Spring 5-22-2021

Impact Assessment, Detection, And Mitigation Of False Data Attacks In Electrical Power Systems

Sagnik Basumallik
Syracuse University, sbasumal@syr.edu

Abstract

The global energy market has seen a massive increase in investment and capital flow in the last few decades. This has completely transformed the way power grids operate - legacy systems are now being replaced by advanced smart grid infrastructures that attest to better connectivity and increased reliability. One popular example is the extensive deployment of phasor measurement units, which is referred to PMUs, that constantly provide time-synchronized phasor measurements at a high resolution compared to conventional meters. This enables system operators to monitor in real-time the vast electrical network spanning thousands of miles. However, a targeted cyber attack on PMUs can prompt operators to take wrong actions that can eventually jeopardize the power system reliability. Such threats originating from the cyber-space continue to increase as power grids become more dependent on PMU communication networks. Additionally, these threats are becoming increasingly efficient in remaining undetected for longer periods while gaining deep access into the power networks. An attack on the energy sector immediately impacts national defense, emergency services, and all aspects of human life. Cyber attacks against the electric grid may soon become a tactic of high-intensity warfare between nations in near future and lead to social disorder. Within this context, this dissertation investigates the cyber security of PMUs that affects critical decision-making for a reliable operation of the power grid. In particular, this dissertation focuses on false data attacks, a key vulnerability in the PMU architecture, that inject, alter, block, or delete data in devices or in communication network channels.

This dissertation addresses three important cyber security aspects - (1) impact assessment, (2) detection, and (3) mitigation of false data attacks. *A comprehensive background of false data attack models targeting various steady-state control blocks is first presented.* By investigating inter-dependencies between the cyber and the physical layers, this dissertation then identifies possible points of ingress and categorizes risk at different levels of threats.

In particular, *the likelihood of cyber attacks against the steady-state power system control block causing the worst-case impacts such as cascading failures* is investigated. The case study results indicate that false data attacks do not often lead to widespread blackouts, but do result in subsequent line overloads and load shedding. The impacts are magnified when attacks are coordinated with physical failures of generators, transformers, or heavily loaded lines. Further, this dissertation *develops a data-driven false data attack detection method that is independent of existing in-built security mechanisms in the state estimator*. It is observed that a convolutional neural network classifier can quickly detect and isolate false measurements compared to other deep learning and traditional classifiers. Finally, this dissertation *develops a recovery plan that minimizes the consequence of threats when sophisticated attacks remain undetected and have already caused multiple failures.* Two new controlled islanding methods are developed that minimize the impact of attacks under the lack of, or partial information on the threats. The results indicate that the system operators can successfully contain the negative impacts of cyber attacks while creating stable and observable islands. Overall, this dissertation presents a comprehensive plan for fast and effective detection and mitigation of false data attacks, improving cyber security preparedness, and enabling continuity of operations.

Impact Assessment, Detection, and Mitigation of False Data Attacks in Electrical Power Systems

By

Sagnik Basumallik

B.Tech., West Bengal University of Technology, 2014

Dissertation

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical & Computer Engineering

Syracuse University

May 2021

Acknowledgements

I wish to acknowledge the Indian philosophy of *Sanatana Dharma* for teaching me the value of *karma-yoga*,

कर्मण्येवाधिकारस्ते मा फलेषु कदाचन।
मा कर्मफलहेतुर्भूर्मा ते सङ्गोऽस्त्वकर्मणि॥

where action is free from attachment of both success and failures, where the concern is with action alone, never with the outcome, and never with inaction. This has helped me develop an equanamous mind which was instrumental in my graduate studies.

I would like to thank my mother Smt. Papiya Basu Mallik and my father Shri. Prasanta Basu Mallik for their wise counsel and support throughout my stay away from India.

I would like to express my sincere gratitude to my advisor Dr. Sara Eftekharnejad for giving me the opportunity to work with her, whose expertise was invaluable in formulating the research questions and methodology. I would want to extend my thanks to Dr. Makan Fardad and Dr. Reza Zafarani for providing me the tools and valuable guidance needed to pursue research and teaching. Special thanks to my committee members Dr. Senem Velipasalar, Dr. Chilukuri Mohan and Dr. Cliff Davidson for their time and considering being on my supervisory committee.

I would like to thank late Professor Wilbur Reed LePage, the Department of Electrical Engineering and Computer Science and the L.C. Smith College of Engineering and Computer Science at Syracuse University for the generous LePage Fellowship that made my graduate studies possible in the United States of America.

I would also like to acknowledge the National Science Foundation, Grant No.1600058, which forms the basis of this dissertation.

I would like to thank Dr. Brian K. Johnson, Dr. Mingguo Hong, Dr. Xiaochuan Luo, Dr. Slava Maslennikov and Dr. Paolo Serafini for their advise and guidance.

In addition, I could not have completed this dissertation without the support of my labmates Rui Ma, Mirjavad Hashemi and Peter Wolf. I am also grateful to my friends Baasansuren Batsukh, Jagdeep Dosanjh, Yaojun Lu, Thiago de Melo, Huzeyfe Demirtas, Joshua Tignor, Benjamin Cook, Soubhik Das and Avijit Mandal, with whom I have had extensive discussions on philosophy, ethics, morality, society, politics, warfare, and religion during my graduate studies.

Dedication

To President Donald Trump and Prime Minister Narendra Modi

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 General Introduction

In a macro-economic system, all major sectors such as agriculture, extraction of natural resources, manufacturing, construction, transport, communication, and health services depend on a reliable supply of electricity. However, the existing electricity infrastructure has increasingly become vulnerable to various cyber attacks. An advanced class of threat is a false data injection attack that modifies power system measurements to impede time-critical operations. False data attacks have been shown to cause incorrect solutions to multiple power system control algorithms, leading to an increase in operation costs, incorrect generation dispatch, and unintentional outages. Consequently, outages disrupt other critical dependent networks like water, gas, and internet, thereby affecting a large number of customers and causing substantial economic loss. The general theory of false data injection attacks and the implications of such attacks are currently an active field of research. This dissertation investigates the impact of false data injection attacks and develops effective detection and mitigation strategies to counter such sophisticated threats.

1.2 Motivation

Power systems are an essential part of our lives and reliable electricity is critical for daily tasks. However, rapid changes in system operating conditions due to the diversity of customer behaviors and demands, uncertainty in renewable generation, stressed transmission

network, aging infrastructure, and increased connectivity between various load-serving entities are some of the challenges that threaten the reliability of power systems. Blackouts have often resulted due to lack of situational awareness, an example of which is the July 2012 blackout in India that affected 700 million people [1].

Situational awareness is improved by deploying more phasor measurement units for real-time monitoring and accurate system condition estimation. Unfortunately, these online monitoring devices are vulnerable to various cyber-attacks that can potentially introduce delays and errors in time-critical operations. Without correct real-time information, the power grid is susceptible to manual or automatic control errors.

Attacks targeted against power networks lead to disruption of major control algorithms including static and dynamic state estimator, optimal power flow and security-constrained economic dispatch [2–30]. Additionally, attacks have been shown to compromise the transient and auxiliary controls [31–37], substation controls and communication architecture [38–44] and other energy control and operation blocks [45–58]. A combination of data falsification and physical attacks against transmission lines and unmanned remote substations may result in line overloads, load curtailment, and in the worst-case, cascading failures.

As a result, power system operators now have to deal with additional security issues arising from the cyber domain. Various factors pose difficult challenges for system operators to understand the very nature of cyber-attacks. These challenges range from 'zero-day' attacks to potential undiscovered 'back-doors' in communication systems and third-party maintenance software. Additionally, insufficient information sharing between utilities and government and the lack of cyber security training complicate the detection of these modern threats. This dissertation conducts a systematic study on the current smart grid cyber security issues and proposes new solutions to address advanced threats like data falsification attacks.

1.3 Research Scopes and Objectives

Figure 1.1 illustrates the three-fold objectives of this dissertation - impact assessment, detection, and mitigation of false data attacks, on steady state power system control blocks. The specific objectives are defined as follows,

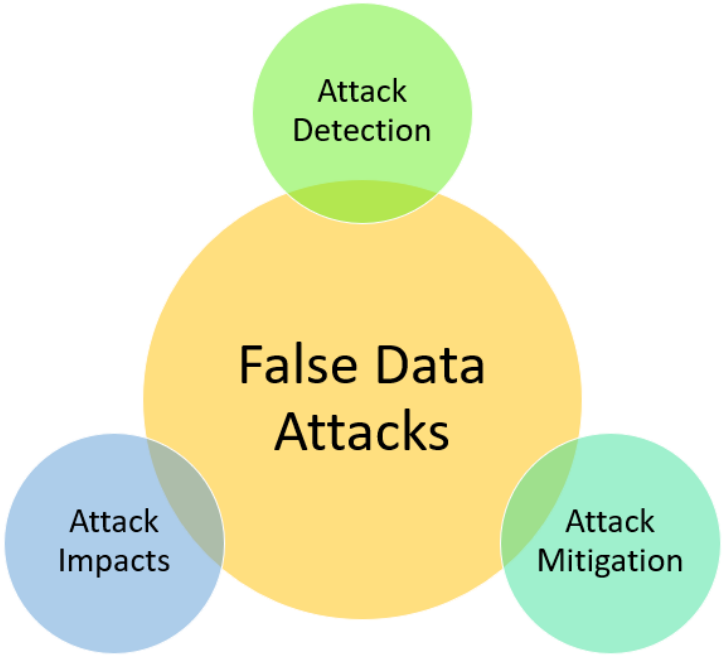

Figure 1.1: Summary of research topics in this dissertation

Impact Assessment of False Data Attacks

- To investigate conditions under which the impacts of false data attacks are the most severe on realistic power grids,
- To study the impacts of false data attacks considering special protection systems such as remedial action schemes (RAS),
- To assess attack impacts considering (a) expected energy not served, (b) loss of observability after cascading failure and controlled islanding, and (c) extent of the recoverability of the grid.

Detection of False Data Attacks

- To verify the correctness of measurements by exploiting historical PMU time-series data,
- To develop a false data detection technique independent of the power system topology and state estimation.

Impact Mitigation of False Data Attacks

- To incorporate the uncertainty of PMU measurements in controlled islanding under the lack of knowledge, or partial knowledge of false data attacks, while creating stable and observable islands,
- To maximize the island observability with a minimum number of PMUs under the lack of knowledge of attacks,
- To isolate vulnerable PMUs in a small island under the partial knowledge of attacks,
- To develop a multi-objective optimization problem for controlled islanding as an effective post-attack mitigation solution, and investigate various optimization techniques for solving the multi-objective problem.

1.4 Contribution of Dissertation

This dissertation is concerned with the detection, impact assessment and impact mitigation of false data attacks against the power system steady state control algorithms. This dissertation is organized into three chapters,

1.4.1 Chapter 2

This chapter first presents a comprehensive analysis on false data injection attacks against the steady-state control of the bulk electrical system. Next, this chapter focuses on estimating the actual impact of false data attacks on realistic power systems. Practical electric grids are designed to operate under large inter-area power transfers for different loading conditions. Depending on the current system loading, compromised measurements can have diverse impacts on power systems - not all data attacks will have the same level of impact on system reliability. To study the scenarios that lead to the most severe consequences, attacks targeting RAS are considered. Such attacks disable or block triggering conditions and prevent automatic RAS from taking timely corrective actions. In addition to attacks against RAS, the false data attack on phasor data concentrators is modeled using a semi-Markov approach that closely mimics practical cyber attack scenarios.

Using a distributed cascading failure algorithm, the direct consequence of the coordinated attack is quantified as the expected energy not served. Further, post-attack impacts are quantified using three indices - Loss of Observability after Cascading Failures (LOCF), Loss of Observability after Controlled Islanding (LOCI), and Lines Recoverable after Controlled Islanding (LRCI). Together, these indices quantify the extent of a grid's recoverability after an attack adversely impacts the system.

1.4.2 Chapter 3

Existing model-based bad data detectors in traditional state estimators are incapable of discovering carefully crafted false measurements. This chapter develops a measurement-based false data attack detector that is independent of the power system topology and state estimation. The false data detector is developed by leveraging historical PMU data collected from phasor data concentrators (PDC) at regional substations. These regional PDCs form one of the most vulnerable points in the entire synchrophasor communication archi-

tecture where multiple concentrating PMU data streams may be compromised at the same time. This detector is designed to serve as an early warning system to detect and isolate vulnerable measurements quickly at any regional substation in the power grid network.

False data streams in the PDCs are detected by exploiting time-based inconsistencies in PMU packet data. Normal events such as load/generation variations and bus/branch faults exhibit strong correlations among multiple time series due to the underlying physical laws governing the dynamic system. However, only a subset of measurements are changed during data falsification attacks, thus altering the underlying statistics and the inherent correlations within the time-series data.

Various deep learning algorithms are used to identify altered data streams based on the differences in spatio-temporal features. A convolutional neural network (CNN)-based data filter is first developed to detect false data attacks. The results of the developed filter is compared with other deep-learning and traditional classifiers.

1.4.3 Chapter 4

If for any reason a sophisticated false data injection attack remains undetected, it is essential to contain the impacts of wrong measurements to only a small part of the system. This chapter develops an effective mitigation strategy to counter the sophisticated data falsification attacks that remain undetected and have already impacted critical lines and transformers. We utilize existing power system islanding techniques and investigate how these methods can be improved to account for PMU measurement uncertainty.

Two controlled islanding techniques are developed to prevent large-scale outages when attacks remain completely undetected, or when partial knowledge on attack is available. Under the lack of knowledge of attacks, the multi-objective optimization problem maximizes the observability of the islands using a minimum number of PMUs. When partial

knowledge of attack is available, the size of the island with vulnerable measurements is minimized to contain the impacts of attacks. The islanding scheme is formulated as a multi-objective optimization problem that minimizes the impact of attacks while simultaneously creating stable and observable islands.

Different scalarization techniques are explored to transform the multi-objective islanding optimization problem into a single objective problem. The impacts of the optimal islanding solutions are then investigated on various realistic power system networks.

1.5 Publications

Part of the work presented in this dissertation has appeared in the following publications as of April 15^{th}, 2021,

Peer Reviewed Journals:

1. **Basumallik, Sagnik**, Sara Eftekharnejad, and Brian K. Johnson. "The impact of false data injection attacks against remedial action schemes." International Journal of Electrical Power & Energy Systems 123 (2020): 106225.
2. **Basumallik, Sagnik**, Rui Ma, and Sara Eftekharnejad. "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network." International Journal of Electrical Power & Energy Systems 107 (2019): 690-702.

Conferences:

1. **Basumallik, Sagnik**, and Sara Eftekharnejad. "Dynamic Islanding in Power Systems Based on Real-Time Operating Conditions." In 2019 North American Power Symposium (NAPS), pp. 1-6. IEEE, 2019.
2. **Basumallik, Sagnik**, Sara Eftekharnejad, Nathan Davis, Nagarjuna Nuthalapati, and Brian K. Johnson. "Cyber security considerations on PMU-based state estima-

tion." In Proceedings of the Fifth Cybersecurity Symposium, pp. 1-4. 2018.

3. **Basumallik, Sagnik**, Sara Eftekharnejad, Nathan Davis, and Brian K. Johnson. “Impact of False data attacks on PMU-based state estimation." In 2017 North American Power Symposium (NAPS), pp. 1-6. IEEE, 2017.

Chapter 2

Impact Assessment of False Data Attacks

2.1 Introduction

The reliable operation of smart power grids depends on situational awareness made possible by real-time monitoring and accurate system condition estimation using PMUs. Unfortunately, the PMU communication architecture is vulnerable to false data attacks. False data attacks comprise of *injection, alteration, blocking, deletion, modification of data and status, or a combination of any of the above, in devices or in communication network channels, that impede the reliable operation of power systems.* Fig. 2.1 shows the chronological development of research in false data injection attacks against the bulk electric grid. Such attacks can lead to uneconomic operation, line overloads, loss of reliability, and unintentional islanding. While attacks could result in power outages, not all attacks will have the same level of impact on system reliability and real-time operations.

This chapter investigates to what extent such coordinated attacks against the power system steady-state control blocks actually lead to large scale blackouts. We specifically seek to identify attack circumstances that lead to the most severe consequences. To consider the worst case scenarios, the impact of false data injection attacks is investigated on realistic power networks under large inter-area power transfers. To further maximize the impact of attacks, threats against the steady-state remedial action schemes are considered, which prevent timely corrective actions. A risk index is developed to quantify the attack im-

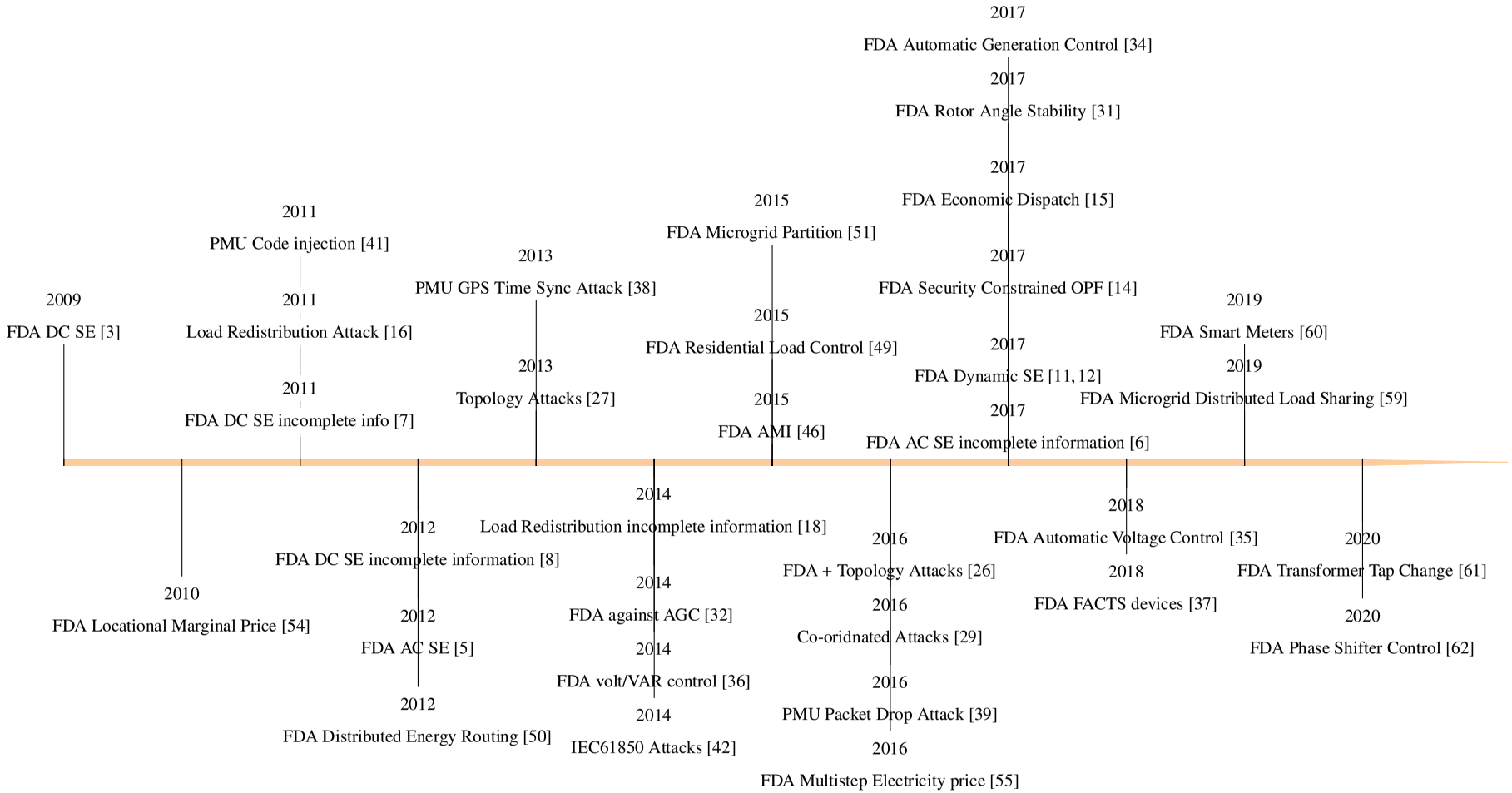

Figure 2.1: Chronology of benchmark research in false data injection attacks against electric power systems [2009-2020]

pacts under various load-generation and network topology conditions. Additionally, three indices are proposed - loss of observability after cascading failures, loss of observability after controlled islanding, and lines recoverable after controlled islanding, to quantify the severity of the attack, and to estimate the extent of recoverability of the grid after attacks have adversely impacted the power grid.

The chapter starts with a brief overview of various power system control and operations blocks, provides a comprehensive background on cyber-security research in electric power grids, and considers attacks against steady-state controls in details, which is the main scope of this dissertation.

2.2 Overview of Power System Control and Operations

We first present a brief overview of the key operating control blocks for the electric power systems susceptible to false data attacks. At the heart of the power system is the master program called the energy management system (EMS), a high-performance critical application overlooking all monitoring, control, and optimization functions of the electric grid. The EMS collects redundant measurements from various PMUs and SCADA devices, sampling current, voltage, and power flow from field instrument transformers. The PMUs sample at the rate of 30/60/120/240 messages per second with a significantly high degree of accuracy compared to traditional SCADA devices, and hence widely deployed by utilities to improve real-time monitoring [63, 64]. The PMUs at the substation level send their measurements to a local phasor data concentrator (PDC) where the data packets are time synchronized and aligned. Data from station level PDCs are concentrated at regional PDCs which further report to a data concentrator at the main control center. The PMU-PDC architecture is shown in Fig. 2.2.

Inside the EMS is the topology processor that estimates the grid network structure from

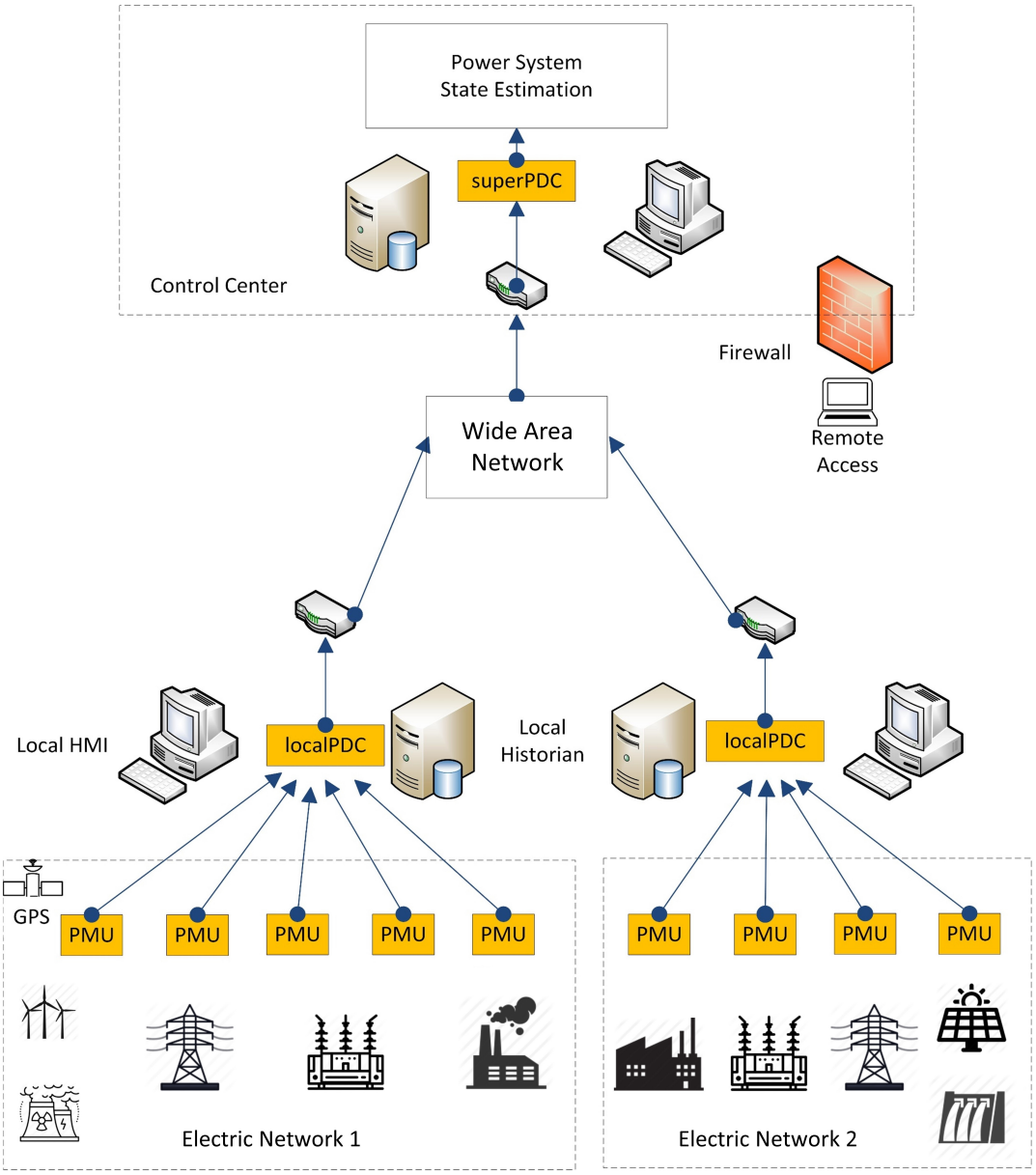

Figure 2.2: Visualization of a PMU-PDC network architecture. The PMUs at the field level send their measurements to a local phasor data concentrator (PDC) at a substation where the data packets are time synchronized and aligned. Data from station level PDCs are concentrated at regional PDCs which further report to a data concentrator at the main control center. The PMU data flows through the wide area network, concentrates at super PDC where it is used for state estimation and other applications. Access to the communication architecture is restricted via user authentication and firewalls. The data is periodically archived in the historians.

circuit breaker contact signals hardwired to Remote Terminal Units (RTUs) [65]. These status signals are incorporated in the PMU packet data flowing through the communication network. For a reliable operation of the power system, a correct estimation of the system topology is the first and the most important step. Once the topology is determined, the state estimator (SE) collects redundant measurements from SCADA and PMUs, eliminates gross errors, and estimates bus voltages and angles using a non-linear weighted least squares method [66]. The SE provides a quasi-static model of the power system under real-time operating conditions. The states are estimated by solving an over-determined set of non-linear power flow equations [67]. A general non-linear hybrid state estimator utilizes bus voltage and branch current phasors in addition to power flows and injections measurements to estimate power system states [68]. To account for different sampling rates, the average of each PMU time series over one state estimation cycle is used in combination with SCADA measurements [69].

DC State Estimation

The linear DC state estimation using conventional SCADA meters only is based on the following linear measurement function [70],

$$z = Hx + e \tag{2.1}$$

where z is a $m \times 1$ vector of measurements, H is the $m \times n$ Jacobian Matrix, x is the $n \times 1$ vector of state variables, e is a $m \times 1$ vector of random Gaussian errors, and m, n are total number of measurements and states respectively. In DC state estimation, the following assumptions hold - (1) the voltage magnitudes at all buses in the network are assumed to be constant and equal to 1 per unit (p.u.); (2) the shunt susceptances and series resistances of transmission lines are neglected; (3) the bus angle differences between two buses are considered to be very small; (4) reactive power is completely neglected and (5) state variables only consist of bus voltage angles.

The measurement residual arising from the difference between measured and estimated states is defined as,

$$r = z - Hx \tag{2.2}$$

The state variables can be estimated by minimizing the objective function J,

$$J(x) = (z - Hx)^T R^{-1}(z - Hx) \tag{2.3}$$

Straightforwardly for DC state estimation, the states are estimates as,

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \tag{2.4}$$

AC State Estimation

The oversimplified DC state estimation model may not be suitable for real time power system state estimation as measurements in power system are related to their states by a non-linear function. The relation between the state variables to the states for AC state estimation can be written as [70]

$$z = h(x) + e \tag{2.5}$$

where z is a $m \times 1$ vector of measurements from SCADA meters and PMUs, h is a set of non-linear power flow functions relating measurements to state variables, x is a $n \times 1$ vector of state variables, e is a $m \times 1$ vector of random Gaussian errors, and m, n are total number of measurements and states respectively.

The non-linear functions $h(x)$ which relate the measurement to the state variables comprise of active and reactive power injections at bus, active and reactive power flow in transmission lines, and branch real and imaginary currents. The real and reactive power injection at bus m is,

$$P_m = V_m \sum_n V_n(g_{mn}cos\delta_{mn} + B_{mn}sin\delta_{mn}) \tag{2.6}$$

$$Q_m = V_m \sum_n V_n(g_{mn}sin\delta_{mn} - B_{mn}cos\delta_{mn}) \tag{2.7}$$

The real and reactive power flow from bus m to bus n is,

$$P_{mn} = {V_m}^2 g_{mn} - V_m V_n[g_{mn}cos(\delta_m - \delta_n) + b_{mn}sin(\delta_m - \delta_n)] \tag{2.8}$$

$$Q_{mn} = -{V_m}^2 b_{mn} - V_m V_n[g_{mn}sin(\delta_m - \delta_n) - b_{mn}cos(\delta_m - \delta_n)] \tag{2.9}$$

The real and imaginary branch current between bus m and bus n is,

$$I_{mn,real} = V_m[g_{mn}cos\delta_m - b_{ij}sin\delta_m] - V_n[g_{mn}cos\delta_n - b_{ij}sin\delta_n] \tag{2.10}$$

$$I_{mn,imag} = V_m[b_{mn}cos\delta_m + g_{ij}sin\delta_m] - V_n[b_{mn}cos\delta_n + g_{ij}sin\delta_n] \tag{2.11}$$

The weighted least squares method is used to minimize the measurement residuals to accurately estimate the states with the objective function defined as [68],

$$J(x) = (z - h(x))^T R^{-1}(z - h(x)) \tag{2.12}$$

where R is the measurement error covariance matrix. The estimates of the state are then

found by an iterative process like Newton Raphson method,

$$\Delta\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} (z - h(x)) \tag{2.13}$$

$$\hat{x}_{i+1} = \hat{x}_i + \Delta\hat{x}_i \tag{2.14}$$

where H is the measurement Jacobian matrix and is defined as $H = \frac{\partial h(x)}{\partial x}$,

$$H = \begin{bmatrix} 0 & \frac{\partial P_i}{\partial \delta} & \frac{\partial Q_i}{\partial \delta} & \frac{\partial P_{ij}}{\partial \delta} & \frac{\partial Q_{ij}}{\partial \delta} & 1 & \frac{\partial I_{ij,real}}{\partial \delta} & \frac{\partial I_{ij,imag}}{\partial \delta} \\ 1 & \frac{\partial P_i}{\partial x} & \frac{\partial Q_i}{\partial x} & \frac{\partial P_{ij}}{\partial x} & \frac{\partial Q_{ij}}{\partial x} & 0 & \frac{\partial I_{ij,real}}{\partial x} & \frac{\partial I_{ij,imag}}{\partial x} \end{bmatrix}^T \tag{2.15}$$

In matrix H, the first and the sixth columns are related to bus voltage magnitude and angle - system states which are directly measured by the PMUs, and hence has an identity relation with the estimated states.

Bad Data Detection

Bad PMU and SCADA data can naturally occur as the result of instrumentation errors, thermal degradation of equipment, or random electrical noise. One of the most popular technique of detecting erroneous measurements is comparing the $L_2 - norm$ of the measurement residuals to a detection threshold τ. For DC state estimation, no bad data is detected when,

$$||z - H\hat{x}|| < \tau \tag{2.16}$$

Similarly for AC state estimation, no bad data is detected when,

$$||z - h(\hat{x})|| < \tau \tag{2.17}$$

In general, the threshold τ is determined obtained from the cumulative chi-square distribution for $m - n$ degrees of freedom [70]. Residuals that satisfy 2.16 and 2.17 are assumed to be free of bad data while those that fail to satisfy this condition are excluded from

the data set for subsequent calculations. The discarded bad data is often substituted by pseudo-measurements obtained from historical values to ensure that SE converges.

Applications of State Estimation

The output of the SE serves as the starting point for all critical applications in the EMS including optimal power-flow (OPF) and economic dispatch, load forecast, and voltage security. The OPF analysis and economic dispatch calculates the line power flow to meet customer demand while simultaneously minimizing operating costs. This is done by solving a set of non-linear power balance equations consisting of generation, load and network equations [71]. An extension of the optimal power flow solution is the security constrained optimum power flow (SCOPF) which has added constraints for generator power limits, transmission line capacity and contingency constraints. The SCOPF ensures that the system is both pre-contingency and post-contingency stable with no SOL violations [72–74].

The results of OPF assist the real-time contingency analysis (RTCA) to determine the binding thermal and voltage constraints, ensuring $N-1$ or $N-1-1$ reliability of the power system under all real-time operating conditions [75]. In other words, this means system operating limits (SOL) are satisfied at every instant. In general, there are three types of SOL that are defined as - 24 hours (normal), 4 hours long term emergency (LTE), and 15 minutes short term emergency (STE). Depending on the current estimated states and the load demand, transfer analysis helps determine the extent to which the current operating system can be moved before being bounded by SOL. To ensure safety and continuous operation, actions against SOL violations range from generation dispatch, load curtailment to other appropriate emergency control actions.

The information from SE and OPF/SCOPF is used in the electricity market to determine the Locational Marginal Prices (LMP). The LMP reflects the price of electricity across different geography and accounts for the customer load pattern, cost of generation, and

transmission line congestion. The electricity market allows generating power plants to sell power at a particular bidding price in the day-ahead (ex-ante market) and the real-time market (ex-post market) while simultaneously satisfying the customer demand [54].

The results of the SE is also used in the Automatic voltage control (AVC) system. The AVC is responsible for maintaining system voltages within the desired range by continuously adjusting the reactive power injection, and is commonly used to monitor inter-area reactive power balances [76, 77]. The operation of AVC can be briefly explained as follows - first, the output of the SE, i.e., voltages and angles, are fed as an input to the OPF block. Once the OPF converges to a valid solution, the results are used to issue trigger commands to vary generator reactive power in order to maintain voltages within the prescribed margin of $0.9 - 1.1$ p.u.

The SE output further drives the automatic generation control (AGC) [78–80], a fundamental power system control and operation block. Inside a designated control area, the AGC maintains a nominal grid frequency and tie-line power flow by regulating the output power of generators, and reduces the area control error (ACE). Further, the estimates of the system states, together with the OPF, are used for calculating generation reserves to ensure reliability in maintaining grid frequency in the event of generation loss.

In summary, the SE is the heart of the power system and a correct estimate of bus voltage and angles is crucial for accurate functioning of all power system control and operation blocks.

2.3 Background of Cyber Attacks against Power Systems

Deployment of energy management systems has improved situational awareness, however, has inadvertently introduced additional cyber security risks in the electric grid. We present an overview of cyber-security research in electric power grids, and then discuss in details

attacks against steady-state controls, which is the main focus of this dissertation.

The authors in [81] have presented a thorough review of smart grid communication infrastructures and related cyber threats and challenges. The vulnerable access points in the electric power grid SCADA and EMS were shown to include field staff remote access computers, local area network (LAN) switches, modems connecting Remote Terminal Units (RTU) and SCADA/EMS master, routers connecting to the Wide Area Network (WAN) and station Human-Machine Interfaces (HMI) for protection relays [82]. It was demonstrated that attacks against these access points can be carried out via distributed denial of service (DDoS), reconnaissance, and port scanning using malware and viruses.

The requirements for privacy, availability, integrity, and authentication for SCADA communication networks were summarized in [83]. Various encryption techniques, key management issues, and security/privacy policies were highlighted in [84–89]. Further, the attacks on the physical side of the grid, in combination with cyber, were discussed in detail by the authors in [90–93]. A qualitative survey of cyber attacks on various control loops in power systems was presented in [90]. Attacks and their corresponding impacts on real cyber-physical test-beds were conducted in [93].

Any attack on the SCADA or PMU-PDC architecture that falsifies or blocks the flow of data can significantly impede the real-time operation. Figure. 2.3 organizes the various false data attack models against major operation and control blocks into four areas. These four areas include steady-state control, transient and auxiliary control, substation control and load control [94]. In this dissertation, we limit our study to false data attacks against steady-state controls only.

The worst-case attack scenarios against steady-state controls involve a coordination of physical attacks, load measurement falsification, and topology alteration attacks that mislead the steady-state control blocks. Fig. 2.4 illustrates the attack impacts on steady-state

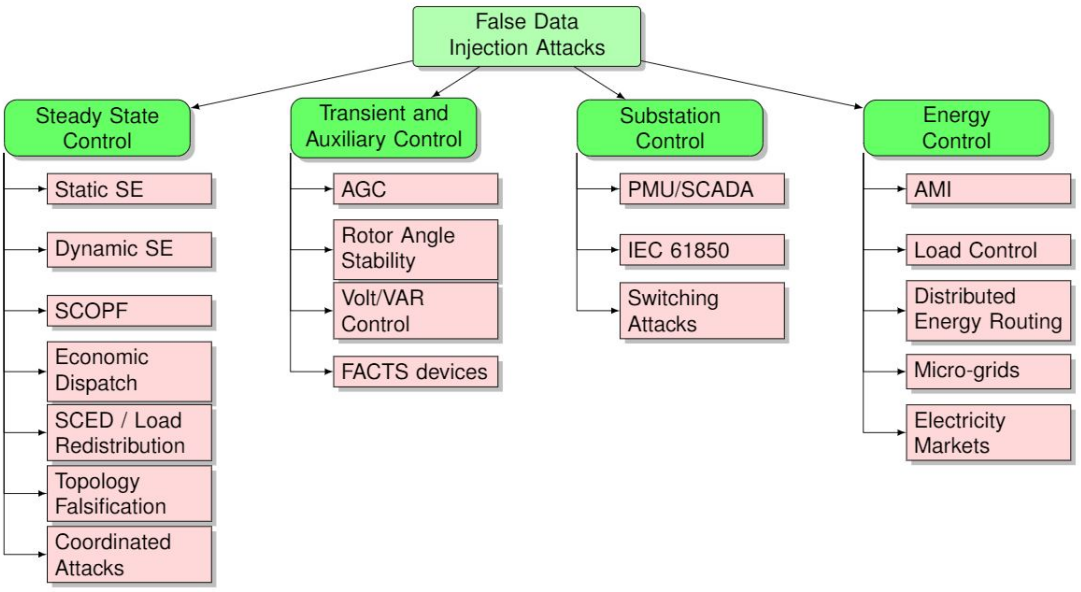

Figure 2.3: A taxonomy of false data injection attacks against various power system control and operation blocks. This dissertation focuses on false data injection attack impacts on steady state control blocks.

control algorithms targeting the SE. Such attacks can affect various mission critical operations such as the OPF, economic dispatch, AGC, AVC, real-time protection and other control algorithms that rely on continuous streaming data. Incorrect solutions further induce overloads that can lead to an increase in generation costs, unwanted line tripping, and in the worst case, may cause extensive power failure.

2.3.1 False Data Attacks against DC State Estimator

False data injection attack against the linear state estimation was first demonstrated by the authors in [3]. In this attack, a non-zero attack vector a is superimposed onto the original measurement to obtain a tampered measurement set,

$$z_b = z + a \tag{2.18}$$

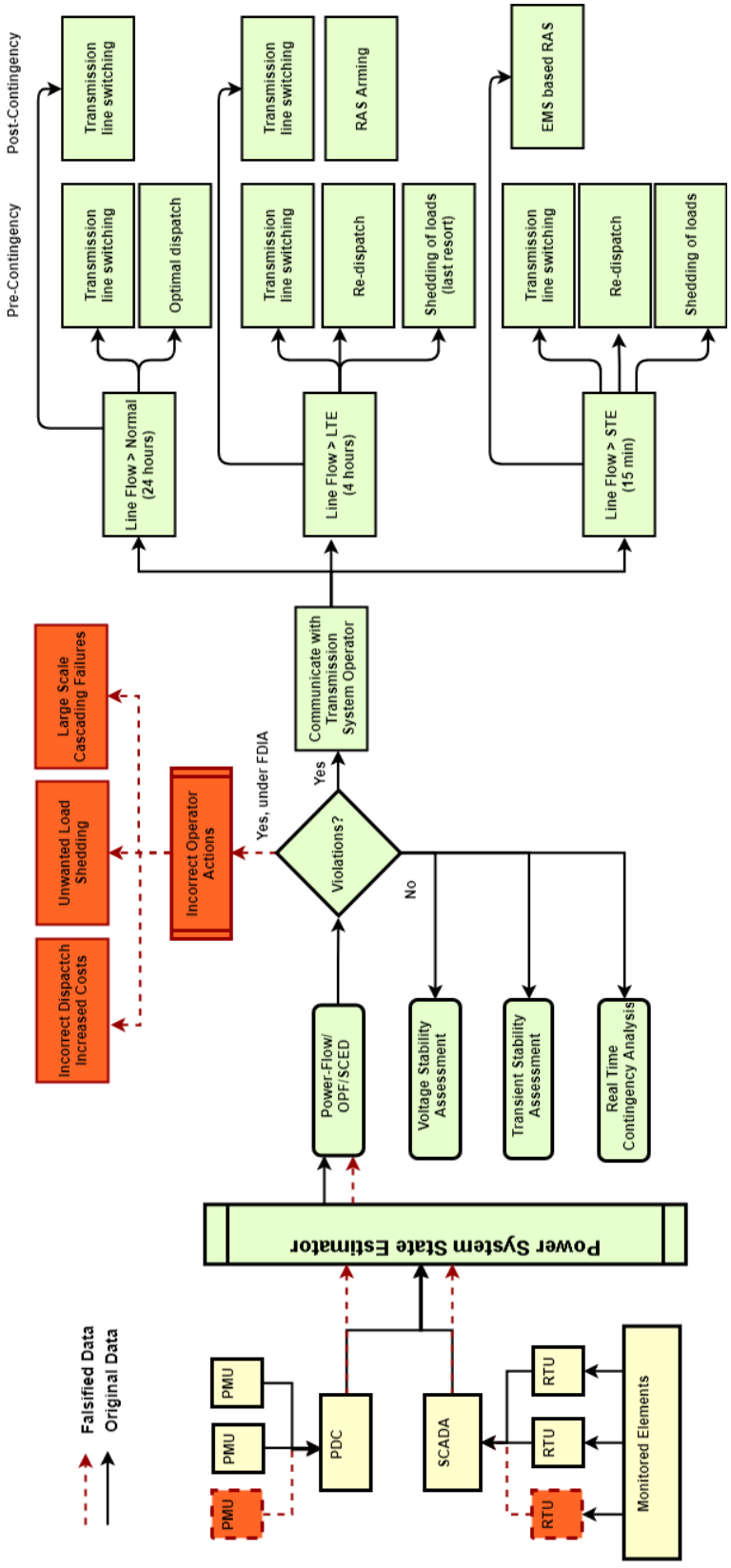

Figure 2.4: Architecture of an energy management system. Operator actions under normal conditions and false data attacks.

The new set of estimated states can be expressed as a combination of original states and a vector c as,

$$\hat{x_b} = \hat{x} + c \tag{2.19}$$

The residual of the tampered measurement and incorrect states of the system can be expressed as,

$$||z_b - H\hat{x}_b|| = ||(z + a) - H(\hat{x} + c)|| \tag{2.20}$$

If the attack vector is selected as $a = Hc$, (2.20) becomes $||z - Hx||$, and the bad data detection system in (2.16) fails to detect the false data. There are several ways to construct the attack vector a. One method is to construct a projection matrix of H as $P = H(H^T H)^{-1} H^T$. It follows that $Pa = PHc = Hc = a$, implying $(P - I)a = 0$. For a successful attack, the adversary finds an attack vector that satisfies $(P - I)a = 0$.

Let $(P - I)$ be represented by matrix B, whose column vectors are $B = (b_1, .., b_m)$. The attack vector is represented as $a = (0, \ldots, a_{i_1}, 0, .., a_{i_2}, 0, .., a_{i_k}, 0, ..0)^T$, where the non-zero elements of a correspond to measurements which are compromised by the adversary. Then, $Ba = 0$ implies $B^* a^* = 0$ where $B^* = (b_{i_1}, b_{i_2}, ..., b_{i_k})$ and $a^* = (a_{i_1}, a_{i_2}, , ..., a_{i_k})^T$. If B^* is rank-deficient, characterizing the null space of $B^* a^* = 0$ yields an infinite number of solutions such that the attack vector $a^* \neq 0$. This attack vector a can now be injected to the original measurement set to construct the false data, and used as input to the state estimator.

The false data injection attack exploits the null-space such that the attack vector is always mapped to the zero vector for some linear transformation. As a result, the residual errors do not change, or in other words, detection of such attacks is extremely difficult.

If $a \neq Hc$, the attacker can exploit the small errors associated with the measurements to inject false data such that (2.16) holds, which can potentially lead to degradation of the

state estimation output.

The attack model was further extended to find the sparsest attack vectors, i.e., the minimum number of measurements require to be compromised (NMRC), to cause maximum deviation in the estimated states. To tackle the combinatorial problem of meter selection for successful attacks, a two level heuristic false data attack model was proposed in [4] where a large network was first divided into smaller area. Next, brute force search was used to obtain reasonable sub-solutions for each area, which was then combined to obtain a global attack vector. This was compared with linear transformation of the Jacobian matrix and heuristic approaches.

2.3.2 False Data Attacks against AC State Estimation

Similar to attacks against DC state estimator, false data attack against the non-linear AC state estimator was investigated by the authors in [5]. Attack vectors were injected such that (a) Kirchhoff's Current Law (KCL) was satisfied at each node, and (b) the residual τ of the altered SE remained below the set threshold. An illustration of false data injection attack is shown in Figure 2.5.

The residual of the tampered measurement and incorrect states of the system can be expressed as,

$$\left\| z_b - h(\hat{x}_b) \right\| = \left\| z + a - h(\hat{x} + c) \right\| \tag{2.21}$$

The necessary condition to determine the correct attack vector is $a = h(\hat{x} + c) - h(\hat{x})$. This ensures that the false data bypasses the bad data detector in (2.17).

A successful false data attack that remains undetected by the bad data detection systems alters all measurements in the sub-graph which are bounded by buses having power injections.

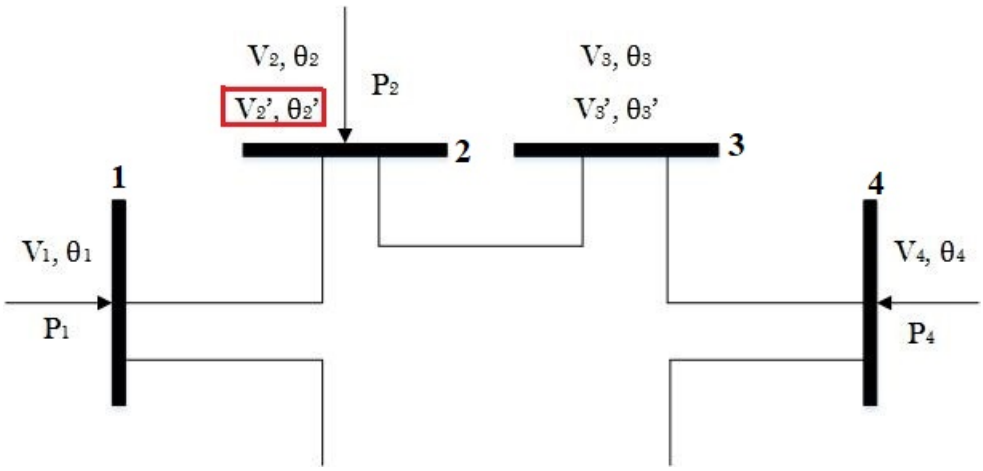

Figure 2.5: Illustration of false data injection attack based on [5]- Consider that the attacker intends to alter the power injection measurement P_2 at bus 2. In order to influence P_2, the attacker has to change the estimated state variables at bus 2, which can be either V_2 or δ_2. This will change power flows in branches $1-2$ and $1-3$ according to (2.8). To compensate for the change in line flow P_{12}, the attacker now alters the power injection measurement at bus 1 which is P_1 to ensure KCL holds at bus 1. Now, bus 3 is a net zero injection bus. In order to adjust the power flow P_{23}, the attacker adjusts the power flow P_{34}, as well as changes the power injection P_4 at bus 4 to ensure KCL holds at bus 4. Changing branch power flow P_{34} and power injection P_4 ensures that the total power injection at bus 3 is zero. This leads to additional changes in the estimated values of voltage and angle at bus 3. The false data injection may lead to incorrect state estimation, wrong generation dispatch, uneconomic operation and system limit violations.

For a successful attack, it was assumed in [5] that attackers have access to the knowledge of the power system network. The assumption of availability of complete network information with the attackers was challenged by the authors in [6–9]. Authors in [6] proposed to estimate the line power flows in the attack region based on the difference between the adjacent estimated bus angles $(\delta_m - \delta_n)$. It was shown that a knowledge of the angle difference is sufficient for the attacker to estimate the branch power flows to carry out a successful attack. In [7], a linear independent component analysis was used to infer topology and states when partial network information was available. The false data attack under incomplete information of circuit breaker status, transformer taps, network connectivity matrix, and admittance matrix was established by Rahman *et al.* [8]. A stochastic convex program was developed using scenario generation methods. Further, the concept of general blind false data attack was introduced by Yu and Chin [9] where an approximation of Jacobian matrix was obtained using principal component analysis. Such approximated attack vectors were proven to be almost stealthy.

2.3.3 False Data Attacks as Load Redistribution Attacks

The authors in [16] identified false data attacks as load redistribution (LR) attacks where the SCOPF algorithm is compromised by falsifying load measurements at specific injection buses. In LR attacks, load injections measurements are increased at certain buses and decreased at other buses (up to 50% of their original set point), keeping the total load unchanged, while subsequently altering related power flow measurements to satisfy KCL at every node. A successful LR attack transferred load measurements from multiple injection buses to the largest load bus in the system to avoid detection. Such attacks lead to a secure operating condition with higher operation costs [13–25].

The LR attack problem in [16] was formulated as a bi-level optimization problem. Here, the upper level problem was solved by the attacker to maximize the total generation and

load-shedding costs. The lower level problem was solved by the system operators to minimize the operation cost by re-dispatching generation or by shedding loads. The operator actions are based on falsified states obtained after an incorrect SE solution as a result of LR attack. The bi-level optimization problem was transformed into an equivalent single level problem using the Karush-Kuhn-Tucker (KKT) conditions to obtain the optimal attack vector. Similar attack models were explored in [13, 17] where the altered load measurements were considered not to exceed 50% of the original value and the maximum number of compromised meters was limited to 20. The authors in [20, 21] considered LR attacks under limited attacker budget which reflected more practical attack scenarios. The feasibility of a LR attack under partial network information was further demonstrated by the authors in [18, 19].

A similar LR attack approach was proposed by the authors in [14] where the objective was to alter generation dispatch such that the system becomes susceptible to a single point failure. The system failure was guaranteed by ensuring that there exists overloads after a single line outage with the new dispatch. A bi-level optimization problem was formulated. In the upper level, the objective of the attacker is to minimize the number of meters required to be compromised, while (1) keeping measurement changes within tolerable limits, (2) ensuring the net load in the system remained unchanged and (3) preventing the compromised line flows to go beyond permitted SOL. In the lower level, the system operators solved the SCOPF (with the perturbed measurements from the upper level) to obtain the new dispatch. The outer level optimization was solved through meta-heuristic techniques while quadrature programming was employed to solve the inner level problem. It was shown that the new dispatch is not $N-1$ compliant, thereby potentially leading to further failures if not discovered quickly.

Further, the authors in [15] proposed a bi-level optimization problem for the LR attack to congest transmission lines. The attackers solved the upper level problem to adjust the

dynamic line ratings (DLR) of transmission lines (equipped with dynamic line limit monitoring devices) to maximize line flow violations. In the lower level, the system operators minimized the operation cost to obtain a suitable a generation dispatch. The falsified measurements from the upper level resulted was shown to congest line flows. The optimization problem was subjected to power flow constraints, load-generation constraints and flow capacity constraints, and was solved using the Karush-Kuhn-Tucker (KKT) conditions.

2.3.4 Coordinated False Data Injection and Physical Attacks

Coordinated attacks, on the other hand, are the worst kind of attacks that combine data falsification, load redistribution and physical attacks, as shown in Fig. 2.6. The goal of such an attack is to mask line outages by sending a combination of incorrect status and altered measurements to the control center.

Under normal condition, the authors in [26] propose line outage residual indices to identify disconnected lines. When the k^{th} line is out of service, the outage residual is given as, $r_k = \min_{f_k^0} ||\Delta\theta_{m,k} - \Delta\theta_{m,k}^{cal}||_2$, where $\Delta\theta_{m,k}$ and $\Delta\theta_{m,k}^{cal}$ are the observed and calculated phase angle changes obtained from the PMUs on the transmission lines. In [26], the line outage residuals were exploited as potential candidates for coordinated false data attacks. By compromising the PMU data packet, the attacks falsified node injection measurements at both end of the candidate transmission line, in addition to falsifying the line connection status. A successful attack was launched by (1) keeping the load injection measurement variations within 50% the rated values to avoid potential discovery, (2) ensuring the line outage residual of the compromised line to be above the minimum detection threshold, and (2) satisfying the KCL at each node to successfully pass the existing bad data detection system in the SE. Similar topology attacks involving falsification of circuit breaker status can be found in [27, 28].

Other coordinated attacks were considered by authors in [29, 30] where physical attacks,

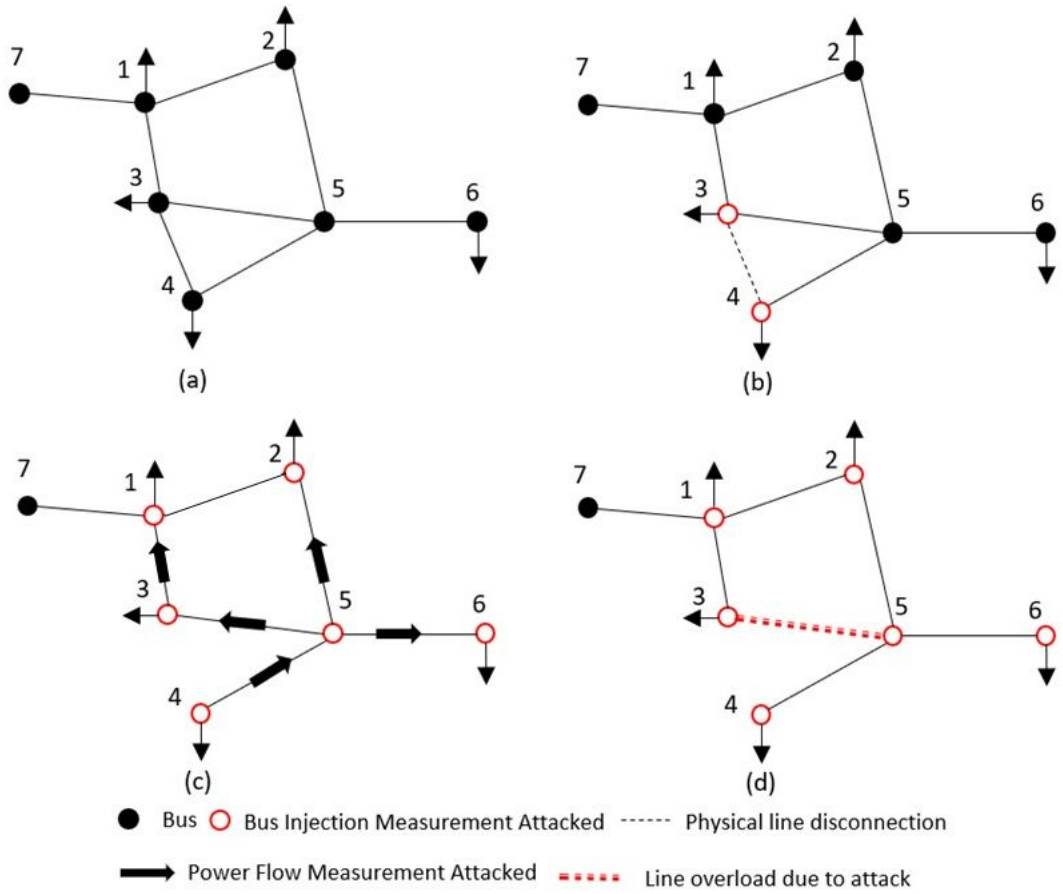

Figure 2.6: Coordinated false data and physical attacks, and their consequences: (a) healthy power system, (b) line 3-4 is physically attacked, and the outage is masked by a coordinated false data injection attack on measurements at nodes 3 and 4, (c) falsification of power flow and injection measurements in attack neighborhood surrounded by all injection buses, resulting in (d) incorrect topology and state estimation, leading to physical overload of line 3-5.

designed as altered power flow measurements, were combined with carefully constructed false data injection. The coordinated attack was formulated as a bi-level optimization [29]. The upper level optimization maximized the impacts of the physical outage while the lower level optimization minimized attack costs by finding a minimum set of measurements to be altered. The proposed mixed-integer nonlinear program was reformulated as a mixed-integer linear program. However, due to non-convexity of the problem, KKT or duality based methods could not be used, and a two-stage sequential approach was proposed to solve the problem.

The general assumptions of carrying out successful false data attacks include [2–5, 7–10, 15, 18, 30],

1. prior complete or partial knowledge on system topology and Jacobian matrix,
2. prior knowledge on transmission line limits,
3. access to dynamic line limit monitoring devices, meter measurements and meter ID mapping in the EMS,
4. prior knowledge on historical load, generation capacity, cost, dispatch sequences and LMP data.
5. changes to measurements within tolerable values,
6. non-attackable zero-injection buses,
7. non-attackable generator measurements, or attackable small distributed generators.

2.4 Impact of False Data Attack

Data falsification attacks leads to incorrect state estimation, which in turn interferes with the real-time operations of a large number of time-critical control blocks in the power system. For example, attacks have shown to mislead power flow solutions, resulting in SOL violations, incorrect line tripping, unwanted re-dispatch of generation and load shedding. Load redistribution attacks were shown to increase operating costs by driving the SCOPF to uneconomic operating conditions, resulting in non-optimal generation dispatch, initiating line overloads and tripping, and resulting in load shedding. The consequences of coordinated attacks are straightforward - when line outages are masked and system topology is incorrect, all three major control blocks - observability analysis, state estimation and bad data detection, fails, and results in erroneous line flows. This directly affects all critical operational algorithms such as SCED, SCOPF and RTCA. Coordinated attacks were shown to result in multiple line overloads and unintended islanding. In the absence of detection and immediate corrective actions, multiple overloaded line trips can further initiate widespread load-shedding.

It was shown in [54, 57, 95] that the electricity market is largely affected by data falsification attacks against the state estimation. Attackers were shown to make economic profit by altering the LMP. Successful attacks are carried out by buying virtual power at lower prices and selling it at higher prices [54, 95]. The attacker first buys and sells virtual power P in the ex-ante market at different locations j_1 and j_2 with prices λ_{j1}^{DA} and λ_{j2}^{DA}. Next, false data is injected to manipulate prices in the real-time market, and the attacker sells and buys the virtual power P at $j1$ and $j2$ with prices λ_{j1} and λ_{j2}. The financial gains obtained by the attacker is, $Profit = (\lambda_{j1} - \lambda_{j2} + \lambda_{j2}^{DA} - \lambda_{j1}^{DA})P$. Additionally, the authors in [55] have discussed false data attacks on multi-step electricity pricing mechanism where the power demand is forged by compromising smart meters, ultimately resulting in higher prices paid by the customers for their electricity.

Further, false data attacks have also shown to mislead the AGC [32]. Corrupt measurements indicating an excess power generation in an area leads to an incorrect generation ramping actions, and eventually results in frequency decay and load shedding. The authors in [33] developed a cyber-physical test-bed to demonstrate the effect of false measurement on the tie-line, leading to an increase in ACE. Sequential attacks resulted in frequency deviation from the nominal set point, which led to mis-operation of remedial action schemes, disconnection of generators and loads, and damage to expensive electrical equipment, eventually triggering widespread blackouts.

The authors in [35] investigated how falsified data attacks distort the functioning of the AVC, triggering unwanted changes in the voltage regulation commands at compromised substations. When carried out during peak load hours, the attacks can adversely affect the closed-loop control algorithm required to maintain voltage stability and power balance. In the worst case, falsified measurements can lead to system-wide outages. Further investigations showed that an attack on both ends of the line in a substation resulted in a total voltage collapse.

2.4.1 Background of Cyber-Physical Impact Assessment

To analyze the risks posed by cyber attacks on the physical grid, a number of general approaches have been proposed. These include attack trees [96], graph-theory [97, 98], hyper-graphs [99], complex network theory [100], Petri nets [101,102], probabilistic methods [103–105], and Markov Decision Processes [106].

Ten et. al [96] proposed an attack tree model to evaluate cyber security risks considering password policies and port auditing. Directed graphs were used in [97] to model the impact of cyber attacks when additive bias was introduced on sensor measurements leading to incorrect control and load shedding. Hahn et. al [98] proposed an exposure graph-based cyber security evaluation that identified untrusted data flows within a network by studying

security mechanisms, privileges and information objects within a network system. Fan et. al [99] adopted a hyper-graph model of substation automation system to identify critical cyber physical elements using extended graph centrality-based indices.

A complex network theory-based approach to model cyber-physical inter-dependencies in a power system was proposed by Zhu et. al [100]. A vulnerability index, based on electrical and cyber in-degree and out-degree, was used to identify the most critical and vulnerable components within the power system network. Laprie et. al [101] proposed a Petri net-based cyber-physical inter-dependency modeling. Chen et. al [102] combined several smaller domain specific petri-nets into a higher level Petri net. These Petri nets enumerated different security states and transitions due to attacker actions.

Falahati et. al [103] calculated the availability and the unavailability state probabilities of cyber and physical devices where a large number of binary variables were used to define device status. Mousavian et. al [104] considered attack propagation from compromised PMUs to uncompromised PMUs through routers. Vellaithurai et. al [105] proposed CPIndex that used conditional probabilities and dependency graphs to calculate the probabilities of system files and processes becoming directly or indirectly tainted.

Davis et. al [106] used partially observable Markov decision processes to study cyber-physical attacks causing malicious circuit breaker trips that result in line outages. Pan and Shames [107, 108] considered attacks against power system SE where the impacts were quantified as errors between the estimated and the actual injected powers. Moya et. al [109] considered coordinated attack sequences combined with impacts on the physical grid, specifically on security constrained economic dispatch. Liu et. al [110] considered cyber attacks where attackers tampered local substation protection systems settings that led to overloads and load shedding.

In general, finding ways to accurately capture the impacts of cyber attacks still remain

an active field of research due to the complex interdependence between the physical grid and the cyber communication infrastructure. The various impact analysis approaches discussed above had multiple drawbacks. For example, approaches using graph network indices in calculating the impact may not best reflect the effects of physical failures [100]. Assuming constant rate of failures for power system states, and using DC power flow model to calculate the impact [103] may underestimate the actual consequences of attack. The approach in [102] needs enumeration of large number of physical and cyber states as well as modeling their interdependencies, which may be impractical for large scale analysis. Propagation models [105] become inadequate when attackers compromise station PDCs and alter multiple measurements at a single point instead of attacking individual PMUs. Further, the extent of line trips resulting in a cascade were not extensively discussed in [106].

One of the major drawback of the above approaches is the failure to include in-built corrective action schemes while estimating the attack impacts. While some of the corrective actions are initiated by an operator, there are automatic special protection schemes or remedial action schemes (RAS) that trigger control actions based on the SE results. Excluding RAS system models in simulations of the power system was one of the contributing factors to September 2011 San Diego blackout [111]. The inclusion of these RAS in our study results in a more realistic attack impact estimation for practical power systems.

2.4.2 Developed Impact Assessment Method

While attacks may have different impact, our approach specifically seeks to identify attack circumstances that lead to the most severe consequences. The procedure for the impact assessment of coordinated false data injection attacks is summarized in Figure. 2.7.

To consider realistic scenarios, we consider power networks that are $N-1$ secure. Further, we design attacks under large inter-area power transfers, an approach which is not

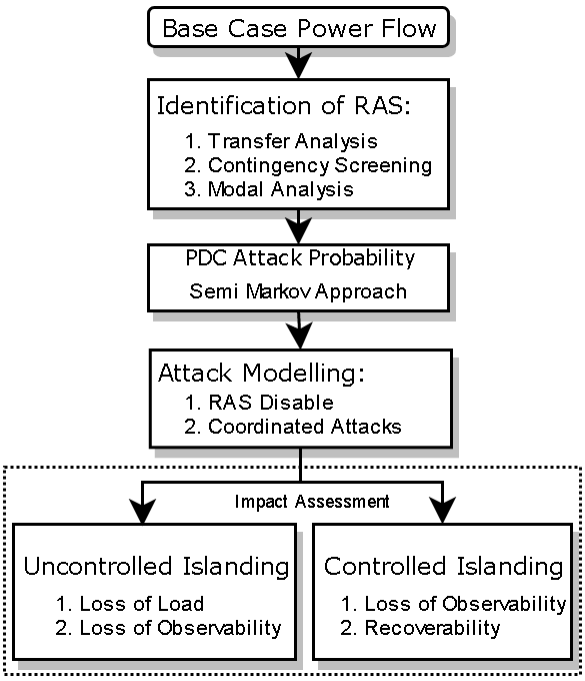

Figure 2.7: Flowchart of developed impact assessment of coordinated false data attack

considered in the literature.

Next, data attacks on parameter-based RAS are considered to study scenarios that can cause the most impact. Locations of RAS are identified through extensive inter-area transfer analysis, contingency screening and modal analysis. This is more practical as additional attacks against RAS prevent timely corrective actions, and lead to transmission line overheating, sagging and unplanned outages, thereby increasing chances of large scale outages.

Next, false data attacks are launched from compromised phasor data concentrators (PDCs). The false data attack was modeled as a semi-Markov process to calculate the probability of a PDC to be in a compromised state at any given time. The rationale behind this approach is inspired by two factors - (1) from the onset of offense to the final recovery, practical cyber attacks transition through various stages with different probability distributions. For example, malwares can be launched at random. However, once a malware infiltrates the system using stolen credentials, it stays dormant for a significantly long time

to acquire critical system information before launching attacks in quick succession [112]. The Semi-Markov Process (SMP) can incorporate both exponential and non-exponential distributions to capture the nature of the real attacks. (2) Propagation models based on conditional probabilities, such as those considered in [105], become unsuitable due to the hierarchical network of PMU-PDC data flow architecture. This is because data once falsified at local-PDC level concentrate directly at super-PDCs and then at the SE buffer. Overall, semi-Markov models are mathematically tractable and have simple interpretation for our study.

Direct consequences of attacks are then quantified as the expected energy not served (EENS) using a Distributed Slack (DS) AC-based cascading failure algorithm. Additionally, post-attack impacts are quantified in terms of loss of system observability under both cascading failure and controlled islanding, as well as extent of recoverability of the grid.

2.5 Modeling Realistic Scenarios

Power systems are complex, and depending on their operating conditions, impact assessment can vary. To construct realistic study scenarios, we consider various operating conditions. Some operating conditions, such as peak load or light load may serve as worst case scenarios while others may have limited impacts during normal contingencies. All base-cases are ensured to be $N-1$ secure. Another aspect of scenario preparation is to identify the location of RAS for a more realistic and practical analysis of the actual impacts of false data attacks.

2.5.1 Transfer Analysis and Contingency Screening

Large power systems are divided into areas which are interconnected through high voltage transmission (tie) lines that transfer bulk power over long distances. The main objective of power transfer analysis is to understand the extent by which the current operating system

can be moved before security limits are violated [113].

Bulk power transfers are often limited by contingencies. As lines become congested, contingencies overload and/or trip other lines, further reducing the transfer capacity. To facilitate smooth power transfer, system operators perform 1-D (between a single source and a sink) or 2-D (among three independent sources or sinks) transfer analysis and screen the most severe contingencies.

For a given transfer, critical contingencies with the smallest voltage stability and thermal security margin are identified. The security margins are calculated based on differences between transfer at the initial point and the last point where post-contingency power flow solution exists [114]. All transfers are carried under maximum limits to determine binding contingencies under worse-case scenarios. After critical contingencies are identified, locations of RAS are determined next. These RAS increase the power transfer capability, as illustrated in Figure 2.8 and Figure 2.9.

2.5.2 Identifying Locations of Remedial Action Schemes

Remedial action schemes are corrective schemes that increase power transfer capacities and ensure critical contingencies do not result in uncontrolled cascades [115]. Installations of RAS are mostly based on operator experience, pre-determined simulations and lookup tables. The general architecture of RAS is shown in Figure. 2.10.

RAS are either event-based or parameter-based. Event-based schemes are open-loop control systems that include rapid pre-determined actions such as immediate generator rejection and load shedding to prevent system wide transient instability after a critical contingency has occurred. A real-world example of an event-based RAS is discussed in [116], where multiple generators are tripped at the onset of transient instability, detected by a pattern matching algorithm. Other examples include [117–119].

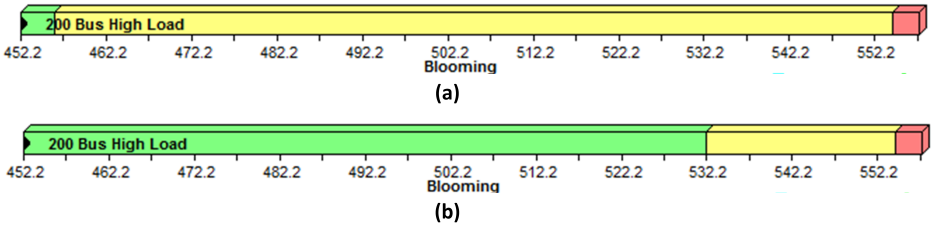

Figure 2.8: Case I: 1-D transfer analysis (a) without RAS and (b) with RAS in the synthetic Illinois 200-bus system. RAS increase the electric power transfer capacity between areas.

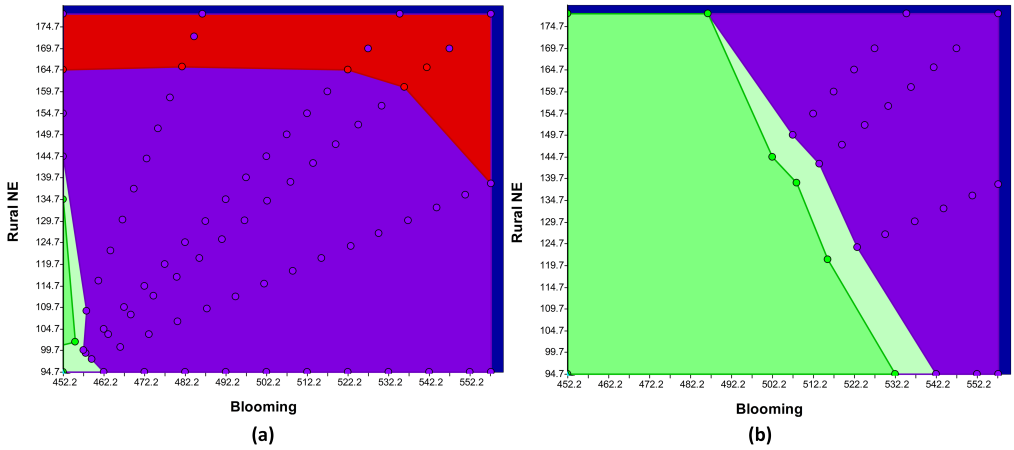

Figure 2.9: Case II: 2-D transfer analysis (a) without RAS and (b) with RAS in the synthetic Illinois 200-bus system. RAS increase the electric power transfer capacity between areas.

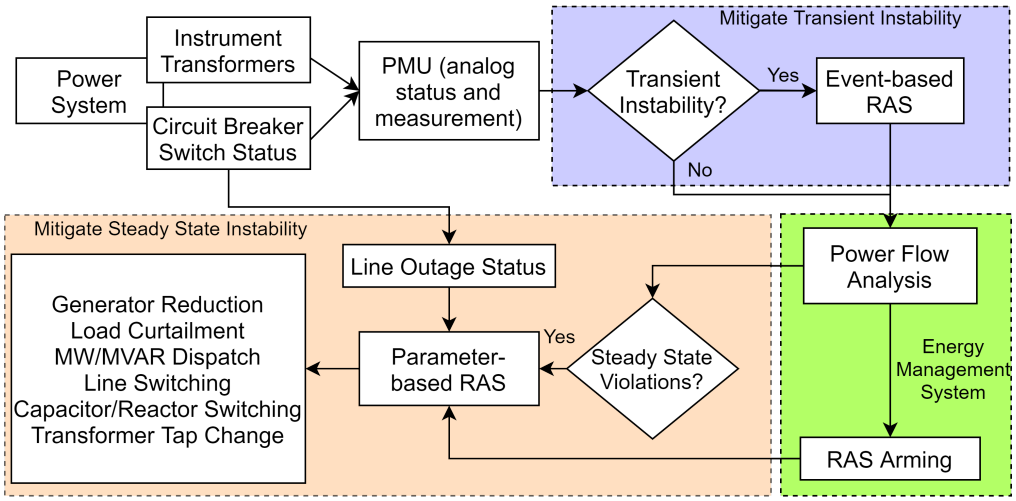

Figure 2.10: General architecture of remedial action schemes.

It is to be noted that modeling of event-based RA for mitigating transient instability is not considered in this dissertation. This is because attacks resulting in transient instability, such as switching attacks [44], are out of scope in this study. Here, we restrict our study to parameter based RAS and attacks that compromise the steady state stability of the system through false data injection attacks.

To identify locations of parameter-based RAS, a modal analysis is carried out at the point of voltage instability under maximum power transfer. This involves an Eigen analysis of the system Jacobian matrix that identifies relative participation of buses at the point of thermal or voltage instability [119]. Buses that have very high contribution to instability are identified as candidate locations for RAS.

In this dissertation, we only consider parameter-based RAS for generator reduction and (in the worst case) load curtailment. While generator re-dispatch is another viable mitigation solution, stealthy cyber attacks have been shown to result in additional line overloads with a new dispatch solution [120]. This further increases the risk of failures as the system may no longer be $N-1$ compliant. Line switching can also mitigate overloads, however topology control suffers from multiple issues - (1) topology control is a NP-hard problem, hence this approach involves high computational complexity. Additional problems include (2) sub-optimal solutions, (3) instability of switching, and (3) performance/economic issues related to re-connection of lines [121, 122]. Further, provisions for line switching, capacitor switching, and transformer tap change options may not be available at every location.

2.6 Attacks against Remedial Action Schemes

To motivate attacks against RAS, we first consider attack scenarios that trigger corrective actions. Let us consider a coordinated cyber physical attack that disconnects lines and fal-

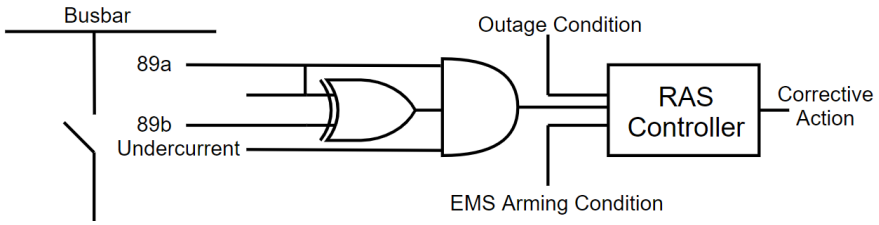

Figure 2.11: Steady state parameter-based remedial action scheme triggering logic. Line trips are detected via a combination of relay output status, circuit breaker auxiliary switch contacts (89a/89b), undercurrent (U) detection devices and EMS arming conditions.

sify measurements to mask outages. The immediate impacts of such an attack are thermal overloads of transmission lines, line disconnection, load loss and voltage instability.

Such coordinated attacks may not necessarily lead to widespread cascading failures. This is because worldwide, utilities are guided by regulations to be $N-1$ secure, and often extend security for selected $N-1-1$ and $N-2$ contingencies. In the aftermath of large blackouts, RAS are being widely deployed by utilities for fast corrective actions to increase power system security in case of critical contingencies. As discussed above, these RAS mitigate steady state thermal violations and voltage violations by reducing generator outputs or tripping loads. Targeted attacks against parameter-based RAS becomes particularly critical as it prevents system operators or automatic controls to take necessary corrective actions, thereby increasing the chances of large scale failures.

The schematic logic diagram for RAS is shown in Figure. 2.11. The central RAS controller receives field analog and digital measurements. Line trips are detected generally through relay output status and further confirmed through a combination of circuit breaker auxiliary switch contacts (89a/89b) and undercurrent (U) detection devices [115]. Under critical contingencies, the following logic is satisfied ,

$$[z_{89a} \cap (z_{89a} \oplus z_{89b}) \cap z_U] == 1 \tag{2.22}$$

and corrective actions are immediately triggered by the central RAS controller to safeguard

the system against the next set of credible contingencies.

To ensure the worst case impacts, FDIA against RAS can be carried out by altering:

1. the status of auxiliary switch contacts and disconnect switch (89A/89B) contacts,

2. the open line terminal status received by the central RAS controller.

As a result, attacks against RAS will block triggers for corrective actions. Without prompt actions, line overloads will persist beyond permitted limits. Excessive current will overheat, sag and ultimately result in unplanned outages, thereby increasing chances of cascading failures.

To disable RAS trigger signals, attackers require prior information about the target breaker and relay that communicate with the central RAS controller. Such information can be obtained by compromising communication channels and accessing relay mappings in the EMS. FDIA against RAS can be launched by embedding malicious codes or launching Denial of Service attacks against IEC 61850 generic object oriented substation events (GOOSE) protocol [123].

2.7 Attacks against Phasor Data Concentrators

Once RAS trigger circuits are disabled, physical attacks, coordinated with data falsification, are launched for maximum impact. Successful data attacks compromise the PMU-PDC communication architecture. In this dissertation, we assume that attackers target PDCs in order to falsify multiple PMU data measurements. The assumption is based on the notion that compromising PDC at local substation requires less resources on an attacker's side compared to attacking multiple PMUs scattered across a large geographic area. Such attacks can be carried out through a combination of reconnaissance, network sniffing, phishing, communication interception, spoof certificates or DDoS [124]. It is

also assumed here that attacks against PDCs incorporate in themselves attacks against the supporting communication infrastructures.

The next step in risk assessment is to calculate the probability that a PDC remains in the compromised state. A Semi-Markov approach is proposed to capture different stages of a realistic attack on a PDC. Authors in [125, 126] have used SMP to model command injection, SQL injection, man-in-the middle attacks, address resolution protocol and buffer overflow attacks against SCADA cyber physical systems. One of the drawback of the above approach is that uniformly distributed sojourn times are not realistic for practical attack scenarios. Our SMP model incorporates both exponential and non-exponential probability distributions, while closely reflects real-life attacks.

2.7.1 Proposed Semi-Markov Process

The objective of the SMP is to calculate the steady-state probability of a PDC remaining in a compromised state over the attack horizon. This is illustrated in Figure. 2.12.

Consider four different states of a PDC under attack, {**W**orking, **V**ulnerable, **A**ttacked and **R**ecovered}, denoted by [**W**, **V**, **A**, **R**] $\in$ § where § is the finite state-space. In general, there may exist other intermediate states between **A** and **R** such as masked compromised state, undetected compromised state, triage state, fail-secure state and graceful degradation state [127]. For simplicity, we absorb the intermediate states into the attacked state **A**.

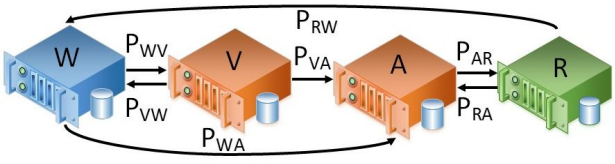

Figure 2.12: States of a phasor data concentrator - (W) Working, (V) Vulnerable, (A) Attacked, and (R) Recovered, with cumulative distributions of sojourn time P_{ij}.

When the PDC is in state **W**, assuming stochastic nature of attacks (often termed as zero-day attacks), a transition into state **V** can be modeled as an exponential distribution with rate λ_{WV}. This is because once the security is compromised and the PDC is in state **V**, chances of an actual attack increases and the system transitions to state **A**. The time spent in state **V** thus mimics a general increasing rate of failure and is modeled by a Weibull distribution (shape parameter θ, scale parameter β) with θ_{VA}, $\beta_{VA} > 1$.

On the other hand, unsuccessful attacks mimic a decreasing failure rate and the transition from **V** $\rightarrow$ **W** is modeled as a Weibull distribution with θ_{VW}, $\beta_{VW} < 1$. Transition from **W** $\rightarrow$ **A** represents an insider attack with prior system information, which is also assumed to be stochastic in nature, and is modeled using exponential distributions with λ_{WA}. Once system operators discover malicious attacks, PDCs are disconnected and patches are installed to fix the vulnerabilities. The system transitions into recovery phase. Transitions from **A** $\rightarrow$ **R** or **R** $\rightarrow$ **A** for both successful/unsuccessful patch installations are considered stochastic in nature.

For zero day attacks, a quick mitigation strategy may not be readily available given the sophistication and novelty of attack. The transition from **R** $\rightarrow$ **W** is simply modeled using an exponential distribution. The main idea of the overall process is to model actions involving increasing/decreasing rate of failures with non-exponential distributions, and stochastic actions with an exponential distribution.

The cumulative distribution functions (CDF) of the time spent in different states are summarized in Table 2.1. Using the state transitions, the steady state probabilities π_i are calculated. The steady state probabilities represent the proportion of time the PDC spends in different states i over the total attack horizon. The detailed mathematical modeling of the semi-Markov Process is discussed next.

Table 2.1: Cumulative Distribution Functions of Time Spent in Different Stages of Attacks

CDF	Distribution	Parameters	Expression
P_{WV}	Exponential	λ_{WV}	$1 - e^{-\lambda_{WV}t}$
P_{WA}	Exponential	λ_{WA}	$1 - e^{-\lambda_{WA}t}$
P_{VW}	Weibull (DFR)	β_{VW}, θ_{VW}	$1 - e^{-(\frac{t}{\beta_{VW}})^{\theta_{VW}}}$
P_{VA}	Weibull (IFR)	β_{VA}, θ_{VA}	$1 - e^{-(\frac{t}{\beta_{VA}})^{\theta_{VA}}}$
P_{AR}	Exponential	λ_{AR}	$1 - e^{-\lambda_{AR}t}$
P_{RW}	Exponential	λ_{RW}	$1 - e^{-\lambda_{RW}t}$
P_{RA}	Exponential	λ_{RA}	$1 - e^{-\lambda_{RA}t}$

2.7.2 Sojourn Time and Transition Probability of Semi-Markov Process

For the Semi-Markov Process (SMP), the system state evolution is described by three chains: (1) $J = (J_n)_{n\in\mathbb{N}}$ where J_n is the system state at the n^{th} time, (2) $S = (S_n)_{n\in\mathbb{N}}$ where S_n is the n^{th} transition time and (3) $X = (X_n)_{n\in\mathbb{N}}$ where $X_n = S_n - S_{n-1}$ is the sojourn time in state J_{n-1} [128]. The chain $(J_n, S_n)_{n\in\mathbb{N}}$ is a Markov renewal chain if $\forall n \in \mathbb{N}$,

$$\begin{aligned} P(J_{n+1} = j, S_{n+1} - S_n = k | J_0, S_0, .., J_n, S_n) = \\ P(J_{n+1} = j, S_{n+1} - S_n = k | J_n) \end{aligned} \tag{2.23}$$

Equation (2.23) denotes that the next transition state and time spent in the present state depend only on the present state of the system. The semi-Markov chain $Z = (Z_k)_{k\in\mathbb{N}}$ associated with the Markov renewal process (J, S) is $Z_k = J_{N(k)}$. Here $N(k)$ represents the number of transitions that occur by time k. The average sojourn time that the SMP spends at each state is evaluated according to,

$$t_i = \int_0^\infty (1 - \mathrm{P}_{ij}(k))(1 - \mathrm{P}_{ik}(k))dk \tag{2.24}$$

where j, k are reachable states from i and $(1 - \mathrm{P}_{ij}(k))$ is the survival function of sojourn time in the state i.

Once state transitions are defined, the average sojourn time that the system stays in a particular state i can be calculated. For example, using equation (2.24), the sojourn time

in state **W** with an exponential distribution is written as,

$$t_1 = \int_0^\infty \overline{P}_{WV}\overline{P}_{WA}dt = \int_0^\infty e^{-(\lambda_{WV}+\lambda_{WA})t}dt \tag{2.25}$$

Similarly, the sojourn time in state **V** having a Weibull distribution is written as,

$$t_2 = \int_0^\infty \overline{P}_{VW}\overline{P}_{VA}dt = \int_0^\infty e^{-(\frac{t}{\beta_{VW}})^{\theta_{VW}}-(\frac{t}{\beta_{VA}})^{\theta_{VA}}}dt \tag{2.26}$$

Sojourn times for state **A** and **R** can be written similarly.

For the evolution of this SMP, a transition probability matrix Q is defined. The elements of $Q = Q_{ij}(k)$ represent the probability of transition from state i to j within time k and are defined as,

$$Q_{ij}(k) = P(J_{n+1} = j, X_{n+1} \leq k | J_n = i) \tag{2.27}$$

If P_{ij} denotes the cumulative distributions of sojourn time in state i corresponding to next state j, the elements of the kernel Q can be evaluated as [129],

$$Q_{ij}(k) = \int_0^k (1 - \mathrm{P}_{ik}(k))d\mathrm{P}_{ij}(k) \tag{2.28}$$

where j, k are reachable states from i and $(1 - \mathrm{P}_{ij}(k))$ is the survival function of sojourn time in the state i.

From Figure. 2.12, the transition probability matrix Q can be formulated as,

$$Q = \begin{bmatrix} 0 & Q_{WV} & Q_{WA} & 0 \\ Q_{VW} & 0 & Q_{VA} & 0 \\ 0 & 0 & 0 & Q_{AR} \\ Q_{RW} & 0 & Q_{RA} & 0 \end{bmatrix} \tag{2.29}$$

where Q_{ij} denote the probabilities as the system transitions from state i to j. Using equation (2.28) , the element Q_{WV} can be written as,

$$Q_{WV} = \int_0^t \overline{P}_{WA}(t) dP_{WV}(t) = \frac{\lambda_{WV}}{\lambda_{WA} + \lambda_{WV}} [1 - e^{-(\lambda_{WA} + \lambda_{WV})t}] \tag{2.30}$$

Similarly, the element Q_{VW} can be written as,

$$\begin{aligned} Q_{VW} &= \int_0^t \overline{P}_{VA}(t) dP_{VW}(t) \\ &= \frac{\theta_{VW}}{\beta_{VW}^{\theta_{VW}}} \int_0^t t^{(\theta_{VW}-1)} e^{-[(\frac{1}{\beta_{VA}})+(\frac{1}{\beta_{VW}})]t} dt \end{aligned} \tag{2.31}$$

Assuming state transitions are independent of time, the one-step transition probability matrix in the steady-state analysis of the SMP is computed as $M = Q(\infty)$. Next, using M, the steady state probability vector of the embedded Markov chain $\mathbf{v} = \{v_1, v_2, ..., v_n\}$ can be calculated by solving the set of linear equations, $\mathbf{v} = \mathbf{v}M$ with $\sum_{i=1}^{n} v_i = 1$. The steady state probabilities π_i are then evaluated as,

$$\pi_i = \frac{v_i t_i}{\sum_{\S} v_i t_i}, \quad i \in \S \tag{2.32}$$

As noted previously, the steady state probabilities represent the proportion of time a PDC spends in different states i over the total attack horizon. The attack probabilities are used to investigate the risk-impact analysis for the coordinated false data injection and physical attack.

2.8 Risk-Impact Analysis

To summarize, coordinated cyber attack considered in this dissertation is carried out in two steps - (1) RAS trigger signals are disabled first, followed by (2) stealthy cyber physical attacks launched through compromised PDCs to mask physical line outages. The impact of coordinated attacks is (1) directly quantified as the amount of load not served after cascading failures, and further extended to assess (2) the loss of observability under both cascading failures and controlled islanding scenarios, as well as (3) the degree of recoverability of the grid after an attack. Considering post-attack impact analysis results in a

more comprehensive impact assessment as compared to the state-of-the-art.

2.8.1 Attack Impacts due to Cascading Failures

To estimate the direct consequences of coordinated false data injection attack, a distributed slack bus (DS) cascading failure algorithm [130] is utilized. This estimates (1) whether attacks actually lead to widespread cascades, and (2) the quantifies impact in terms of total load lost. The DS power-flow is based on the participation factors of the generators in the pre-contingency state [131, 132],

$$PRTCF_i = \frac{Pg_i}{\sum_{j=1}^{N_g} Pg_i} \tag{2.33}$$

where Pg_i is the i^{th} generated power for the set of N_g generators. The generation-load mismatch Err is given as,

$$Err = max(tot_{load} + loss - Dispatch_{gen}, 0) \tag{2.34}$$

This mismatch is distributed among the current generators in the system based on their percentage of participation in total generation capacity. The new generation becomes,

$$Pg_i^{new} = Pg_i^{old} + Err + PRTCF_i \tag{2.35}$$

The cascading failure algorithm starts with a secure power flow solution at a given transfer point. Under RAS attacks, a set of parent lines become overloaded. Parent lines are disconnected to mimic physical failure and further analyzed for the next set of overloads and failures using AC power flow analysis. The cascading process stops (1) when there are no more line overloads or (2) when the power flow solution diverges. The cascading failures results are stored in a database for further analysis. The total EENS is calculated as,

$$EENS = \Delta D = \frac{\sum_{i \in L'} P_i}{\sum_{i \in L} P_i} \tag{2.36}$$

where $L' \subset L$ is the set of surviving load buses in the network after cascading failure with corresponding load P_i.

If a set of $\mathbb{P}$ data concentrators are compromised to launch a successful attack, the associated risk $\mathcal{R}_{FDIA}$ is evaluated as,

$$\mathcal{R}_{FDIA} = \text{Total Attack Probability} \times \Delta D = \prod_{\mathbb{P}} \pi_A^{\mathbb{P}} \times \Delta D \tag{2.37}$$

where π_A is the steady state probability of a PDC under attack. The risk index $\mathcal{R}_{FDIA}$ takes into account (a) the ease of launching successful cyber attacks through vulnerable PDCs and (b) the corresponding load lost under uncontrolled cascading failure as a direct consequence of the attack.

2.8.2 Loss of Observability after Cascading Failures

While most impact assessments consider direct physical consequences such as the amount and the type of load not served, and percentage of line overloads, the analysis in this dissertation is extended to quantify the loss of observability after cascading failures due to line outages and elimination of untrustworthy PDCs.

For a completely observable system, sufficient measurements are available to correctly estimate all system states. Optimal PMU placements are intended to ensure complete observability with adequate PMU measurements [133]. The placements of PMUs can further be extended to ensure observability due to loss of line, loss of measurement or considering controlled islanding [134]. Loss of observability is directly associated with risks of incorrect state estimation solution and problems during island re-synchronization.

Consider the linearized DC power flow where power flow measurements and bus voltage angles (states) are expressed as,

$$P_{ij} = \theta_i - \theta_j \tag{2.38}$$

With sufficient measurements, the relationship between the measurements and states is,

$$z = H\theta \tag{2.39}$$

where H is the system Jacobian matrix. The states are estimated from the measurements by,

$$\hat{\theta} = (H^T H)^{-1} H^T z = (G)^{-1} H^T z \tag{2.40}$$

where $G = (H^T H)$ is the gain matrix. If there exists sufficient number of bus voltage and current phasors measured by PMUs, the rank of the gain matrix is n, where n is the number of system buses. When the system is not completely observable, the upper triangular factor of G obtained using $LU-$decomposition has zero pivots corresponding to unobservable buses. For example, consider the topological Jacobian matrix H for a toy 9-bus system shown in Figure. 2.13(a),

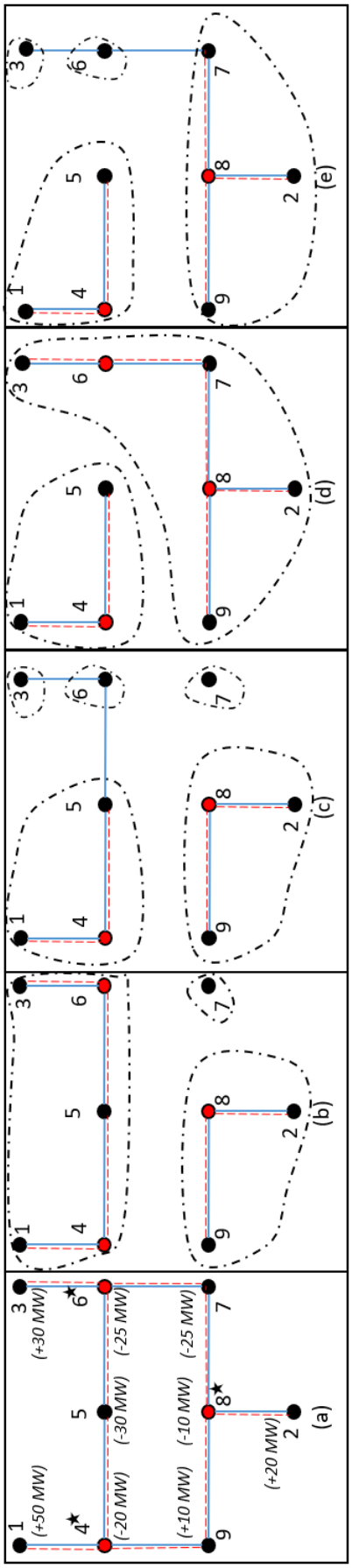

Figure 2.13: (a) Original fully observable 9 bus system with PMUs/PDCs at bus $4, 6$ and 8. (b) physical and observable/unobservable islands after cascading failure due to coordinated attacks, (c) increase in the number of unobservable islands after suspicious PDC at bus 6 is removed. (d) To prevent cascading failures, the system is partitioned into stable islands (controlled islanding) with 0 MW imbalance in each island, and (e) loss of observability after suspicious PDC at bus 6 is removed.

$$
H = \begin{array}{c} \\ I_{4-1} \\ I_{4-5} \\ I_{4-9} \\ I_{6-3} \\ I_{6-5} \\ I_{6-7} \\ I_{8-2} \\ I_{8-7} \\ I_{8-9} \\ V_4 \\ V_8 \\ V_6 \end{array}
\begin{array}{c}
\begin{array}{ccccccccc} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} & \mathbf{9} \end{array} \\
\begin{pmatrix}
-1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{pmatrix}
\end{array}
$$

Both the topological Jacobian matrix and the corresponding Gain matrix have full-rank, and the system is a single observable island.

When attacks result in cascading failure and unintentional partitioning of the system, multiple physical islands are formed. The number of physical islands can be obtained by calculating the total number of connected sub-graphs in the power network using Kosaraju's algorithm [135]. Let for the 9-bus system, attacks are launched from PDC at bus 6. The resulting system in the aftermath of coordinated attack is shown in Figure. 2.13(b). The new connectivity matrix organized by clustering each individual island is obtained as,

$$A' = \begin{bmatrix} A_1 & A_2 & A_3 \end{bmatrix} =$$

	1	**3**	**4**	**5**	**6**	**2**	**8**	**9**	**7**
l_{4-1}	-1	0	1	0	0	0	0	0	0
l_{4-5}	0	0	1	-1	0	0	0	0	0
l_{6-3}	0	-1	0	0	1	0	0	0	0
l_{6-5}	0	0	0	-1	1	0	0	0	0
l_{8-2}	0	0	0	0	0	-1	1	0	0
l_{8-9}	0	0	0	0	0	0	1	-1	0

The connectivity matrix and the system Jacobian matrix are organized according to the size of the physical islands, for example, rank(A_1) $\geq$ rank(A_2) $\geq \cdots \geq$ rank(A_n). This is because we are interested in the largest surviving island post-attack.

After successful attacks have already impacted the system, operators may rely on partial knowledge on attacks to identify vulnerable PDCs. Attacks may be identified by analyzing signatures on the time series data [136, 137]. All measurements, corresponding to vulnerable PDCs and outaged lines, are removed from H. Removal of measurements lead to the formation of a number of unobservable islands. In this scenario, when vulnerable PDC 6 is removed, the new H matrix corresponding to Figure. 2.13(c), organized by the largest physical islands, is,

$$H' = \begin{bmatrix} H_1 & H_2 & H_3 \end{bmatrix} = \begin{array}{c} \\ I_{4-1} \\ I_{4-5} \\ I_{8-2} \\ I_{8-9} \\ V_4 \\ V_8 \end{array} \begin{array}{c} \begin{array}{ccccc|ccc|c} \mathbf{1} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{2} & \mathbf{8} & \mathbf{9} & \mathbf{7} \end{array} \\ \left(\begin{array}{ccccc|ccc|c} -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \end{array}$$

To quantify the observability of the largest physical island, an index referred to as the *Loss of Observability after Cascading Failure* (LOCF), is proposed,

$$LOCF = \frac{n_1 - rank(H_1)}{rank(A_1)} \tag{2.41}$$

where n_1 is the number of buses in the largest island. For Figure. 2.13(c), the LOCF = $\frac{5-3}{5} = \frac{2}{5}$. In other words, 40% of the largest surviving grid has lost observability.

The LOCF index is a measure of the extent to which state estimation of the largest island is lost. Loss of large number of measurements and subsequent use of pseudo-measurements have been shown to produce undesirable SE solutions, resulting in gross errors in estimated voltage angles [138]. Loss of observability also adversely affects grid re-synchronization process when remaining smaller islands are connected to the main island.

2.8.3 Loss of Observability after Controlled Islanding

Often, when the system evolves through cascading failures, intentional controlled islanding is used as a last resort to prevent a total system collapse. Timely taken controlled islanding decisions damp large oscillations and separate the system into smaller stable islands that can be rapidly restored [139]. The details of controlled islanding are presented

in Chapter 4. Here, controlled islanding is assumed to be triggered when multiple lines are outaged during the evolution of cascading failures. To quantify the impact of attacks on the resulting islands due to line outages and elimination of untrustworthy PDCs, a new index, *Loss of Observability after Controlled Islanding* (LOCI), is developed.

Let the power system be partitioned into $h = \{1, ..., k\}$ islands based on real-time load-generation. Figure. 2.13(d) shows the partitions obtained for the 9-bus system. Both the H and the A matrices are re-organized corresponding to individual islands. The outaged lines and suspicious PDC measurements are subsequently removed as shown in Figure. 2.13(e) and the matrix H is updated. To quantify the observability in newly formed islands, the LOCI for the h^{th} island is formulated as,

$$LOCI_h = \frac{n_h - rank(H_h)}{rank(A_h)} \tag{2.42}$$

Here, n_h is the number of buses, H_h and A_h are the corresponding Jacobian and connectivity matrix respectively for the h^{th} island. For Figure. 2.13(e), loss of observability for island 1 is measured as $LOCI_1 = \frac{6-4}{6} = 33\%$ and for island 2 is $LOCI_2 = \frac{3-3}{3} = 0\%$.

Similar to LOCF, LOCI helps determine the number of pseudo-measurements to be added for a feasible state estimation solution when the new islands are operating as individual self-sustainable grids. Bigger physical islands with large number of observable buses are desired for a more reliable operation of the power system. The problem of creating maximally observable islands is later discussed in Chapter 4.

2.8.4 Lines Recoverable after Controlled Islanding

After controlled islanding partitions the system, the next step is to synchronize the individual islands. Contemporary method of reconnecting lines uses synchroscopes to observe the difference in the standing phase angles between the two substation buses, which is around

50° to 60° for 132kV and lower, 30° to 40° for 230kV lines, and 20° for lines 400kV and above [140].

As stable islands are created based on the real-time load-generation conditions, the candidate set of transmission lines to be disconnected is not fixed. This is unlike traditional approaches where pre-selected transmission lines are disconnected. Hence, the availability and subsequent usage of PMUs cannot be assumed at all buses. Only buses with PMUs can directly observe the system states [141], and hence can be utilized for re-synchronization.

To this end, we develop an index, *Lines Recoverable after Controlled Islanding* (LRCI), which reflect the extent of recoverability of a power system considering re-synchronization of the smaller islands.

When buses are observable at the two ends of outaged lines (after controlled islanding), the remaining islands can be reconnected. Let $E_{i,j}$ be a line between node i and j. The binary variable γ denotes the status of the line: $\gamma_{i,j} = 0$ indicates line outage and $\gamma_{i,j} = 1$ indicates line in service. Let O be the set of observable buses obtained from LU factorization of the Gain matrix. The sets of outage and recoverable branches are defined respectively as,

$$\mathbb{S}^{out} = \{(i,j) : E_{ij}, \forall \gamma_{i,j} = 0\}$$

$$\mathbb{S}^{rec} = \{(i,j) : E_{ij} \in \mathbb{S}^{out}, i \in O, j \in O\}$$

To quantify the recoverability of the power grid, the LRCI is defined as,

$$LRCI = \frac{\text{Recoverable branches}}{\text{Outaged branches}} = \frac{|\mathbb{S}^{rec}|}{|\mathbb{S}^{out}|} \tag{2.43}$$

This index measures the number of outaged lines between different islands whose end buses are both observable and can be safely reconnected.

From Figure. 2.13(e), it can be seen that line 5-6 cannot be connected as bus 6 is not

observable. However, line 4-9 can be used to re-synchronize the islands as both buses 4 and 9 are either directly or indirectly observable by PMUs.

Apart from the loss of observability and degree of recoverability of the grid, the physical impact is also quantified as the total transmission MW power flow capacity lost corresponding to all lines that are not recoverable. This is important as unavailable transmission lines cannot be used for power dispatch, essentially constraining the economic dispatch algorithm.

2.9 Simulation Results

In this section, the impacts of coordinated attacks are evaluated on synthetic Illinois 200-bus and South Carolina 500-bus test cases. All analyses are performed using DSATools™, Gurobi and MATLAB on an Intel(R) i5-4460 CPU @ 3.20GHz 16 GB RAM.

2.9.1 Scenario Setup

The 200-Bus system is a synthetic test bed of a central part of Illinois with 245 transmission lines (both 230 kV and 115 kV), 49 generators, and six areas. The 500-bus system is a synthetic power system of South Carolina with 13.8kV, 138kV, and 345kV lines, 90 generators, and two areas [142]. The test case details are presented in Table 2.2. The zonal generation-load imbalance is shown in Table 2.3. These zonal imbalances determine the power transfers between different areas of the system.

The six zones for the 200 bus system are shown in Figure. 2.14. Rural NE and Blooming are generation rich while Champaign and Rural SW are load rich. Different voltage levels and lines with flow above 50 MW are illustrated in Figure. 2.15 and Figure. 2.16 respectively. Major tie lines are shown in Figure. 2.17.

Three different 1-D and 2-D power transfers up to maximum limits are considered. At

Table 2.2: Basecase Scenarios

Base-case	Lines	Gen (MW)	Load (MW)	Loading
200 bus	245	1771	1750	60 %
500 bus	597	6568	6500	74 %

the point of instability during contingencies, modal analysis is used to identify parameter-based RAS locations. For example, line 81-55 is a major and only tie-line between Rural NE and Blooming that carries 94 MW. Loss of 81-55 increases the power flow between Blooming and Champaign from 189 MW to 262 MW, overloading 187-121. With RAS, the output of generator 189 is reduced to 530 MW. A total of 29 such RAS are identified, a few of which are shown in Table 2.4.

The three major power transfer cases investigated are,

1. **Case I:** $1-$D transfer between Blooming and Rural SW: transfer is limited by multiple contingencies at 452MW. With RAS, the transfer capability increases to 532 MW, as shown in Figure 2.8.

2. **Case II:** $2-$D transfer from Blooming and Rural NE to Rural SW: With RAS, Blooming and Rural NE can supply additional 50 MW and 90 MW respectively as shown in in Figure 2.9.

3. **Case III:** $1-$D transfer between Springfield and Champaign: RAS increase transfer from 94 MW to 314 MW.

For 500 bus system with two regions, the maximum transfer between Upstate and Midlands with RAS is 4206 MW.

2.9.2 Attack Probability of Phasor Data Concentrators

False data attacks are launched by infiltrating the PMU-PDC communication architecture. The probability of a PDC being in a vulnerable state is calculated using the Semi-Markov

Table 2.3: Zonal Load-Generation Imbalance

Case	Zone	Name	Generation (MW)	Load (MW)	Imabalnce (MW)
200 Bus	2	Peoria	386.82	536.81	-149.99
	3	Springfield	94.3	159.22	-64.92
	4	Rural SW	70.32	270.06	-199.74
	5	Champaign	5.64	275.16	-269.52
	6	Rural NE	94.66	81.31	13.35
	7	Blooming	1120.87	427.44	693.43
500 Bus	1	Upstate	4192.15	4119.05	73.10
	2	Midlands	2376.25	2380.83	-4.58

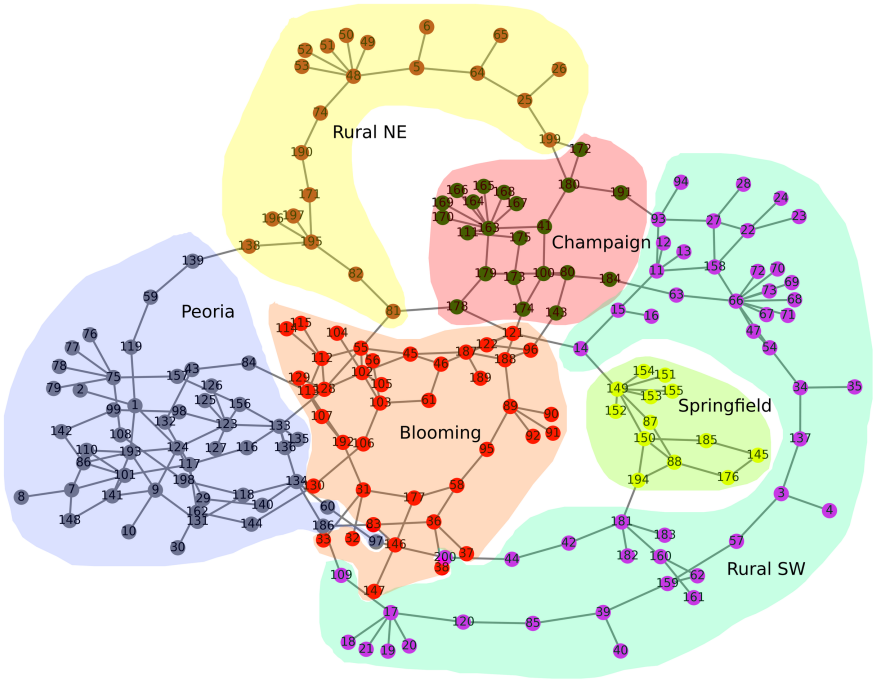

Figure 2.14: Six different zones in the Illinois 200 bus system

Table 2.4: Examples of Few Parameter-Based RAS for the 200 Bus System

Critical Contingencies	Overload	Remedial Action
81-178, 81-55,174-188, 174-188 186-109,134-60, 60-97, 143-96	16-15 or 187-121	Gen 189 decrease to 530 MW
199-25	16-15 or 187-121	Gen 65 decrease by 60 MW
45-187	187-121	Shed 100% Load at 181 Shed 30% Load at 129

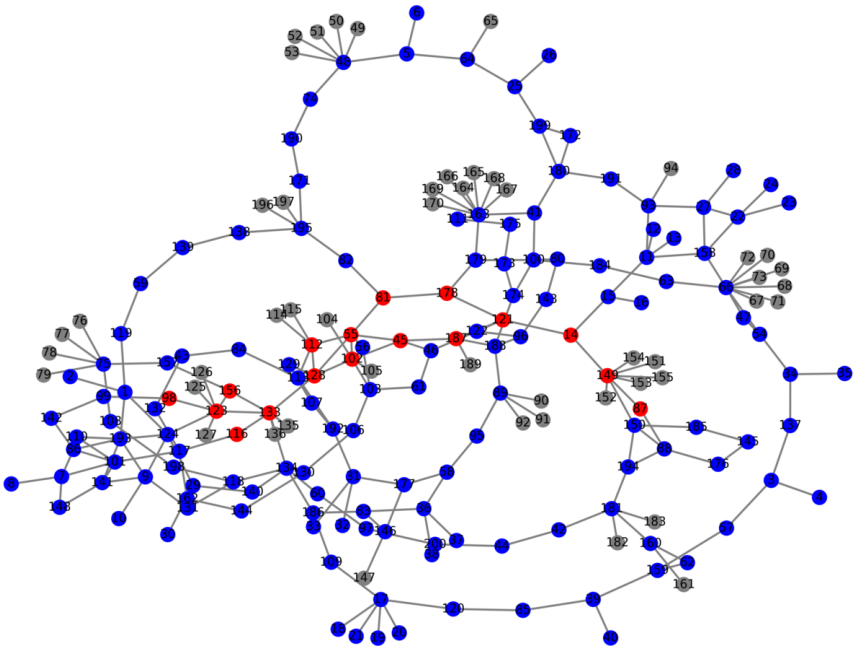

Figure 2.15: Different Voltage levels: (Red - 230 kV, Blue - 115 kV). The 230 kV lines form the backbone of the Illinois 200 bus system.

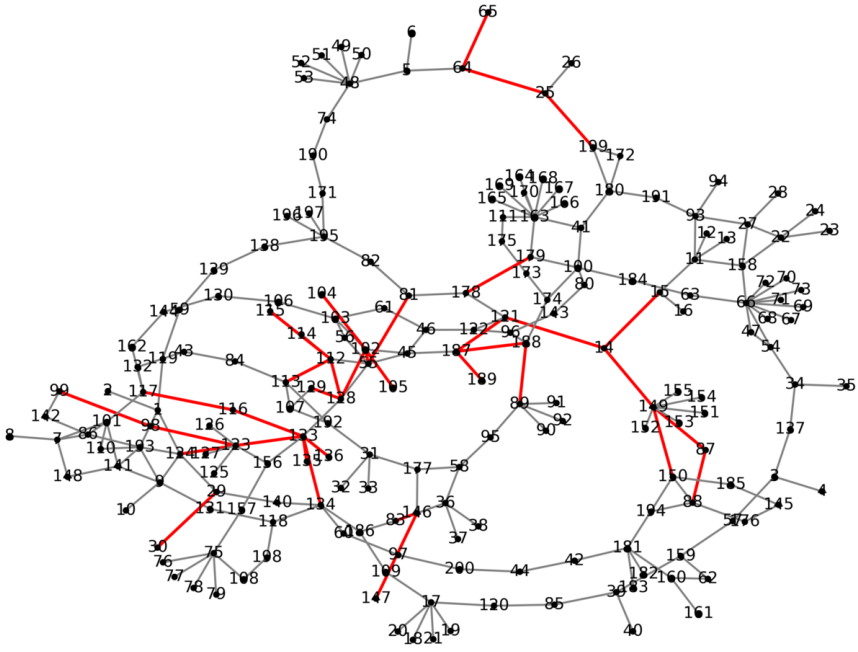

Figure 2.16: Lines with flow greater than 50 MW in the Illinois 200 bus system

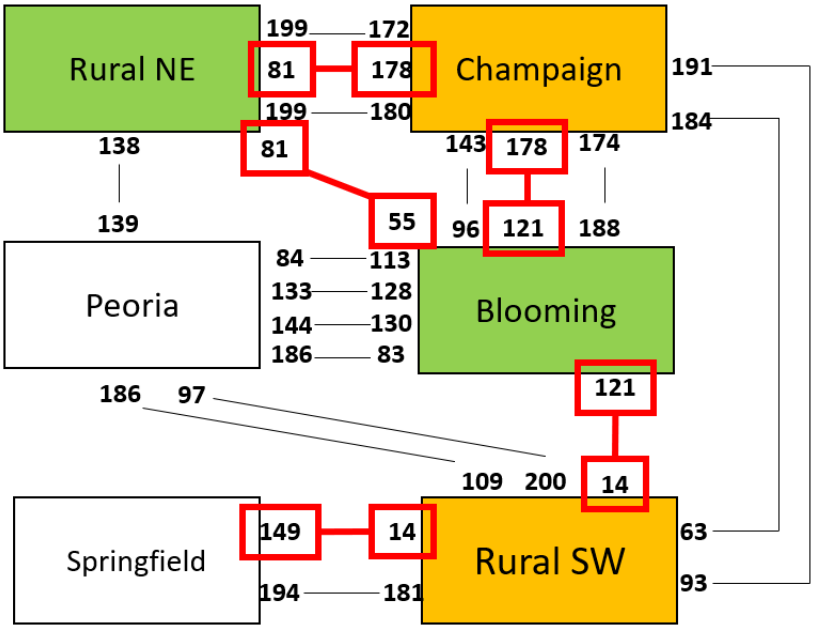

Figure 2.17: Inter-area tie-lines in the 200 bus system. The tie-lines responsible for major power transfer between different areas are highlighted. These tie-lines are a part of the 230 kV backbone.

process. Since attack statistics on PMU-PDC based SE are not publicly available, the probability distribution parameters are modeled following a realistic attack [112] - $\lambda_{WV} = 5/12$, $\lambda_{WA} = 1/12$, $\beta_{VW} = 0.99$, $\theta_{VW} = 0.5$, $\beta_{VA} = 1.5$, $\theta_{VA} = 2.7$, $\lambda_{AR} = 1$, and $\lambda_{RA} = 1$. For utilities, these parameters can be obtained from historical data of failures, attacks and recovery times. Using the above parameters, one-step transition probability matrix M, the sojourn time spent by PDC at each state, and transition probability matrix of the embedded Markov chain are calculated. Finally, the steady state probabilities of PDC are evaluated as, $\pi_W = 0.3009, \pi_V = 0.1669, \pi_A = 0.2852, \pi_R = 0.2470$.

2.9.3 Attack Impacts: Cascading Failure and Load Loss

To launch attacks through compromised PDCs, the attack neighborhoods are first identified using [5]. These attack neighborhoods contain the minimum number of measurements required to compromise (NMRC) the system. Figure. 2.18 shows the attack neighborhood for the two systems.

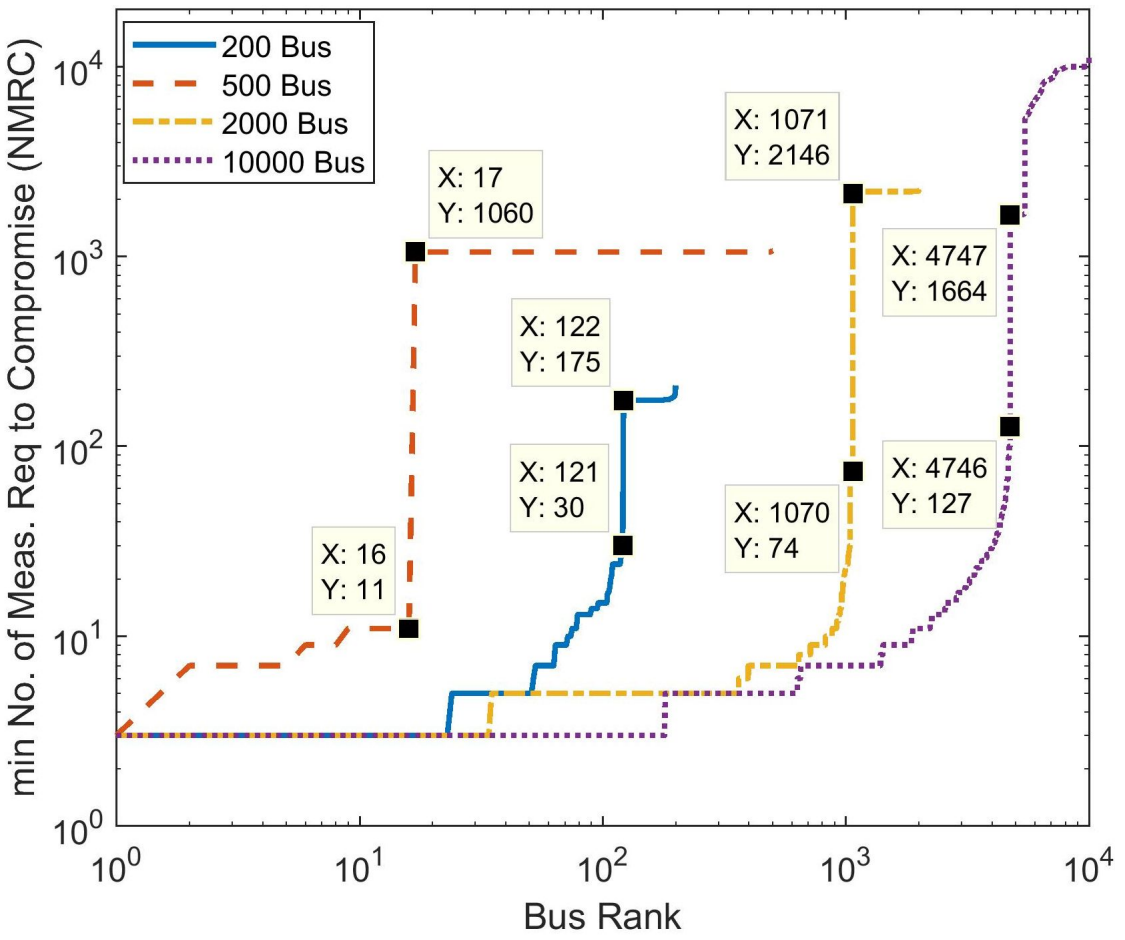

Figure 2.18: Size of false data injection attack neighborhood - all buses are ranked and sorted based on the minimum number of measurements required to compromise (NMRC) the system. A large jump in minimum NMRC is observed due to the distribution of zero-injection buses and is referred to as the NMRC-gap. All buses that precede the NMRC-gap need lesser effort to be compromised and are labeled as low-NMRC buses. For example, point $(16, 11)$ represents 16 out of 500 buses require 11 or less measurements to be altered. The point $(17, 1060)$ illustrates that a successful attack requires at least 1060 measurements to be altered for the remaining buses to be compromised. Similar observations are made for the remaining systems.

In this study, single and multiple line outage attacks are considered under maximum power transfers. Additionally, coordinated false data injection attacks are launched from the attack neighborhoods to mask line outages.

Attacks Disconnecting Single Lines

For all the three power transfer scenarios in the 200 bus system, 93 attackable candidate lines are identified from the set of low-NMRC buses. The selected lines have load injection buses in the attack neighborhood which are compromised to launch coordinated attacks. No cascading failures are observed for **Case I** and **Case II**, even after increasing the system loading by 80.68% of its original value. One example of a case where a cascading outage occurred is as follows:

- **Case III**, disconnection of line 143-96: A careful investigation of the system conditions prior to the outage revealed that Springfield is importing 314 MW from Champaign through Blooming. Line 143-96 has 76 MW of power flow and is a part of the interface between Blooming and Champaign. Under normal circumstances, the failure of line 143-96 triggers RAS that result in the reduction of generator 189 output from 638 MW to 530 MW. With RAS attacks, loss of 143-96 leads to line power flow increase in lines 188-174, 80-143, and 179-178. Sustained overloads on line 179-178 result in overloading and subsequent disconnection of multiple lines, leading to severe low voltages on several buses. Figure. 2.19 shows the changes in the power flow of lines in the vicinity of the largest generator for the first two generations of cascades. It is however to be noted that this coordinated attack requires compromising PDCs from both Champaign and Blooming.

For the 500 bus system, the following 14 lines are found attackable: {100-99, 101-99, 99-465, 109-108, 108-472, 108-495, 186-185, 445-185, 185-467, 280-279, 279-340, 279-468, 341-340 and 445-461}. At maximum transfer, coordinated false data attacks did not

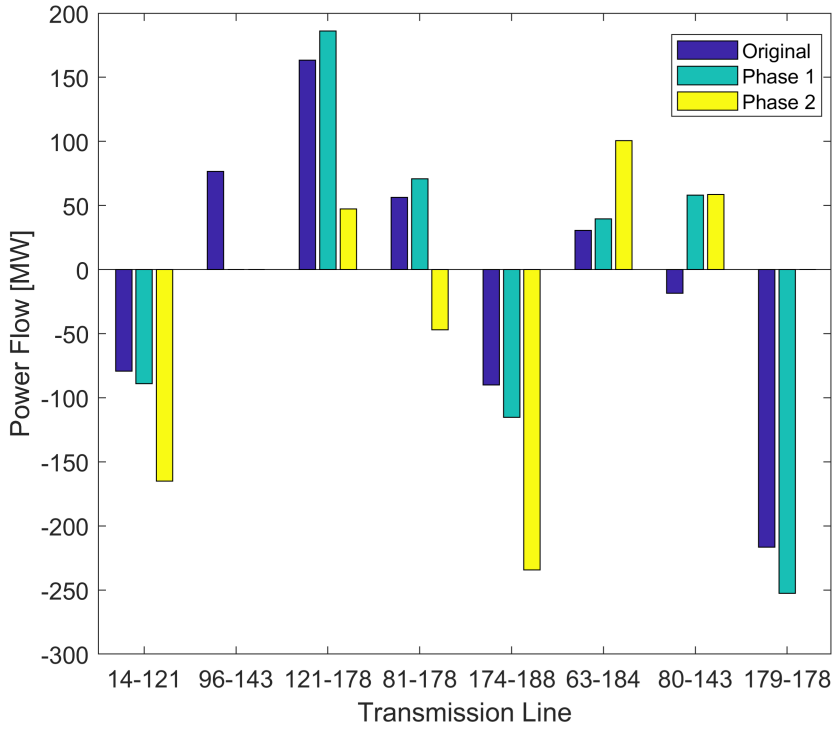

Figure 2.19: Changes in line flows in the vicinity of the largest generator bus, 189, for first two phases of cascading failure in the 200 bus system for Case III, where attacks disable RAS associated with line 143-96.

result in widespread cascades. However, attacks resulted in subsequent line overload and load shedding, which corroborated the findings in [29, 30]. In all the case studies, the transient stability of the system was verified for the single line disconnection to ensure the attacks are not discovered by the system operators.

Attacks on Multiple Lines

Attacks disconnecting multiple lines are considered next. Attacks involving many simultaneous line outages, such as those described in [29] disconnecting seven lines, are extremely aggressive and have higher chances of quick discovery. This study restricts to stealthy double line outages that are comparatively easier to conceal. All attack scenarios are considered under both basecase and maximum power transfers. The number of all the possible $N-2$ outages under an attack are shown in Table 2.5. For each case, transient stability is verified to ensure the attacks remain undiscovered.

Table 2.5: All Possible Line Failures for 200 Bus

Basecase	All N-1	N-1 (Attack)	All N-2	N-2 (Attack)
200 bus	245	93	$\binom{245}{2}$=29890	$\binom{93}{2}$=4278
500 bus	597	14	$\binom{597}{2}$=177906	$\binom{14}{2}$=91

Table 2.6: N-2 Contingency Analysis for 200 Bus Basecase under Attack

Contingency	Outage Branch	Impact	Cascade
A35-48	48-74, 82-195	Voltage Collapse	Yes
A42-96	60-97, 186-109	Thermal Overload	No
A50-80	83-146, 146-177	Thermal Overload	Yes

For attacks on the 200 bus system basecase, only 2 out of 4278 $N-2$ outages caused cascading failures. Disconnection of lines 83-146 and 146-177 in the vicinity of the generator bus 147, supplying 122 MW, resulted in overload of line 187-121. Under normal conditions, RAS reduce the generation output of bus 189. When RAS is disabled under attack, line overloads leads to physical outage, subsequent line overloads and generator outages, resulting in a total voltage collapse. The impacts are concisely summarized in Table 2.6. While several other N-2 outages also caused voltage instability or line overloads, such lines may not be easily attackable due to the high number of load injection buses needed to be compromised for a successful attack.

Next, attacks under maximum transfers are investigated. For **Case I** and **Case II**, no RAS attacks resulted in cascading failures. For **Case III**, 7 out of 4278 RAS attacks resulted in large load loss, between 1100 MW - 1970 MW, with the rest causing minimal load loss of mostly radial buses. Results for cascading failures, the compromised set of PDCs, the number of physical islands formed, and the associated risks are summarized in Table 2.7.

For the 500 bus system, RAS attacks causing double line outage did not result in cascading failures. A maximum of 7% of the total 7750 MW load was lost under attacks. The candidate lines disconnected under attack scenarios include {31-205, 185-467}, {31-218, 185-467}, {185-467, 279-340}, {185-467,279-468 },{40-39, 445-185} and {39-332, 445-

Table 2.7: Risk analysis of RAS attacks due to cascading failures for Case III

No.	Branch Outage	Attacked PDC	Load Lost	Physical Islands	Normalized Risk
C1	63-184,100-184	5	1102.97	2	0.3444
C2	41-180,63-184	4,5	1970.05	200	0.1754
C3	96-143,100-184	5,7	1936.42	187	0.1724
C4	41-180,100-184	4,5	1187.51	2	0.1057
C5	93-191,63-184	5,7	1152.93	6	0.1026
C6	93-191,96-143	4,5,7	1970.05	200	0.05003
C7	63-184,96-143	4,5,7	1936.42	186	0.04918

185}. Successful attacks are launched either by compromising PDC 1 or PDC 2.

From the above simulation results, it is noted that attacks lead to loss of load and unintentional islanding, however, not all attacks necessarily result in cascading failures. The two reasons for low probability of cascading failures due to cyber attacks are as follows: (1) Attack neighborhoods are surrounded by load injection buses with no generators or transformers inside. When the lines connected to these load clusters are lost, power is rerouted. This is significantly less severe than losing generators, transformers, tie-lines, or heavily loaded lines in the vicinity of large generators, which often initiate cascades. When radial loads are lost as a result of an attack, the power flow of lines serving the load decreases, reducing the chances of a cascade; (2) the feasibility of attack also depends on the distribution of zero-injection buses. For example in Figure. 2.18, 97.4% of buses in the 500 bus system require 1060 or more measurements to be altered for a stealthy coordinated attack. In such cases, attackers need an extensive attack budget to launch successful attacks, which may not be practical.

2.9.4 Post-Attack Impacts: Observability and Recoverability

Post-attack impacts on loss of observability are considered in this section. It is to be noted that loss of observability is assumed to be caused both due to loss of lines after cascading failure and elimination of untrustworthy PDC measurements. Specifically, seven candi-

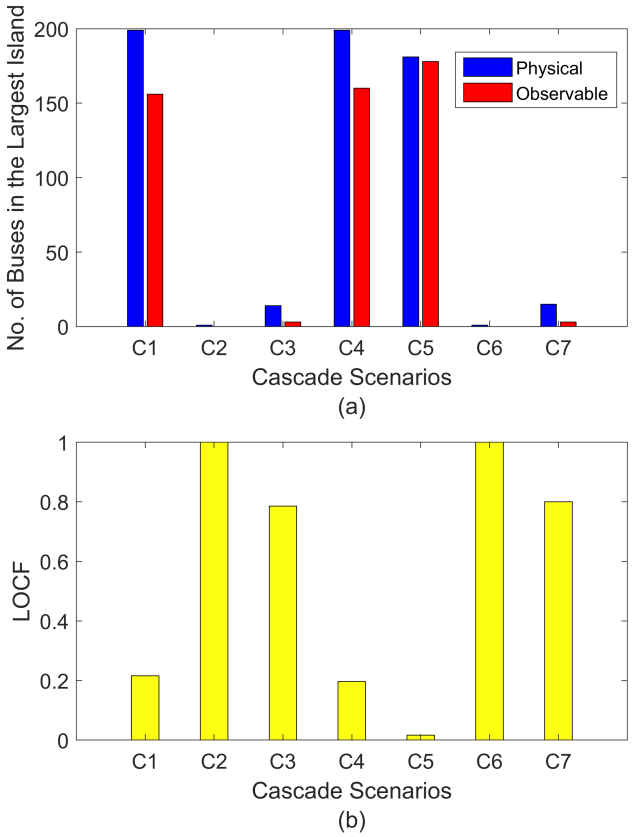

Figure 2.20: Results for cascading failure scenarios C1-C7 - (a) total number of observable buses in the largest physical island. Note their are multiple smaller islands which is a direct consequence of uncontrolled cascading failures, and (b) the corresponding Loss of Observability after Cascading Failures (LOCF) index of the largest island. A higher LOCF index implies that a large portion of the largest island is unobservable.

date scenarios C1-C7, given in Table 2.7, are studied for 200 bus system. All attacks are considered for double line outages.

Figure. 2.20 demonstrates the condition of the grid after coordinated attacks. Observability in the largest island and corresponding LOCF are recorded. Case 2 and Case 6 demonstrate a total system collapse. Case 3 and Case 7 show extensive cascading failures resulting in a small surviving island. Case 1 and Case 4 show large portions of the grid remain unobservable. Case 5 indicates that a large part of the affected power system is still observable, as indicated by a low LOCF value.

To prevent line outages from evolving into cascading failures, controlled islanding is ini-

Table 2.8: Loss of Observability and Recoverability after Controlled Islanding

No	Load-Generation Imbalance (MW)		LOCI		LRCI	Lines not Recoverable	Line MVA lost
	Island 1	Island 2	Island 1	Island 2			
C1	3.63	7.54	$\frac{16}{96} = 16\%$	$\frac{2}{103} = 1\%$	$\frac{31}{32} = 96.8\%$	{81-178}	402
C2	9.49	1.68	$\frac{17}{102} = 16\%$	$\frac{19}{98} = 19\%$	$\frac{29}{32} = 90.6\%$	{97-200}, {137-3}, {62-159}	663
C3	6.48	4.69	$\frac{17}{94} = 18\%$	$\frac{1}{106} = 1\%$	$\frac{31}{32} = 96.8\%$	{121-178}	402
C4	9.23	1.94	$\frac{28}{95} = 29\%$	$\frac{11}{105} = 10\%$	$\frac{25}{28} = 89.2\%$	{62-159}, {159-62}, {137-3}, {97-60}	663
C5	9.17	2.00	$\frac{17}{103} = 17\%$	$\frac{1}{97} = 1\%$	$\frac{25}{26} = 96.1\%$	{121-178}	402
C6	7.37	3.80	$\frac{33}{98} = 33\%$	$\frac{6}{102} = 6\%$	$\frac{21}{24} = 87.5\%$	{97-200}, {120-17}, {159-57}	663
C7	4.62	6.55	$\frac{32}{102} = 31\%$	$\frac{7}{98} = 7\%$	$\frac{35}{38} = 92.1\%$	{97-200}, {85-120}, {14-15}	742

tiated after the second phase of cascades. The system is partitioned into two islands while maintaining the load-generation conditions in each partition. The impact on observability and recoverability is summarized in Table 2.8. The LOCI index in each island shows that large parts of both islands, up to 33%, remain unobservable. However, from the LRCI index, it is seen that up to 96% of lines outaged under controlled islanding can be reconnected back to restore the power grid to normal operating conditions.

2.10 Discussions

While the above studies demonstrate that very few coordinated attack scenarios under heavily loaded conditions resulted in cascading failures, system-wide outages are more common when simultaneous attacks are carried out on multiple critical system components. These included coordinated attacks on major generators, transformers or critical transmission lines. This confirmed some findings in [24].

For example, in the 200 bus system, attacks on line {109-17, 17-120, 60-97, 97-200,

Table 2.9: Major Cascading Patterns in the 200 bus System

Failure	Line Failure Sequence Prior to System Divergence
Generator loss	{115-112}→{ 179-178}→{164-163, 174-188}→{169-163}
	{65-64}→{ 179-178}→{164-163, 174-188, 63-66} →{165-163, 166-163, 169-163}
	{189-187}→{ 179-178}→{122-96, 122-121, 164-163} →{165-163, 166-163, 169-163, 63-66, 92-89}
	{105-102 }→{ 179-178}→{164-163, 174-188} →{165-163, 166-163, 169-163, 63-66, 69-66, 92-89}
Line loss	{188-187} →{187-121} →{147-146, 104-102, 105-102} →{128-133, 83-186, 115-112, 65-64}
	{187-121}→{179-178}→{122-96,122-121 }→{89-95, 92-89, 95-58, 164-163} →{41-180,69-66}

and 186-109} coordinated with the loss of large generators {64, 105 or 189} or major lines {188-187 or 187-121} triggered cascades when RAS are disabled. Cascades evolved through multiple stages before the power flow diverged. Few major cascading patterns in the 200 bus system for Case I, coordinated with attacks on critical system components, are summarized in Table 2.9. Similar results are obtained for the 500 bus system. Evidence of cascading failures as a result of a generator loss can be seen during the August 14, 2003 Northeast blackout which started with the trip of a 597 MW generator [143].

Furthermore, the impacts of attacks can become worse under the following possible scenarios - (1) incorrect SE solution due to gross measurement errors, missing measurements, or incorrect topology, (2) RAS failure due to circuit breaker malfunction, delayed operations or undesired RAS-RAS interactions; (3) introduction of uncertainty in generation due to intermittent nature of renewable resources, for example, loss of a solar array output due to a cloud cover; (4) stressed transmission system and aging grid infrastructure; (5) differences in deployment of cyber-assets across utilities; and (6) operator errors in missing critical system warnings.

The risk impact analysis remains incomplete without a discussion of challenges faced. In general, risk assessments pose three important questions - (1) What are the different events that can happen? (2) How probable are such events? and (3) What are their consequences?

While the list of scenarios under investigation can be technically infinite, only major 1-D and 2-D realistic transfer analysis across multiple areas are considered to reflect practical power system operating conditions. Similarly, attacks can theoretically outage any number of lines, however, for a more practical and tractable study, attacks disconnecting single and double line outages are considered here.

Challenges also exist when quantifying attack probabilities. This is due to the sparse nature of attacks and the unavailability of historical data. Moreover, to keep the analysis simple, attack on the complex network of PMU-PDC communication and cyber infrastructure is abstracted using the Semi-Markov process. The choice of exponential and non-exponential distribution is motivated by real-life attack patterns where different stages of attacks have different probability distributions. In particular, Weibull distribution is used as it has a close form solution and has the ability to model decreasing, constant and increasing failure rates. It is to be noted that the assumption on the sojourn time probability distribution does not directly affect the normalized risk indices. This is because the risk index of an attack is derived from the product of steady-state probabilities of PDCs remaining in the attack state and the total load loss. If additional details on attacks are available, other appropriate probability distributions can possibly be used to model attacks against PDCs. Our approach reflects one such way of abstracting cyber attacks.

There is also a major challenge in quantifying the consequences of RAS attacks. The authors in [29,30,144] have formulated the attacks as multi-level optimization problems, and have shown the outage of lines leading to overloads, unintentional islanding, and possibly cascading failures. Our approach considers additional attacks on RAS to reflect more practical power system scenarios. Actions of RAS are often localized and difficult to parameterize in an optimization problem. To overcome this, the impacts of attacks on RAS are incorporated through a distributed slack bus cascading failure algorithm. Attack impacts are then quantified as the amount of load not served. Further, the impact is quantified

in terms of loss of observability and degree of recoverability after attacks, that gives an insight on what portion of the grid can be safely operated after attack. For a more realistic analysis, the span of the outages, the number of customers affected, substation restoration time, the availability of black-start units, and socio-economic factors can be incorporated in future investigations.

In general, the concept of risk analysis is a broad question by itself. In a complex power system, a thorough risk assessment of coordinated attacks require an in-depth understanding of different system components and their interactions. Risk analysis in general becomes heavily dependent on the knowledge of deployed cyber assets and the general design of the system under consideration. There can be multiple approaches towards risk impact assessment and this chapter presents one way to evaluate the consequences of coordinated attacks on realistic power system networks under practical operating conditions.

2.11 Conclusions

This chapter examines to what extent false data injection attacks lead to widespread power outages. The attack model is designed as follows - physical attacks are carried out by disconnecting single and double lines and remedial actions schemes are disabled to maximize the consequences of the attack. Additionally, false data is injected in targeted phasor data concentrators to mask physical outages. The false data attack is modeled using a Semi-Markov approach that incorporates different probability distribution of the states of a data concentrator under attack. The consequences of the attack are analyzed using a distributed slack bus cascading failure algorithm under different 1-D and 2-D power transfer analysis, and quantified as the expected energy not served. Additionally, three metrices are developed considering the loss of observability after cascading failure, the loss of observability after controlled islanding, and the extent of recoverability of the grid. From the conducted experiments on the realistic power system test cases, it was concluded that coordinated

attacks against power systems do not often lead to large-scale blackouts, but do result in subsequent line overloads and load shedding. The results demonstrate that widespread failures are mostly initiated when false data attacks are coordinated with attacks targeting generators, transformers, or heavily loaded lines in the vicinity of large generators. Successful attacks often require multiple data concentrators to be compromised across different utilities having different cyber-security policies. Further, it was observed that the feasible attack region is largely restricted by the distribution of zero injection buses in the network. All of the above factors make coordinated false data attacks less prone to widespread physical failures.

Chapter 3

Detection of False Data Attacks

3.1 Introduction

This chapter is concerned with determining the correctness of measurement data when malicious false data injection attacks on PMU devices remain undetected by existing bad data detection algorithms. We develop a data-driven attack detection method that is independent of both power system topology and state estimation algorithms. Multi-variate synchronized PMU time-series measurements, aggregated in phasor data concentrators at different regional control centers, are utilized for attack detection. A large amount of real-time current, voltage and power flow measurements are collected under diverse load-generation profiles, and different system topologies. This data corresponded to multiple events such as line faults and trips, generation and load fluctuations, shunt disconnections and false data attacks. Various deep-learning algorithms and traditional classifiers are utilized to analyze this massive volume of data to detect anomalies in PMU measurements. The performance of the false data attack detectors are then compared for accuracy and training time. The developed data-driven deep-learning detection techniques are able to identify false data attacks repeatedly in a very short period of time, prior to each cycle of the state estimation, thereby providing an early warning to the system operators.

3.2 Background

Detecting anomalous time series data for critical real-time processes has been investigated thoroughly in [145]. Anomaly detection on large scale time series data can be found

in [146–151]. Various techniques were used for detection, some of which include calculating correlation, entropy, periodicity and self-similarity for single time series data, and using principal component analysis (PCA), hierarchical temporal memory, distance measurements and box-modeling on multiple time series data.

In power systems, data-driven approaches and various machine learning algorithms have been widely used for detection, classification and diagnosis of faults and cyber attacks [152–160]. For example, the authors in [152, 153] used neural networks, decision trees and support vector machine (SVM) for fault identification. Identification of Denial of Service, data integrity, man-in-the-middle and replay attacks have been considered in [154–158]. The authors in [159] use common path mining to identify fault replay attacks, relay tripping attacks and relay disabling attacks based on malicious remote commands identified by Snort intrusion detection systems. The authors in [160] proposed an intrusion detection system which identified power system faults and maintenance operations from different cyber events such as disabled relays, command injection and fault replay.

In [161], the authors trained a deep belief network, combined with Gaussian-Bernoulli Deep Boltzmann Machine, on artificially generated data-set using verified compromised load patterns. The authors in [162] combined normal demand usage pattern and demand forecasts to identify unnatural deviations in power consumption to detect false data attacks. Based on difference between falsified and rated voltage data, the authors in [163] proposed two different indices to identify anomaly - the control signal from controller to static VAR compensator and node voltage stability index, to detect falsified measurements. The authors in [164, 165] used principal component analysis to identify anomalies in power flow measurements by analyzing regular and irregular sub-spaces. Further, the authors in [166] used margin setting algorithm on hourly PMU angle and frequency measurements to detect falsified measurements. Two types of attack were considered - playback attack where the PMU data was played back in reverse, and time attack where the PMU data was re-

sampled respectively.

To detect false data attacks from normal conditions, various binary classification techniques were proposed [167–170]. The authors in [167] proposed to detect false data using SVM. The sparsity (fraction of compromised measurements) and variance (deviation from normal measurements) of the attack vector were exploited for this purpose. In [168], the authors solved the binary classification problem by studying the deviation in measurements and applying supervised method and unsupervised classification methods. The authors in [169] employed mean and standard deviation of wavelet coefficients of estimated states with a convolutional neural network (CNN). The authors in [170] obtained load data over a period of five years. False data was added as instances in the load data set, and the correlation between previous and current power flow measurements were exploited to identify the attacks using recurrent neural networks (RNN).

The various false data injection detectors discussed above had multiple drawbacks. For example, cases of false data were investigated on maximum four transmission lines [164]. This is not very realistic as our analysis in Figure 2.18 in Chapter 2 indicate that very often, more than four line measurements are often required to be simultaneously altered for a successful attack to cause large impact. Further, studying past states estimates to detect data attacks [169] may often produce false positives if the state estimator solution is incorrect due to gross errors or missing measurements. Further, detection of FDIA under gross measurement errors with high variance, or cases of contingencies or sudden loss of load, or loss of sensor measurement, all of which can alter the temporal correlation of the data, were not considered [167, 168].

Our proposed method to identify false data injection attack addresses the above drawbacks. For example, our approach of attack detection utilizes multi-variate PMU packet data streams accumulated at data concentrators. Analyzing the data concentrated at PDCs for false data serves as an early warning tool prior to each cycle of state esti-

mation. As a result, our method do not depend on state estimation or system topology. Further, in contrast to binary classification, our approach is a multi-class classification problem where the proposed data filter is able to distinguish various normal operating conditions, several different types contingencies, and various of false data. Further, the developed approach is robust in detecting anomalous data under large variances of noise, missing measurements and garbage data.

3.3 Synchrophasor System Architecture

Voltage and current measurements from instrument transformers are sampled by PMUs and converted to digital signals using an analog-digital converter. Time stamp information from Global Positioning System (GPS) is added to synchronize all PMU measurements. Data is then sent to the data concentrator in the form of packets through wide area networks (WAN). Packets from several PMUs are combined at the regional PDCs after it has been synchronized and grouped. Data from regional PDCs are forwarded to the control centers, where they are used for state estimation or archived in superPDCs [165].

The IEEE Standard for Synchrophasors for Power Systems (C37.118.1-2011) defines four different message types: data, configuration, header, and command. Any standard PMU provides current and voltage data in both in rectangular and polar format. The phasors provided by the PMUs are 16-bit integer values. These phasors can be single or three phase positive, negative or zero sequence values. Industry grade PMUs often support 8 voltage and 12 current measurements, at the rate of 60 messages per second while PDCs can process data from more than 500 PMUs at a maximum data rate of 240 messages per second [171]. A large number of data packets are available in the PMU buffer prior to calculation of the state variables. One estimate suggests that a network with 100 PMUs having 20 different measurements each at 30 messages per second can generate about 50 gigabyte of data per day [172].

3.4 False Data Attack Injection

This multi-variate data flowing through the PMU-PDC hierarchical communication infrastructure can be subjected to decryption and modification before being sent to the main control center [38–41]. The PMU-PDC architecture can be targeted by reconnaissance attacks [173] and traffic analysis attacks [174] where attackers gather system or communication information from open ports or IP address. Attacks also include packet data injection [173] where malicious sensor or command/request packets are injected in correct data format. Other kinds of attacks include Denial of Service which disrupts communication channels by injecting huge volume of traffic often making the system unresponsive [173], time synchronization attacks which involves GPS spoofing to disrupt synchronized PMU measurements [38] and man-in-the-middle attack data integrity attacks that compromise measurements [175]. Once the PMU network is infiltrated, the attacker may either compromise the time series measurements at individual PMUs or those aggregated at the PDC. Modified packet data with false measurements pass the inbuilt cyclic redundancy check [165] as shown in Figure 3.1.

As seen in Chapter 2, such attacks potentially interfere with real-time operation and may result in a targeted (unwanted) action from the operator on the otherwise healthy system with large economic or reliability consequences.

In this chapter, we are particularly interested in false data attacks that can be carried out at different substation PDCs where multiple PMU data streams aggregate. Assuming that the SE runs every minute, and the sampling rate of PMUs are 30 messages/second [69], this leads to accumulation of 1800 measurements in the data buffer. Once all the time series measurements accumulate in the PMU buffer, the SE uses the last set of received measurements, or the mean of the measurements to estimate the states of the system. Thus, the SE renders itself blind to sudden changes on voltage/current time series during an attack. Fal-

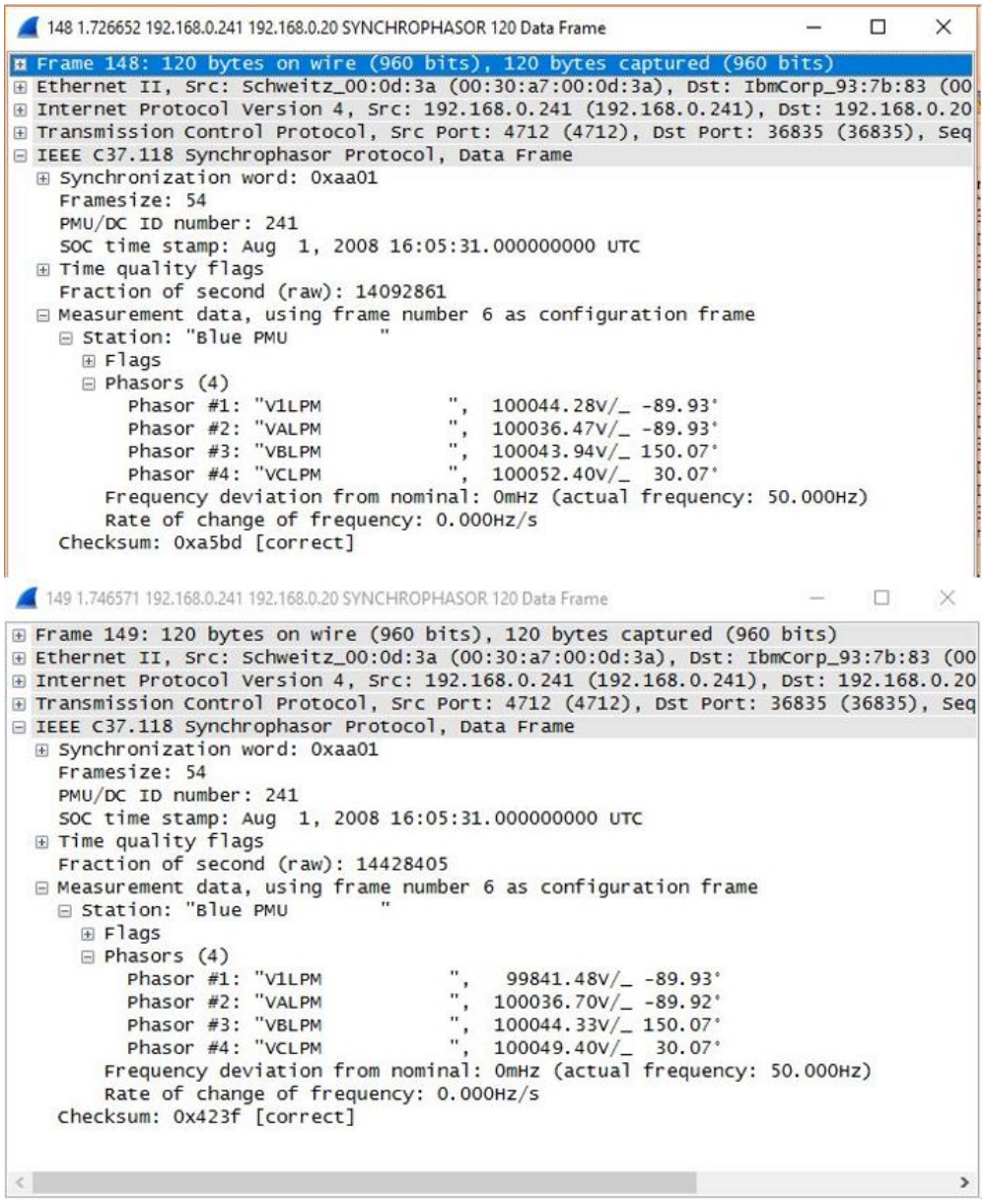

Figure 3.1: Normal PMU packet (top) and compromised PMU packet (bottom) with false phasor measurement in channel #1 altering voltage data. Further, a modified checksum is injected to avoid detection.

sified data values will persist in the next SE cycle, inevitably corrupting the system states. Thus, analyzing the historically stored data in the PMU-PDC data buffer, prior to SE, will lead to good insights into the behavior of the system during data falsification attacks and normal or transient events.

To develop a false data detector that is independent of system topology and SE algorithms, we focus our concentration on the inherent characteristics of the compromised data. There are two specific ways attackers can falsify data streams - (a) using fault replay attacks to pretend a transient fault prior to changing measurements, or (b) by changing a number of time series simultaneously. The minimum number of measurements required to compromise the system to carry out a successful attack is visualized in Figure. 2.18. First, we first combine fault replay attacks with carefully constructed attack vector. At a particular instant of time, the original set of PMU measurements are replaced with the altered measurements to mimic fault replay attack following the equation,

$$z^t_{false} = z_{2bad} + [sin(\omega_1 t - \theta) + cos(\omega_2 t - \theta)]e^{-\xi_1 t + \xi_2} \tag{3.1}$$

with ω_i, ξ_i and t as oscillation frequency, damping coefficients and time of occurrence of fault replay attack respectively. The sinusoidal part models the oscillatory behavior of voltage and current phasor while the exponential part models the damping under power system faults with normal clearing [176]. Apart from simulating fault replay attacks, false data is also injected by simultaneously changing a number of time series measurements.

In both the cases, the final values of the altered data stream correspond to the the attack vector the adversary targets to inject to change the required states.

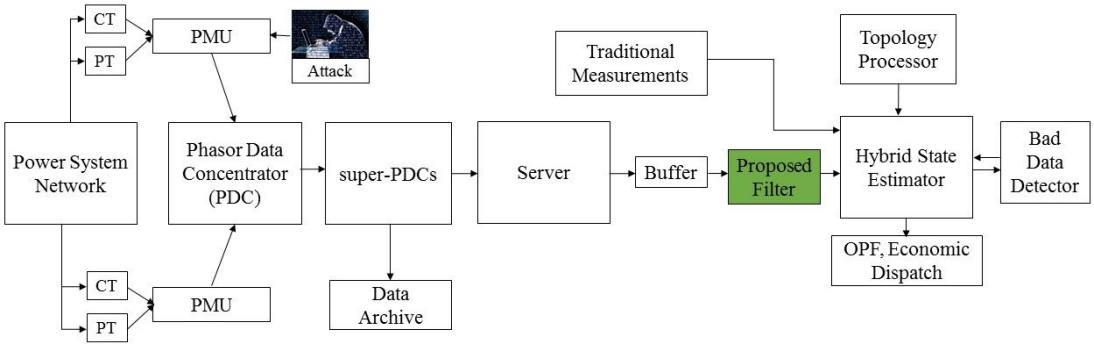

Figure 3.2: Overview of the proposed Convolutional Neural Network (CNN)-based false data filter. This data filter, installed at regional control center, serves as an early warning system to detect falsified data stream prior to each cycle of state estimation.

3.5 Detecting False Data Attacks

For detecting modified PMU data streams, we propose a false data filter that exploits the spatio-temporal characteristics of PMU packet data concentrating at regional PDC. The overview of the entire process is given in Figure. 3.2. To ensure that our proposed false data detection method is independent of network size, we divide the power network into several cyber-security regions corresponding to different utility jurisdictions (and their security policies). The false data filter can then be integrated in each regional PDC to monitor aggregated PMU time series measurements. This eliminates the need of analyzing every time series from each and every PMU in large network (which might also be practically infeasible given that data sharing policies may be restricted between different utilities).

Let us consider the PDC data set A where,

1. A contains d multi-variate PMU packet data items, $A = \{A^1, A^2, ..., A^d\}$.

2. Each data item A^i, $i = \{1, ..., d\}$, consists of n univariate voltage and current phasor data stream, represented as a^i_j and stored in the data concentrator for d different instances.

3. Depending upon the PMU sampling rate and buffer length, the length of each time

series a_j^i, $j = \{1, ..., n\}$ takes values corresponding to synchronized time stamps $\{1, ..., t\}$.

Given a set of PMU observations A, we aim to classify this multi-variate data item into k different classes where $\mathcal{C}_1 = \{A^1_{\mathcal{C}_1}, A^2_{\mathcal{C}_1}, .., A^{k1}_{\mathcal{C}_1}\}$, $\mathcal{C}_2 = \{A^1_{\mathcal{C}_2}, A^2_{\mathcal{C}_2}, .., A^{k2}_{\mathcal{C}_2}\}$,..., $\mathcal{C}_k = \{A^1_{\mathcal{C}_k}, A^2_{\mathcal{C}_k}, .., A^{k3}_{\mathcal{C}_k}\}$ corresponding to different events. Our fundamental approach to identify anomalies in data stream is based on the underlying correlation between different PMU data packets in the multivariate dataset. We start by extracting features from each time series data item using Pearson's correlation coefficient, which is defined between two different time series a_1 and a_2 as,

$$\sigma(a_1, a_2) = \frac{\sum_{t=1}^{t}(a_1^t - \tilde{a}_1)(a_2^t - \tilde{a}_2)}{(t-1)\sigma_{a_1}\sigma_{a_2}} \tag{3.2}$$

where $\tilde{a}_i$ and σ_{a_i} are the mean and standard deviation of time series i. Once the correlation coefficients for all time series item are computed, we use the correlation matrix $\Upsilon(A)$ to classify our data set. As this is a multi-class classification problem, we represent our classes by k-dimensional vector by one hot encoding (binary coding which is all 0 except for a single 1 at the index of the particular class).

To identify FDIA against PMU based state estimation, we exploit recent advances in deep learning. Deep learning has proven to be very effective in extracting features from different data sets and has been used widely in areas of natural language processing and computer vision [177]. We first use a convolutional neural network to extract high level features from raw PMU data without relying on prior domain knowledge. The CNN extracts high-level features from the correlation matrix to classify different power system events. The performance of the filter is then compared with (a) other deep learning algorithms such as Recurrent Neural Networks (RNN), Long Short Term Memory (LSTM), and (b) traditional classifiers such as SVM and ensemble methods. A brief introduction of all the three algorithms, CNN, RNN and LSTM, is presented next.

3.5.1 Convolutional Neural Networks

Convolutional Neural Networks (CNN) are deep neural networks which exploit spatial correlation by studying local connections between adjacent neurons. For a detailed discussion on CNN, we refer the readers to [178–180]. The process of feature extraction from multiple time series dataset and event classification using CNN is summarized in Figure 3.3.

The CNN network is represented as a feed-forward process of cascading functions f_k, operating on inputs X and learnable parameters W_k as

$$f(X) = f_k(....f_3(f_2(f_1(X, W_1), W_2,), W_3), ...W_k) \tag{3.3}$$

The input to the CNN is the correlation matrix $\Upsilon(A)$ of size $h \times b \times d$ where h, b, d are the dimensions of the input image (correlation matrix) to the network. High level features are extracted from the input image by CNN over multiple layers. The convolution layer performs a convolution between a portion of the input with learnable filters (or weights W). The discrete convolution between the input $\Upsilon(A^i)$ and weight W can be written as,

$$(\Upsilon * W)(i) = \sum_{j=-\infty}^{\infty} \Upsilon_j W_{(i-j)} \tag{3.4}$$

Multiple filters are used to obtain several feature maps $\mathcal{F}$ from the inputs at each layer. These feature maps are stacked together and fed as inputs to the next layer. These filters have small spatial dimensions but extend to the entire input depth. They resemble local receptive fields, learning from one specific sub-region of the input (image). Unlike traditional neural network, CNN introduces the concept of parameter sharing where each filter is used at every position of the image. The number of filters and convolution layers can be varied depending on the input dimension of the data and computation capacity.

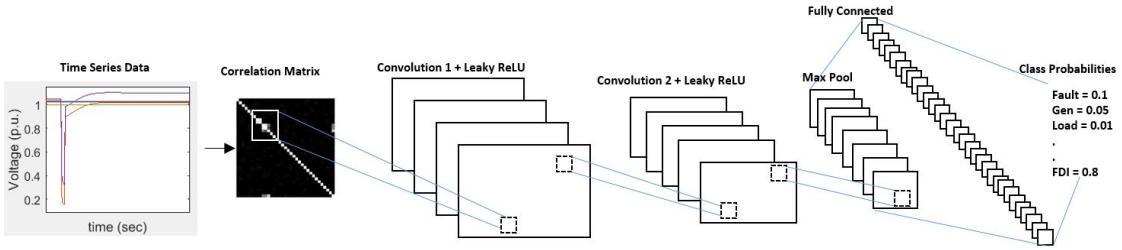

Figure 3.3: Overview of feature extraction and classification process using CNN

Once the feature maps are generated after convolving with different filters, each element is passed through a non-linear activation function which squashes the output between certain thresholds. These include non-linear activation functions such as sigmoid, rectified linear units (ReLu) or leaky-Rectified linear unit (LeakyReLU) which introduce non-linearity between the input and output of the convolutional layer. To alleviate the problem of dying gradients in ReLu, LeakyReLU is used by introducing an additional parameter $\alpha = 0.001$. The non-linear layer can then be expressed as, $g_{i,j,k} = max(\alpha\mathcal{F}, \mathcal{F})$.

After the non-linear activation function is applied to the feature maps, the output is further down sampled along the spatial dimensions using a pooling layer. This layer combines local feature from a small neighborhood into one single value $\mathcal{F}'$. This can be done using average, weighted average, max-pooling or $L_2 - norm$. In this thesis, we consider the max-pooling function which returns the maximum value within the local neighborhood, given as $\mathcal{L}_{i,j,k} = max(\mathcal{F}'_{i,j,k})$.

To reduce over-fitting of the data (especially when the number of attack samples is not large), a dropout layer is used. At the time of training, the dropout layer 'drops' a random set of neurons with a probability p. This ensures that the network is less biased to specific weights of neurons and provides better generalization.

The expected output of any particular neuron is given as, $E(neuron) = p\hat{y} + (1-p)\hat{y}$, where $\hat{y}$ was the original output of the neuron. The final layer of the CNN-based data classifier is the fully-connected (FC) layer. Local features extracted from the feature maps

by previous layers are combined in this layer to produce an output vector of dimension k, where k is the number of classes. The final classification is performed using a Softmax classifier which is given as $f_k(v) = e^{v_k}/\sum_k e^{v_k}$. Once the vector of final scores v is computed by the fully-connected layer, the Softmax function normalizes it to have values within $(0, 1)$. The Softmax function is combined with the cross-entropy loss function as,

$$L = -log(e^{v_k}/\sum_k e^{v_k}) \tag{3.5}$$

This loss function minimizes the cross-entropy between the original and the predicted distribution. In other words, the objective function minimizes the negative log likelihood of the correct class. The k-dimension vector obtained in the output layer can be intuitively thought of as normalized class probabilities for different events under study.

3.5.2 Recurrent Neural Networks

In addition to CNN, the recurrent neural network is another deep learning architecture that uses iterative learning and allows provisions for 'memory' [181, 182]. One of the major advantage is that they not only analyze the current input but can also learn from the past inputs and incorporate long-term dependencies. In general, the structure of RNN can be iteratively described through time $t = 1 \rightarrow T$ using the following set of equations [183],

$$\begin{aligned} u_t &= W_{hv}v_t + W_{hh}h_t + b_h \\ h_t &= e(u_t) \\ o_t &= W_{oh}h_t + b_o \\ z_t &= g(o_t) \end{aligned} \tag{3.6}$$

Here, W is vector of different weights, b is the set of biases, v is the input sequence, h are the hidden states and o is the output sequence respectively. The variables e and g refer to the non-linear functions at the hidden and output gates. Two of the major drawbacks of

using RNN are the problem of exploding and vanishing gradients during back-propagation [184, 185].

3.5.3 Long Short Term Memory

To overcome the problems of RNN, the authors in [186] proposed long short term memory. The LSTM uses 'memory units' to store information for longer periods of time. It also incorporates 'gated units' such as the 'input', 'forget' and 'output' gates to control the flow of new information into the memory, decide how long it stays and when it is used for the output respectively. In general, the structure of LSTM can be iteratively described through time $t = 1 \rightarrow T$ using the following set of equations [183],

$$\begin{aligned} h_t &= tanh(W_{hh}h_{t-1} + W_{hv}v_t + W_{hm}\tilde{m}_{t-1}) \\ i_t^g &= e(W_{igh}h_t + W_{igv}v_t + W_{igm}\tilde{m}_{t-1}) \\ i_t &= tanh(W_{ih}h_t + W_{iv}v_t + W_{im}\tilde{m}_{t-1}) \\ o_t &= e(W_{oh}h_t + W_{ov}v_t + W_{om}\tilde{m}_{t-1}) \\ f_t &= e(W_{fh}h_t + W_{fv}v_t + W_{fm}\tilde{m}_{t-1} + b_f) \\ m_t &= m_{t-1} \odot f_t + i_t \odot i_t^g \\ \tilde{m}_t &= m_t \odot o_t \\ z_t &= g(W_{yh}h_t + W_{ym}\tilde{m}_t) \end{aligned} \tag{3.7}$$

where W is the vector of different weights, b is the set of biases, i^g is the vector of input gates, i is the vector of memory unit inputs and o is the vector of output gates respectively. Other variables include the vector of forget gates f, input vector v, hidden states h, memory states m, memory state to determine if information can leave the memory unit $\tilde{m}$, output vector z, and desired output of the supervised learning y. The variables e and g refer to the non-linear functions at different gates while $\odot$ refers to element wise multiplication. Detailed description of the functioning of different layers of LSTM can be found

in [183, 186].

3.5.4 Parameter Updates

Each of the deep learning algorithm is used to train the multivariate PMU time series data to classify data falsification attacks and other power system events. To ensure that the networks are able to learn features extracted from the time series data, the weights in CNN, RNN and LSTM are updated using back-propagation method after each forward run, [187], i.e. weights w are incremented based on the gradient of the loss function after each iteration t using learning rate λ,

$$w(t+1) = w(t) - \lambda \nabla L(w(t)) \tag{3.8}$$

Different variants of gradient descend algorithms such as batch gradient, stochastic gradient and mini-batch gradient can be used. In this study, we use mini-batch technique which divides the entire training data into batches and updates the weights more frequently. Advantages of using mini-batch include higher convergence rate, avoidance of local minima, and lower memory requirement. These advantages become significant when a large amount of PMU time series dataset is trained [187].

To improve the convergence rate of the deep learning model, we use Nesterov Adam (Nadam) gradient descent optimization algorithm. Nadam incorporates the momentum update from RMSProp and Nesterov accelerated gradient, combining exponentially decaying past gradients and their squares [188]. The gradient of the loss function g_t at iteration t, the first order and second order moments of the gradient $\hat{m}_t$ and $\hat{v}_t$ respectively are,

$$g_t = \nabla L(w(t)) \tag{3.9}$$

$$\hat{m}_t = \frac{\beta_1 m_{t-1} + (i-\beta_1) g_t}{1-\beta_1^t}; \hat{v}_t = \frac{\beta_2 v_{t-1} + (i-\beta_2) g_t^2}{1-\beta_2^t} \tag{3.10}$$

The Nadam update can then be written as [188],

$$w(t+1) = w(t) - \frac{\lambda}{\sqrt{\hat{v}_t} + \eta}[\beta_1 \hat{m}_t + \frac{(1-\beta_1)}{1-\beta_1^t} g_t] \tag{3.11}$$

where β_1 and β_2 are the exponential decay rates of first and second order moment estimates, and $\eta = 10^{-8}$ is used to prevent division by zero.

3.5.5 Traditional Classifiers

The performance of the proposed deep learning based data filter is compared with different traditional classifiers [189, 190]. Methods used to extract features from the multi-variate time series include $1)$ variances explained by the first few principal components (PC) , $2)$ statistical properties such as mean, standard deviation and variance of detail and approximate wavelet coefficients [191], and $3)$ correlation coefficients. The features obtained are used with traditional classifiers such as Support Vector Machine (SVM) [192], Bagged trees [193], Boosted [194] and RUS-Boosted trees [195]. Bagging first trains multiple smaller classifiers and then obtains the mean of the resulting outputs to reduce the classification error. On the other hand, Boosting combines the predictions of multiple smaller classifiers (also called 'decision stubs') to learn and further predict the output. To alleviate the class imbalance problem, an extension of AdaBoost called RUS-Boosted tree is used. It achieves a more uniform class distribution by randomly dropping instances of classes with more labeled dataset. This is particularly useful as the number of false data injection scenarios is comparatively smaller to the number of normal and event scenarios.

3.6 Simulation Results

In this section, the effectiveness of the proposed CNN-based data filter to classify different power system events from false data is investigated on IEEE-30 bus and IEEE-118 bus system. All simulations are carried out using DSATools, MATLAB and Python on an Intel

Table 3.1: PMU Placement

System	PMU Bus
IEEE-30 Bus	2,4,6,10,12,15, 27
IEEE-118 Bus	12,15,32,49,54,56,59,69,70,77,80,85

Table 3.2: Different Events under Study

Scenario	IEEE-30 Bus	IEEE-118 Bus
Bus/Branch faults	283	1152
Line Trip	163	680
Load Changes	420	364
Generation Changes	115	216
Shunt Disconnection	120	224
False Data	200	400
Normal	200	256
Total	**1501**	**3292**

Core i5-4460 CPU @ 3.20Ghz and 8 GB RAM.

3.6.1 Scenario Setup

We consider fully observable electric power grids. The candidate PMU buses are given in Table 3.1. For IEEE-30 bus system, thirty-five time series are collected. For IEEE-118 bus system, we divide the network into four cyber-security zones shown in Figure 3.4. From each zonal PDC, 25 PMU time series are collected. To ensure that the proposed classifier is robust under different power system operating conditions, we consider four scenarios with varying load-generation patterns and network topologies,

- Scenario 1: Peak load
- Scenario 2: Light load
- Scenario 3: Light load with one generator switched off
- Scenario 4: N-1 contingent system under peak load

Six different events are simulated under each scenario along with normal operation con-

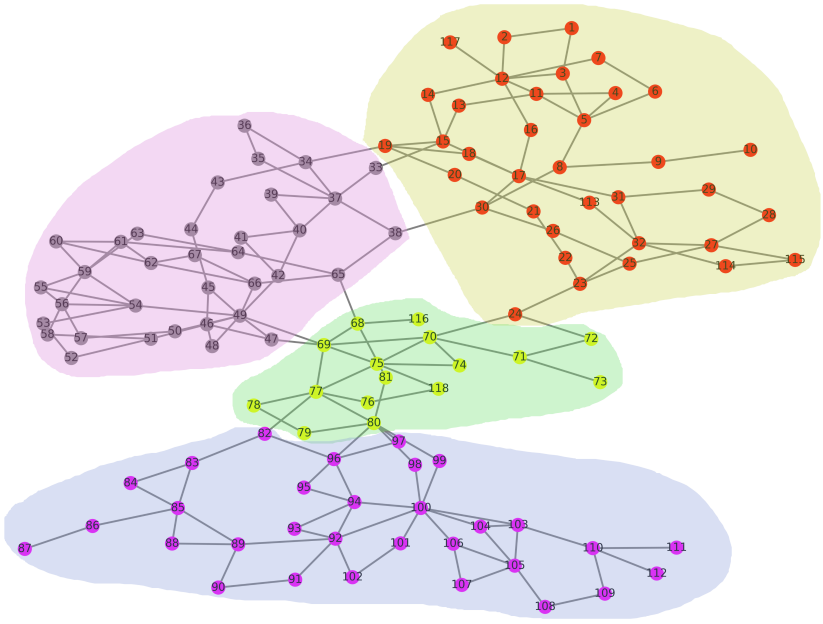

Figure 3.4: Four areas in the IEEE-118 bus.

ditions. Faults are randomly simulated between 0 to 100% of the transmission line length and are cleared after 5 cycles. Random load and generation changes between 2% to 10% are considered to mimic real-time fluctuations in PMU measurements under daily normal operating conditions. Other events such as line trips due to schedule maintenance and shunt disconnections are also considered to encompass a large variety of data set.

To generate falsified data streams that mimic fault replay attacks combined with false data, the parameters in (3.1) are set as $\omega_1, \omega_2 \in (1, 3)$, $\xi_1 \in (-0.3, -0.8)$ and $\xi_2 = 0.05$. In addition to fault replay, FDIA also includes changing a set of PMU measurement packets. The final value of the falsified attack vector can be obtained by the methods described in Chapter 2, Section 2.3.1.

For IEEE-30 bus and IEEE-118 bus systems, a total of 1501 and 3292 different scenarios are simulated, respectively, which are summarized in Table 3.2. PMU voltage buffer data for few scenarios is given in Figure 3.5 for illustration.

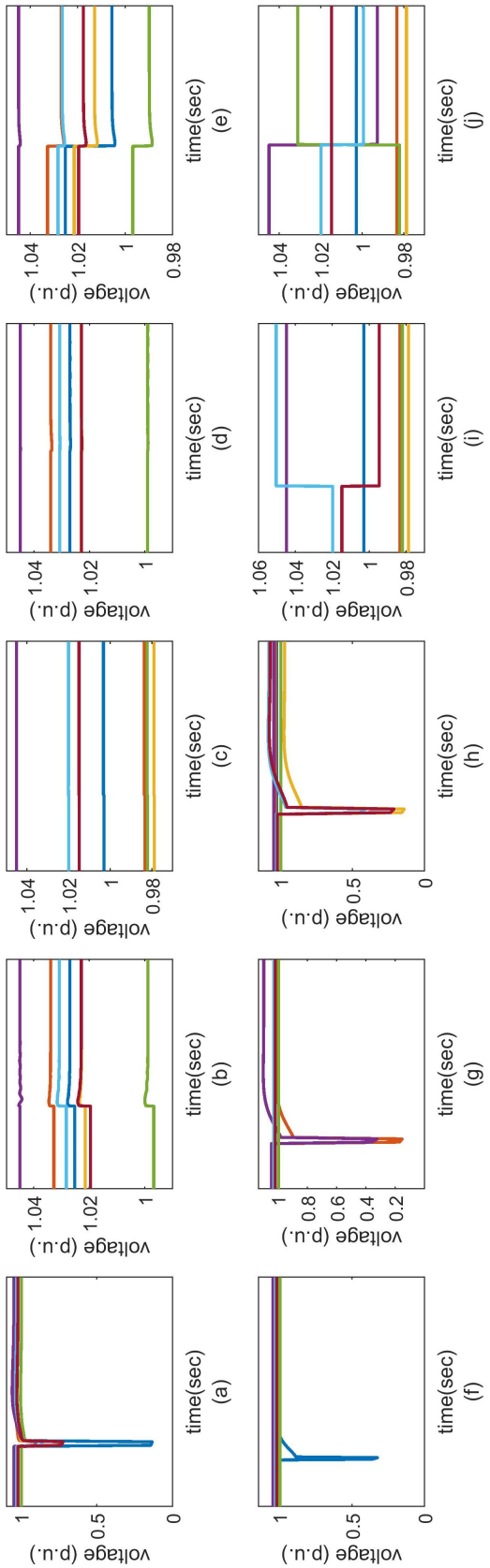

Figure 3.5: Visualization of PMU time-series data for $t = 15$s - (a) Three phase faults, (b) Line trip for maintenance, (c) Load changes, (d) Generation changes, (e) Shunt disconnection, (f)-(h) Fault replay attack combined with false data attack, (i)-(j) False data attack with multiple time series data altered

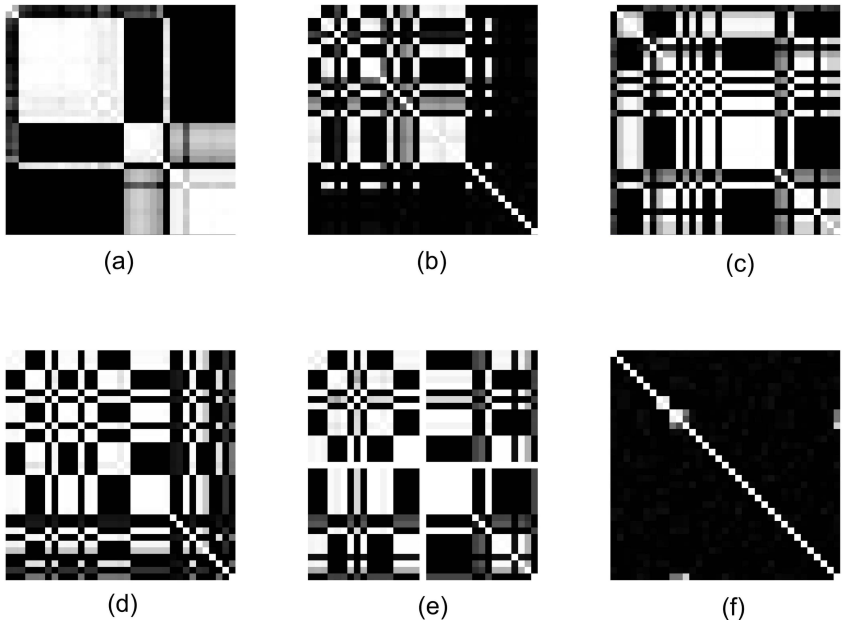

Figure 3.6: Sample Gray-scale visualization of correlation matrix for six events - (a) Three phase faults, (b) Line trip for maintenance, (c) Load changes, (d) Generation changes, (e) Shunt disconnection, (f) False data attack. The correlation matrix is used as a feature for the CNN-based data filter.

3.6.2 Feature Extraction and Training

First, we obtain the correlation matrix Υ consisting of pairwise correlations between each time-series. This is the input to the CNN architecture. Once enough training samples are provided, the CNN learns from the features and updates the weight at different layers by minimizing the cross-entropy loss function. Gray-scale image representation of the correlation matrix in Figure 3.6 shows different signatures for various power system events and attacks.

For IEEE-30 bus and IEEE-118 bus systems, the size of the inputs are $35 \times 35 \times 1$ and $25 \times 25 \times 1$ respectively. The original dataset is divided into 80% training and 20% testing sets.

For CNN, the learning rates and different parameters such as filter size, number of layers and dropout were varied. To prevent over-fitting of the data, several precautions are taken,

1. The data was split into training and validation sets using 10-fold cross-validation (CV). To account for class imbalance, we have used stratified k-fold CV which takes into account the relative distribution of classes. This method helps preserve the sample distribution in each class.

2. The training and validation accuracies and losses are monitored for every epoch. The training is stopped when the validation accuracy shows no improvements above 0.0001, which is set as the minimum change to qualify as improvement after 10 epochs. The average number of epochs before early-stopping was found to vary roughly between 25 to 30.

3. The training data is randomly shuffled before each epoch.

Classification using RNN and LSTM is performed using the same correlation matrix. To compare how CNN with traditional machine learning algorithms (such as SVM, Boosted and Bagged trees), we extract the following features from the time series - (1) principal components, (2) wavelets decomposition coefficients, and (3) correlation coefficients. The first 10 principal components are used as features as they explained around 98% of the variation in data. Statistical features of mean, standard deviation and variance were obtained from detailed and approximate wavelet coefficients. Additionally, Pearson's correlation was used to calculate the pairwise correlation between different time series data. All extracted features are then used as inputs to the traditional classifiers.

3.6.3 Attack Detection Results

We compare the performance of 15 different CNN models whose corresponding architectures and accuracies are shown in Table 3.3. It is seen that CNN-2d results in the highest classification accuracy of 98.67% with $\lambda = 0.0001$. The parameters for CNN-2d model are given in Table 3.4. The performance of the CNN-based data filter is summarized in the

Table 3.3: Different CNN Models for IEEE-30 Bus

Network	Filter 1	Filter 2	Filter 3	Filter 4	Accuracy	Time(sec)
CNN-1a	3x3x8	-	-	-	96.87	421
CNN-1b	3x3x16	-	-	-	98.10	498
CNN-1c	5x5x8	-	-	-	95.51	487
CNN-1d	5x5x16	-	-	-	97.34	518
CNN-1e	5x5x32	-	-	-	97.71	605
CNN-2a	3x3x16	3x3x16	-	-	98.23	597
CNN-2b	5x5x16	5x5x16	-	-	96.58	617
CNN-2c	3x3x16	5x5x16	-	-	97.11	536
CNN-2d	**3x3x8**	**3x3x8**	**-**	**-**	**98.67**	**540**
CNN-2e	3x3x8	5x5x8	-	-	98.24	532
CNN-3a	3x3x16	3x3x16	5x5x32	5x5x32	98.10	745
CNN-3b	3x3x16	3x3x16	3x3x32	3x3x32	97.10	720
CNN-3c	3x3x8	3x3x8	3x3x16	3x3x16	98.02	652
CNN-3d	3x3x8	3x3x8	3x3x16	5x5x16	94.57	789
CNN-3e	3x3x8	3x3x8	5x5x16	5x5x16	95.58	765

Table 3.4: CNN-2d Model Parameters for IEEE-30 Bus

Parameters	CNN-1	CNN-2	Max-Pool	FC
Input size	35x35x1	35x35x8	33x33x8	17x17x8
Filter size	3	3	2x2	-
Filters	8	8	1	-
Stride	1	1	2	-
Padding	1	1	-	-
Output size	35x35x8	33x33x8	17x17x8	6

confusion matrices shown in Figure. 3.7. For IEEE-30 bus, CNN correctly classifies all false data attacks, shunt disconnections, generation changes and normal operations. One instance of fault is misclassified as shunt disconnection while two line trips are misclassified as load changes. This was due to similarity in transient signatures of voltage and current data streams between a line trip and a sudden 10% reduction of the largest load of 96 MVA at bus 5.

The plots for training and validation accuracies for IEEE-30 bus system are shown in Figure. 3.8. It is seen for 300 iterations, the error on the validation set does not exceed that of the training set. Observations from Table 3.3 indicate that increasing the number of layers in the network does not result in an increase in accuracy. On the other hand, it leads to increased computation time, more learnable parameters, and over-fitting of data with higher validation loss compared to training loss.

For detecting false data attacks, the CNN-2d model in Table 3.4 *with 2 layers, dropout probability of 0.5 and fully connected layer with 512 neurons with a 98.67% accuracy was chosen as the desired filter.*

Similar observations are made for CNN on IEEE-118 bus system where the best performing filter had an accuracy of 94.53% for batch size = 32, epochs = 30, hidden units = 512, 10-fold CV, dropout = 0.5 and two filters of size $3 \times 3 \times 8$ and $3 \times 3 \times 8$ respectively.

Next, we compare the proposed CNN-based filter with RNN and LSTM based classifiers. To reduce the training time, early stopping was employed when there was no further improvement in validation accuracy after 10 epochs. The accuracies and training time for both the power system networks with the three deep learning algorithms are compared in Table 3.5. It is seen that both RNN and LSTM classifiers under-perform when compared to the proposed CNN-based filter.

One of the reasons CNN has a superior performance is because of the ability to recognize

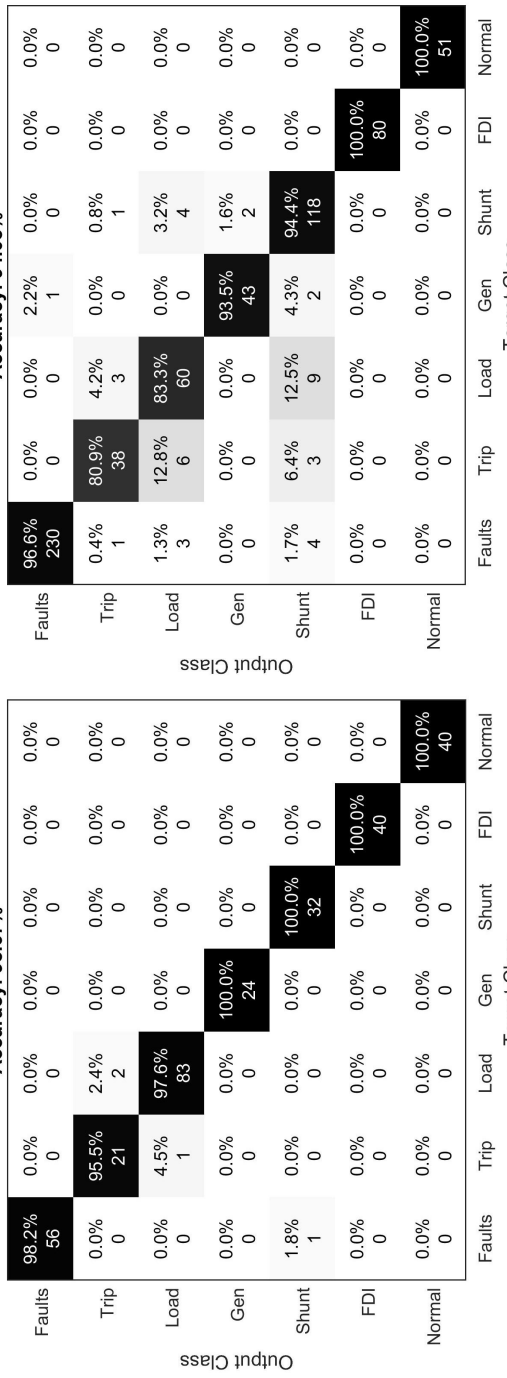

Figure 3.7: Confusion matrix obtained from the CNN based data filter for (a) IEEE 30 Bus, (b) IEEE 118 Bus

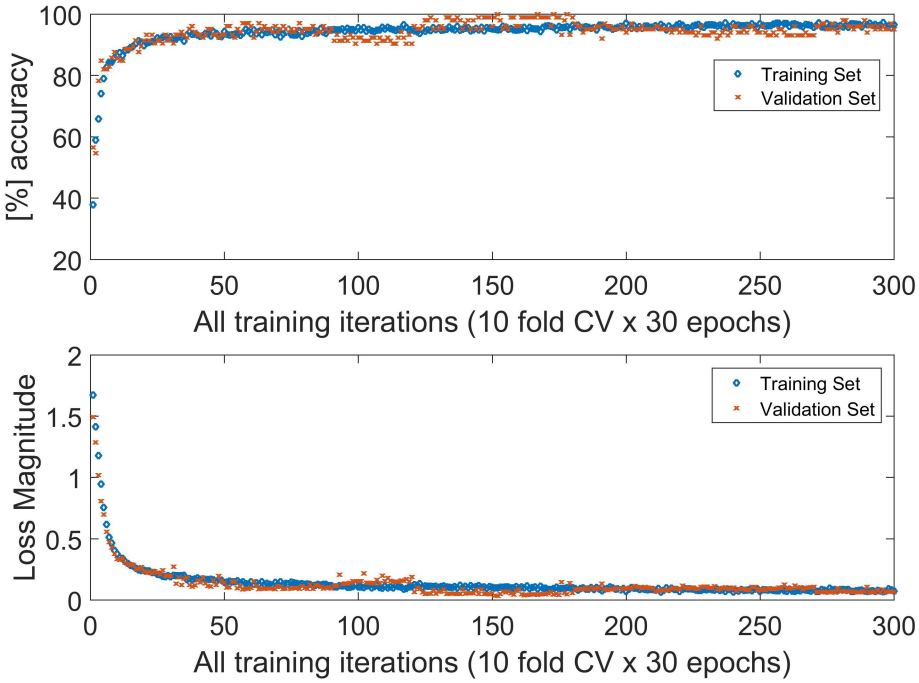

Figure 3.8: Accuracy and training loss obtained for the developed CNN-based data filter on both test data and validation data for the IEEE-30 Bus system.

Table 3.5: Accuracy (%) and Execution Time for Deep Learning Algorithms

Test Case	**IEEE-30 Bus**			**IEEE-118 Bus**		
Algorithm	**CNN**	**RNN**	**LSTM**	**CNN**	**RNN**	**LSTM**
Accuracy	98.67	91.18	83.18	94.53	71.01	72.61
Time (sec)	540	2006	3244	145	5950	7688

the spatial patterns in the input data. CNN is particularly effective for our analysis where we utilize the inter-time series correlation matrix to detect FDIA. CNN is able to extract features by performing convolutions with smaller filters and learning from the entire correlation matrix image.

When compared with other deep learning algorithms, RNN misclassified 25 instances of false data as faults and 15 instances as shunt, while LSTM misclassified 36 instances of false data as faults for IEEE-30 and IEEE-118 bus systems. In the case of RNN or LSTM, information in the hidden layers from the previous time steps are added into the next step. Both RNN and LSTM save the present state of the system and combine it with future steps to take into account time dependencies. For the classification of false data attacks, it is not necessary to learn the historical pattern within the input vector, but it is sufficient to study the spatial correlations between time series. Moreover, RNN and LSTM are computationally expensive and require larger training time compared to CNN, as shown in Table 3.5. This demonstrates that the proposed CNN-based filter is able to accurately identify all normal, transient, and false data events with very high accuracy among other machine learning algorithms.

Next, we evaluate the performance of traditional classifiers. The results are summarized in Table 3.6. It is seen that SVM performed poorly for all given features and failed to correctly classify no more than 62.50% of the time series on an average. A significant number of false data attacks were seen to be misclassified as transient faults, and generation changes were seen to be misclassified as load changes. Among the traditional classifiers, Boosted trees showed a superior performance with an accuracy of 93.78% when combined with correlation between multiple time series. Statistical parameters obtained from wavelets and PCA, when combined with boosted trees resulted in 94.02% and 82.37% accuracy respectively. Bagged trees, combined with mean of wavelet coefficients, resulted in 93.56% accuracy while RUS-Boosted trees, combined with correlation, resulted in 92.66%

Table 3.6: Accuracy (%) of Traditional Classifiers for IEEE-30 Bus

Classifier	Var	Corr	Mean_WV	SD_WV	Var_WV
SVM	80.05	51.16	59.88	60.92	60.53
Bagged Trees	81.69	91.05	93.56	92.70	91.26
Boosted Trees	82.37	93.78	93.55	92.57	94.02
RUS-Boosted	83.75	92.66	91.97	88.21	87.23

accuracy. Both Boosted and Bagged trees misclassified instances of FDI as shunt changes and line faults. The training time for SVM, Bagged and Boosted trees were around 18, 27 and 91 seconds. Comparing results in Table 3.3 and Table 3.6 show that CNN has better performance at the expense of higher offline learning time compared to the traditional classification methods.

3.7 Discussions

We observe that CNN outperforms deep learning algorithms such as RNN and LSTM, as well as traditional classification algorithms to detect false data streams in PMU-PDC architecture. With the increase in number of data streams, the training time for CNN increases, but this should be of little concern as the model can be trained off-line with large amount of available historical data. Taking advantage of the high sampling rate of PMUs and large amount of data available in the buffer, the CNN-based filter can be potentially employed as a data filter, independent of existing bad data detectors, to detect anomalous data streams in PMU-based state estimators.

3.7.1 Parameter Tuning and Loss Functions

To study the effectiveness of different optimization algorithms in updating the CNN weights iteratively, we use different variations of gradient descent. The optimizer with the highest accuracy is then tuned for its hyper-parameters such as learning (λ) and decay rates (β). In order for the network to learn, the loss function is minimized by updating the weights in

the direction opposite to the gradient of the loss. A mini-batch gradient descent is utilized on multiple time series data with different optimizers to update parameters in the CNN-2d model.

The corresponding accuracies are: Stochastic Gradient Descent $= 95.15\%$, Adagrad $= 97.52\%$, Adadelta $= 97.23\%$, Adam $= 97.01\%$, Adamax $= 95.35\%$ and Nadam $= 98.67\%$. From Figure 3.9 (a), it is seen that Nadam has the fastest learning rate and the lowest training loss compared to other optimizers.

Next, we tune the CNN-2d model for various learning (λ) and decay rates (β_1, β_2) with Nadam. Learning rates were varied between 1 and 10^{-6}. The accuracy varied slightly between 97.8% and 98.67% when learning rate is between 0.001 to 10^{-6}. It is seen from Figure 3.9 (b) that for a fixed epoch of 30, the network under-performed for learning rates above 0.01 resulting in exponentially increased test loss. A low learning rate results in reliable training at the cost of increased computation time. If higher learning rates are used, it is possible that the optimizer overshoots, increasing losses and decreasing accuracy.

Next, we analyze the effect of different loss functions on our model. Test loss and accuracies corresponding to different loss functions are shown in Figure 3.9 (c)-(d). Hinge and squared-hinge loss showed poor learning performance with higher test loss, while other loss functions such as mean squared error, mean absolute error, mean squared logarithmic error, categorical hinge, categorical cross-entropy and Kullback-Leibler divergence showed considerable low losses and high accuracies, with categorical cross-entropy having the highest accuracy of 98.67%.

All PMU data streams are then tested on the CNN-2d model with Nadam optimizer and cross entropy loss function with parameters $\lambda = 0.001$*, decay rates* $\beta_1 = 0.9$ *and* $\beta_2 = 0.99$*.*

For RNN and LSTM, Nadam optimizer with categorical cross-entropy loss function was

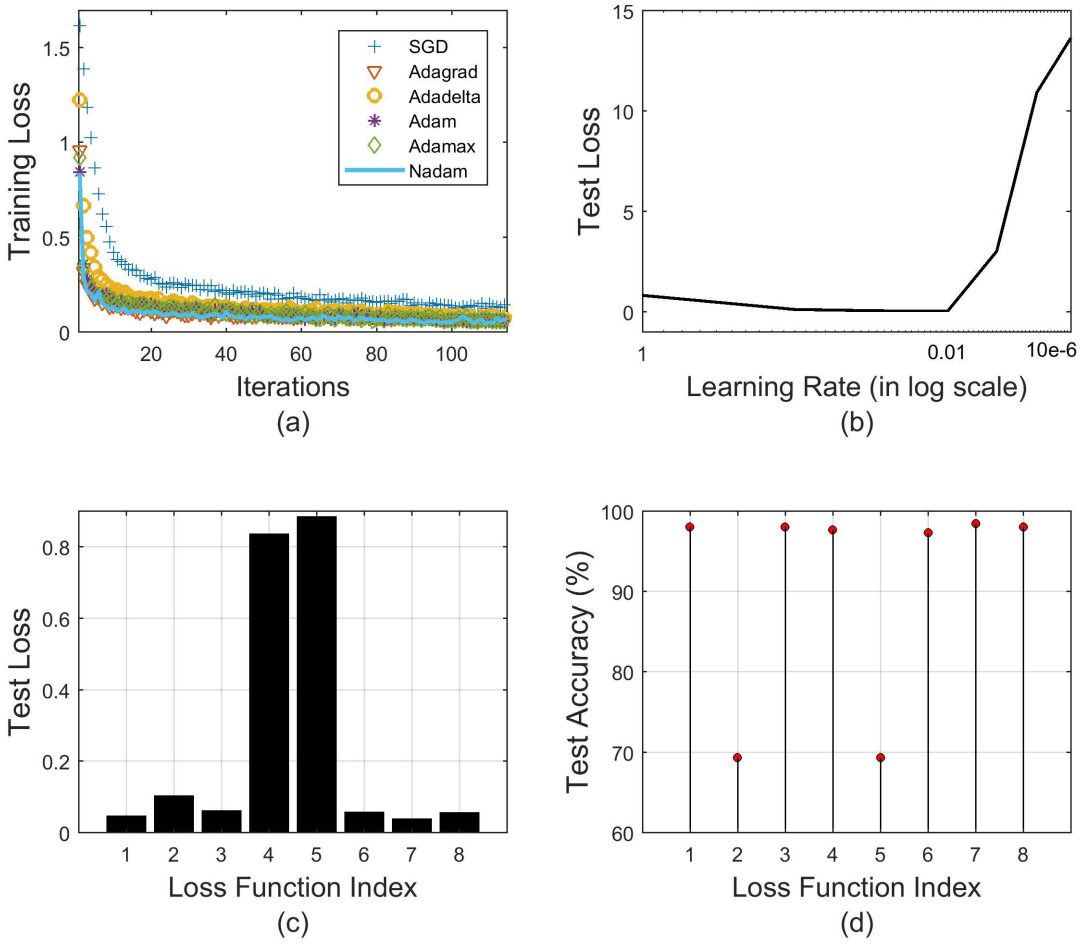

Figure 3.9: For CNN-based filter, (a) Training cost with different optimizers - (b) For Nadam optimizer, test loss with different learning rates, (c)-(d) test loss and accuracy with different loss functions - 1. mean squared error 2. mean absolute error, 3. mean squared logarithmic error, 4. hinge loss, 5. squared-hinge loss, 6. categorical hinge, 7. categorical cross-entropy and 8. Kullback-Leibler divergence

Table 3.7: Different Parameters and Accuracy (%) of RNN for IEEE-30 bus

Batch Size	Epochs	Hidden Units	Learning Rate	Cross Validation	Accuracy	Time (s)
32	15	128	0.000001	5	70	2030
32	30	512	0.0001	5	30	1800
32	30	300	0.00001	5	78.9	1420
32	**30**	**300**	**0.00001**	**10**	**91.18**	**2006**
32	20	300	0.00001	10	90.42	1550
50	30	200	0.00001	10	87.73	1022

Table 3.8: Different Parameters and Accuracy (%) of LSTM for IEEE-30 bus

Batch Size	Epochs	Hidden Units	Learning Rate	Cross Validation	Accuracy	Time (s)
32	30	300	0.00001	5	67.81	4782
32	30	300	0.00001	10	70.88	7679
32	30	128	0.0001	10	72.79	3761
32	30	256	0.0001	10	73.18	6656
50	**25**	**128**	**0.0001**	**10**	**83.18**	**3244**
32	25	200	0.00001	10	66.2	3782

considered to compare with the CNN model. The parameters such as batch size, number of hidden units, epochs, learning rates and cross validations were varied. The resultant accuracies and computation times are shown in Table 3.7 and Table 3.8. It is observed that both RNN and LSTM have lower accuracies and significantly higher computation times.

3.7.2 Robustness under Noisy and Faulty Measurements

To ensure that the proposed CNN filter is robust, we consider noisy PMU measurements as well as missing/garbage measurements. A white Gaussian noise with SNR varying between 30 and 80 dB is added [196]. The convergence plots for training and validation accuracies and the corresponding test accuracy and loss are shown in Figure. 3.10.

It is seen that CNN exhibits good performance over the noise of SNR above 30 dB. The average accuracy for noisy signal between SNR 30 to 80 dB was 94.7% with CNN and 55.25%, 89.85% and 89.99% with SVM, Bagged and Boosted trees respectively. Compared to traditional classifiers, under a SNR below 30 dB, correlations with SVM, Boosted

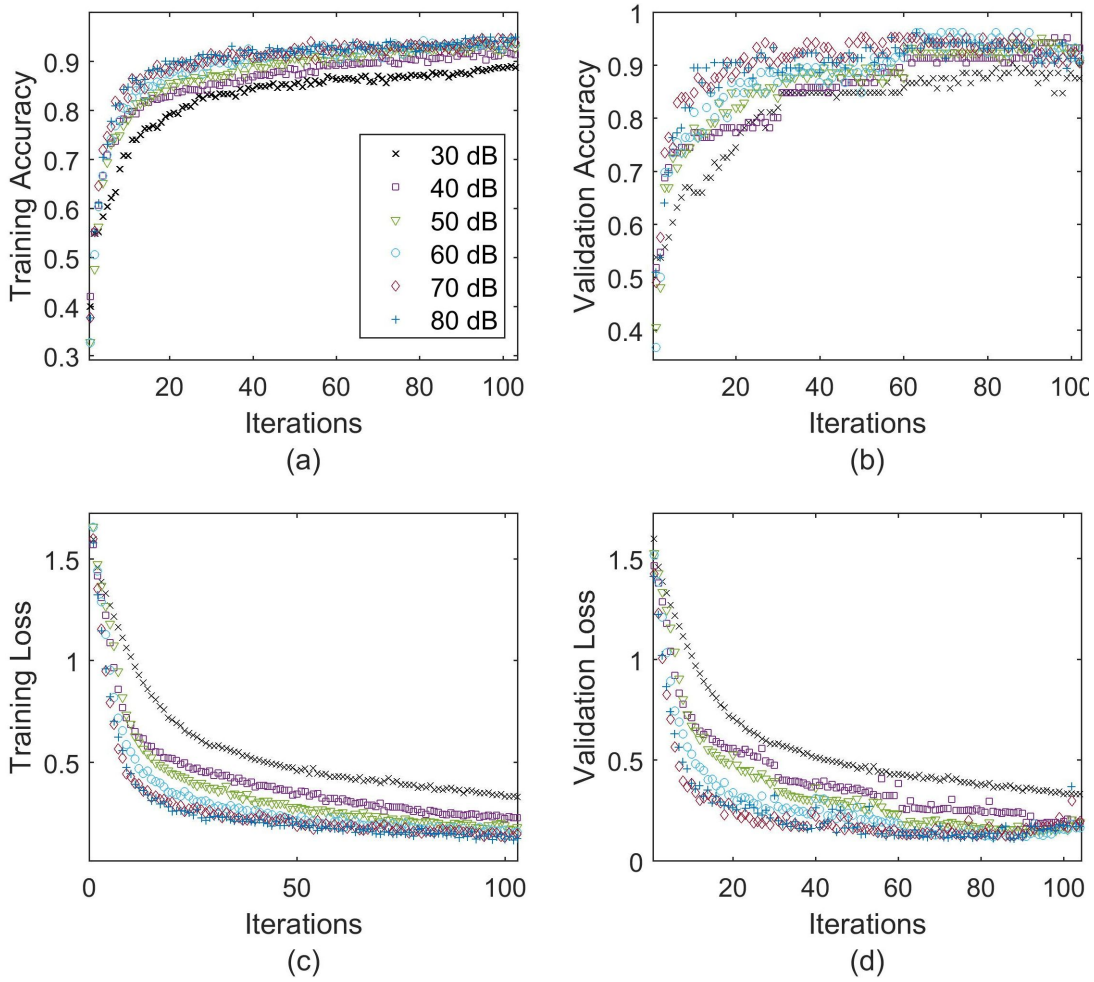

Figure 3.10: Training and validation accuracies, and training and validation loss for the developed CNN filter under different PMU measurement noise - white Gaussian noise between SNR 30dB to 80dB for CNN

and Bagged Trees had 43.3%, 67.2% and 69.0% accuracies respectively, compared to CNN which had 71.3% accuracy. This illustrates that the developed filter is able to correctly identify anomalous data streams even when the PMU data is corrupted with large noise or errors.

To account for faulty measurements or non-responsive/garbage PMU data channels, we simulate three cases of PMU time series data,

1. **Case 1** - $2 \sim 3$ time series measurements were randomly dropped to 0 at random instances of time,

Table 3.9: Accuracy (%) and Execution Time for IEEE-118 bus with Faulty Measurements

Faulty Measurements	**Case 1**	**Case 2**	**Case 3**
Accuracy	94.68	94.56	94.71
Time (sec)	147	155	140

2. **Case 2** - $3 \sim 5$ time series measurements were dropped randomly to 0 at particular instance of time, and

3. **Case 3**- all measurements from a random PMU were dropped to a random garbage value at a particular time.

The accuracies of the proposed filter with faulty measurements are shown in Table 3.9. It can be seen from all the above analysis that CNN is able to successfully identify instances of data falsification attacks from faulty measurements with significantly high accuracies.

3.8 Conclusions

False data injection attack targets PMU-based state estimator and is a major threat to the reliable operation of electric grids. If such attacks are not detected promptly, they may lead to line overloads resulting in incorrect dispatch, undesired actions such as line tripping or load shedding, or in the worst case, widespread blackouts. It is thus crucial to identify any falsified data stream prior to each cycle of state estimation. This chapter developed a data-driven attack detection algorithm by utilizing the historical PMU data archived at regional PDCs. The features of the PMU time series data are subsequently used to train multiple machine learning models to discover and detect false data and events in real-time. It is observed that the convolutional neural network based detector demonstrates a superior performance over all other classifiers such as recurrent neural networks, long short term memory, support vector machine, and Bagged-and-Boosted trees. Additionally, the CNN-based data classifier was able to accurately classify more than 94% of the false data streams under large PMU measurement errors. This makes the CNN based detector suitable to be

employed at regional substations for detecting anomalous PMU data streams. The model can be periodically trained offline with updated dataset, and subsequently deployed to safeguard against false data in near real-time, prior to each run of the state estimator. As a result, this approach provides the utilities an early warning system to detect sophisticated data attacks and enable better decision making for reliable grid operations.

Chapter 4

Mitigation of False Data Attacks

4.1 Introduction

The proliferation of phasor measurement units, albeit transformative to grid operations, has increased the risk of cyber-threats in power systems. One consequence of these cyber-threats is incorrect operator actions based on misleading data. While a single operator action might not result in a cascading outage, a series of wrong actions impacting critical lines and transformers, combined with pre-existing faults or scheduled maintenance, may result in a widespread blackout. Examples of such cyber-attack induced cascading failures were explored in Chapter 2.

This chapter first provides a background of current mitigation approaches to counter data falsification attacks. Next, this chapter addresses power system recovery plans when sophisticated cyber-attacks, combined with other system pre-conditions, have already impacted the system. Traditionally, controlled islanding techniques serve as countermeasures to stabilize the system following a fault by creating smaller islands that can be restored rapidly. However, controlled islanding is only effective when the received measurements are trustworthy. We investigate how existing islanding methods need to be modified to accommodate uncertainty of PMU measurements under false data attacks.

Two controlled islanding strategies are developed under the lack of knowledge, or partial knowledge of cyber attacks. Under the lack of knowledge of attacks, the multi-objective optimization problem maximizes the observability of the islands using a minimum number of PMUs. When partial knowledge of attack is available, the size of the island with vul-

nerable measurements is minimized to contain the impacts of attacks. In both the cases, additional objectives are included to minimize the load-generation imbalance of the islands and the total line powerflow disconnection. The islanding problem is configured as a multi-objective optimization problem which provides system operators the flexibility to create islands according to their preferences. The trade-offs between multiple optimal solutions are investigated on realistic power system scenarios by varying objective priority, relative weights, and solution degradation tolerances. The developed islanding approach is designed as an effective strategy to quickly recover power grids from unexpected cyber and physical events.

4.2 Background

Phasor measurement units (PMU) can significantly enhance grid situational awareness. Specifically, by providing accurate real-time measurements, PMUs improve network observability, to yield accurate state estimation solutions. However, PMUs are thought to be vulnerable to sophisticated cyber-attacks [38, 41, 197, 198]. Attacks originating from the cyber space exploit existing vulnerabilities in commonly used IEC 61850 and IEEE C37.118 PMU/SCADA control and communication architecture [38, 42]. Attacks can modify time stamps to change phase angle measurements [38], or inject false data in voltage and current measurements to alter the estimated states [197, 198]. The worst-case attacks could be unobservable [198] and result in wrong power flow, incorrect generator dispatch, and line overloads [18, 199]. Attacks may result in a series of incorrect operator actions impacting critical lines and transformers, resulting in load shedding and unintentional islanding [29, 30].

4.2.1 Mitigation Approaches to Counter False Data Attacks

For system response and recovery from cyber attacks, current critical infrastructure protection (CIP) standards propose utilization of redundant systems, backup and storage of information, proper incident handling, attack containment, eradication and resolution [200]. However, countermeasures to alleviate the impact of ever increasing sophisticated cyber-attacks still remain rudimentary. Several novel preventive mitigation techniques have been proposed to prevent cyber attacks from adversely impacting the electric grid.

The first line of preliminary defense includes defending an optimal set of meters that protect a set of state variables [201]. The problem of optimal meter protection was proven to be a variant of the minimum Steiner tree problem, thus NP-hard, and was solved using (a) Steiner vertex enumeration and (b) mixed integer linear programming with a tree pruning heuristic [201].

Rahman et al. [202] proposed the randomization of state estimation measurement sets while maintaining complete observability. Additionally, physical line admittance values were proposed to be altered using Flexible AC Transmission System (FACTS) devices to deter attacks.

Khanna et al. [203] proposed a generator mismatch index and a zero injection bus index based on power mismatch. False data attacks against AGC was detected by exploiting inconsistencies between the observed and the predicted frequency deviations [204]. For correct computation of ACE, power export deviation estimates were replaced by load forecast. Further, direct time-delay attacks against ACE was mitigated through a two-stage methodology [205] - (1) tuning of PI controller gain to extend the region of stable operation followed by (2) allowable load shedding. Safety boundaries for both the stages were obtained using extreme learning machine techniques.

To mitigate effects of false data attacks against distributed energy resources, Johnson et al. [206] proposed adjusting frequency and voltage ride-though trip settings, establishing maximum ramp rates for DER during normal and start-up operation, constraining watt-power factor controls to prevent voltage excursions and limiting active-power control by frequency-watt functions.

Other preventive measures include (a) IP Fast Hopping to conceal IP address to prevent unauthorized access [207] and (b) temporary disconnection of suspicious PMUs for troubleshooting [204, 208].

Most of the above threat mitigation approaches are, to an extent, preventive in nature. Research on impact mitigation, when successful cyber attacks have already bypassed the inherent system security and yielded severe consequences, are limited. Kushal et al. [209] proposed the use of autonomous battery backup system, independent of the central EMS, to counter attacks targeting load curtailment. The authors in [210] propose re-closing strategic lines that limit inrush currents and power swings as a recovery mechanism when attacks result in multiple line trips. Ashrafuzzaman et al. [211] conceptualized the Grid-watch model that aimed to create independent self-sustainable partitions with local control, denying attackers access to the most valuable assets such as generators and transformers. A detail analysis on local controls are however missing.

In the worst case scenarios, coordinated false data attacks result in a series of incorrect operator or automatic control actions that can impact critical lines, generator and transformers. When combined with faults and other system pre-conditions, it may result in widespread blackouts, as discussed in Chapter 2.

4.2.2 Traditional Controlled Islanding Approaches

Controlled islanding is the last resort solution that prevents cascading failures by isolating the faulty regions from the rest of the grid, and creating smaller partitions that can be restored rapidly [139, 141, 212–219]. An example of controlled islanding that partitions the system into four islands following a delayed clearing of generator fault is illustrated in Figure. 4.1.

Typically after a severe disturbance such as large faults, sudden loss of large generators, load clusters or critical tie-lines, there exist two kinds of motions. Generators close to the fault point have fast non-coherent motions while those further away exhibit slow coherent motions. For a total of n states, the system is partitioned into $(n-r)$ fast states and r slow states [220]. The number of slow states r correspond roughly to the number of generator clusters that exhibit slow oscillations (coherency) w.r.t other clusters in their neighborhood and is independent of the disturbance size. To identify the coherent generators, the following steps are performed [220, 221],

1. linearize the non-linear electro-mechanical model of the system, $\ddot{x} = M^{-1}Kx = Ax$, where M, K, A are the inertia, connection and system matrix respectively,

2. compute the eigenvectors and eigenvalues $[V, D] = eig(A)$,

3. find the largest eigen-gap r which approximately defines the number of coherent areas in the system,

4. compute the basis matrix V for r slowest modes,

5. perform Gaussian elimination on V and assign the elements of the first r rows as the reference generators,

6. assign the rest of the generators to the reference generators.

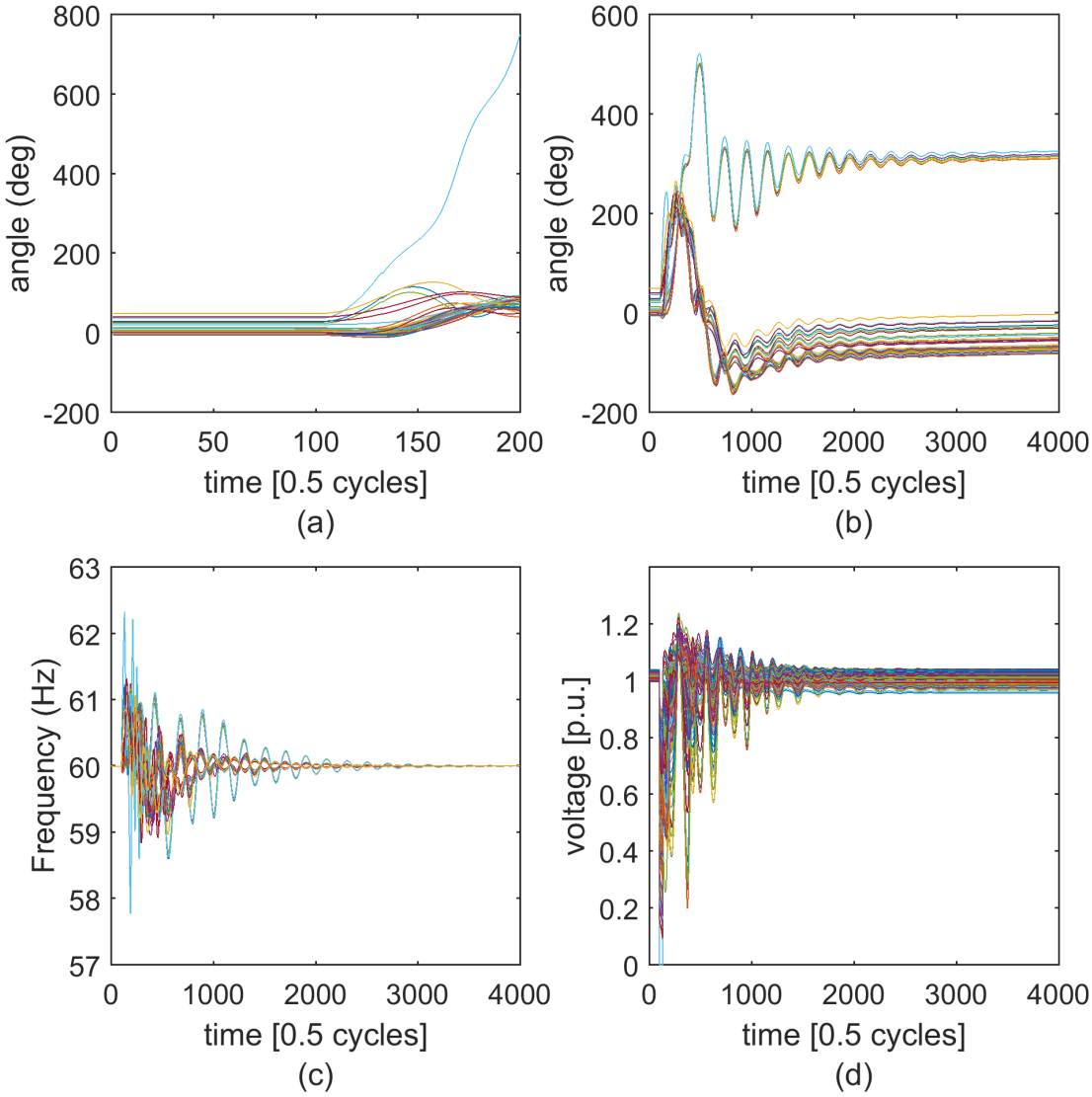

Figure 4.1: Visualization of generator angle, frequency and voltage under fault and islanding conditions - (a) Generator angle exceeds set point due to stuck breaker after fault, (b) controlled islanding partitions the system into 4 islands to prevent system wide instability by maximizing the load-generation balance in each island, (c) island frequency is restored to 60 Hz, (d) voltage stabilizes to 1 p.u. with controlled islanding.

These inter-area coherent generator clusters are connected through long distance transmission lines and have weak electrical connections between them. During controlled islanding, the partitions are obtained based on the coherent generator sets and weak interconnections between areas [214, 219, 222, 223]. An example in Figure 4.2 demonstrates the coherent groups of generators for a fault on line 25-199 in the 200-bus system. It is seen that generator cluster containing generator buses $49, 50, 51, 52, 53$ and 65 in Coherent Group 1, near the fault location, exhibit large oscillations compared to other generators in Coherent Group 2.

The coherent set of generators can also be quickly identified using a hierarchical clustering on real-time PMU measurements [224]. Figure 4.3 shows the coherent generators obtained from the hierarchical clustering algorithm.

Traditionally, islanding pursues two objectives: (1) minimizing the load-generation imbalance in each island to enhance the steady-state stability [139, 219], and (2) minimizing the total line power-flow disconnection to enhance the system transient stability [215–218].

Minimizing the load-generation imbalance improves steady state stability, prevents frequency excursions, minimizes load loss and reduces dependencies on large black-start units [139, 225]. The idea of creating balanced partition was investigated by Sun. et al [139] where the objective is to constrain the total active power injections (positive for generation and negative for load) in an island within a user-defined tolerance. The splitting problem is a typical satisfiability checking problem and a three-phase method was introduced to reduce the computational complexity. The power network was first simplified using (a) node removal and merging, (b) node combination on same voltage level and (c) edge cut off, and an exhaustive search was then performed to find feasible solutions.

On the other hand, most research consider the objective of minimizing the line power flow disconnection during controlled islanding [218, 226–229]. This is because islands

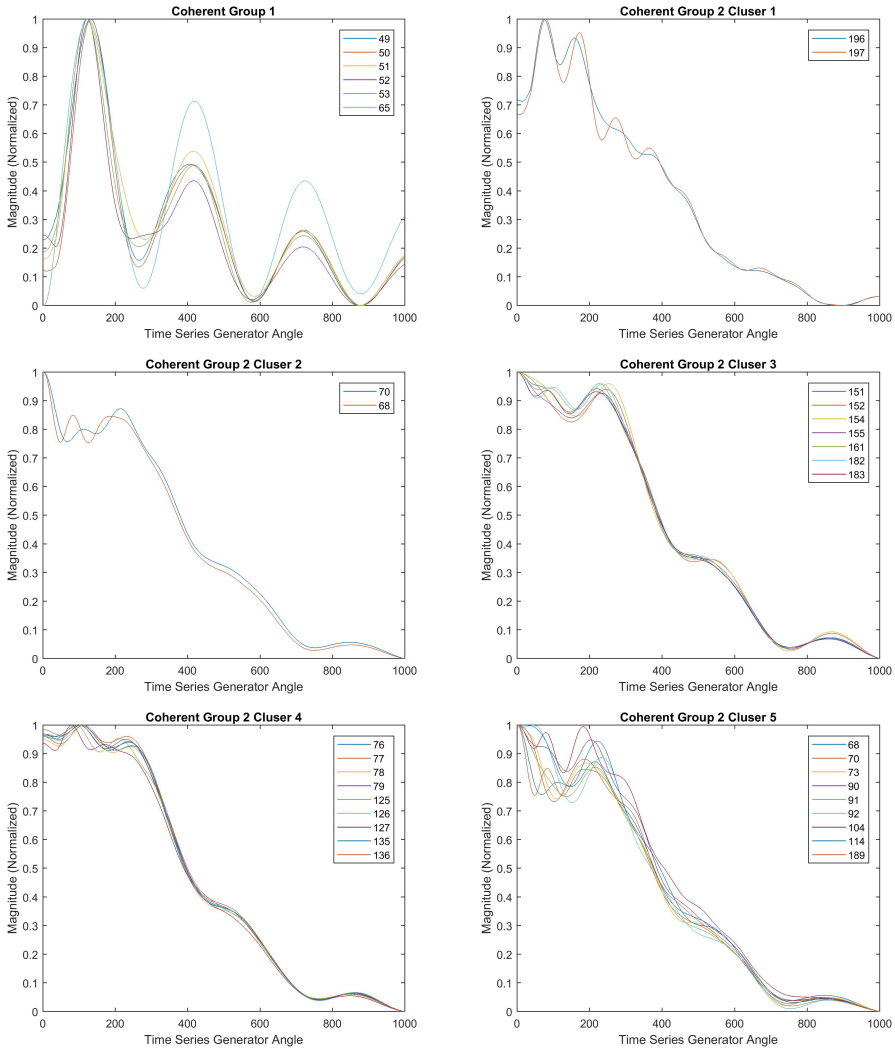

Figure 4.2: Visualization of rotor angles for coherent Generators following delayed clearing of fault on line 25-199 in the 200 bus system. There exists two distinct coherent set of generators. Coherent group 1 is near the fault and has large swings. Coherent group 2 is further away from the fault location.

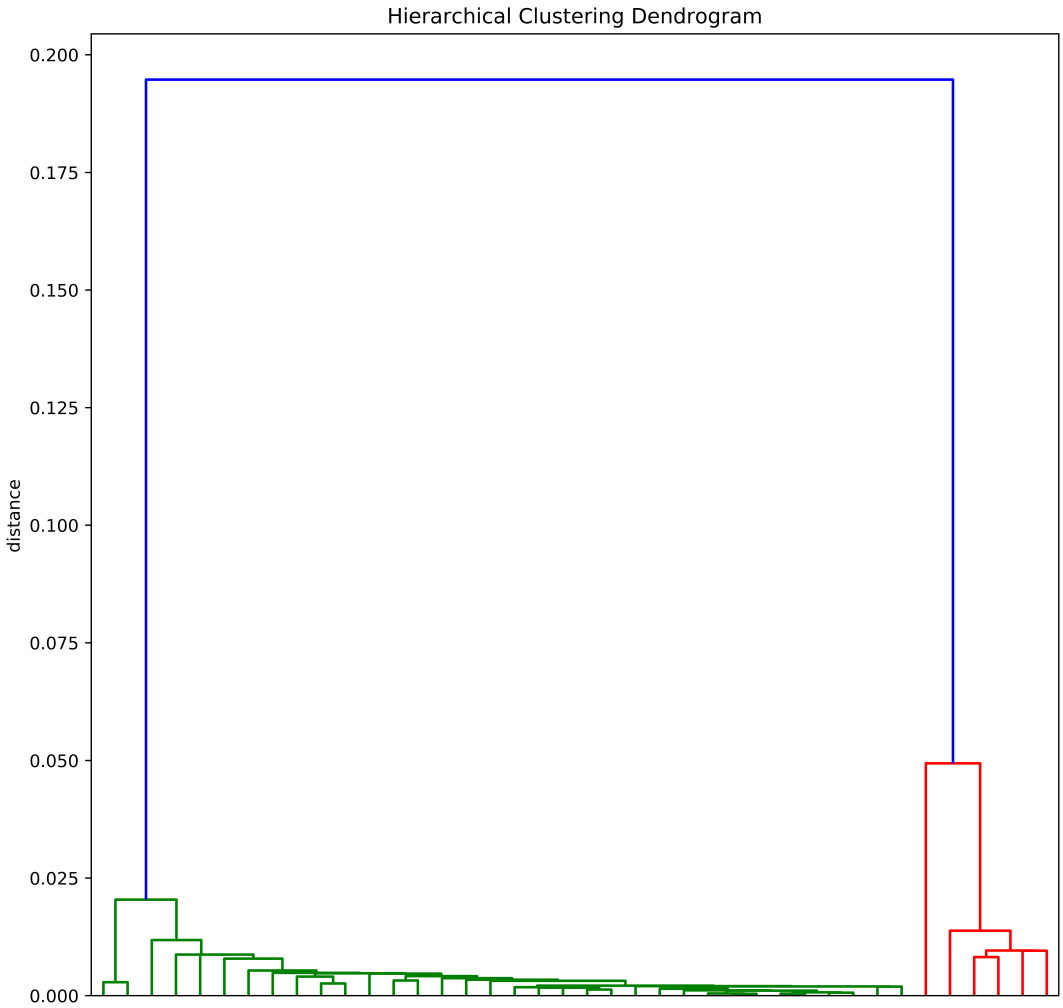

Figure 4.3: Coherent generators obtained using hierarchical clustering algorithm on rotor-angle time series data. Two distinct coherent set of generators are obtained following fault on line 25-199. The clusters are indicated by different colors.

with negative transient stability index are more susceptible to collapse than islands with load-generation imbalance [215]. This is because load-generation imbalance can be mitigated using load and generator shedding. The problem of minimizing the line power flow disconnection is formulated as a variant of max-flow/min-cut problem and solved using efficient heuristics. Provisions to minimize both MW and MVAR flow outage were considered in [217, 218, 230]. A multilevel recursive bisection algorithm was applied with intermediate steps of coarsening, partitioning, un-coarsening and solution refinement [218]. Trodden et al. [230] used a piece-wise linear AC power flow to accommodate both voltage and reactive power constraints during islanding. Additional penalties were introduced to reduce transmission line disconnection, generator shut-down, and outage of heavily-loaded lines. To mitigate large imbalances, provisions to include black-start units were proposed by Tortós et al. [227]. Further, mixed integer linear programming models for controlled islanding were proposed by authors in [216, 217, 228]. These models introduced system splitting at the busbar-switch level [216] and recursive linearization based on electrical distance [217]. Additional discussions on the existence of multiple islanding solutions was presented in [228].

Traditional controlled islanding techniques have shown to stabilize the system from evolving into a cascading failure by creating smaller islands that can be restored rapidly. However, the islanding decision is particularly effective for steady state and transient stability assuming that the received information about the status of the system is trustworthy. This chapter questions this assumption and specifically seeks to modify existing controlled islanding techniques by incorporating cyber attack uncertainty, an approach which has not been considered in the literature. As a result, our approach seeks to curtail attacks and limit the adverse impacts to the largest extent possible.

4.3 Incorporating Cyber Attack Uncertainties in Islanding

Controlled islanding is only effective when the received information about the status of the system is trustworthy. As sophisticated attacks may prevent system operators to identify what part of the network is compromised, we study how existing islanding methods need to be modified to accommodate PMU measurement uncertainties. The developed controlled islanding strategies are considered under two distinct scenarios of cyber threats,

1. **Scenario 1 under complete attack uncertainty:** maximize the island observability with minimum number of additional (non-secure) PMUs; and

2. **Scenario 2 under partial attack uncertainty:** isolate vulnerable PMUs to a small island.

Figure. 4.4 illustrates the overall process developed in the chapter. With no prior knowledge of false measurements, designing a recovery approach is inherently difficult. If the locations of the vulnerable PMUs, that provide synchronized measurements, cannot be identified, the attack impacts are minimized by creating islands that require a minimal number of PMU measurements for maximal observability in state estimation. To the best of our knowledge, the problem of creating maximally observable islands with minimum PMUs has not been addressed before. In contrast, if the operators can identify the location of the potential attack by analyzing PMU measurements [231], the aforementioned mitigation approach isolates vulnerable PMUs to only a small part of the system while creating stable and observable islands. With this introduction, the main contributions of this chapter over the existing controlled islanding schemes can be summarized as,

1. Incorporating measurement uncertainties: Two new strategies are developed for controlled islanding under the lack of knowledge, or partial knowledge of false mea-

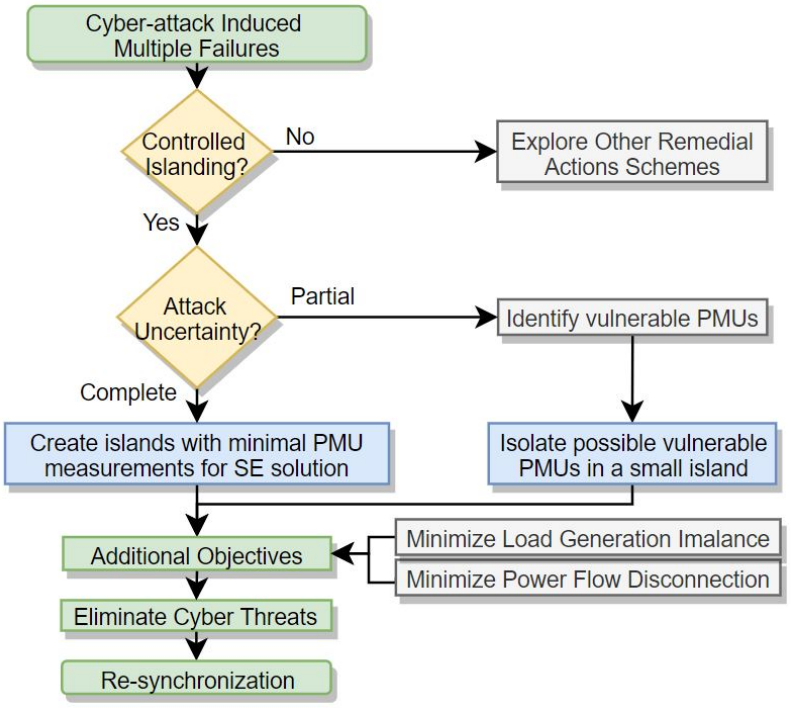

Figure 4.4: Flowchart of recovery process from successful cyber attack

surements on the system. The problem of controlled islanding is formulated as a multi-objective optimization problem that yields stable and observable islands, while ensuring wrong PMU measurements impact a minimal number of partitions. Trade-offs between the observability of islands, the total line power flow disconnection, and the size and location of the islands are investigated.

2. Minimizing the loss of observability: A new method is developed to minimize the loss of observability during the partition process. This approach is particularly effective when system operators seek to obtain reliable state estimation solutions for the newly-formed islands with minimum PMUs in each island.

4.4 Scenario 1: Islanding under Complete Uncertainty

In this section, a controlled islanding strategy with two competing objectives will be developed to (1) maximize the observability of islands and (2) minimize the number of utilized

PMU measurements. The most notable advantage is that more resources can be deployed to secure a small subset of PMUs for maximal observability. This leads to a more reliable state estimation and improves the island re-synchronization process. The minimum number of retained PMUs for observability also depends on additional steady-state and transient stability objectives described in Section 4.6. For the rest of the chapter, it is assumed that,

1. the power network is completely observed by a redundant set of PMUs [133], and

2. there exists a subset of PMUs that observe critical generators, transformers, and tie-lines, and are secured by prior design [232].

To formulate this problem, first, the power network is represented as a graph $\mathcal{G}(\mathcal{N}, \mathcal{Z})$, where $\mathcal{N}$ is the set of all buses and $\mathcal{Z}$ is the set of all transmission lines [215]. Further, $\mathcal{Z}_S$ and $\mathcal{Z}_{\setminus S}$ denote the set of lines with secure and non-secure PMU measurements respectively.

4.4.1 Objective 1: Maximize Island Observability

A non-PMU bus is observable when it is incident to a line with a current phasor measurement from a neighboring PMU [134]. Loss of observability occurs when lines with secure or nonsecure PMU measurements are disconnected during islanding [134, 233]. This chapter explores a new scenario that leads to further loss of observability.

Consider the situation when the system is already impacted by sophisticated false data injections that may remain undetected for a long time. To stabilize the system, prompt controlled islanding decisions are imperative. In the absence of any information on the trustworthiness of the measurements, the approach introduced here aims to utilize only a small number of strategically placed nonsecure PMUs to minimize the impact of wrong PMU measurements in each island. Additional security can now be established for the

smaller set of PMUs, thereby improving system recovery. In this process, other nonsecure PMU measurements, which may be possibly compromised, are not used, which leads to the unobservability of buses.

To take into account the loss of observability under both situations, two binary variables are defined. Variable $z_{i,j}, \forall (i,j) \in \mathcal{Z}$ denotes a line status as,

$$z_{i,j} = \begin{cases} 0 & \text{if line } (i,j) \text{ is disconnected} \\ 1 & \text{if line } (i,j) \text{ is in service} \end{cases} \tag{4.1}$$

and the second binary variable $d_{i,j}, \forall (i,j) \in \mathcal{Z}_{\setminus S}$ denotes the measurement status,

$$d_{i,j} = \begin{cases} 1 & \text{if line measurement } (i,j) \text{ is retained} \\ 0 & \text{if line measurement } (i,j) \text{ is discarded} \end{cases} \tag{4.2}$$

Note that lines with secure measurements can be disconnected during islanding, however, their measurements are never intentionally discarded. Non-secure lines can be disconnected, and their measurements discarded, which is accounted for by the product of the two binary variables, $d_{i,j} z_{i,j}$.

Remark 1. The product of the two binary variables $d_{i,j} z_{i,j}$ is replaced by an additional binary variable $v_{i,j}$ and the following set of linear constraints,

$$v_{i,j} \leq d_{i,j} \tag{4.3}$$

$$v_{i,j} \leq z_{i,j} \tag{4.4}$$

$$v_{i,j} \geq d_{i,j} + z_{i,j} - 1 \tag{4.5}$$

The constraints (4.3)-(4.4) imply $v_{i,j} = 0$ when $d_{i,j} = 0$ or $z_{i,j} = 0$. The constraint (4.5) implies $v_{i,j} = 1$ only when both the variables are one.

The observability decision matrix $\boldsymbol{Z} \in \mathbb{R}^{m \times m}$ is defined as,

$$\boldsymbol{Z} = \left[\begin{array}{c|c} \boldsymbol{Z_S} & 0 \\ \hline 0 & \boldsymbol{Z_{\backslash S}} \end{array}\right] = \left[\begin{array}{cc|c} . & & \\ & z_{j,k} & 0 \\ & . & \\ \hline & & . \\ 0 & & v_{i,j} \\ & & . \end{array}\right] \tag{4.6}$$

where the diagonal sub-matrices $\boldsymbol{Z_S}$ and $\boldsymbol{Z_{\backslash S}}$ correspond to lines that are secure $(j,k) \in \mathcal{Z}_S$ and non-secure $(i,j) \in Z_{\backslash S}$, respectively.

Next, the matrix for topological observability $\boldsymbol{H}$ at the bus/branch level is constructed using the line current measurements. The elements of matrix $\boldsymbol{H}$ corresponding to states V_i and V_j are set as 1 when a line current flow between nodes i and j is measured, and is shown as [65],

$$\boldsymbol{H} = \left[\frac{\boldsymbol{H_S}}{\boldsymbol{H_{\backslash S}}}\right] = \begin{array}{c} \\ . \\ I_{j,k} \\ . \\ \hline . \\ I_{i,j} \\ . \end{array} \begin{array}{c} \begin{array}{cccccc} \hat{V}_i & . & \hat{V}_k & . & \hat{V}_j & \hat{V}_n \end{array} \\ \left[\begin{array}{cccccc} . & . & . & . & . & . \\ 0 & 0 & 1 & . & 1 & 0 \\ . & . & . & . & . & . \\ \hline . & . & . & . & . & . \\ 1 & 0 & 0 & . & 1 & 0 \\ . & . & . & . & . & . \end{array}\right] \end{array} \tag{4.7}$$

where the sub-matrices $\boldsymbol{H_S}, \boldsymbol{H_{\backslash S}}$ correspond to the secure and the non-secure lines respectively. The system is fully observable when the gain matrix $\boldsymbol{G} = \boldsymbol{H^T H}$ has a full rank [234]. To incorporate the measurement uncertainties during controlled islanding, a new gain matrix is constructed as,

$$\boldsymbol{G} = (\boldsymbol{ZH})^{\boldsymbol{T}}(\boldsymbol{ZH}) = \boldsymbol{H^T Z^T ZH} = \boldsymbol{H^T ZH} \tag{4.8}$$

Here, $\boldsymbol{Z}$ is a binary diagonal matrix and hence $\boldsymbol{Z^T Z} = \boldsymbol{Z}$.

When diagonal elements of $\boldsymbol{Z}$ become zero during controlled islanding, it drives an entire column of $\boldsymbol{G}$ to zero. In this scenario, a node becomes unobservable if it is not observed directly or indirectly by another PMU. Thus, the objective of maximizing the system observability is defined as,

$$\tilde{F_1} \quad = \quad \text{rank}(\boldsymbol{H^T Z H}) \tag{4.9}$$

The $\text{rank}(\boldsymbol{H^T Z H}) = \text{rank}(\boldsymbol{G})$ is the number of the corresponding non-zero eigenvalues. As $\boldsymbol{G}$ is positive semi-definite, $\text{rank}(\boldsymbol{G})$ is a quasiconcave function and NP-hard to maximize. Instead, $\text{rank}(\boldsymbol{G})$ is replaced with $\text{trace}(\boldsymbol{G})$, which serves as a convex proxy [235]. Hence, (4.9) becomes convex as,

$$F_1 \quad = \quad \text{trace}(\boldsymbol{H^T Z H}) \tag{4.10}$$

Remark 2. The convex proxy or convex hull of a function is the largest convex underestimator of the function. The convex hull of the function $rank(\tilde{\boldsymbol{G}})$ is the nuclear norm $||\tilde{G}||_*$ where $||\tilde{\boldsymbol{G}}||_*= \sum_{i=1}^{m} \sigma_i$, i.e, the sum of singular values. When $\tilde{\boldsymbol{G}}$ is symmetric and positive semi-definite, $\sigma_i = \lambda_i$, i.e. the singular values are equal to the eigenvalues and the nuclear norm reduces to $\text{trace}(\tilde{\boldsymbol{G}})$. The proof [236] relies on the fact for any function F, the conjugate of the conjugate F^{**} is the convex hull of the function F. The conjugate of the rank function can be written as $\phi^*(\boldsymbol{A}) = \sup_{||\tilde{\boldsymbol{G}}||\leq 1}(\text{Trace}(\boldsymbol{A^T}\tilde{\boldsymbol{G}}) - \phi^*(\tilde{\boldsymbol{G}}))$. The conjugate of the conjugate can similarly be written as $\phi^{**}(\boldsymbol{B}) = \sup_{||\boldsymbol{A}||\leq 1}(\text{Trace}(\boldsymbol{B^T A}) - \phi^*(\boldsymbol{A}))$. Using Von Neumann's trace theorem and some algebraic manipulation, it can be proved that $\phi^{**}(\boldsymbol{B}) = \sum_{i=1}^{m} \sigma_i = ||\boldsymbol{B}||_*$. When matrix $\tilde{\boldsymbol{G}}$ is symmetric and positive semi-definite, $\tilde{\boldsymbol{G}}v = \lambda v \Rightarrow \tilde{\boldsymbol{G}}^{\boldsymbol{T}}\tilde{\boldsymbol{G}}v = \tilde{\boldsymbol{G}}^{\boldsymbol{T}}\lambda v$. Since $\tilde{\boldsymbol{G}}^{\boldsymbol{T}} = \tilde{\boldsymbol{G}}$, hence $\tilde{\boldsymbol{G}}^{\boldsymbol{T}}\tilde{\boldsymbol{G}}v = \lambda^2 v$. Further $\lambda \geq 0$, $\sqrt{\lambda^2} = \lambda$, thus the singular values are equal to the eigenvalues. The trace of the positive semi-definite matrix $\tilde{\boldsymbol{G}}$ is equal to the sum of eigenvalues and hence

$||\tilde{\boldsymbol{G}}||_*$= trace($\tilde{\boldsymbol{G}}$). The trace($\tilde{\boldsymbol{G}}$) is the convex hull of rank($\tilde{\boldsymbol{G}}$), and is a convex function.

Remark 3. While using commercial solvers, coding the expression $\mathrm{trace}(\boldsymbol{H^T Z H})$ in (4.10) creates matrices that hold binary variables (instead of floating point numbers). For a large power system, this consumes extensive memory. Instead, using the properties of the trace of matrix products, the term in (4.10) is conveniently written as,

$$\mathrm{trace}(\boldsymbol{H^T Z H}) = \mathrm{trace}(\boldsymbol{Z H H^T}) = Z_{i,i} \sum_{j=1}^{n} H_{ij}^2 \tag{4.11}$$

4.4.2 Objective 2: Minimize the Number of Retained PMUs

The challenging problem of system recovery under complete uncertainty is addressed by creating smaller islands that require a minimum number of additional non-secure PMU measurements for maximal observability. This allows the system operators to deploy targeted resources to secure a specific subset of PMUs. The objective of retaining a minimum number of additional non-secure PMUs is formulated as,

$$F_2 \quad = \quad \sum_{(i,j)\in \mathcal{Z}_{\setminus S}} \beta_i d_{i,j} \tag{4.12}$$

where β_i is the measure of vulnerability defined for PMU i. One way to calculate β_i is to measure how frequently PMU i appears in all possible attack scenarios, using the algorithm in [5]. It can also be estimated based on how often a measurement leads to bad data based on historical data.

To ensure all non-critical PMU line measurements are either simultaneously used or discarded by the operator, an additional constraint is added as,

$$d_{i,j} = d_{i,k} \qquad \forall k, \quad \forall (i,j),(i,k) \in \mathcal{Z}_{\setminus S} \tag{4.13}$$

Combining objectives F_1 and F_2 allows the system operators to maximize island observability using a minimum number of additional non-secure PMUs. During the post-attack recovery, this approach leads to minimizing the resources required, by securing only a small subset of PMUs.

4.5 Scenario 2: Islanding under Partial Uncertainty

In this section, a new controlled islanding strategy under partial information on cyber-attacks is developed to,

1. isolate vulnerable PMUs to a small island, and

2. maximize the observability of the islands.

The size of the island also depends on the additional load generation and transient stability objectives described in Section 4.6.

4.5.1 Objective 1: Isolate PMUs under Attack

Consider false data injections that alter specific PMU measurements to bypass the state estimator. Partial information on potentially vulnerable PMUs may be identified by scanning ports, user logs, and registry entries [237]. False measurements are also discerned by analyzing PMU measurements using *model-based* and *data-driven* detection techniques [168, 231]. With model-based approaches, false data may be partially detected by (1) estimation-based methods that compare the estimated states with the state measurements, and (2) direct calculation-based methods that combine measurements and system parameters to detect anomalies. On the other hand, data-driven methods employ various supervised and unsupervised machine learning algorithms to detect data anomalies.

Assume node i is flagged as vulnerable based on the partial information that may be obtained from any of the above described methods. To ensure effective isolation, the objec-

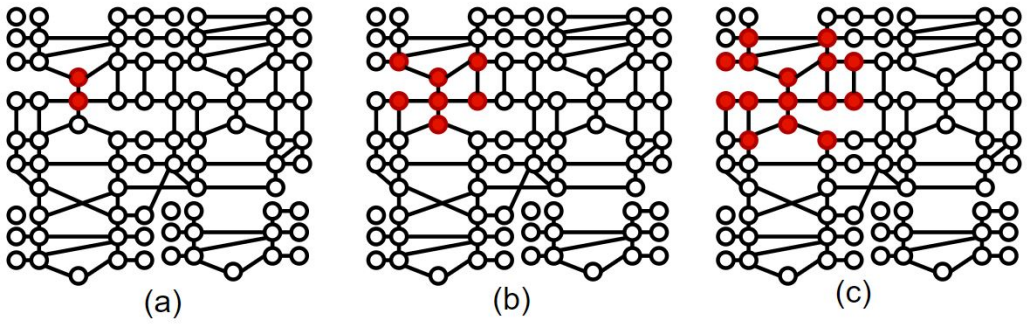

Figure 4.5: Scenario 2: (a) PMUs (shaded nodes) identified as untrustworthy, (b) 1-hop and (c) 2-hop distance neighbors. All PMUs at R-hop distance are assumed vulnerable and will be isolated in a single small island. Additional nodes are added during the optimization process to maintain island stability and observability.

tive is to isolate all possible vulnerable PMUs into a single island. The idea is illustrated in Fig. 4.5. Centered at node i, all nodes $\mathcal{N}_i$ at a radius R are labeled as vulnerable. A standard breadth-first search is employed for this purpose, where the search starts at the root node i and explores all neighboring nodes in the same level before moving at the next depth [238]. The value of R may be determined by the system operator based on the PMU communication network architecture. The process is repeated for each suspected node.

The optimization problem is designed as follows. First, a binary variable $x_i, \forall i \in \mathcal{N}$ is defined that denotes the placement of node i in an island as,

$$x_{i,h} = \begin{cases} 1 & \text{if node } i \text{ is in island } h \\ 0 & \text{otherwise} \end{cases} \tag{4.14}$$

The size of the island with vulnerable PMUs is minimized with the objective function defined as,

$$F_3 \quad = \quad x_{1,h} + x_{2,h} + ... + x_{n,h} = \sum_{i=1}^{n} x_{i,h} \tag{4.15}$$

In (4.15), $h = 1$ is explicitly set to indicate that all potentially compromised PMUs are contained in partition '1'. This smaller partition is denoted by sub-graph $\mathcal{G}' \subseteq \mathcal{G}$. When

combined with additional objectives described in Section 4.6, the optimization problem in (4.15) will isolate all possible vulnerable PMUs while creating stable partitions.

4.5.2 Objective 2: Maximize Island Observability

An additional objective is introduced to maximize the observability of the newly formed islands. Buses may lose observability when multiple lines are disconnected during islanding. An observability decision matrix is defined as,

$$\boldsymbol{Z} = \text{diag}(z_{i,j}) \qquad \forall (i,j) \in \mathcal{Z}_{\setminus S} \tag{4.16}$$

where $z_{i,j}$ is described in (4.1). The decision matrix $\boldsymbol{Z}$ takes into account the impact of physical line disconnection on system observability. The optimization problem is defined as maximizing the $\text{trace}(\boldsymbol{H^T Z H})$, where H is the topological observability matrix described in (4.7). This problem is similar to (4.10).

4.6 Additional Objectives and Islanding Constraints

4.6.1 Load-Generation Balance

For **Scenario 1** and **Scenario 2** additional objectives are considered to maintain the load-generation balance and minimize the total power flow outage. Consider P_i as the net injected power at node i. The load-generation imbalance in each island is minimized as [239],

$$\tilde{F}_4 \quad = \quad \sum_{h=1}^{K} \left| \sum_{i=1}^{n} P_i x_{i,h} \right| \tag{4.17}$$

To tackle the absolute values, the equation in (4.17) is written as a linear program by introducing slack variables. Let the slack variable $S_h = \left| \sum_{i=1}^{n} P_i x_{i,h} \right|$ denote the mismatch

in island h. Accordingly, (4.17) is written as,

$$F_4 \quad = \quad \sum_{h=1}^{k} S_h \tag{4.18}$$

with two additional constraints which are defined as,

$$\sum_{i=1}^{n} P_i x_{i,h} \geq -S_h \tag{4.19a}$$

$$\sum_{i=1}^{n} P_i x_{i,h} \leq S_h \tag{4.19b}$$

The process of islanding is guided by coherent generator sets and weak interconnection between areas [213,214]. Balanced islands in (4.18) prevent frequency excursions, minimize load interruption and reduce dependencies on black-start units.

4.6.2 Line Power Flow Disconnection

On the other hand, the objective to minimize the total line powerflow disconnection is defined as [217],

$$F_5 \quad = \quad \frac{1}{2} \sum_{(i,j)\in\mathcal{Z}} (1 - z_{i,j}) P_{i,j} \tag{4.20}$$

Minimizing the line powerflow outage prevents the creation of islands with a negative transient-stability margin, and thereby avoids system collapse [215].

4.6.3 Partitioning and Connectivity Constraints

The details of the partition and the connectivity constraints are described below [217]. The binary variables $z_{i,j}$ and $x_{i,h}$ are coupled through another binary variable $w_{i,j,h}$ as,

$$z_{i,j} = \sum_{h} w_{i,j,h} \tag{4.21}$$

$$w_{i,j,h} \leq x_{i,h} \tag{4.22}$$

$$w_{i,j,h} \leq x_{j,h} \tag{4.23}$$

$$z_{i,j} = z_{j,i} \tag{4.24}$$

The constraint restricting a node to a single island is given by,

$$\sum_{h} x_{i,h} = 1 \tag{4.25}$$

Additionally, ensuring at least M nodes are present in an island is enforced by the constraint,

$$\sum_{i \in \mathcal{N}} x_{i,h} \geq M \tag{4.26}$$

For each island h, one bus j is designated as a source node - (a) to act as a reference bus for state estimation, and (b) to ensure islands are connected. The source node is set as,

$$u_{j,h} = 1 \qquad\qquad j \in \mathcal{N}_s \tag{4.27}$$

where $\mathcal{N}_s$ is the set of all source nodes. The following constraint is added to ensure coherent generators are connected in each area,

$$x_{i,h} = 1, \quad i \in V_{gen}, V_{gen} \subset V, h \in K \tag{4.28}$$

To ensure islands are connected, an arbitrary network flow variable $f_{i,j,h} \in \mathbb{R}$ is defined as,

$$0 \leq f_{i,j,h} \leq n z_{i,j} \tag{4.29}$$

The source variable and the connectivity flow variable together ensure that the optimization problem yields connected islands by exploiting basic network flow concepts. If a unit flow $f_{i,j,h}$ is sent from $u_{j,h}$ to each node in area h and if each node consumes one unit flow (with $f_{i,j,h}$ and $f_{j,i,h}$ being the node inflow and outflow respectively), islands are connected when,

$$u_{j,h} \sum_{i \in \mathcal{N}} x_{i,h} - x_{j,h} + \sum_{\substack{i,j \in \mathcal{N}, \\ (i,j) \in \mathcal{Z}}} f_{i,j,h} = \sum_{\substack{i,j \in \mathcal{N}, \\ (j,i) \in \mathcal{Z}}} f_{j,i,h} \tag{4.30}$$

4.7 Multi-Objective Optimization

The two islanding strategies under cyber-attack uncertainties are formulated as multi-objective optimization problems, which find pertinent trade-offs between all the aforementioned objective functions. The multi-objective optimization problem for **Scenario 1** is written as,

$$\begin{aligned}
\textbf{minimize} \quad & F = [F_1, F_2, F_4, F_5] = \\
& [-\text{trace}(\boldsymbol{H}^{\boldsymbol{T}} \boldsymbol{Z} \boldsymbol{H}), \quad \sum_{(i,j) \in \mathcal{Z} \setminus S} \beta_i d_{i,j}, \\
& \sum_{h=1}^{k} S_h, \quad \sum_{(i,j) \in z} \frac{1}{2}(1 - z_{i,j}) P_{i,j}] \\
\textbf{subject to} \quad & \text{(4.3) - (4.5), (4.13), (4.19a) - (4.19b), (4.21) - (4.30)}
\end{aligned} \tag{4.31}$$

Table 4.1: Methods for multi-Objective Optimization

Solution	**Formulation**
Hierarchical	minimize $F_i \quad i = 1, ..., 4$ subject to $F_j \leq F_j^* + \eta_j, j = 1, .., i-1$
Weighted-sum	minimize $\sum_{i=1}^{4} \gamma_i F_i$
$\epsilon-$constraint	minimize $\sum_i \gamma_i F_i + \sum_j \rho_j F_j \quad i \neq j$ subject to $F_j \leq \epsilon_j \quad j = 1, .., i-1, i+1, ..4$
Weighted Chebyshev	minimize $b + \sum_{j=1}^{4} \rho_j F_j$ subject to $\gamma_i [F_i^* - F_i] \leq b, \quad i = 1, ..., 4$
Benson	minimize $\sum_{i=1}^{4} b_i$ subject to $F_i^0 - F_i = b_i, \quad i = 1, .., 4$

where $d_{i,j}, v_{i,j}, z_{i,j}, x_{i,h}, w_{i,j,h} \in \{0, 1\}$ and $S_h, f_{i,j,h} \in \mathbb{R}$ are the optimization variables. Similarly, the multi-objective optimization problem for **Scenario 2** is written as,

$$\begin{aligned} \textbf{minimize} \quad & F = [F_1, F_3, F_4, F_5] = \\ & [-\text{trace}(\boldsymbol{H^T Z H}), \quad \sum_i x_{i,h=1}, \\ & \sum_{h=1}^{k} S_h, \quad \sum_{(i,j)\in z} \frac{1}{2}(1 - z_{i,j}) P_{i,j}] \\ \textbf{subject to} \quad & \text{(4.19a) - (4.19b), (4.21) - (4.30)} \end{aligned} \tag{4.32}$$

where $z_{i,j}, x_{i,h}, w_{i,j,h} \in \{0, 1\}$ and $S_h, f_{i,j,h} \in \mathbb{R}$ are the optimization variables. Any vector solution of (4.31) and (4.32) is a Pareto optimal (non-dominated) solution. Due to the competing nature of the objectives, no ideal solution exists that simultaneously minimizes every objective [240, 241]. The choice of an acceptable solution largely depends on the preference of the reliability coordinator overseeing the islanding.

4.7.1 Solution Approaches

The multi-objective optimization problems are solved using the hierarchical optimization approach and the results are compared with four different scalarization techniques, (1) weighted sum, (2) ϵ-constraint, (3) weighted Chebyshev and (4) Benson's method. The different approaches are outlined in Table 4.1.

Hierarchical Optimization

The *hierarchical approach* allows the system operator to assign an objective priority and solve each individual objective in the multi-objective problem iteratively [242]. The optimal solution for the lower priority objective is obtained from among all solutions that degrade the higher priority objective by the system operator defined tolerance η. The objective function is defined as $F_i, \quad i = 1, ..., 4,$ with constraints iteratively added as.

$$F_j \leq F_j^* + \eta_j, \quad j = 1, .., i-1 \tag{4.33}$$

where F_j^* is obtained from the upper level optimization. Additionally, the tolerance η_j in the hierarchical approach allows system operators to define optimal solution degradation. For example, if the optimal solution for the minimum load-generation imbalance (priority = 1) is 20 MW and $\eta_1 = 5$ MW, the optimization will minimize the loss of rank (priority = 2) considering an imbalance of $20 + 5 = 25$ MW or better. In general, an optimal solution for a lower priority objective is selected from among all solutions that degrade the optimal solution of the higher priority objective by η. Note that solutions do not remain Pareto optimal when solution degradation tolerances are used for hierarchical approach.

Weighted-Sum Approach

This weighted-sum approach captures relative importance between objectives through weights γ_i. The objective function is defined as,

$$\sum_{i=1}^{4} \gamma_i F_i \tag{4.34}$$

For $\gamma_i > 0, \forall\gamma$, every solution of (4.34) is a supported, non-dominated solution [241].

$\epsilon-$Constraint Approach

The $\epsilon-$*constraint approach* transforms the less important objective into bounded constraints with operator-specified tolerances and optimizes the most important objective(s). The objective function is defined as,

$$\sum_{i} \gamma_i F_i + \sum_{j} \rho_j F_j \quad i \neq j \tag{4.35}$$

with the following constraint,

$$F_j \leq \epsilon_j \tag{4.36}$$

The optimal solution is obtained under the assumption that bounds ϵ_j do not result in an empty feasible space. The additional term $\sum_j \rho_j F_j$ with ρ being small positive scalar ensures that any optimal solution obtained using the $\epsilon-$constraint approach is strictly non-dominated solution, in addition to being efficient [241].

The implementation of the $\epsilon-$*constraint approach* is explained as follows. First, the objective function that minimizes the total load-generation imbalance in each island in (4.18) is converted into inequality constraints as $\sum_{h=1}^{k} S_h \leq \epsilon_{\text{load}}$. Here, ϵ_{load} depends on the available blackstart capacity in the islands. Similarly, the objective function in (4.15) is

converted to a constraint $\sum_{i=1}^{n} x_{i,h=1} \leq \epsilon_{\text{size}}$ to ensure that the maximum size of the island with vulnerable PMUs is constrained to a pre-determined fraction of the entire system. For example, when $\epsilon_{\text{size}} = 20$, vulnerable PMUs are isolated in a single small island that will not contain more than 20 nodes.

Weighted Chebyshev Approach

This approach minimizes the maximum weighted difference between the current solution and a reference point (often the ideal solution F^*) set by the system operator [241]. The objective function is defined as,

$$\max_{i=1,\ldots,4} \left\{ \gamma_i [F_i^* - F_i] \right\} + \sum_{j=1}^{4} \rho_j F_j, \tag{4.37}$$

The additional term $\sum_{j=1}^{4} \rho_j F_j(r)$ with small positive scalar values of ρ guarantees strict non-dominated solutions.

Benson's Approach

Similar to weighted Chebyshev, Benson's approach obtains efficient solutions by maximizing the sum of the non-negative distances between the current solution and a dominated feasible reference solution F_i^0. The objective function is defined as,

$$\sum_{i=1}^{n} v_i \tag{4.38}$$

with the following constraints,

$$\begin{aligned} & F_i^0 - F_i = v_i, \quad i = 1, .., 4 \\ & v \geq 0 \end{aligned} \tag{4.39}$$

4.7.2 Solution Trade-off

By varying (a) the scalarization parameters, (b) the objective priority, and (c) the objective degradation tolerances, the system operators may obtain a range of solutions for the islanding problem. The quality of the solutions is evaluated in terms of the trade-offs between multiple objectives. For a chosen optimal solution $\boldsymbol{r^*}$, the trade-off utility (TU) quantifies the maximum ratio of the worst deterioration to the best improvement among all other solutions $\boldsymbol{r_i}$ [243],

$$\text{Trade-off Utility}(\boldsymbol{r^*}) = \frac{\max_i[\boldsymbol{r^*} - \boldsymbol{r_i}]}{\max_i[\boldsymbol{r_i} - \boldsymbol{r^*}]} \tag{4.40}$$

Solutions with a smaller TU value are preferred as they reflect greater desirability among other alternatives.

4.7.3 Improving Computation Time

Controlled islanding is a general graph partition problem that is NP-hard, i.e., there exists no known algorithm to solve the problem in polynomial time [139]. To improve the computation time, three steps are taken.

First, for the $\epsilon-$constraint approach, the objective function to minimize the total load-generation imbalance in each island in (4.19) is converted into an inequality constraint as $\sum_{h=1}^{k} S_h \leq \epsilon_{\text{load}}$. Here, ϵ_{load} depends on the available black-start capacity in the islands.

Similarly, the objective function in (4.15) is converted to a constraint $\sum_{i=1}^{n} x_{i,h=1} \leq \epsilon_{\text{size}}$ to ensure that the maximum size of the island with vulnerable PMUs is limited to a predetermined fraction of the entire system in **Scenario 2**. For example, when $\epsilon_{\text{size}} = 20$, vulnerable PMUs are isolated in a single small island that will not contain more than 20 nodes.

Second, critical elements such as the slack bus and nodes in areas completely unaffected by false data, are pre-assigned as not vulnerable in **Scenario 2**. Pre-assignment of buses prior to islanding has been shown to drastically reduce the computation time [217].

Third, the integrality constraints on binary variables are relaxed, until binary solutions are obtained.

4.8 Case Studies

The developed controlled islanding strategies under complete and partial uncertainty are tested on the synthetic Illinois 200-bus, South Carolina 500-bus and Texas 2000-bus systems [142]. A branch-and-cut approach [244] is employed to solve the multi-objective mixed integer program in Gurobi, on an Intel(R) i5-4460, 3.20GHz with 16 GB RAM.

A combination of cutting planes and branch-and-bound method is used to solve the mixed integer optimization problem [244]. In the process, the integer variables are relaxed and valid inequalities are generated to constrain the feasible solution set such that the extreme points are binary. The feasible region is divided into subsets and the optimization problem is solved over each subset. The optimality gap is explicitly set to 0 to ensure the linear relaxations of the integer problem and the dual of the relaxation have feasible integral solutions. For more details on the time complexity of generating valid inequalities, the readers are referred to discussions in [245].

4.8.1 Test Case and Parameter Setup

The power system network is made observable through an optimal PMU placement scheme [133] where each node is observed at least by two PMUs. Any critical element (generator/line), that is not already observed, is made observable by additional PMUs. All PMUs observing critical elements in the network are assumed secure [232]. The detailed case

Table 4.2: Details of the Studied Test Cases

System	Load (MW)	Generation (MW)	# Secure PMUs	# Non-secure PMUs
200	1750	1765	25	130
500	7750	7832	63	394
2000	67109	68728	132	1247

descriptions including the total number of secure and non-secure PMUs are summarized in Table 4.2.

The trade-offs between the competing objectives, i.e., (1) maximizing the observability of islands with minimum additional nonsecure PMUs, (2) maintaining steady-state and transient stability, and (3) minimizing the size of the island with vulnerable PMUs, and their actual impacts on the studied power systems are explored through the multi-objective optimization approach.

For **Scenario 1** under complete uncertainty, the observability of the islands is maximized while utilizing a limited number of non-secure PMUs. With no prior information on false data, each non-critical PMU is assumed equally vulnerable, and the corresponding weights β_i are set to one.

For **Scenario 2** under partial knowledge of an attack, the vulnerable PMUs are isolated to only a small part of the system. If PMU i is regarded as vulnerable, a distance of $R = 3$ is set to label all neighboring PMUs as vulnerable. A total of $27, 13$, and 19 buses are initially designated as untrustworthy for the $200, 500$, and 2000-bus systems, respectively. The parameters β_i and R can be tuned by the operator when more information becomes available. For both scenarios, additional objectives described are incorporated to maintain island stability.

The scalarization parameters for the multi-objective optimization are given in Table 4.3 - Table 4.5. In the weighted-sum approach, every solution is a non-dominated solution when

Table 4.3: Scalarization Parameters

System	γ_1	γ_2	γ_3	γ_4	ϵ_{load}	ϵ_{size}
200	0.1	1	1	1	10	40
500	0.01	1	1	1	30	50
2000	0.01	0.1	1	1	50	350

Table 4.4: Reference Solutions for Chebyshev's Approach

System	**Rank**	**Size**($\mathcal{G}'$)*	**Imbalance(MW)**	**Flow Out(MW)**
200	412	29	0	28.03
500	1028	24	0	274.26
2000	4232	303	0	5373.29

Table 4.5: Reference Solutions for Benson's Approach

System	**Rank**	**Size**($\mathcal{G}'$)	**Imbalance(MW)**	**Flow Out(MW)**
200	400	50	20	50
500	1000	200	350	2000
2000	4000	400	20	7000

* Size($\mathcal{G}'$) refers to the size of partition with vulnerable PMUs

weights $\gamma_i > 0$. The weights γ_i associated with the four objectives are given in Table 4.3.

In the ϵ-constraint approach [241], the objectives pertaining to the load-generation imbalance and the size of the island with vulnerable PMUs are converted into inequalities to reduce the objectives of the optimization. The tolerances ϵ_{load} and ϵ_{size}, given in Table 4.3, reflect to what extend the system operators can relax the objectives without incurring major risks. Extremely tight tolerances may result in an empty feasible space.

Methods such as Chebyshev's approach and Benson's approach utilize ideal (reference) solutions supplied by the system operator. For Chebyshev's approach, the ideal solution is considered as the best solution each objective can individually achieve in the feasible region. Examples of the reference solutions are given in Table 4.4 . Chebyshev's approach aims to find the closest solution to the ideal solution [241].

For Benson's approach, the reference solution is set as any dominant solution, the examples of which are given in Table 4.5. Benson's approach generates a Pareto optimal solution that is as far away from the dominant reference solution as possible [246].

4.8.2 Performance of Controlled Islanding Under Uncertainty

For **Scenario 1**, the observability of islands is maximized using a minimum number of non-secure PMUs, while maintaining island stability. The hierarchical approach in Table 4.1 is used to solve the problem.

Fig. 4.6 demonstrates the performance of the developed islanding strategy for **Scenario 1** under complete uncertainty considering the two objectives of interest in this paper, i.e., the rank of the islands and the percent of non-secure PMUs retained. It is observed in Fig. 4.6 that the percent of the retained rank in the islands reduces at a much slower rate as the number of retained non-secure measurements is decreased. For example, retaining only 60% of the non-critical PMUs results in almost 90% observability in the islands for **Scenario 1**. Additionally, when maintaining load-generation balance has a higher priority, the islands have a total of 17.57 MW imbalance, and 437.61 MW line flow is disconnected. When maintaining transient-stability has a higher priority, the line flow disconnection reduces to 240.05 MW at the expense of 348.62 MW of load-generation imbalance. Similar results are noted for the 500-bus and 2000-bus systems in Fig. 4.6. This demonstrates that the optimization problem is successful in identifying a small number of nonsecure PMUs to maximize the island observability while maintaining island stability.

For **Scenario 2**, the size of the island with vulnerable PMUs is minimized while maximizing the island observability, steady-state and transient stability. A wide range of islanding solutions are obtained by varying the objective priority and the solution degradation tolerance in the hierarchical optimization approach described in Table I. The results are summarized in Table 4.6 - Table 4.8.

Table 4.6 illustrates the effect of optimal solution degradation. Consider rows 1 and 3 of Table 4.6. With objective degradation tolerance of 50 MW for flow disconnection and 10 MW for load-generation imbalance, the size of the uncertain island $\mathcal{G}'$ decreases from 42

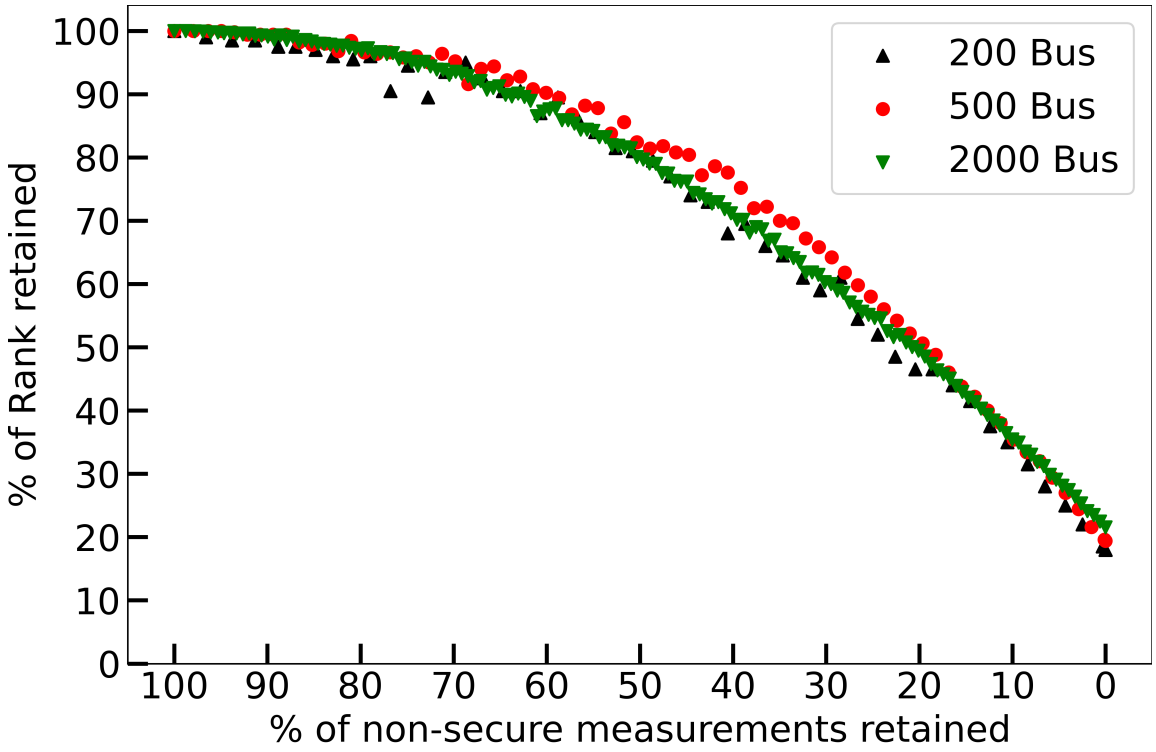

Figure 4.6: Scenario 1: Maximizing island observability with minimum number of non-secure measurements. For example, retaining 60% of the non-secure sensors help observe almost 90% of the grid. The percentage of the retained rank in the islands reduces at a much slower rate as the number of retained non-secure measurements is decreased.

Table 4.6: Scenario 2: Hierarchical optimization for 200-bus system

Optimal Solution [Priority, Degradation]				
Rank	**Size($\mathcal{G}'$)**	**Imbalance(MW)**	**Flow Out(MW)**	**Time(s)**
196 [3,0]	42 [2,0]	9.80 [4,0]	28.03 [1,0]	0.27
197 [3,0]	29 [2,0]	32.3 [4,0]	54.16 [1,50]	0.36
197 [3,0]	38 [2,0]	0.0 [4,10]	35.76 [1,50]	0.69

Table 4.7: Scenario 2: Hierarchical Optimization for 500-bus system

Optimal Solution [Priority, Degradation]				
Rank	**Size($\mathcal{G}'$)**	**Imbalance(MW)**	**Flow Out(MW)**	**Time(s)**
499 [3,0]	191 [2,0]	226.35 [4,0]	274.26 [1,0]	0.69
500 [4,0]	24 [1,0]	337.67 [2,0]	1955.3 [3,0]	0.55
500 [1,0]	62 [3,0]	1944.58 [2,0]	1664.5 [4,0]	1.44
499 [3,0]	191 [4,0]	226.35 [2,0]	1664.5 [1,0]	0.70

Table 4.8: Scenario 2: Hierarchical Optimization for 2000-bus system

Optimal Solution [Priority, Degradation]				
Rank	**Size($\mathcal{G}'$)**	**Imbalance(MW)**	**Flow Out(MW)**	**Time(s)**
1979 [4,0]	312 [1,0]	370.5 [2,0]	8519.1 [3,0]	511.5
1980 [4,0]	352 [1,40]	0.0 [2,0]	5650.4 [3,0]	131
1891 [4,0]	351 [1,40]	8.9 [2,10]	5526.9 [3,0]	3.4

to 38, the imbalance improves from 9.8 MW to 0 MW. The improvements, however, come at an expense of a 7.7 MW increase in flow outages. The system remains 98% observable in both cases.

In addition to the objective degradation, hierarchical optimization allows the system operators to assign individual importance to objectives during the islanding process. The impact of objective prioritization is explored in Table 4.7 for the 500-bus system. Consider row 1 in Table 4.7 - only 274 MW line powerflow is disconnected when the top priority is minimizing the total line flow disconnection. On the other hand, consider row 2 when isolating uncertain measurements is the top priority. The vulnerable PMUs are contained in an island of size 4.8% of the entire system. This example shows the flexibility of the optimization process in designing islands that cater to a particular operator's need.

The solutions obtained from the hierarchical optimization approach are compared to dif-

ferent scalarization methods. Here, **Scenario 2** is considered for comparison purposes. The results of the scalarization methods are summarized in Table 4.9 - Table 4.11. Consider the 200-bus system in Table IX. For all four scalarization methods, it is observed that flow disconnection of around 35 MW yields partitions with imbalances less than 3 MW and observability around 98%. Additionally, the size of the uncertain island is restricted to only 19% of the entire system. Fig. 4.7 illustrates the partitions for the 200-bus system corresponding to row 1 of Table 4.9. All solutions are Pareto optimal.

The trade-offs between the Pareto optimal solutions are more prominent for larger systems and hence investigated on the 500-bus and the 2000-bus systems. Consider the results for the 500-bus system summarized in Table 4.10. The weighted-sum approach yields 0.36 MW imbalance and 1529 MW of flow disconnection while restricting the size of the island with vulnerable PMUs to 16% of the size of the entire network. In comparison, the optimal solution obtained from the $\epsilon-$constraint approach reduces the size of the smaller island by 38.75% at the expense of 321 MW of additional line flow outage and 5.7 MW of additional imbalance. The Chebyshev method reduces the line MW flow outage by 541 MW compared to the $\epsilon-$constraint, while drastically increasing the load-generation imbalance to 517 MW, and expanding the size of the smaller island to 20% of the entire grid. The partitions may collapse if the islands lack substantial black-start capability. Similar observations are made for the 2000-bus system in Table 4.11. The results conducted on the test systems demonstrate that the proposed recovery scheme is effective in isolating attacks while creating balanced and observable islands. The optimal islanding decisions ultimately depend on how system operators choose to maintain a balance between multiple competing objectives.

The computation times for the hierarchical optimization are summarized in Tables 4.6 - 4.8 while those for the scalarization approaches are given in Table 4.12. The comparison demonstrates that hierarchical approaches often lead to a larger solution time. This is

Table 4.9: Scenario 2: Scalarization Results for the 200-Bus System

Scalarization	**Rank**	**Size($\mathcal{G}'$)**	**Imbalance(MW)**	**Flow Out(MW)**
Weighted-Sum	197	38	0.07	35.76
$\epsilon-$Constraint	196	39	2.93	34.98
Chebyshev	197	38	0.07	35.76
Benson	197	38	0.07	35.76

Table 4.10: Scenario 2: Scalarization Results for the 500-Bus System

Scalarization	**Rank**	**Size($\mathcal{G}'$)**	**Imbalance(MW)**	**Flow Out(MW)**
Weighted-Sum	499	80	0.36	1529.44
$\epsilon-$Constraint	499	49	6.08	1850.77
Chebyshev	498	101	517.53	1309.32
Benson	499	80	0.36	1529.44

Table 4.11: Scenario 2: Scalarization Results for the 2000-Bus System

Scalarization	**Rank**	**Size($\mathcal{G}'$)**	**Imbalance(MW)**	**Flow Out(MW)**
Weighted-Sum	1981	374	4.07	5468.49
$\epsilon-$Constraint	1981	350	12.83	5518.02
Chebyshev	1979	340	1.85	5743.29
Benson	1980	353	0.02	5501.86

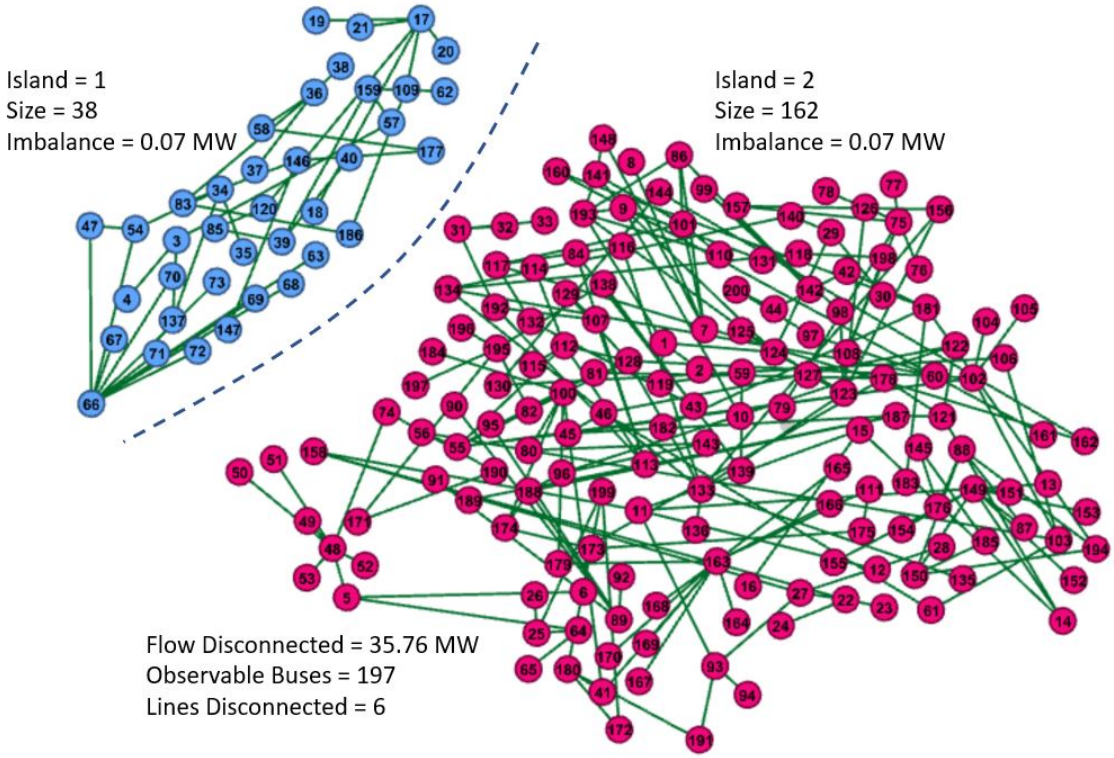

Figure 4.7: Details of the partitions for the 200 bus system corresponding to Scenario 2, as described in row 1 of Table 4.9

attributed to the fact that the hierarchical technique solves multiple single-objective problems in an iterative manner to obtain the final solution.

However, the provision for optimal solution degradation makes the hierarchical approach particularly attractive for larger power systems when prompt islanding decisions are needed at the expense of non-optimal but acceptable solutions. For example, as shown for the 2000-bus system in Table 4.8, the solution degradation reduces the computation time from 511s to 3.4s - a reduction of almost 99% at the expense of 4.45% decrease in observability and 8.9 MW increase in imbalance. Solution degradation in fact offers similar flexibility as the $\epsilon-$constraint approach. The hierarchical method is more intuitive, as preferences on objectives are assigned according to their importance.

In contrast, the correct choice of weights in scalarization methods may not be readily determined unless multiple instances of the optimization problem are solved. Furthermore, the reference solutions for Chebyshev and Benson's approach have to be pre-determined, which may not be feasible during the fast islanding decision-making process. A drawback of the hierarchical approach is that the number of additional constraints that are imposed in each iteration step increases as the number of objectives becomes large. This is of little concern here as the number of objectives is limited to four in this chapter. Overall, the hierarchical approach offers greater flexibility in designing islands in a very short period at the expense of non-optimal but acceptable solutions.

Admittedly, the multi-objective islanding problem remains NP-complete and is computationally challenging. To improve the solution time, the integrality constraints on some variables are relaxed and the impact on the optimal solution is investigated. For example, when variables $z_{i,j}$ and $w_{i,j}$ are relaxed in the 200-bus system, binary solutions are promptly obtained. Similar results are noted when the binary variable $z_{i,j}$ is relaxed for the 500 and the 2000-bus systems. The improvements in the computation time are illustrated in Table. 4.12.

Table 4.12: Simulation Time in (s) for Scalarization Methods

System	200 Bus		500 Bus		2000 Bus	
Relaxation	No	Yes	No	Yes	No	Yes
Weighted Sum	0.07	0.05	0.63	0.18	69.96	0.70
ϵ-Constraint	0.00	0.00	0.30	0.18	10.00	1.58
Chebyshev	0.15	0.00	1.52	0.33	148.82	2.85
Benson	0.15	0.033	0.80	0.25	14.64	6.72

4.8.3 Comparison of multiple solutions

The approach introduced in this chapter allows system operators to create islands considering a wide spectrum of choices, which in turn affect the operation of the islands. For example, a loss of substantial MW flow outage negatively impacts the transient stability of the system, thereby increasing the chances of further outages. On the other hand, low observability increases dependency on pseudo-measurements and yields poor state estimation results. Furthermore, a higher load-generation imbalance results in load loss, large frequency excursions, and increased reliance on black-start units.

The trade-off utility, TU, quantifies the preference of one optimal solution over the other competing solutions. Consider the results in Table 4.10 for an evaluation on the trade-offs. As the optimal solutions have different orders of magnitude, the total MW line flow disconnection is weighted by 0.1 to ensure uniformity during comparison. Let the preferred solution $\boldsymbol{r}^*$ corresponding to row 1 is $\boldsymbol{r}^* = [80, 499, 0.36\text{MW}, 152.9\text{MW}]$. The TU between $\boldsymbol{r}^*$ and all other solutions, as computed using equation (4.40) as,

$$\begin{aligned}\text{TU} &= \frac{\max[(80-49),(152-130.9)]}{\max[(101-80),(499-498),(517-0.36),(6-0.36),(185-152)]} \\ &\approx 0.06\end{aligned}$$

The TU for all points in Table 4.10 are similarly computed as $[0.06, 0.10, 24.2, 0.06]$. Solution $\boldsymbol{r}^*$ has the lowest TU and is preferred over all other solutions. Intuitively, $\boldsymbol{r}^*$ balances all four objectives of (a) restricting the size of the uncertain islands, (b) minimizing loss of

rank, (c) minimizing load-generation imbalance, and (d) minimizing the net flow outage, among all other solutions.

4.8.4 Discussions

This section discusses the limitations of the developed islanding strategies and introduces possible solutions. The first limitation arises when attacks are distributed and span multiple regions. In such scenarios, isolating vulnerable PMUs in one single island will not be desired. While such large-scale distributed attacks are rare due to the inherent safety measures of the electric grid, they are not impossible. The developed method can be extended to create multiple smaller islands to isolate attacks. This comes at the expense of an increase in the number of binary variables, longer computation times, and difficulties in the coordination of multiple smaller islands.

Second, the optimization problem of controlled islanding remains NP-hard. As future work, the authors plan to explore approximation algorithms [247, 248]. These approximation techniques can help find near-optimal solutions and accelerate computation times when a prompt and reliable islanding solution is desired.

Lastly, the set of candidate lines for controlled islanding is not fixed and changes with the real-time load, generation, and flow information. To ensure line open signal is sent to the correct set of circuit breakers during partitioning, additional studies leveraging topology signals at substations are underway.

4.9 Conclusion

The growing sector of organized cyber-crime seeks to jeopardize power system operations through increasing volume of sophisticated attacks. Carefully crafted threats can bypass the existing cyber-security defense mechanisms, remain undetected and are capable of

triggering widespread failures. This chapter presents controlled islanding methods that incorporate different degrees of PMU measurement uncertainties under false data injection attacks. Uncertainties are considered under the the lack of knowledge, or partial knowledge on PMU measurement trustworthiness. When attacks remain undetected, the impact of measurements in each island is minimized by creating islands that require a minimal number of PMU measurements for a state estimation solution. This allows system operators to allocate additional security to a minimum number of nodes in the network, thereby improving recovery plans. When partial information on bad data is available, the impact is minimized by isolating the vulnerable PMUs in a single island. This prevents malicious attacks from spreading to larger sections of the grid.

The findings demonstrate that system operators can successfully limit the impact of bad PMU data while creating islands that display maximal observability and sufficient steady-state and transient stability margins. The developed approach offers considerable flexibility to operators in designing islands that cater to a particular objective. The improvements to traditional islanding address post-incident analysis, enable quick recovery, and ensure continuity of grid operations. Such a consistent and collaborative approach will help contain threats and help power utilities minimize operational losses and financial threats in the face of contingencies.

Chapter 5

Summary and Future Research

Electric power systems serve as the backbone of modern society by generating and transmitting electrical power to geographically diverse customers. Often, these customers require power for critical loads such as hospitals, emergency response centers, and manufacturing process plants that are uninterruptible. It is therefore necessary for the power systems to be highly reliable. The reliability of the electricity service is improved by continuously monitoring the system state to detect and quickly mitigate any abnormal behavior. State estimation methods have been developed to estimate the state of the power network based on measurements obtained from PMU and SCADA meters strategically placed in the system. This has led to an increase in the dependency on the network communication infrastructure. Consequently, this has ushered a new era of sophisticated cyber attacks on the power state estimation. One such threat is false data injection attack that aims to change time-critical measurements flowing through the communication network. Such attack has been shown to cause incorrect generation dispatch, uneconomic operation, line overloads, voltage violations, increase in load shedding, and in the worst-case, widespread failure of the power grid. This thesis carried out an extensive analysis on the attack impacts, detection, and successful recovery methods from such growing cyber-threats. This chapter summarizes the main findings of our work and provides recommendations for future research directions.

5.1 Summary

For the impact analysis of false data injection attacks, the research was set up in the following way. On synthetic electric networks modeled after real systems, two different loading conditions, winter low and summer high, were considered. Extensive 1-D and 2-D transfer analysis were carried out to screen critical contingencies in the system. For each critical contingency, the corresponding RAS were identified. These realistic power system scenarios were utilized to estimate the risks associated with cyber intrusions, specifically attacks that combined physical line failures with measurement falsification. Additional attacks were modeled against RAS to block line disconnection trigger signals coming from auxiliary switch contacts of circuit breakers. To study the impact of line failures, a distributed slack-bus cascading failure algorithm was used to assess whether attacks actually led to widespread cascades. A new cyber-physical risk index was developed which combined the actual impact on the system in terms of load lost, along with the effort needed by the attacker to launch a successful coordinated false data attack. Additional indices were proposed to quantify the attack impacts considering cascading failures, and controlled islanding.

5.1.1 Key Findings 1

Investigations revealed the following key outcomes,

1. *In the studied power system test cases, it was observed that most coordinated false data injection attacks did not lead to large scale outages. This was mainly because attack neighborhoods are surrounded by load injection buses with no generators or transformers inside. When lines connected to these load clusters are lost, power is rerouted. When radial loads are lost, the power flow of lines serving the load decreases, thereby reducing the chances of a cascade.*

2. *Coordinated attacks resulted in subsequent line overloads and load shedding.*

3. *Widespread failures were mostly initiated when attacks were coordinated with loss of generators, transformers or heavily loaded lines in the vicinity of large generators.*

4. *Successful attacks often required multiple PDCs to be compromised across different utilities.*

5. *Feasible attack space largely depended on the distribution of zero injection buses in the network.*

Next, the historical PMU time series data was utilized to verify the correctness of PMU measurements. The developed data filter was designed to be independent of the existing state estimation bad data detector. First, multi-variate voltage, current and power flow measurement time series were collected from the phasor data concentrator data buffer prior to each cycle of state estimation. Then, a convolutional neural network-based data classifier was trained on the multi-variate time series data to detect various event signatures and identify false data attacks. The detection method was based on the pairwise correlation between PMU time-series data. The convolutional neural network model was then compared with other deep learning algorithms such as recurrent neural networks and long short term memory, and traditional classifiers such as bagged and boosted trees. To ensure that the proposed classifier is robust under different power system operating conditions, different scenarios were considered with varying load-generation patterns and network topologies. Additionally, the proposed false data attack detector was tested on various levels of measurement noises and missing measurements.

5.1.2 Key Findings 2

It was found that,

1. *The CNN-based filter was able to identify false data attacks at a higher accuracy rate compared to other deep learning and traditional classifiers such as RNN, LSTM, SVM, and Bag and Boosted Trees.*

2. *The CNN model was successfully able to identify false data injection attacks under a wide variety of power system load-generation and topology conditions. In addition, the developed filter was found to exhibit significantly high accuracies under instances of high signal-to-noise ratio in the PMU data, and cases of multiple missing/garbage data.*

3. *While the detection method is extremely fast, one of the major challenge is the training time. However, this is of little concern as the model can be trained periodically off-line at regional substations with limited data streams.*

Finally, this study considered the worst-case situations when successful cyber-attacks have already yielded severe consequences such as multiple line failures. Such worst case scenarios may arise due to a series of incorrect operator actions impacting critical lines and transformers, combined with other system conditions such as faults and maintenance. The mitigation strategy to limit the impact of coordinated false data attack was formulated as a controlled islanding problem under PMU measurement uncertainties. Two multi-objective islanding methods are developed that serve as an efficient post-attack mitigation strategy when wrong PMU measurements remain completely or partially undetected. While minimizing the attack impacts, the trade-offs between multiple objectives are quantified on the observability, the steady-state stability, the transient-state stability, and the size of newly formed islands. The multi-objective optimization was solved using hierarchical approaches and the optimal solutions were investigated by varying the objective priority, the relative weights, and the solution degradation tolerance. The hierarchical approach was then compared with various scalarization methods that transformed the multi-objective to a single-objective problem.

5.1.3 Key Findings 3

The results indicate the following key outcomes,

1. *The developed controlled islanding methods is able to minimize the impacts of false data attacks in each island, while creating islands that display maximal observability, large steady state and transient state stability.*

2. *When attacks remain undetected, the developed method resulted in islands that require a minimal number of PMU measurements for a SE solution. This enables operators to deploy security resources to a small subset of PMUs during the recovery process.*

3. *When partial information on an attack is available, our method successfully isolated vulnerable PMUs in a single island to enable quicker isolation of attacks.*

4. *It was further noted that the hierarchical approach of solving the multi-objective problem gave considerable flexibility to system operators compared to scalarization approaches in designing islands that cater to a particular objective*

5. *The modifications to traditional controlled islanding methods to incorporate attack uncertainties improve the post-incident analysis, and ensure prompt recovery and continuity of operations following a successful cyber attack.*

5.2 Future Research Directions

Cyber attacks are a direct consequence of the increased dependency of smart grid architecture on digital communication systems. This section highlights future research direction in areas of recovery from successful attacks. While developing recovery plans to mitigate the undesired attack consequences, it should be ensured that the recovery approach is resilient

in itself to prevent further failures. With this motivation, we aim to investigate different operational uncertainties as an effort to improve the resiliency of the newly formed islands.

The operational uncertainties will be investigated on (1) traditional islanding approach and (2) the islanding approach developed in Chapter 4 of this dissertation. Traditional controlled islanding approach disconnects pre-selected circuit breakers, and will be considered as a base case. Multi-objective controlled islanding schemes from Chapter 4 will be used to create islands that consider minimizing the total line MW and MVAR flow disconnection, maximizing the system observability, and minimizing the total load-generation imbalance in each island.

The resiliency of the islands will be investigated under various scenarios of uncertainty. Some of these include contingencies due to thermal violations or faults and reactive power violations due to voltage constraints inside the smaller island. Further, uncertainty due to failure and loss of renewable energy resources, variation in capacity production, and renewable prediction errors due to intermittency, will be incorporated in the study. To this end, a modified failure interaction model, based on [249] will be utilized to study the impact, and the method will further be verified using an AC-based cascading failure algorithm. The results of the analysis will be utilized to develop a resilience metric that assesses the stability of the newly formed islands under multiple operational uncertainties. The information from the developed resilience metric will enable system operators to improve the initial islanding procedures, and develop targeted corrective actions to prevent the smaller islands from collapsing. All simulations will be carried out under the synthetic Illinois 200-bus and the South Carolina 500-bus systems under different system load-generation conditions.

Glossary

AC Alternating Current.

ACE Area Control Error.

AGC Automatic Generation Control.

AMI Advanced Metering Infrastructure.

AVR Automatic Voltage Regulator.

CDF Cumulative Distribution Function.

CIP Critical Infrastructure Protection.

CNN Convolutional Neural Network.

DC Direct Current.

DFR Decreasing Failure Rate.

DLR Dynamic Line Rating.

DOE Department Of Energy.

DS Distributed Slack.

EENS Expected Energy Not Served.

EMS Energy Management System.

FACTS Flexible Ac Transmission System.

FDA/FDIA False Data Attack/False Data Injection Attack.

GOOSE Generic Object Oriented Substation Event.

GPS Global Positioning System.

IEC International Electrotechnical Commission.

IEEE Institute Of Electrical And Electronics Engineers.

IFR Increasing Failure Rate.

IP Internet Protocol.

KCL Kirchhoff's Current Law.

KKT Karush–Kuhn–Tucker Conditions.

KVL Kirchhoff's Voltage Law.

LAN Local Area Network.

LMP Locational Marginal Price.

LOCF Loss Of Observability After Cascading Failures.

LOCI Loss Of Observability After Controlled Islanding.

LR Load Redistribution.

LRCI Lines Recoverable After Controlled Islanding.

LSTM Long Short Term Memory.

MVA Mega Volt Ampere.

MW Mega Watt.

NERC North American Electric Reliability Corporation.

NISTIR National Institute Of Standards And Technology Interagency Internal Report.

NMRC Number Of PMUs Required To Compromise.

NP Non-Deterministic Polynomial-Time.

OPF Optimal Power Flow.

PCA Principal Component Analysis.

PDC Phasor Data Concentrator.

PMU Phasor Measurement Unit.

RAS Remedial Action Schemes.

RNN Recurrent Neural Network.

RTCA Real Time Contingency Analysis.

RTU Remote Terminal Unit.

SCADA Supervisory Control And Data Acquisition.

SCED Security Constraint Economic Dispatch.

SCOPF Security Constraint Optimal Power Flow.

SE State Estimation.

SMP Semi-Markov Process.

SNR Signal-To-Noise Ratio.

SOL System Operating Limits.

SQL Structured Query Language.

SVM Support Vector Machine.

TU Trade-Off Utility.

VAR Volt-Ampere Reactive.

WAN Wide Area Network.

References

[1] L. L. Lai, H. T. Zhang, C. S. Lai, F. Y. Xu, and S. Mishra, "Investigation on july 2012 indian blackout," in *2013 International Conference on Machine Learning and Cybernetics*, vol. 1. IEEE, 2013, pp. 92–97.

[2] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can Attackers With Limited Information Exploit Historical Data to Mount Successful False Data Injection Attacks on Power Systems?" *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4775–4786, 9 2018.

[3] Y. Liu, M. K. Reiter, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*, vol. 14, no. 1. New York, New York, USA: ACM Press, 5 2009, p. 21.

[4] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei 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, 3 2014.

[5] 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, 9 2012.

[6] X. Liu and Z. Li, "False Data Attacks Against AC State Estimation With Incomplete Network Information," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2239–2248, 9 2017.

[7] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 244–248.

[8] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Global Communications Conference (GLOBECOM), 2012 IEEE*. Citeseer, 2012, pp. 3153–3158.

[9] Z.-H. Yu and W.-L. Chin, "Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 5 2015.

[10] S. Basumallik, S. Eftekharnejad, N. Davis, and B. B. K. Johnson, "Impact of false data injection attacks on PMU-based state estimation." IEEE, 9 2017, pp. 1–6.

[11] R. Chen, D. Du, and M. Fei, "A Novel Data Injection Cyber-Attack Against Dynamic State Estimation in Smart Grid." Springer, Singapore, 2017, pp. 607–615.

[12] H. Karimipour and V. Dinavahi, "On false data injection attack against dynamic state estimation on smart power grids," in *2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, 8 2017, pp. 388–393.

[13] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power Systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 6 2011.

[14] K. Khanna, B. K. Panigrahi, and A. Joshi, "Bi-level modelling of false data injection attacks on security constrained optimal power flow," *IET Generation, Transmission & Distribution*, vol. 11, no. 14, pp. 3586–3593, 9 2017.

[15] D. Shelar, P. Sun, S. Amin, and S. Zonouz, "Compromising Security of Economic

Dispatch in Power System Operations," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 6 2017, pp. 531–542.

[16] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power Systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 6 2011.

[17] Yuan, Yanling, Li, Zuyi, and Ren, Kui, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[18] X. Liu and Z. Li, "Local Load Redistribution Attacks in Power Systems With Incomplete Network Information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 7 2014.

[19] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of Local False Data Injection Attacks With Reduced Network Information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 7 2015.

[20] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 35–47, 2018.

[21] Y. Xiang, Z. Ding, and L. Wang, "Power system adequacy assessment with load redistribution attacks," in *Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society*. IEEE, 2015, pp. 1–5.

[22] Y. Xiang and L. Wang, "A game-theoretic approach to optimal defense strategy against load redistribution attack," in *Power & Energy Society General Meeting, 2015 IEEE*. IEEE, 2015, pp. 1–5.

[23] Y. Xiang, L. Wang, and N. Liu, "A framework for modeling load redistribution attacks coordinating with switching attacks," in *Power & Energy Society General Meeting, 2017 IEEE*. IEEE, 2017, pp. 1–5.

[24] Y. Xiang, L. Wang, D. Yu, and N. Liu, "Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks," in *Power & Energy Society General Meeting, 2015 IEEE*. IEEE, 2015, pp. 1–5.

[25] A. Pinceti, L. Sankar, and O. Kosut, "Load redistribution attack detection using machine learning: A data-driven approach," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5.

[26] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking Transmission Line Outages via False Data Injection Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1592–1602, 7 2016.

[27] 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, 7 2013.

[28] J. Lin, W. Yu, D. Griffith, X. Yang, G. Xu, and C. Lu, "On distributed energy routing protocols in the smart grid," in *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*. Springer, 2013, pp. 143–159.

[29] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 9 2016.

[30] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 9 2017.

[31] A. Farraj, E. Hammad, and D. Kundur, "On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3322–3333, 12 2017.

[32] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 3 2014.

[33] A. Ashok, Pengyuan Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on Automatic Generation Control using a CPS Security Testbed," in *2015 IEEE Power & Energy Society General Meeting*. IEEE, 7 2015, pp. 1–5.

[34] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and Mitigating Impact of False Data Injection Attacks on Automatic Generation Control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, 7 2017.

[35] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of Reinforcement Learning Based False Data Injection Attack to Automatic Voltage Control," *IEEE Transactions on Smart Grid*, pp. 1–1, 2018.

[36] 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 *2014 American Control Conference*. IEEE, 6 2014, pp. 4372–4378.

[37] G. O. Rubio-Marroquin, C. R. Fuerte-Esquivel, and E. A. Zamora-Cardenas, "Impact of bad data injection attacks in the estimation of FACTS controllers parame-

ters," in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2 2018, pp. 1–5.

[38] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 3 2013.

[39] S. Pal, B. Sikdar, and J. Chow, "An Online Mechanism for Detection of Gray-Hole Attacks on PMU Data," *IEEE Transactions on Smart Grid*, pp. 1–1, 2018.

[40] H. Varmaziari and M. Dehghani, "Cyber-attack detection system of large-scale power systems using decentralized unknown input observer," in *2017 Iranian Conference on Electrical Engineering (ICEE)*. IEEE, 5 2017, pp. 621–626.

[41] L. Yuan, W. Xing, H. Chen, and B. Zang, "Security Breaches as PMU Deviation: Detecting and Identifying Security Attacks Using Performance Counters," in *ACM SIGOPS Asia-pacific Workshop on Systems*, 2011.

[42] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC61850 substation automation system network," in *Proceedings of the 6th International Conference on Information Technology and Multimedia*. IEEE, 11 2014, pp. 5–10.

[43] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, and E. Savary, "A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 9 2016, pp. 1–4.

[44] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1183–1195, 2014.

[45] B. Li, R. Lu, and G. Xiao, "HMM-Based Fast Detection of False Data Injections in Advanced Metering Infrastructure," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. IEEE, 12 2017, pp. 1–6.

[46] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 9 2015.

[47] K. Khanna, B. K. Panigrahi, and A. Joshi, "Data integrity attack in smart grid: optimised attack to gain momentary economic profit," *IET Generation, Transmission & Distribution*, vol. 10, no. 16, pp. 4032–4039, 12 2016.

[48] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 11 2012, pp. 395–400.

[49] S. Mishra, X. Li, A. Kuhnle, M. T. Thai, and J. Seo, "Rate alteration attacks in smart grid," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 4 2015, pp. 2353–2361.

[50] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On False Data Injection Attacks against Distributed Energy Routing in Smart Grid," in *2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE, 4 2012, pp. 183–192. [Online]. Available: http://ieeexplore.ieee.org/document/6197400/

[51] X. Zhang, X. Yang, J. Lin, and W. Yu, "On false data injection attacks against the dynamic microgrid partition in the smart grid," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 6 2015, pp. 7222–7227.

[52] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 7 2016, pp. 1–5.

[53] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback Control for Isochronous Energy Storage Systems in Autonomous Microgrids Under Denial-of-Service Cyber-Attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4702–4711, 9 2018.

[54] L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," in *2010 First IEEE International Conference on Smart Grid Communications*. IEEE, 10 2010, pp. 226–231.

[55] J. Lin, W. Yu, and X. Yang, "Towards Multistep Electricity Prices in Smart Grid Electricity Markets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 286–302, 1 2016.

[56] K. Chatterjee, V. Padmini, and S. A. Khaparde, "Review of cyber attacks on power system operations," in *2017 IEEE Region 10 Symposium (TENSYMP)*. IEEE, 7 2017, pp. 1–6.

[57] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 4 2017.

[58] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 7 2017.

[59] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1543–1551, 2 2019.

[60] Y. Wu, B. Chen, J. Weng, Z. Wei, X. Li, B. Qiu, and N. Liu, "False load attack to smart meters by synchronously switching power circuits," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2641–2649, 2018.

[61] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5161–5173, 2020.

[62] ——, "Detection of malicious command injection attacks on phase shifter control in power systems," *IEEE Transactions on Power Systems*, 2020.

[63] A. Phadke, "Synchronized phasor measurements in power systems," *IEEE Computer Applications in Power*, vol. 6, no. 2, pp. 10–15, 4 1993.

[64] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized Phasor Measurement Applications in Power Systems," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 20–27, 6 2010.

[65] A. Monticelli, *State estimation in electric power systems: a generalized approach*. Springer Science & Business Media, 2012.

[66] F. Schweppe and J. Wildes, "Power System Static-State Estimation, Part I: Exact Model," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, no. 1, pp. 120–125, 1 1970.

[67] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[68] G. N. Korres and N. M. Manousakis, "State estimation and bad data processing for systems including PMU and SCADA measurements," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1514–1524, 7 2011.

[69] V. Murugesan, Y. Chakhchoukh, V. Vittal, G. T. Heydt, N. Logic, and S. Sturgill, "PMU Data Buffering for Power System State Estimators," *IEEE Power and Energy Technology Systems Journal*, vol. 2, no. 3, pp. 94–102, 9 2015.

[70] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[71] P. S. Kundur, N. Balu, and M. Lauby, *Power System Stability and Control*, 1994.

[72] F. Capitanescu, M. Glavic, D. Ernst, and L. Wehenkel, "Contingency Filtering Techniques for Preventive Security-Constrained Optimal Power Flow," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1690–1697, 11 2007.

[73] R. S. Wibowo, T. P. Fathurrodli, O. Penangsang, and A. Soeprijanto, "Security constrained optimal power flow incorporating preventive and corrective control," in *2014 Electrical Power, Electronics, Communicatons, Control and Informatics Seminar (EECCIS)*. IEEE, 8 2014, pp. 29–34.

[74] Feng Dong, "Practical applications of Preventive Security Constrained Optimal Power Flow," in *2012 IEEE Power and Energy Society General Meeting*. IEEE, 7 2012, pp. 1–5.

[75] "NERC Reliability Concepts Ver.:l.0.2," Tech. Rep., 2007.

[76] Y. G. Rebours, D. S. Kirschen, M. Trotignon, and S. Rossignol, "A Survey of Frequency and Voltage Control Ancillary Services—Part I: Technical Features," *IEEE Transactions on Power Systems*, vol. 22, no. 1, pp. 350–357, 2 2007.

[77] H. Yoshida, K. Kawata, Y. Fukuyama, S. Takayama, and Y. Nakanishi, "A particle swarm optimization for reactive power and voltage control considering voltage security assessment," *IEEE Transactions on Power Systems*, vol. 15, no. 4, pp. 1232–1239, 2000.

[78] N. Jaleeli, L. VanSlyck, D. Ewart, L. Fink, and A. Hoffmann, "Understanding automatic generation control," *IEEE Transactions on Power Systems*, vol. 7, no. 3, pp. 1106–1122, 1992.

[79] D. Apostolopoulou, P. W. Sauer, and A. D. Dominguez-Garcia, "Automatic Generation Control and Its Implementation in Real Time," in *2014 47th Hawaii International Conference on System Sciences*. IEEE, 1 2014, pp. 2444–2452.

[80] "IEEE Standard Definitions of Terms for Automatic Generation Control on Electric Power Systems," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, no. 6, pp. 1356–1364, 7 1970.

[81] 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, 21 2013.

[82] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 7 2010.

[83] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 24 2012.

[84] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4,

pp. 981–997, 24 2012.

[85] P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," *Security and Communication Networks*, vol. 9, no. 3, pp. 262–273, 2 2016.

[86] T. B. Rasmussen, G. Yang, A. H. Nielsen, and Z. Dong, "A review of cyber-physical energy system security assessment," in *2017 IEEE Manchester PowerTech*. IEEE, 6 2017, pp. 1–6.

[87] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*. IEEE, 12 2011, pp. 1–8.

[88] L. Kotut and L. A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids," in *2016 Cybersecurity Symposium (CYBERSEC)*. IEEE, 4 2016, pp. 32–37.

[89] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 8 2012.

[90] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 1 2012.

[91] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun, and Y. Liu, "A survey on bad data injection attack in smart grid," in *2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. IEEE, 12 2013, pp. 1–6.

[92] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," in *SoutheastCon 2017*. IEEE, 3 2017,

pp. 1–4.

[93] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 7 2018.

[94] S. Basumallik, "A taxonomy of data attacks in power systems," *arXiv preprint arXiv:2002.11011*, 2020.

[95] L. Jia, R. J. Thomas, and L. Tong, "Impacts of Malicious Data on Real-Time Price of Electricity Market Operations," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 1 2012, pp. 1907–1914.

[96] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, 7 2010.

[97] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. B. Purry, "Towards modelling the impact of cyber attacks on a smart grid," *International Journal of Security and Networks*, vol. 6, no. 1, p. 2, 2011.

[98] A. Hahn and M. Govindarasu, "Cyber Attack Exposure Evaluation Framework for the Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, 12 2011.

[99] Y. Fan, J. Li, and D. Zhang, "A Method for Identifying Critical Elements of a Cyber-Physical System Under Data Attack," *IEEE Access*, vol. 6, pp. 16 972–16 984, 2018.

[100] W. Zhu and J. V. Milanovic, "Interdepedency modeling of cyber-physical systems using a weighted complex network approach," in *2017 IEEE Manchester PowerTech*, 2017.

[101] J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *International conference on computer safety, reliability, and security*. Springer, 2007, pp. 54–67.

[102] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, 12 2011.

[103] B. Falahati, Y. Fu, and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1515–1524, 9 2012.

[104] S. Mousavian, J. Valenzuela, and J. Wang, "A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 156–165, 1 2015.

[105] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, 2015.

[106] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, 9 2015.

[107] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3044–3056, 2018.

[108] I. Shames, F. Farokhi, and T. H. Summers, "Security analysis of cyber-physical systems using H2 norm," 2017. [Online]. Available: www.ietdl.org

[109] C. Moya and J. Wang, "Developing a Correlation Index to Identify Coordinated Cyber-Attacks to Power Grids," 2017.

[110] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems," *IEEE Transactions on Smart Grid*, 2017.

[111] N. Ferc, "Arizona-southern california outages on 8 september 2011: causes and recommendations," *FERC and NERC*, 2012.

[112] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[113] I. Dobson, S. Greene, R. Rajaraman, C. L. DeMarco, F. L. Alvarado, M. Glavic, J. Zhang, and R. Zimmerman, "Electric power transfer capability: concepts, applications, sensitivity and uncertainty," *PSERC Publication*, no. 01-34, 2001.

[114] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 7.

[115] W. R. W. Group, "Remedial action scheme design guide," 2017.

[116] Z. Yao, V. R. Vinnakota, Q. Zhu, C. Nichols, G. Dwernychuk, and T. Inga-Rojas, "Forewarned is forearmed: An automated system for remedial action schemes," *IEEE Power and Energy Magazine*, vol. 12, no. 3, pp. 77–86, 2014.

[117] D. L. Donaldson and D. M. Piper, "Advances in remedial action scheme modeling for power system analysis," in *2015 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. IEEE, 2015, pp. 1–5.

[118] J. McCalley, O. Oluwaseyi, V. Krishnan, R. Dai, C. Singh, and K. Jiang, "System protection schemes: limitations, risks, and management," *Final Report to the Power*

Systems Engineering Research Center (PSERC), 2010.

[119] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz, "Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 188–197, 2017.

[120] K. Khanna, B. K. Panigrahi, and A. Joshi, "Bi-level modelling of false data injection attacks on security constrained optimal power flow," *IET Generation, Transmission & Distribution*, vol. 11, no. 14, pp. 3586–3593, 2017.

[121] X. Li, P. Balasubramanian, M. Sahraei-Ardakani, M. Abdi-Khorsand, K. W. Hedman, and R. Podmore, "Real-time contingency analysis with corrective transmission switching," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 2604–2617, 2016.

[122] S. Wang and J. Baillieul, "Paradigm and paradox in topology control of power grids," in *2018 IEEE Conference on Decision and Control (CDC)*. IEEE, 2018, pp. 4863–4868.

[123] R. Kalluri, L. Mahendra, R. S. Kumar, and G. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power scada," in *2016 national power systems conference (NPSC)*. IEEE, 2016, pp. 1–5.

[124] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 4 2018.

[125] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of scada cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4379–4394, 2016.

[126] Y. Xiang, "Reliability evaluation and defense strategy development for cyber-physical power systems," 2017.

[127] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Performance Evaluation*, vol. 56, no. 1-4, pp. 167–186, 2004.

[128] V. S. Barbu and N. Limnios, *Semi-Markov chains and hidden semi-Markov models toward applications: their use in reliability and DNA analysis*. Springer Science & Business Media, 2009, vol. 191.

[129] S. Distefano and K. S. Trivedi, "Non-Markovian State-Space Models in Dependability Evaluation," *Quality and Reliability Engineering International*, vol. 29, no. 2, pp. 225–239, 3 2013.

[130] P. Rezaei, "Cascading failure risk estimation and mitigation in power systems," PhD dissertation, 2016.

[131] Shengwei Mei, Fei He, Xuemin Zhang, Shengyu Wu, and Gang Wang, "An Improved OPA Model and Blackout Risk Assessment," *IEEE Transactions on Power Systems*, vol. 24, no. 2, pp. 814–823, 5 2009.

[132] M. H. Gavgani and S. Eftekharnejad, "Critical component identification under load uncertainty for cascading failure analysis," in *2020 IEEE Texas Power and Energy Conference (TPEC)*. IEEE, 2020, pp. 1–6.

[133] B. Xu and A. Abur, "Optimal placement of phasor measurement units for state estimation, final project report," *Power Systems Engineering Research Center*, pp. 05–58, 2005.

[134] L. Huang, Y. Sun, J. Xu, W. Gao, J. Zhang, and Z. Wu, "Optimal pmu placement

considering controlled islanding of power system," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 742–755, 2013.

[135] "Stanford University: Notes on Strongly Connected Components," http://theory.stanford.edu/~tim/w11/l/scc.pdf, 2011, online; accessed 10th October, 2019.

[136] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in pmu-based state estimator using convolutional neural network," *International Journal of Electrical Power & Energy Systems*, vol. 107, pp. 690–702, 2019.

[137] R. Ma, S. B. Mallik, and S. Eftekharnejad, "A pmu-based multivariate model for classifying power system events," *IEEE Systems Journal*, 12 2018.

[138] C. González-Pérez and B. F. Wollenberg, "Analysis of massive measurement loss in large-scale power system state estimation," *IEEE Transactions on Power Systems*, vol. 16, no. 4, pp. 825–832, 2001.

[139] K. Sun, D.-Z. Zheng, and Q. Lu, "Splitting strategies for islanding operation of large-scale power systems using obdd-based methods," *IEEE transactions on Power Systems*, vol. 18, no. 2, pp. 912–923, 2003.

[140] D. Hazarika and A. Sinha, "Standing phase angle reduction for power system restoration," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 145, no. 1, pp. 82–88, 1998.

[141] P. Demetriou, M. Asprou, and E. Kyriakides, "A real-time controlled islanding and restoration scheme based on estimated states," *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 606–615, 2018.

[142] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid Structural Characteristics as Validation Criteria for Synthetic Networks," *IEEE Transac-*

tions on Power Systems, vol. 32, no. 4, pp. 3258–3265, 7 2017.

[143] "Interim report: Causes of the august 14th blackout in the united states and canada: U.s.-canada power system outage task force," 2003.

[144] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2016.

[145] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han, "Outlier Detection for Temporal Data: A Survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 1, 2014.

[146] R. J. Hyndman, E. Wang, and N. Laptev, "Large-Scale Unusual Time Series Detection."

[147] S. Ahmad and S. Purdy, "Real-Time Anomaly Detection for Streaming Analytics."

[148] S. Ben-David, J. Gehrke, and D. Kifer, "Detecting Change in Data Streams."

[149] L. Rettig, M. Khayati, P. Cudre-Mauroux, and M. Piorkowski, "Online anomaly detection over Big Data streams," in *2015 IEEE International Conference on Big Data (Big Data)*. IEEE, 10 2015, pp. 1113–1122.

[150] S. Papadimitriou, J. Sun, and C. Faloutsos, "Streaming Pattern Discovery in Multiple Time-Series."

[151] P. Chan and M. Mahoney, "Modeling Multiple Time Series for Anomaly Detection," in *Fifth IEEE International Conference on Data Mining (ICDM'05)*. IEEE, pp. 90–97. [Online]. Available: http://ieeexplore.ieee.org/document/1565666/

[152] J. Morais, Y. Pires, C. Cardoso, and A. Klautau, "An overview of data mining techniques applied to power systems," *intechopen.com*, 2009.

[153] M. Al Karim, M. Chenine, K. Zhu, L. Nordstrom, and L. Nordström, "Synchrophasor-based data mining for power system fault analysis," in *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*. IEEE, 10 2012, pp. 1–8.

[154] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 8 2014, pp. 1–8.

[155] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in *2014 North American Power Symposium (NAPS)*. IEEE, 9 2014, pp. 1–6.

[156] C. B. Vellaithurai, S. S. Biswas, R. Liu, and A. Srivastava, "Real Time Modeling and Simulation of Cyber-Power System." Springer, Berlin, Heidelberg, 2015, pp. 43–74.

[157] Y. Soupionis, S. Ntalampiras, and G. Giannopoulos, "Faults and Cyber Attacks Detection in Critical Infrastructures." Springer, Cham, 10 2016, pp. 283–289.

[158] U. Adhikari, T. H. Morris, N. Dahal, S. Pan, R. L. King, N. H. Younan, and V. Madani, "Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in RTDS," in *2012 IEEE Power and Energy Society General Meeting*. IEEE, 7 2012, pp. 1–7.

[159] 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, 11 2015.

[160] U. Adhikari, T. Morris, and S. Pan, "Applying Hoeffding Adaptive Trees for Real-Time Cyber-Power Event and Intrusion Classification," *IEEE Transactions on Smart Grid*, pp. 1–1, 2017.

[161] Y. He, G. J. Mendis, and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 9 2017.

[162] M. G. Kallitsis, G. Michailidis, and S. Tout, "Correlative monitoring for detection of false data injection attacks in smart grids," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 11 2015, pp. 386–391.

[163] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving Efficient Detection Against False Data Injection Attacks in Smart Grid," *IEEE Access*, vol. 5, pp. 13 787–13 798, 2017.

[164] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1052–1062, 5 2013.

[165] Z. Mao, T. Xu, and T. J. Overbye, "Real-time detection of malicious PMU data," in *2017 19th International Conference on Intelligent System Application to Power Systems (ISAP)*. IEEE, 9 2017, pp. 1–6.

[166] 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.

[167] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with

supervised learning," in *2016 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 7 2016, pp. 1395–1402.

[168] 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, 9 2017.

[169] J. J. Yu, Y. Hou, and V. O. Li, "Online False Data Injection Attack Detection with Wavelet Transform and Deep Neural Networks," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2018.

[170] A. Ayad, H. E. Z. 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, 2 2018, pp. 1–5.

[171] E. O. Schweitzer, D. Whitehead, A. Guzmán, Y. Gong, and M. Donolo, "Advanced Real-Time Synchrophasor Applications," *Journal of Reliable Power*, vol. 2, no. 2, 2010.

[172] P. H. Gadde, M. Biswal, S. Brahma, and H. Cao, "Efficient Compression of PMU Data in WAMS," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2406–2413, 9 2016.

[173] T. H. Morris, Shengyi Pan, and U. Adhikari, "Cyber security recommendations for wide area monitoring, protection, and control systems," in *2012 IEEE Power and Energy Society General Meeting*. IEEE, 7 2012, pp. 1–6.

[174] B. Sikdar and J. H. Chow, "Defending Synchrophasor Data Networks Against Traffic Analysis Attacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, 2011.

[175] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 9 2013.

[176] C. Alexander, M. Sadiku, and M. Sadiku, *Fundamentals of electric circuits*, 2009.

[177] M. Xia, T. Li, L. Xu, L. Liu, and C. W. de Silva, "Fault Diagnosis for Rotating Machinery Using Multiple Sensors and Convolutional Neural Networks," *IEEE/ASME Transactions on Mechatronics*, vol. 23, no. 1, pp. 101–110, 2 2018.

[178] C. C. J. Kuo, "Understanding Convolutional Neural Networks with A Mathematical Model," 9 2016. [Online]. Available: http://arxiv.org/abs/1609.04112

[179] B. Xu, N. Wang, T. Chen, and M. Li, "Empirical Evaluation of Rectified Activations in Convolutional Network," 5 2015. [Online]. Available: http://arxiv.org/abs/1505.00853

[180] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A Simple Way to Prevent Neural Networks from Overfitting," *Journal of Machine Learning Research*, vol. 15, pp. 1929–1958, 2014.

[181] R. J. Williams and D. Zipser, "A Learning Algorithm for Continually Running Fully Recurrent Neural Networks," *Neural Computation*, vol. 1, no. 2, pp. 270–280, 6 1989.

[182] M. Schuster and K. Paliwal, "Bidirectional recurrent neural networks," *IEEE Transactions on Signal Processing*, vol. 45, no. 11, pp. 2673–2681, 1997.

[183] I. Sutskever, "Training Recurrent Neural Networks," Ph.D. dissertation, 2013.

[184] Y. Bengio, P. Simard, and P. Frasconi, "Learning long-term dependencies with gradient descent is difficult," *IEEE Transactions on Neural Networks*, vol. 5, no. 2, pp.

157–166, 3 1994.

[185] S. Hochreiter, S. Hochreiter, Y. Bengio, P. Frasconi, and J. Schmidhuber, "Gradient Flow in Recurrent Nets: the Difficulty of Learning Long-Term Dependencies," 2001.

[186] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 11 1997.

[187] S. Ruder, "An overview of gradient descent optimization algorithms," 9 2016. [Online]. Available: http://arxiv.org/abs/1609.04747

[188] T. Dozat, "Incorporating Nesterov Momentum into Adam," 2016.

[189] S. Papadimitriou, J. Sun, and C. Faloutsos, "Streaming Pattern Discovery in Multiple Time-Series," *VLDB '05 Proceedings of the 31st international conference on Very large data bases*, 2005.

[190] S. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 7, pp. 674–693, 7 1989.

[191] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE transactions on pattern analysis and machine intelligence*, vol. 11, no. 7, pp. 674–693, 1989.

[192] M. Hearst, S. Dumais, E. Osuna, J. Platt, and B. Scholkopf, "Support vector machines," *IEEE Intelligent Systems and their Applications*, vol. 13, no. 4, pp. 18–28, 7 1998.

[193] L. Breiman, "Bagging Predictors," *Machine Learning*, vol. 24, no. 2, pp. 123–140, 1996.

[194] Y. Freund and R. E. Schapire, "A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting," *Journal of Computer and System Sciences*, vol. 55, no. 1, pp. 119–139, 8 1997.

[195] C. Seiffert, T. M. Khoshgoftaar, J. Van Hulse, and A. Napolitano, "RUSBoost: A Hybrid Approach to Alleviating Class Imbalance," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 1, pp. 185–197, 1 2010.

[196] M. Brown, M. Biswal, S. Brahma, S. J. Ranade, and H. Cao, "Characterizing and quantifying noise in PMU data," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 7 2016, pp. 1–5.

[197] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "False data injection attacks on phasor measurements that bypass low-rank decomposition," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2017, pp. 96–101.

[198] P. Gao, M. Wang, J. H. Chow, S. G. Ghiocel, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of successive "unobservable" cyber data attacks in power systems through matrix decomposition," *IEEE Trans. on Signal Processing*, vol. 64, no. 21, pp. 5557–5570, 2016.

[199] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. on Power Systems*, vol. 34, no. 2, pp. 1513–1523, 2018.

[200] NERC, "Standard cip-009-1 - cyber security – recovery plans for critical cyber assets." [Online]. Available: https://www.wecc.org/Reliability/CIP-009-1%20BC.pdf

[201] 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.

[202] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proceedings of the First ACM Workshop on Moving Target Defense*, 2014, pp. 59–68.

[203] K. Khanna, B. K. Panigrahi, and A. Joshi, "Feasibility and mitigation of false data injection attacks in smart grid," in *2016 IEEE 6th International Conference on Power Systems (ICPS)*. IEEE, 2016, pp. 1–6.

[204] R. Tan, H. H. Nguyen, E. Y. Foo, D. K. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, 2017.

[205] X. Lou, C. Tran, R. Tan, D. K. Y. Yau, and Z. T. Kalbarczyk, "Assessing and mitigating impact of time delay attack: A case study for power grid frequency control," in *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems*. New York, NY, USA: Association for Computing Machinery, 2019, p. 207–216.

[206] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for der cyberattacks," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 240–249, 2019.

[207] V. Krylov, K. Kravtsov, E. Sokolova, and D. Lyakhmanov, "Sdi defense against ddos attacks based on ip fast hopping method," in *2014 International Science and*

Technology Conference (Modern Networking Technologies)(MoNeTeC). IEEE, 2014, pp. 1–5.

[208] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 886–899, 2016.

[209] T. R. B. Kushal, K. Lai, and M. S. Illindala, "Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4741–4750, 2018.

[210] F. Wei, Z. Wan, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Trans. on Smart Grid*, 2019.

[211] M. Ashrafuzzaman, H. Jamil, Y. Chakhchoukh, and F. Sheldon, "A best-effort damage mitigation model for cyber-attacks on smart grids," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2. IEEE, 2018, pp. 510–515.

[212] P. Trodden, W. Bukhsh, A. Grothey, and K. McKinnon, "Milp formulation for controlled islanding of power networks," *International Journal of Electrical Power & Energy Systems*, vol. 45, pp. 501–508, 2013.

[213] J. H. Chow, *Power system coherency and model reduction*. Springer, 2013, vol. 84.

[214] H. You, V. Vittal, and X. Wang, "Slow coherency-based islanding," *IEEE Transactions on Power Systems*, vol. 19, no. 1, pp. 483–491, 2004.

[215] L. Ding, F. M. Gonzalez-Longatt, P. Wall, and V. Terzija, "Two-step spectral clustering controlled islanding algorithm," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 75–84, 2012.

[216] P. Trodden, W. Bukhsh, A. Grothey, and K. McKinnon, "Milp islanding of power networks by bus splitting," in *Power and Energy Society General Meeting, 2012 IEEE*. IEEE, 2012, pp. 1–8.

[217] A. Kyriacou, P. Demetriou, C. Panayiotou, and E. Kyriakides, "Controlled islanding solution for large-scale power systems," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 1591–1602, 2018.

[218] J. Li, C.-C. Liu, and K. P. Schneider, "Controlled partitioning of a power network considering real and reactive power balance," *IEEE Transactions on Smart grid*, vol. 1, no. 3, pp. 261–269, 2010.

[219] G. Xu and V. Vittal, "Slow coherency based cutset determination algorithm for large power systems," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 877–884, 2010.

[220] J. H. Chow, G. Peponides, P. Kokotovic, B. Avramovic, and J. Winkelman, *Time-scale modeling of dynamic networks with applications to power systems*. Springer, 1982, vol. 46.

[221] J. Stadler, H. Renner, and K. Köck, "An inter-area oscillation based approach for coherency identification in power systems," in *2014 Power Systems Computation Conference*. IEEE, 2014, pp. 1–6.

[222] H. You, V. Vittal, and Z. Yang, "Self-healing in power systems: an approach using islanding and rate of frequency decline-based load shedding," *IEEE Transactions on Power Systems*, vol. 18, no. 1, pp. 174–181, 2003.

[223] B. Yang, V. Vittal, G. T. Heydt, and A. Sen, "A novel slow coherency based graph theoretic islanding strategy," in *2007 IEEE Power Engineering Society General Meeting*. IEEE, 2007, pp. 1–7.

[224] M. Ali, B. A. Mork, L. J. Bohmann, and L. E. Brown, "Detection of coherent groups of generators and the need for system separation using synchrophasor data," in *2013 IEEE 7th International Power Engineering and Optimization Conference (PEOCO)*. IEEE, 2013, pp. 7–12.

[225] S. Basumallik and S. Eftekharnejad, "Dynamic islanding in power systems based on real-time operating conditions," in *2019 North American Power Symposium (NAPS)*. IEEE, 2019, pp. 1–6.

[226] X. Wang and V. Vittal, "System islanding using minimal cutsets with minimum net flow," in *IEEE PES Power Systems Conference and Exposition, 2004.* IEEE, 2004, pp. 379–384.

[227] J. Q. Tortós and V. Terzija, "Controlled islanding strategy considering power system restoration constraints," in *Power and Energy Society General Meeting, 2012 IEEE*. IEEE, 2012, pp. 1–8.

[228] T. Ding, K. Sun, C. Huang, Z. Bie, and F. Li, "Mixed-integer linear programming-based splitting strategies for power system islanding operation considering network connectivity," *IEEE Systems Journal*, vol. 12, no. 1, pp. 350–359, 2015.

[229] P. Demetriou, A. Kyriacou, E. Kyriakides, and C. Panayiotou, "Applying exact milp formulation for controlled islanding of power systems," in *Power Engineering Conference (UPEC), 2016 51st International Universities*. IEEE, 2016, pp. 1–6.

[230] P. A. Trodden, W. A. Bukhsh, A. Grothey, and K. I. McKinnon, "Optimization-based islanding of power networks using piecewise linear ac power flow," *IEEE Transactions on Power Systems*, vol. 29, no. 3, pp. 1212–1220, 2013.

[231] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, 2019.

[232] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. on Power Systems*, vol. 33, no. 5, pp. 4868–4877, 2018.

[233] S. Azizi, A. S. Dobakhshari, S. A. N. Sarmadi, and A. M. Ranjbar, "Optimal pmu placement by an equivalent linear formulation for exhaustive search," *IEEE Trans. on Smart Grid*, vol. 3, no. 1, pp. 174–182, 2012.

[234] A. Abur, A. Gomez Exposito, A. Gomez-Exposito, and A. Abur, *Power system state estimation: theory and implementation*. Marcel Dekker, 2004.

[235] S. M. Fazel, "Matrix rank minimization with applications." 2003.

[236] M. Fazel, H. Hindi, and S. P. Boyd, "A rank minimization heuristic with application to minimum order system approximation," in *Proceedings of the 2001 American Control Conference.(Cat. No. 01CH37148)*, vol. 6. IEEE, 2001, pp. 4734–4739.

[237] D. Gibert, C. Mateu, and J. Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," *Journal of Network and Computer Applications*, vol. 153, p. 102526, 2020.

[238] A. Bundy and L. Wallen, "Breadth-first search," in *Catalogue of artificial intelligence tools*. Springer, 1984, pp. 13–13.

[239] S. Basumallik and S. Eftekharnejad, "Dynamic islanding in power systems based on real-time operating conditions," in *2019 North American Power Symposium (NAPS)*. IEEE, 2019, pp. 1–6.

[240] A. A. Keller, *Multi-objective optimization in theory and practice i: classical methods*. Bentham Science Publishers, 2017.

[241] C. H. Antunes, M. J. Alves, and J. Clímaco, *Multiobjective linear and integer programming*. Springer, 2016.

[242] K.-W. Jee, D. L. McShan, and B. A. Fraass, "Lexicographic ordering: intuitive multicriteria optimization for imrt," *Physics in Medicine & Biology*, vol. 52, no. 7, p. 1845, 2007.

[243] M. S. M. A. Braun, "Scalarized preferences in multi-objective optimization," 2018.

[244] J. E. Mitchell, "Branch-and-cut algorithms for combinatorial optimization problems," *Handbook of applied optimization*, vol. 1, pp. 65–77, 2002.

[245] M. Grotschel, "Geometric algorithms and combinatorial optimization," 1988.

[246] R. Kasimbeyli, Z. K. Ozturk, N. Kasimbeyli, G. D. Yalcin, and B. I. Erdem, "Comparison of some scalarization methods in multiobjective optimization," *Bulletin of the Malaysian Mathematical Sciences Society*, vol. 42, no. 5, pp. 1875–1905, 2019.

[247] D. P. Williamson and D. B. Shmoys, *The design of approximation algorithms*. Cambridge university press, 2011.

[248] V. V. Vazirani, *Approximation algorithms*. Springer Science & Business Media, 2013.

[249] R. Ma, S. Jin, S. Eftekharnejad, R. Zafarani, and W. P. J. Philippe, "A probabilistic cascading failure model for dynamic operating conditions," *IEEE Access*, vol. 8, pp. 61 741–61 753, 2020.

Vita

Details

1. Name - Sagnik Basumallik
2. Place of Birth - Durgapur, India
3. Contact - sagnikbm2000@gmail.com

Education

1. Syracuse University, PhD, 2021
2. West Bengal University of Technology, B.Tech, 2014

Professional Experience

1. Independent System Operator, New England, 2020
2. Brookhaven National Lab, New York, 2019
3. TATA Consultancy Services, 2014 - 2015
4. Siemens, 2013
5. Indian Institute of Technology, Bombay, 2013
6. Durgapur Projects Limited, 2012

Teaching Assistant Experience

1. CIS 321 - Introduction to Probability and Statistics, 2018 - 2020
2. CIS 563 - Introduction to Data Science, 2018 - 2019
3. ELE 314 - Introduction to Power Engineering, 2018
4. ELE 232 - Electrical Engineering Fundamentals, 2017

Service to Department

1. Graduate Circle for Diversity and Inclusion, 2019
2. University Senator, 2018
3. Finance Committee, Graduate Student Organization, 2018 - 2019
4. Department Representative, 2017 - 2018
5. Department Representative, 2010 - 2014

Awards and Honors

1. Le-Page PhD Fellowship, 2015 - 2021
2. Winner - Graduate Student Research Competition, 2021
3. Outstanding Teaching Assistant Award, 2020
4. Certification in University Teaching, Future Professoriate Program, 2019