Cyber-Physical Security of Wide-Area Frequency-based Applications in Power Systems

by

Mohsen Badr Hasanien Khalaf

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

Waterloo, Ontario, Canada, 2020

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Khaled Kamel Professor, Colleague of Science, Engineering and Technology Texas Southern University
Supervisor(s):	Ehab El-Saadany Adjunct Professor, ECE Department, University of Waterloo Magdy Salama Professor, ECE Department, University of Waterloo
Internal Member:	Kankar Bhattacharya Professor, ECE Department, University of Waterloo Sheshakamal Jayaram Professor, ECE Department, University of Waterloo
Internal-External Member:	Kumaraswamy Ponnambalam Professor, Systems Design Engineering, University of Waterloo

Author's Declaration

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

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

Abstract

Modern power systems are continuously developing into large and interconnected ones. However, at the same time, restructuring within the power industry and reduced investment in transmission system expansions mean that power systems are operating closer and closer to their limits, leaving them more vulnerable to fault outages than before. The aspects of protection and control within power systems have thus become increasingly important as well as complicated. Concurrently, the continuous technological development in communication and measurement has accelerated the occurrence and application of Wide-Area Monitoring, Protection and Control (WAMPAC), a new kind of advanced scheme based on wide-area measurements. The blackouts happened in North America as well as in other countries over the past few years are also providing more incentives to scientists and engineers to study wide-area protection and control systems. Communication networks in smart grids bring increased connectivity at the cost of increased security vulnerabilities and challenges. A smart grid can be a prime target for cyber terrorism because of its critical nature. As a result, smart grid security has already attracted significant attention from governments, the energy industry, and consumers, leading to several important studies.

WAMPAC is the concept of using system-wide information via a centralized control center or Energy Management System (EMS) to monitor and control the whole system. Based on the situation and the required control action, the control center shares selected data with specific remote locations that are in need of the data. The utilization of system-wide information makes it easier to monitor the entire system and make better control and protection decisions by the EMS. Although the communication system is the backbone of these recent schemes, it makes them vulnerable to different types of cyber attacks. This thesis aims to investigate the problem of cyber security in frequency-related WAMPAC schemes. Two main schemes are considered as case studies: Automatic Generation Control (AGC) and Wide-Area Under-Frequency Load Shedding (WAUFLS) protection schemes. In addition, the cyber security of Power System State Estimation (PSSE), as a Wide-Area Monitoring (WAM) scheme, has been revisited. As WAMPAC schemes are so varied in their purpose and implementation, there is no general analysis to illustrate the potential

impact of a cyber attack on all such schemes. However, some general types of system responses are considered in this work.

First, with regard to AGC systems, a Kalman filter-based approach is proposed to detect False Data Injection (FDI) in AGC systems. Because detecting FDI and removing the compromised measurements are not enough in practical situations, the use of a simultaneous input and state estimation-based algorithm to detect and concurrently compensate for FDI attacks against the measurements of AGC systems is investigated. Throughout the use of this algorithm, the FDI attack signal is dealt with as an unknown input and its value is estimated accordingly. Then, the estimated value for the FDI is used to compensate for the effect of the attack so that the control center makes its decisions based on the corrected sensor signals, not the manipulated ones. Unlike other approaches, and as an extension to this work, the effect of AGC nonlinearities is studied during the attack time. Recurrent Neural Networks (RNN)-based approach is proposed to detect FDI during a time where any of the nonlinearities is affecting the system. The RNN-based approach is used to classify and identify the attacks according to their behavior.

Second, with regard to WAUFLS protection schemes, this thesis investigates the problem of cyber attacks on WAUFLS. This is followed by a detailed analysis showing that an adversary can launch an FDI attack against existing WAUFLS schemes in three different ways depending on they access level to system data, which may lead to equipment damage and/or system-wide blackout. To address this issue, a new mitigation scheme, that is robust against cyber attacks, is proposed to mitigate the effect of FDI attacks on WAUFLS. The proposed scheme depends on trusted system states to run power flow, so the power mismatch in the system is calculated. Finally, the calculated magnitude of disturbance is used to decide on the amount and locations of the load shedding.

All proposed detection and mitigation methods in the thesis are tested using simulations of benchmark and practical systems. In addition, sensitivity analysis is given after each method.

Acknowledgements

First, I praise and thank Allah Almighty for providing me with the ideas and patience necessary for the successful completion of this thesis.

Second, I would like to extend my genuine appreciation and gratitude to my supervisors; Prof. Ehab El-Saadany, who provided me with his continuous support throughout the last four years, and Prof. Magdy Salama, for all his guidance, patience, and advice during the last year. My heartiest appreciation goes to Dr. Amr Youssef, for offering me his valuable time and rich guidance. I am honored that this dissertation has been examined by Prof. Khaled Kamel, Prof. Kumaraswamy Ponnambalam, Prof. Sheshakamal Jayaram, and Prof. Kankar Bhattacharya. I owe respect and thanks to them for their time and insight.

I cannot describe my feelings toward my parents, my wife Sara, my brother Islam, my sisters Norhan and Omnia, my son Moaaz, and my daughter Zainah. Without their sacrifices, love, and affection, I would not have been able to accomplish this research abroad. They are my source of endless motivation, and they have never failed to pick me up in the most difficult moments. My parents' single mission has been keeping me and my siblings successful and happy. For that I will always be in debt to them.

I am truly fortunate that Abdelrahman Ayad accompanied me during my Ph.D. program. I will always be grateful for the endless memories, countless moments of laughter, and one true everlasting bond! I would also like to thank my companions on this journey, Aboelsood Zidan, Mohamed Abdelwahed, Haytham Abdelrahman, Hamouda Abo Maro, Ahmed Abdelrahman, Ahmed Mustafa, and all the friends I met in Waterloo. These friends made my stay in Canada feel more like home.

To my best friends, who always, encouraged and motivated me, I would like to express my gratefulness. Thank you Mohamed Elhussini, Mostafa Thabet, Mohamed Elbesealy, Ehab Aly, Mohamed Mahmoud, and Heikal. We are brothers for life, wherever we are.

I wish to extend special thanks to Fran Pappert-Shannon, Ghada Hamouda and Ahmad Okiel for always being my family in Canada.

Thank you all!

Dedication

This thesis is dedicated to my father, Badr, my mother Najah, my wife Sara, and to the soul of my grandfather, Hasanien.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACE Area Control Error. 17, 19, 20, 33, 34, 66, 90, 100

AGC Automatic Generation Control. iv, v, xii, 2, 4–6, 16–20, 23, 26, 28–31, 34, 35, 57, 61, 62, 66, 68, 70, 72, 74, 77, 89, 90, 97, 98, 100, 103, 125

AMI Advanced Metering Infrastructure. 8

APTs Advanced Persistent Threats. 3

BDD Bad Data Detection. 12, 16, 21, 38, 106

BPTT Back Propagation Through Time. 95, 96

CEDS Cyber security for Energy Delivery Systems. 3, 4

CI Critical Infrastructures. 2

CIP Critical Infrastructure Protection. 4

CUSUM CUmulative SUM. 64, 67, 125

DOE Department of Energy. 3, 4

DoS Denial of Service. 2, 11, 12, 14

DSE Distribution State Estimation. 25

EDS Energy Delivery Systems. 3

EMS Energy Management System. iv, 29

EWMA Exponential Weighted Moving Average. 63

FDI False Data Injection. v, ix, x, xii, 3, 5, 6, 11, 12, 14, 18–22, 26, 28, 30, 33, 34, 37, 42, 48, 49, 57, 61, 67–69, 71, 77, 89, 100, 104, 113, 115, 124–126

GDB Dead-band of Speed Governor. 89, 90

GPS Global Positioning System. 1, 15

GRC Generation Rate Constraints. 26, 90

ICCP Inter-utility Control Center Communication Protocol. 1

ICS Industrial Control Systems. 3

IEDs Intelligent Electronic Devices. 1

IT Information Technology. 3

LAN Local Area Network. 1

LFC Load Frequency Control. 20

MAC Media Access Control. 11

NERC North American Electric Reliability Corporation. 4

NIST National Institute for Standards and Technology. 4, 7

NISTIR NIST Interagency Report. 4

OE Office of Electricity Delivery and Energy Reliability. 3, 4

OOS Out-of-Step. 2, 126

OP Operating Point. 17

PDS Power Distribution Systems. 12

PMU Phasor Measurement Unit. 12, 16, 22, 26

PMUs Phasor Measurement Units. 1, 15, 16, 22, 25, 38, 105

PSSE Power System State Estimation. iv, 2, 5, 15, 16, 21, 23, 26, 28, 35, 105, 114, 125

PSSE-PF Power System State Estimation-Power Flow. 105, 111, 113, 114, 125

RAS Remedial Action Schemes. 2, 16, 126

RMP Risk Management Process. 4

RNN Recurrent Neural Networks. v, 6, 91, 94–100, 103, 125

ROCOF Rate of Change of Frequency. 24, 25, 38, 42, 51, 104, 113, 114

RTUs Remote Terminal Units. 1

SCADA Supervisory Control And Data Acquisition. 1–3, 16, 17

SE State Estimation. 12, 19, 20

UFLS Under-Frequency Load Shedding. 2, 23–25, 71, 73

UVLS Under-Voltage Load Shedding. 2, 126

WAM Wide-Area Monitoring. iv

WAMPAC Wide-Area Monitoring, Protection and Control. iv, viii, xii, 1, 2, 4, 5, 14–16, 28, 57, 124, 126

WAMS Wide-Area Monitoring Systems. 2, 15

WAN Wide Area Network. 1

WAP Wide-Area Protection. 23

WAUFLS Wide-Area Under-Frequency Load Shedding. iv, v, ix, x, xii, xiv, 4–6, 23, 24, 26, 28, 38, 39, 57, 104, 114, 116, 125

WLS Weight Least Squares. 15, 21, 36

Chapter 1

Introduction

The electric power grid is one of the most complex engineering machines ever built by humans. It is a highly interdependent cyber-physical system, where the dynamics of one system are tightly coupled to those of another. The latest smart grids contain a large number of interconnected areas, each of which has its own generators, loads and local Supervisory Control And Data Acquisition (SCADA) systems.

System data are collected from Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), integrated remote substations, and local SCADA systems under a framework of standard communication protocols such as IEC-60870 and IEC-61850. These data are exchanged over a Wide Area Network (WAN) via an Inter-utility Control Center Communication Protocol (ICCP). The SCADA/EMS efficiently uses IEDs for performing remote monitoring and control actions. The IEDs, as monitoring and control interfaces to the power system equipment, are installed in remote site/substation control centers and can be integrated using suitable communication networks. The IEDs and local communication can be locally accessed over a Local Area Network (LAN), while the remote site control center is connected to the SCADA/EMS and other engineering systems through the power system WAN [2].

WAMPAC utilizes system-wide information and sends selected data to specific remote locations. Phasor Measurement Units (PMUs), driven by the Global Positioning System

(GPS), provide real-time synchrophasor measurements for voltage and current phasors throughout the grid. These measurements offer real-time visibility to the dynamics of the power system that complement traditional SCADA measurements. Synchrophasor networks can give significant advantages by providing fast and precise measurements that can be reported at rates as high as 60 times per second [3]. This is mainly because SCADA measurements, in Wide-Area Monitoring Systems (WAMS), are unable to provide a timely assessment of the system due to low sampling rates as well as a lack of time synchronization [4].

Recently, and due to the availability of PMU measurements, WAMPAC is being used in different applications. These applications include PSSE, AGC, real-time contingency analysis, Remedial Action Schemes (RAS), security constrained optimal power flow, economic dispatch, unit commitment, phase angle monitoring, power oscillation monitoring, power damping monitoring, voltage stability monitoring, and dynamic line rating [5]. The common remedial actions against wide-area disturbances are generator rejection, load rejection, Under-Frequency Load Shedding (UFLS) schemes, Out-of-Step (OOS) relaying, Under-Voltage Load Shedding (UVLS) schemes, etc.

1.1 Motivation and Challenges

Traditionally, SCADA systems were not built with security as an important design criterion. The exposure of SCADA network infrastructure to cyber threats has thus increased enormously due to the enhanced interconnectivity of SCADA and public network infrastructures. Over the past decade, the power grid's SCADA and several other Critical Infrastructures (CI) such as banking, water distribution, oil and natural gas, smart grids, etc., are increasingly being targeted by advanced, sophisticated adversaries, as these infrastructures are critical to national security and societal well-being [6–8]. Therefore, the data being transmitted in the communication system represent an attractive target for attackers, increasing the vulnerability of these critical systems [9]. In smart grids, the common types of cyber attacks are smart grid Denial of Service (DoS) attacks, timing

de-synchronization attacks, malware attacks, and FDI and manipulation attacks [10, 11].

A recent example of malware that targets Industrial Control Systems (ICS) is Win32/ Industroyer, which is a sophisticated malware designed to disrupt the working processes of ICS used in electrical substations. Other examples include Stuxnet, which struck an Iranian nuclear facility in 2010 [12, 13], and the attack against Ukraine's power system in December 2015. In the latter incident, the attackers were able to install a malware called BlackEnergy on the control center computers of three energy distribution companies in Ukraine and temporarily disrupt the electricity supply to the end consumers, which resulted in thousands of homes and facilities suffering a power outage for several days [14]. This cyber attack showed the inadequacy of relying on just infrastructure- based traditional cyber security measures when dealing with a resourceful and sophisticated adversary. The adversary was able to steal valid credentials through social engineering to get into the control network and perform reconnaissance and planning for several months. These types of incidents, similar in nature to insider threats, highlight the need to go beyond a single layer of security in order to detect and quickly recover from a sophisticated cyber attack.

The need to develop intelligent countermeasures in multiple layers, to secure SCADA infrastructure elements and the fundamental applications they support, is being increasingly recognized. Several governmental reports have highlighted various weaknesses in cyber security for the electric sector that could result in major impacts due to emerging Advanced Persistent Threats (APTs) and also the urgent need to take measures to protect them [15]. The Department of Energy (DOE)'s Office of Electricity Delivery and Energy Reliability (OE) was set up for the main purpose of overseeing activities that enhance the reliability and resilience of the nation's energy infrastructure.

The Cyber security for Energy Delivery Systems (CEDS) program, created by the DOE OE, has adopted a strategic and hierarchical approach to funding several R&D projects that specially target multiple domains. Their aim is to develop novel solutions that go beyond traditional Information Technology (IT) infrastructure-based security to leverage the physical properties of the grid as part of application layer security [8]. Recognizing the importance of the cyber security of the Energy Delivery Systems (EDS), the DOE

OE released a road map in September 2011 to address the issues and concerns relevant to energy sector cyber security [16]. Also, the OE created the cyber security for the CEDS program to assist the energy sector asset owners (electric, oil, and gas) by developing cyber security solutions for energy delivery systems through integrated planning and a focused R&D effort [17].

The DOE, in coordination with the National Institute for Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC) developed a cyber security Risk Management Process (RMP) for the electric sector that will enable organizations to proactively manage cyber security risk [18]. Additionally, several efforts, like NERC Critical Infrastructure Protection (CIP) [19] and NIST Interagency Report (NISTIR) 7628 [20], are being made at the national level to ensure that the appropriate standards and safeguards are put in place to protect the electric power grid from potential cyber vulnerabilities and threats.

In addition to the above efforts, lots of research efforts are done to assess and address the problem of cyber attacks in power systems. However, the area of WAMPAC, in general, has been barely visited. The developers of the current WAMPAC schemes did not consider the problem of cyber attacks during the design stage, and still use the communication channels and communication standards that can be attacked. In addition, most of the approaches that have been proposed recently to tackle this problem are not real-time and are based on unpractical and/or simplified assumptions.

Among different WAMPAC applications, the cyber security of wide-area frequency-based schemes have not been given enough consideration in the literature claiming that power frequency is a global parameter and any attack to frequency measurements can be easily detected. However, this is not the case for the application that depend on the frequency variations between different areas in the same power system e.g., AGC and WAUFLS schemes. There is a lack of research in the area of mitigating cyber attacks on AGC systems. In addition, the current WAUFLS schemes still depend on traditional ways on evaluating system disturbance and performing load shedding. Therefore, there is a need for developing wide-area frequency-based applications that takes the problem of

cyber security into consideration during the design process of these schemes.

1.2 Objectives

The main objective of this thesis is to investigate the effect of cyber attacks on WAMPAC applications, including AGC, PSSE and WAUFLS, and go beyond traditional security solutions, i.e., to develop new real-time attack-detection and mitigation methods for critical wide-area frequency-related applications. These developed methods leverage both cyber and physical aspects of the grid. This is in addition to proposing new WAMPAC schemes that take cyber security issues into consideration.

1.3 Outline of the Thesis

Chapter 2 presents a thorough literature review of all considered topics in this research. It also includes a discussion and a list of gaps extracted from previous works.

Chapter 3 investigates in detail the problem of cyber attacks on frequency-related wide-area applications, including AGC and WAUFLS. In addition, a brief overview of FDI attacks on PSSE is provided to serve the content of the thesis. An attack model (i.e., attacker capabilities as well as possible damage to a power system) and a mathematical formulation of the problems are presented, and different simulation scenarios that show the problem are discussed.

Chapter 4 proposes a method using a Kalman filter to detect FDI attacks on AGC systems. In addition, a simultaneous input and state estimator is utilized to mitigate the effect of FDI attacks on AGC systems in real time. A linearized AGC model is used throughout this chapter. System stability after mitigation using the proposed approach is then studied. Different case studies are carried out to show the accuracy and efficiency of the proposed approach.

Chapter 5 proposes detection and mitigation schemes against FDI attacks on AGC systems considering system nonlinearities. RNN-based approache is proposed as a detection and identification mean. For mitigation, load forecast is used.

Chapter 6 presents a new WAUFLS protection scheme that is robust against cyber attacks. The proposed scheme is explained in detail. A practical system is used to test the scheme, and simulation results are given to show its accuracy, robustness against attacks, speed, and reliability.

Chapter 7 provides the conclusion of the thesis. It also articulates the platform for future research work.

Chapter 2

Background and Literature Review

2.1 Cyber-Physical Security of Smart Grids

"The grid" refers to the electric grid, which is a network of generation stations, transmission lines, substations, transformers and more that deliver electricity from the power plant to the end user. According to the NIST's conceptual model of a smart grid [21], what makes a grid "smart" is the digital technology that allows for two-way communication between the utility and its customers and the metering along the transmission lines. Markets, Service Provider, Operations, Bulk Generation, Transmission, Distribution and Customer are the seven logical domains of a smart grid. The first three deal with data collection and power management, while the last four deal with power and information flows in the smart grid. These domains are connected to each other through variety of communication links that are governed by various communication protocols.

In addition, smart grids have different components and assets, such as power generation, distribution, consumers, regional control centers, substations, field devices, communication and networking devices, phase-measuring units, protecting relays, intelligent electronic devices, remote terminal units, human machine interfaces, home appliances, circuit breakers, log servers, data concentrators, protocol gateways, tap changers, smart meters, etc. All of

these components are connected in a smart grid to operate, monitor, and control power flow and measurements.

However, the legacy cyber-security techniques are no longer sufficient to meet the cyber-security requirements of the smart grid and its assets. For instance, consumers are concerned about their privacy, as their lifestyle could be exposed to malicious users due to compromised data communication networks. Similarly, Advanced Metering Infrastructure (AMI), commonly known as smart meters, can be easily compromised; once they are, it is almost impossible to change their passwords (PINs), as these devices do not have their own keyboards to change passwords/PINs. Thus, a controller may be needed to deploy new passwords automatically once a smart meter is compromised. Thus, smart grid systems have unique features, goals, objectives and challenges when providing a reliable power supply and robust communications [9].

2.1.1 Security Requirements in Smart Grids

Smart grids present a variety of technical and regulatory challenges for security [22,23]. These challenges include: 1) the complexity and scale of future power systems; 2) traditional communication vulnerabilities; 3) new communication requirements; 4) trustworthiness among all participants (users, protocol, devices, etc.); 5) legacy devices; 6) heterogeneous technologies and protocols; 7) proprietary systems; and 8) users' privacy. To overcome these challenges, a broad range of security properties are required by the power systems, such as availability, confidentiality, integrity, authentication, authorization, freshness, efficiency, privacy, scalability, adaptability and evolvability, and authenticity [9, 10, 22, 24–33]. These requirements can be defined as follows:

Availability: Availability means that the data must be available to the authorized parties when there is a need for these data, without any security compromise [9, 10, 32, 33]. It ensures that all network resources (e.g., data, bandwidth, equipment, servers) are always available at all nodes for the authorized parties [24, 27, 29]. The importance of the availability of data stems from the fact that the cyber layer in power systems manages the

continuous power flow in the physical layer. Therefore, any data shortage may drive power system operators to make wrong decisions.

Confidentiality: Confidentiality means that data are disclosed only to authorized individuals or systems [9,10,27,29,32,33]. Critical data in power system (e.g., meter data) should be confidential. Meter data are critical because they provide information about the usage patterns for individual appliances, which can reveal personal activities through nonintrusive appliance monitoring. For this purpose, meter data should be protected such that only intended parties can access the information. Price information and control commands are not critical as long as they are public knowledge. [30].

Integrity: Integrity refers to the assurance that the accuracy and consistency of the data are maintained. No unauthorized modification, destruction or loss of data goes without being detected [9,10,24,27,29,32,33]. Integrity of price information, meter data, control commands, and software used in power system substations is critical. For instance, negative prices injected by an attacker can cause an electricity utilization spike, as numerous devices would simultaneously turn on to take advantage of the low price. The impact of attacking the integrity of meter data and control commands is mostly limited to revenue loss. However, the integrity of software is critical, since compromised software or malware can control any device and component in the power system [30].

Authorization: Authorization is also known as access control because it makes sure that the access rights of every entity in the substation are defined for the purposes of access control [27]. While distinguishing between valid and invalid users for all other security objectives, e.g., confidentiality, integrity, etc., authorization in relation to access control restricts the ability to issue commands to the plant control system. Violation of authorization may cause safety issues [28].

Authentication: Authentication simply refers to verifying the identity of a communication system practitioner and linking this identity to a system-internal principal (e.g., valid user account) by which this user is known to the system. In other words, authentication is validation that the communicating parties are who they claim to be, and that messages supposedly sent by these parties are indeed sent by them [27]. Other security ob-

jectives, most notably authorization, distinguish between legitimate and illegitimate users based on authentication [28]

Non-repudiation: Non-repudiation is one of the most important regulatory requirements. It means the assurance that irrefutable proof will exist to verify the truthfulness of any claim of an entity [27, 28] which is relevant to establish accountability and liability.

Privacy: Privacy issues have to be covered with the derived customer consumption data created in metering devices. Consumption data contains detailed information that can be used to gain insights on a customer's behavior [28].

Freshness: Freshness indicates that the data in the power system are fresh and not replayed by an attacker. There are two main quantities that should be included in any message: the data needed to be communicated, and the delay information. If the message has only the data without the delay information, it is referred to as having weak freshness. However, if the message also includes information that can be used to estimate the delay, it has strong freshness. Weak freshness is sufficient for applications where preventing a message replay attack is of main concern, but strong freshness is needed for applications such as time synchronization within networks [24].

Efficiency: Depending on where the solution will be employed, the grid has varying real-time requirements that make efficiency essential. Common use of constrained devices and networks add to this need [22].

Scalability: Due to the increasing scale of the power system, scale is important regarding the number of devices and the increasing number of interactions between grid entities [22]. Current smart grid implementations have a small number of devices, e.g., AMI. With more AMIs, the transmitted data volume will increase, together with the bandwidth usage. The physical tampering of smart meters needs to be addressed in wide AMI deployment [23].

Adaptability and Evolvability: Adaptability and evolvability refer to a device's design being able to allow for adaptation and evolution, as most devices last decades, with some even outlasting the lifetimes of cryptographic tools [22].

2.1.2 Classification of Threats

Many threats can affect the operation of smart grids at different stages and layers. These threats are classified in Table 2.1 according to the attack target [34, 35]. A more detailed explanation for each threat is given below the table.

Table 2.1: Classification of Cyber-Physical Attacks on Smart Grids

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

- **Man-in-the-middle attacks:** By gaining access to a communication channel, an adversary can alter metering devices and thus compromise the availability and integrity of power system data. Conditions and impacts of such attacks are presented in [36] and a data-framing attack is proposed in [37]. The replay attack is another form of man-in-the-middle attack that can incur catastrophic negative impacts [38].

- **DoS:** DoS attacks target the availability security objective by attempting to corrupt, delay or block critical communication links through flooding the communication with bogus traffic [39]. Different communication layers in the power systems are found to be susceptible to DoS attacks [29]: (i) Channel Jamming can occur on the physical layer, with effects ranging from delayed delivery of messages to complete denial of service [40]; (ii) in the Media Access Control (MAC) layer, attackers can modify MAC parameters and cause a spoofing attack. An intrusion-detection method is proposed

in [41] to detect threats on an IEC61850 automated substation; (iii) network and transport layer targeted attacks can severely affect the performance of end-to-end communication. For example, [42] investigated the vulnerability of real hardware and software to DoS.

- **Rogue Devices:** If an attacker gains physical access to field devices such as sensors or Phasor Measurement Units (PMUs), they can replace the device with a rogue that sends corrupted signals or falsely acknowledges the performance of a specific operation [35, 43].

- **False Data Injection (FDI):** FDI attacks result from injecting (corrupting) measurements data, with the goal of initiating wrong control actions. A well-known FDI model attacks areas that target the State Estimation (SE) process and bypasses the Bad Data Detection (BDD), as first introduced by Liu *et al.* [44]. Several assumptions, conditions and scenarios have been studied to launch successful attacks, such as the usage of AC power flow model [45], attacks on Power Distribution Systems (PDS) [46], attacks with incomplete information [47], and attacks targeting electricity markets [48]. Counter-measure techniques for attack detection and mitigation have been investigated in [49–51].

In the present work, we will elaborate more on FDI attacks, as these represent some of the most common types of cyber attacks on smart grids that target grid integrity. In these attacks, the adversary targets different signals on the communication system and injects false data, which then leads to wrong decisions. The result is often significant damage to power system components as well as power disruption to a large number of customers. The stages, range, and threats of FDI attacks against critical information infrastructures are investigated in [52]. Different templates for FDI attacks that are used mainly to test false data detection approaches are mentioned in the literature [53]. A general expression of these attacks can be written as:

$$x_a = a_1(t)x + a_2(t) \tag{2.1}$$

where x_a is the attacked signal that the control center operator sees, x is the original signal that the attacker needs to manipulate, $a_1(t)$ is the scaling attack value, and $a_2(t)$ is the additive attack value. Let's assume that an attack starts at time t_1 and ends at t_2, the attack value varies based on the used template as follows.

1. ***Scaling Attack***: This type of attack modifies the communication signal so that the new value becomes higher or lower, depending on the scaling attack parameter. Mathematically, it is a multiplication process of the true signal by the scaling attack parameter.

$$a_1(t) = \begin{cases} c & t_1 < t < t_2 \\ 0 & otherwise \end{cases} \tag{2.2}$$

$$a_2(t) = 0 \tag{2.3}$$

2. ***Ramp Attack***: This type of attack can be applied by gradually modifying the true signal through the addition of an increasing or decreasing attack signal.

$$a_1(t) = 0 \tag{2.4}$$

$$a_2(t) = \begin{cases} c.(t - t_1) & t_1 < t < t_2 \\ 0 & otherwise \end{cases} \tag{2.5}$$

3. ***Step Attack***: This attack technique involves adding a positive or negative value to the signal at the moment of disturbance, prompting a transition from zero to the step magnitude (rising or falling edges).

$$a_1(t) = 0 \tag{2.6}$$

$$a_2(t) = \begin{cases} c & t_1 < t < \infty \\ 0 & otherwise \end{cases} \tag{2.7}$$

4. ***Pulse Attack***: This attack form represents a special case of the step attack, where the attacker implements the attack over a specified time.

$$a_1(t) = 0 \tag{2.8}$$

$$a_2(t) = \begin{cases} c & t_1 < t < t_2 \\ 0 & otherwise \end{cases} \tag{2.9}$$

5. ***Random Attack***: This attack mode takes place by the addition of a random value to the true signal.

$$a_1(t) = 0 \tag{2.10}$$

$$a_2(t) = \begin{cases} random & t_1 < t < t_2 \\ 0 & otherwise \end{cases} \tag{2.11}$$

where c is constant and t represents the time.

In [54], the authors studied the performance of a Kalman filter under false data injection attacks and proved a necessary and sufficient condition under which the attacker could make the estimation error unbounded without being detected. The authors in [55–57] also used a Kalman filter, this time to detect false data injection and DoS attacks. They fed both the Kalman filter estimates and system measurements into an χ^2-detector to detect faults and cyber attacks. However, the detection technique using an χ^2-detector was unable to detect statistically derived FDI attacks. Therefore, the authors in [55, 56] employed Euclidean distance metrics, which are able to identify such sophisticated injection attacks. The authors in [57] used the cosine similarity approach instead.

A sequential detector based on a likelihood ratio to detect malicious data and FDI against state estimation was proposed in [58]. Another real-time detector which detects FDI on the smart grid through state estimation was presented in [59], where the detector aimed at detecting the FDI as quickly as possible. The authors analyzed their proposed scheme using a constructed Markov chain-based model that allowed them to configure the system parameters for guaranteed performance in terms of some predefined metrics.

2.2 Wide-Area Monitoring, Protection and Control

WAMPAC is the concept of using system-wide information and sending selected data to specific remote locations that are in need of the data. The utilization of system-wide information makes it easier to monitor the entire system and make better control and

protection decisions by the energy management system (control center). Figure 2.1 shows a high-level schematic of the WAMPAC.

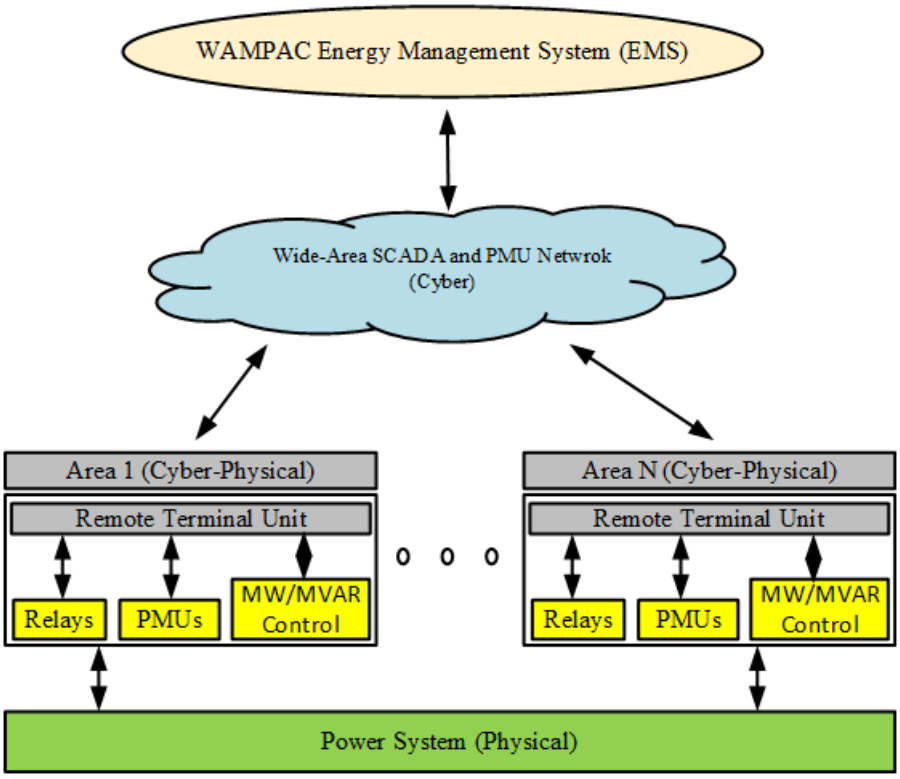


Figure 2.1: High-level schematic of WAMPAC

One of the WAMS is PSSE, which is utilized as a well-established mechanism for monitoring the variables of a system's state. By relying on power measurements as inputs to the PSSE process, system operators are able to estimate the states and achieve system observability. As measurements are not free of error or noise, a major component of the PSSE algorithm is error minimization between the estimated and actual states, such as the Weight Least Squares (WLS) algorithm [60].

Recently, the integration of PMUs has facilitated obtaining more accurate measurements at a higher resolution, managed by the GPS. As a consequence, instantaneous system monitoring has become easier and more frequent. PMUs enable real-time synchrophasor

measurements for voltage and current phasors over the grid. They can also be used to measure frequency in the power grid.

In addition, phasor measurements provide visibility to the dynamics of the power system in real time, complementing traditional SCADA measurements that generate one measurement every 2 to 4 seconds. This is mainly because of the low sampling rates and the lack of time synchronization in SCADA measurements. Therefore, standalone SCADA systems are unable to provide real-time assessment of the power system. [4].

On the other hand, significant advantages can be obtained from synchrophasor networks, as they provide accurate measurements that are deliverable at high rates of up to 60 times per second [3]. Even with the great advantages offered by PMUs, economic constraints are still limiting the wide-spread use of PMUs in practice [61]. Several approaches have been proposed on how to improve monitoring by optimally augmenting SCADA measurements with the more reliable PMU phasor measurements in the PSSE process [62, 63]. To protect against possible errors or cyber attacks during the PSSE process, defense mechanisms, such as BDD, have been implemented to detect measurements with high error levels [64].

2.3 Cyber Security of WAMPAC

Generally speaking, an attacker can access WAMPAC schemes through the communication system, as shown in Fig. 2.2. The problem of cyber attacks is general in all WAMPAC schemes. However, as mentioned previously, these schemes are so varied in their purpose and implementation, there is probably no general analysis to illustrate the potential impact of a cyber attack on all such schemes. Nevertheless, we can generalize some types of system responses. In the following subsections, a review of each type of these schemes is given. It is important to mention here that many publications have studied the effect of cyber attacks on AGC systems. However, the effect of cyber attacks on RAS schemes has not yet been investigated, except for some publications that propose general architecture for cyber security in smart grids.

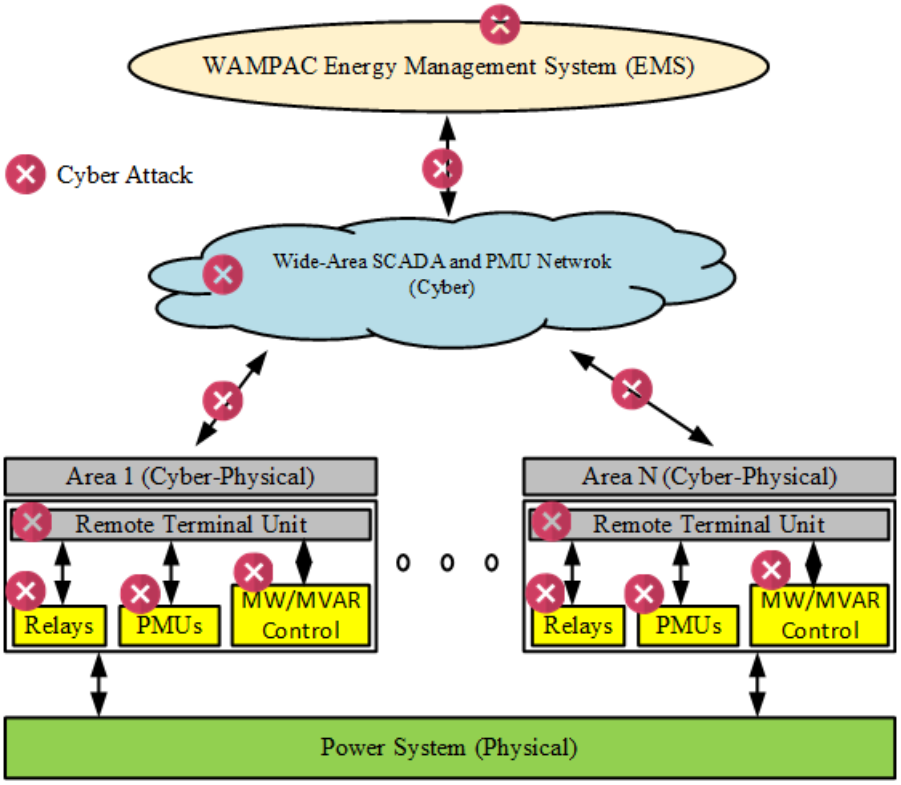


Figure 2.2: Cyber attacks on WAMPAC systems

2.3.1 Automatic Generation Control

Automatic Generation Control is a control scheme which maintains grid frequency and minimizes tie-line power deviations by adjusting the output power of generators according to the measurements collected from the distributed sensors in the grid [53, 65, 66]. The AGC algorithm uses frequency deviation as well as tie-line power flow provided by the SCADA telemetry system to determine the Area Control Error (ACE), which is the needed correction that is used to calculate the new Operating Point (OP). The new OP is then sent to each area. In a system with n areas, the area control error of Area i is

$$ACE_i = \sum_{j=1}^{n} a_{ij} \Delta P_{tie,ij} + \beta_i \Delta f_i \tag{2.12}$$

where Δf_i is the frequency deviation of Area i and $\Delta P_{tie,ij}$ is the tie-line power between areas i and j.

A cyber attack on AGC systems not only has a direct effect on the system frequency but can also impact the stability and economical operation of the power grid [11]. This is because frequency changes can trigger some protection actions that may lead to equipment damage and blackouts [53]. Figure 2.3 shows the data communication links in a two-area AGC system.

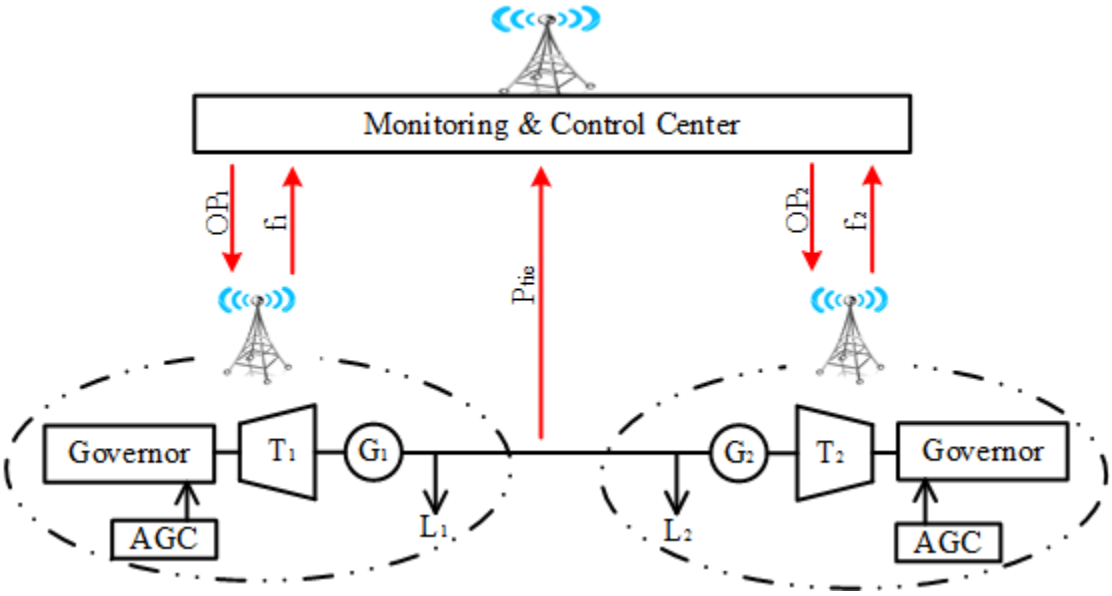


Figure 2.3: Data communication in a simple two-area AGC system

The impact of cyber attacks, including FDI attacks, on AGC systems has been investigated [66–74]. As well, several approaches have been proposed in the literature to detect FDI in AGC systems [68, 75–82]. However, approaches to mitigating cyber attacks on AGC systems are discussed in only a few publications [53, 80–82].

Using reachability analysis, the authors in [69] showed that the attacker can craft a controlled attack against a two-area AGC system to drive the system frequency away from its allowable range. They also showed a case of violating the power exchange constraint between the two areas that might directly or indirectly lead to a swing in the exchange power. In [70], the authors added more constraints by assuming that the attacker has limited access to system parameters. They proposed two methods using Markov Chain Monte Carlo (MCMC) optimization and a linearized AGC model to show the impact of cyber attacks on AGC.

In [66, 71], the impact of time-delay attacks on the operation of the AGC systems was investigated. The impact of FDI attacks on AGC systems were also examined in [67] through feasibility analysis. Additionally, [72] investigated AGC system vulnerability to FDI attacks experimentally through testing a system in Iowa, USA, showing FDI attacks to be potential sources of under-frequency conditions that could result in unnecessary load shedding.

Different attack scenarios and a detection strategy were proposed in [75]. The detection scheme is based on a Multi-Layer Perception (MLP) classifier that is used to extract the differences of ACE under attack and in normal situations, thus distinguishing compromised signals from normal ones. A universal unknown input and state estimator [79] was proposed to estimate the values of system states. The obtained system states are then used to calculate different measurements and compare them with received ones. The obtained error is used to detect the FDI on AGC systems, if it exceeds a pre-defined threshold.

In [53, 68], the authors used the DC State Estimation (SE) to calculate the values of the tie-line powers, which they employed to calculate the ACE. A model was developed for an optimal FDI attack, assuming the attackers' knowledge of the flow measurements that are fed to the SE algorithm. They then proposed a method to detect and mitigate the attacks where the compromised sensors are isolated and only the healthy measurements are fed to the SE algorithm to calculate the ACE. This was based on the fact that the SE is an over-determined problem, and therefore removing several compromised elements in the measurement vector may not affect the estimation much. The authors evaluated the

impact of a number of compromised sensors on the accuracy of attack-mitigating SE and concluded that if the number of compromised signals is larger than a specific threshold, the attack-mitigating SE becomes under-determined and the approach fails to mitigate against the FDI.

In [80], different attack templates on AGC systems were developed. These attacks modified the frequency and tie-line power flow measurements to drive the frequency out of the allowable range. Real-time load forecasts were calculated, after which the anomaly detection algorithm used this real-time load forecast to predict AGC operations over a given time period. During operations, the performance of the AGC is compared to this prediction to identify anomalies. If an attack is detected, the mitigation strategy utilizes the forecast load to calculate and forecast the ACE instead of using the received data to calculate it. The effect of the noise was only considered in the ACE forecasting, but the process and measurement noise were not explicitly modeled.

Law et al. [81] presented security games for risk minimization in AGC. In particular, the authors provided a model for the attacker-defender interactions using stochastic (Markov) security games to analyze the best defensive actions under resource constraints. Nevertheless, the paper did not focus on the design of attacks, defenses or the controller, but on the game-theoretic modeling of system risk dynamics under the actions of the attacker and defender for any given system.

More recently, in [82], the authors proposed a mitigation scheme for FDI attacks against Load Frequency Control (LFC) systems. The technique described in this reference is not very practical, since the authors assumed the existence of a number of redundant communication channels that cannot be simultaneously controlled by the attacker. The FDI attack detection is performed using a neural network algorithm. When an attack is detected against the active communication channel, a command is issued to the transmitter to request a new channel.

2.3.2 Power System State Estimation

Power System State Estimation (PSSE) is employed as a well-established mechanism for monitoring the variables of system states. Relying on power measurements as inputs to the SE process, system operators are able to estimate the states and achieve system observability. As measurements are not free of error or noise, and the number of measurements is more than the unknown states, a major component of the SE algorithm is error minimization between the estimated and actual states, such as the WLS algorithm [60].

The most serious type of cyber attack against PSSE is an FDI attack, as it is able to bypass the BDD to corrupt measurements. There has been a massive research effort to formulate detection and mitigation techniques against these types of attacks, with [83] surveying recent work in this area.

In [84, 85], the authors proposed online deep learning techniques to detect attacks based on temporal and spatial measurement variations caused by the attacks. A nonlinear interval observer is proposed in [86] for attack detection and isolation of targeted sensors. The technique is based on estimating the interval state of the internal physical system and is used both as a reference and to raise an alarm when the interval residual does not include the zero value. The authors in [87] compare four algorithms based on a matrix separation technique to detect FDI attacks with higher efficiency and faster computation performance in large-scale systems.

Bobba et al. [88] explored how to detect FDI attacks: One way is to secure basic measurements which are selected strategically, while another way is to verify state variables independently, after selecting them strategically. Specifically, the authors showed that protecting basic measurements is sufficient and necessary for the detection of FDI attacks. The protection of meter measurements includes both physical and software methods, such as guard patrolling, video monitoring, tamper-proof communication systems, sophisticated authentication protocols, asymmetric encryption mechanisms, etc.

In their work, Dan and Sandberg [89] proposed greedy algorithms for perfect and partial countermeasures against FDI attacks. Perfect defense means that no FDI attacks can occur.

Due to so many meters in power systems, to make all devices encrypted overnight is not possible. Since the defense budget might not be sufficient for perfect countermeasures, the control center would consider protecting a subset of meters to maximize the increased system security. The authors also investigated the protection metric of maximizing the minimal attack cost among all meters.

Kosut et al. [90] considered two regimes of FDI attacks on state estimation in smart grids, where for the weak attack regime, the number of meters that the attacker manipulates is smaller than that in the strong attack regime. The problem is addressed by the adversary from a decision theoretic point of view [91, 92]. For the system operator, a generalized likelihood ratio test (GLRT) detector is devised with incorporation of historical data. The Bayesian formulation can take advantage of priori information to preserve and trace the likely state of the system.

Kim and Poor [93] proposed strategic countermeasures against FDI attacks on the power grid based on linearized measurement models. They first suggested devising a new low-complexity attacking strategy, after which they designed a greedy approach to protect a number of meter measurements for defense. Finally, they developed another greedy approach to promote the PMU deployment to defend against such attacks.

Giani et al. [94, 95] investigated unobservable data integrity attacks on power systems. First, an efficient approach was presented to obtain all the sparse attacks where a modest number of meter measurements are compromised. Known-secure PMUs were used as countermeasures against such cyber attacks. Finding a way to ascertain the minimum number of necessary PMUs at carefully chosen buses was finally analyzed for defense.

Bi and Zhang [96] proposed countermeasures against FDI attacks by protecting critical state variables. To this end, the authors carefully selected a minimum number of meter measurements to be protected. Both optimal and complexity-reduced suboptimal approaches were provided to obtain the defense objective at the minimum cost. After characterizing the problem into a Steiner tree in graph theory, the researchers leveraged graphical methods to select the minimum number of meter measurements [49]. In addition, by jointly considering the conventional protecting meter measurements and the covert

topological information, they further proposed a mixed protection strategy, in case either of them failed to obtain the defense objective [50, 97].

2.3.3 Wide-Area Under-Frequency Load Shedding Protection

There has been massive number of publications in the literature that discussed the topic of cyber attacks on AGC and PSSE as explained in the previous sections. Nevertheless, the cyber security of Wide-Area Protection Schemes (including WAUFLS schemes) have been barely touched or just been visited quickly in the papers that discusses the cyber security of WAMPAC in general like [98]. To the best knowledge of the authors, only one reference has discussed the data integrity attacks to load shedding schemes in power systems [99], not to under-frequency load shedding specifically. In this subsection, the recent trends in UFLS protection schemes are discussed.

Generally speaking, Wide-Area Protection (WAP) is a new centralized kind of protection system that is based on wide-area measurements. It can also coordinate with conventional protections to protect critical loads, rapidly isolate faulty electrical components, reliably and accurately perform online security analysis for the post-fault or post-disturbance system, and take appropriate measures when necessary to prevent the power system from cascading or outages or even blackouts from occurring [100]. WAUFLS protection schemes have recently been replacing conventional under-frequency protection relays.

The main reason for under-frequency in a power system is the unbalance between generation and load. This takes place when a large generator is tripped, a sudden load is connected, or a large interconnection line is disconnected. Load shedding is a process used to relieve this mismatch by regaining the balance between load and generation [101]. Under-frequency load shedding schemes must have the following four characteristics [102]:

1. Their action should be quick so that the frequency drop is halted before more catastrophic events can occur.

2. Unnecessary actions must be avoided.

3. The protection system should be liable and redundant, as a malfunction of it would surely lead to power system cascading.

4. The amount of load to be shed should always be the minimum possible but still sufficient to restore the security of the grid and to avoid the minimum allowable frequency being overcome.

Traditionally, UFLS schemes were local and depended only on the absolute value of the frequency [102, 103]. These techniques basically shed a certain amount of the load under relief when the system frequency falls below a certain threshold. If the frequency keeps on falling after the first shed, further sheds are performed when lower thresholds are passed. The values of the thresholds and the relative amounts of load to be shed are decided off-line, on the basis of experience and simulations. Some of these techniques are based on measuring the Rate of Change of Frequency (ROCOF) when a certain frequency threshold is reached. These strategies are called semi-adaptive techniques [102].

Many centralized WAUFLS schemes have recently been proposed [104–109] that utilize the ROCOF and depend on the system frequency response. The value of ROCOF at the moment of disturbance is proportional to the size of the disturbance through the inertia constant H. Thus, given the value of the system inertia, the value of ROCOF at the moment of the disturbance provides an indication of the size of the disturbance, thereby enabling the activation of load shedding. One disadvantage of this method is that if generators or large synchronous motors are disconnected during the disturbance, the inertia of the system needs to be adapted accordingly. It has been proven that this method works efficiently with large systems characterized by high inertia. [102]. In the following paragraphs, schemes that are considered for testing in this work are reviewed.

In [104], a UFLS scheme based on the voltage stability of the system was proposed. Following a disturbance, a voltage stability risk index (VSRI) is calculated at all load buses. This index is then used to suggest a dynamic voltage stability criterion by which suitable locations for load shedding can be chosen. Another approach of adaptive UFLS was presented in [105], where the authors used the non-recursive Newton-type algorithm to

locally estimate the frequency of the system as well as the ROCOF. These values are sent to the control center and used to calculate the amount of disturbance, if any. Accordingly, a control action was then derived and distributed throughout the power system.

In [106], an approach for obtaining a few-seconds-in-advance frequency prediction was tested. This technique makes decisions about the amount of load to be shed, while at the same time being aware that inaccuracies in the procedure are inevitable. The scheme depends on calculating the frequency of the wide area by calculating the average of PMUs measurements. It then tries to approximate the deviation of the frequency to a second-order polynomial or a straight line based on the frequency declination. Accordingly, it can predict the time or frequency at which the system frequency violates the allowable values and, depending on the predicted values, it can calculate the amount of load to be shed. This process continues until reaching the nominal value of the frequency again.

In [108], a centralized adaptive under-frequency load shedding controller (CAULSC) based on UFLS and Distribution State Estimation (DSE) was proposed for microgrids with distributed resources when they are operated as isolated islands. The proposed controller calculates the amount of disturbance in two different ways according to the nature of the disturbance. If the microgrid is islanded from the grid or if one of the generators in the microgrid is disconnected and the microgrid has already been islanded, the power flow model of the system is used to calculate the magnitude of disturbance. If the disturbance is a sudden change in the load demand, the frequency at the center of inertia of the system and the ROCOF are utilized, using the swing equation to calculate the magnitude of disturbance. Finally, the DSE estimates the load demand at each bus and distributes the load shedding between different buses accordingly.

Two centralised adaptive load shedding algorithms are proposed in [109]. The first algorithm is response-based and the second one is a combination of event-based and response-based methods. The proposed methods are capable of preserving power system instability even for large disturbances and combinational events. They use both frequency and voltage variables to select appropriate amounts of load shedding.

2.4 Discussion and List of Gaps

There are numerous existing applications of wide-area protection and control systems, with some examples described and discussed above. Existing implementations use simple measurements, and sometimes the measurements are local only. In most cases, however, the measurements and actions use wide-area information and communications systems. Therefore, more attention must be paid towards the security of these applications, as otherwise, catastrophic disasters may occur.

Based on the literature survey conducted above, the following list of gaps has been extracted:

1. The impact of FDI attacks on AGC systems has been investigated using different methodologies. Nevertheless, the mitigation against the effect of FDI on AGC systems has barely been touched [53, 80–82].

2. The above-mentioned papers provided their solutions and some case studies where their solutions apply. None of them provides formal proofs for the stability of the system after incorporating the attack mitigation scheme nor the unbiasedness of the estimated signals.

3. All the above works considered a linear model of the AGC system. In other words, none of these works considered the different sources of AGC nonlinearities, which include dead-band of speed governor, transmission delay, and Generation Rate Constraints (GRC). Consequently, the derived FDI attack detection schemes proposed in the preceding studies may fail when the underlying AGC system is nonlinear.

4. Despite the fact that the problem of cyber attacks against wide-area control and monitoring schemes (for example AGC and PSSE) is considered in many publications, the impact on all other schemes, including RAS schemes, has barely been acknowledged.

5. Despite the above-mentioned advancements in wide-area monitoring using PSSE based on PMU measurements, the current WAUFLS protection schemes still depend on older techniques to evaluate system disturbances. These techniques rely

only on the characteristics of system frequency measurements, which are prone to cyber attacks. An attacker can drag the system to blackout if access to any of these frequency measurements is gained.

Chapter 3

Problem Formulation

This chapter investigates the problem of cyber-physical attacks on AGC systems, PSSE, and WAUFLS protection schemes. As well, attacker capabilities and possible damage that can be caused to the power system as a result of an attack are also given, along with the mathematical formulation of each attack scenario. To support the formulations, various attack scenarios are simulated in MATLAB/Simulink and PSCAD/EMTDC, using practical systems.

3.1 False Data Injection (FDI) Attack Model

WAMPAC schemes use IEC 61850 communication protocols. These protocols use different communication media i.e., wireless, fiber optics and Microwave, and support increased communication between both local and remote substation devices. However, this increases the exposure of the remote substations to cyber attacks because these substations are geographically dispersed and often maintain limited physical network protections [8, 41, 98, 110–112]. Therefore, it is assumed that the attacker has access to a subset of system measurements through the communication system. This subset includes both frequency and power flow measurements. It is also assumed that these measurements are

sent through a wireless medium that the attacker can access, but that the attacker cannot physically access the system at any point. In addition, the attacker cannot access/tamper with control decisions of the control center/EMS decisions [81]. Without this constraint, it is a trivial exercise for any attacker that has successfully penetrated the protected network to trigger cascading failures across the power grid. It is therefore conceivable that an energy provider would make protecting its EMS its foremost priority. Protecting every other single communication link in the power system is extremely expensive, especially in large power systems that mainly depend on the communication network that carries hundreds of signals.

Table 3.1 summarizes the objectives, capabilities and limitations of the attacker as well as the assumptions that this work is based on. The attack model mentioned in Table 3.1 is used throughout the work.

Table 3.1: Attack Model

Attacker	**Objective(s)**	- cause system-wide blackout - cause equipment damage - cause power disruption
	Capabilities	- has access to any or all frequency measurements - has access to power flow measurements
	Limitation(s)	- cannot access the system physically - has no access to the control decision signals
Assumption(s)		- system measurements are sent through wireless communication

3.2 FDI Attacks on AGC Systems

3.2.1 State-Space Model of the AGC System

The control block diagram of the utilized two-area AGC system used throughout the first part of this study is described in [65]. A modified version of this block diagram is

shown in Fig. 3.1, where three additional inputs, labeled d_1, d_2 and d_3, are added to model the effect of FDI attacks on the frequency deviation in Area 1, Δf_1, frequency deviation in Area 2, Δf_2, and tie-line power ΔP_{tie}, respectively. Table A.1 shows the assumed numerical values for the system parameters.

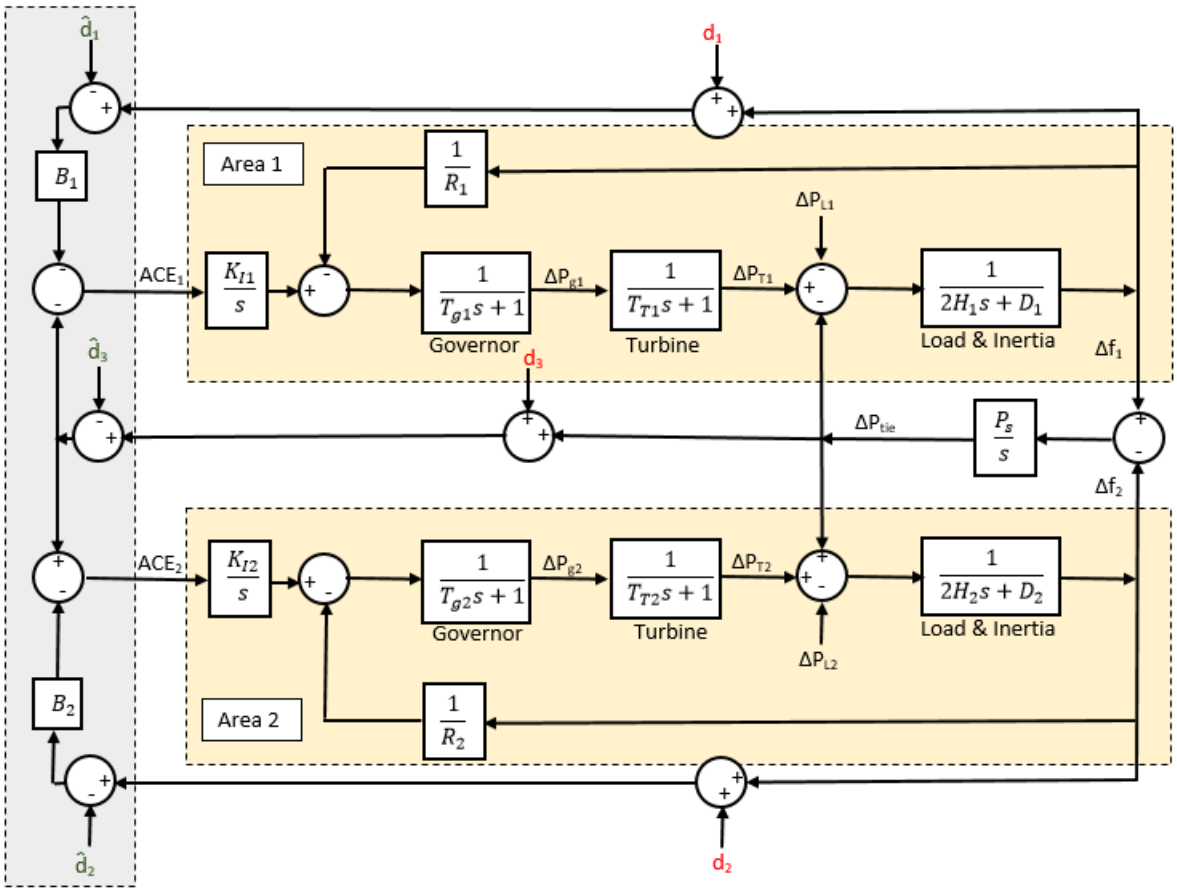


Figure 3.1: Block diagram of the two-area AGC system, where d_1, d_2, d_3 denote the FDI attack signals and $\widehat{d}_1, \widehat{d}_2, \widehat{d}_3$ denote the corresponding estimates

The system is modeled using the following state-space equation:

$$\dot{x}(t) = A_c x(t) + B_c u(t) + \omega(t) \tag{3.1}$$

where the system state vector $x(t)$ includes changes in the frequency Δf, the mechanical turbine power ΔP_m, the steam valve position (governor power) ΔP_V, the AGC integrator output for both areas, and the tie-line power. More precisely,

$$x = [\Delta f_1, \Delta P_{T1}, \Delta P_{g1}, \Delta f_2, \Delta P_{T2}, \Delta P_{g2}, \Delta P_{tie}, ACE_1, ACE_2]^\top \tag{3.2}$$

The load disturbances in Area 1 and Area 2 are denoted by $u(t) = [u_1(t), u_2(t)]^\top$, and $\omega(t)$ indicates the process noise. Following [71, 113], the state-space matrices for the two-area AGC system considered throughout our investigation are obtained as explained below.

Area 1 includes three system state variables, namely the frequency deviation at Area 1, Δf_1, the turbine output power ΔP_{T1}, and the governor output power ΔP_{g1}. These state variables can be calculated as follows:

$$\dot{\Delta f_1} = \frac{-D_1}{2H_1}\Delta f_1 + \frac{1}{2H_1}\Delta P_{T1} - \frac{1}{2H_1}\Delta P_{tie} - \frac{1}{2H_1}u_1 \tag{3.3}$$

$$\dot{\Delta P_{T1}} = \frac{-1}{T_{T1}}\Delta P_{T1} + \frac{1}{T_{T1}}\Delta P_{g1} \tag{3.4}$$

$$\dot{\Delta P_{g1}} = \frac{-1}{R_1 T_{g1}}\Delta f_1 - \frac{1}{T_{g1}}\Delta P_{g1} + \frac{1}{T_{g1}}ACE_1 \tag{3.5}$$

Similar to Area 1, the state variables related to Area 2 can be calculated as follows:

$$\dot{\Delta f_2} = \frac{-D_2}{2H_2}\Delta f_2 + \frac{1}{2H_2}\Delta P_{T2} + \frac{1}{2H_2}\Delta P_{tie} - \frac{1}{2H_2}u_2 \tag{3.6}$$

$$\dot{\Delta P_{T2}} = \frac{-1}{T_{T1}}\Delta P_{T2} + \frac{1}{T_{T1}}\Delta P_{g2} \tag{3.7}$$

$$\dot{\Delta P_{g2}} = \frac{-1}{R_2 T_{g2}}\Delta f_2 - \frac{1}{T_{g2}}\Delta P_{g2} + \frac{1}{T_{g1}}ACE_2 \tag{3.8}$$

The tie-line power is related to the frequency deviation in both areas, as follows:

$$\dot{\Delta P_{tie}} = P_s\Delta f_1 - P_s\Delta f_2 \tag{3.9}$$

The ACE for each area is defined as:

$$A\dot{C}E_1 = -K_{I1}B_1\Delta f_1 - K_{I1}\Delta P_{tie} - K_{I1}B_1 d_1 - K_{I1}d_3 \tag{3.10}$$

$$A\dot{C}E_2 = -K_{I2}B_2\Delta f_2 + K_{I2}\Delta P_{tie} - K_{I2}B_2 d_2 - K_{I2}d_3 \tag{3.11}$$

where

$$B_1 = \frac{1}{R_1} + D_1, B_2 = \frac{1}{R_2} + D_2$$

Therefore, the state-space matrices for the system are given by:

$$A_c = \begin{bmatrix} \frac{-D_1}{2H_1} & \frac{1}{2H_1} & 0 & 0 & 0 & 0 & \frac{-1}{2H_1} & 0 & 0 \\ 0 & \frac{-1}{T_{T1}} & \frac{1}{T_{T1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-1}{R_1 T_{g1}} & 0 & \frac{-1}{T_{g1}} & 0 & 0 & 0 & 0 & \frac{1}{T_{g1}} & 0 \\ 0 & 0 & 0 & \frac{-D_2}{2H_2} & \frac{1}{2H_2} & 0 & \frac{-1}{2H_2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{T_{T2}} & \frac{1}{T_{T2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{R_2 T_{g2}} & 0 & \frac{-1}{T_{g2}} & 0 & 0 & \frac{1}{T_{g2}} \\ P_s & 0 & 0 & -P_s & 0 & 0 & 0 & 0 & 0 \\ -K_1 B_1 & 0 & 0 & 0 & 0 & 0 & -K_1 & 0 & 0 \\ 0 & 0 & 0 & -K_2 B_2 & 0 & 0 & K_2 & 0 & 0 \end{bmatrix}$$

$$B_c = \begin{bmatrix} \frac{-1}{2H_1} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{-1}{2H_2} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$C_c = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

To make (3.1) suitable for numerical simulations, it has to be discretized. The sampled discrete-time model of the A_c and B_c matrices is given by:

$$A = e^{A_c \times T_s} \tag{3.12}$$

$$B = \int_{\tau=0}^{T_s} e^{A_c \times \tau} B_c d\tau \tag{3.13}$$

where T_s is the sampling period. Therefore, the discretized state-space model of the considered two-area power system is:

$$x_{k+1} = Ax_k + Bu_k + \omega_k \tag{3.14}$$

where x_k and u_k are the state and input vectors at time step k, respectively. The sampling rate is considered to be 10 ms in this work.

3.2.2 Stealthy FDI Attacks on AGC Systems

The attacker can manipulate the frequency signals of different areas, the tie-line power signals, or both. When these falsified data are reported to the control center, the control center operator calculates a false value for the ACE of different areas, and false generator correction values are sent to different generators. For an n area system, the new value of the area control error in Area i due to the attack is:

$$ACE_{ia} = \sum_{j=1}^{n} a_{ij}(\Delta P_{tie,ij} + A_P) + \beta_i(\Delta f_i + A_f) \tag{3.15}$$

where A_f and A_P are the FDI attack signals in frequency measurements and tie-line power, respectively.

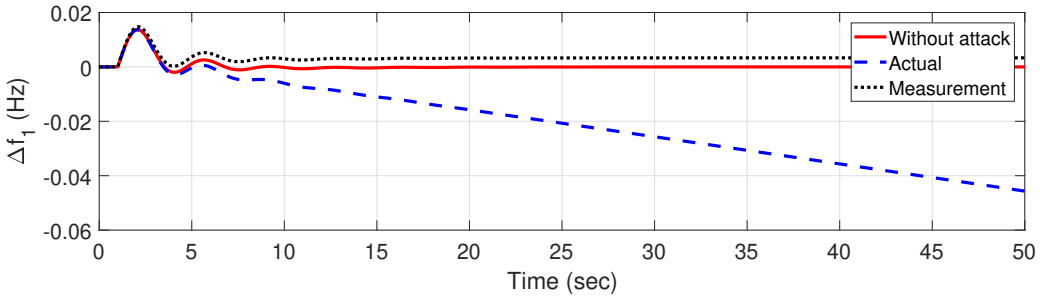
For an FDI attack to be stealthy, it needs to bypass the bad data detection algorithms implemented within the control center. Moreover, the grid operator may apply other data quality checks on the received measurements. For instance, the measurements should not change significantly over a short period. Intuitively, if each element of the FDI attack vector is bounded around zero, these data quality checks, designed to be insensitive to natural random noises in the measurements, will not be alerted [53]. Thus, for the attack to be effective, the selection of attack parameters (e.g., magnitude and rate of change) is critical from the attacker's perspective. The parameters have to be selected such that the attack creates the desired impact but does not trigger any data quality alarms in the control center. For example, in AGC systems, abrupt changes and excessive values for the ACE would be avoided by attackers to evade detection. For Area i, this can be formulated mathematically using the following expression:

$$|\frac{ACE_{i,t} - ACE_{i,t+T}}{T}| < \psi \tag{3.16}$$

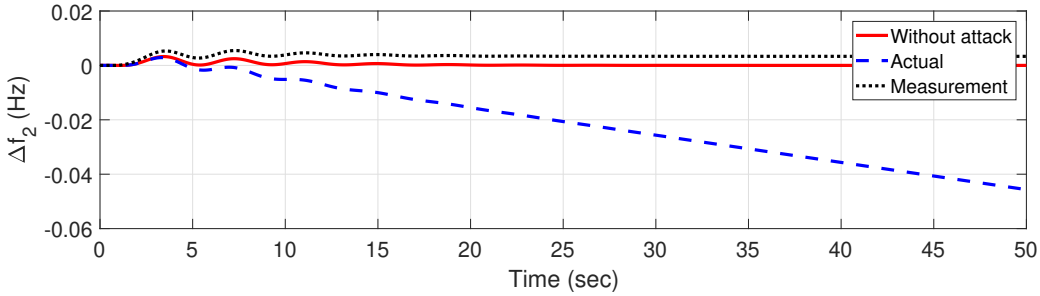
where $ACE_{i,t}$ is the ACE signal at time t for Area i, T is the time interval where two successive ACE samples are measured, and ψ is the maximum ACE signal curve slope [80]. In this work, detection and mitigation of slowly varying attack signals are considered because they satisfy the above conditions and allow for stealthy attacks. Nevertheless, the proposed approach, in this chapter, is not restricted to this class of attacks and can detect and mitigate other types of FDI attacks.

A stealthy attack scenario is carried out to show the effectiveness of FDI attacks on the operation of a two-area AGC. A pre-scheduled load reduction of 20% took place in Area 1. To simulate a gradual increase in the system frequency, the attacker injected a ramp signal with a slope of 0.001 to the frequency measurement signals of areas 1 and 2. Due to this attack, the control center operator sees that there is an over-frequency condition in the system. Accordingly, and based on the calculated ACE, the control center operator decides to reduce the generation to avoid the over-frequency condition. However, the real situation in the system is the opposite, i.e., the system frequency is dropping and an under-frequency condition has developed, as shown in Fig. 3.2. This situation might

force the under-frequency control in the generator to shut down, causing a system-wide blackout.



(a) Frequency deviation in Area 1



(b) Frequency deviation in Area 2

Figure 3.2: AGC performance under attack scenario 1

3.3 FDI Attacks on PSSE

Power System State Estimation (PSSE) is employed to ensure system stability and observability of state variables, such as voltage magnitudes and phase angles of all buses. These states are estimated based on available field measurements. In the general formulation of ac PSSE, power flow measurements are related to the system states by:

$$z = h(x) + e \tag{3.17}$$

where z is the power flow measurement vector that includes voltage, active/reactive power injection, and active/reactive power flows from system meters, x is the system state vector of voltage magnitudes and angles, $h(x)$ is a nonlinear function that maps the states to the measurements, and e is the measurement error vector. The optimal estimates of the system states are obtained by means of a WLS optimization problem:

$$minimize\ J(x) = (z - h(x))^T W (z - h(x)) \tag{3.18}$$

where W is the co-variance diagonal matrix of error inverses, representing weights based on meter accuracy. The standard procedure for solving (3.18) is applying iterative methods [64], where the first optimal condition is given by:

$$\frac{\partial J(x)}{\partial(x)}|_{x=\hat{x}} = -2\left[\frac{\partial h(\hat{x})}{\partial(\hat{x})}\right]^\top W(z - h(\hat{x})) \tag{3.19}$$

where $\hat{x}$ is the estimated state vector, obtained by the iterative process of the resulting nonlinear equation.

Note that the attacker can manipulate voltage magnitudes, phase angles, or both. In this work, only voltage magnitudes are considered as target state variables to be manipulated, as per the attack objective. This can be done indirectly by altering the measurements which are dependent on any given state variable. The Jacobian matrix of $h(x)$, J_h, maps the relation between the system states and measurements and thus allows it to determine which measurements to alter in order to affect a specific state variable, as shown below:

$$J_h = \begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_1}{\partial x_2} & \cdots & \frac{\partial h_1}{\partial x_{n-1}} & \frac{\partial h_1}{\partial x_n} \\ \frac{\partial h_2}{\partial x_1} & \frac{\partial h_2}{\partial x_2} & \cdots & \frac{\partial h_2}{\partial x_{n-1}} & \frac{\partial h_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\partial h_{m-1}}{\partial x_1} & \frac{\partial h_{m-1}}{\partial x_2} & \cdots & \frac{\partial h_{m-1}}{\partial x_{n-1}} & \frac{\partial h_{m-1}}{\partial x_n} \\ \frac{\partial h_m}{\partial x_1} & \frac{\partial h_m}{\partial x_2} & \cdots & \frac{\partial h_m}{\partial x_{n-1}} & \frac{\partial h_m}{\partial x_n} \end{bmatrix} \tag{3.20}$$

The J_h rows correspond to m measurements and the columns correspond to n state variables. For any measurement that is directly dependent on the a specific state variable, the corresponding element in row and column must be non-zero.

To find the set of measurements needed to alter a specific state variable, the attacker considers the rows of measurements for which the column of the targeted state has non-zero elements. This analysis yields the upper bound on the number of measurements to be attacked. In order to determine the value of manipulation of these measurements, the attacker then considers the power flow equations:

$$\begin{aligned} P_{ij} =& V_i^{'2} \cdot g_{ij} - V_i' V_j \cdot g_{ij} \cos(\theta_i - \theta_j) \\ & - V_i' V_j \cdot b_{ij} \sin(\theta_i - \theta_j) \end{aligned} \tag{3.21}$$

$$\begin{aligned} Q_{ij} =& - V_i^{'2} \cdot \left(b_{ij} + b_{ij}^{sh}\right) + V_i' V_j \cdot b_{ij} \cos(\theta_i - \theta_j) \\ & - V_i' V_j \cdot g_{ij} \sin(\theta_i - \theta_j) \end{aligned} \tag{3.22}$$

where V_i' is the voltage magnitude to be altered at bus i, θ_i is the voltage angle at bus i, and g_{ij}, b_{ij}, and b_{ij}^{sh} are the conductance, susceptance, and shunt susceptance of the line between node i and j, respectively. Active and reactive power injection at node i are represented by:

$$P_i = \sum_{j \in \Omega} P_{ij} \tag{3.23}$$

$$Q_i = \sum_{j \in \Omega} Q_{ij} \tag{3.24}$$

where Ω is the system bus's set. It follows that in order to change the voltage magnitude at bus i, power flow equations (3.21)-(3.24) are solved to determine the required changes in measurements. Let vector $\vec{c}$ represent the vector of values to be added to the state variables. Based on this attack formulation, the condition for a stealthy FDI attack has been outlined for ac systems, as follows:

$$\begin{aligned} \|z_a - h(\hat{x}_{bad})\| &= \|z + a - h(\hat{x} + c)\| \\ &= \|z - h\hat{x}\| \leq \tau \end{aligned} \tag{3.25}$$

where $\vec{a}$ is the attack vector and $\vec{z_a}$ is the resulting manipulated measurements vector. Therefore, the criteria for a stealthy hidden attack are given by:

$$a = h(\hat{x} + c) - h(\hat{x}) \tag{3.26}$$

This attack vector manipulates state variables without raising the BDD alarm. The algorithm is grounded in the following assumptions [45]: 1) All measurements in the sub-graph surrounding a power injecting bus are to be changed; 2) power injection change summations must be kept at zero; and 3) attack vector sparsity depends on system topology. It is worth mentioning that the attack strategy must also adhere to the electrical laws of the power networks (e.g., current and power nodal balances).

3.4 FDI Attacks on UFLS Schemes

3.4.1 Operation of WAUFLS

According to the literature, and as depicted in Fig. 3.3, the general procedure of WAUFLS schemes [114] can be summarized as follows:

i. The control center receives frequency measurements for different areas from the PMUs installed in the system. The ROCOF is calculated either by the PMUs or locally at the control center in the grid.

ii. The frequency measurement and ROCOF values are used to evaluate system disturbance. Currently, the magnitude of disturbance is calculated by swing equations for all generators [104–107, 109, 115]. For the i-th generator in a system with N generators, it can be written as:

$$\Delta P_i = P_{m_i} - P_{e_i} = \frac{2H_i}{f_n}\frac{df_i}{dt} \tag{3.27}$$

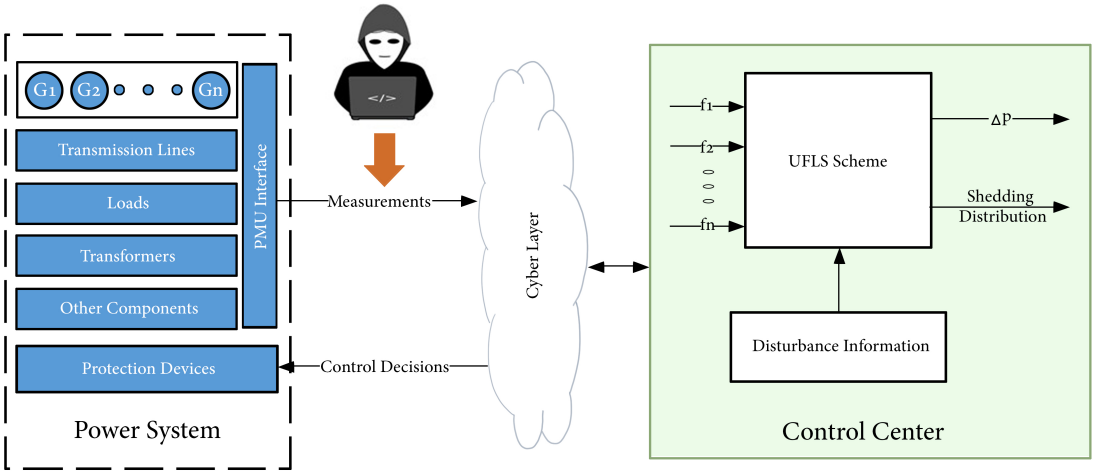


Figure 3.3: Schematic of WAUFLS protection schemes

where ΔP_i is the imbalance between generation and load(s) in pu, P_{m_i} is the pu input mechanical power, P_{e_i} is the pu output electrical power, H_i is the inertia constant in sec, f_i is the frequency in Hz, and f_n is the system nominal frequency in Hz. The total resulting magnitude of disturbance can be obtained by summing the individual disturbances from each generator, as follows:

$$\Delta P = \sum_{i=1}^{N} \Delta P_i = \frac{2\sum_{i=1}^{N} H_i}{f_n} \frac{df_c}{dt} \tag{3.28}$$

$$f_c = \frac{\sum_{i=1}^{N} H_i f_i}{\sum_{i=1}^{N} H_i} \tag{3.29}$$

where f_c is the frequency of the equivalent center of inertia.

iii. The control center determines the amount of load to be shed (power mismatch) based on the amount of the disturbance and system spinning reserve as [104, 107]:

$$P_{shed} = 1.05 \times (\Delta P - P_{th}) \tag{3.30}$$

where P_{th} is the the threshold value of power mismatch (available spinning reserve), and 1.05 is introduced for compensating the simplifying hypotheses adopted to develop the reduced SFR model.

iv. Finally, a shedding control action is sent by the control center to an area or shared between different areas based on disturbance information, which includes the nature of the disturbance, the location of the disturbance, and a load sensitivity analysis. To achieve load shedding, a combination of loads is selected such that the sum of their total active powers is as close as possible to P_{shed}. There are different criteria by which load shedding locations can be selected. However, the most common criteria used in wide-area applications is the voltage collapse-based load shedding, as the voltage collapses rapidly after a disturbance [104, 107, 109, 116–118].

The shedding locations are mainly selected based on the location of disturbance [104]. In other words, the load shedding is distributed between the buses that are close to the disturbance according to their voltage dip during the disturbance. All area buses are ranked based on voltage dips. Accordingly, the load shedding at bus i is proportional to the bus rank, as follows

$$P_{shed,i} = \frac{\Delta V_i}{\sum_i^{N_v} \Delta V_i} \times P_{shed} \tag{3.31}$$

where ΔV_i is the voltage dip at bus i immediately after the disturbance, and N_v is the set of buses that have the highest voltage dip. Once the load to be shed is known for all buses, the shedding process takes place in steps.

3.4.2 Attack Strategies

The following subsections explain in detail three different scenarios by which the attacker can target the operation of the WAUFLS schemes in the power systems. Depending

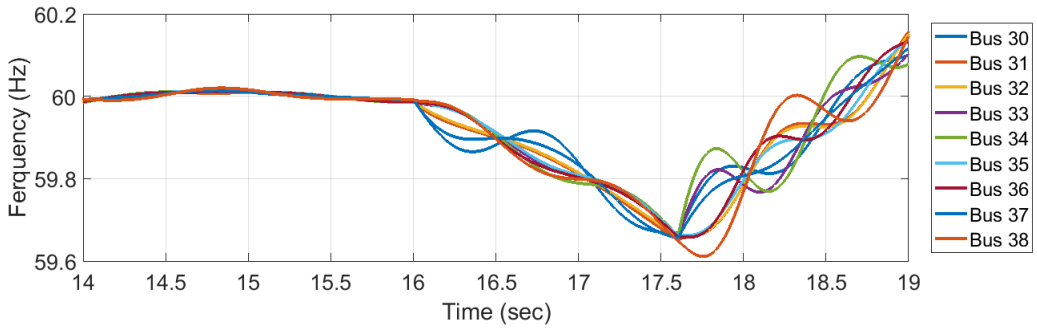


Figure 3.4: Frequency values at different buses

on what data are available for the attacker (attacker's access level), the attacker can launch an attack. The first scenario explains how can the attacker launch an attack if they have access to one or more frequency signals. It is shown that the attacker will have a full control over the amount of load to be shed. The second scenario explains the case where the attacker has access to PFMs. In this case, the attacker cannot manipulate the amount of load to be shed, but they can force the control center operator to shed load from incorrect locations. Finally, if the attacker has access to both PFMs and frequency measurements, they can fake a disturbance and cause unnecessary load shedding by the control center.

A. Targeting the magnitude of disturbance

Power system frequency is usually dealt with as a global parameter. However, many results in the literature indicate that the frequency slightly differs from one neighboring area to another during system transients [119]. This is also shown in the simulation results of Fig. 3.4 for the IEEE 39 bus system, where small deviations between frequency values at different buses can be seen clearly. The deviations give attackers an opportunity to manipulate each frequency measurement value separately. In some systems, point-to-point secure communication links are used for frequency measurements, but due to the cost of the links, not all control systems implement them to secure frequency measurements.

As mentioned above, control centers make use of the values of a frequency and its

derivative to evaluate system-wide disturbances using swing equations to calculate the amount of load required to be shed. Equation (3.28) also shows that the magnitude of disturbance given by the swing equation (ΔP) depends more on the ROCOF than on the frequency value itself. This allows the attacker to construct an FDI attack that does not change the magnitude of the frequency significantly, though it does change the slope of the frequency signal to affect the calculated magnitude of disturbance. In other words, the attacker works on manipulating the ROCOF, not the frequency magnitude, in order to have the maximum effect on the swing equation output. Hence, the attacker can control the output of the swing equation (ΔP) to force the control center operator to make a wrong action, either by shedding a lower load amount (leading to system blackout) or shedding a higher load amount (causing damage to system equipment due to over-frequency conditions). To launch such an attack, the attacker does not need to access the system physically. However, he or she does need to access one or more frequency measurement signals, which can occur if that signal is sent through wireless communication.

To formulate the attack mathematically, it is assumed that the attacker injects a linear varying signal to one or more frequency measurements. Without loss of generality, it is assumed that the FDI takes place on all frequency values. The frequency value of generator i after manipulation is:

$$f_{ia} = f_i \pm m_i t \tag{3.32}$$

where m_i is the slope of the attack signal. Substituting the new frequency values into (3.29), the center of inertia frequency is:

$$\begin{aligned} f_{ca} &= \frac{\sum_{i=1}^{N} H_i f_i \pm \sum_{i=1}^{N} H_i m_i t}{\sum_{i=1}^{N} H_i} \\ &= f_c \pm \frac{\sum_{i=1}^{N} H_i m_i t}{\sum_{i=0}^{N} H_i} \end{aligned} \tag{3.33}$$

The new magnitude of disturbance can be calculated by substituting into (3.28), as follows:

$$\begin{aligned}\Delta P_a &= \frac{2\sum_{i=1}^{N} H_i}{f_n}\frac{df_{ca}}{dt} \\ &= \frac{2\sum_{i=1}^{N} H_i}{f_n}\frac{d}{dt}\left[f_c \pm \frac{\sum_{i=1}^{N} H_i m_i t}{\sum_{i=0}^{N} H_i}\right] \\ &= \Delta P \pm \frac{2\sum_{i=1}^{N} H_i m_i}{f_n} = \Delta P \pm \Delta P_{attack} \end{aligned} \tag{3.34}$$

Hence, the attacker needs only to calculate the slopes of the injected signal to change the magnitude of disturbance, which then changes the total amount of load to be shed. The above model of the attack is generic, i.e., the attacker can manipulate only one or two frequency values. In this case, the value of the injected signals into other frequency measurements is zero.

B. Targeting Load Shedding Distribution

As aforementioned, system operators utilize bus voltage magnitudes in order to accurately perform load shedding, using (3.31), from buses with the highest voltage dips. Therefore, an attacker needs to manipulate the voltage magnitudes on target buses in order to compromise the load shedding process. In this section, the stealthy FDI attack formulation that allows manipulation of specific bus voltages is presented. This formulation serves as a basis for the attack scenario that involves compromising the shedding distribution.

Equipped with the ability to target specific buses and manipulate voltage magnitudes, the attacker can easily compromise the load shedding distribution process. This is accomplished by changing the load shedding amount on a given bus and/or inducing load shedding on a bus outside of the initial load shedding setting. In other words, voltage disturbances at target locations (i.e., those which have a high voltage dip) are shown if they have a negligible voltage dip. At the same time, voltages of targeted buses (i.e., those which have a low voltage dip) are shown if they have the highest voltage dip. The attack can be formulated as follows:

i. Let set Ψ represent the initial set of buses on which load shedding is to be performed, with a load shedding amount of P_{shed_ψ}, where $\psi \in \Psi$. Also, let set Φ represent the set of buses the attacker is targeting to shed power from, with a load shedding amount of P'_{shed_ϕ}, where $\phi \in \Phi$. The selection of set Φ can be based on a sensitivity analysis of the system to power shedding, buses with lowest voltage dips, or buses with critical loads.

ii. The attacker then aims to change the voltage magnitudes to

$$V'_\phi = V_\phi + c_\phi, \quad \forall \phi \in \Phi \tag{3.35}$$

$$V'_\psi = V_\psi + c_\psi, \quad \forall \psi \in \Psi \tag{3.36}$$

where V'_ϕ (V'_ψ) is the new voltage magnitude for bus ϕ (ψ) after adding the attack value c_ϕ (c_ψ), as per (3.25) and (3.26). For set Φ, the attacker increases the voltage dip to incur more load shedding using (3.35) while decreasing the voltage dip of set Ψ to reduce the load shedding using (3.35).

iii. Due to the variation in voltage magnitude, the amount of shedding power for each bus P_{shed_ψ} changes. However, the total shedding amount must remain constant, as follows:

$$\sum_{\psi \in \Psi} P_{shed_\psi} = \sum_{\psi \in \Psi} P'_{shed_\psi} \tag{3.37}$$

Note that sets Φ and Ψ are independent and may overlap in certain buses. A special case of this attack will occur if the attacker chooses to have $\Phi = \Psi$ and only change the load distribution within the set.

C. Faking Underfrequency Conditions

In the previous subsections, we saw that the attacker has to synchronize the attack launch with a system disturbance. However, in the scenario considered here, the attacker's objective is to trick the system into responding as if it were experiencing under-frequency conditions that require activation of WAUFLS. In essence, the attacker fakes a disturbance

condition that misguides the system operator to launching an unnecessary load shedding process.

In this attack scenario, the attacker manipulates both the frequency measurements and the power flow measurements $\boldsymbol{z}$. This gives the attacker access to a higher number of meters, depending on the disturbance size, type and location. For example, if the attacker needs to fake a disturbance that includes the tripping of a specific generator, the attacker has to manipulate both the system frequency measurements and the power flow measurements of the meters that are close to this generator to reflect the disturbance on the state estimation results. This subsection explains how the attacker can fake disturbance conditions by considering different access levels to the system.

In disturbances that affect system frequency, it is expected that the voltage magnitudes would strongly deviate from the steady-state voltage profile. The FDI attack formulation given by (3.26) indicates that the attacker manipulates the power flow measurement to change the voltage profile to resemble a post-disturbance one. Undoubtedly, there is always a limitation on the number of measurement nodes the attacker is able to compromise. Thus, the objective of the attack is to manipulate the minimum number of measurements while simultaneously attempting to generate a voltage profile that matches as much as possible an actual post-disturbance voltage profile for all the buses.

Keep in mind that the attacker prioritizes stealth in the attacks, which limits the available techniques. Nonetheless, there are several approaches for targeting the manipulated states, such as minimizing the number of attacked measurements, constraining the attacks to a subset of states, and minimizing the probability of detection [45]. In this scenario, the attacks are launched based on the formulation in the previous section, in addition to selecting a subset of buses based on a threshold criterion.

The first step is to analyze variations between voltage magnitudes for each bus in the system at steady-state and post-disturbance. As expected, there is an inverse relation between the number of buses and the magnitude of ΔV. We devise the FDI strategy based on the ΔV threshold, as follows:

i. Simulate a disturbance scenario and determine the deviation index D_i, between

steady-state (V_{ss}) and post-disturbance voltage magnitude (V_d) for each bus $i \in \Omega$ at time step t in the simulation period T:

$$D_i = \max\left\{\text{abs}(V(t)_{d_i} - V(t)_{ss_i})\right\}, \quad \forall t \in T, \forall i \in \Omega \tag{3.38}$$

Note that max operator ensures that the threshold is based on the entirety of the simulation period T, and the absolute value is considered to account for positive and negative voltage deviations. The purpose of this step is to determine the maximum deviation of voltages during the disturbance for all buses.

ii. Classify each bus i according to whether it belongs to the attack set Ω_a, if it exceeds the pre-defined threshold γ, i.e., Bus $i \in \Omega_a$ if $D_i \geq \gamma$. The threshold represents the maximum allowable tolerance for voltage deviation between the disturbance and steady-state cases. A higher threshold γ implicates a smaller attack subset Ω_a, while at the same time giving a higher probability for raising suspicion with the system operator, as more buses would have a steady-state voltage profile rather than a disturbance profile. In effect, in this step, the attacker makes a compromise between the size of the attack vector and the probability of being detected. The threshold is determined by analyzing the voltage profile and normal deviations in voltages during steady-state operation.

iii. Launch a constrained FDI attack on power flow measurements that only targets buses belonging to the subset Ω_a. An indispensable condition for the success of such an attack is the ability to target specific state variables, as outlined in the attack formulation. It is intended to leave the remaining buses voltages unchanged from the state estimation process, as the variation between the state estimation voltages and the disturbances voltages would be of lesser magnitude and importance, respectively, based on the chosen case threshold. The index i determines the value of the attack element c_i to be added to the system state estimate $\hat{x}_i$, as per (3.26), as follows:

$$\hat{x}_{att,i} = \begin{cases} \hat{x}_i + c_i, & \text{if } i \in \Omega_a \\ \hat{x}_i, & \text{otherwise} \end{cases} \tag{3.39}$$

where $\hat{x}_{att,i}$ is the attacked state estimate. For this scenario, the attacker launches the attacks based on the pre-determined threshold γ. A compromise is made between the number of attacked measurements and the allowed deviation between perceived and expected voltage profiles.

3.4.3 Simulation Results

The attack scenarios discussed above are implemented on the IEEE 14 and IEEE 39 bus systems- shown in Fig. 3.5 and Fig. 3.6, respectively- to assess their impact on the power network. Detailed models of both systems are simulated in PSCAD and used for the study. Different attack scenarios are applied to simulate healthy system conditions, normal system disturbances, and transient conditions.

A. Targeting the magnitude of disturbance

The following scenarios show the system frequency (i.e., frequency of center of inertia) as well as the magnitude of disturbance with and without an attack. They also show how the attacker can target higher or lower amounts of load to be shed. The first two scenarios show the effect of the attack on the calculated magnitude of disturbance. However, scenarios 3 and 4 show how this attack can affect the whole system if the control center operator makes load shedding decisions based on manipulated measurements.

Scenario 1: With the outage of generator G3 in the IEEE 14 bus system, which is connected to bus 2, the transmission line connecting buses 2 and 5 is tripped due to overloading at $t = 20$ sec. At this moment, the attacker starts increasing the measurement of f_2 using a false signal of slope $m = 0.02$. The control center operator, in response, decides to shed a lower amount of load because the magnitude of calculated disturbance becomes lower (i.e., 0.55 pu instead of 1.05 pu) at the instant of disturbance, as shown in Fig. 3.7b. Figure 3.7 shows the center of inertia frequency as well as the magnitude of disturbance based on real and manipulated frequency values.

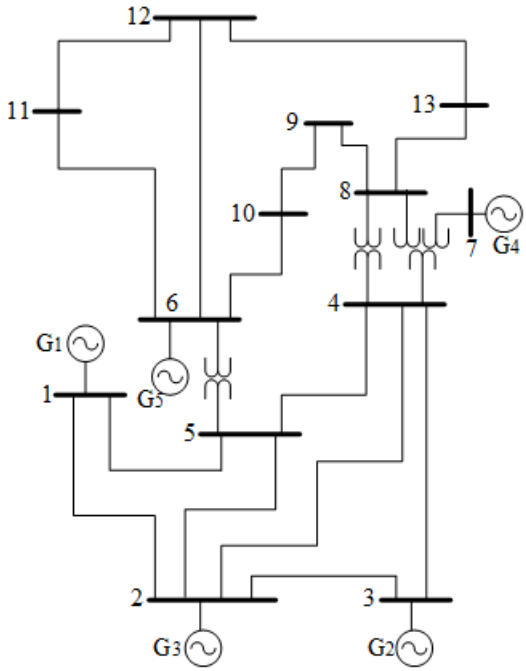


Figure 3.5: IEEE 14 bus system

Scenario 2: During an overload condition, e.g., when the IEEE 14 bus system has 20% additional load, the line connecting buses 1 and 5 is tripped at $t = 20$ sec. At this moment, the attacker decreases the measurement corresponding to the frequency of G5 using a signal that has a slope $m = -0.05$, as shown in Fig. 3.8a, aiming to increase the amount of load shedding. This results in a higher magnitude of disturbance (i.e., 2 pu instead of 1 pu), as shown in Fig. 3.8b.

It can be shown from the previous scenarios that injecting FDI into frequency measurements has a direct effect on the calculated magnitude of disturbance. Moreover, if the control center uses the falsified measurements to make load shedding decisions, disaster events might take place, as discussed in the following scenarios.

A large system disturbance takes place at $t = 16$ sec in the IEEE 39 bus system. The accepted variation in the value of f_c, where load shedding is not needed, is set at $\pm 1\%$ of

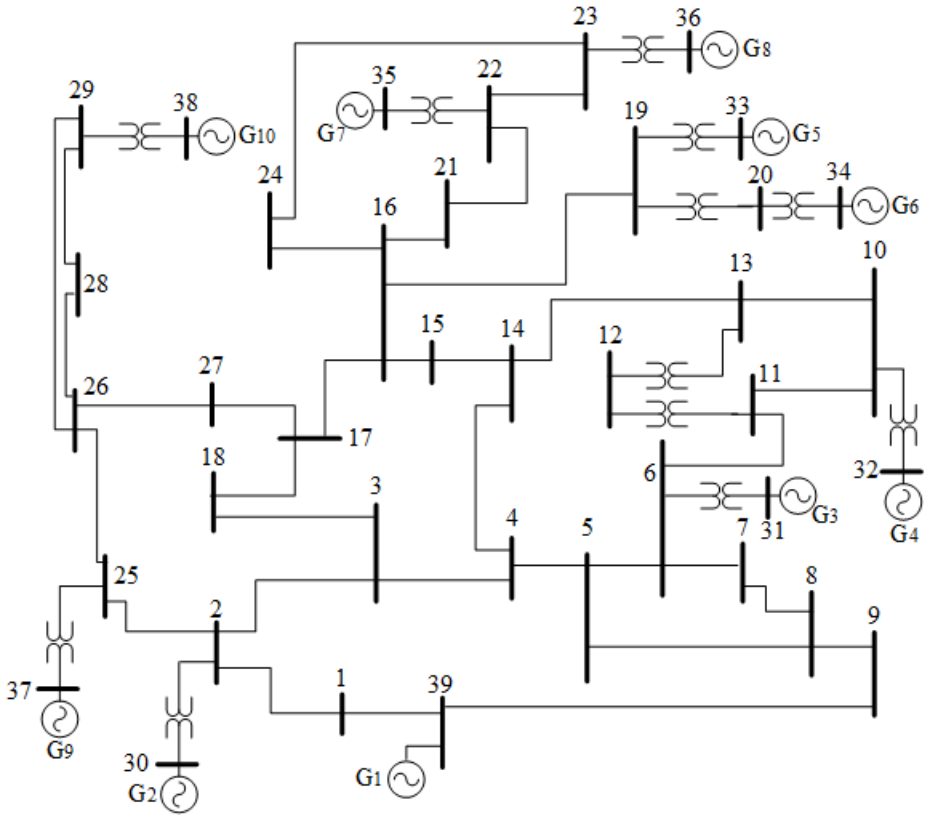
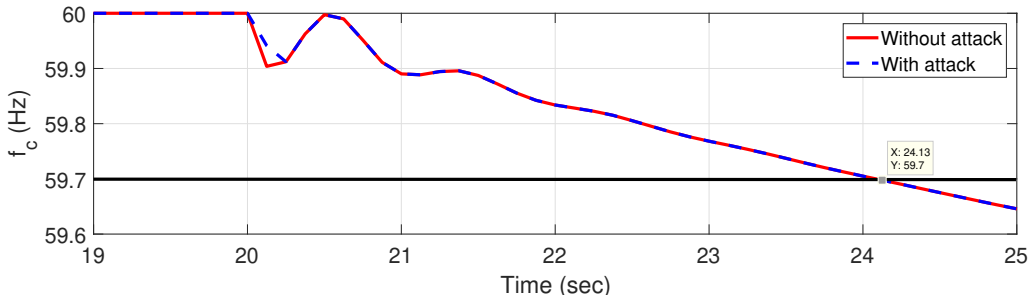


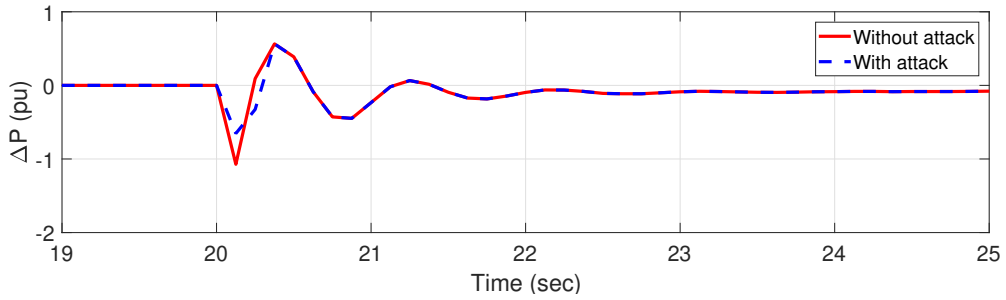
Figure 3.6: Schematic of IEEE 39 New England system

the nominal frequency values ($59.4 - 60.6\ Hz$ for the used 60 Hz system). The shedding process starts when the frequency of the center of inertia falls below 59.3 Hz. Scenarios 1 and 2 show how an attacker can manipulate system frequency signals to either increase or decrease the amount of load shedding and how this affects system frequency. In these scenarios, the values of the FDI on the frequency signal of generator i, given by $m_i t$, are chosen arbitrarily just to show the effect of the attack.

Scenario 3: Using the IEEE 39 bus New England system, the attacker manipulates the measurement corresponding to the frequency of generator G8 by increasing it, using an FDI signal that has a slope $m_8 = 0.02$. The center of inertia frequency f_c is then calculated to be higher than the system's actual center of inertia frequency. This causes



(a) Real and manipulated center of inertia frequency

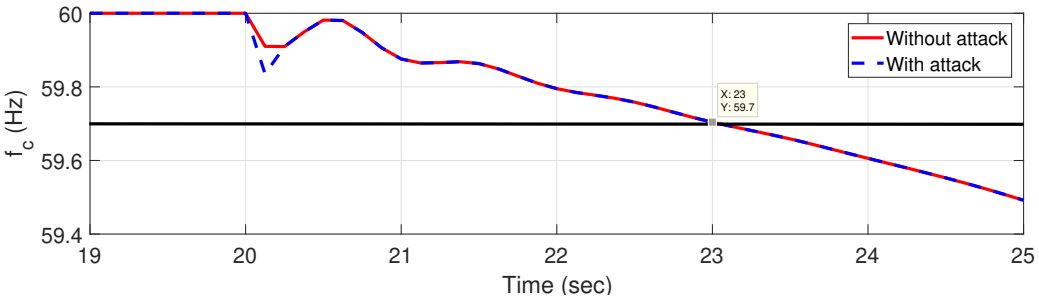


(b) Real and manipulated amount of disturbance

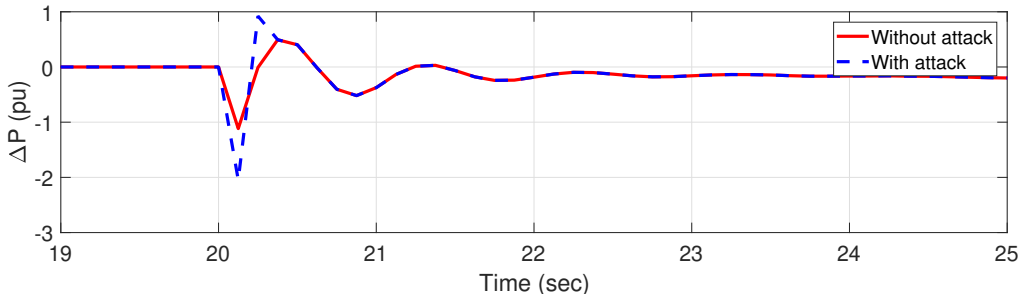
Figure 3.7: Targeting lower amount of load shedding

the calculated magnitude of disturbance ΔP to be 0.3 pu, which is lower than the actual disturbance in the system ($\Delta P_a < \Delta P$), as shown in Fig. 3.9a. Consequently, as seen from Fig. 3.9b, the control center operator will perform only one shedding step with a lower amount of load, whereas two shedding steps are needed. The highlighted shedding step is the one prompted by the attack. As can be seen, the attack causes the system frequency to keep falling, thus forcing the under-frequency control in the generators to shut down and cause a system-wide blackout.

Scenario 4: In this scenario, it is assumed that the attacker is able to manipulate the generator G6 frequency by adding a signal that has a slope $m_6 = -0.05$. This causes the calculated magnitude of disturbance ΔP to be 0.7 pu, which is higher than the actual disturbance in the system ($\Delta P_a > \Delta P$), as shown in Fig. 3.10a. Hence, the decision of the control center is to shed an amount of load that is higher than necessary. The highlighted



(a) Real and manipulated center of inertia frequency

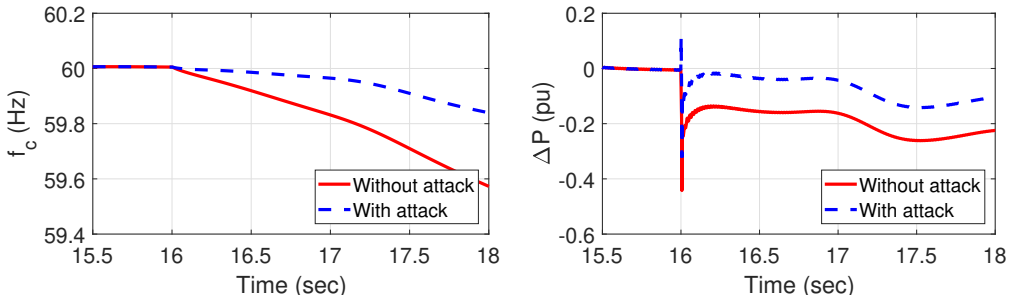


(b) Real and manipulated amount of disturbance

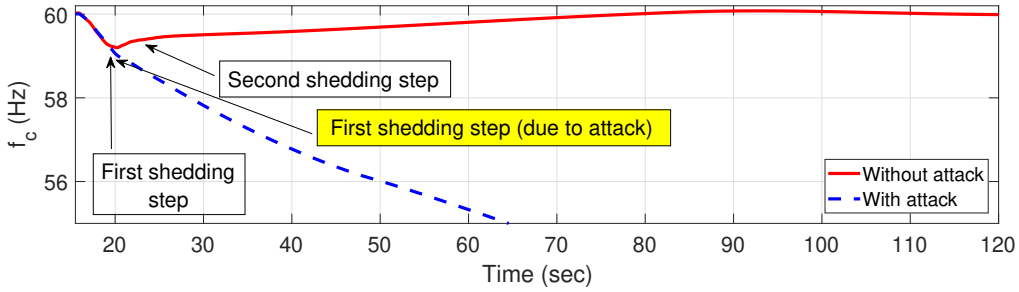
Figure 3.8: Targeting higher amount of load shedding

shedding steps in Fig. 3.10b are executed due to the attack. Consequently, as shown in the same figure, over-frequency occurs for a long period of time, which might cause damage to system equipment.

In the scenarios described above, the attacker injects a small attack signal, which does not affect the magnitude of the frequency (i.e., it bypasses the bad data detection) but does affect the ROCOF. In other words, the attacker can control how the frequency signals change. As a result, the attacker can control the slope of the frequency signal as well as the magnitude of disturbance. Ultimately, the attacker has full control of the amount of load to be shed.



(a) Real and manipulated center of inertia frequency frequency



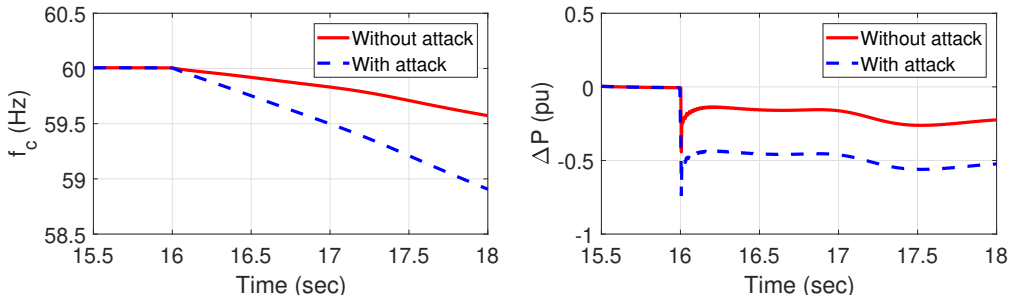
(b) Real and manipulated amount of disturbance

Figure 3.9: Targeting lower amounts of load shedding

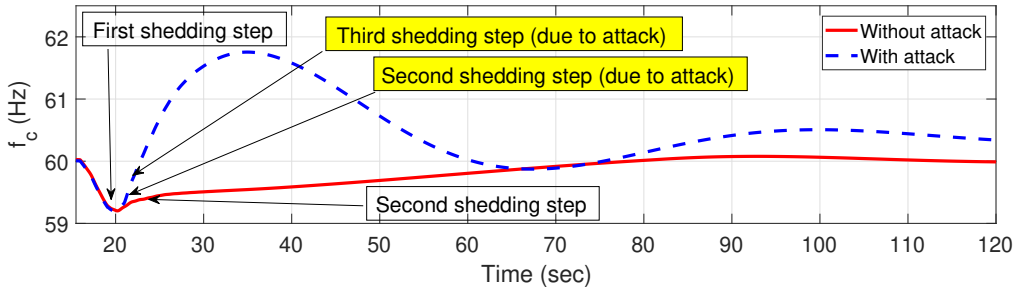
B. Targeting Load Shedding Distribution

Following a disturbance that requires load shedding of 1000 MW in the IEEE 39 bus system, the subset of buses that have the highest voltage dips are: $\{39, 9, 8, 7, 1\}$. As bus 9 and 1 have no load to shed, the distribution process can only take place on buses 39, 8, and 7, following (3.31), as shown in Table 3.2, where i is the bus number, $V_{pd,i}$ is the pre-disturbance voltage magnitude at bus i, and $V_{d,i}$ is the disturbance voltage magnitude at bus i. In the following two scenarios, the attacker has nothing to do with the magnitude of frequency disturbance, i.e., the attacker does not attack the frequency measurements. Instead, FDI attacks take place on the power flow measurements to alter voltage magnitudes, as they represent the main variable in the load shedding process.

Scenario 5: This scenario features an attack scenario of maliciously changing the



(a) Real and manipulated system frequency and magnitude of disturbance



(b) UFLS with and without attack

Figure 3.10: Targeting higher amounts of load shedding

amount of load shedding $P_{shed,i}$, calculated from (3.31) on bus j, by varying the disturbance voltage values of the shedding buses. Figure 3.11 depicts the effects of an FDI attack on shedding distribution, while Table 3.3 demonstrates the change of load shedding distribution following the attack.

Scenario 6: An alternative scenario aims to deceive the system operator in order to shed loads from healthy sensitive locations. The attacker targets the disturbance voltage at a specific bus to give the appearance of negligible voltage dips. Meanwhile, the attacker misleadingly shows a different subset of buses that have high voltage dips. In response, the control system operator applies the load shedding at the new subset of buses.

This scenario can be demonstrated in two parallel steps: (1) The attacker manipulates the power flow measurements to increase the voltages at bus subsets $\{39, 8, 7\}$, as shown in Table 3.4. (2) The attacker manipulates the measurements such that the control system

Table 3.2: No attack load shedding distribution

Bus i	$V_{pd,i}$ **(pu)**	$V_{d,i}$ **(pu)**	ΔV_i **(pu)**	$P_{shed,i}$ **(MW)**
39	1.004328	0.858811	0.145517	500
8	0.983386	0.895909	0.087477	276
7	0.984816	0.900548	0.084268	233

Table 3.3: Attacks targeting load shedding distribution

Bus i	$V_{pd,i}$ **(pu)**	$V_{d,i}$ **(pu)**	ΔV_i **(pu)**	$P_{shed,i}$ **(MW)**
39	1.004328	0.804011	0.200317	545
8	0.983386	0.899909	0.083477	227
7	0.984816	0.900548	0.084268	229

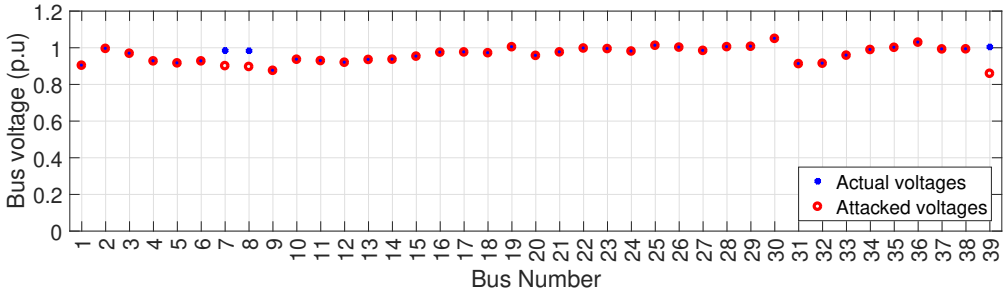


Figure 3.11: Changing the shedding order

operator sees the voltages at bus subsets $\{23, 25, 26, 28, 29\}$ as if they have the highest voltage dip, as shown in Fig. 3.12. As a result, the control center operator sheds the total load of the latter (step 2) set of buses instead of the former (step 1). Consequently, by applying this attack scenario, the attacker is able to misguide the control system operator to shed some sensitive loads that may cause substantial financial losses.

In the above scenarios, even though the attacker has no access to the frequency measurements, they are still able to manipulate power flow measurements and control shedding distribution by changing the buses' voltage values.

Table 3.4: Targeting shedding locations

Bus i	$V_{pd,i}$ **(pu)**	$V_{d,i}$ **(pu)**	ΔV_i **(pu)**	$P_{shed,i}$ **(MW)**
39	1.004328	1.003001	0.001327	Zero
8	0.983386	0.970087	0.013298	Zero
7	0.984816	0.982816	0.002	Zero

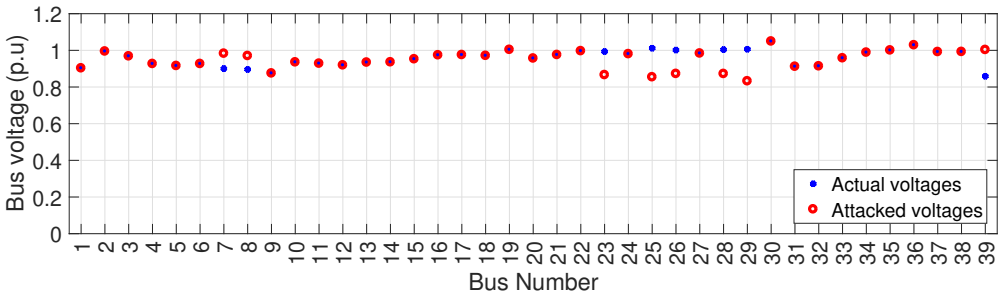


Figure 3.12: Changing the shedding buses locations

C. Faking Underfrequency Conditions

Scenario 7: In this scenario, the attacker's objective is to falsify the voltage profile perceived by the system operator in order to match the expected behaviour of voltage variations. First, the attacker simulates a disturbance and considers the voltage deviations across all buses. Second, the attacker calculates the deviation index D_i from (3.38) and compares it with the pre-determined threshold γ in order to define the attack bus's subset Ω_a. Figure 3.13 shows the number of buses which have a specific voltage variation threshold γ for three test cases of 0.05, 0.08, and 0.125 p.u. For each γ, bus $i \in \Omega_a$ if $D_i \geq \Delta V$. Table C.2 shows three cases of defined thresholds γ in p.u. voltages. For a threshold of 0.05 p.u., bus 34 exceeds the threshold in voltage variation, while only three buses exceed the threshold for 0.125 p.u. For each case, a bus i is selected that belongs to the subset Ω_a and a bus j if it doesn't belong. Figure 3.14 depicts case 3. The first graph shows bus 18, which belongs to subset Ω_a, as D_{18} exceeds the threshold of 0.125. On the other

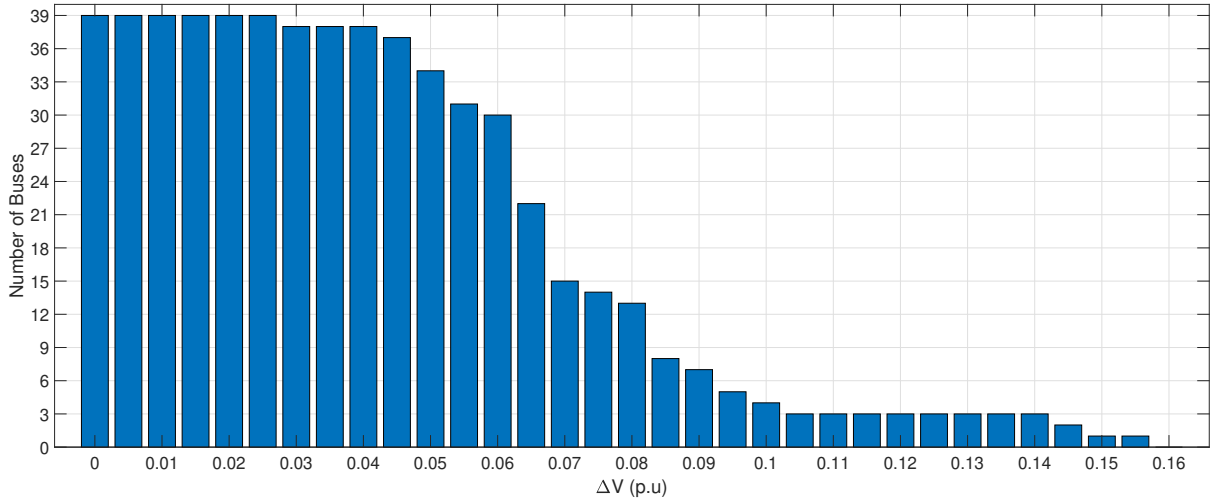


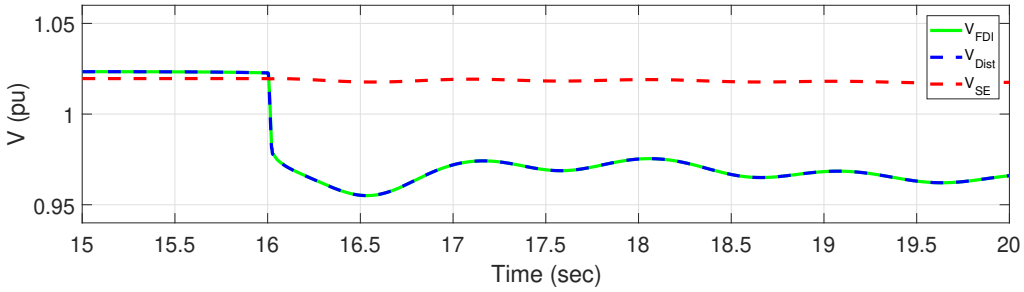
Figure 3.13: Number of buses $\in \Omega_a$ as function of threshold variation

Table 3.5: γ in p.u voltages

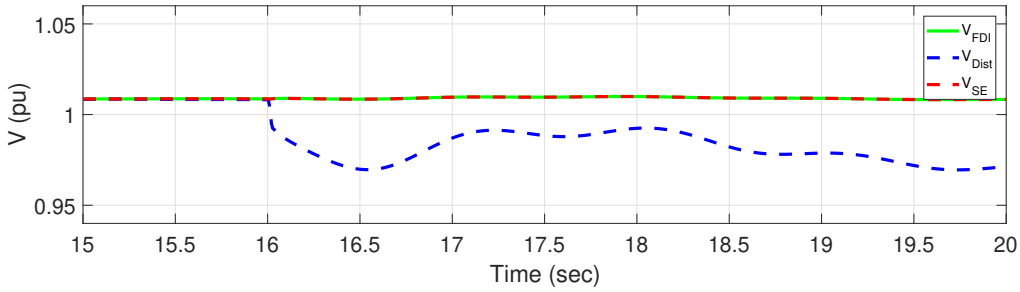
Case #	γ **(p.u)**	**size** Ω_a	**Bus** i	**Bus** j	**max** ΔV **bus** i **(p.u)**	**max** ΔV **bus** j **(p.u)**
1	0.05	34	18	34	0.0627	0.0389
2	0.08	13	6	17	0.1148	0.0586
3	0.125	3	9	13	0.1464	0.0985

side, D_{34} does not exceed the threshold, therefore the received voltage of that bus matches the results from the state estimation process. Similarly, Fig. 3.15 and Fig.3.16 show the difference in voltage profile for the buses pairs 6,17 and 9,13 to compare the voltage profile for a bus that belongs to Ω_a (6,9), and buses that do not (17,13).

Scenario 8: Following the same approach of manipulating both frequency and power flow measurements, the attacker can mask a real disturbance that occurs in the system. In this scenario, individual frequency values are falsified by adding $(60 - f_i)$ to the frequency signals, such that the control center perceives all frequency values closely around the corresponding optimal value. This is demonstrated in Fig. 3.18, where the faked fre-



(a) Alteration of Bus 18 to match disturbance voltage profile



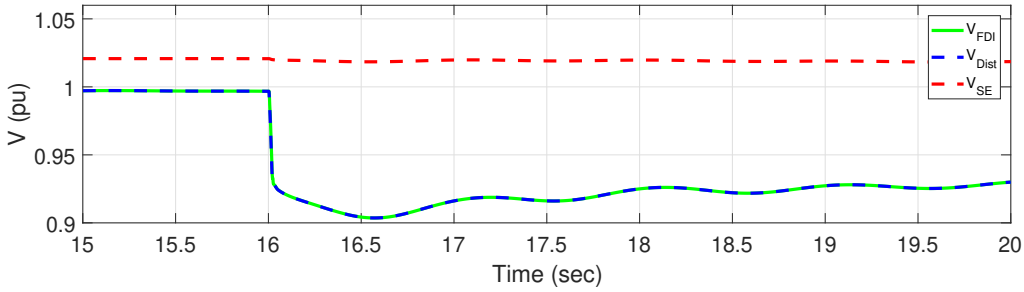
(b) Un-attacked bus 34 voltage profile matches state estimation

Figure 3.14: Voltage profile for Buses in attack subset

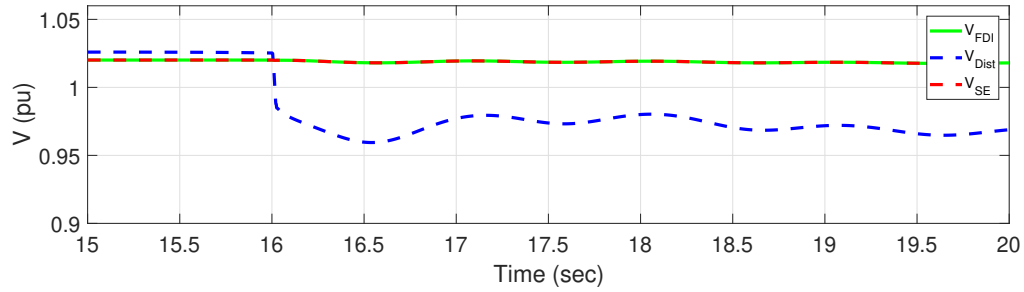
quency measurements show the system frequency to be around 60 Hz, whereas in reality the frequency is dropping.

3.5 Summary

FDI attacks represent a real challenge to the cyber-physical security of modern WAMPAC schemes. In this chapter, it was shown that an attacker can launch a cyber attack on a power system during its steady-state and/or small/large disturbance conditions. The attacker can target the operation of the AGC during small dynamics in the power system or the operation of WAUFLS schemes during large disturbances. Simulations on practical systems were done to prove the severity of this problem. In the following chapters, detection and mitigation techniques are proposed to address these serious issues and fill the



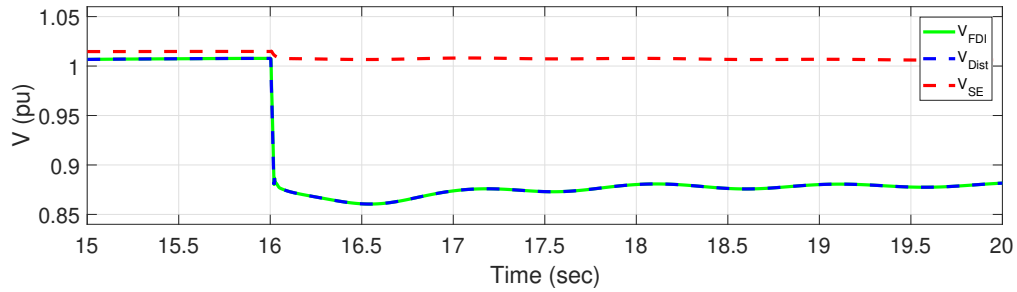
(a) Alteration of Bus 6 to match disturbance voltage profile



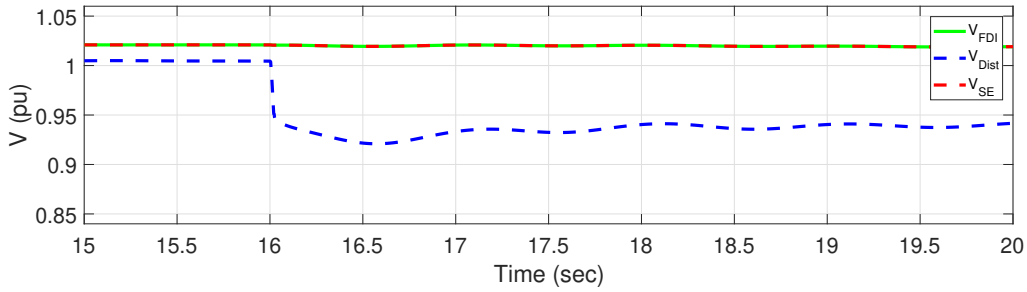
(b) Un-attacked bus 17 voltage profile matches state estimation

Figure 3.15: Voltage profile for Buses in attack subset

gaps in the literature that were mentioned in Chapter 2.



(a) Bus $9 \in \Omega_a$ and attacked (perceived) voltage (V_{FDI}) matches disturbance voltage (V_{Dist})



(b) Bus $13 \notin \Omega_a$ and attacked (perceived) voltage (V_{FDI}) matches state estimation voltage (V_{SE})

Figure 3.16: Voltage profile for Buses in attack subset

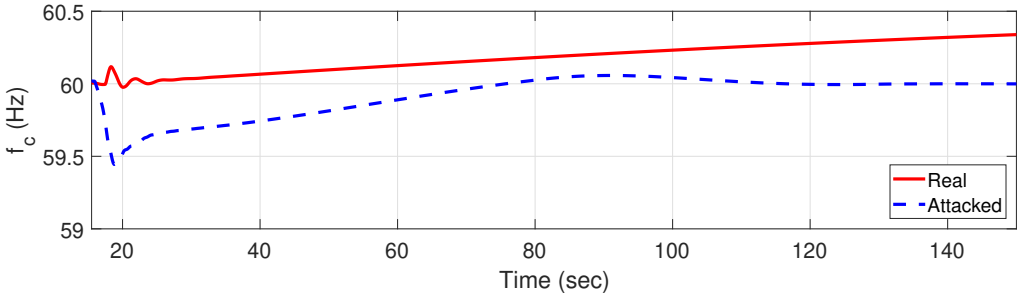


Figure 3.17: System frequency response after faking the disturbance

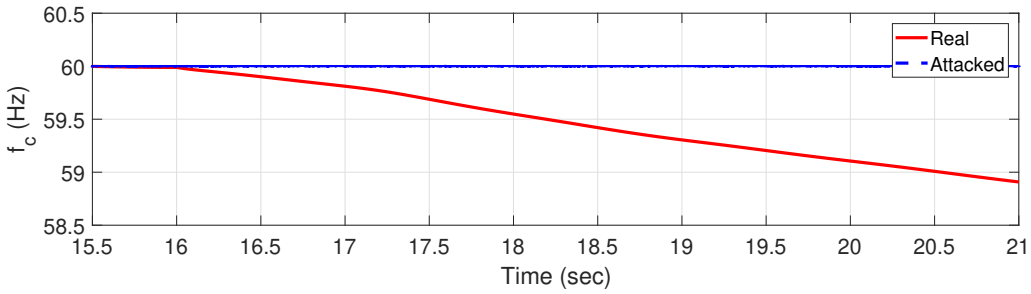


Figure 3.18: Hiding the actual status of the system

Chapter 4

Detection and Mitigation of False Data Injection (FDI) in AGC Systems Considering a Linear Model

The ability to maintain the system frequency within its specified operating limits is crucial for the stability and proper operation of power systems. Any deviation out of the permissible frequency range must be well-mitigated by the AGC system, as otherwise it may result in disruption of operations and/or damage to the power grid equipment. The data required by the AGC control system are sent to the control center through communication links, which are susceptible to cyber attacks. Therefore, such AGC systems have to be well-protected against FDI attacks.

Since mitigation against FDI attacks on AGC systems has been barely touched in the literature, and the existing techniques do not provide formal proof of system stability after incorporating the attack mitigation, this chapter focuses on these concerns. In the chapter, a Kalman filter-based method is used to detect FDI attacks on AGC systems. In addition, the use of a simultaneous input and state estimation-based algorithm to detect and concurrently compensate for FDI attacks against AGC systems is investigated. Formal proofs for the stability of the system after incorporating the attack mitigation scheme and

the unbiasedness of the estimated signals are discussed in detail. Note that this chapter considers the linear model of the AGC system, while the nonlinearities are considered in Chapter 5.

4.1 Detection of FDI Attacks Using a Kalman Filter

One method for detecting attacks in a system is to compare the behavior of that system with another identical one that is not under attack. Naturally, this approach is not feasible in power systems. An alternative method is to analyze the behavior of the system over time using a mathematical model which predicts how the system is supposed to behave under no attack. The estimated observations are then compared with the ones obtained from the actual sensor readings. A significant deviation between them would indicate the presence of an attack. This approach is known as analytical redundancy. Kalman filtering [55, 56, 78] is an algorithm that produces accurate estimates of unknown variables using a series of measurements (possibly noisy) observed over time.

4.1.1 Principle of Operation

In order to estimate the states of the system, the following observation equation is considered: [120, 121]

$$y_k = Cx_k + v_k, \tag{4.1}$$

where v_k denotes the measurement's noise. The iterations of the Kalman filter can be written as:

$$\widehat{x}_{k+1|k} = A\widehat{x}_k + Bu_k \tag{4.2}$$
$$P_{k|k-1} = AP_{k-1}A^T + Q \tag{4.3}$$
$$K_k = P_{k|k-1}C_k^T(C_kP_{k|k-1}C_k^T + R)^{-1} \tag{4.4}$$
$$P_{k|k} = P_{k|k-1} - K_kC_kP_{k|k-1} \tag{4.5}$$
$$\widehat{x}_k = \widehat{x}_{k|k-1} + K_k(y_k - C_k\widehat{x}_{k|k-1}) \tag{4.6}$$

The Kalman gain converges in few steps, where the Kalman filter equation can be updated as:

$$\widehat{x}_{k+1} = A\widehat{x}_k + Bu_k + K[y_{k+1} - C(A\widehat{x}_k + Bu_k)] \tag{4.7}$$

where $P \triangleq \lim_{k\to\infty} P_{k|k-1}$ and $K = PC^\top(CPC^\top + R)^{-1}$. Then, the residual r_{k+1} at time $k+1$ is defined as:

$$r_{k+1} \triangleq y_{k+1} - C(A\widehat{x}_k + Bu_k) \tag{4.8}$$

One way to detect the attacks is to calculate the Mahalanobis norm of the residual vector g_k as:

$$g_k = r_k \times \Phi \times r_k^\top \tag{4.9}$$

where Φ denotes the covariance matrix of r_k. Then, the detector compares g_k with a predefined threshold which is chosen based on the historical values of g_k without an attack.

In a stateful test, an additional statistic S_k, which keeps track of the historical changes of r_k (no matter how small it is), is calculated. An alert is generated if $S_k \geq \tau$, i.e., if there is a persistent deviation across multiple time-steps. Many tests can keep track of the historical behavior of the residual r_k, such as taking an average over a time window, an exponential weighted moving average Exponential Weighted Moving Average (EWMA),

or using change detection statistics like the non-parametric CUmulative SUM (CUSUM) statistic.

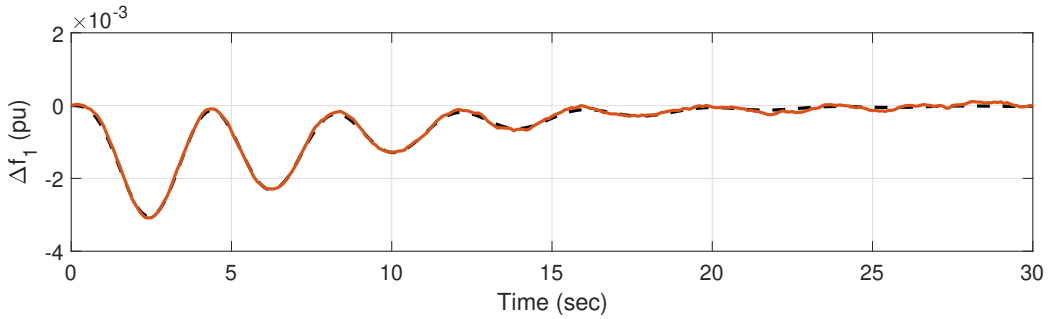
In this work, the applicability of these stateful approaches is illustrated by using a non-parametric CUSUM, which is basically a sum of the residuals. In this case, the CUSUM statistic is defined recursively as $S_0 = 0$ and $S_{k+1} = (S_k + |r_k| - \delta)^+$, where $|x|^+$ represents $\max(0, x)$ and δ is selected so that the expected value of $|r_k - \delta| < 0$ when there is no attack. An alert is generated whenever the statistic is greater than a previously defined threshold $S_k\tau$ and the test is restarted with $S_{k+1} = 0$ [122, 123]. In other words, in each iteration, the most recent m values of the residual is used to calculate the moving average of the accumulating residual. Compared to other approaches that use the value of the residual itself, this approach improves the speed of attack detection, especially for cases where the effect of the attack takes place gradually, e.g., for (small slope) ramp attacks.

4.1.2 Simulation Results

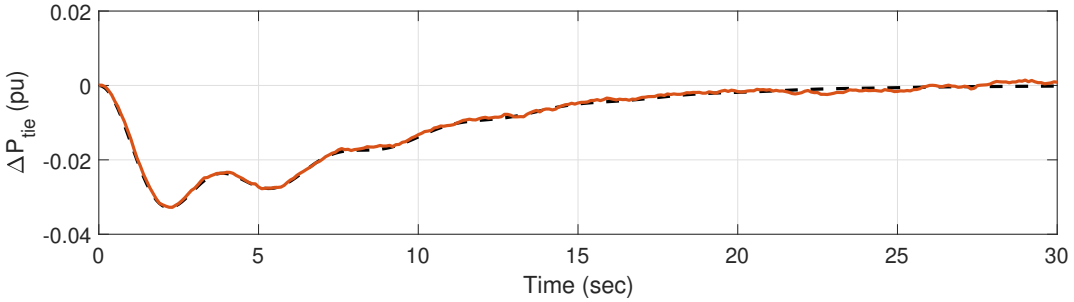
In practice, the covariance matrices for the process noise and the measurement noise can be determined by performing some actual field measurements from the power system itself. However, for the purpose of our simulations, the components of w_k and v_k are assumed to be independent and identically distributed Gaussian random variables with a zero mean and a standard deviation of $\sigma = 10^{-5}$.

The utilized Kalman filter is tested without any attack to confirm its ability to estimate different state variables accurately. To perform this, a load disturbance of 0.1785 pu at $t = 0$ is applied to Area 1. A sample of the Kalman filter output is depicted in Fig. 4.1, which shows the measured versus estimated values of the frequency deviation in Area 1 as well as the tie-line power flow. The solid lines show the estimated values, while the dashed ones indicate the actual measured ones.

Figure 4.2 shows the Mahalanobis norm g_k and the CUSUM S_k samples of the system with no attacks. As can be seen, the threshold, which is chosen based on the historical



(a) Frequency deviation in Area 1



(b) Tie-line power deviation

Figure 4.1: State estimation under normal operation (no attack)

behavior of the residual values, is higher than the maximum value of these residuals in a case of no attack. In our simulations, it is chosen to be 10^{-5}.

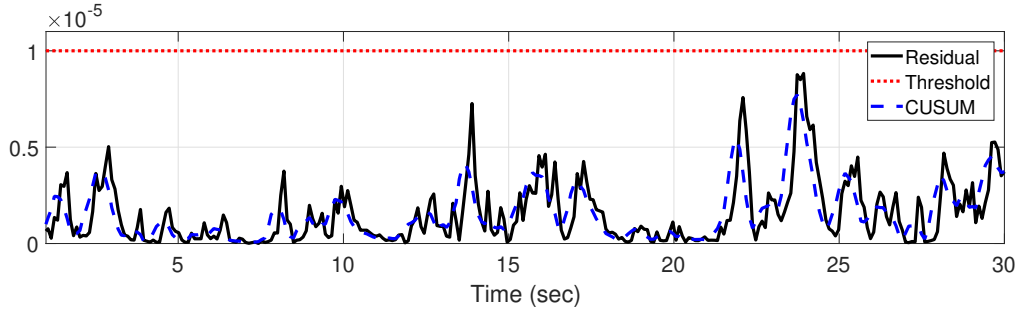
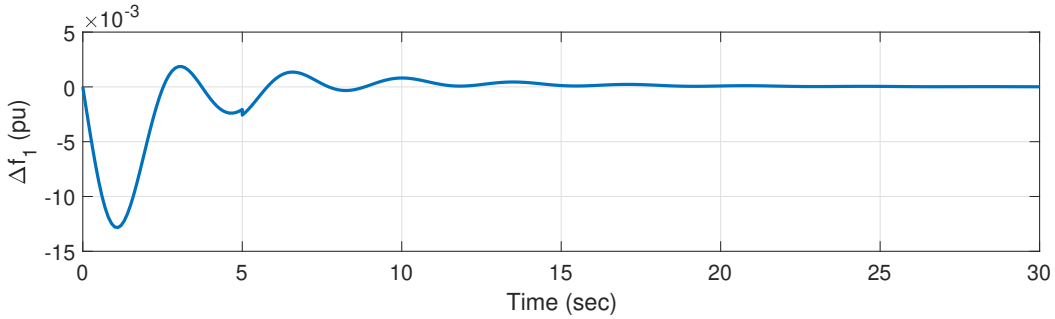


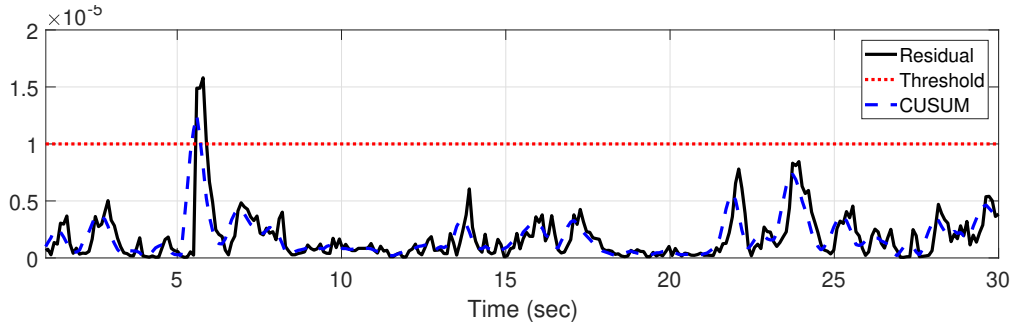
Figure 4.2: Residual of the output with no attack

To confirm the detection capabilities of the proposed solution, different attacks are constructed and applied to the AGC system. These attacks target both measurements and control signals of the AGC system, e.g., frequency deviation signals, tie-line power signals, and ACE signal. A normal load disturbance of 0.1785 pu is applied in Area 1 at $t = 0$ sec. The attacks target both measurements and control signals. In the presented two scenarios, the attacks are applied at $t = 5$ sec.

Scenario 1: A scaling attack with a scaling parameter of 1.25 is applied to the reading of the frequency deviation in Area 1, Δf_1, as shown in Fig. 4.3a. An alarm trigger signal appears at the moment of the attack, as shown in Fig. 4.3b.



(a) Frequency deviation in Area 1

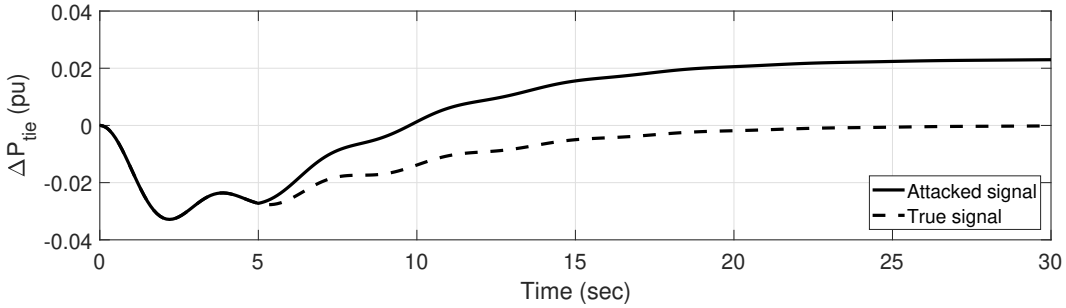


(b) Mahalanobis norm of error vector g_k and CUSUM S_k

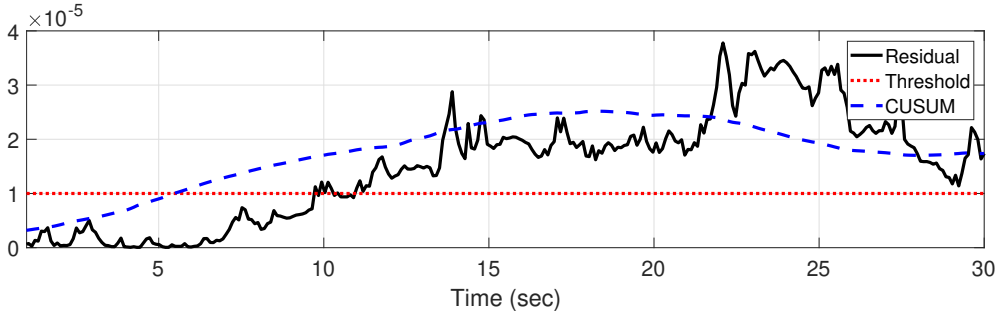
Figure 4.3: Scaling attack on Δf_1

Scenario 2: In this scenario, a ramp signal with a slope of 0.005 is used to manipulate the signal ΔP_{tie}. Figure 4.4a, which also includes the true signal, shows the effect of the attack. As illustrated in Fig. 4.4b, the error residual increases gradually until it hits the

predetermined threshold as an indication of the attack. In this case, the attack is applied at $t = 5$ sec, and the residual norm detector detects it later when the residual value exceeds the threshold value. This is due to the nature of the ramp attack whose effect increases gradually; a ramp attack with a higher slope will be detected faster. The figure also shows how the use of the CUSUM stateful approach improves the detection time in this case.



(a) Tie-line power



(b) Mahalanobis norm of error vector g_k and CUSUM S_k

Figure 4.4: Ramp attack on ΔP_{tie}

4.2 Mitigation Using Joint Input and State Estimation Algorithm

Despite the simplicity of the Kalman Filter solution presented above, in practice, it is not enough to detect the occurrence of FDI attacks. In other words, the attacked sensors

cannot be isolated because the AGC system needs these readings in order to perform its required real-time control operation accurately. To address this deficiency, an input/state estimation-based algorithm [124, 125] is utilized to detect and simultaneously compensate for FDI attacks on AGC systems. The discrete-time linear system with the attack signals can be represented as:

$$x_{k+1} = Ax_k + Bu_k + Gd_k + \omega_k \tag{4.10}$$

$$y_k = Cx_k + Du_k + Hd_k + v_k \tag{4.11}$$

where $x_k \in \mathbb{R}^n$ is the state vector at time k, $u_k \in \mathbb{R}^m$ is the natural system disturbance, $d_k \in \mathbb{R}^p$ is the FDI vector, and $y_k \in \mathbb{R}^l$ is the measurement vector. For the two-area AGC system under consideration, the values of G_c and H_c are:

$$G_c = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ -K_1B_1 & 0 & -K_1 \\ 0 & -K_2B_2 & K_2 \end{bmatrix},$$

$$H_c = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

In this model, the FDI vector is treated as the unknown input. In other words, d_k is fed to the algorithm as an unknown input in order to estimate it. The process noise ω_k and the measurement noise v_k are assumed to be mutually uncorrelated, zero-mean, white Gaussian noise with known covariance matrices, Q_k and R_k, respectively.

4.2.1 Algorithm Description

A three-step recursive filter is used, as shown in Algorithm 1. The three steps are time update, measurement update, and the estimation of the unknown input. In the first step, measurements up to time $k-1$ are given, the next state is predicted using Equation (4.12), and the error in the propagated state estimation and its covariance matrix is calculated. In the second step, the propagated estimate $\widehat{x}_{k|k-1}$ is updated using the measurement y_k, as in Equation (4.13), and the covariance matrix $P^x_{k|k}$ of the updated state estimate error is obtained. Finally, in the last step, the unknown input is estimated, as shown in Equation (4.14).

$$\widehat{x}_{k|k-1} = A\widehat{x}_{k-1|k-1} + Bu_{k-1} + G\widehat{d}_{k-1} \tag{4.12}$$

$$\widehat{x}_{k|k} = \widehat{x}_{k|k-1} + L_k(y_k - C\widehat{x}_{k|k-1}) - Du_k) \tag{4.13}$$

$$\widehat{d}_k = M_k(y_k - C\widehat{x}_{k|k} - Du_k) \tag{4.14}$$

After estimating the FDI, the value of the estimated signal $\widehat{d}_k$ is subtracted from the received one to compensate for the attack and estimate the system state at time k, as shown in Fig. 3.1. This algorithm can be thought of as a generalization of the Kalman filter [125] and can be utilized to simultaneously perform detection, estimation, and compensation in FDI attacks.

4.2.2 Simulation Results

The above algorithm is tested under different attack scenarios. In each of the following scenarios, an attack in the form of a false data injection is applied to one of the communication signals of Δf_1, Δf_2 or ΔP_{tie}. The figures show the actual versus estimated attacks.

Algorithm 1 Unknown Input and State Estimation [124, 125]

Initialize: $\widehat{x}_{0|0} = \mathbb{E}[x_0]$; $\widehat{d}_0 = H^{\dagger}(y_0 - C\widehat{x}_{0|0} - Du_0)$; $P^x_{0|0} = \mathcal{P}^x_0; P^{xd}_0 = \mathcal{P}^{xd}_0; P^d_0 = \mathcal{P}^d_0$;

for $k = 1$ to N **do**

▷ Time update

$\widehat{x}_{k|k-1} = A\widehat{x}_{k-1|k-1} + Bu_{k-1} + G\widehat{d}_{k-1}$;

$P^x_{k|k-1} = AP^x_{k-1|k-1}A^{\top} + GP^{xd\top}_{k-1}A^{\top} + AP^{xd}_{k-1}G^{\top} + GP^d_{k-1}G^{\top} + Q_{k-1}$;

$\tilde{R}_k = CP^x_{k|k-1}C^{\top} + R_k$;

▷ Measurement update

$K_k = P^x_{k|k-1}C^{\top}\tilde{R}^{-1}$;

$L_k = K_k(I - H(H^{\top}\tilde{R}^{-1}_k H)^{-1}H^{\top}\tilde{R}^{-1}_k)$;

$\widehat{x}_{k|k} = \widehat{x}_{k|k-1} + L_k(y_k - C\widehat{x}_{k|k-1}) - Du_k)$;

$P^x_{k|k} = (I - CL_k)P^x_{k|k-1}(I - CL_k)^{\top} + L_kR_kL^{\top}_k$;

▷ Estimation of unknown inputs

$\tilde{R}^{\star}_k = (I - CL_k)\tilde{R}_k(I - CL_k)^{\top}$;

$P^d_k = (H^{\top}\tilde{R}^{\star -1}_k H)^{-1}$;

$M_k = P^d_k H^{\top}\tilde{R}^{\star -1}_k$;

$\widehat{d}_k = M_k(y_k - C\widehat{x}_{k|k} - Du_k)$;

$P^{xd}_k = -P^x_{k|k}C^{\top}M^{\top}_k + L_kR_kM^{\top}_k$;

end for

They also show the true, the manipulated, and the compensated communication sensor readings. The simulation start time is the time of occurrence of the physical disturbance of the system (e.g., load increase/decrease or generator tripping). The duration of the attack is chosen by the attacker in order to drive the AGC system out of control or deceive the control center into making the wrong decision (e.g., trigger under-/over-frequency protection devices without a need to do so).

Recall that the AGC regulates grid frequency by adjusting the set-points of a power plant's governors. To calculate these set-points, the control center receives sensor readings,

i.e., frequency and tie-line power measurements from different areas. It is impossible to exhaust all FDI injection patterns. Throughout our work, the FDI attack signal is modeled as an additive signal which is added to the sensor readings. While this additive signal can be of any value, throughout the literature, ramp, pulse and step attack signals are usually used [80] to test different attack scenarios, as they model slowly varying attacks, attacks of short duration, and attacks that aim to cause a sudden variation in the system. Furthermore, stealthy attacks also have to satisfy the constraints imposed by equations (1) and (2).

Scenario 1: In this scenario, under steady-state conditions, i.e., with no system load disturbance, a pulse signal that has a magnitude of 0.002 is used to manipulate the frequency deviation in Area 1, Δf_1, as shown in Fig. 4.5. Figure 4.5a shows the actual and estimated attacks. Figures 4.5b, 4.5c and 4.5d show the true, attacked, and compensated signals for Δf_1, Δf_2 and ΔP_{tie}, respectively. As depicted in Fig. 4.5c, the system operator sees the frequency at Area 2 lower than its actual value. This may drive the system operator to use the UFLS schemes, if the frequency comes below a specific value, which may result in shedding loads when there is no need to do so.

Scenario 2: Under a system disturbance of 0.2 pu at Area 1, a step attack is applied to the signal Δf_1 starting at $t = 10$ sec. The magnitude of the step is 0.003. Figure 4.6a shows that the attack is well-estimated with reasonable accuracy. The other sub-figures of Fig. 4.6 show the true, attacked, and mitigated system signals.

Scenario 3: A system disturbance of 0.2 pu is applied to Area 1 at $t = 0$ sec. At the same time, a ramp attack with a slope of 0.0001 is applied to the signal Δf_2. Figure 4.7 shows the attack estimation as well as the system performance with and without compensated measurements.

Scenario 4: At $t = 0$ sec, a system disturbance of 0.15 pu takes place at Area 2. At $t = 10$ sec, a step signal with a magnitude of -0.02 is used to manipulate the value of ΔP_{tie}. Figure 4.8 shows the attack estimation as well as the system performance with and without compensated measurements.

Scenario 5: In this scenario, a case where the attacker targets more than one signal

in the communication system is considered. At $t = 0$ sec, a system disturbance of -0.2 pu takes place at Area 2. At the same time, a ramp attack with a slope of 0.0001 is applied to Δf_1. At $t = 10$ sec, a pulse signal with a magnitude of 0.01 is used to manipulate the value of ΔP_{tie}. Figure 4.9 shows the simulation results corresponding to this scenario.

To address the applicability of the proposed approach to real-world scenarios, the proposed algorithm is also simulated under different types of attacks in a 12-bus, four-area system with multi-generator units in each area. The 12-bus model utilized in this study is practical and comes from North America, representing the Manitoba Chicago network. (See Fig. 4.10). The data for this system is taken from [126, 127] and is summarized in Table A.2.

Scenario 6: To show the effect of FDI injections at transient conditions, a pulse attack with a magnitude of 0.003 is injected to the signal of the frequency deviation in Area 4, Δf_4 at $t = 15$ sec, when the system is under a natural system disturbance of 0.2 pu at Area 2. Figure 4.11 shows the attack estimation and mitigation as well as its effect on the attacked signal.

Scenario 7: Figure 4.12 shows a scenario where a ramp attack that starts at $t = 15$ sec with a rising slope of 0.0005 is used to manipulate the signal ΔP_{tie13}. The FDI takes place under a system disturbance of 0.15 pu at Area 3.

Scenario 8: In this scenario, the attacker manipulates both Δf_1 and ΔP_{tie34}. The attacker injects a ramp signal with a slope of 0.0002 at $t = 0$ sec to Δf_1. Then, at $t = 15$ sec, the attacker injects a step signal with a magnitude of 0.03 to ΔP_{tie34}. Figure 4.13 shows the attack's estimation and mitigation in different system signals.

All of the above-presented simulation results confirm the effectiveness of the proposed approach in estimating the value of the injected attack signals under different operating conditions and attack scenarios and successfully compensating for it so that the AGC system can continue its normal operation.

4.3 Sensitivity Analysis of the Mitigation Technique

4.3.1 Impact of Noise

To illustrate the impact of the sensor noise, Fig. 4.14 shows Scenario 7 with a higher value for the sensor noise, $\sigma = 10^{-2.5}$. As can be seen, the proposed algorithm is capable of mitigating the attack even in the presence of this relatively high sensor noise.

4.3.2 Estimation Accuracy

The accuracy of the estimation is guaranteed through the use of the utilized optimal filter (see Theorems 2, 3 below). On the other hand, if the estimation accuracy is impacted because of any unforeseen reason in practice, this inaccuracy would then lead to some degradation in the system performance. To illustrate this, a hypothetical form of Scenario 7 is simulated (see Fig. 4.15) to show the behavior of the system under an inaccurate estimation process. The inaccuracy is modeled by adding independent and identically distributed Gaussian random noise with zero mean and a standard deviation of 10^{-5} and $10^{-3.5}$ to each component of the estimated state $\widehat{x}$ and estimated attack signal $\widehat{d}$, respectively.

Another scenario that shows how the controller may make a wrong decision is the case where the model used in the state/attack estimation algorithm (Algorithm 1) is not accurate. This inaccuracy was simulated by uniformly perturbing the elements of the matrices A_c and B_c. We do so by multiplying each element of these matrices by $1+r$, where $r \in [-\epsilon, +\epsilon]$ is a uniformly distributed random variable and ϵ denotes the perturbation percentage. In practice, this might occur if there is an error in the process modeling or in the linearizion of the original model. Figure 4.16 shows the system response under a ramp attack for a model perturbation $\epsilon = 20\%$. As illustrated by the figure, there is a deviation between the actual attack signal and the estimated one. This affects the mitigation process, in that the control center may initiate the UFLS protection scheme at $t = 205$ sec when the estimated value for the mitigated frequency f_4 reaches 59.7 Hz.

4.4 Features of Proposed Mitigation Technique

It should be noted that the sufficient conditions required for the boundedness of the error covariance of the used input and state estimator and its exponential stability are satisfied for the systems considered throughout our work. By invoking the separation principle [128], this also implies the stability of the overall system. More precisely, the following properties have been verified for the considered two-area and four-area AGC system models.

4.4.1 Strong Detectability

A linear time-invariant discrete-time system is strongly detectable if and only if:

$$rankP(z) := rank \begin{bmatrix} zI - A & -G \\ C & H \end{bmatrix} = n + p, \forall z \in \mathbb{C}, |z| \geq 1 \tag{4.15}$$

The exponential stability of the filter is directly related to the strong detectability of the time-varying system, without which unbiased state and input estimates cannot be obtained, even in the absence of stochastic noise [125]. The considered AGC models are confirmed to be strongly detectable by verifying that the above condition holds. Note that the above condition is equivalent to the system being minimum-phase (i.e., the invariant zeros of P(z) are stable).

4.4.2 Exponential Stability

Algorithm 1 can be considered as a special case of the algorithm presented in [125]. In the general case considered in [125], no assumption is made on H to be either a zero matrix (no direct feedthrough) or to have full column rank when there is direct feedthrough. Consequently, when $rank(H) = p_H \leq p$, using singular value decomposition, H can be written as:

$$H = \begin{bmatrix} U_1 & U_2 \end{bmatrix} \begin{bmatrix} \Sigma & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} V_1^\top \\ V_2^\top \end{bmatrix} \tag{4.16}$$

where $\Sigma \in \mathbb{R}^{P_H \times P_H}$ is a diagonal matrix of full rank, $U_1 \in \mathbb{R}^{l \times P_H}$, $U_2 \in \mathbb{R}^{l \times (l-P_H)}$, $V_1 \in \mathbb{R}^{P \times P_H}$ and $V_2 \in \mathbb{R}^{P \times (P-P_H)}$. In that case, the following theorem applies.

Theorem 1 *[125]: For a linear time-invariant system, if ($\tilde{A}$, $\tilde{Q}^{0.5}$) is stabilizable, Algorithm 1 in [125] is exponentially stable, i.e., the expected estimate errors decay exponentially.*

In the above theorem, $\tilde{A}$ and $\tilde{Q}$ are defined (using the notation introduced in [125]) as:

$$\begin{aligned} \tilde{A} &= (I - G_2 \tilde{M}_2 C_2)\widehat{A} + G_2 \tilde{M}_2 C_2 \\ \tilde{Q} &= (I - G_2 \tilde{M}_2 C_2)\widehat{Q} + G_2 \tilde{M}_2 C_2 \end{aligned} \tag{4.17}$$

where

$$\begin{aligned} \widehat{A} &= A - G_1 M_1 C_1 \\ \widehat{Q} &= Q + G_1 \Sigma^{-1} R_1 \Sigma^{-1\top} G_1^\top \\ G_1 &= G V_1 \\ C_1 &= [I_p - U_1^\top R U_2 (U_1^\top R U_2)^{-1}] C \\ M_1 &= \Sigma^{-1} \\ G_2 &= G V_2 \\ C_2 &= I_{(l-P_H)} U_2^\top C \\ \tilde{M}_2 &= (C_2 G_2)^\dagger \end{aligned} \tag{4.18}$$

In our case, the direct feedback matrix H is a full-rank matrix. Thus, H can be rewritten as:

$$H = U \Sigma V^\top \tag{4.19}$$

where $\Sigma \in \mathbb{R}^{p \times p}$. In other words, the matrices U_2 and V_2 vanish, and consequently all the corresponding matrices C_2, G_2, and $\tilde{M}_2$ also vanish, i.e., these matrices will correspond to

empty matrices (an empty matrix is one in which the number of rows or columns [or both] is zero). By substituting into (4.17), it follows that:

$$\begin{aligned} \tilde{A} &= \widehat{A} \\ \tilde{Q} &= \widehat{Q} \end{aligned} \tag{4.20}$$

Thus, for the particular case where $rank(H) = p$, which corresponds to our case, the following corollary applies:

Corollary 1 *If $(\widehat{A},\ \widehat{Q}^{0.5})$ is stabilizable, Algorithm 1 is exponentially stable, i.e., the expected estimate errors decay exponentially.*

4.4.3 Unbiasedness

Using the notation in Algorithm 1, the following theorems, from [124], show the condition for Algorithm 1 to provide the unbiased estimation of both the state and the input of the system.

Theorem 2 *[124]: The minimum-variance unbiased state estimator is obtained with the gain matrix L_k given by:*

$$L_k = P^x_{k|k-1} C^\top \tilde{R}^{-1} (I - H(H^\top \tilde{R}_k^{-1} H)^{-1} H^\top \tilde{R}_k^{-1} \tag{4.21}$$

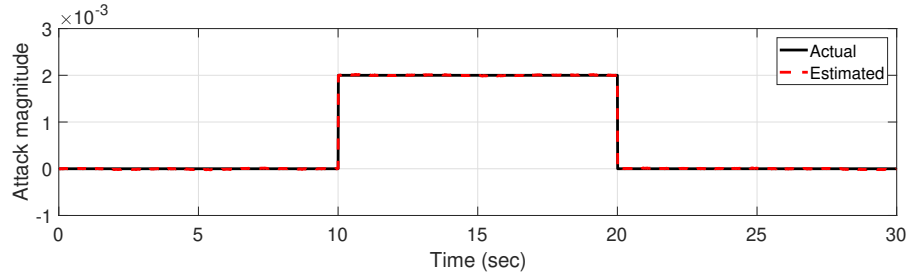
where $\tilde{R}_k := C P^x_{k|k-1} C^\top + R_k$, if and only if $(H^\top \tilde{R}_k^{-1} H)$ is nonsingular, i.e. $rank(H) = p$.

Theorem 3 *[124]: Let $\widehat{x}_{k|k}$ be unbiased, then the input estimate given by line 13 in Algorithm 1, is unbiased if and only if $M_k H = I$, and consequently, $rank(H) = p$.*

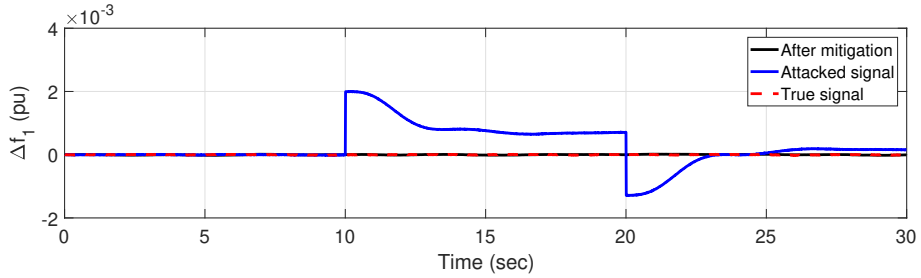
It follows that the condition $rank(H) = p$, which is satisfied in our case, is a necessary and sufficient condition to guarantee the unbiasedness of the unknown input and state estimate.

4.5 Summary

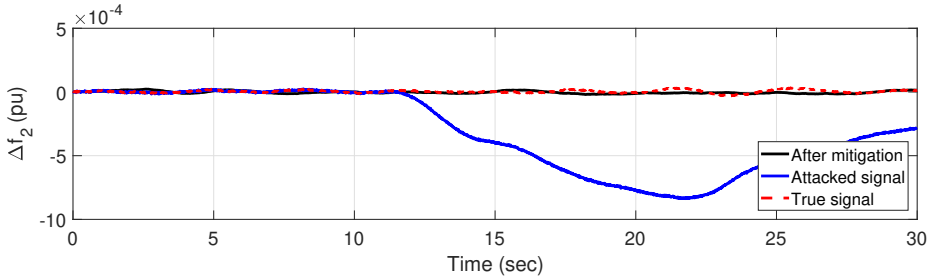
In this chapter, an approach to detect FDI attacks on AGC systems was proposed. Because detection of FDI only is not enough, another approach that jointly detects, estimates, and compensates for FDI attacks against AGC systems was presented. The utilized input/state estimation-based algorithm considered the FDI as unknown input and estimated its value accordingly. The estimated values for the FDI were then used to compensate for the effect of the attack in real time so that the AGC system could continue its operation under attack until the main reasons for the attack could be eliminated. The simulation results for two-area and four-area practical systems confirmed the effectiveness of the proposed approach against different forms of FDI attacks. It should be noted that such an analytical redundancy solution is not meant to replace cyber-based intrusion detection systems, and that it should be thought of as a solution which provides another layer of defense against FDI attacks on AGC systems. One should also note that the proposed approach is generic enough to be applied to mitigate FDI attacks in other smart grid security applications.



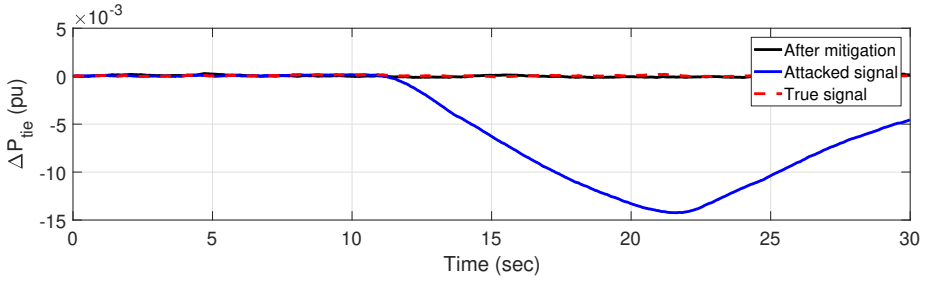
(a) Pulse attack with a magnitude of 0.002



(b) Frequency deviation at Area 1

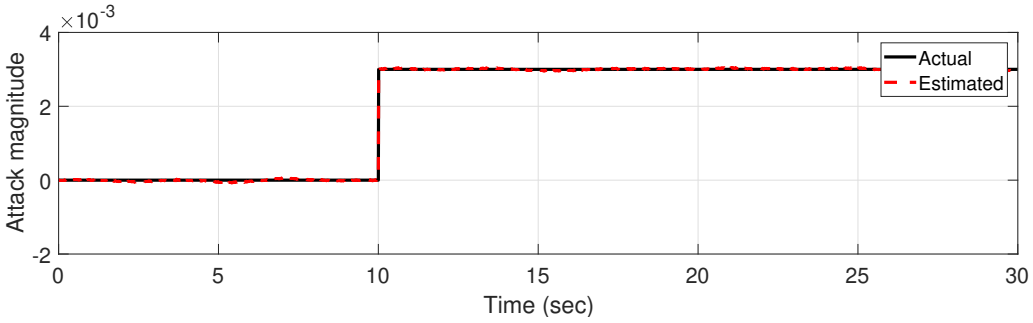


(c) Frequency deviation at Area 2

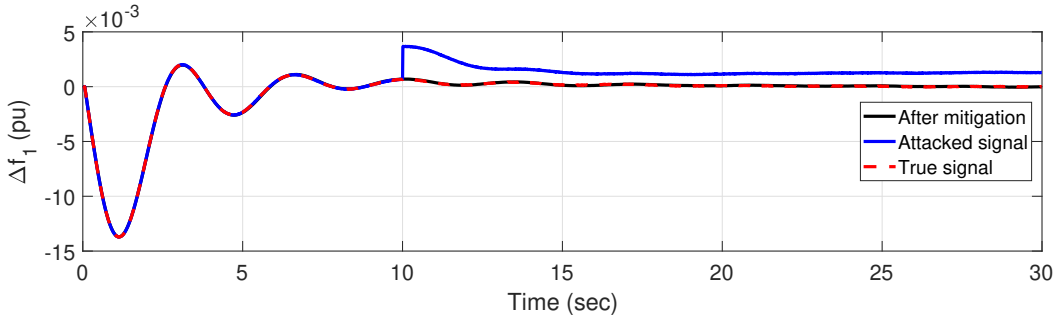


(d) Tie-line power

Figure 4.5: Pulse attack at steady-state condition

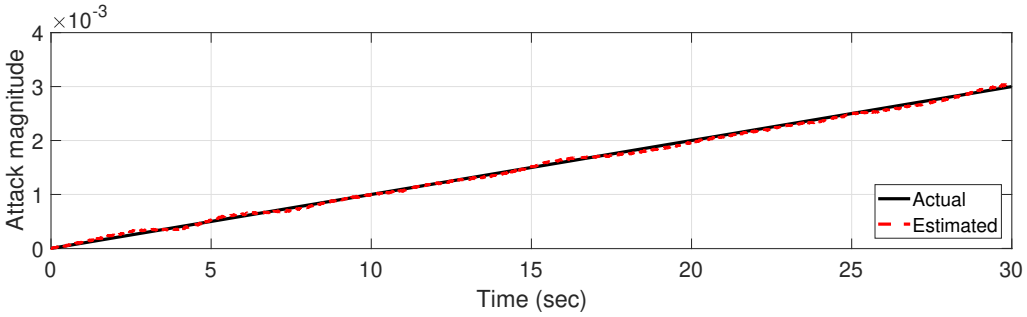


(a) Step attack with a magnitude of 0.001

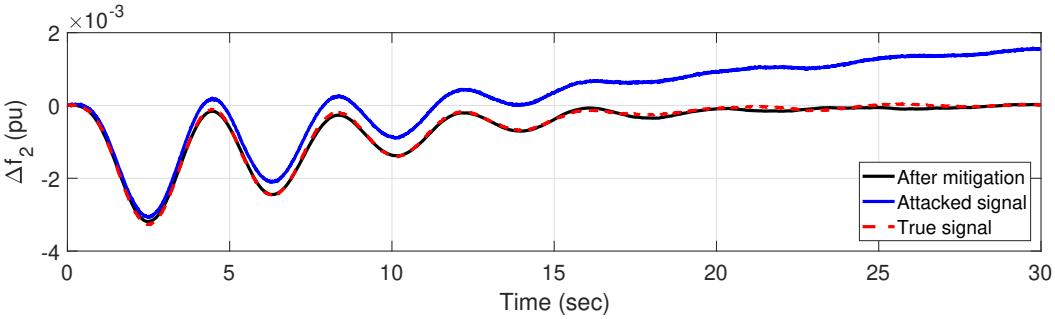


(b) Frequency deviation at Area 1

Figure 4.6: Step attack at system disturbance condition

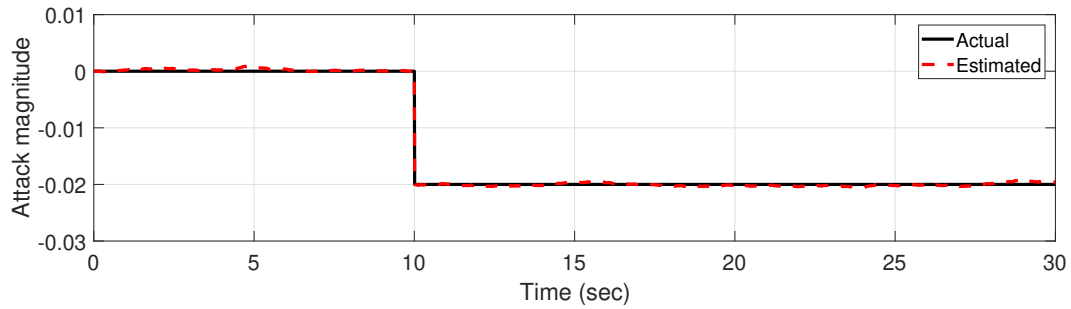


(a) Ramp attack with a slope of 0.001

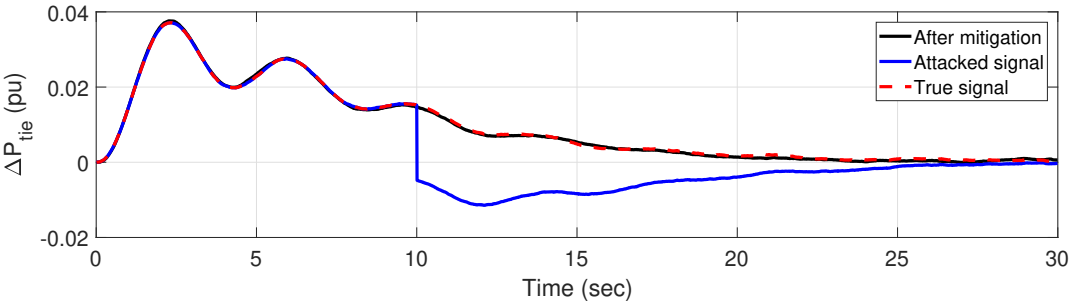


(b) Frequency deviation at Area 2

Figure 4.7: Ramp attack at system disturbance condition

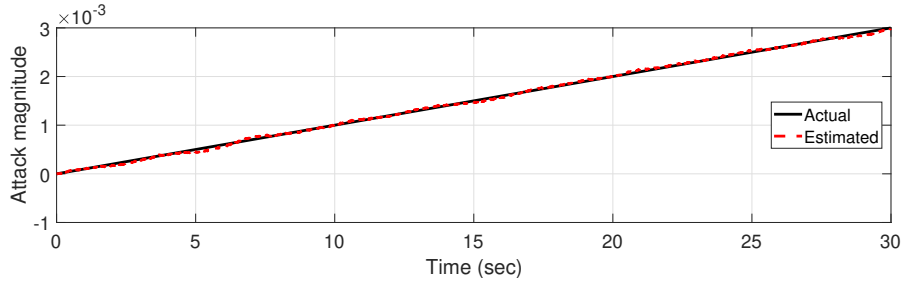


(a) Step attack with a magnitude of -0.02

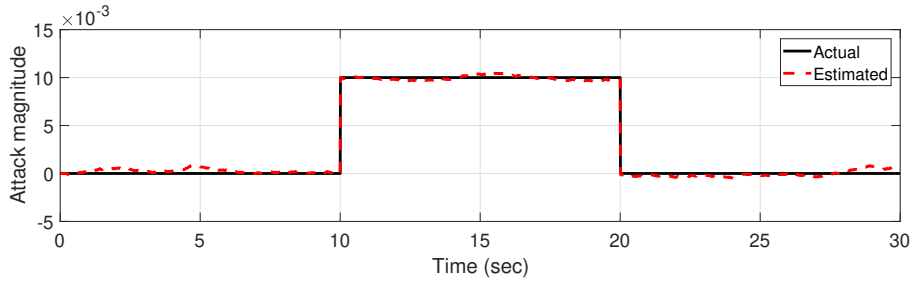


(b) Tie-line power

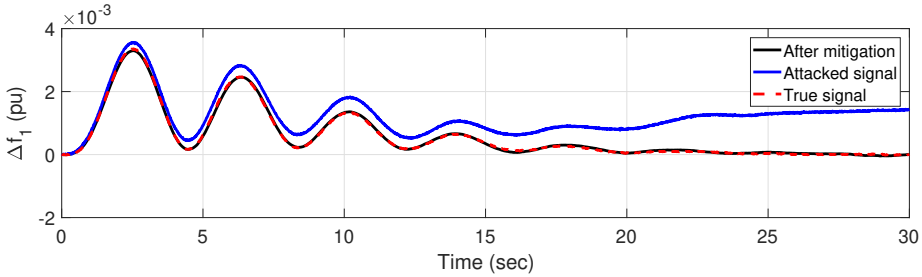
Figure 4.8: Step attack at system disturbance condition



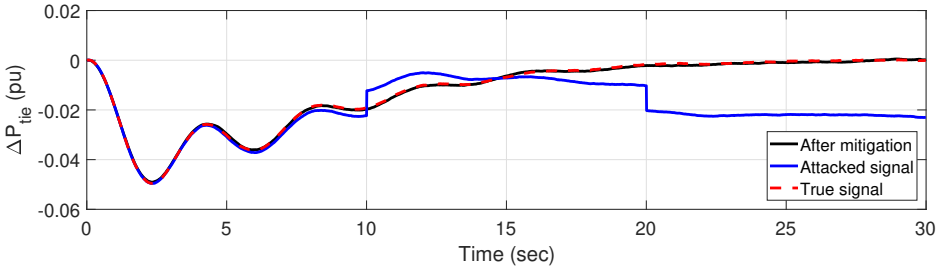
(a) Ramp attack with a slope of 0.001 to Δf_1



(b) Pulse attack with a magnitude of 0.01 to ΔP_{tie}



(c) Frequency deviation at Area 1



(d) Tie-line power

Figure 4.9: Combined attack 1 at system disturbance condition

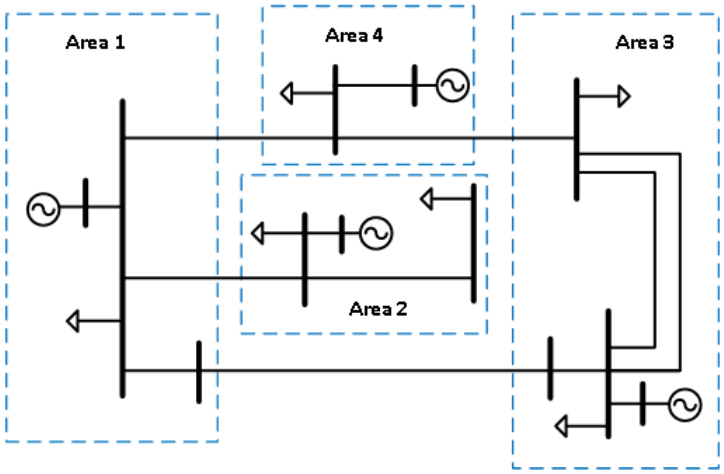
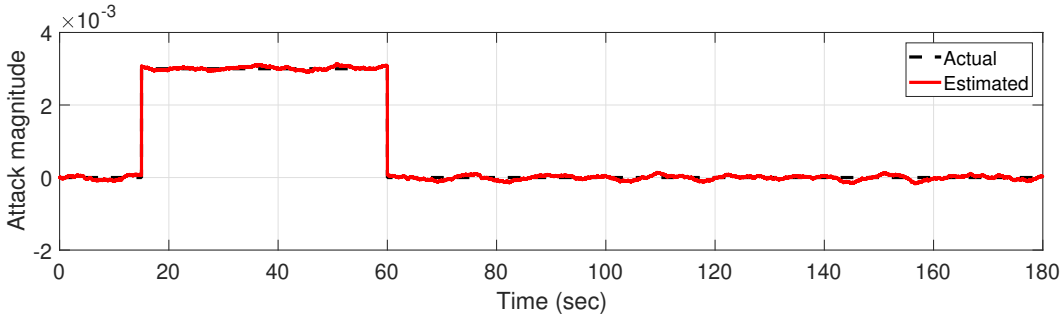
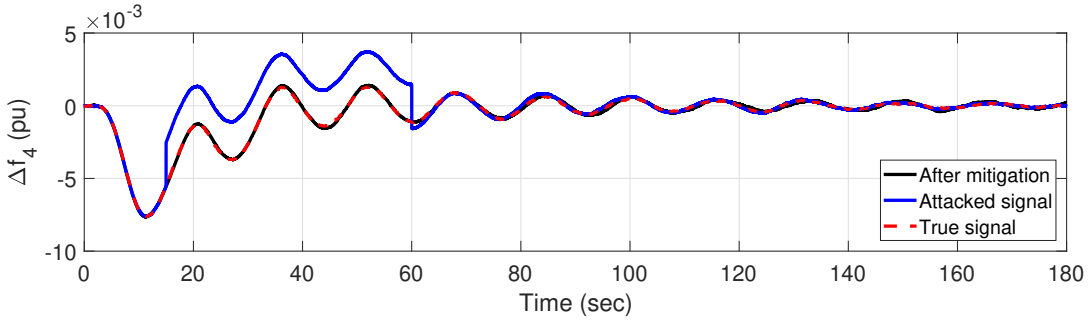


Figure 4.10: 4-Area Manitoba Chicago network

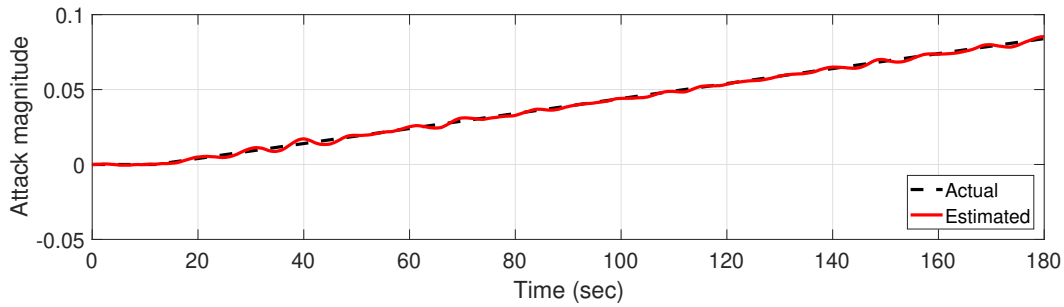


(a) Pulse attack with a magnitude of 0.003 to Δf_4

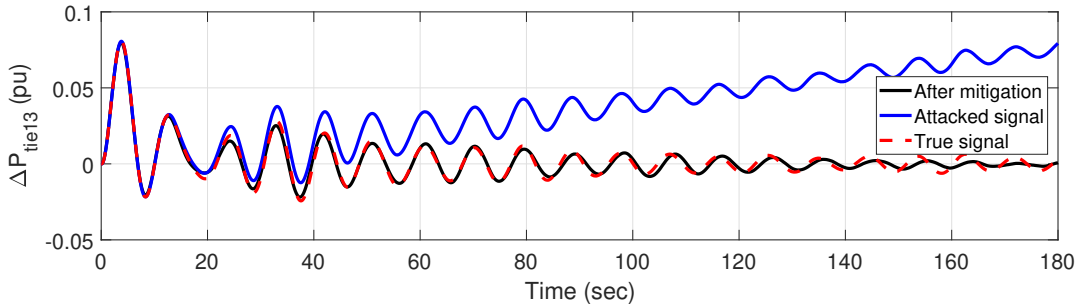


(b) Frequency deviation at Area 4

Figure 4.11: Pulse attack at system disturbance condition

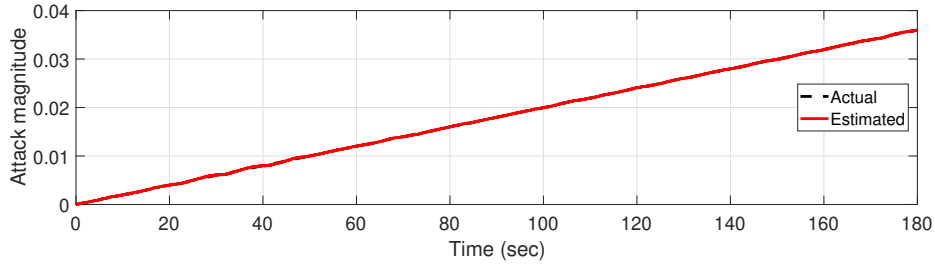


(a) Ramp attack with a slope of 0.0005 against ΔP_{tie13}

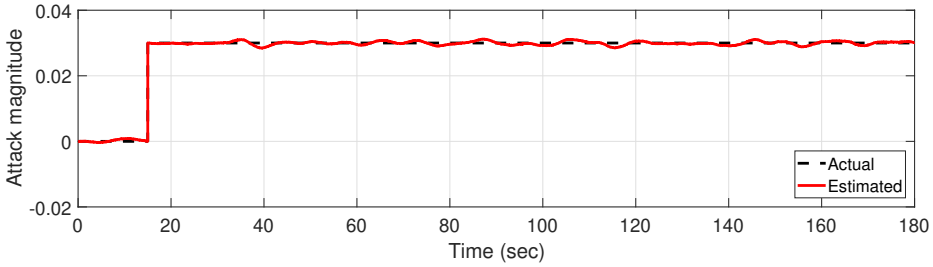


(b) Tie-line 1-3 power

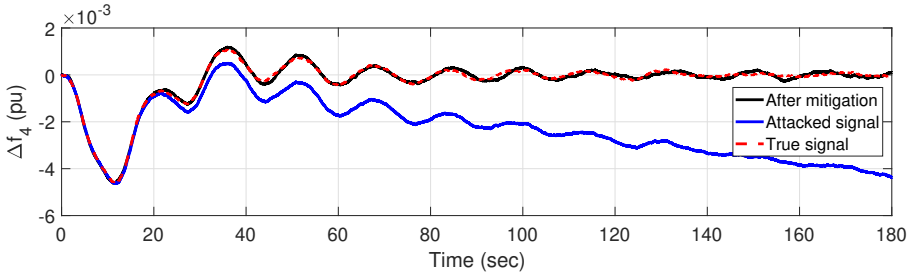
Figure 4.12: Ramp attack at system disturbance condition



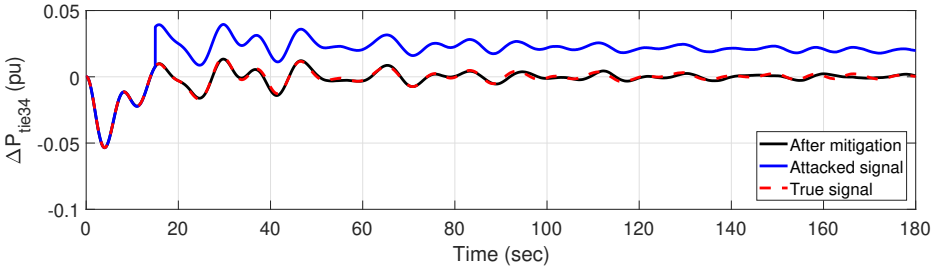
(a) Ramp attack with a slope of 0.0002 against Δf_1



(b) Step attack with a magnitude of 0.03 against ΔP_{tie34}

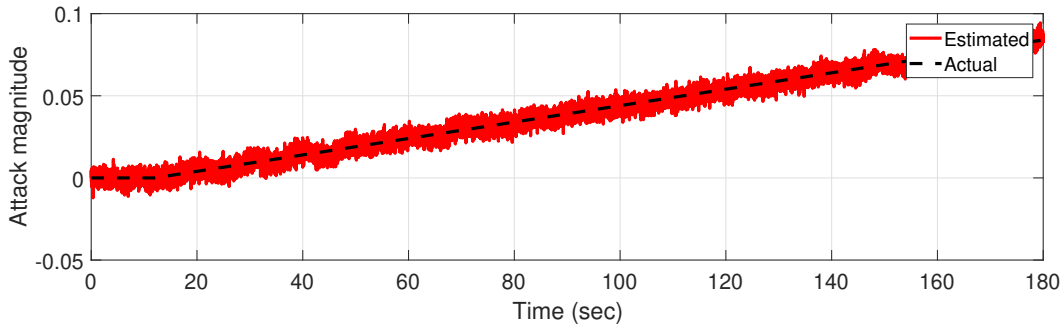


(c) Frequency deviation in Area 4

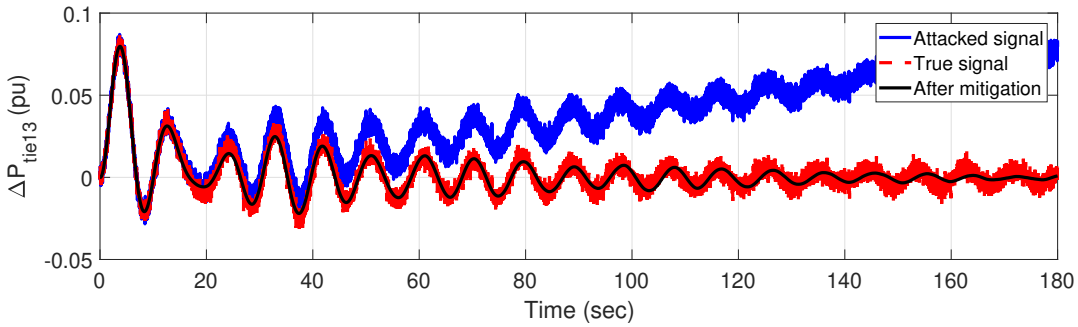


(d) Tie-line 3-4 power

Figure 4.13: Combined attack 2 at system disturbance condition

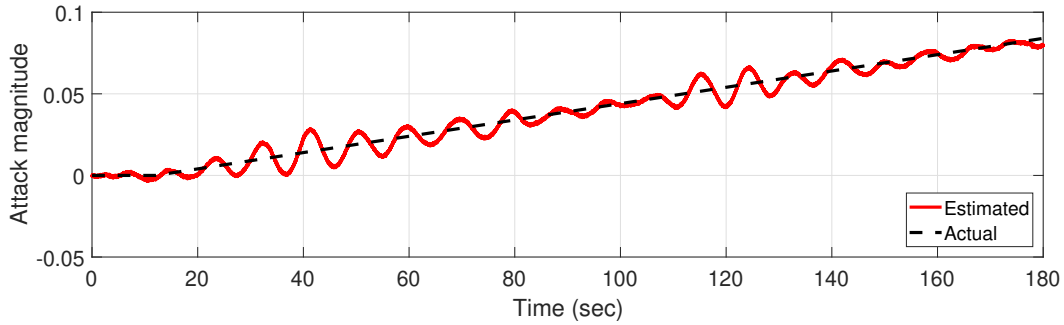


(a) Ramp attack with a slope of 0.0005 against ΔP_{tie13}

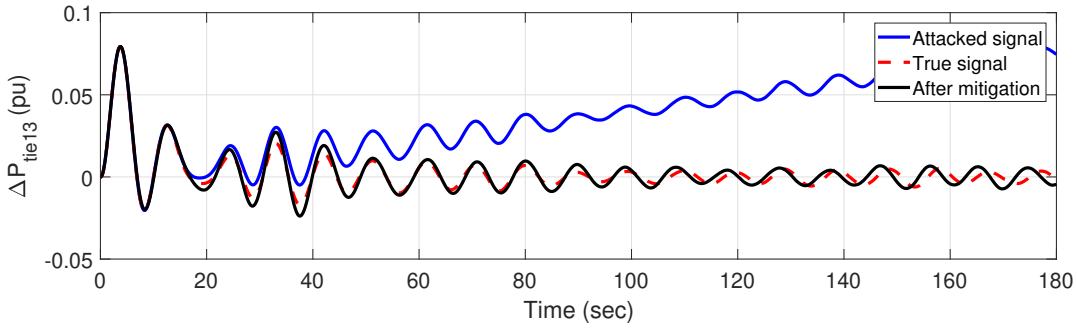


(b) Tie-line 1-3 power

Figure 4.14: Estimation and mitigation of a ramp attack in the presence of large sensor noise ($\sigma = 10^{-2.5}$)

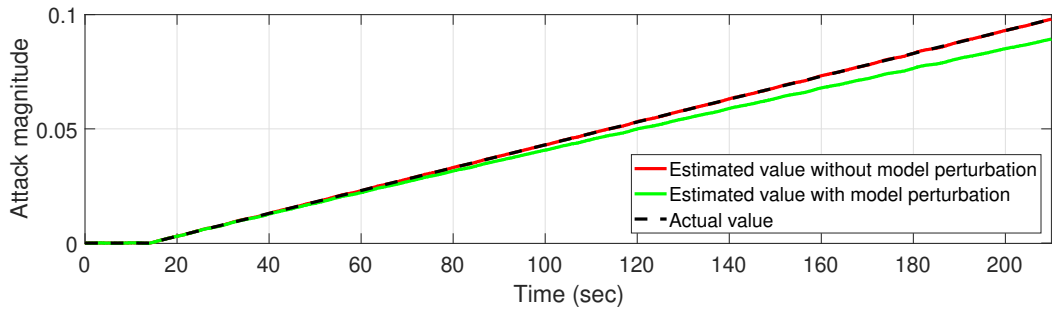


(a) Ramp attack with a slope of 0.0005 against ΔP_{tie13}

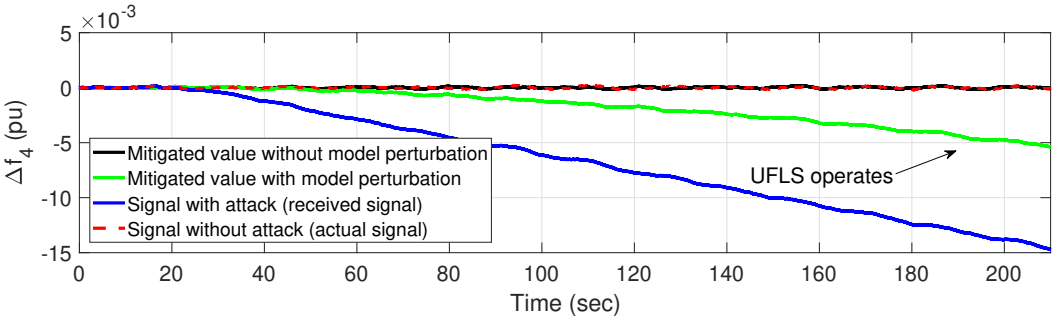


(b) Tie-line 1-3 power

Figure 4.15: System performance with inaccurate estimation for a ramp attack



(a) Estimation of ramp attack



(b) Frequency deviation at Area 4

Figure 4.16: Effect of inaccurate model estimation (20% perturbation of model parameters)

Chapter 5

Detection and Mitigation of False Data Injection (FDI) in AGC Systems Considering Nonlinearities

None of the previous works considered the nonlinearity of AGC systems, which means that the proposed solutions are only effective under the over-simplified assumed linearity of the AGC model. Because AGC nonlinearities rarely occur, the consequences of such an attack can be catastrophic, as none of the existing approaches that depend on the linear model will be able to detect or mitigate it. In this chapter, the work proposed in Chapter 4 is extended to address this deficiency and propose a new approach to detect and identify FDI attacks on AGC systems by considering three types of AGC nonlinearities.

5.1 AGC Nonlinearities and System Model

The nonlinearities of the AGC systems include but are not limited to the following:

- **Dead-band of Speed Governor (GDB):** If the absolute difference between governor power and disturbance power is lower than the dead band's value, the dead

band's output for the next control cycle remains constant. If it is higher, the dead band's output for the next control cycle is equal to the governor power [129, 130].

- **Generation Rate Constraints (GRC):** In power systems with thermal plants, power generation can be changed only at a specified maximum rate. The generation rate for reheat turbines is very low. If these constraints are not considered, the system is likely to chase large momentary disturbances, resulting in undue wear and tear on the controller. It is thus extremely important to understand the influence of GRC in the AGC problem. GRCs result in larger deviations in ACEs, as the rate at which generation can change in the area is constrained by the limits imposed. Therefore, the duration for which power needs to be imported increases considerably in comparison to cases where the generation rate is not constrained [131].

- **Transportation Delay Time (ΔT):** This results from the delay in the communication system as well as the delay in the response of the mechanical system.

To show the effectiveness of the aforementioned nonlinearities on the response of AGC system, the previous 2-area AGC system is updated as shown in Fig. 5.1 and tested with and without including the nonlinearities under similar disturbance conditions. In this work, the values of ΔT and Dead-band of Speed Governor (GDB) are adopted from [130] as 2 sec and 0.036 Hz, respectively, for both areas. In addition, the GRC is modeled similar to [130]. The simulated disturbance is a load increase of 0.18 *pu* in Area 1.

Figure 5.2 shows the differences in the main AGC signals that the control center operator use to make a decision e.g. frequency deviations and tie-line power. It can be seen that the response of AGC is completely different if the nonlinearities are considered. In other words, the control decision that is to be made based on the red signals (with nonlinearities) is totally different than that made based on the red signals (linear model response). This appears clearly in Fig. 5.3 in the ACE signals that are used to calculate the new operating point for each region.

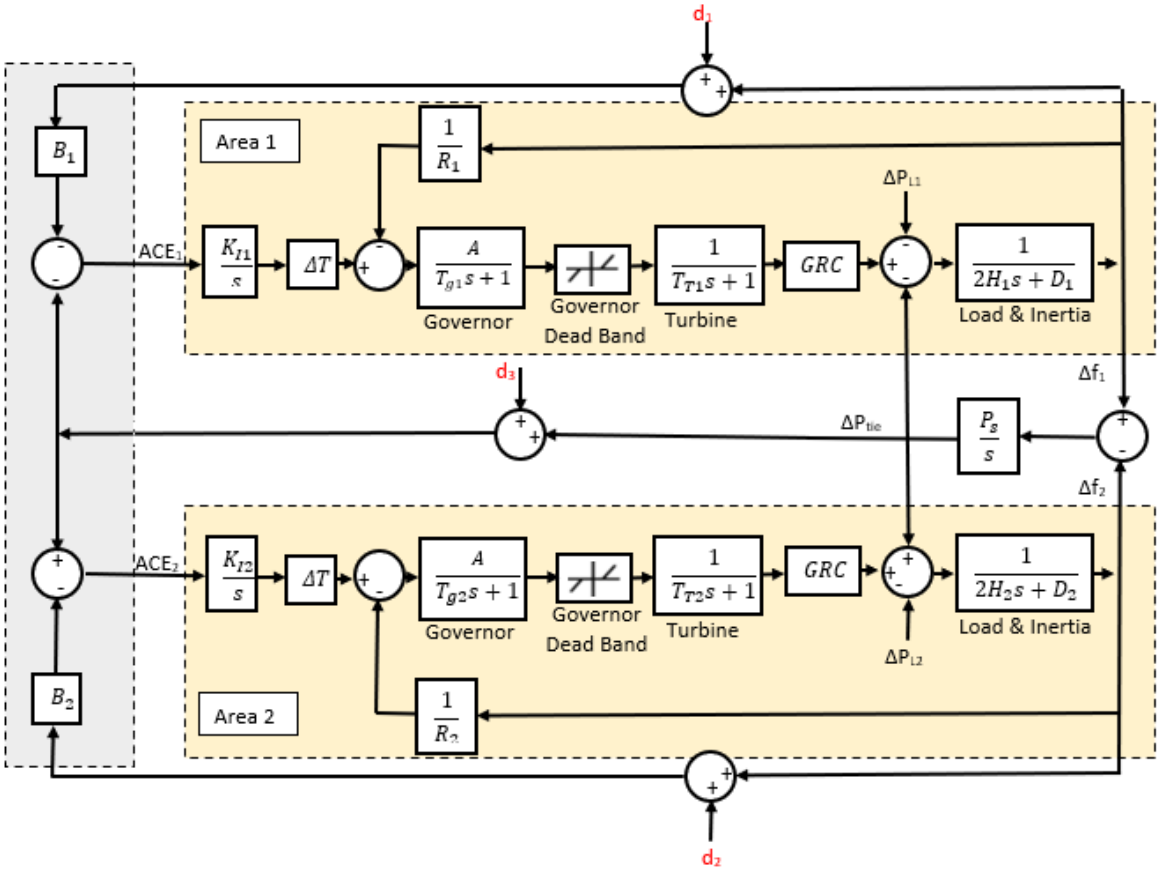
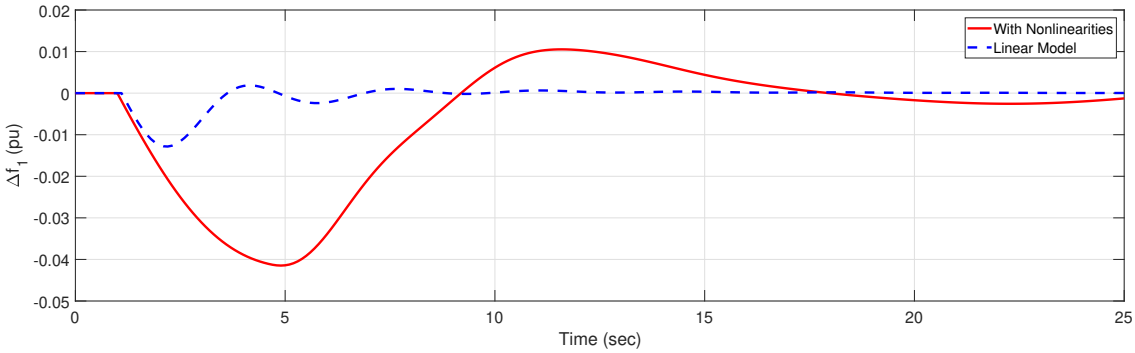


Figure 5.1: AGC model of a two-area system, including nonlinearities.

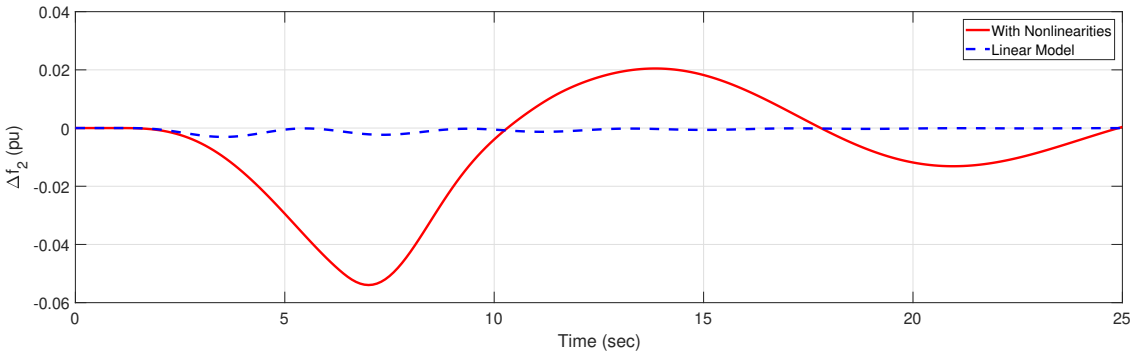
5.2 Detecting, Classifying and Identifying FDI Attacks on AGC Systems Using Recurrent Neural Networks

5.2.1 Recurrent Neural Networks

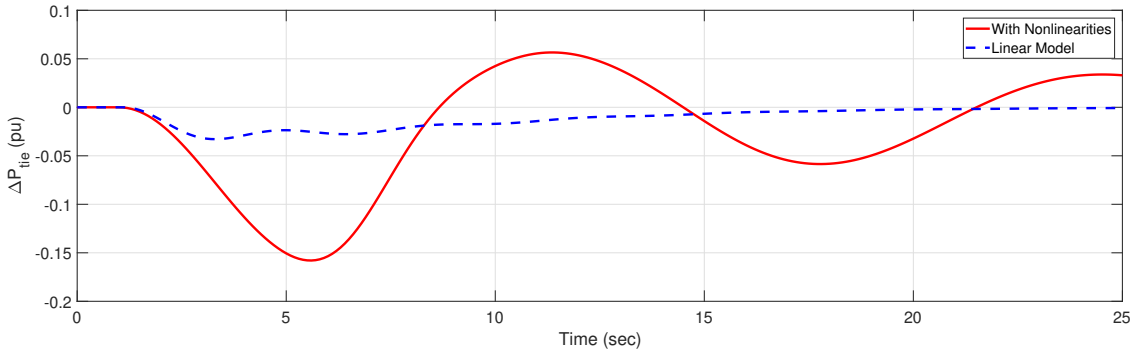
Recurrent Neural Networks (RNN) is a special type of neural network by which a



(a) Frequency deviation in Area 1

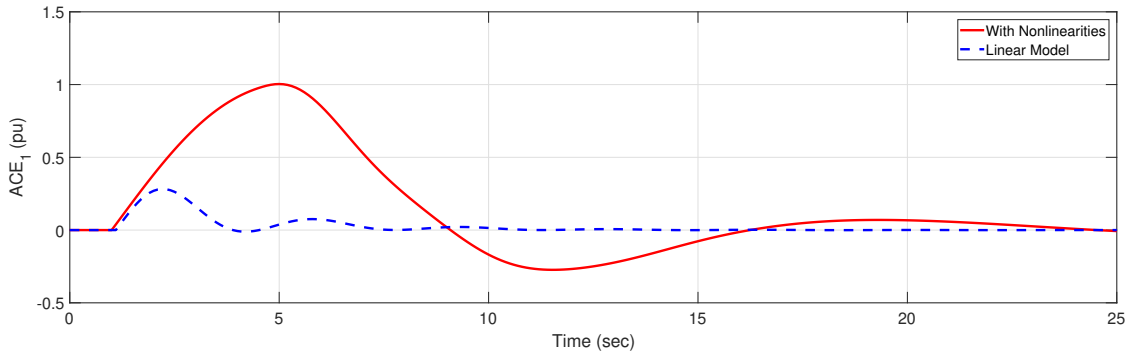


(b) Frequency deviation in Area 2

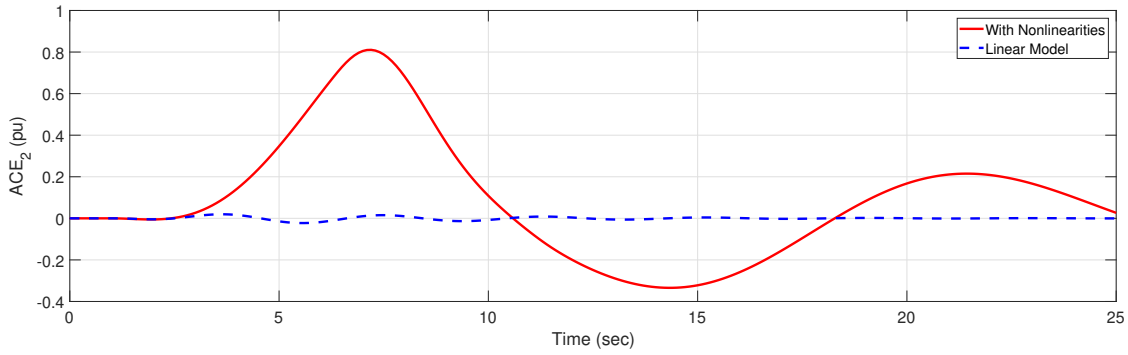


(c) Tie-line power

Figure 5.2: System response with and without nonlinearities



(a) Area 1 control error



(b) Area 2 control error

Figure 5.3: Area control error with and without nonlinearities

sequence of features (inputs) is mapped to labels (outputs). The RNN uses previous inputs and outputs to adjust the weights of the networks, thus creating a memory to improve its performance [132]. The structure of RNN can be mathematically modeled as [1]:

$$\boldsymbol{h}_t = f(\boldsymbol{h}_{t-1}, \boldsymbol{x}_t) \tag{5.1}$$

where $\boldsymbol{h}_t$ is the hidden state, $\boldsymbol{h}_{t-1}$ is the previous hidden state, $\boldsymbol{x}_t$ is the current feature observed, and f is a nonlinear mapping function from the input features to the output labels. Equation (5.1) presents the essence of RNN and what differentiates it from regular neural networks. The hidden state $\boldsymbol{h}_t$ is used as a memory to capture sequence information. Figure 5.4 shows the unfolding of RNN during computation.

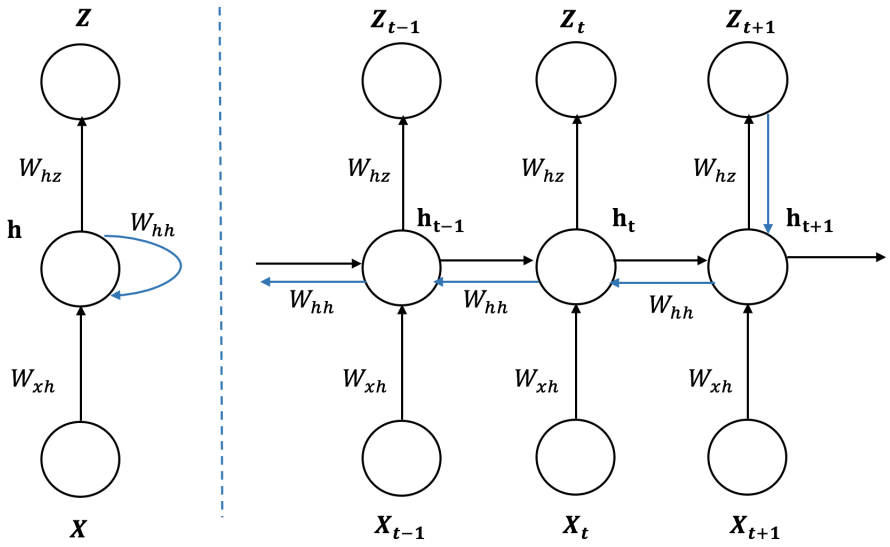


Figure 5.4: Left: Recursive Description of RNN. Right: Corresponding Extended RNN model for time sequence [1]

During the training phase, the RNN inputs a stream of data, which it then analyzes by relating the different input features (signals) and their corresponding labels (presence of attack and its type). The network screens the sequential data by creating a time window

of pre-specified number of time steps, and attempts to discern a temporal pattern across the features and labels in this window. The window slides over the entire sequence of data and updates the weights accordingly.

RNN employs a gradient descent technique to minimize the network cumulative error, namely the Back Propagation Through Time (BPTT) algorithm [133] and [134]. BPTT is an extension of the back propagation algorithm over a time sequence, where the gradient at each output depends on calculations of current as well as previous steps.

Starting with the RNN model described in Fig. 5.4, parameters are assumed to be the same across the whole sequence in each time step. This assumption is used to simplify the gradient calculations [1]. At time t, we have:

$$\boldsymbol{h_t} = \tanh(W_{hh}\boldsymbol{h_{t-1}} + W_{xh}\boldsymbol{x_t} + \boldsymbol{b_h}) \tag{5.2}$$

$$z_t = softmax(W_{hz}\boldsymbol{h_t} + \boldsymbol{b_z}) \tag{5.3}$$

where $b_{\boldsymbol{h}}$ and b_z are the bias terms for the hidden state and prediction at time step t. The $softmax$ function is the used loss function, which is commonly employed as the final layer in neural networks architecture for multiple class classification. The maximum likelihood is used to estimate the model parameters, while the minimization of the objective function of negative log likelihood is [1]:

$$\mathcal{L}(\boldsymbol{x}, y) = -\sum_t y_t \log z_t \tag{5.4}$$

where z_t is the prediction at time step t. For simplicity, the notation $\mathcal{L}$ will be used as the objective function. The notation $\mathcal{L}(t)$ indicates the output at time t while $\mathcal{L}(t+1)$ indicates the output at time $t+1$. The derivative of equation (5.4) with respect to z_t is:

$$\frac{\partial \mathcal{L}}{\partial z_t} = -\sum_t y_t \frac{\partial log z_t}{\partial \boldsymbol{h}_t} = -\sum_t y_t \frac{1}{z_t}\frac{\partial z_t}{\partial \boldsymbol{h}_t} \tag{5.5}$$

Using the chain rule and by deriving the gradient of the $softmax$ function from (5.3), we get:

$$\frac{\partial \mathcal{L}}{\partial z_t} = -(y_t - z_t) \tag{5.6}$$

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

$$\frac{\partial \mathcal{L}}{\partial W_{hz}} = \sum_t \frac{\partial \mathcal{L}}{\partial z_t} \frac{\partial z_t}{\partial W_{hz}} \tag{5.7}$$

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

$$\frac{\partial \mathcal{L}}{\partial b_z} = \sum_t \frac{\partial \mathcal{L}}{\partial z_t} \frac{\partial z_t}{\partial b_z} \tag{5.8}$$

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

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{hh}} = \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \boldsymbol{h}_{t+1}} \frac{\partial \boldsymbol{h}_{t+1}}{\partial W_{hh}} \tag{5.9}$$

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

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{hh}} = \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \boldsymbol{h}_{t+1}} \frac{\partial \boldsymbol{h}_{t+1}}{\partial \boldsymbol{h}_t} \frac{\partial \boldsymbol{h}_t}{\partial W_{hh}} \tag{5.10}$$

Then, by aggregating gradients with respect to W_{hh} over the whole sequence and using the BPTT from time t to 0, we get:

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{hh}} = \sum_{t} \sum_{k=1}^{t+1} \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \boldsymbol{h}_{t+1}} \frac{\partial \boldsymbol{h}_{t+1}}{\partial \boldsymbol{h}_k} \frac{\partial \boldsymbol{h}_k}{\partial W_{hh}} \tag{5.11}$$

The same process applied in (5.7)-(5.11) is also applied to the weights W_{xh}, by taking the gradient with respect to W_{xh} over the whole sequence to obtain:

$$\frac{\partial \mathcal{L}(t+1)}{\partial W_{xh}} = \sum_{t} \sum_{k=1}^{t+1} \frac{\partial \mathcal{L}(t+1)}{\partial z_{t+1}} \frac{\partial z_{t+1}}{\partial \boldsymbol{h}_{t+1}} \frac{\partial \boldsymbol{h}_{t+1}}{\partial \boldsymbol{h}_k} \frac{\partial \boldsymbol{h}_k}{\partial W_{xh}} \tag{5.12}$$

5.2.2 Simulation Results

To validate the approach of using RNN for detecting attacks on the AGC system, typical statistical measures are applied to diagnose the detection classification ability of the RNN model, such as accuracy, sensitivity, specificity, and precision calculations. First, RNN is used as a binary classifier to detect the anomaly (attack) present in the signal, without differentiating the type of the attack. Secondly, RNN is used to detect the different types of attacks and identify the attacked signal.

The RNN model employed in the simulations is trained using the following parameters: 1) Input dimension of 5. The input (features) are tie-line power and frequency signals. 2) Output dimension of 1. The output (labels) represents an indication of attack type and the attacked signal, if any, for each time step. 3) Batch size of 64. This batch size is chosen as it outputs the best results over multiple iterations of training. 4) Epoch size of 100. The model did not improve results for an epoch number greater than 100. 5) An RMSprop optimizer is chosen, as it provides superior performance in RNN models with similar objectives [135]. The model is implemented using the Keras RNN-LSTM stacked architecture [136].

The predictions of both detection and identification models can be analyzed by considering the two (four) possibilities for each output label $l \in L$, i.e., attack detection (attack location), by considering an output l as positive and all others output as negative: (1) True

Positive (TP) describes a positive prediction of an actual positive case, (2) True Negative (TP) describes a negative prediction of an actual negative case, (3) False Positive (FP) describes a positive prediction of an actual negative case, and (4) False Negative (FN) describes a negative prediction of an actual positive case. Based on these possible outcomes, the following four statistical metrics are introduced:

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \tag{5.13}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{5.14}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{5.15}$$

$$f_1 \text{ Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5.16}$$

where the Accuracy metric measures the probability of classifying fault cases correctly and is a general indicator of the overall classifier performance; the Precision metric measures the probability of correct positive classification, and is an indicator of the confidence in the predicted positive cases; the Recall metric demonstrates the probability of correct classification in all positive labels, and is an indicator of ability to predict positive cases; and finally the f_1 Score represents the balance between the Precision and Recall.

The training data are generated using the results of 3,000 different scenarios for the AGC under normal operation (no attacks) as well as under different types of attacks. The results in tables 5.1 and 5.2 are based on a validation data set composed of 192,000 data samples taken from the 3,000 simulated scenarios. These data points are presented as one long stream of data, simulating the data that is gathered by the data center. In both cases, a threshold window limit k_T is implemented to count a detection or the identification of the attack. For an attack at time step $T = T_0$, the RNN should detect the attack at $T \leq T_0 + K_T$, in order to count as a valid detection. For our simulations, $K_T = 10$ is used, which represents one second in real time.

The results confirm the capability of RNN to detect with high statistical measures, in less than one second of the attack, given a sample time rate of 10 ms. The model achieves a precision rate of 99.01, 99.22 and 99.43 in the detection, classification and identification

tasks, respectively. The RNN performance measure is on par with accuracy metrics of other data-driven machine learning models used in related power system problems [135, 137]. After attack detection, the attacks are identified to be in Δf_1 (Signal '1'), Δf_2 (Signal '2') or ΔP_{tie} (Signal '3'). The following case studies show simulations where our approach is tested under different types of attacks.

Table 5.1: Performance Table for RNN Detector

Criteria	**Score**
Number of data samples	192000
True Positive (TP)	117429
False Positive (FP)	1174
True Negative (TN)	64425
False Negative (FN)	8972
Accuracy	94.72%
Sensitivity	98.21%
Specificity	92.90%
Precision	99.01%

Table 5.2: Performance Table for RNN identifier

Criteria	**Score**
Number of data samples	192000
True Positive (TP)	117678
False Positive (FP)	925
True Negative (TN)	64425
False Negative (FN)	8972
Accuracy	94.85%
Sensitivity	98.58%
Specificity	92.92%
Precision	99.22%

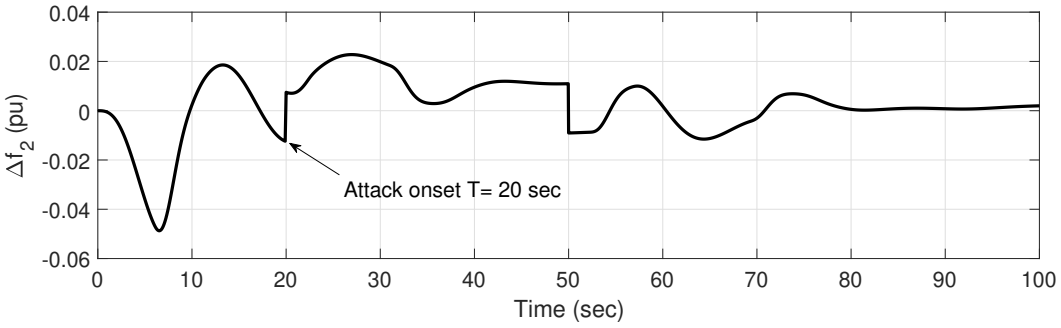
In our case studies, the parameters of the previously mentioned attacks (e.g., magnitude, and rate of change) are selected carefully such that the attack is hidden and bypasses the bad data detectors in the control system. To be more precise, the measurements should not change significantly over a short period. Intuitively, if each element of the FDI attack vector is bounded around zero, these bad data detectors, designed to be insensitive to natural random noises in the measurements, will not be changed [53]. The parameters have to be selected such that the attack creates the desired impact and at the same time does not trigger any data quality alarms in the control center.

Case 1: Pulse attack to Δf_2 In this case, under a system disturbance of 0.15 pu in Area 1, the signal Δf_2 is manipulated using a pulse signal with a magnitude of 0.2. The attack, which started at $T = 20sec$. Fig. 5.5, shows that the proposed approach detected the attack in less than 1 sec. Also, the attack is classified as Type '1' and is identified to be in Δf_2. A sample of the tested case studies that show the detection and classification processes is given below.

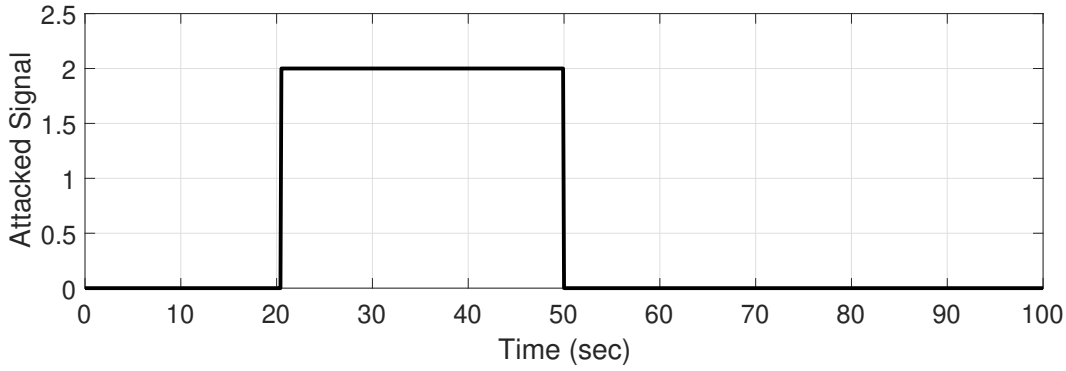
Case 2: Ramp attack to ΔP_{tie} Under a system disturbance of 0.2 pu in Area 2, a ramp signal with a slope of 0.001 is injected in the signal of ΔP_{tie} at $t = 5sec$. Figure 5.6 shows that the attack is detected in Signal '3' at $t = 5.7sec$ and classified as a Type '2' attack.

5.3 Mitigation Using Load Forecast

In scenarios where an attack is detected while the AGC is working in the nonlinear region, the attack detection technique based on RNN will be effective to detect, classify and identify the attack. However, the mitigation technique, described in the previous chapter can no longer be trusted. The control center will be "flying blind" while trying to match the load and generation. Therefore, there is a need to use a technique that makes an educated guess based on system knowledge and appropriately issues ACE commands to generators without the need for system measurements.

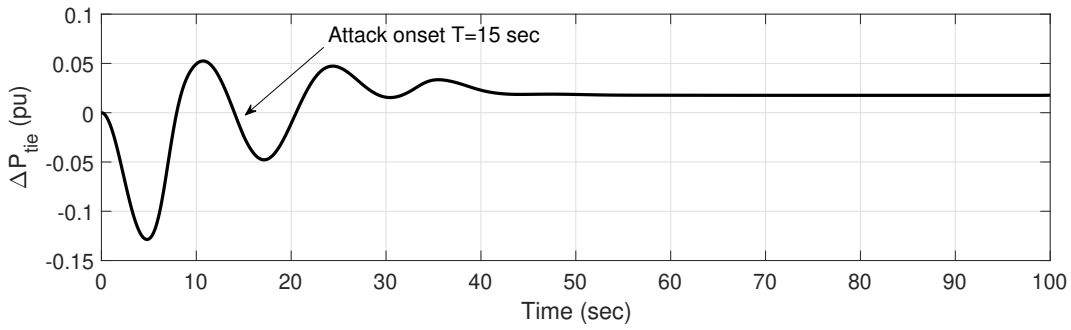


(a) Frequency deviation in Area 1

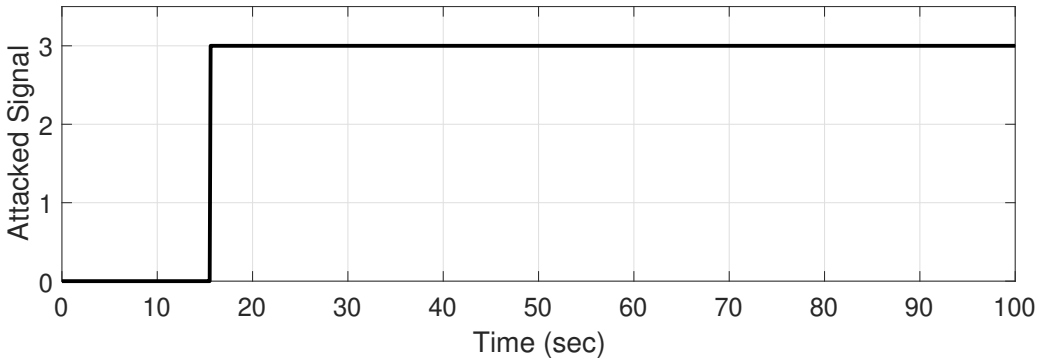


(b) Attack identification

Figure 5.5: Pulse attack to Δf_2



(a) Tie-line power



(b) Attack identification

Figure 5.6: Ramp attack to ΔP_{tie}

In the literature, regression models, neural networks and statistical learning algorithms are used to calculate real-time load forecasts. Weather forecasts, seasonal effects and other factors are considered in these approaches to arrive at a load forecast. Generally speaking, making the decisions based on load forecast might not be accurate, as discussed in section 2.3.1. In addition, the accuracy of the proposed mitigation scheme in the previous chapter is sufficient in case the AGC is working in the linear region. Therefore, in this work, the mitigation-based load forecast algorithm mentioned in [80] is suitable to be used if an attack is detected by the particle filter or RNN, and only if the AGC is working in the nonlinear region. In this case, only the attacked signal can be calculated using the load forecast after it has been identified using the RNN identifier.

5.4 Summary

In this chapter, the effect of AGC nonlinearities was included. RNN-based method was proposed for detecting and identifying attacks on AGC systems. Different attack templates representing different types of data manipulation were discussed and simulated and various attack scenarios were applied. The proposed detection techniques were able to detect all of them. The results confirmed the capability of RNN for detecting and identifying different types of attacks with high statistical measures in less than one second of the attack's onset. The first step was developing an RNN detector, and then adapting the model in order to identify the location of the attack. The RNN model achieved a precision rate of 99.01 and 99.22 in the detection and identification tasks, respectively.

Chapter 6

Mitigating False Data Injection (FDI) Attacks on Wide-Area Under-Frequency Load Shedding (WAUFLS) Schemes

Relying solely on the value of ROCOF to evaluate system disturbances makes the current WAUFLS schemes vulnerable to cyber attacks, as shown in section 3.4. They are also inaccurate in small systems, as system inertia changes if one of the generators is tripped [102]. In addition, using the swing equation to determine the magnitude of disturbance is valid only at the moment of disturbance and does not give a real-time monitoring of system mismatch [105]. In this chapter, a new WAUFLS scheme that overcomes these drawbacks inherent in the current schemes is proposed. Because it works based on trusted system states, it is able to evaluate system disturbances accurately, even if there are FDI attacks on the frequency signals.

6.1 Description of the Proposed WAUFLS Scheme

The proposed scheme calculates power mismatches using dynamic power flow analysis. However, the data used to run the dynamic power flow must be obtained from a trusted source. Therefore, PSSE represents an in-between layer that processes system measurements and provides trusted data, using the proposed measurement classification-based method explained in Section 6.2, that can be used in the power flow.

The logic of the proposed scheme is depicted in a flowchart in Fig. 6.1. First, the frequency and power flow measurements are received from various sensors and PMUs in the system. Then, the frequency of center of inertia (f_c) is calculated and compared to a predefined threshold (F_{min}). A value less than the threshold means that there is an under-frequency condition in the system due to a disturbance. At that point, power flow measurements are used to run the PSSE, and trusted system states (V and δ at each bus) are obtained.

The next step is to use these trusted states to run a dynamic power flow that calculates the power mismatch caused by the disturbance. Based on the calculated mismatch, a load shedding process is performed. After shedding the needed load amount, f_c is calculated based on the updated values for system frequency measurements and compared with the nominal value of system frequency (F_n). Finally, if $f_c < F_n$, the updated power flow measurements are used to repeat the Power System State Estimation-Power Flow (PSSE-PF) process until the system frequency returns to its nominal value. It is worth mentioning that the topology of the system should be updated as needed, prior to running both PSSE and the power flow. In the following subsections, the used models of PSSE as well as dynamic power flow are described.

6.2 Securing PSSE using Measurement Classification

In order to run the PSSE, the control center operator relies on PFMs that guarantee system observability. In practice, the system operator has access to redundant PFMs which

generate a high number of essential sets [60]. The proposed mitigation method depends on two main steps: i) securing only the subset of critical PFMs, and ii) employing different PFMs for running the PSSE. By securing only the critical PFMs, we minimize the cost of securing the power network. Furthermore, by employing a different observable (essential) PFMs set, the attacker has virtually zero chance of knowing the PFMs to attack. Therefore, any attempted attack will be easily detected by the PSSE BDD.

For the PSSE operation, as outlined in Section 3.3, the PFM including voltage V, phase angles θ, active power injection P_i, and reactive power injection Q_i, which can be obtained from the sensors installed at each bus. This is in addition to active and reactive power flow values which can be obtained from the sensors installed at the transmission lines. Therefore, the maximum possible number of PFM that can be obtained in a system is $N_{max} = 4N + 2b$ where N is the number of buses and b is the number of transmission lines. Since it impractical to install sensors everywhere in the power system, it is assumed that the installed sensors provide a set of data A where $A \subset M$ and M is the set that includes all the possible measurements in that system. In this work, the available data set A can be classified into essential E and non-essential W data subsets i.e., $A = E \cup W$. Essential data subset is the minimum number of PFM that is required to achieve system observablity. Essential data subsets are not unique and many subsets can be identified for a system based on the number of the available data in the set A. The intersection of all essential data sets gives a critical data subset C i.e., $C = E_1 \cap E_2 \cap E_3 \ ... \ \cap E_n$ where n is the maximum number of essential subsets. The critical data subset is a unique subset of data that is required by the PSSE to converge [60]. This classification is shown in Fig. 6.2. Using the i_{th} essential subset E_i, the critical PFM for a system can be obtained by ordering the essential measurements first, then partitioning the matrices and rewriting equation (3.17) as:

$$\begin{bmatrix} h_E(x) \\ h_W(x) \end{bmatrix} . \begin{bmatrix} x \end{bmatrix} = \begin{bmatrix} z_E \\ z_W \end{bmatrix} \tag{6.1}$$

where the rows of $h_E(x)$, z_E and $h_W(x)$, z_W correspond to the essential and non essential measurements, respectively. Applying the Peters-Wilkinson decomposition and substitut-

ing in (6.1)

$$Z_E = L_1.U.x \tag{6.2}$$

$$Z_W = L_2.U.x \tag{6.3}$$

Eliminating $U.x$, the linear dependency among the essential and non-essential measurements can be given by (6.5). Hence, an element of z_E is critical if the corresponding column of T is null.

$$z_W = L_2.L_1^{-1}.z_1 \tag{6.4}$$

$$z_W = T.z_1 \tag{6.5}$$

The proposed mitigation scheme in this work is to install secured communication channels for all the critical PFM such that the attacker cannot access the measurements included in the subset C. In addition, given the fact that a number of essential PFM sets can be identified, a second layer of security can be added if the control center operator selects -randomly- one of these sets at each run. If it is possible for the attacker to identify these sets, it is impossible for him/her to know which set is used at the current instant. Therefore, the attacker will never be able to launch a hidden attack. However, the attacker can manipulate some measurements and this will be detected easily using the BDD in the PSSE.

6.3 Calculating the Power Mismatch Using a PSSE-PF Module

After estimating a trusted vector of system states, including voltage magnitude and phase angle at each bus, these trusted values are used to run a power flow to calculate total system mismatch. To capture small changes in the power system during transients, a second-order power flow model [138] is used to calculate the total power mismatch. For a system with n buses, the power mismatch at bus i can be defined as the sum of the power

flows in all elements, i.e., generators, loads, transmission lines, etc., connected to this bus. Using Taylor series expansion, the active power mismatch $P_{mis,i}$ at bus i can be defined as:

$$P_{mis,i} = \sum_{j=1}^{N} \frac{\partial P_i}{\partial \delta_j} \Delta\delta_j + \sum_{j=1}^{N} \frac{\partial P_i}{\partial V_j} \Delta V_j + \frac{1}{2} \sum_{j=1}^{N} \frac{\partial^2 P_i}{\partial \delta_j^2} (\Delta\delta_j)^2 + \frac{1}{2} \sum_{j=1}^{N} \frac{\partial^2 P_i}{\partial V_j^2} (\Delta V_j)^2 + \sum_{j=1}^{N-1} \sum_{r=j+1}^{N} \frac{\partial^2 P_i}{\partial \delta_j \partial \delta_r} \Delta\delta_j \Delta\delta_r + \sum_{j=1}^{N} \sum_{r=1}^{N} \frac{\partial^2 P_i}{\partial \delta_j \partial V_r} \Delta\delta_j \Delta V_r + \sum_{j=1}^{N-1} \sum_{r=j+1}^{N} \frac{\partial^2 P_i}{\partial V_j \partial V_r} \Delta V_j \Delta V_r \quad (6.6)$$

where P_i is the active power injection into bus i, δ_j and V_j are the phase angle and magnitude of voltage at bus j, respectively, N is the number of system buses, and Δ represents small changes in the variables. Real power injection into bus i can be mathematically expressed as:

$$P_i = \sum_{j=1}^{N} |V_i V_j Y_{ij}| cos(\delta_i - \delta_j - \theta_{ij}) \quad (6.7)$$

where $Y_{ij} = |Y_{ij}| \angle \theta_{ij}$ is the admittance of the transmission line connecting buses i and j. Substituting (6.7) into (6.6) and after simplifications [138]:

$$P_{mis,i} = \sum_{j=1}^{N} \frac{\partial P_i}{\partial \delta_j} \Delta\delta_j + \sum_{j=1}^{N} \frac{\partial P_i}{\partial V_j} \Delta V_j + \frac{\partial^2 P_i}{\partial V_j^2} (\Delta V_j)^2 + \sum_{j=1, j\neq i}^{N} \frac{\partial^2 P_i}{\partial \delta_i \partial V_j} \Delta\delta_i \Delta V_j + \sum_{j=1, j\neq i}^{N} \frac{\partial^2 P_i}{\partial \delta_j \partial V_j} \Delta\delta_j \Delta V_j + \sum_{j=1}^{N} \frac{\partial^2 P_i}{\partial \delta_j \partial V_i} \Delta\delta_j \Delta V_i \quad (6.8)$$

Finally, the total system mismatch P_{mis}, which is also equal to the difference between the total generation P_G and the total load P_L, is equal to the summation of the single

mismatch values at each bus and can be evaluated as (6.9). It is worth mentioning that while system losses can be neglected in large systems, in this work they are included in P_L.

$$P_{mis} = P_L - P_G = \sum_{i=1}^{N} P_{mis,i} \tag{6.9}$$

6.4 Load Shedding Process

Since the proposed approach performs online monitoring of the amount of power mismatch, the amount of load to be shed P_{shed} is the same as the amount of power mismatch P_{mis} because the spinning reserve is already embedded in the calculations. This contrasts with other approaches that require knowledge of the system spinning reserve because they calculate the magnitude of disturbance, not the actual power mismatch in the system.

To achieve load shedding, a combination of loads is selected such that the sum of their total active powers is as close as possible to P_{shed}. There are different criteria by which load shedding locations can be selected. However, the most common criteria used in wide-area applications is voltage collapse-based load shedding, as the voltage collapses rapidly after a disturbance [104, 107, 109, 116–118].

For the sake of subject completeness, the shedding criterion used in the simulations of this paper will be discussed. The shedding locations are mainly selected based on the location of disturbance [104]. In other words, the load shedding is distributed between the buses that are close to the disturbance according to their voltage dip during the disturbance. All area buses are ranked based on voltage dips. Accordingly, the load shedding at bus i is proportional to the bus rank, as follows:

$$P_{shed,i} = \frac{\Delta V_i}{\sum_i^{N_v} \Delta V_i} \times P_{shed} \tag{6.10}$$

where ΔV_i is the voltage dip at bus i immediately after the disturbance, and N_v is the set of buses that have the highest voltage dip. Once the load to be shed is known for all

buses, the shedding process takes place in steps. It is worth mentioning that the trusted values of buses voltage are used for this purpose, which means that this process is robust to cyber attacks.

6.5 Reliability and Accuracy of the Proposed Method

The proposed mitigation approach depends on running the PSSE, which is an essential operation in the power grid. The approach relies on adding a security layer for the PSSE process by using secure PFMs. However, this added security layer does not have any significant delays in the PSSE scheme. Fig. 6.3 depicts the required number of iterations for PSSE convergence for different accuracy thresholds, which is the typical number of iterations for PSSE schemes. In addition, Fig. 6.4 shows the probability of finding an observable set against employing a specific percentage of available PFMs (with all possible combinations at this percentage). For example, in the IEEE 39 bus New England system, of all PFMs sets combination of size 80% of available PFMs, 40% are essential sets that can be used for PSSE. Therefore, by using different PFMs sets of various sizes, the probability of the attacker to find the employed essential set drastically diminished, which highly increases the reliability of the PSSE. As the protection strategy depends on utilising different observable sets to obtain trusted states from the PSSE, we calculate the probability of a successful FDI attack (scheme failure probability) for a PFMs subset size as the inverse of the available number of observable sets times the probability of obtaining an observable set (as shown in Fig. 6.4). The probability of the mitigation scheme failure against the PFMs subset size used for the PSSE is depicted in Fig. 6.5. The figure shows that applying a smaller subset of PFMs reduces the probability of a successful attack, as it allows a larger number of PFMs combinations to obtain the PSSE. The system operator, however, does not need to be restricted to a specific PFMs subset size.

6.6 Simulation Results

In this section, the robustness of the proposed scheme is tested against the shortcomings of traditional approaches, as discussed in the previous section. In so doing, we will calculate load shedding under disturbance conditions, through the usage of the PSSE-PF module. The following scenarios are simulated in PSCAD/EMTDC using the IEEE 39 bus New England system. The measures of system stability after incorporating load shedding are defined in [116–118, 139]. Accordingly, system voltage at each bus as well as system frequency are recorded and shown in the following scenarios to make sure they are within the standard limits that achieve system stability.

6.6.1 Tripping of a Large Generator

In this scenario, the proposed scheme is used to relieve the system after tripping generator G1. Figure 6.6a shows the variations in system load versus the drop in system generation due to the disturbance. The value of the initial mismatch is 1 pu, so this is the amount of load to be shed in the first step when the frequency reaches the minimum threshold ($59.3Hz$). Due to the transient which occurred after shedding the load, the generation power drops slightly, necessitating a smaller second shedding step. The calculated mismatch value, illustrated in Fig. 6.6b, shows the accuracy of using the PSSE-PF module to calculate it at different stages of the disturbance. It also shows that the power mismatch is reduced to zero after the shedding process. As a result, the frequency of center of inertia reverts to the nominal value, as depicted in Fig. 6.6c, which reflects the frequency stability of the system after incorporating the proposed shedding scheme. In addition, Fig. **??** shows the system voltage response at buses 5, 6, 7, 8, 12, 31 and 32 during and after incorporating the load shedding. It can be seen that after incorporating the proposed scheme, system voltage at each bus returns back to its normal value, which achieves voltage stability as well.

6.6.2 Islanding Scenario

This scenario includes a sudden load increase of 0.45 *pu* at bus 15 at $t = 16$ *sec*, resulting in the disconnection of the transmission lines that connect buses 1-2 and 8-9 at $t = 17$ *sec* due to thermal limits. Because of this disturbance, the system becomes two islands, with one having an unbalance between load and generation due to being disconnected from the system's main supply. The system can be viewed as two areas: Area 1, which includes buses 1, 9 and 39, and Area 2, which includes the rest of the system. An analysis of each area is carried out separately below.

A. Analysis of Area 1

Area 1 includes the largest supply G_1. However, as seen in Fig. 6.8a, the generation is less than the load, and the rest of load power is taken from the generators in Area 2. At the moment of disturbance, G_1 is willing to participate in the load increase that occurs in Area 2, so the output power of this generator increases. Following the disconnection of the transmission line at $t = 17$ *sec*, Area 1 becomes isolated and includes only G_1 and a load of 1.15 *pu*. The frequency of Area 1 remains stable after the disturbance, as shown in Fig. 6.8c, because the area power mismatch is zero (see Fig. 6.8b). Therefore, no load shedding is needed in Area 1.

B. Analysis of Area 2

Area 2 experiences extra generation prior to the load increase that occurs at $t = 16$ *sec*. This extra generation power is supplied to Area 1, as discussed above and as shown in Fig. 6.9a. After the transmission lines are disconnected, a mismatch of 0.15 *pu* exists in Area 2 (see Fig. 6.9b) because the generators in this area are not able to supply the entire load demand. Hence, the system frequency begins to drop, as illustrated in Fig. 6.9c, and reaches the load shedding threshold at $t = 24$ *sec*. A load shedding process then takes place and the frequency of the area returns to its nominal value.

It can be seen that the frequency in the two areas went back to the nominal value after incorporating the proposed load shedding. In addition, Fig. 6.10 shows that the voltages at selected buses recovers after the disturbance as well. Therefore, the values of both system frequency and voltages achieve system stability.

6.7 Advantages of the Proposed WAUFLS Scheme

The results from the above analyses indicate that the approach of calculating a power mismatch during a disturbance has several advantages compared to the swing equation used in other schemes. These advantages include the following:

i. The calculated value of the power mismatch is trusted, regardless of the existence of FDI in the power flow measurements, because the proposed approach uses trusted system states to calculate it. In contrast, the calculated value using the swing equation could be inaccurate if there is an FDI on frequency measurements. Therefore, the proposed scheme is more robust against cyber attacks.

ii. The proposed mitigation scheme uses a PSSE-PF module, which gives real-time monitoring for the value of power mismatch due to the fact that PSSE is used in almost all recent control centers to provide real-time monitoring of the system based on the PMUs measurements that are being sent in high resolution. Nevertheless, because of the dynamic response of governors, turbines, loads and other control elements, the validity of the swing equation output is limited and considered only at the moment of disturbance [105].

iii. The proposed mitigation scheme uses only the frequency magnitude to detect disturbances, which means it can work with any frequency signal from the system. This is because the frequency magnitude at different points in the system is the same, with only the ROCOF changing from point to point, as shown in Fig. 3.4. Afterwards, it uses the system states, which are continuously available. The swing equation, on the

other hand, uses both ROCOF and the frequency of center of inertia (f_c) to calculate the mismatch. The accuracy of the f_c calculation depends on the number of available frequency measurements, with higher measurements being more accurate. Therefore, the proposed scheme is more reliable.

iv. The proposed approach is valid for large and small systems, whereas the approaches that use the swing equation are valid only for large systems. Following a large disturbance that includes tripping of the generators or large synchronous motors, the swing equation does not give accurate results because it depends on the inertia of the system. This can be approximated in large systems by assuming that most of the total inertia is still available. However, for small systems, an underestimation of the actual disturbance might result [102]. Therefore, the proposed scheme is more accurate for a wider range of system sizes.

v. The proposed scheme calculates the power mismatch, which is the amount of load to be shed directly, because it monitors the system online and runs power flow at every time step. On the other hand, the swing equation calculates the magnitude of disturbance, which still requires the control center operator to find and obtain information about the available spinning reserve in order for a decision to be made about the amount of load to be shed.

6.8 Summary

As a mitigation approach, a new WAUFLS scheme that works based on trusted measurements was proposed. A PSSE-PF module was used to calculate the total system mismatch. This module has two main components: the PSSE, which uses power flow measurements and calculates trusted system states, and the power flow, which utilizes these trusted states to determine the mismatch and hence the amount of load to be shed. Accordingly, the load shedding is distributed between the buses based on the proximity to the disturbance according to their voltage dip during the disturbance. The proposed scheme

was tested and validated under a range of system conditions. The results show that it is able to protect the system during under-frequency conditions, regardless of the existence of an FDI on system measurements. The results thus confirm the accuracy and reliability of the proposed scheme.

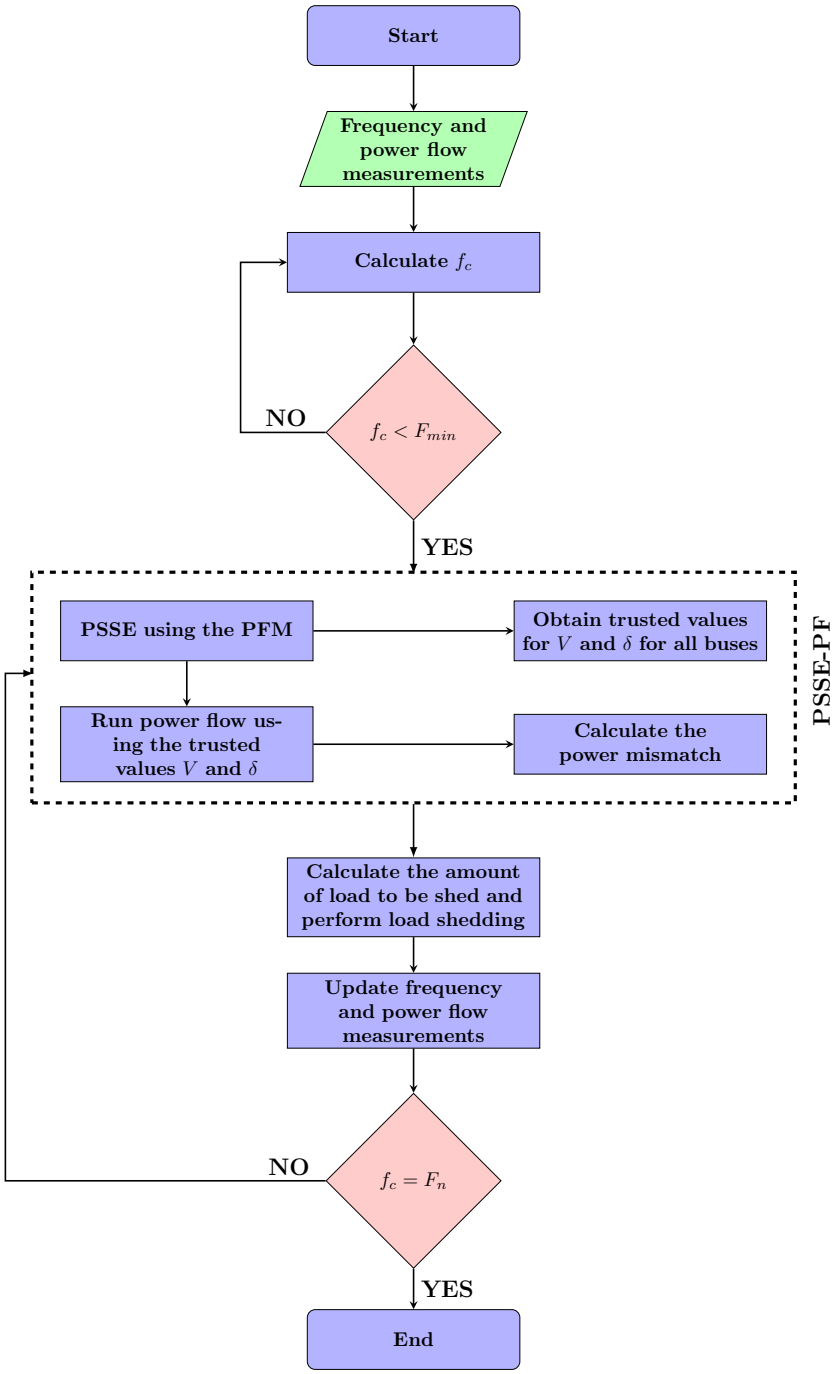


Figure 6.1: Flowchart of the proposed WAUFLS protection scheme

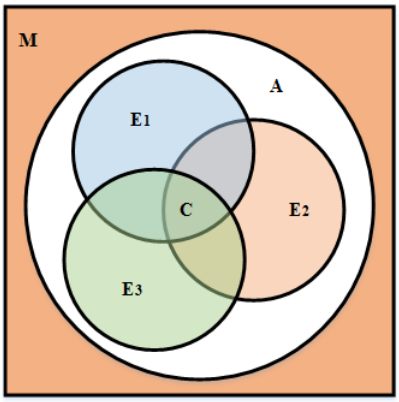


Figure 6.2: Measurements classification into three essential sets

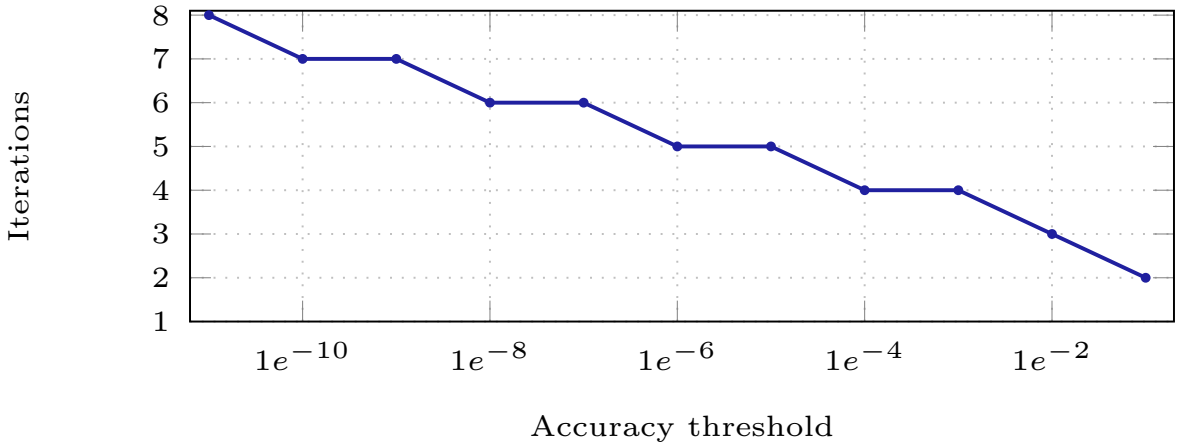


Figure 6.3: PSSE iterations for required accuracy

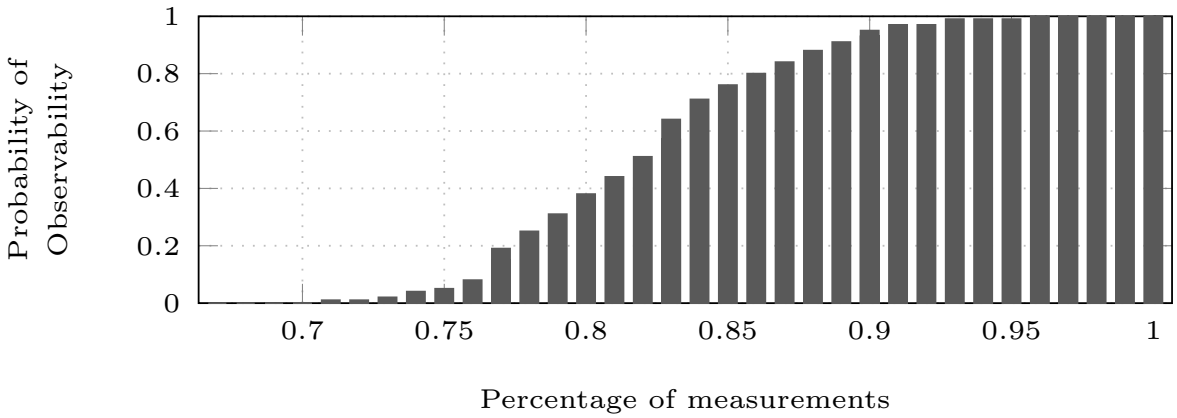


Figure 6.4: PSSE Observability

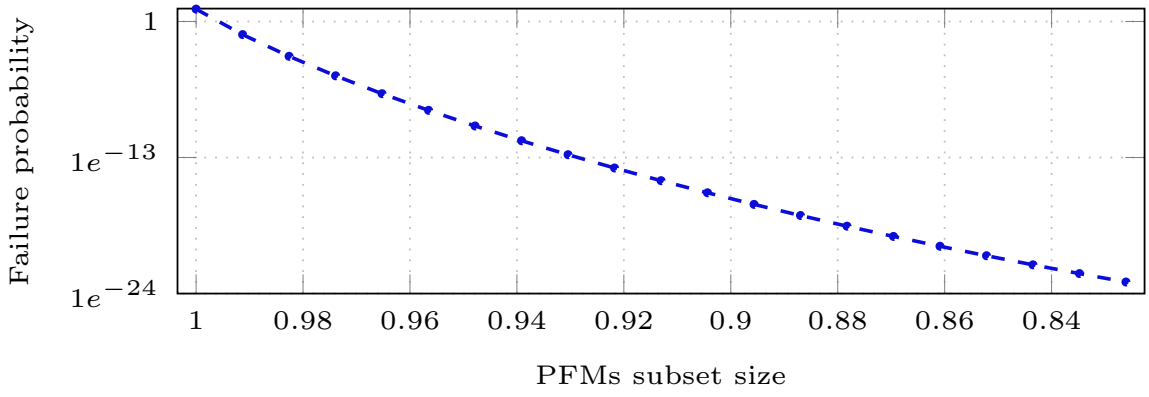
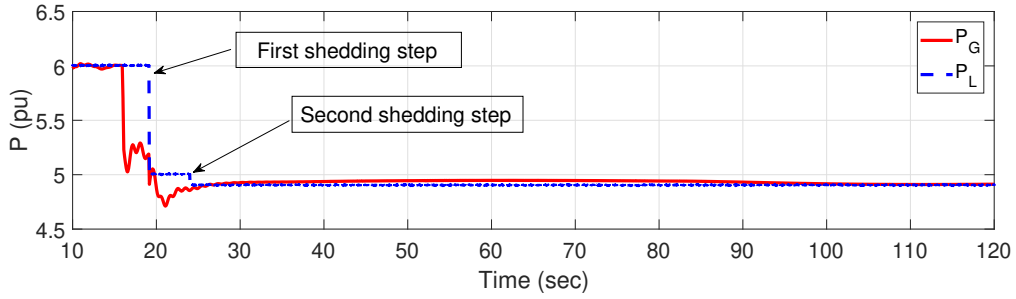
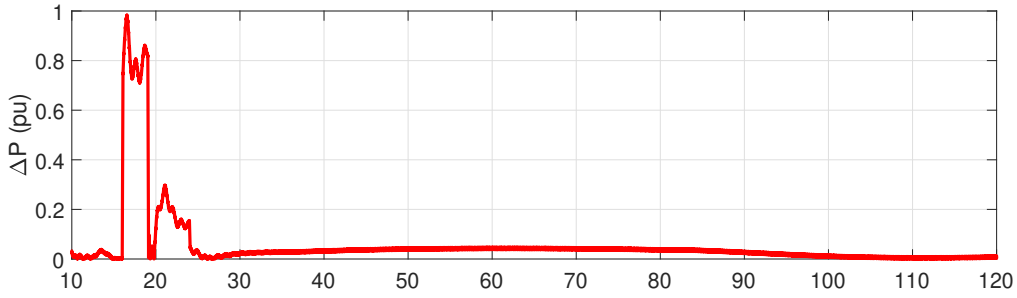


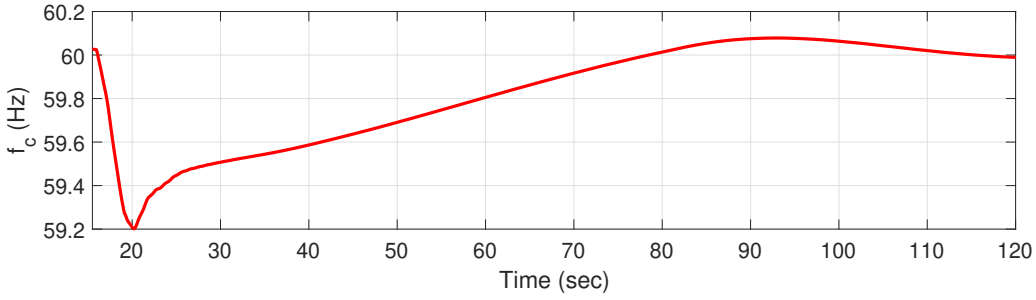
Figure 6.5: Failure probability of the mitigation scheme



(a) Power generation vs. load power



(b) Power mismatch



(c) Frequency of center of inertia

Figure 6.6: Load shedding after G1 tripping and the effects on power mismatch and frequency values

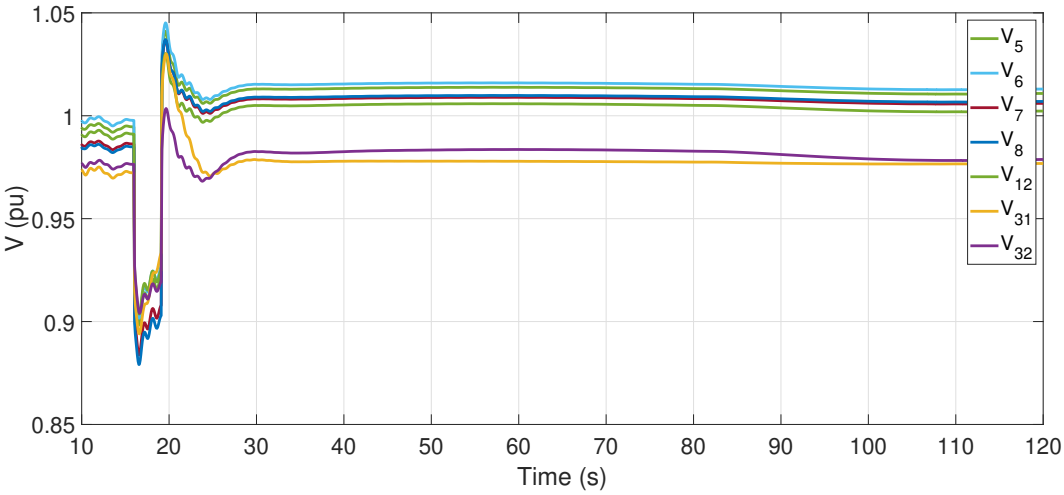
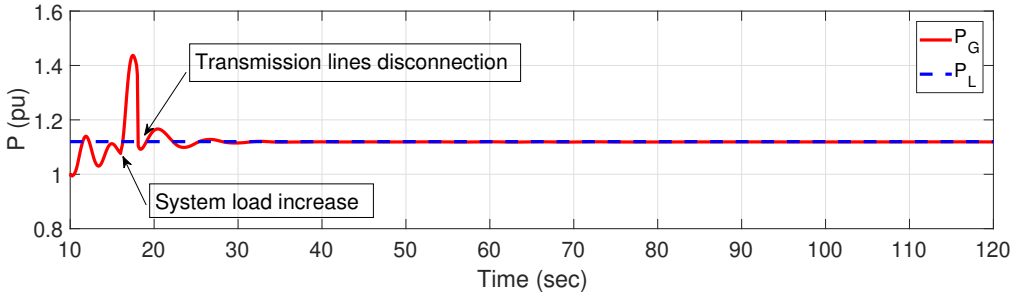
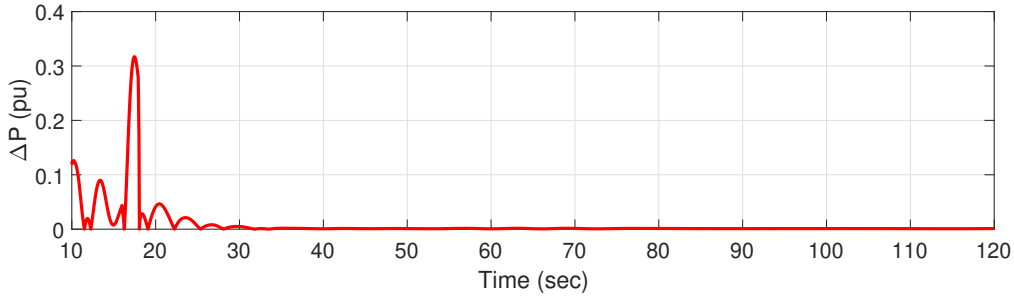


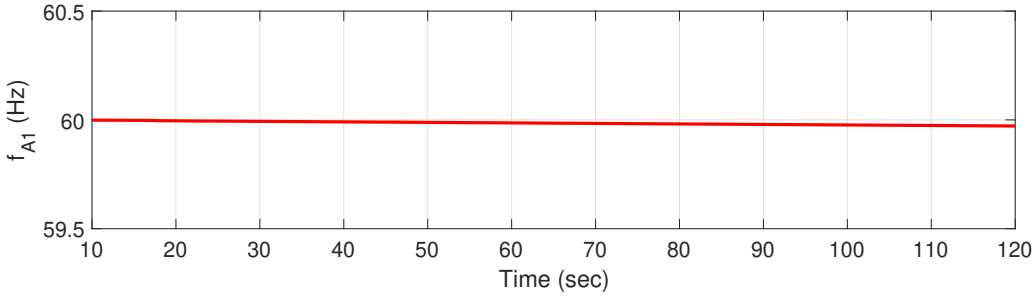
Figure 6.7: Voltage at selected buses



(a) Power generation vs. load power

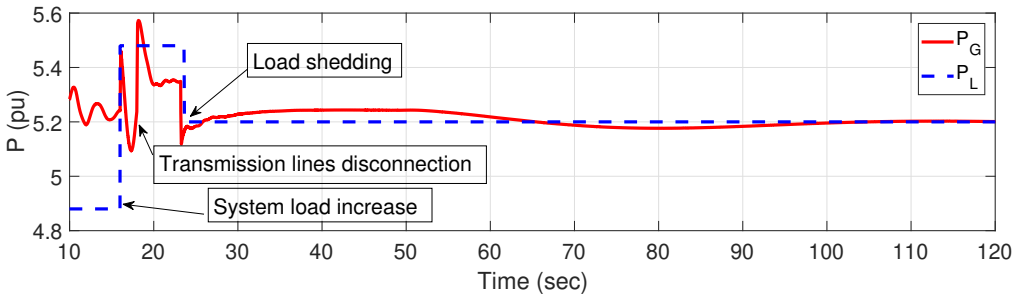


(b) Power mismatch

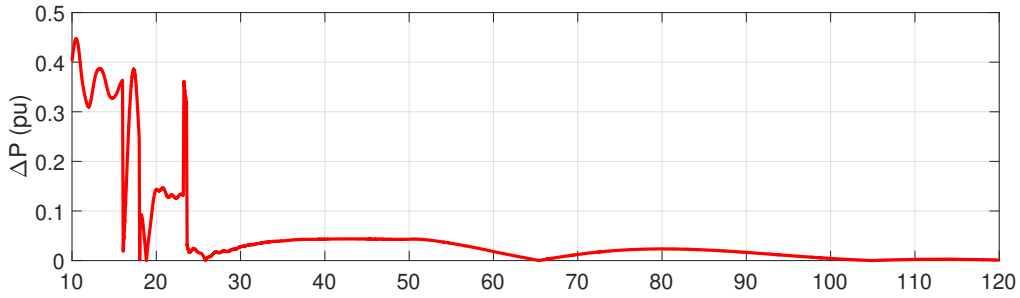


(c) Frequency of center of inertia

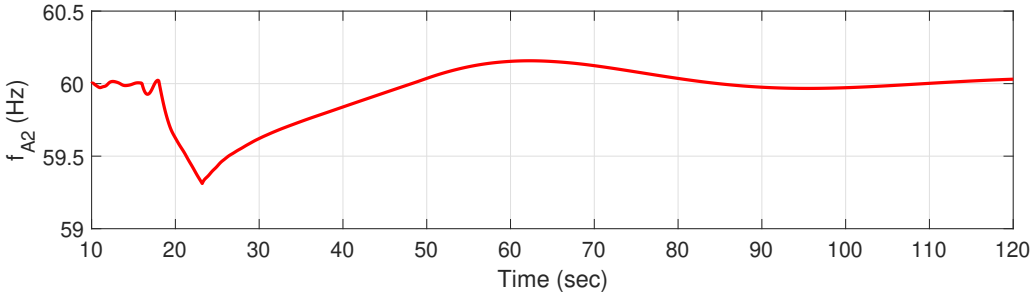
Figure 6.8: Power mismatch and frequency of Area 1



(a) Power generation vs. load power



(b) Power mismatch



(c) Frequency of center of inertia

Figure 6.9: Power mismatch and frequency of Area 2

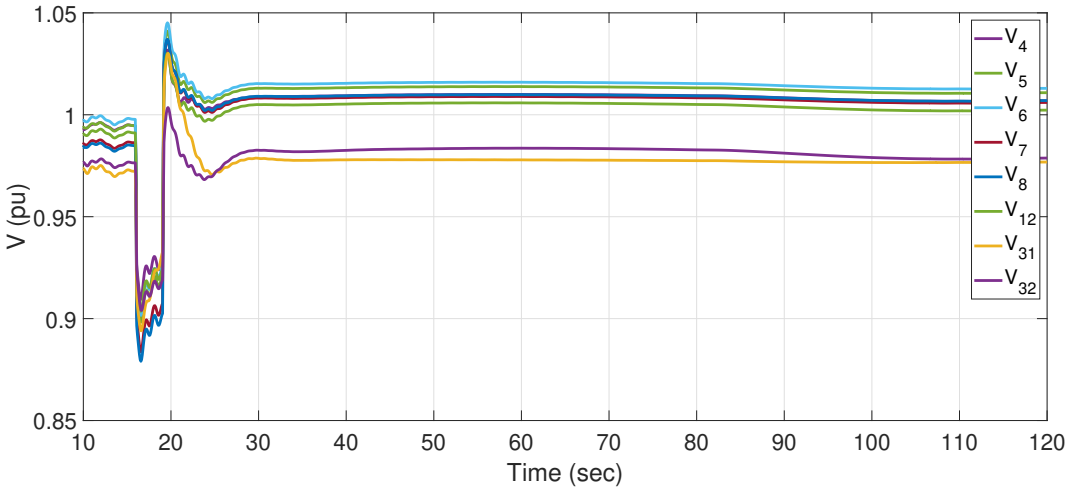


Figure 6.10: Voltage at selected buses for the islanding scenario

Chapter 7

Conclusions

7.1 Summary and Conclusions

Communication networks in smart grids are bringing increased connectivity to the energy industry, revolutionizing it in terms of reliability, performance, and manageability. This is accomplished by providing bidirectional communications to operate, monitor, and control power flow and measurements. However, communication networks also bring severe security vulnerabilities. Because of their critical nature and the significant socioeconomic impact of blackouts, smart grids can be a prime target for cyber terrorism. Cyber attacks present a real threat to WAMPAC schemes. While cryptographic authentication mechanisms, e.g., through the use of Message Authentication Codes (MAC), may enable us to detect malicious modifications to sensor measurements, they do not prevent attackers from modifying these data. Therefore, in smart grid applications that require real-time response, such as WAMPAC schemes, real-time mitigation for cyber attacks is still required after attack detection. The main contributions of this thesis can be summarized in the following points:

- The analysis presented in this work demonstrated that current wide-area frequency-related schemes are vulnerable to FDI attacks.

- The effect of FDI attacks on AGC systems as well as WAUFLS protection schemes was studied in detail. The problem formulation was driven mathematically and simulations of FDI scenarios on practical systems were tested.

- An approach to detect FDI attacks on AGC using the Kalman filter was proposed. System measurements were estimated using the filter and then compared with the received ones. The norm of the residual as well as a CUSUM were used to decide on the existence of an attack on the measurements. The results indicate that while the proposed approach can detect FDI instantaneously, it cannot mitigate its effect.

- An approach to jointly detect, estimate and compensate for FDI attacks against AGC systems was presented. The utilized input/state estimation-based algorithm considered the FDI as an unknown input and estimated its value accordingly. The estimated values for the FDI were then used to compensate for the effect of the attack in real time so that the AGC system could continue its operation under attack until the main reasons for the attack were eliminated. The simulation results confirm the effectiveness of the proposed approach against different types of FDI attacks.

- An RNN-based approach for detecting the FDI in AGC systems was also proposed that considered system nonlinearities. The RNN analyzed the sequential stream of signals and built a memory of previous system states to detect any anomalies or attacks on the signals. The results confirm RNN's ability to detect, classify and identify different types of attacks with high statistical measures within less than one second of the attack.

- A new mitigation scheme that works based on trusted measurements was proposed to mitigate the effect of FDI attacks on WAUFLS. A PSSE-PF module was used to calculate the total system mismatch. This module has two main components: the PSSE, which uses power flow measurements and calculates trusted system states, and the power flow, which utilizes these trusted states to determine the mismatch and hence the amount of load to be shed. The load-shedding is distributed between the buses based on the proximity to the disturbance, according to their voltage dip

during the disturbance. The proposed scheme was tested and validated under a range of system conditions. The results show that it is able to protect the system during under-frequency conditions, regardless of the existence of an FDI on system measurements. The results thus confirm the accuracy, speed, and reliability of the proposed scheme.

7.2 Directions for Future Work

More work can be done to address several key topics. These include novel methods for risk assessment that capture cyber attack threats and impacts, and attack detection and mitigation techniques that leverage cyber and physical properties of the grid without interfering with its critical energy delivery functions. There are several potential directions that could be pursued to extend the work discussed in this thesis. The following points can be considered for future research:

- In general, the effect of cyber attacks on other WAMPAC can be given more consideration. Since there is no general model that can represent the response of all WAMPAC schemes, each scheme or each group of similar schemes should be dealt with separately.
- The problem of cyber security of RAS schemes, including UVLS and OOS, should be investigated in detail. Attack models on these schemes should be studied and defense mechanisms should be proposed.

References

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

[2] Hassan Bevrani. *Robust power system frequency control*. Springer, 2014.

[3] Jaime De La Ree, Virgilio Centeno, James S Thorp, and Arun G Phadke. Synchronized phasor measurement applications in power systems. *IEEE Transactions on Smart Grid*, 1(1):20–27, 2010.

[4] Hamid Gharavi and Bin Hu. Synchrophasor sensor networks for grid communication and protection. *Proceedings of the IEEE*, 2017.

[5] Aditya Ashok, Manimaran Govindarasu, and Jianhui Wang. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the IEEE*, 2017.

[6] Göran N Ericsson. Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, 25(3):1501–1507, 2010.

[7] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[8] Aditya Ashok. Attack-resilient state estimation and testbed-based evaluation of cyber security for wide-area protection and control. 2017.

[9] Danda Rawat and Chandra Bajracharya. Cyber security for smart grid systems: Status, challenges and perspectives. In *SoutheastCon*, pages 1–6. IEEE, 2015.

[10] Yi Yang, Tim Littler, Sakir Sezer, Kieran McLaughlin, and HF Wang. Impact of cyber-security issues on smart grid. In *2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, pages 1–7. IEEE, 2011.

[11] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2012.

[12] Yaakov Katz. Stuxnet virus set back iran's nuclear program by 2 years. *Jerusalem Post*, 15, 2010.

[13] David Kushner. The real story of stuxnet. *IEEE Spectrum*, 50(3):48–53, 2013.

[14] Chih-Che Sun, Chen-Ching Liu, and Jing Xie. Cyber-physical system security of a power grid: State-of-the-art. *Electronics*, 5(3):40, 2016.

[15] Christopher J Baker. Cybersecurity for critical infrastructure. Technical report, Air Command And Staff College Maxwell Air Force Base United States, 2015.

[16] Energy Sector Control Systems Working Group et al. Roadmap to achieve energy delivery systems cyber security. *Energetics, Inc.*, 2011.

[17] Office of Electricity Delivery and Energy Reliability. Cyber security research, development and demonstration (RD&D) for energy delivery systems. 2011.

[18] Office of Electricity Delivery and Energy Reliability. Cybersecurity risk management process (RMP). 2011.

[19] North American Electricity Reliability Council (NERC). Critical infrastructure protection (CIP) reliability standards. 2009.

[20] National Institute of Standards and Technology (NIST). Nistir 7628: Guidelines for smart grid cyber security. 2010.

[21] What is the smart grid?

[22] Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah A Frincke. Smart-grid security issues. *IEEE Security & Privacy*, 8(1), 2010.

[23] Vasco Delgado-Gomes, João F Martins, Celson Lima, and Paul Nicolae Borza. Smart grid security issues. In *Compatibility and Power Electronics (CPE), 2015 9th International Conference on*, pages 534–538. IEEE, 2015.

[24] IH Lim, S Hong, MS Choi, SJ Lee, TW Kim, SW Lee, and BN Ha. Security protocols against cyber attacks in the distribution automation system. *IEEE Transactions on Power Delivery*, 25(1):448–455, 2010.

[25] Todd Mander, Lin Wang, Richard Cheung, and Farhad Nabhani. Adapting the pretty good privacy security style to power system distributed network protocol. In *Power Engineering, 2006 Large Engineering Systems Conference on*, pages 79–83. IEEE, 2006.

[26] Todd Mander, Farhad Nabhani, Lin Wang, and Richard Cheung. Integrated network security protocol layer for open-access power distribution systems. In *Power Engineering Society General Meeting, 2007. IEEE*, pages 1–8. IEEE, 2007.

[27] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4):1933–1954, 2014.

[28] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys and tutorials*, 14(4):998–1010, 2012.

[29] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[30] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[31] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE communications surveys & tutorials*, 15(1):5–20, 2013.

[32] Kishan Bhat, Vikram Sundarraj, Shravani Sinha, and Ankur Kaul. *IEEE cyber security for the smart grid*. IEEE, 2013.

[33] Salsabeel Shapsough, Fatma Qatan, Raafat Aburukba, Fadi Aloul, and AR Al Ali. Smart grid cyber security: Challenges and solutions. In *International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pages 170–175. IEEE, 2015.

[34] Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, and Chadi Assi. Communication security for smart grid distribution networks. *IEEE Communications Magazine*, 51(1):42–49, 2013.

[35] Teklemariam Tsegay Tesfay. Cybersecurity solutions for active power distribution networks. Technical report, EPFL, 2017.

[36] J. Kim and L. Tong. On topology attack of a smart grid: Undetectable attacks and countermeasures. *IEEE Journal on Selected Areas in Communications*, 31(7):1294–1305, July 2013.

[37] J. Kim, L. Tong, and R. J. Thomas. Data framing attack on state estimation. *IEEE Journal on Selected Areas in Communications*, 32(7):1460–1470, July 2014.

[38] S. Ntalampiras. Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling. *IEEE Transactions on Industrial Informatics*, 11(1):104–111, Feb 2015.

[39] Teklemariam Tsegay Tesfay, Jean-Pierre Hubaux, Jean-Yves Le Boudec, and Philippe Oechslin. Cyber-secure communication architecture for active power distribution networks. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, pages 545–552. ACM, 2014.

[40] Zhuo Lu, Wenye Wang, and Cliff Wang. From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. In *INFOCOM, 2011 Proceedings IEEE*, pages 1871–1879. IEEE, 2011.

[41] Upeka Kanchana Premaratne, Jagath Samarabandu, Tarlochan S Sidhu, Robert Beresh, and Jian-Cheng Tan. An intrusion detection system for iec61850 automated substations. *IEEE Transactions on Power Delivery*, 25(4):2376–2383, 2010.

[42] Dong Jin, David M Nicol, and Guanhua Yan. An event buffer flooding attack in dnp3 controlled scada systems. In *Simulation Conference (WSC), Proceedings of the 2011 Winter*, pages 2614–2626. IEEE, 2011.

[43] Chen-Ching Liu, Alexandru Stefanov, Junho Hong, and Patrick Panciatici. Intruders in the grid. *IEEE Power and Energy magazine*, 10(1):58–66, 2012.

[44] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[45] Gabriela Hug and Joseph Andrew Giampapa. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on Smart Grid*, 3(3):1362–1370, 2012.

[46] Ruilong Deng, Peng Zhuang, and Hao Liang. False data injection attacks against state estimation in power distribution systems. *IEEE Transactions on Smart Grid*, 2018.

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

[48] L. Xie, Y. Mo, and B. Sinopoli. Integrity data attacks in power market operations. *IEEE Transactions on Smart Grid*, 2(4):659–666, Dec 2011.

[49] Suzhi Bi and Ying Jun Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Transactions on Smart Grid*, 5(3):1216–1227, 2014.

[50] Suzhi Bi and Ying Jun Zhang. Using covert topological information for defense against malicious attacks on dc state estimation. *IEEE Journal on Selected Areas in Communications*, 32(7):1471–1485, 2014.

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

[52] Lorena Cazorla, Cristina Alcaraz, and Javier Lopez. Cyber stealth attacks in critical information infrastructures. *IEEE Systems Journal*, 2016.

[53] Rui Tan, Hoang Nguyen, Eddy Foo, David Yau, Zbigniew Kalbarczyk, Ravishankar Iyer, and Hoay Gooi. Modeling and mitigating impact of false data injection attacks on automatic generation control. *IEEE Transactions on Information Forensics and Security*, 12(7):1609–1624, 2017.

[54] Y Mo and B Sinopoli. False data injection attacks in cyber physical systems. In *First Workshop on Secure Control Systems*, 2010.

[55] Kebina Manandhar, Xiaojun Cao, Fei Hu, and Yao Liu. Combating false data injection attacks in smart grid using kalman filter. In *International Conference on Computing, Networking and Communications (ICNC)*, pages 16–20. IEEE, 2014.

[56] Kebina Manandhar, Xiaojun Cao, Fei Hu, and Yao Liu. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE transactions on control of network systems*, 1(4):370–379, 2014.

[57] Danda B Rawat and Chandra Bajracharya. Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Processing Letters*, 22(10):1652–1656, 2015.

[58] Shang Li, Yasin Yılmaz, and Xiaodong Wang. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Transactions on Smart Grid*, 6(6):2725–2735, 2015.

[59] Yi Huang, Jin Tang, Yu Cheng, Husheng Li, Kristy Campbell, and Zhu Han. Real-time detection of false data injection in smart grid networks: an adaptive cusum method and analysis. *IEEE Systems Journal*, 10(2):532–543, 2016.

[60] Ali Abur and Antonio Gomez Exposito. *Power system state estimation: theory and implementation*. CRC press, 2004.

[61] Arun G Phadke and John Samuel Thorp. *Synchronized phasor measurements and their applications*, volume 1. Springer, 2008.

[62] Neelabh Kashyap, Stefan Werner, Yih-Fang Huang, and Taneli Riihonen. Power system state estimation under incomplete pmu observability—a reduced-order approach. *IEEE Journal of Selected Topics in Signal Processing*, 8(6):1051–1062, 2014.

[63] Junbo Zhao, Gexiang Zhang, Kaushik Das, George N Korres, Nikolaos M Manousakis, Avinash K Sinha, and Zhengyou He. Power system real-time monitoring by using pmu-based robust state estimation method. *IEEE Transactions on Smart Grid*, 7(1):300–309, 2015.

[64] 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*, 3(3):1362–1370, Sep. 2012.

[65] Hadi Saadat. *Power system analysis*. WCB/McGraw-Hill, 1999.

[66] Kaveh Rahimi, Abhineet Parchure, Virgilio Centeno, and Robert Broadwater. Effect of communication time-delay attacks on the performance of automatic generation

control. In *North American Power Symposium (NAPS), 2015*, pages 1–6. IEEE, 2015.

[67] Maria Vrakopoulou, Peyman Mohajerin Esfahani, Kostas Margellos, John Lygeros, and Göran Andersson. Cyber-attacks in the automatic generation control. In *Cyber Physical Systems Approach to Smart Electric Power Grid*, pages 303–328. Springer, 2015.

[68] Rui Tan, Hoang Hai Nguyen, Eddy Foo, Xinshu Dong, David KY Yau, Zbigniew Kalbarczyk, Ravishankar K Iyer, and Hoay Beng Gooi. Optimal false data injection attack against automatic generation control in power grids. In *Proceedings of the 7th International Conference on Cyber-Physical Systems*, page 2. IEEE Press, 2016.

[69] Peyman Esfahani, Maria Vrakopoulou, Kostas Margellos, John Lygeros, and Göran Andersson. Cyber attack in a two-area power system: Impact identification using reachability. In *American Control Conference (ACC)*, pages 962–967. IEEE, 2010.

[70] Peyman Esfahani, Maria Vrakopoulou, Kostas Margellos, John Lygeros, and Göran Andersson. A robust policy for automatic generation control cyber attack in two area power network. In *49th IEEE Conference on Decision and Control (CDC)*, pages 5973–5978. IEEE, 2010.

[71] Arman Sargolzaei, Kang K Yen, and Mohamed N Abdelghani. Preventing time-delay switch attack on load frequency control in distributed power systems. *IEEE Transactions on Smart Grid*, 7(2):1176–1185, 2016.

[72] Aditya Ashok, Pengyuan Wang, Matthew Brown, and Manimaran Govindarasu. Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed. In *Power & Energy Society General Meeting*, pages 1–5. IEEE, 2015.

[73] Saroj Biswas and Arif Sarwat. Vulnerabilities in two-area automatic generation control systems under cyberattack. In *Resilience Week (RWS), 2016*, pages 40–45. IEEE, 2016.

[74] Mehedi Hassan, NK Roy, and Md Sahabuddin. Mitigation of frequency disturbance in power systems during cyber-attack. In *International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE)*, pages 1–4. IEEE, 2016.

[75] Chunyu Chen, Kaifeng Zhang, Kun Yuan, Lingzhi Zhu, and Minhui Qian. Novel detection scheme design considering cyber attacks on load frequency control. *IEEE Transactions on Industrial Informatics*, 2017.

[76] Alireza Abbaspour, Arman Sargolzaei, and Kang Yen. Detection of false data injection attack on load frequency control in distributed power systems. In *Power Symposium (NAPS), 2017 North American*, pages 1–6. IEEE, 2017.

[77] Mostafa Mohammadpourfard, Ashkan Sami, and Yang Weng. Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations. *IEEE Transactions on Sustainable Energy*, 2017.

[78] Mohsen Khalaf, Amr Youssef, and Ehab El-Saadany. Detection of false data injection in automatic generation control systems using kalman filter. In *Electrical Power and Energy Conference (EPEC17)*, pages 343–348, Saskatoon, Canada, October 2017. IEEE.

[79] Amir Ameli, Ali Hooshyar, Ehab El-Saadany, and Amr Youssef. Attack detection and identification for automatic generation control systems. *IEEE Transactions on Power Systems*, 2018.

[80] Siddharth Sridhar and Manimaran Govindarasu. Model-based attack detection and mitigation for automatic generation control. *IEEE Transactions on Smart Grid*, 5(2):580–591, 2014.

[81] Yee Wei Law, Tansu Alpcan, and Marimuthu Palaniswami. Security games for risk minimization in automatic generation control. *IEEE Transactions on Power Systems*, 30(1):223–232, 2015.

[82] Arman Sargolzaei, Alireza Abbaspour, Mohammad Abdullah Al Faruque, Anas Salah Eddin, and Kang Yen. Security challenges of networked control systems. In *Sustainable Interdependent Networks*, pages 77–95. Springer, 2018.

[83] Ruilong Deng, Gaoxi Xiao, Rongxing Lu, Hao Liang, and Athanasios V Vasilakos. False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. *IEEE Transactions on Industrial Informatics*, 13(2):411–423, 2016.

[84] 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)*, pages 1–5, Feb 2018.

[85] JQ James, Yunhe Hou, and Victor OK Li. Online false data injection attack detection with wavelet transform and deep neural networks. *IEEE Transactions on Industrial Informatics*, 14(7):3271–3280, 2018.

[86] Xinyu Wang, Xiaoyuan Luo, Yuyan Zhang, and Xinping Guan. Detection and isolation of false data injection attacks in smart grids via nonlinear interval observer. *IEEE Internet of Things Journal*, 2019.

[87] Boda Li, Tao Ding, Can Huang, Jubo Zhao, Yongheng Yang, and Ying Chen. Detecting false data injection attacks against power system state estimation with fast go-decomposition (godec) approach. *IEEE Trans. Ind. Inform.*, 2018.

[88] Rakesh B Bobba, Katherine M Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt, and Thomas J Overbye. Detecting false data injection attacks on dc state estimation. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, volume 2010, 2010.

[89] Gyorgy Dan and Henrik Sandberg. Stealth attacks and protection schemes for state estimators in power systems. In *2010 First IEEE International Conference on Smart Grid Communications*, pages 214–219. IEEE, 2010.

[90] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Malicious data attacks on the smart grid. *IEEE Transactions on Smart Grid*, 2(4):645–658, 2011.

[91] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Limiting false data attacks on power system state estimation. In *2010 44th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6. IEEE, 2010.

[92] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *2010 First IEEE International Conference on Smart Grid Communications*, pages 220–225. IEEE, 2010.

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

[94] Annarita Giani, Eilyan Bitar, Manuel Garcia, Miles McQueen, Pramod Khargonekar, and Kameshwar Poolla. Smart grid data integrity attacks. *IEEE Transactions on Smart Grid*, 4(3):1244–1253, 2013.

[95] Annarita Giani, Eilyan Bitar, Manuel Garcia, Miles McQueen, Pramod Khargonekar, and Kameshwar Poolla. Smart grid data integrity attacks: characterizations and countermeasures π. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 232–237. IEEE, 2011.

[96] Suzhi Bi and Ying Jun Zhang. Defending mechanisms against false-data injection attacks in the power system state estimation. In *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, pages 1162–1167. IEEE, 2011.

[97] Suzhi Bi and Ying Jun Zhang. Mitigating false-data injection attacks on dc state estimation using covert topological information. In *2013 IEEE Global Communications Conference (GLOBECOM)*, pages 766–771. IEEE, 2013.

[98] Aditya Ashok, Adam Hahn, and Manimaran Govindarasu. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *Journal of advanced research*, 5(4):481–489, 2014.

[99] Jie Duan and Mo-Yuen Chow. Data integrity attack on consensus-based load shedding algorithm for power systems. In *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*, pages 7641–7646. IEEE, 2017.

[100] Jian Xiao, Fushuan Wen, CY Chung, and KP Wong. Wide-area protection and its applications-a bibliographical survey. 2006.

[101] Under frequency load shedding, NERC.

[102] B Delfino, S Massucco, A Morini, P Scalera, and F Silvestro. Implementation and comparison of different under frequency load-shedding schemes. In *Power Engineering Society Summer Meeting, 2001*, volume 1, pages 307–312. IEEE, 2001.

[103] Sohrab Banijamali and Turaj Amraee. Semi adaptive setting of under frequency load shedding relays considering credible generation outage scenarios. *IEEE Transactions on Power Delivery*, 2018.

[104] K Seethalekshmi, Sri Niwas Singh, and Suresh C Srivastava. A synchrophasor assisted frequency and voltage stability based load shedding scheme for self-healing of power system. *IEEE Transactions on Smart Grid*, 2(2):221–230, 2011.

[105] Vladimir V Terzija. Adaptive underfrequency load shedding based on the magnitude of the disturbance estimation. *IEEE Transactions on Power Systems*, 21(3):1260–1266, 2006.

[106] Urban Rudez and Rafael Mihalic. Wams-based underfrequency load shedding with short-term frequency prediction. *IEEE Transactions on Power Delivery*, 31(4):1912–1920, 2016.

[107] M Sanaye Pasand and H Seyedi. New centralized adaptive under frequency load shedding algorithms. In *Power Engineering, 2007 Large Engineering Systems Conference on*, pages 44–48. IEEE, 2007.

[108] M Karimi, P Wall, H Mokhlis, and V Terzija. A new centralized adaptive underfrequency load shedding controller for microgrids based on a distribution state estimator. *IEEE Transactions on Power Delivery*, 32(1):370–380, 2017.

[109] H Seyedi and M Sanaye-Pasand. New centralised adaptive load-shedding algorithms to mitigate power system blackouts. *IET generation, transmission & distribution*, 3(1):99–114, 2009.

[110] Mauricio Gadelha da Silveira and Paulo Henrique Franco. Iec 61850 network cybersecurity: Mitigating goose message vulnerabilities. 2019.

[111] Muhammad Talha Abdul Rashid, Salman Yussof, Yunus Yusoff, and Roslan Ismail. A review of security attacks on iec61850 substation automation system network. In *Proceedings of the 6th International Conference on Information Technology and Multimedia*, pages 5–10. IEEE, 2014.

[112] Maëlle Kabir-Querrec, Stéphane Mocanu, Jean-Marc Thiriet, and Eric 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)*, pages 1–4. IEEE, 2016.

[113] Pingkang Li, Xiuxia Du, and Nan Duan. Closed loop identification for multi-area agc systems with power plant time delay dynamics. In *International Conference on Power System Technology*, pages 1–8, Chongqing, China, 2006. IEEE.

[114] Mohsen Khalaf, Ali Hooshyar, and Ehab El-Saadany. On false data injection in wide area protection schemes. In *2018 IEEE Power & Energy Society General Meeting (PESGM)*, pages 1–5. IEEE, 2018.

[115] Jafar Jallad, Saad Mekhilef, Hazlie Mokhlis, and Javed Ahmad Laghari. Improved ufls with consideration of power deficit during shedding process and flexible load selection. *IET Renewable Power Generation*, 12(5):565–575, 2018.

[116] Tohid Shekari, Farrokh Aminifar, and Majid Sanaye-Pasand. An analytical adaptive load shedding scheme against severe combinational disturbances. *IEEE Transactions on Power Systems*, 31(5):4135–4143, 2015.

[117] Alireza Saffarian and Majid Sanaye-Pasand. Enhancement of power system stability using adaptive combinational load shedding methods. *IEEE Transactions on Power Systems*, 26(3):1010–1020, 2010.

[118] Moein Abedini, Majid Sanaye-Pasand, and Sadegh Azizi. Adaptive load shedding scheme to preserve the power system stability following large disturbances. *IET Generation, Transmission & Distribution*, 8(12):2124–2133, 2014.

[119] Ahmed M Khalil and Reza Iravani. A dynamic coherency identification method based on frequency deviation signals. *IEEE Transactions on Power Systems*, 31(3):1779–1787, 2016.

[120] Mohinder Grewal and Angus Andrews. *Kalman Filtering: Theory and Practice using MATLAB*. John Wiley and Sons, Inc., 2001.

[121] Kebina Manandhar, Xiaojun Cao, and Fei Hu. Attack detection in water supply systems using Kalman filter estimator. In *35th Sarnoff Symposium (SARNOFF)*, pages 1–6. IEEE, 2012.

[122] Michèle Basseville and Igor Nikiforov. *Detection of abrupt changes: theory and application*, volume 104. Prentice Hall Englewood Cliffs, 1993.

[123] David Urbina, Jairo Giraldo, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Nils Tippenhauer, Justin Ruths, Richard Candell, and Henrik Sandberg. *Survey and new directions for physics-based attack detection in control systems*. US Department of Commerce, National Institute of Standards and Technology, 2016.

[124] Sze Yong, Minghui Zhu, and Emilio Frazzoli. Simultaneous input and state estimation for linear discrete-time stochastic systems with direct feedthrough. In *52nd Annual Conference on Decision and Control (CDC)*, pages 7034–7039. IEEE, 2013.

[125] Sze Yong, Minghui Zhu, and Emilio Frazzoli. A unified filter for simultaneous input and state estimation of linear discrete-time stochastic systems. *Automatica*, 63:321–329, 2016.

[126] Elyas Rakhshani, Daniel Remon, Antoni Mir Cantarellas, Jorge Martinez Garcia, and Pedro Rodriguez. Virtual synchronous power strategy for multiple hvdc interconnections of multi-area agc power systems. *IEEE Transactions on Power Systems*, 32(3):1665–1677, 2017.

[127] Elyas Rakhshani and Pedro Rodriguez. Active power and frequency control considering large-scale res. In *Large Scale Renewable Power Generation*, pages 233–271. Springer, 2014.

[128] Sze Zheng Yong. *Control and estimation of hidden mode hybrid systems with applications to autonomous systems*. PhD thesis, Massachusetts Institute of Technology, 2016.

[129] Ignacio Egido, Fidel Fernández-Bernal, Luis Rouco, Eloisa Porras, and Ángel Sáiz-Chicharro. Modeling of thermal generating units for automatic generation control purposes. *IEEE transactions on control systems technology*, 12(1):205–210, 2004.

[130] H Golpira and H Bevrani. Application of ga optimization for automatic generation control design in an interconnected power system. *Energy Conversion and Management*, 52(5):2247–2255, 2011.

[131] Gaddam Mallesham and Akula Rajani. Automatic generation control using fuzzy logic. In *Proc. of 8th International Conference on Development and Application Systems, Suceava, Romania*, pages 128–137, 2006.

[132] Tomáš Mikolov, Martin Karafiát, Lukáš Burget, Jan Černockỳ, and Sanjeev Khudanpur. Recurrent neural network based language model. In *Eleventh Annual Conference of the International Speech Communication Association*, 2010.

[133] Ronald J Williams and David Zipser. A learning algorithm for continually running fully recurrent neural networks. *Neural computation*, 1(2):270–280, 1989.

[134] John A Hertz, Anders S Krogh, and Richard G Palmer. *Introduction to the theory of neural computation*, volume 1. Basic Books, 1991.

[135] Senlin Zhang, Yixing Wang, Meiqin Liu, and Zhejing Bao. Data-based line trip fault prediction in power systems using lstm networks and svm. *IEEE Access*, 2017.

[136] François Chollet et al. Keras. https://keras.io, 2015.

[137] Fazle Karim, Somshubra Majumdar, Houshang Darabi, and Shun Chen. Lstm fully convolutional networks for time series classification. *arXiv preprint arXiv:1709.05206*, 2017.

[138] MS Sachdev and TKP Medicherla. A second order load flow technique. *IEEE Transactions on Power Apparatus and Systems*, 96(1):189–197, 1977.

[139] K Seethalekshmi, SN Singh, and SC Srivastava. Wams assisted frequency and voltage stability based adaptive load shedding scheme. In *2009 IEEE Power & Energy Society General Meeting*, pages 1–8. IEEE, 2009.

[140] MA Pai. *Energy function analysis for power system stability*. Springer Science & Business Media, 2012.

APPENDICES

Appendix A

Data of the AGC Systems

A.1 Parameters of the Two-Area System

Table A.1 shows the different parameters of the two-area AGC system used throughout this work. These data are obtained from [65].

Table A.1: Parameters of the Two-Area System

Parameters	**Area 1**	**Area 2**
D_i (pu/Hz)	0.6	0.3
H_i (sec)	5	4
R_i (Rad/pu)	0.05	0.0625
K_{Ii}	0.3	0.3
T_{Ti} (sec)	0.5	0.6
T_{gi} (sec)	0.2	0.3

A.2 Parameters of the Four-Area System

The 12-bus four-area (Fig 4.10) system used in this study is a practical system from North America. The parameters for each area are taken from [126] and are summarized in Table A.2.

Table A.2: Parameters of the Four-Area System

Parameters	**Area 1**	**Area 2**	**Area 3**	**Area 4**
K_{pi} (rad/puMW)	76	141.7	139.6	114.2
T_{pi} (sec)	14.4	19.1	9.39	9.12
R_i (Hz/pu)	3	3	3	3
B_i (pu/Hz)	0.416	0.377	0.378	0.388
K_{Ii}	0.131	0.131	0.131	0.131
T_{TGi} (sec)	0.38	0.38	0.38	0.38

Appendix B

Data of the IEEE 14-Bus System

Table B.1: Bus Data

Bus	**Type (0=P-Q) (1=P-V)**	**Volts**	**Load P+jQ**	**Gen P+jQ**
1	1	1.06	0	114.14-j16.9
2	1	1.045	21.7+j12.7	40
3	1	1.01	94.2+j19	0
4	0	–	47.8+j4	0
5	0	–	7.6+j1.6	0
6	1	1.07	11.2+j7.5	0
7	1	1.09	0	0
8	0	–	29.5+j16.6	0
9	0	–	9+j5.8	0
10	0	–	3.5+j1.8	0
11	0	–	6.1+j1.6	0
12	0	–	13.5+j5.8	0
13	0	–	14.9+j5	0

Table B.2: Line Data

Bus #		R	X	B	Taps	
From	To				Mag.	Ang.
1	2	0.01938	0.05917	0.02640	0	0
1	5	0.05403	0.22304	0.02190	0	0
2	3	0.04699	0.19797	0.01870	0	0
2	4	0.05811	0.17632	0.02460	0	0
2	5	0.05695	0.17388	0.01700	0	0
3	4	0.06701	0.17103	0.01730	0	0
4	5	0.01335	0.04211	0.00640	0	0
4	8	0	0.55618	0	0.969	0
5	6	0	0.25202	0	0.932	0
6	10	0.09498	0.1989	0	0	0
6	11	0.12291	0.25581	0	0	0
6	12	0.06615	0.13027	0	0	0
8	9	0.03181	0.0845	0	0	0
8	13	0.12711	0.27038	0	0	0
9	10	0.08205	0.19207	0	0	0
11	12	0.22092	0.19988	0	0	0
12	13	0.17093	0.34802	0	0	0

Table B.3: Detailed Model Unit Data

Unit #	H (sec)	R_a	x'_d	x'_q	x_d	x_q	T'_{do}	T'_{qo}	x_l
1	10.296	0	0.2995	0.646	0.8979	0.646	7.4	0	0.2396
2	13.08	0.0031	0.185	0.36	1.05	0.98	6.1	0.3	0
3	13.08	0.0031	0.185	0.36	1.05	0.98	6.1	0.3	0
4	10.12	0.0014	0.232	0.715	1.25	1.22	4.75	1.5	0.134
5	10.12	0.0014	0.232	0.715	1.25	1.22	4.75	1.5	0.134

Table B.4: Detailed Model Unit Excitation System Data

Unit #	K_A	T_A	V_{RMIN}	V_{RMAX}	T_r	T_E	K_F	T_F	A_e	B_e
1	300	0.02	0	7.32	0.001	0.2	0.002	1	0.0006	0.9
2	20	0.02	0	4.38	0.001	1.98	0.001	1	0.0006	0.9
3	20	0.02	0	4.38	0.001	1.98	0.001	1	0.0006	0.9
4	20	0.02	1.395	6.81	0.001	0.7	0.001	1	0.0006	0.9
5	20	0.02	1.395	6.81	0.001	0.7	0.001	1	0.0006	0.9

Appendix C

Data of the IEEE 39-Bus System

The single line diagram, bus data, line, generator and excitation system data are given in the following pages. Data for the detailed model of the system are taken from [140]

Table C.1: Bus Data

Bus	**Type (0=P-Q) (1=P-V)**	**Volts**	**Load P+jQ**	**Gen P+jQ**
1	0	–	0	0
2	0	–	0	0
3	0	–	322+j2.4	0
4	0	–	500+j184	0
5	0	–	0	0
6	0	–	0	0
7	0	–	233.8+j84	0
8	0	–	522+j176	0
9	0	–	0	0
10	0	–	0	0
11	0	–	0	0

12	0	–	7.5+j88	0
13	0	–	0	0
14	0	–	0	0
15	0	–	320+j153	0
16	0	–	329+j32.3	0
17	0	–	0	0
18	0	–	158+j30	0
19	0	–	0	0
20	0	–	628+j103	0
21	0	–	274+j115	0
22	0	–	0	0
23	0	–	247.5+j84.6	0
24	0	–	308.6-j92.2	0
25	0	–	224+j47.2	0
26	0	–	139+j17	0
27	0	–	281+j75.5	0
28	0	–	206+j27.6	0
29	0	–	283.5+j26.9	0
30	1	1.0475	0	250+j0
31	1	0.982	9.2+j4.6	–
32	1	0.9831	0	650+j0
33	1	0.9972	0	632+j0
34	1	1.0123	0	508+j0
35	1	1.0493	0	650+j0
36	1	1.0635	0	560+j0
37	1	1.0278	0	540+j0
38	1	1.0265	0	830+j0
39	1	1.03	1104+j250	1000+j0

Table C.2: Line Data

Bus #		R	X	B	Taps	
From	**To**				**Mag.**	**Ang.**
1	2	.0035	.0411	.6987	0	0
1	39	.0010	.0250	.7500	0	0
2	3	.0013	.0151	.2572	0	0
2	25	.0070	.0086	.1460	0	0
3	4	.0013	.0213	.2214	0	0
3	18	.0011	.0133	.2138	0	0
4	5	.0008	.0128	.1342	0	0
4	14	.0008	.0129	.1382	0	0
5	6	.0002	.0026	.0434	0	0
5	8	.0008	.0112	.1476	0	0
6	7	.0006	.0092	.1130	0	0
6	11	.0007	.0082	.1389	0	0
7	8	.0004	.0046	.0780	0	0
8	9	.0023	.0363	.3804	0	0
9	39	.0010	.0250	1.2000	0	0
10	11	.0004	.0043	.0729	0	0
10	13	.0004	.0043	.0729	0	0
13	14	.0009	.0101	.1723	0	0
14	15	.0018	.0217	.3660	0	0
15	16	.0009	.0094	.1710	0	0
16	17	.0007	.0089	.1342	0	0
16	19	.0016	.0195	.3040	0	0
16	21	.0008	.0135	.2548	0	0
16	24	.0003	.0059	.0680	0	0
17	18	.0007	.0082	.1319	0	0
17	27	.0013	.0173	.3216	0	0

21	22	.0008	.0140	.2565	0	0
22	23	.0006	.0096	.1846	0	0
23	24	.0022	.0350	.3610	0	0
25	26	.0032	.0323	.5130	0	0
26	27	.0014	.0147	.2396	0	0
26	28	.0043	.0474	.7802	0	0
26	29	.0057	.0625	1.029	0	0
28	29	.0014	.0151	.2490	0	0
12	11	.0016	.0435	0	1.006	0
12	13	.0016	.0435	0	1.006	0
6	31	.0000	.0250	0	1.070	0
10	32	.0000	.0200	0	1.070	0
19	33	.0007	.0142	0	1.070	0
20	34	.0009	.0180	0	1.009	0
22	35	.0000	.0143	0	1.025	0
23	36	.0005	.0272	0	1	0
25	37	.0006	.0232	0	1.025	0
2	30	0	.0181	0	1.025	0
29	38	.0008	.0156	0	1.025	0
19	20	.0007	.0138	0	1.060	0

NOTE: The parameters of the block diagram in Fig. C.1 are computed as follows:

$$EX_2 = \frac{V_{RMAX}}{K_E + C2} \tag{C.1}$$

$$EX_1 = 0.75EX_2 \tag{C.2}$$

$$S_E = Ae^{BE_f} \tag{C.3}$$

Table C.3: Detailed Model Unit Data

Unit #	**H (sec)**	R_a	x'_d	x'_q	x_d	x_q	T'_{do}	T'_{qo}	x_l
1	500.0	0	.006	.008	.02	.019	7.0	.7	.003
2	30.3	0	.0697	.170	.295	.282	6.56	1.5	.035
3	35.8	0	.0531	.0876	.2495	.237	5.7	1.5	.0304
4	28.6	0	.0436	.166	.262	.258	5.69	1.5	.0295
5	26.0	0	.132	.166	.67	.62	5.4	.44	.054
6	34.8	0	.05	.0814	.254	.241	7.3	.4	.0224
7	26.4	0	.049	.186	.295	.292	5.66	1.5	.0322
8	24.3	0	.057	.0911	.290	.280	6.7	.41	.028
9	34.5	0	.057	.0587	.2106	.205	4.79	1.96	.0298
10	42.0	0	.031	.008	.1	.069	10.2	.0	.0125

$$B = \ln \frac{C2/C1}{EX_2 - EX_1} \tag{C.4}$$

$$A = \frac{C2}{e^{B*EX_2}} \tag{C.5}$$

Unit # 1 has constant excitation.

Table C.4: Detailed Model Unit Excitation System Data

Unit #	K_A	T_A	V_{RMIN}	V_{RMAX}	K_E	T_E	K_F	T_F	**C1**	**C2**
1	0	0	0	0	0	0	0	0	0	0
2	6.2	.05	-1.	1.0	-.633	.405	.057	.5	.66	.88
3	5.0	.06	-1.	1.0	-.0198	.5	.08	1.0	.13	.34
4	5.0	.06	-1.	1.0	-.0525	.5	.08	1.0	.08	.314
5	40.0	.02	-10.0	10.0	1.0	.785	.03	1.0	.07	.91
6	5.0	.02	-1.	1.0	-.0419	.471	.0754	1.246	.064	.251
7	40.0	.02	-6.5	6.5	1.0	.73	.03	1.0	.53	.74
8	5.0	.02	-1.0	1.0	-.047	.528	.0854	1.26	.072	.282
9	40.0	.02	-10.5	10.5	1.0	1.4	.03	1.0	.62	.85
10	5.0	.06	-1.	1.0	-.0485	.25	.04	1	.08	.26

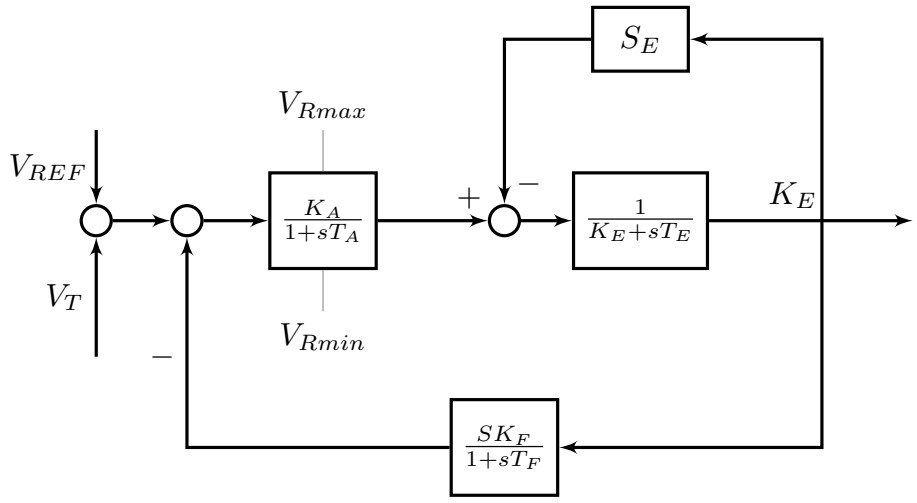


Figure C.1: IEEE Type 1 rotating excitation system model