplify the gradient calculations. At time t we have,

$$\mathbf{h_t} = \tanh(W_{hh}\mathbf{h_{t-1}} + W_{xh}\mathbf{x_t} + \mathbf{b_h}) \tag{4.2}$$

$$z_t = softmax(W_{hz}\mathbf{h_t} + \mathbf{b_z}) \tag{4.3}$$

where $b_\mathbf{h}$ and b_z are the bias terms for the hidden state and prediction at time step t. The maximum likelihood is used to estimate the model parameters. The minimization of objective function of negative log likelihood is

$$\mathcal{L}(\mathbf{x}, y) = -\sum_t y_t \log z_t \tag{4.4}$$

where z_t is the prediction at time step t. The notation $\mathcal{L}$ will be used as objective function for simplicity. The notation $\mathcal{L}(t)$ indicates the output at time t while $\mathcal{L}(t+1)$ indicates the output at time $t+1$. The derivative of equation (4.4) with respect to z_t is

$$\frac{\partial \mathcal{L}}{\partial z_t} = -\sum_t y_t \frac{\partial log z_t}{\partial \mathbf{h}_t} = -\sum_t y_t \frac{1}{z_t}\frac{\partial z_t}{\partial \mathbf{h}_t} \tag{4.5}$$

Applying the chain rule and by deriving the gradient of the $softmax$ function from (4.3), we get

$$\frac{\partial \mathcal{L}}{\partial z_t} = -(y_t - z_t) \tag{4.6}$$

The weight W_{hz} between the hidden state $\mathbf{h}$ and output z is the same across all time sequence. Therefore it can be differentiated at each time step and summed as follows:

$$\frac{\partial \mathcal{L}}{\partial W_{hz}} = \sum_t \frac{\partial \mathcal{L}}{\partial z_t}\frac{\partial z_t}{\partial W_{hz}} \tag{4.7}$$

The gradient with respect to a bias unit b_z is obtained similarly as:

$$\frac{\partial \mathcal{L}}{\partial b_z} = \sum_t \frac{\partial \mathcal{L}}{\partial z_t} \frac{\partial z_t}{\partial b_z} \tag{4.8}$$

Considering the time step $t \rightarrow t+1$, the gradient is derived with respect to the weight W_{hh} as

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{hh}} = \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \mathbf{h}_{t+1}} \frac{\partial \mathbf{h}_{t+1}}{\partial W_{hh}} \tag{4.9}$$

The above equation only considers the time step $t \rightarrow t+1$. As the RNN model uses previous state for subsequent state calculation, the hidden state $\mathbf{h}_{t+1}$ depends partially on hidden state $\mathbf{h}_t$. Similar to W_{hz}, the weight W_{hh} is shared across the whole time sequence. Therefore we get

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{hh}} = \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \mathbf{h}_{t+1}} \frac{\partial \mathbf{h}_{t+1}}{\partial \mathbf{h}_t} \frac{\partial \mathbf{h}_t}{\partial W_{hh}} \tag{4.10}$$

Aggregating gradients with respect to W_{hh} over the whole sequence and using the BPTT from time t to 0

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{hh}} = \sum_t \sum_{k=1}^{t+1} \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \mathbf{h}_{t+1}} \frac{\partial \mathbf{h}_{t+1}}{\partial \mathbf{h}_k} \frac{\partial \mathbf{h}_k}{\partial W_{hh}} \tag{4.11}$$

The same process applied in Equation (4.7)-(4.11) is also applied on the weights W_{xh}, by taking the gradient with respect to W_{xh} over the whole sequence to obtain

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{xh}} = \sum_t \sum_{k=1}^{t+1} \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \mathbf{h}_{t+1}} \frac{\partial \mathbf{h}_{t+1}}{\partial \mathbf{h}_k} \frac{\partial \mathbf{h}_k}{\partial W_{xh}} \tag{4.12}$$

It is worth mentioning that the same advantage feature of RNN, of having an internal memory, represents a major challenge in some applications such as text prediction, namely the problem of vanishing or exploding gradients. This however is not a problem in the application of anomaly detection, as a large memory is not required. When propagating over a long sequence, that gradient value will vanish after a few time steps, as it shrinks layer after layer. Thus, the far away states do not contribute significantly to the gradient computing. On the other side of the problem spectrum, gradient explosion results from large value in matrix multiplication of while computing the gradient over the sequence.

4.3 RNN Parameters Tuning

Based on the RNN theory, an algorithm is developed to detect the FDI attacks. After generating the flow measurements, adding the attack vectors, and taking a subset of the data, the first step is to find the optimal parameters for the RNN. There are three main parameters which add recurrent time delayed connections to the RNN [145]:

1. Input delays $dIn \in [0, 1, 2, ...]$: This allows the output to not only depend on current input, but also on previous inputs. For regular neural networks, $dIn = [0]$. The benefit of the Input delay is to use the temporal correlation between successive inputs to predict the next output.

2. Internal delays $dInternal \in [0, 1, 2, ...]$: This allows the current internal states to depend on previous $dInternal$ internal states, and specifies how many previous internal states to be used. For regular neural networks, $dInternal = [0]$.

3. Output delays $dOut \in [0, 1, 2, ...]$: This determines how many previous output states are used to predict current output. For regular neural networks, $dOut = [0]$. This parameter controls the recurrent behavior of using current output for subsequent outputs. Previous outputs are particularly important in applications where the predicted output heavily depends on previous outputs.

The optimal set of parameters that achieves least error has been determined by training the network several times using the BPTT algorithm. After finding the optimal parameters, the network is used to predict the attacks in the test data. As the output of the network is not constrained to a binary output, a threshold is used to determine the classification of output either 1 (indicating the presence of attack vector), and 0 (indicating normal measurement vector).

4.4 RNN Model Evaluation

After building the RNN model as per the previous section, it is trained and tested on actual measurements to detect FDI attacks injected into the data stream. First, the AC power flow model is used to generate the power flow measurements for the IEEE-34 distribution bus system. The actual load data is obtained over a period of five years from the Ontario Independent Electricity System Operator (IESO) [2]. The data is available with an hourly resolution and depicted in Figure 4.2, and is shown as 43800 data points. To better

model a practical the attacks scenarios, the resolution of the data is increased to 5-minutes resolution by interpolating the hourly data points. The attack vectors are constructed

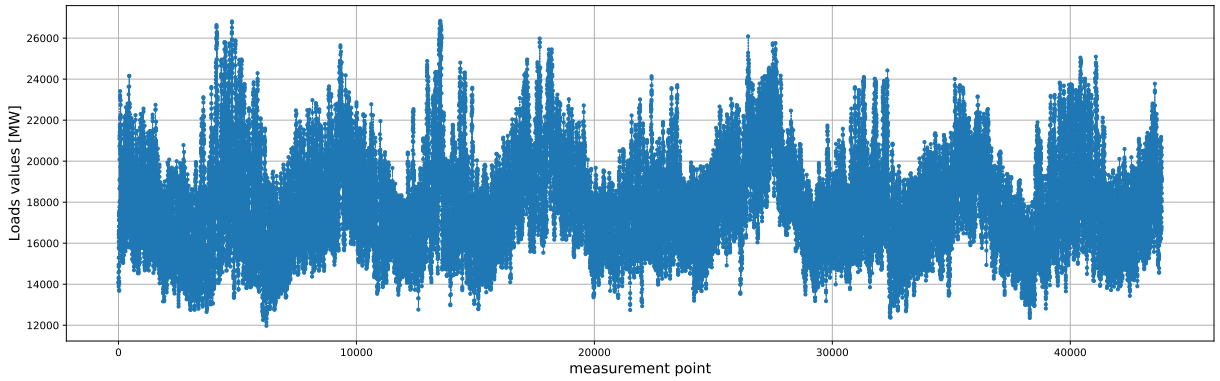

Figure 4.2: Five years power loads [2]

according to the procedure prescribed in section 3, which ensures that it will bypass the traditional BDD within the DSSE process. A total number of 100 attack instances were randomly injected in the measurements. Each attack instance was contained a random number between 6-12 of attack vectors. It is assumed that the attacker will not launch less than 6 attack vectors to induce a noticeable effect in the measurement. Each attack vector added to the flow measurements was per Equation (3.1). The measurements error is modeled as a Gaussian noise vector with a sound to noise ratio (SNR) equal to 12. The IESO data is divided into training data and testing data, representing roughly 60% (three years of data) and 40% (two years of data), respectively. Attacks are added to the measurements in the form of instances. For each attack instance, random attack vectors between six and twelve vectors are added. It was assumed that the adversary would not corrupt less than six attack vectors to achieve any practical damage through the launched attack. Attack instances are randomly distributed along all the training data as well as the testing data. All simulations were implemented in MATLAB environment. The RNN is trained for 100 iterations and, with one iteration means passing over all input data points. Figure 4.3 shows the decrease of the log of the error function, based on Equation (4.4) over the 100 iterations. This indicates the improvement of the classifier to correctly predict the state of the input whether a normal or compromised measurement value. For the data set and system under consideration, after adjusting the RNN parameters, it has been found that the optimal number of delay input is $dIn = 1$, $dInternal = 1$, and $dOut = 5$. This is due to the characteristics of data presented to the network. In the case of power flow measurements, where the load does not witness a sudden decrease or increase,

there should be a correlation between the current output and previous inputs (power flow measurements). For the data set in use, increasing $dOut > 5$ causes gradients explosion and does not yield better results. The stream of measurements over five years with increased

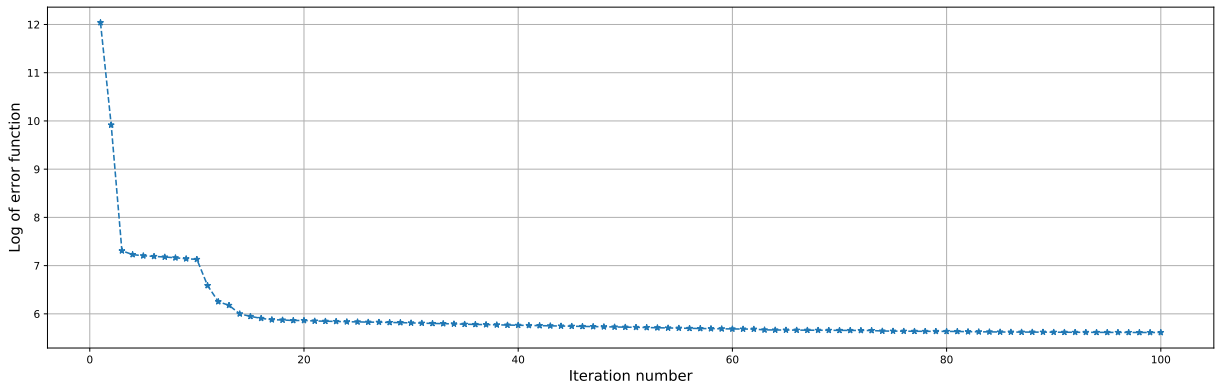

Figure 4.3: Log of the RNN error function

resolution has 262800 data points, with 60%(315360) data points for training and cross-validation, and 40%(210240) data points for testing. The measurements points were labeled either 0 or 1: state 0 meant no attack, and state 1 meant attack. Accordingly, the RNN model worked as a binary classifier that predicted the state of the measurements: either 0 or 1. Figure 4.4 shows the RNN predictions over the testing data points, with the zoomed-in portion showing individual data points detected as compromised. The zoomed-in portion affirms the value of historical data to identify attack vectors. Measurement points 80568 through 80579 were compromised with the FDI attack vectors, and therefore have the attack state of 1. However, measurement points 80568 and 80569 were not detected, and the predicted state of the RNN is 0. After only two attack points, the RNN was able to correctly flag the subsequent ten points as attacks, and predicted a state 1 for the measurements. In order to formally measure the effectiveness of the classification model, statistical analysis is performed on the output predictions. A commonly used evaluation approach is based on the confusion matrix. It is based on the count of correct prediction of each class in the tackled problem. The confusion matrix shown in Table 4.1 breaks down the four different categories (possibilities) of a predicted value for a given actual value The actual values represent the correct label (ground truth), while predicted values represent the output label (prediction) of the classifier. The four categories are defined as follows:

- **True Positive:** Actual value is positive and prediction is positive
- **False Positive:** Actual value is negative and prediction is positive

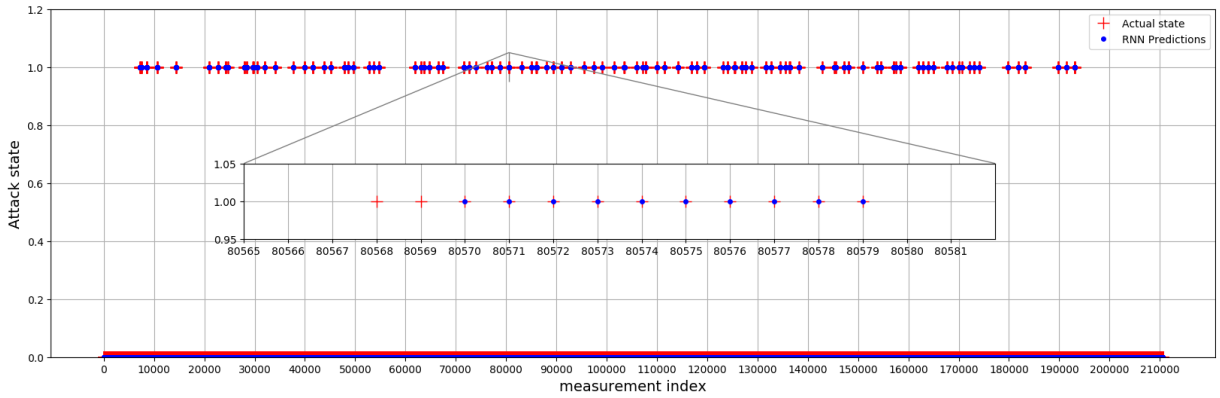

Figure 4.4: RNN Predictions for FDI attacks on IEEE-34 bus

Table 4.1: Confusion matrix

		Actual Values	
		Positive (1)	Negative (0)
Predicted Values	Positive (1)	True Positive (TP)	False Positive (FP)
	Negative (0)	False Negative (FN)	True Negative (TN)

- **False negative:** Actual value is positive and prediction is negative
- **True negative:** Actual value is negative and prediction is negative

Based on counts of each categories, specific evaluation is performed by the following metrics:

- **Accuracy** is considered the basic performance measure, as it measures the prediction of positive and negative instances. In this case, the accuracy represents the ability to differentiate between the attack state (positive) and non-attack state (negative). Mathematically, accuracy is represented by

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \tag{4.13}$$

- **Sensitivity** measures the ratio of correctly positive predictions to the sum of True Positive and False Negative. Sensitivity is also called True Positive Rate (TPR) or Recall. In this case, the sensitivity measures the proportion of correctly predicted attack states (positive) to all (actual) attack states. Mathematically, sensitivity is represented by:

$$Sensitivity = \frac{TP}{TP + FN} \tag{4.14}$$

- **Specificity** measures the ratio of correctly negative predictions to the sum of True Negative and False Positive. The False Positive Rate (FPR) is measured as (1 - Specificity). In this case, specificity measures the proportion of correctly predicted non-attack states (negative) to all (actual) non-attack states. Mathematically, specificity is represented by:

$$Specificity = \frac{TN}{TN + FP} \tag{4.15}$$

- **Precision** measures the ratio of True Positive to the sum of all positive instances. In this case, precision indicates the ration of correct predictions of attack states (positive), to all predictions of attack states (positive). Mathematically, precision is represented by:

$$Precision = \frac{TP}{TP + FP} \tag{4.16}$$

The RNN has been able to detect every attack instance, where an attack instance consisted of a random number of consecutive attack vectors. In addition, the RNN has very good indications of all statistical performances for attack vectors as shown in Table 4.2. All 100 attack instances have been detected correctly, and no attack instance has been flagged outside an attack instance, and, overall, only 20 attack vectors were not detected by the model. These FP vectors were usually an additional point (or two) at the attack end, that were classified as attack vectors. The 167 FN vectors represent the lagging of the RNN to flag an attack. The mean delay is 1.67 vector, and ranged between zero (no delay) and two attack vectors (maximum delay). The results therefore indicate that this model will be effective in the case that the attack instance is compromised of more than two attack vectors. In the attack detection model, the accuracy and sensitivity are the most important indices. The high accuracy is the first good indicator of the RNN model. The sensitivity is not as high as the other metric, due to the 167 missed attack vector. However, since these vectors represented a delay in response, and all other vectors in the same attack instance were detected, it is not a major performance issue.

Another statistical important indicator is the the Receiver ROC curve, depicted in Figure 4.5. The ROC illustrates the diagnostic ability of the binary classifier and is a plot of the (TPR) against the (FPR), and is compared to the curve of a random classifier (50% accuracy). The random classifier has an area of 0.5, while the RNN classifier has an area of 0.99, which approaches the prefect classifier area of 1.

Table 4.2: Performance Table for RNN FDI attacks detection model on the IEEE 34-Bus power flow measurements

Criteria	**Score**
# Attack Instances	100
# Detected Instances	100
# Attack Vectors	1015
# Detected Vectors	868
True Positive (TP)	848
False Positive (FP)	20
True Negative (TN)	209493
False Negative (FN)	167
Accuracy	99.91%
Sensitivity	83.55%
Specificity	99.96%
Precision	97.72%

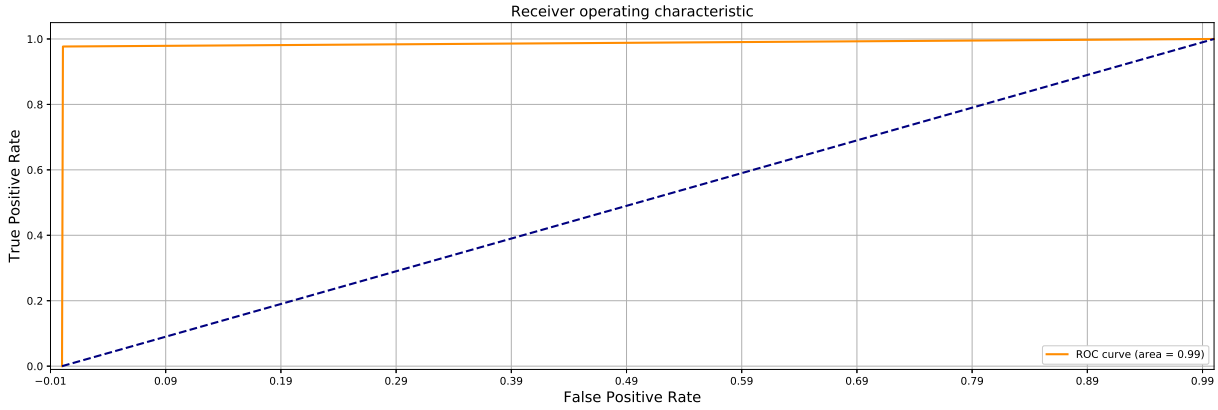

Figure 4.5: ROC curve

4.5 Conclusion

This chapter proposed the usage of the RNN to detect the stealthy attacks that otherwise bypass the conventional BDD techniques. The RNN model constructed a memory by considering multiple time steps when fitting the weights of the minimization algorithm. By analyzing the temporal correlation of inputs and outputs, the RNN was able to detect the attacks in the measurements data in a fast and accurate manner. The model was tested

using real-world data over the span of five years, and the performance of the model was evaluated using the confusion matrix statistical indices. With overall very good performance, the RNN was able to detect all attack instances and with a maximum delay of two attack vectors in any given attack instance.

Chapter 5

Conclusion

5.1 Summary

The FDI attacks on distribution level systems have been investigated. The studies were based on a detailed, 3-phases unbalanced radial system, which included VVC devices. The objective of the research was twofold: Investigating the optimal stealthy attack strategy from the attacker perspective, and proposing a detection model to identify these attacks using a machine learning technique. First, a detailed model was developed to analyze impact of the stealthy attacks on the DSSE and DSOPF. By utilizing the BCSE for the DSSE, the model analyzed the effects of attacks on each phase separately. The attacks were formulated based on a optimization problem that is similar in structure to the DSOPF, however aims to oppose the objective function of the system operator. Given the nature of the considered radial distribution system, the DSOPF was based on the SDP relaxation. The effects of attacks were investigated on the voltage profile and the injection of VVC devices. Also, the sensitivity of loads types to the power manipulation were investigated. Second, a ML approach was proposed to tackle the problem of detecting stealthy attacks, which are not detected through conventional BDD methods. The main concept was to analyze multiple measurement points to flag any anomalies in the measurements. Using five years of real-world data, the load profile was used to train a RNN model to detect the stealthy attacks. The method depended on the temporal correlation of the data to identity the FDI attacks vectors.

5.2 Contributions

The main contributions of this thesis can be highlighted as follows:

1. **Optimal FDI attacks strategy on DSOPF**: An optimal FDI attack strategy that targets the DSOPF was derived, based on a 3-phases unbalanced PDS. The attacker aims to maximize the losses of the objective function of the operator's DSOPF, by incorporating the attacks in the constraints of an optimization problem that mimics the behaviour of the operators' DSOPF.
2. **Attacks Detection using RNN**: The RNN was applied as a machine learning technique to analyze the stream of power flow measurements and detect any anomaly in the data. The mechanism facilitated identifying attacks on three-phase unbalanced distribution systems in a fast and reliable method.

5.3 Future Work

Future research on the cyber-physical security of PDS can include the following:

1. Inclusion and exact modelling of Volt/Var Control devices
2. Integrating DERs in the modelled system and DSOPF problem
3. Investigating effects of FDI on distributed DSSE techniques
4. Considering different attacks models on the PDS

References

[1] G. Chen, "A gentle tutorial of recurrent neural network with error backpropagation," *arXiv preprint arXiv:1610.02583*, 2016.

[2] IESO, "http://www.ieso.ca/power-data/data-directory." [Online]. Available: http://www.ieso.ca/power-data/data-directory

[3] J. P. Lopes, N. Hatziargyriou, J. Mutale, P. Djapic, and N. Jenkins, "Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities," *Electric power systems research*, vol. 77, no. 9, pp. 1189–1203, 2007.

[4] H. E. Farag, E. F. El-Saadany, and R. Seethapathy, "A two ways communication-based distributed control for voltage regulation in smart distribution feeders," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 271–281, 2012.

[5] T. T. Tesfay, "Cybersecurity solutions for active power distribution networks," EPFL, Tech. Rep., 2017.

[6] C. Abbey, D. Cornforth, N. Hatziargyriou, K. Hirose, A. Kwasinski, E. Kyriakides, G. Platt, L. Reyes, and S. Suryanarayanan, "Powering through the storm: Microgrids operation for more efficient disaster recovery," *IEEE power and energy magazine*, vol. 12, no. 3, pp. 67–76, 2014.

[7] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[8] T. T. Tesfay, J.-P. Hubaux, J.-Y. Le Boudec, and P. Oechslin, "Cyber-secure communication architecture for active power distribution networks," in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*. ACM, 2014, pp. 545–552.

[9] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42–49, 2013.

[10] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE communications surveys & tutorials*, vol. 15, no. 1, pp. 5–20, 2013.

[11] S. Wang, D. Liang, L. Ge, and X. Wang, "Analytical frtu deployment approach for reliability improvement of integrated cyber-physical distribution systems," *IET Generation, Transmission & Distribution*, vol. 10, no. 11, pp. 2631–2639, 2016.

[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys and tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[13] Q. Yang, J. A. Barria, and T. C. Green, "Communication infrastructures for distributed control of power distribution networks," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 2, pp. 316–327, 2011.

[14] A. Keane, L. F. Ochoa, C. L. Borges, G. W. Ault, A. D. Alarcon-Rodriguez, R. A. Currie, F. Pilo, C. Dent, and G. P. Harrison, "State-of-the-art techniques and challenges ahead for distributed generation planning and optimization," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1493–1502, 2013.

[15] D. D. Giustina, M. Pau, P. A. Pegoraro, F. Ponci, and S. Sulis, "Electrical distribution system state estimation: measurement issues and challenges," *IEEE Instrumentation Measurement Magazine*, vol. 17, no. 6, pp. 36–42, December 2014.

[16] A. Primadianto and C. Lu, "A review on distribution system state estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3875–3883, Sep. 2017.

[17] A. Primadianto and C.-N. Lu, "A review on distribution system state estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3875–3883, 2017.

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

[19] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, 2018.

[20] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[21] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*. IEEE, 2011, pp. 2195–2201.

[22] M. A. Azzouz, H. E. Farag, and E. F. El-Saadany, "Real-time fuzzy voltage regulation for distribution networks incorporating high penetration of renewable sources," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1702–1711, 2017.

[23] Q. Yang, M. Li, X. Mu, and J. Wang, "Application of artificial intelligence (ai) in power transformer fault diagnosis," in *2009 International Conference on Artificial Intelligence and Computational Intelligence*, vol. 4, Nov 2009, pp. 442–445.

[24] Y. Tang, Y. Huang, H. Wang, C. Wang, Q. Guo, and W. Yao, "Framework for artificial intelligence analysis in large-scale power grids based on digital simulation," *CSEE Journal of Power and Energy Systems*, vol. 4, no. 4, pp. 459–468, Dec 2018.

[25] A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in internet of things," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 4, pp. 208–218, 2018.

[26] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov 2015.

[27] J. Li, L. Liu, C. Zhao, K. Hamedani, R. Atat, and Y. Yi, "Enabling sustainable cyber physical security systems through neuromorphic computing," *IEEE Transactions on Sustainable Computing*, vol. 3, no. 2, pp. 112–125, April 2018.

[28] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds." *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 446–464, 2017.

[29] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57–64, 2010.

[30] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE power and energy magazine*, vol. 7, no. 2, pp. 52–62, 2009.

[31] R. Walling, R. Saint, R. C. Dugan, J. Burke, and L. A. Kojovic, "Summary of distributed resources impact on power delivery systems," *IEEE Transactions on power delivery*, vol. 23, no. 3, pp. 1636–1644, 2008.

[32] H. E. Farag and E. F. El-Saadany, "A novel cooperative protocol for distributed voltage control in active distribution systems," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1645–1656, 2013.

[33] H. Zhu and H. J. Liu, "Fast local voltage control under limited reactive power: Optimality and stability analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3794–3803, 2016.

[34] S. Ghosh, S. Rahman, and M. Pipattanasomporn, "Distribution voltage regulation through active power curtailment with pv inverters and solar generation forecasts," *IEEE Transactions on Sustainable Energy*, vol. 8, no. 1, pp. 13–22, 2017.

[35] K. E. Antoniadou-Plytaria, I. N. Kouveliotis-Lysikatos, P. S. Georgilakis, and N. D. Hatziargyriou, "Distributed and decentralized voltage control of smart distribution networks: models, methods, and future research," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2999–3008, 2017.

[36] H. J. Liu, W. Shi, and H. Zhu, "Distributed voltage control in distribution networks: Online and robust implementations," *IEEE Transactions on Smart Grid*, 2017.

[37] A. Kulmala, S. Repo, and P. Järventausta, "Coordinated voltage control in distribution networks including several distributed energy resources," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 2010–2020, 2014.

[38] Y.-J. Kim, S.-J. Ahn, P.-I. Hwang, G.-C. Pyo, and S.-I. Moon, "Coordinated control of a DG and voltage control devices using a dynamic programming algorithm," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 42–51, 2013.

[39] C. Ahn and H. Peng, "Decentralized voltage control to minimize distribution power loss of microgrids," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1297–1304, 2013.

[40] N. Yorino, Y. Zoka, M. Watanabe, and T. Kurushima, "An optimal autonomous decentralized control method for voltage control devices by using a multi-agent system," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2225–2233, 2015.

[41] L. Yu, D. Czarkowski, and F. De León, "Optimal distributed voltage regulation for secondary networks with dgs," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 959–967, 2012.

[42] B. Zhang, A. Y. Lam, A. D. Domínguez-García, and D. Tse, "An optimal and distributed method for voltage regulation in power distribution systems," *IEEE Transactions on Power Systems*, vol. 30, no. 4, pp. 1714–1726, 2015.

[43] J. Barr and R. Majumder, "Integration of distributed generation in the volt/var management system for active distribution networks," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 576–586, 2015.

[44] D. Della Giustina, M. Pau, P. A. Pegoraro, F. Ponci, and S. Sulis, "Electrical distribution system state estimation: measurement issues and challenges," *IEEE Instrumentation & Measurement Magazine*, vol. 17, no. 6, pp. 36–42, 2014.

[45] K. Li, "State estimation for power distribution system and measurement impacts," *IEEE Transactions on Power Systems*, vol. 11, no. 2, pp. 911–916, May 1996.

[46] M. E. Baran and A. W. Kelley, "State estimation for real-time monitoring of distribution systems," *IEEE Transactions on Power Systems*, vol. 9, no. 3, pp. 1601–1609, Aug 1994.

[47] J. . Teng, "Using voltage measurements to improve the results of branch-current-based state estimators for distribution systems," *IEE Proceedings - Generation, Transmission and Distribution*, vol. 149, no. 6, pp. 667–672, Nov 2002.

[48] M. E. Baran, J. Jung, and T. E. McDermott, "Including voltage measurements in branch current state estimation for distribution systems," in *2009 IEEE Power Energy Society General Meeting*, July 2009, pp. 1–5.

[49] A. K. Ghosh, D. L. Lubkeman, M. J. Downey, and R. H. Jones, "Distribution circuit state estimation using a probabilistic approach," *IEEE Transactions on Power Systems*, vol. 12, no. 1, pp. 45–51, Feb 1997.

[50] Z. J. Simendic, C. Vladimir, and G. S. Svenda, "In-field verification of the real-time distribution state estimation," in *CIRED 2005 - 18th International Conference and Exhibition on Electricity Distribution*, June 2005, pp. 1–4.

[51] N. Katic, L. Fei, G. Svenda, and Z. Yongji, "Field testing of distribution state estimator," in *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)*, June 2013, pp. 1–4.

[52] J. Wu, Y. He, and N. Jenkins, "A robust state estimator for medium voltage distribution networks," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1008–1016, May 2013.

[53] H. Li, "An improved state estimator in distribution systems," in *2011 IEEE International Conference on Computer Science and Automation Engineering*, vol. 3, June 2011, pp. 30–34.

[54] C. Muscas, M. Pau, P. A. Pegoraro, S. Sulis, F. Ponci, and A. Monti, "Multiarea distribution system state estimation," *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 5, pp. 1140–1148, May 2015.

[55] L. D. A. Garcia and S. Grenard, "Scalable distribution state estimation approach for distribution management systems," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*. IEEE, 2011, pp. 1–6.

[56] S. Sarri, M. Paolone, R. Cherkaoui, A. Borghetti, F. Napolitano, and C. A. Nucci, "State estimation of active distribution networks: comparison between wls and iterated kalman-filter algorithm integrating pmus," in *Proceedings of the 3rd IEEE PES Innovative Smart Grid Technologies Europe (2012 ISGT Europe)*, vol. 1, no. EPFL-CONF-183296. IEEE Power Engineering Society and Technische Universität Berlin, Germany, 2012, pp. 1–8.

[57] M. B. Do Coutto Filho and J. C. S. de Souza, "Forecasting-aided state estimationpart i: Panorama," *IEEE Transactions on Power Systems*, vol. 24, no. 4, pp. 1667–1677, 2009.

[58] E. Manitsas, R. Singh, B. C. Pal, and G. Strbac, "Distribution system state estimation using an artificial neural network approach for pseudo measurement modeling," *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 1888–1896, Nov 2012.

[59] A. Gomez-Exposito and A. Abur, *Power system state estimation: theory and implementation*. CRC press, 2004.

[60] M. E. Baran and A. W. Kelley, "A branch-current-based state estimation method for distribution systems," *IEEE transactions on power systems*, vol. 10, no. 1, pp. 483–491, 1995.

[61] W. H. Kersting, "Radial distribution test feeders," in *Power Engineering Society Winter Meeting, 2001. IEEE*, vol. 2. IEEE, 2001, pp. 908–912.

[62] A. Monticelli, "Fast decoupled state estimator," in *State Estimation in Electric Power Systems*. Springer, 1999, pp. 313–342.

[63] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. John Wiley & Sons, 2012.

[64] J. Carpentier, "Contribution a letude du dispatching economique," *Bulletin de la Societe Francaise des Electriciens*, vol. 3, no. 1, pp. 431–447, 1962.

[65] R. Burchett, H. Happ, and K. Wirgau, "Large scale optimal power flow," *IEEE Transactions on Power Apparatus and Systems*, no. 10, pp. 3722–3732, 1982.

[66] F. Capitanescu and L. Wehenkel, "Improving the statement of the corrective security-constrained optimal power flow problem," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp. 887–889, 2007.

[67] X. Liu and Z. Li, "Revealing the impact of multiple solutions in dcopf on the risk assessment of line cascading failure in opa model," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 4159–4160, 2016.

[68] R. Busam and E. Freitag, *Complex analysis*, 2009.

[69] Y. Wang, N. Zhang, H. Li, J. Yang, and C. Kang, "Linear three-phase power flow for unbalanced active distribution networks with pv nodes," *CSEE Journal of Power and Energy Systems*, vol. 3, no. 3, pp. 321–324, 2017.

[70] H. Yuan, F. Li, Y. Wei, and J. Zhu, "Novel linearized power flow and linearized opf models for active distribution networks with application in distribution lmp," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 438–448, 2018.

[71] M. J. Dolan, E. M. Davidson, I. Kockar, G. W. Ault, and S. D. McArthur, "Distribution power flow management utilizing an online optimal power flow technique," *IEEE Transactions on Power Systems*, vol. 27, no. 2, p. 790, 2012.

[72] S. Frank and S. Rebennack, "An introduction to optimal power flow: Theory, formulation, and examples," *IIE Transactions*, vol. 48, no. 12, pp. 1172–1197, 2016.

[73] M. E. Baran and F. F. Wu, "Optimal capacitor placement on radial distribution systems," *IEEE Transactions on power Delivery*, vol. 4, no. 1, pp. 725–734, 1989.

[74] J. Lavaei and S. H. Low, "Zero duality gap in optimal power flow problem," *IEEE Transactions on Power Systems*, vol. 27, no. 1, p. 92, 2012.

[75] L. Gan and S. H. Low, "Convex relaxations and linear approximation for optimal power flow in multiphase radial networks," in *Power Systems Computation Conference (PSCC), 2014*. IEEE, 2014, pp. 1–9.

[76] L. Gan, N. Li, U. Topcu, and S. Low, "Branch flow model for radial networks: convex relaxation," 2012.

[77] M. Farivar and S. H. Low, "Branch flow model: Relaxations and convexificationpart i," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2554–2564, 2013.

[78] L. Gan, N. Li, U. Topcu, and S. H. Low, "Exact convex relaxation of optimal power flow in tree networks," *arXiv preprint arXiv:1208.4076*, 2012.

[79] S. H. Low, "Convex relaxation of optimal power flowpart i: Formulations and equivalence," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 1, pp. 15–27, 2014.

[80] E. Dall'Anese, H. Zhu, and G. B. Giannakis, "Distributed optimal power flow for smart microgrids." *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1464–1475, 2013.

[81] Z. Wang, D. S. Kirschen, and B. Zhang, "Accurate semidefinite programming models for optimal power flow in distribution systems," *arXiv preprint arXiv:1711.07853*, 2017.

[82] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM review*, vol. 38, no. 1, pp. 49–95, 1996.

[83] T. Van Cutsem and C. Vournas, "Voltage stability analysis of electric power systems," 1998.

[84] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Power and Energy Society General Meeting, 2010 IEEE*. IEEE, 2010, pp. 1–5.

[85] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[86] C. Alcaraz, J. Lopez, and S. Wolthusen, "Ocpp protocol: Security threats and challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017.

[87] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with pvs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2016.

[88] A. Teixeira, G. Dan, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures," in *American Control Conference (ACC), 2014*. IEEE, 2014, pp. 4372–4378.

[89] H. F. Habib, C. R. Lashway, and O. A. Mohammed, "A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency," *IEEE Transactions on Industry Applications*, vol. 54, no. 2, pp. 1194–1207, 2018.

[90] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar pv and ess control systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1330–1339, 2017.

[91] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, and M. Guizani, "Cognitive radio based hierarchical communications infrastructure for smart grid," *IEEE network*, vol. 25, no. 5, 2011.

[92] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, A. D. Domı *et al.*, "Spoofing gps receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 2013.

[93] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure (ami)," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*. IEEE, 2008, pp. 1–5.

[94] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, 2010.

[95] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues," in *Compatibility and Power Electronics (CPE), 2015 9th International Conference on*. IEEE, 2015, pp. 534–538.

[96] D. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *SoutheastCon*. IEEE, 2015, pp. 1–6.

[97] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, "Impact of cyber-security issues on smart grid," in *2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*. IEEE, 2011, pp. 1–7.

[98] K. Bhat, V. Sundarraj, S. Sinha, and A. Kaul, *IEEE Cyber Security for the Smart Grid*, 2013.

[99] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. Al Ali, "Smart grid cyber security: Challenges and solutions," in *International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*. IEEE, 2015, pp. 170–175.

[100] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[101] I. Lim, S. Hong, M. Choi, S. Lee, T. Kim, S. Lee, and B. Ha, "Security protocols against cyber attacks in the distribution automation system," *IEEE Transactions on Power Delivery*, vol. 25, no. 1, pp. 448–455, 2010.

[102] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, July 2013.

[103] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1460–1470, July 2014.

[104] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 104–111, Feb 2015.

[105] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy magazine*, vol. 10, no. 1, pp. 58–66, 2012.

[106] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 1871–1879.

[107] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for iec61850 automated substations," *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2376–2383, 2010.

[108] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in dnp3 controlled scada systems," in *Simulation Conference (WSC), Proceedings of the 2011 Winter*. IEEE, 2011, pp. 2614–2626.

[109] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[110] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, pp. 1–1, 2018.

[111] A. Ayad, M. Khalaf, and E. El-Saadany, "Detection of false data injection attacks in automatic generation control systems considering system nonlinearities," in *2018 IEEE Electrical Power and Energy Conference (EPEC)*, Oct 2018, pp. 1–6.

[112] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec 2011.

[113] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, 2014.

[114] ——, "Using covert topological information for defense against malicious attacks on dc state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1471–1485, 2014.

[115] A. Tarali and A. Abur, "Bad data detection in two-stage state estimation using phasor measurements," in *Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES International Conference and Exhibition on*. IEEE, 2012, pp. 1–8.

[116] A. Majumdar, Y. Agalgaonkar, B. C. Pal, and R. Gottschalg, "Centralized volt-var optimization strategy considering malicious attack on distributed energy resources control," *IEEE Transactions on Sustainable Energy*, 2017.

[117] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "Gridlab-d: An open-source power systems modeling and simulation environment," in *Transmission and distribution conference and exposition, 2008. t&d. IEEE/PES*. IEEE, 2008, pp. 1–5.

[118] J. Wang, L. C. Hui, S. Yiu, E. K. Wang, and J. Fang, "A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities," *Pervasive and Mobile Computing*, vol. 39, pp. 52–64, 2017.

[119] J. Liang, O. Kosut, and L. Sankar, "Cyber attacks on ac state estimation: Unobservability and physical consequences," in *PES General Meeting— Conference & Exposition, 2014 IEEE*. IEEE, 2014, pp. 1–5.

[120] A. Majumdar and B. C. Pal, "Bad data detection in the context of leverage point attacks in modern power networks," *IEEE Transactions on Smart Grid*, 2016.

[121] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2014.

[122] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[123] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Universities Power Engineering Conference (UPEC), 2010 45th International*. IEEE, 2010, pp. 1–6.

[124] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[125] L. Kotut and L. A. Wahsheh, "Survey of cyber security challenges and solutions in smart grids," in *Cybersecurity Symposium (CYBERSEC), 2016*. IEEE, 2016, pp. 32–37.

[126] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, 2017.

[127] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, 2014.

[128] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, 2017.

[129] J. Kelly and W. Knottenbelt, "Neural NILM: Deep neural networks applied to energy disaggregation," in *Proceedings of the 2nd ACM International Conference on Embedded Systems for Energy-Efficient Built Environments*. ACM, 2015, pp. 55–64.

[130] A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, "Detection of fault data injection attack on uav using adaptive neural network," *Procedia computer science*, vol. 95, pp. 193–200, 2016.

[131] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, 2014.

[132] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning," *IEEE Access*, 2018.

[133] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, "Deep learning-based interval state estimation of ac smart grids against sparse cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4766–4778, 2018.

[134] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2017.

[135] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26 022–26 033, 2017.

[136] K. Khanna, B. K. Panigrahi, and A. Joshi, "Ai-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Generation, Transmission & Distribution*, vol. 12, no. 5, pp. 1052–1066, 2017.

[137] D. Wilson, Y. Tang, J. Yan, and Z. Lu, "Deep learning-aided cyber-attack detection in power transmission systems," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5.

[138] A. Majumdar and B. C. Pal, "Bad data detection in the context of leverage point attacks in modern power networks," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 2042–2054, May 2018.

[139] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[140] M. Grant, S. Boyd, and Y. Ye, "Cvx: Matlab software for disciplined convex programming," 2008.

[141] A. Ayad, H. E. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2018, pp. 1–5.

[142] R. J. Williams and D. Zipser, "Gradient-based learning algorithms for recurrent networks and their computational complexity," *Backpropagation: Theory, architectures, and applications*, vol. 1, pp. 433–486, 1995.

[143] ——, "A learning algorithm for continually running fully recurrent neural networks," *Neural computation*, vol. 1, no. 2, pp. 270–280, 1989.

[144] J. A. Hertz, A. S. Krogh, and R. G. Palmer, *Introduction to the theory of neural computation*. Basic Books, 1991, vol. 1.

[145] D. Atabay, "pyrenn: First release. zenodo." [Online]. Available: http://doi.org/10.5281/zenodo.45022

APPENDICES

Appendix A

IEEE 34 Test system

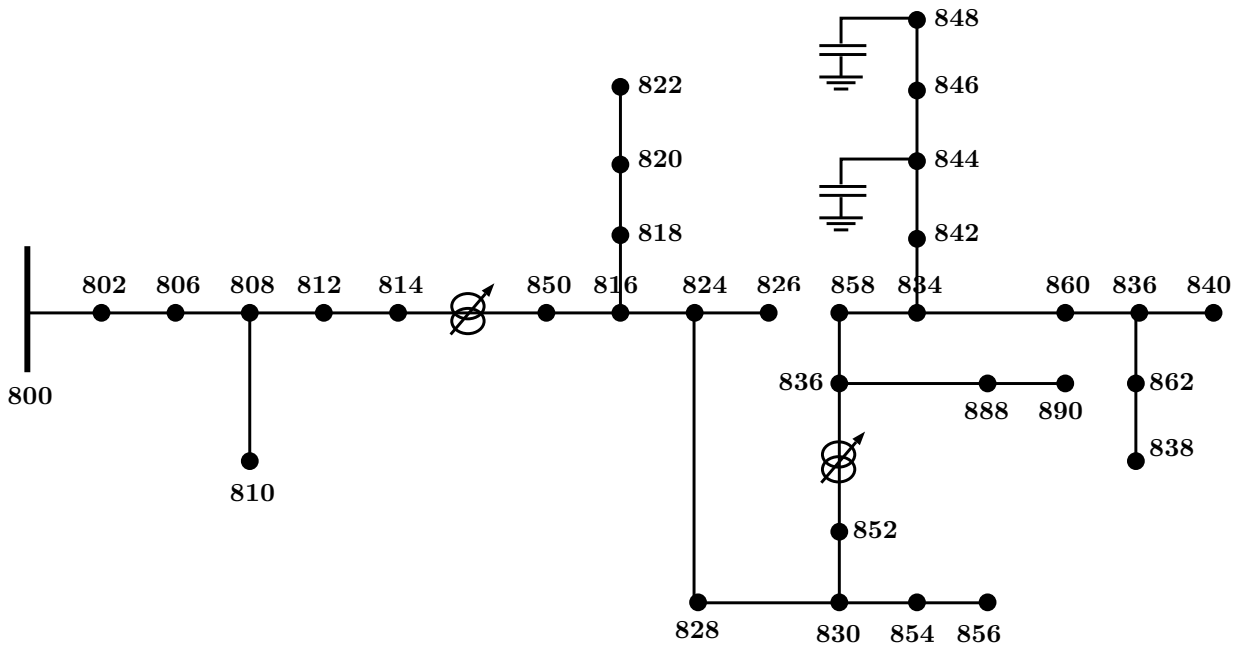

Figure A.1: IEEE-34 Distribution System

Table A.1: Distributed loads

Node A	**Node B**	**Load Model**	**Ph-A kW**	**Ph-A kVAr**	**Ph-B kW**	**Ph-B kVAr**	**Ph-C kW**	**Ph-C kVAr**
802	806	Y-PQ	0	0	30	15	25	14
808	810	Y-I	0	0	16	8	0	0
818	820	Y-Z	34	17	0	0	0	0
820	822	Y-PQ	135	70	0	0	0	0
816	824	D-I	0	0	5	2	0	0
824	826	Y-I	0	0	40	20	0	0
824	828	Y-PQ	0	0	0	0	4	2
828	830	Y-PQ	7	3	0	0	0	0
854	856	Y-PQ	0	0	4	2	0	0
832	858	D-Z	7	3	2	1	6	3
858	864	Y-PQ	2	1	0	0	0	0
858	834	D-PQ	4	2	15	8	13	7
834	860	D-Z	16	8	20	10	110	55
860	836	D-PQ	30	15	10	6	42	22
836	840	D-I	18	9	22	11	0	0
862	838	Y-PQ	0	0	28	14	0	0
842	844	Y-PQ	9	5	0	0	0	0
844	846	Y-PQ	0	0	25	12	20	11
846	848	Y-PQ	0	0	23	11	0	0

Table A.2: Spot Loads

Node	**Load Model**	**Ph-A kW**	**Ph-A kVAr**	**Ph-B kW**	**PhB2 kVAr**	**Ph-C kW**	**Ph-C kVAr**
860	Y-PQ	20	16	20	16	20	16
840	Y-I	9	7	9	7	9	7
844	Y-Z	135	105	135	105	135	105
848	D-PQ	20	16	20	16	20	16
890	D-I	150	75	150	75	150	75
830	D-Z	10	5	10	5	25	10

Table A.3: Line data

Node A	**Node B**	**Length(ft.)**	**Config.**
800	802	2580	300
802	806	1730	300
806	808	32230	300
808	810	5804	303
808	812	37500	300
812	814	29730	300
814	850	10	301
816	818	1710	302
816	824	10210	301
818	820	48150	302
820	822	13740	302
824	826	3030	303
824	828	840	301
828	830	20440	301
830	854	520	301
832	858	4900	301
832	888	0	XFM-1
834	860	2020	301
834	842	280	301
836	840	860	301
836	862	280	301
842	844	1350	301
844	846	3640	301
846	848	530	301
850	816	310	301
852	832	10	301
854	856	23330	303
854	852	36830	301
858	864	1620	302
858	834	5830	301
860	836	2680	301
862	838	4860	304
888	890	10560	300

Table A.4: Impedance configurations

Impedance Configuration	R_{aa} **Ω per mile**	X_{aa} **Ω per mile**	R_{ab} **Ω per mile**	X_{ab} **Ω per mile**	R_{ac} **Ω per mile**	X_{ac} **Ω per mile**	R_{bb} **Ω per mile**	X_{bb} **Ω per mile**	R_{bc} **Ω per mile**	X_{bc} **Ω per mile**	R_{cc} **Ω per mile**	X_{cc} **Ω per mile**
300	1.3368	1.3343	0.2101	0.5779	0.213	0.5015	1.3238	1.3569	0.2066	0.4591	1.3294	1.3471
301	1.93	1.4115	0.2327	0.6442	0.2359	0.5691	1.9157	1.4281	0.2288	0.5238	1.9219	1.4209
302	2.7995	1.4855	0	0	0	0	0	0	0	0	0	0
303	0	0	0	0	0	0	2.7995	1.4855	0	0	0	0

Table A.5: Shunt Capacitors

Node #	**Ph-A kVAr**	**Ph-B kVAr**	**Ph-C kVAr**
844	200	200	200
848	250	250	250