

**DETECTION OF FALSE DATA INJECTION
ATTACKS AGAINST OPTIMAL POWER
FLOW IN POWER SYSTEMS**

BY
SANI UMAR

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES
KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE
In
COMPUTER ENGINEERING

NOVEMBER 2020

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

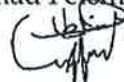
DEANSHIP OF GRADUATE STUDIES

This thesis, written by **SANI UMAR** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER NETWORKS**.

Thesis Committee



Dr. Muhamad Felemban (Adviser)



Prof. Tarek Sheltami (Member)



Dr. Yahya Osais (Member)



Prof. Aiman El-Maleh
Department Chairman



Prof. Suliman S. Al-Homidan
Dean of Graduate Studies



Date

©Sani Umar
2020

*I dedicated this work to my family, especially my beloved parents,
whose prayers, care, and love always light my way*

ACKNOWLEDGMENTS

Alhamdulillah! All praise is to Allah the Most Beneficent, the Most Merciful. I would like to use this medium to express my special appreciation to my thesis Advisor Dr. Muhamad Felemban. Your advice on both research and my career is priceless. You have been my role model and you have been guiding me when I faltered. You have given me an opportunity to explore and learn. Also, I would like to use this opportunity to thank my thesis committee members Prof. Dr. Tarek Sheltami and Dr. Yahya Osais. I wish to acknowledge your efforts for being my committee members in your tight schedules. My gratitude goes to King Fahd University of Petroleum and Minerals and the Kingdom of Saudi Arabia for giving me this opportunity to pursue master's degree under a fully-funded scholarship. Also, I would like to thank my family for the non-stop encouragement which serve as a source of my strength throughout my academic career. Besides, I would like to thank the Nigerian Community University of Petroleum and Minerals (NCUPM) and my dear friends who made my stay at King Fahd University of Petroleum and Minerals indelible. Lastly, a special mention goes to Farouq Muhammad Aliyu, who has been my mentor starting from day one of my stay here at King Fahd University of Petroleum and Minerals. Thank you so much for your effort, you have impacted my academic career significantly.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	v
LIST OF TABLES	viii
LIST OF FIGURES	x
ABSTRACT (ENGLISH)	xii
ABSTRACT (ARABIC)	xiv
CHAPTER 1 INTRODUCTION	1
1.1 Problem Statement	4
1.2 Research objectives	4
1.3 Thesis organization	5
CHAPTER 2 BACKGROUND AND RELATED WORK	6
2.1 Attacks on Power Systems	6
2.2 Detection of False Data Injection Attacks	10
2.3 Bus System Model	14
2.4 The Energy Management System	17
2.5 The Optimal Power Flow Problem	19
2.6 Metaheuristics	22
2.6.1 Simulated Annealing	24
2.6.2 Genetic Algorithm	26
2.6.3 Particle swarm Optimization	27

2.6.4	Tabu Search Algorithm	28
CHAPTER 3 ADVANCED PERSISTENT THREAT BASED FALSE		
	DATA INJECTION ATTACKS	30
3.1	Research Methodology	31
3.1.1	False Data Injection Attacks Plan	32
3.1.2	FDIA mitigation	39
3.2	APT-based Attack Strategy	39
3.2.1	Initialization	40
3.2.2	Optimization problem	42
3.3	FDIA targets in the power systems	45
3.4	Minimum effort FDIA	46
3.5	Unbounded effort FDIA	50
CHAPTER 4 RULE-BASED DETECTION SYSTEM FOR FDIA		55
CHAPTER 5 RESULTS AND DISCUSSIONS		60
5.1	Simulation setup	60
5.2	APT-based FDIA on IEEE 6 Bus systems	63
5.3	APT-based FDIA on IEEE 9-bus system	67
5.4	APT-based FDIA on IEEE 30-bus system	70
5.5	APT-based FDIA on IEEE 118-bus system	73
5.6	FDIA Detection Results	82
CHAPTER 6 CONCLUSION AND FUTURE WORK		99
APPENDIX A BUS SYSTEMS PARAMETERS		101
APPENDIX B PUBLICATIONS		112
REFERENCES		113
VITAE		123

LIST OF TABLES

1.1	Examples of cyber attacks on power systems [1].	3
2.1	Modeling parameters	21
3.1	Notations	41
3.2	Generation cost increase under minimum effort FDIA(\$hr)	47
3.3	6 Bus-system C values calculation	52
3.4	9 Bus system C values calculation	53
3.5	Generation cost increase under minimum effort FDIA(\$hr)	54
4.1	Truth table of the secondary FDIA detection features	59
5.1	Simulation parameters	61
5.2	Maximum cost increase under attack on different bus systems using SA	76
5.3	Maximum cost increase under attack on different bus systems using GA	77
5.4	Maximum cost increase under attack on different bus systems using PSO	78
5.5	Maximum cost increase under attack on different bus systems using TS	79
5.6	Minimum, average, and Maximum cost increase under attack on dif- ferent bus systems	80
5.7	Comparison between our work and the work in [2]	81
A.1	6 Bus-system Transmission line Parameters	101
A.2	6 Bus-system generator cost coefficients and limitations	102
A.3	9 Bus-system Transmission line Parameters	103
A.4	9 Bus-system generator cost coefficients and limitations	104
A.5	30 Bus-system Transmission line Parameters	105

A.6	30 Bus-system generator cost coefficients and limitations	106
A.7	118 Bus-system Transmission line Parameters I	107
A.8	118 Bus-system Transmission line Parameters II	108
A.9	118 Bus-system Transmission line Parameters III	109
A.10	118 Bus-system Transmission line Parameters IV	110
A.11	118 Bus-system Transmission line Parameters V	111

LIST OF FIGURES

2.1	Classifications of attacks in energy industry [1]	9
2.2	Schematic diagram of a 5-bus system	16
2.3	System architecture of the energy management system [2].	18
2.4	Classification of Metaheuristics	23
3.1	flowchart of the Attack plan	33
3.2	Crossover	36
3.3	Mutation	37
5.1	6-Bus systems Percentage increase in generation cost	65
5.2	6-bus systems generator output variation	66
5.3	9-Bus systems Percentage increase in generation cost	68
5.4	9-bus systems generator output variation	69
5.5	30-Bus systems Percentage increase in generation cost	71
5.6	30-Bus systems generator output variation	72
5.7	118-Bus systems Percentage increase in generation cost	74
5.8	118-Bus systems generator output variation	75
5.9	6-bus increase in cost before and after detection and prevention	85
5.10	6-bus Percentage of False Negatives (FN) accuracy metric vs Threshold	86
5.11	6-bus systems accuracy metrics at $\text{Tau}-P_d = 130$	87
5.12	9-bus increase in cost before and after detection and prevention	88
5.13	9-bus Percentage of False Negatives (FN) accuracy metric vs Threshold	89
5.14	9-bus systems accuracy metrics at $\text{Tau} - P_d = 300$	90
5.15	30-bus increase in cost before and after detection and prevention	91

5.16	30-bus Percentage of False Negatives (FN) accuracy metric vs Threshold	92
5.17	30-bus systems accuracy metrics at $Tau - P_d = 150$	93
5.18	118-Bus systems increase in cost before and after detection and prevention	94
5.19	118-bus Percentage of False Negatives (FN) accuracy metric vs Threshold	95
5.20	118-bus systems accuracy metrics at $Tau - P_d = 1200$	96
5.21	Comparison of accuracy metrics rates on 30-bus systems	97
5.22	Comparison of accuracy metrics rates on 118-bus systems	98

THESIS ABSTRACT

NAME: SANI UMAR

TITLE OF STUDY: Detection of false data injection attacks against optimal power flow in power systems

MAJOR FIELD: Computer Networks

DATE OF DEGREE: NOVEMBER 2020

Cyber-security of modern power systems has captured a significant interest due the surge in cyber-attacks on power systems. Such attacks lead to the Russian Trinitrotoluene (TNT) explosion in 1982, the USA generator explosion in 2007, the Turkey oil explosion in 2008, energy generation and distribution problem in Saudi Arabia and Qatar in 2012, and the Ukraine blackout in 2015. We have analyzed the impact of False Data Injection Attacks (FDIA) on the cost of power generation and the physical component of the power systems. We have introduced a new FDIA strategy that intends to maximize the cost of power generation and proposed a rule-based detection and prevention system. The viability of the attacks and the detection and prevention systems is shown using simulations. Metaheuristics are used to find the suitable attack targets and execute the FDIA. We have found that the attacks are capable of increasing

the power system generation cost by up to 15.6%, 45.1%, 60.12%, and 74.02% on the 6-bus, 9-bus, 30-bus, and 118-bus systems, respectively. Accuracy metrics are used to evaluate the performance of the developed rule-based FDIA detection and prevention system. We have found that the False Negatives (FN) rates become significantly low as the value of load demand threshold τ_{pd} increases. Specifically, the FN rates approaches 0 when $\tau_{pd} > 130\text{MW}$, $\tau_{pd} > 300\text{MW}$, $\tau_{pd} > 150\text{MW}$, and $\tau_{pd} > 1200\text{MW}$ for the standard IEEE 6-bus, 9-bus, 30-bus, and 118-bus systems respectively.

ملخص الرسالة

الاسم الكامل: ساني عمر

عنوان الرسالة: الكشف عن هجمات حقن البيانات الخاطئة ضد تدفق الطاقة الأمثل في أنظمة الطاقة

التخصص: شبكات الحاسب

تاريخ الدرجة العلمية: تشرين الثاني 2020

حظي الأمن السيبراني لأنظمة الطاقة الحديثة باهتمام كبير بسبب تصاعد الهجمات الإلكترونية على أنظمة الطاقة. أدت مثل هذه الهجمات إلى انفجار روسي المعروف بـ (TNT) Trinitrotoluene في عام 1982، وانفجار مولد في الولايات المتحدة الأمريكية في عام 2007، وانفجار شركة النفط تركي في عام 2008، ومشكلة توليد وتوزيع الطاقة في المملكة العربية السعودية وقطر في عام 2012، وانقطاع التيار الكهربائي في أوكرانيا في عام 2015.

لقد قمنا بتحليل تأثير هجمات حقن البيانات الزائفة على تكلفة توليد الطاقة والمكون المادي لأنظمة الطاقة. لقد أدخلنا استراتيجية جديدة FDIA تهدف إلى زيادة تكلفة توليد الطاقة إلى الحد الأقصى واقترحنا نظام الكشف والوقاية المستند إلى القواعد

جدوى الهجمات والكشف عنها ومنعها يتم عرض الأنظمة باستخدام المحاكاة. وتم استخدام Metaheuristics للعثور على أهداف الهجوم المناسبة وتنفيذ FDIA. لقد وجدنا أن الهجمات قادرة على زيادة تكلفة توليد نظام الطاقة بنسبة تصل إلى 15.6٪ و 45.1٪ و 60.12٪ و 74.02٪ على أنظمة 6-bus و 9-bus و 30-bus و 118-bus على التوالي.

لقد تم استخدام مقاييس الدقة لتقييم أداء الكشف والوقاية المستندة إلى القواعد النظام. لقد وجدنا أن معدلات السليبيات الكاذبة تصبح منخفضة بشكل ملحوظ مع زيادة قيمة عتبة طلب الحمل. τ_{pd} على وجه التحديد، تقترب معدلات FN من 0 عندما $\tau_{pd} > 130MW$ و $pd > 300MW$ و $pd > 150MW$ و $\tau_{pd} > 1200MW$ لأنظمة IEEE 6-bus و 9-bus و 30-bus و 118-bus على التوالي.

CHAPTER 1

INTRODUCTION

Smart power systems are complicated cyber-physical systems. An example of such a system is the modern power systems, which consist of physical infrastructure and cyber-infrastructure. The physical infrastructure is responsible for generating, transmitting, and distributing electric power. On the other hand, the cyber infrastructure includes the telemetry and the communication equipment connected to the power systems. The cyber components help in enhancing decision making and monitoring of the power systems. Furthermore, cyber components such as meters are used to measure parameters such as the load demand of a particular node (i.e bus) within the power system network. The energy management system is composed of network topology, economic dispatch calculations, Power Systems State Estimator (PSSE), Automatic Generation Control (AGC), contingency analysis, and Optimal Power Flow (OPF). Moreover, the energy management system is responsible for the controlling, monitoring, and optimizing the performance of the performance of the power systems [2].

Recently, the cyber-security of power systems has captured a significant interest [3], [4], [5], [6], [7], [8], [9], [10], [11]. This is because the world has seen a surge in

cyber-attacks on power systems. Example of such attacks include the USA generator explosion in 2007 [1], the Ukraine blackout in 2015 [12], and the Turkey oil explosion in 2008 [1]. Table 1.1 presents examples of some major attacks that happened in the energy industry. In these attacks, an adversary leverages the vulnerabilities in the cyber infrastructure to attack the power systems. This leads to catastrophic consequences that impact the physical components of the power systems.

The objective of this thesis is to analyze the impact of False Data Injection Attack (FDIA) [13] on power systems. In particular, we analyze Advanced Persistence Threat (APT) based FDIA on the cost of power generation and the physical component of the power systems.

We propose a novel FDIA strategy that allows attackers to attack multiple nodes to maximize the impacts of the attacks on power systems. We formulate the attack model as an optimization problem with the objective to maximize the cost of power generation. We use metaheuristics techniques, namely, Genetic Algorithm (GA), Simulated Annealing (SA) algorithm, Tabu search (TS), and Particle Swarm Optimization (PSO) to generate an attack strategy. Subsequently, we proposed a rule-based detection and prevention system to mitigate FDIA in power systems. Finally, we evaluate the attacks and the detection and prevention system by running simulations on the standard IEEE bus systems using MATPOWER in MATLAB[14].

Table 1.1: Examples of cyber attacks on power systems [1].

Attacks	Year	Region	Consequences
False Data Injection Attacks	2015	Kyiv, Ukraine	Several hours of power outage (blackout). Affecting about 225,000 customers.
	2008	Turkey	Explosion of oil pipeline in which 30,000 barrels of oil is spilled in water.
	2007	Idoha National Lab, USA	Generator exploded.
Code Manipulation	1999	Bellingham, USA	Three people were killed by a huge fireball and many others were injured.
	1982	Russia	Explosion of 3 kilotons of Trinitrotoluene (TNT)
Malware Injection	2012	Saudi Arabia, and Qatar	Energy distribution, and energy generation are affected.
	2003	Ohio, USA	System shutdown for 5 hours.

1.1 Problem Statement

Due to the significant impact of false data injection attacks, it is necessary to study its impact on the cost of power generation and its impact on the performance of the physical components of the power systems. Moreover, is it important to provide a detection and prevention mechanism for such attacks. The detection and prevention mechanisms will help to detect and mitigate such attacks. In addition, the detection and prevention mechanism will safeguard the power systems and ensure its normal operation. Existing FDIA models do not consider the objective of imposing maximum damage to the system. Therefore, an attack strategy that intends to maximize the negative impact on the power systems needs is proposed. This attack can provide a picture of the impact of FDIA on power systems and will help in determining which detection mechanism is best to mitigate FDIA in power systems.

1.2 Research objectives

The objectives of this thesis is as follows:

1. Develop and analyze the effect of FDIA on 1) the cost of OPF and 2) the performance of the system components.
2. Develop a detection and prevention mechanism to mitigated false data injection attacks.
3. Perform simulation studies that show the viability of false data injection attacks and the detection and prevention mechanism.

1.3 Thesis organization

The remaining chapters of this thesis are as follow: Chapter 2 presents the related work and highlights the background concept of this thesis. Chapter 3 presents the proposed attack strategy. Chapter 4 presents the proposed FDIA detection system. Chapter 5 discusses our findings. Finally, conclusion and future work are presented in chapter 6.

CHAPTER 2

BACKGROUND AND RELATED WORK

This section highlights the the related work and background of the problem. First, we present a classification of attacks based on the way the attacks are executed. Then, we present studies that attempt to propose various mechanisms to detect data integrity attacks in power systems. Next, we present the model of the system under investigation. Using system model, we present a mathematical model of the OPF problem, which is in the form of a combinatorial optimization problem.

2.1 Attacks on Power Systems

As a form of a cyber-physical system, power system is vulnerable to different types of attacks. Attacks on cyber-physical systems can be cyber-based, communication-based, network-based, or physical-based attacks [1]. There are various research efforts in the literature to investigate different cyber attacks on power systems. Suna et al.

[15] present a survey on the state-of-the-art of pertinent issues related to cybersecurity in power systems. A survey of communication-based cybersecurity issues is presented in [16]. Authors in [17] and [18] present a survey on cyber attacks and defensive strategy in power systems. Cyber-based attacks are executed through the cyber layer of a system. Cyber-based FDIA occurs when an attacker injects false information into the cyber components of the system [19]. Code manipulation occurs when an adversary manipulates the code implementation of the system software. Malware injection occurs when a virus is injected into the system. All the aforementioned attacks are considered cyber-based attacks. This is because they can be executed through the cyber layer of the power systems.

Network-based attacks are executed through unauthorized access to the network. In such attacks, the system software and the physical communication links are not affected. Denial of service (DoS) attack is considered network-based attacks. In a DoS attack, an adversary floods the network with fake request packets that render the network inaccessible to legitimate activities. Other network-based attacks include packet sniffing attack and man in the middle attack [20]. Moreover, FDIA can be executed through the network layer of a system. False information can be injected into the packets that traverse across the network. Other types of attacks that fall under this category include packet sniffing, man in the middle, and black hole attacks.

Physical-based threats are types of attacks whereby an adversary gains physical access to the system and damage its components. This can disturb the normal operation of the target systems. FDIA in which an adversary has physically accessed, compromised devices, and inject false information into their input is considered a

physical-based attack. Other kinds of attacks in this category Emission Security (Em-sec) attack and the use of electromagnetic pulse to physically damage systems [21]. Communication-based attacks are types of attacks that impact communication links. Message replay and channel jamming attacks are categorized under communication-based attacks [22]. This is because they can be executed on the communication links to impose negative consequences on the normal operation of the target systems [1].

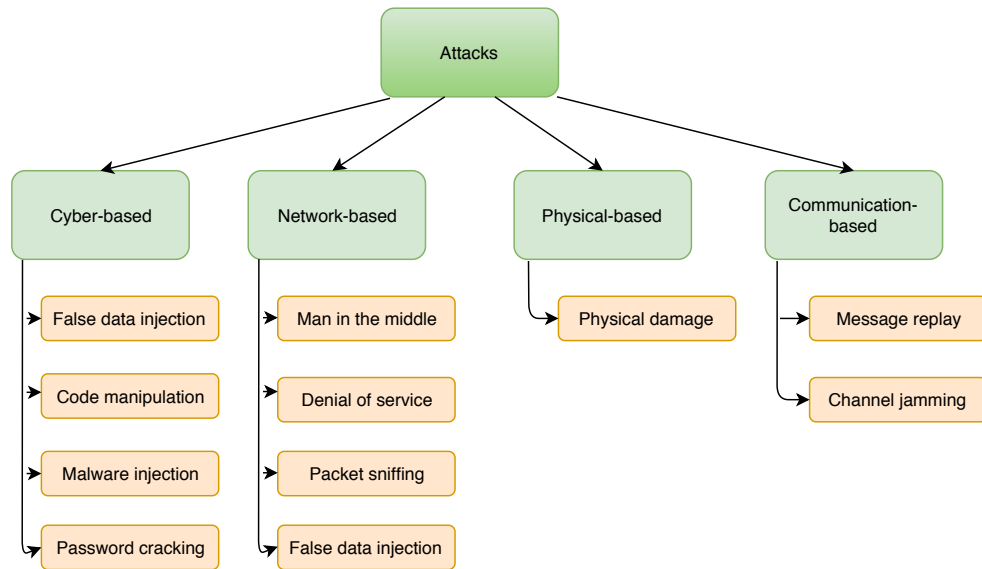


Figure 2.1: Classifications of attacks in energy industry [1]

2.2 Detection of False Data Injection Attacks

Some studies attempt to propose various mechanisms to detect data integrity attacks in power systems [23] [24] [25] [26] [27] [28] [29] [30]. The detection algorithms can be data-driven based [31] [32] [33] [34] or model-based [35] [36] [2]. In data-driven based detection algorithms, machine learning algorithms are utilized to processed data collected from the power systems to detect false data injection attacks.

Rahman *et al.* [36], present a formal model of undetected data integrity attack on state estimation that can deviate from the bad data detection module and compromise the solution provided by the optimal power flow module in the smart grid. The proposed model is utilized in investigating and verifying the influence of false data injection attacks on the optimal power flow. The proposed attack model is based on the formalization of certain attributes. These attributes include the adversary's knowledge of the network, adversary's resource constraints, and accessibility to the resources and suitable attack targets. Moreover, an example case study was carried out on the IEEE 5-bus system. This is to delineate the proposed model. It was shown that the feasible attack increases the cost of operation of the OPF by up to two percent (2%).

Yang et al. [2] investigate the data integrity attack as a kind of a cybersecurity threat to the OPF in power systems. A critical attack vector is modeled in such a way that the attacker can execute attacks with minimum effort. From the adversary's perspective, the target buses to compromise are selected by examining the difference between the real transmission power and line capacity limitation. Therefore, a trans-

mission line with the smallest difference is selected as the target line, and all nodes connected to that particular line are selected as the target nodes to compromise. An efficient defensive strategy is presented. This includes both detection-based strategy and protection-based. The detection based strategy detects the presence of false measurements. The protection based strategy protects against data integrity attacks by deploying smart meters and sensors.

Esmalifalak et al.[31] proposed a machine learning-based detection mechanism against stealthy false data injection attack in power systems. The proposed technique utilizes a labeled data set collected from the operation of the smart grid. The dataset is used to train a supervised distributed support vector machine. It was shown that the normal operation of the smart grid can be strategically distinguished from its operation under false data injection attacks. Furthermore, the three commonly used supervised machine learning classifiers (i.e., k-nearest neighbor (kNN), extended nearest neighbor (ENN), and support vector machine (SVM)) are utilized in [32] to detect false data injection attack in power systems. All three classifiers yield more than 80% accuracy on the IEEE standard 30-bus system. The 30-bus system was chosen as a benchmark test case. It was shown that supervised learning-based detectors are an effective way to combat false data injection attacks in power systems. Real-time detection of false data injection attacks using Artificial Neural Networks (ANNs) is proposed by Erik *et.al.*[33]. The proposed detection techniques is capable of detecting not only data integrity attacks but can also detect sensor failures and replay attacks. An SVM based detection technique is used to compare the performance of the proposed real-time detection mechanism. Experimental results showed that the proposed detection

techniques achieved 99% accuracy. However, the authors failed to narrate the amount of training data required for the proposed learning-based technique to detect data integrity attacks.

Authors in [37] studied false data injection attacks on security-constrained OPF. A bi-level optimization problem model of a false data injection attack is utilized to figure out the minimum number of sensors required to compromise. Moreover, vulnerable critical generators and transmission lines are identified. The standard IEEE 14 and 30 test cases are used to investigate the vulnerability of the power system against false data injection attacks. Apart from the detection techniques of False data injection attack proposed in the literature, various prevention-based techniques for false data injection attacks have also been investigated. Abdallah *et.al.*[38] proposed an efficient prevention-based technique for False data injection attacks in power system. The proposed technique aims to prevent the occurrence of false data injection attacks by assuring the availability and integrity of power systems measurements from all units in the network. Simulation results indicate that the proposed prevention technique has negligible computational complexity and communication overhead. Manandhar *et al.* [39] discuss various drawbacks in the security of power systems considering the telemetry and communication equipment including sensors and actuators.

In literature [7], the authors viewed FDIA as a matrix separation problem. They examine the sparse nature of FDIA and the dimensionality of measurements of the power systems. A novel FDIA detection technique is proposed. The technique can detect a malicious attack and identify a normal system state. This is done by using the factorization of the low-rank matrix and minimization of the nuclear norm. The

authors conducted a series of numerical simulations on both real data and synthetic data to validate the effectiveness of the proposed detection technique. However, the authors do not analyze the impact of FDIA especially on the cost of power generation and the impact on the physical components of the power systems.

Lei et al. [40] proposed a Deep Belief Networks (DBN)-based detection of FDIA in the smart grid. The authors used an unsupervised machine learning approach to train the detection technique in order to differentiate between the malicious system state and the normal system state. Backpropagation is used as an algorithm to fine-tune the parameters of the model and propagate the errors. To evaluate the effectiveness of the proposed detection mechanism, a series of simulations were carried out on the IEEE standard systems. The authors found that their proposed FDIA detection performed better than support vector machine (SVM)-based FDIA detection.

Zhang et al.[41] studied the security issues of dynamic state estimators when the communication and telemetry equipment are compromised by adversaries using FDIA. The authors proposed a sufficient conditions such that the attack can be executed with stealthily. Moreover, the energy of the attacks stealthiness were introduced. Lastly, the superiority of the attacks were illustrated on the standard IEEE 6-bus systems.

In addition, Lu et al. [42] investigate FDIA on power systems state estimator in the presence of telemetry and communication equipment failure. The power system under investigation is equipped with the bad data detection mechanism. An undetectable FDIA is modeled to worsen the performance of the power system state estimation. Finally, the effectiveness of the attacks model is evaluated using the IEEE standard 5-bus, 9-bus, and 30-bus systems.

Sayghe et al. [43] presented a survey of machine learning methods to detect FDIA in power systems. The authors presented comprehensive background information on FDIA, the impact of FDIA on power systems, and the FDIA defense mechanisms that utilize the machine learning approach to detect FDIA in power systems. The detection mechanism includes protecting the least number sets of meter, game theory-based defense, cryptographic based defense, topology, and proactive based defense against FDIA. Besides, the limitation of those detection mechanics include intensive computation, adversary ability to predict new systems configuration, protection only limited set measurements, and modeling challenges. Ashrafuzzaman et al. [44] proposed a data-driven based mechanism to detect FDIA using an ensemble-based machine learning approach. Several classifiers are used to detect FDIA in the proposed approach. In addition, two ensembles are used in which one utilizes supervised classifiers and the other uses unsupervised classifiers. The proposed detection mechanism is evaluated on the IEEE standard 14-bus system using simulated data. Their results show that the ensembles are better than the individual classifiers for the unsupervised models.

2.3 Bus System Model

Figure 2.2 depicts an example of the physical infrastructure, known as the IEEE 5-Bus system. Examples of other IEEE standard systems include; 9-Bus, 14-Bus, 24-Bus, 30-Bus system, 39-Bus, 57-Bus, and 118-Bus [14]. The power system depicted in Figure 2.2 consists of four components [45]: generators, telemetry equipment, busses, and transmission lines. The generators (g_1, g_2, g_3, g_4 , and g_5) are responsible for power

generation. On the other hand, the telemetry equipment (Pd_2, Pd_3, Pd_4) are devices such as meters and sensors that collect power systems measurements. The buses ($Bus_1, Bus_2, Bus_3, Bus_4$, and Bus_5) are the connecting point between transmission lines and generators. Transmission lines are the lines connecting two buses, which are responsible for the transmission of power from one location to another, across a country or region.

For example, the 5-bus system, depicted in Figure 2.2, consists of two generators (g_1 and g_2) attached to bus number 1, one generator (g_3) attached to bus number 3, one generator (g_4) attached to bus number 4, and one generator (g_5) attached to bus number 5. A residential load which mainly consists of heating, lighting, and cooling is connected to bus numbers 2, 3, and 4 which represent the transmission substations. The loads are represented by the variables P_{d2}, P_{d3} , and P_{d4} , respectively. All buses are connected by transmission lines to form a power system network and enable power flow between them. In the system model, it is assumed that all generators are secure and cannot be attacked by an adversary. That is, false data cannot be injected into the measurement related to the generator output. Therefore, the only measurement available to the attacker is the measurement related to the load demand in the power system network. Hence, the attacker can only deviate the optimal generator output by falsifying the load demand of certain nodes in the power systems network.

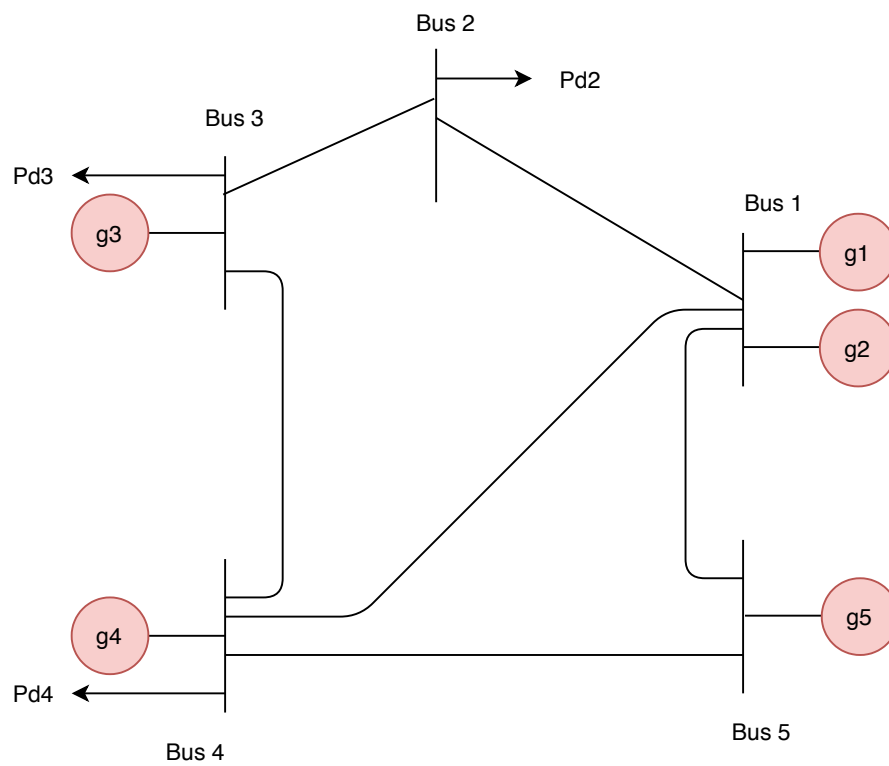


Figure 2.2: Schematic diagram of a 5-bus system

2.4 The Energy Management System

In power systems, the energy management system is responsible for the control, monitoring, and optimization of the performance of the power systems [2]. As depicted in Figure 2.3, the energy management system is composed of network topology, economic dispatch calculations, Power Systems State Estimator (PSSE), Automatic Generation Control (AGC), contingency analysis, and Optimal Power Flow (OPF).

Network topology is the representation of the entire network. The network topology is composed of the connectivity of the buses and how the loads and generators are connected to the buses within the network. The economic dispatch calculations module is used to determine the target power output of all generators in the network. PSSE is one of the critical components of power systems. The PSSE estimates the state of power systems based on data collected by the sensors from the power systems network. The AGC module is used to adjust the power generation output of all generators so that the change in the load demand is satisfied. This is because there is a need to meet the power flow constraint that requires that the generated power and load demand of the power systems is balanced. The contingency analysis module is used to identify unexpected failures of power systems components such as failure of transmission lines or generators. In the following section, we discuss the OPF component.

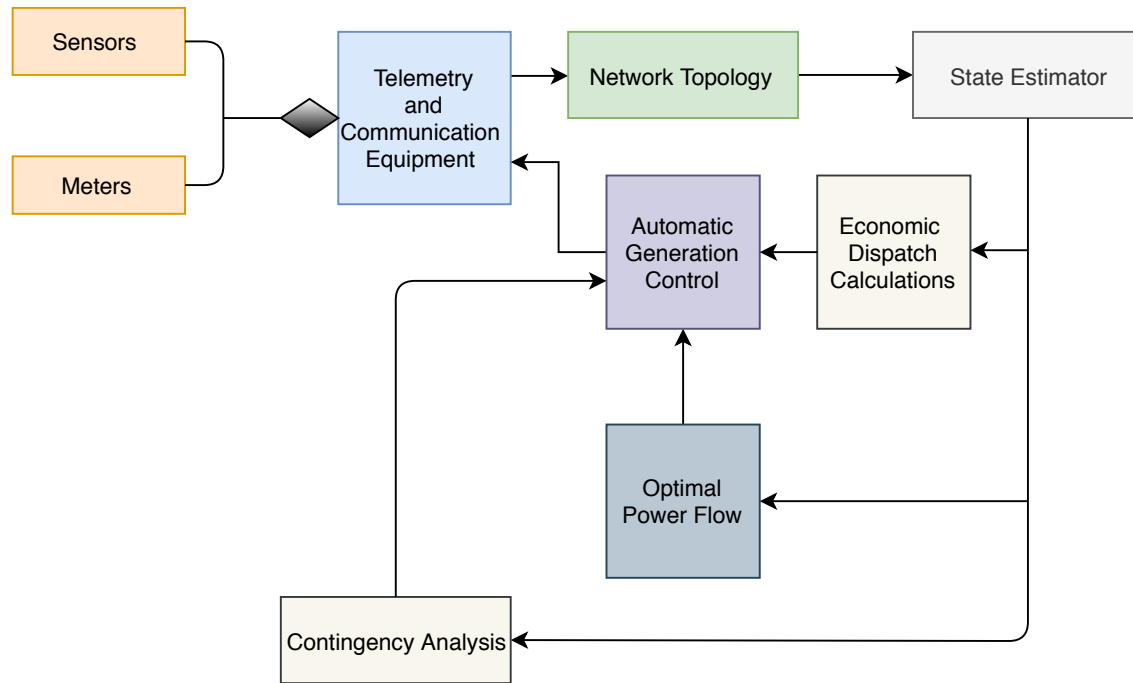


Figure 2.3: System architecture of the energy management system [2].

2.5 The Optimal Power Flow Problem

OPF depends on the output of the state estimation module to accurately determine the optimal operating level of the generators. This is required for automatic generation control. Recent research efforts have shown the vulnerability of the state estimation to cyber-attacks [46]. Consequently, an attacker can inject false information into the telemetered measurements that corrupt the output of the state estimation and consequently mislead the OPF mechanism.

An OPF mechanism is utilized in determining the optimal operating level of generators. The objective of the OPF mechanism is to reduce the overall cost of generation while meeting the load demand, generations, and transmission constraints. These constraints include the capacity limitation of the generators and the transmission lines. Since the OPF mechanism depends on power systems measurements from meters and sensors, the compromised false measurements will mislead the operation of the OPF mechanism in determining the optimal operating level of the power systems.

The OPF problem can be mathematically formulated as follows. Consider a power system with a set of buses Ω_{net} , a set of transmission lines Ω_L , and a set of generation points Ω_g . The OPF Problem formulation consists of the cost function, inequality and equality constraints. The main objective of OPF is to minimize the generation cost of all generators in the network. The cost of a particular generator i is modeled as a quadratic cost function provided in Equation 2.1 where a_i , b_i , and c_i are the cost coefficients related to the fuel cost. The cost coefficients are determined by the properties of the generator. Moreover, the inequality constraints of the formulation

of the OPF optimization problem includes the capacity limitation of the transmission lines and generators as shown in equation (2) and (3) respectively. P_{ij} represents the power flow from bus i to bus j and P_g represent the generator output. Furthermore, the OPF optimization problem formulation includes equality constraints as shown in equation (4). B_{ij} is the line admittance between bus i and j and $\delta_i - \delta_j$ is the difference between the voltage phase angle at node (bus) i and j . Also, as shown in equation (5), the equality constraints include the equation that balances the real power inflow and outflow at each buses in the power systems network. Table 3.1 summarizes the modeling parameters.

The following is the formulation of the OPF optimization problem according to [45]:

$$\mathbf{min} \ F(P_{g_i}) = \sum_{i \in \Omega_g}^n a_i P_{g_i}^2 + b_i P_{g_i} + c_i \quad (2.1)$$

s.t.

$$P_g^{min} \leq P_g \leq P_g^{max} \quad (2.2)$$

$$|P_{ij}| \leq P_{ij}^{max}, \quad \forall i, j \in \Omega_{net} \quad (2.3)$$

$$P_{ij} = B_{ij} * (\delta_i - \delta_j), \quad \forall i, j \in \Omega_{net} \quad (2.4)$$

$$P_{g_i} - P_{d_i} - \sum_{j \in \Omega_{net}} P_{ij} = 0, \quad \forall i, j \in \Omega_{net} \quad (2.5)$$

Table 2.1: Modeling parameters

Notation	Notation definition
Ω_{net}	Set of all nodes (buses) in the network
Ω_d	Set of all nodes (buses) in which a demand/load is connected
Ω_g	Set of all nodes (buses) in which a generator is connected
Ω_{L_i}	Set of all lines connected to the i^{th} node (bus)
P_{g_i}	Generator output of i^{th} generator
P_g^{min}	Lower bound of the generator output
P_g^{max}	upper bound of the generator output
P_{d_i}	Load/demand at node (bus) i
δ_i	Voltage phase angle of node (bus) i
P_{ij}	Power flow between bus i and j
P_{ij}^{max}	Upper bound of the Power flow between node (bus) i and j
B_{ij}	Line admittance between node (bus) i and j
$C_i(P_{g_i})$	Cost function of the generator at i^{th} node (bus)

2.6 Metaheuristics

Metaheuristics are designed to solve optimization problems in the case where other methods are either inefficient, ineffective or failed. Metaheuristics are considered one of the most practical methods for solving many optimization problems and it is applies to the real-world problems that have the nature of combinatorial problems [47]. Metaheuristics can be single solution-based such as Simulated Annealing, population-based such as Genetic Algorithm and Tabu Search (TS) or swarm intelligence such as Particle Swarm Optimization (PSO). Figure 3.3 presents the classification of the selected metaheuristics of this research

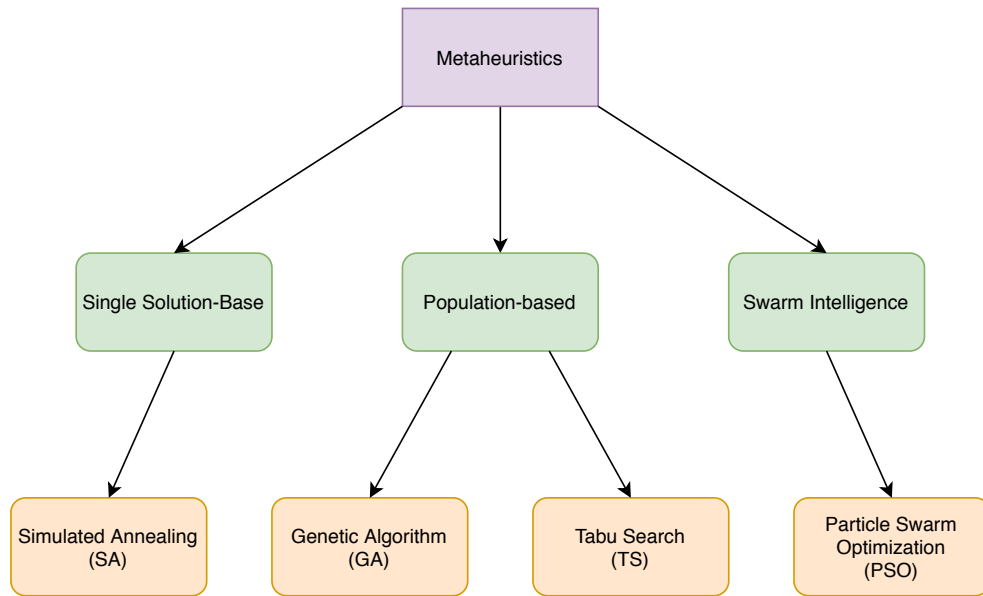


Figure 2.4: Classification of Metaheuristics

2.6.1 Simulated Annealing

To make a perfect and strong metallic object, a controlled metal cooling procedure is followed, this procedure is known as annealing. It refers to the heating of the metal to a very high temperature and follows a controlled cooling process by reducing the temperature in steps. In every step, the temperature is maintained for the metal to attain thermal equilibrium [48]. The simulated annealing metaheuristics proposed in the year 1983 is based on the analogy of simulating the annealing of metal to solve optimization problems. The algorithm mimics the process of crystallizing a melted metal into a solid. The same analogy is applied to computer science algorithms to solve problems [49]. Algorithm 1 presents the Simulated Annealing algorithm. [50].

Algorithm 1 Simulated annealing algorithm

begin

. INITIALIZATION

. $C = C_{init}$

. iteration = 0

. From $T = T_{max}$ to T_{min}

. repeat

. PERTURB (config. i $\rightarrow$ config. j, $\Delta C_{i,j}$)

. if $\Delta C_{i,j} \geq 0$

. $ACCEPT$

. else if $\exp(-\Delta C_{i,j}/T) > \text{rand}(0,1)$

. $ACCEPT$

. if $ACCEPT$ then $UPDATE(\text{config. j})$

. until *equilibrium*

. iteration = iteration + 1

end

2.6.2 Genetic Algorithm

A genetic algorithm is a heuristic search that is used to solve a wide range of optimization problems. This flexibility makes the algorithm applicable to several optimization problems in practice. The basics of genetic algorithm is the evolution [51]. The success of different varieties of species is a good reason to believe in the power of evolution. Species can develop a structure that enables them to compete and survive in different types of habitat. The genetic algorithm is based on a group of individual candidate solutions that constitute a solution to the optimization problem needed to be solved. A fitness function is used to know the quality of the candidate solutions. In this research, we have used the power generation cost function for the OPF mechanism to determine the fitness of the candidate solutions. The genetic algorithm goes from one generation to another as the number of iterations increases. In every iteration, only the fittest candidate solutions survived after going through genetic operators of mutation and crossover. This allows the algorithm to approach the best solution as the number of iterations increases. Algorithm 3 presents the Genetic Algorithm.

Algorithm 2 Genetic algorithm [52]

```
begin
.  INITIALIZATION
.  While (iteration  $\leq$  iterationmax)
.      Calculate fitness of each candidate solution
.      Select parents according to their fitness
.      Perform Crossover()
.      Perform Mutation()
.      Select fittest offspring
.      iteration = iteration + 1
end while
```

2.6.3 Particle swarm Optimization

In Particle Swarm Optimization, particles are distributed in the search space to determine the best solution of an optimization problem. Each particle evaluates the objective function at its current position. Then, each particle decide its movement in the search space by comparing its current position and its best fitness position from the past and the group's (swamp) best fitness. In every iteration, the swamps moves closer to the best solution to the objective function[53]. Algorithm 3 presents the Particle Swarm Optimization algorithm.

Algorithm 3 Particle Swarm Optimization [54]

```
begin
.   Initialize
.   For (Each particle)
.       Evaluate the optimization fitness function
.       Compare particle's fitness with its  $P_{best}$ 
.       If (Current fitness  $\geq P_{best}$ )
.            $P_{best} = Currentfitness$ 
.            $P_i = currentlocation$ 
.       Find group best fitness
.       Update velocity and location based on PSO equation
.       iteration = iteration + 1
end
```

2.6.4 Tabu Search Algorithm

Tabu Search Algorithm is another metaheuristics technique that is used to solve combinatorial optimization problems. The algorithm is proven to be effective in solving such kind of optimization problems [55]. Algorithm 4 present the tabu search algorithm.

Algorithm 4 Tabu Search Algorithm

begin

. Generate initial solution

. Repeat

. Compute current solutions for the neighborhood

. Compute all fitness of possible solutions of the neighborhood

. Next solution = Best solution from the neighborhood

. If next solution is not part of the tabu list and it is better than current solution

. Update current solution to the next solution

. End if

. Update the Tabu list

. If Tabu list size is greater than max list size

. Remove worst element from the Tabu list

. End if

. Increase number of iterations by 1

. until max number of iterations

end

CHAPTER 3

ADVANCED PERSISTENT THREAT BASED FALSE DATA INJECTION ATTACKS

There are three ways for an attacker to manipulate measurements in FDIA [12]. The attackers can compromise measurement equipment physically. The attacker can intercept data packets in the power system network while they are transferred to the control center. Also, the attacker can modify the database of the control center through unauthorized access. The attacker cannot launch an attack on the power systems generators, because they are assumed to be secure [2]. That is, measurements related to the power generators are not available to the attacker. Therefore, only the load demand is available for the attacker to falsify. The attacker instigates a collusive strategy to manipulate at least two nodes simultaneously. The attacker reduces load demand of one node and increases the load demand of another node by the same

amount, such that the total load demand on the system before the attack is equal to the total load demand on the system after the attack in order to reserves the OPF constraints. This is because the system will be unstable if the OPF constraints are not satisfied. The currently proposed FDIA models are not effective because there is no consideration of imposing maximum damage to the system. Therefore, another approach is to use the APT strategy to execute FDIA. In APT strategy, an adversary sustains prolonged access to the network and injects false data stealthily in order to impose maximum damage to the system. Moreover, the attacker can only falsify power demand information. The attacker has information related to the actual power flow and power limitations on the transmission lines of the power system network. The attacker intends to launch an attack to maximize the cost of power generation in power systems using the APT strategy.

3.1 Research Methodology

This section represent the methodology of this research. The section is divided to two sections. First, from the attackers perspective we have highlighted the FDIA attack plan. Second, from the defensive perspective we have highlighted the FDIA mitigation. In Chapter 5, we have compared our results with the results presented in [2] from the literature. We have selected this particular paper because they have achieved better results compared to the other research papers from the literature. Specifically, looking from the attackers perspective with the aim of imposing maximum damage to the system in terms of the increase in generation cost. To the best of our

knowledge, the authors have achieved the highest increase in generation cost when the standard IEEE bus systems are under FDIA attacks.

3.1.1 False Data Injection Attacks Plan

In this research, we have analyzed the impact of FDIA on the power systems in terms of the generation cost and the performance of power systems generators. Then, we have introduced a novel APT-based attack strategy with the objective to maximize the operation cost of power generation. We have modeled the attack strategy as an optimization problem and we have used metaheuristics to solve the formulated optimization problem. Four metaheuristics are used, namely simulated annealing, genetic algorithm, particle swarm optimization and tabu search to solve the optimization problem and obtain the attack plan. The reason we have used metaheuristics is because they are considered one of the most practical methods for solving many optimization problems and it is applied to the real-world problems that have the nature of combinatorial optimization problems [47].

The output of the solved optimization problem are the set of targets and the load demand to falsify. Figure 3.2 highlights the flowchart of the attack plan. Since the problem is formulated as an optimization problem, we need to have a mechanism to know how good is the solution in order to decide whether to accept the solution or not. In simulated annealing (SA), starting from T_{max} to T_{min} , a scenario to determine the suitable attack target is formulated as follows. First, we find the initial cost (C_{init}) of power generation without falsifying any load demand.

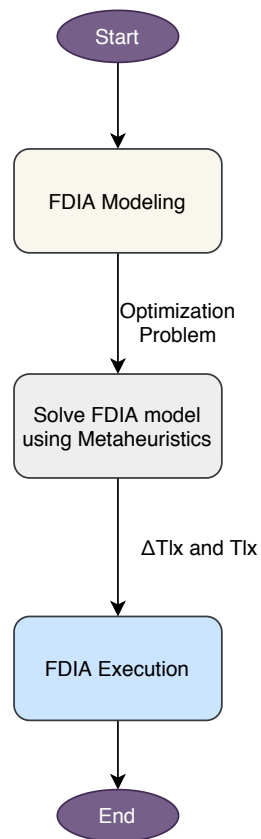


Figure 3.1: flowchart of the Attack plan

To change the state of the system from one state to another, an arbitrary transmission line is selected and falsify the load demand of the buses at the two ends of the transmission line. Then, the difference between the initial cost and the current cost ($\Delta C_{i,j}$) is calculated. If the difference is positive, we accept the new systems state, else we accept the new systems state only if $\exp(\frac{-\Delta C_{i,j}}{T})$ is greater than $\text{rand}(0,1)$. The $\text{rand}(0,1)$ gives a uniformly distributed random number on the interval of zero to one. This process is repeated until the system state with the maximum cost is found. The Simulated Annealing algorithm is similar to the metropolis hasting algorithm that combines both the notion of exploring and exploiting. Exploring is the idea of visiting more search space with the hope that the algorithm will get a better solution. However. the notion of exploiting is that the algorithm is always trying to find a global optimum as quickly as possible, this can lead it to stuck at a local optimum. That is, during the hill-climbing, the algorithm always wanted to exploit. Combining the two notions exploring and exploiting manse that the algorithm does not always improve, sometimes the algorithm wander away from the current system state with the hope of finding a better system state in next iteration.

To solve the formulated optimization using a genetic algorithm, we have followed the following steps. The first step starts with a random selection of the initial set of solutions. That is, selecting arbitrary transmission lines to attack and selecting arbitrary load demand value to falsify. This selected initial set of solutions are called “chromosomes” and this first step is also known as initializing population. The population is the sets of all chromosomes. That is, the set of all possible attack targets and the

possible load demand values to falsify. A random uniform distribution function is used to generate the initial possible values of load demand to falsify and the possible attack targets.

In the second step, the value of the objective function of the chromosomes are calculated. This is also known as the fitness value. This step is called “selection”. This is because only the fittest chromosomes are chosen from the initial population generated in step 1. Hence, subsequent operations are applied to the selected fittest chromosomes in order to get better results.

The next step is known as “crossover”. Here, the chromosomes are represented in terms of genes. This is done by changing the values of the chromosomes into binary. That is, the values are expressed in only zeros (0) and ones (1). As an example, the binary representation of a decimal number 8 is 1000. Moreover, crossover simply means a change in a single gene or group of genes of parents chromosomes to reproduce offspring chromosomes. This process is also known the mate of two parent chromosomes.

Next step is known as “mutation”. In this step, value of genes are altered by replacing zeros (0) with ones (1). For example, if the offspring chromosome is 1100, it becomes 0011 after the process of mutation. After the process of mutation, chromosomes in binary values are all converted to the decimal form. Then fitness are calculated accordingly until the chromosomes produces the target fitness (the highest cost of generation).

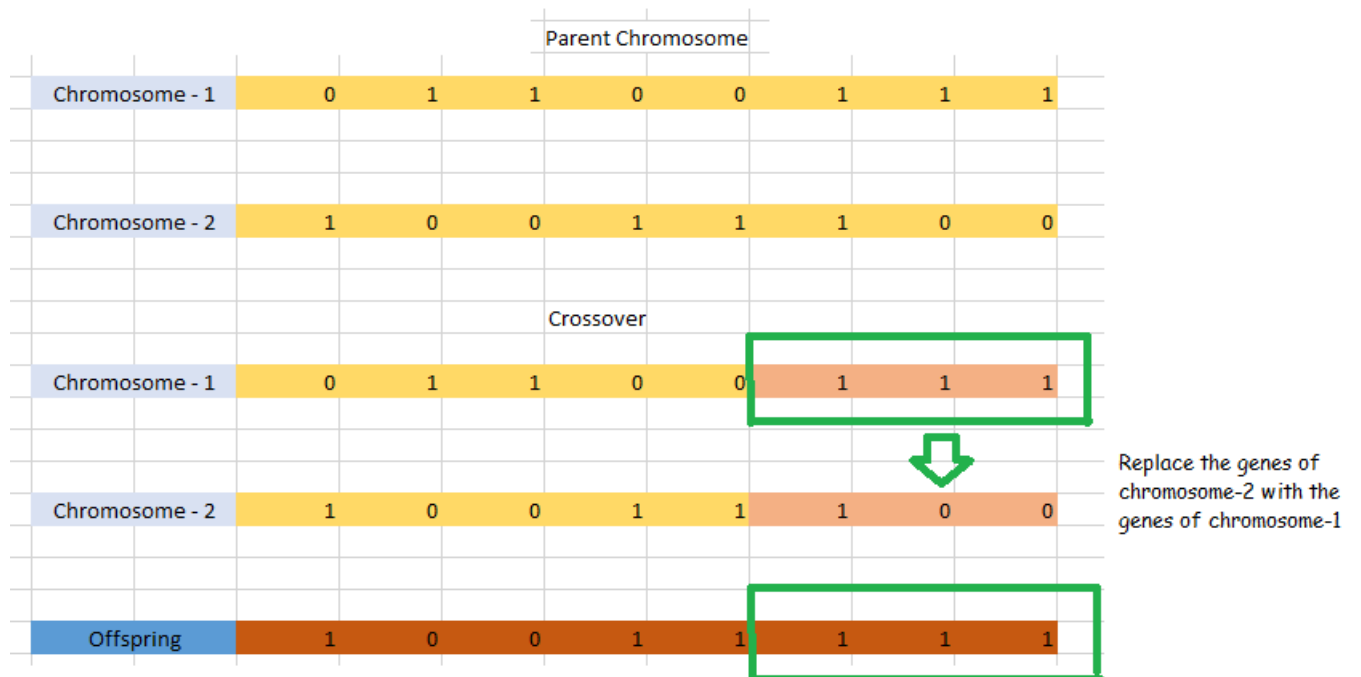


Figure 3.2: Crossover

				Offspring chromosomes in binary							
Offspring1	1	0	0	1	1	1	1	1	1		
Offspring2	0	1	0	1	1	1	1	1	0		
Offspring3	0	1	1	0	1	1	1	1	1		
Offspring4	0	1	1	1	0	0	0	0	1		
											
				Mutation							
Offspring1	1	0	0	0	1	1	1	1	1		
Offspring2	0	1	1	1	1	1	1	1	0		
Offspring3	0	1	1	0	0	1	1	1	1		
Offspring4	0	1	1	1	0	0	1	1	1		

Figure 3.3: Mutation

Particle swarm optimization algorithm is also used to solve the formulated optimization problem. It is a swarm intelligence based metaheuristics. A population called swarms of particles (candidate solutions) are used. In simple words, Particle swarm optimization algorithms mimic a group of birds flying and searching for food in an area known as a search space. Therefore, the algorithm is inspired by the social behavior of birds. Each candidate solution changes its position and velocity in order to move toward the optimal solution of the problem. The movement of the candidate solutions is influenced by the group's best position and the individual's best-known position. This guide the movement of individual particle towards the best-known position in the search space which will lead to the optimal solution. The search space can be large or small depending on the bus system under investigation. It also represents the range in which the algorithm calculates the optimal values. In this research, each particle represents a candidate solution of a target transmission line to attack and the value of load demand to falsify. This candidate solution changes at random and moves toward a value that provides the maximum increase in generation cost in the power systems.

Another metaheuristic called tabu search is used to solve the formulated optimization problem. Tabu search are widely used to solve combinatorial optimization problems. This metaheuristic is a form of neighborhood search approach. It guides a local search to explore the whole solution search space beyond just local optimum. This is being done by the use of a list called Tabu list. A flexible storage is used to restrict the next iteration solution choice to some subset of neighbors of the current solutions. In this research, the instances of the tabu list are the set of the target

transmission lines and the set of the suitable load demand value to falsify that incur the highest increase in the generation cost of the power systems.

Finally, the output of the solved optimization problem (i.e the set of target transmission lines and the set of load demand values to falsify) are used to execute the FDIA. The attacker falsify the load demand of the targets. This causes highest increase in generation cost of the power systems.

3.1.2 FDIA mitigation

As explained fully in chapter 4, in order to mitigate FDIA a rule-based detection and prevention mechanism is developed with primary and secondary detection features. Also, to evaluate the performance of the detection and prevention mechanism, we have used accuracy metrics. The accuracy metrics are the True Positive (TP) rate, True Negative (TN) rate, False Positive (FP) rate, and False Negative (FN) rate. The results of the accuracy metrics are compared with the results presented in [2] from the literature.

3.2 APT-based Attack Strategy

The proposed APT-based attack strategy address the following questions. **Which set of transmission lines to attack? In which order should the transmission lines be attacked? What values of load demand on the nodes connecting the target transmission lines are feasible to falsify?** The problem of finding the attack targets in power systems can be viewed as a search problem. There are different

combinations of buses to attack and load demand values to falsify, each of which will impose different impacts on the power systems. The search space depends on the bus system network topology. We formulate the attack strategy as the following.

3.2.1 Initialization

The objective of our attack is to maximize the cost of power generation in the power system. Therefore, we use Equation 1 as an objective function for our attack strategy. We denote the set of the attacked transmission line as $T_{Lx} \in \Omega_L$. Furthermore, we denote the false load demand value for the attacked transmission lines as ΔT_{Lx} .

Table 3.1: Notations

Notation	Notation definition
T_{Lx}	Target transmission lines
ΔT_{Lx}	False load demand value
R	Set of all From nodes
L	Set of all To nodes
α	Control parameter
$C_i(P_{g_i})$	Cost function
Ω_L	Set of all transmission lines
P_{g_i}	Generator output of i^{th} generator
P_g^{min}	Lower bound of the generator output
P_g^{max}	upper bound of the generator output
P_{d_i}	Load/demand at node i
δ_i	Voltage phase angle of node (bus) i
P_{ij}	Power flow between bus i and j
P_{ij}^{max}	Upper bound of the Power flow between node (bus) i and j
B_{ij}	Line admittance between node (bus) i and j

3.2.2 Optimization problem

We model the APT-based attack strategy as an optimization problem with the objective to maximize the cost function modeled in Equation 3.1. The outcomes of the optimization problem are the set T_{Lx} and ΔT_{Lx} . The problem is formulated as the following.

$$\max_{\Delta T_{Lx}, T_{Lx}} F(P_{g_i}) \quad (3.1)$$

s.t.

$$|T_{Lx}| \leq |\alpha * \Omega_L| \quad (3.2)$$

$$\Delta T_{Lx} \leq P_{d_i}^{max} \quad (3.3)$$

$$P_g^{min} \leq P_g \leq P_g^{max} \quad (3.4)$$

$$|P_{ij}| \leq P_{ij}^{max}, \quad \forall i, j \in \Omega_{net} \quad (3.5)$$

$$P_{ij} = B_{ij} * (\delta_i - \delta_j), \quad \forall i, j \in \Omega_{net} \quad (3.6)$$

$$P_{g_i} - P_{d_i} - \sum_{j \in \Omega_{net}} P_{ij} = 0, \quad \forall i, j \in \Omega_{net} \quad (3.7)$$

This optimization problem is similar to the problem modeled by Equations 3.1-3.5. However, two inequality constraints have been added. Equation 4.2 bounds the number of attacked transmission lines using a defined parameter α . Equation 4.3

bounds the amount load demand the attacker can falsify. To compute $P_{d_i}^{max}$, we find the set of values of load demands that will increase the power flow on each transmission line to its maximum. The remaining constraints are used to check that the system satisfies the constraints in Equations 3.2-3.5.

FDIA can be executed in a naive manner by just falsifying the load demand of randomly selected nodes without consideration of imposing maximum damage to the system. In this thesis, we have used an APT strategy [56] to execute FDIA in order to impose maximum damage to the system. Algorithm 5 presents the pseudocode for the FDIA attack. In the algorithm, the attacker performs a reconnaissance. The first step is to explore information related to power systems. The second step highlight how the attacker executes FDIA on power systems.

Algorithm 5 Attack algorithm

STEP 1: Collection of information

$From_Node \leftarrow$ Node on one end of a transmission lines

$To_Node \leftarrow$ Node on the other end of a transmission lines

$P_d^i \leftarrow$ Power demand at node i

$\Delta T_{Lx} \leftarrow$ load demand to falsify

$\Omega_{net} \leftarrow$ Set of all nodes

$T_{Lx} \leftarrow$ Target

STEP 2: Attack execution

$$P_d^{From_Node_{T_{Lx}}} = P_d^{From_Node_{T_{Lx}}} - \Delta T_{Lx}$$

$$P_d^{To_Node_{T_{Lx}}} = P_d^{To_Node_{T_{Lx}}} + \Delta T_{Lx}$$

$$\sum_{i=1}^{\Omega_{net}} P_d^i \text{ (Before attack)} = \sum_{i=1}^{\Omega_{net}} P_d^i \text{ (After attack)}$$

3.3 FDIA targets in the power systems

In power systems, the potential and most critical FDIA targets are load demand (power demand), power supply (generation), network state, and electricity pricing[57]. Load demand is one of the most critical attack targets as it can easily increase both the cost of power generation and customer cost of power consumption. Moreover, FDIA on energy demand can render the power system unstable. This can happen when the falsified energy demand is far more than the actual energy required by the customers, or when the falsified energy demand is much less than the actual energy required by the customers. The amount of actual power generation is provided by the power generation nodes within the power systems network. FDIA on power generation can lead to starvation of the load demand nodes or an increase in the cost of power generation. Power systems network parameters such as the transmission line capacity and the network topology are also potential targets for false data injection attacks. An attacker can isolate a node within the power system network. This can mislead the power distribution process of the power system. Also, electricity pricing is another potential target for FDIA. False electricity pricing would lead to the loss of revenue to the power generation companies.

3.4 Minimum effort FDIA

FDIA can be executed with minimum effort from the attackers' perspective. The effort is in terms of the number of buses to compromise and the amount of False information to be injected into the attack targets. Therefore, the attacker intends to compromise the minimum number of buses and inject a minimum amount of false information. To attack the system with the minimum effort from the attacker's perspective. The transmission line with the smallest difference between power limitation and actual power flow is selected as the target line. The nodes that connect this particular line are selected as nodes to compromise [2]. Algorithm 6 present our formulated pseudocode for the FDIA with minimum effort from the attackers' perspective.

Table 3.2: Generation cost increase under minimum effort FDIA(\$hr)

Bus-Systems	Normal systems state	Minimum effort attack
6-bus systems	3046.413	3059.031 (0.41%)
9-bus systems	5216.026	5216.477 (0.008%)
30-bus systems	951.62	951.62 (0%)
118-bus systems	125947.88	125948.37 (0.0004%)

To evaluate the performance of the FDIA with a minimum effort from the attackers' perspective, we have conducted a series of experiments on the standard IEEE 6, 9, 30, and 118 bus systems. We have found that there is no significant increase in the power generation cost when different bus systems are attacked with minimum effort from the attackers' perspective. As shown in table 5.1 the attack deviates the minimum cost of power generation by up to 0.41%, 0.008%, 0.0004% for the IEEE 6-bus, 9-bus, and 118-bus respectively. Hence, the attack with minimum effort does not have a significant impact on the cost of power generation. Therefore, we need to formulate an attack strategy that will provide a significant impact on the bus systems.

Algorithm 6 Minimum effort attack algorithm

$P_{L_i}^{max} \leftarrow$ Power limitation on transmission lines L_i
 $P_{L_i} \leftarrow$ Actual power on transmission lines L_i
 $\text{From-Node}_{L_i} \leftarrow$ Node connected to transmission lines L_i
 $\text{To-Node}_{L_i} \leftarrow$ Node connected to transmission lines L_i
 $N \leftarrow$ Number of transmission lines in the network
 $T \leftarrow$ Attack target

while $i \leq N$ **do**

$$\left| \Delta P_{L_i} = \left| P_{L_i}^{max} - P_{L_i} \right| \right|$$

end

sort ΔP_{L_i} in ascending order

$T \leftarrow L_1$: Minimum effort FDIA

while $j \leq \text{Iterations}$ **do**

$$P_d^{\text{From_Node}_T} = P_d^{\text{From_Node}_T} - \text{Attack_intensity}$$

$$P_d^{\text{To_Node}_T} = P_d^{\text{To_Node}_T} + \text{Attack_intensity}$$

if $\left| P_{L_i}^{max} - P_{L_i} \right| = 0$ **then**

$$\left| \Delta P_d^i = j \right|$$

end

end

3.5 Unbounded effort FDIA

Algorithm 7 presents the pseudocode for the FDIA attack with an unbounded effort from the attackers' perspective. In the algorithm, the attacker performs reconnaissance in the first step to explore information related to the power systems. The second step highlight how the attacker executes FDIA. To execute an FDIA with an unbounded effort, the transmission line with the highest difference between actual power flow and its power limitation is selected as the preferred target line. To select the target node, a defined parameter called C is calculated using the generators' cost coefficients, power flow, and average power flow difference. The node with the highest C value is selected as the preferred target node. The attacker executes a collusive strategy to falsify load demand on two nodes simultaneously. The same amount of load demand is added on one node and decreases on the other node of the target transmission line. This is to preserve the power balance equation so that the power systems remain stable after the attack execution. To evaluate the performance of the FDIA with an unbounded effort, we have conducted experiments on the standard IEEE 6-bus and 9-bus systems. Table 5.2 and Table 5.3 presents the C value calculations for the 6-bus and 9-bus systems. As shown in table 5.4 the attack deviates the cost of power generation by up to 2.74% and 0.5% on the IEEE 6-bus and 9-bus, respectively. Also, the attack with an unbounded effort does not have a significant impact on the cost of power generation. Therefore, we formulated an APT-base FDIA strategy with the intention of providing a significant impact on the bus systems in terms of power generation cost and the impact on the physical components of the power systems.

Algorithm 7 Unbounded effort Attack algorithm

STEP 1: Collection of information

$P_d^i \leftarrow$ Power demand at node i

$P_{L_i}^{max} \leftarrow$ Power limitation on transmission lines L_i

$P_{L_i} \leftarrow$ Actual power on transmission lines L_i

$\Delta P_{L_i} \leftarrow$ Difference between power flow and power limitation on transmission lines L_i

$From - Node_{L_i} \leftarrow$ Node connected to transmission lines L_i

$To - Node_{L_i} \leftarrow$ Node connected to transmission lines L_i

$Tp \leftarrow$ Power systems topology

$N \leftarrow$ Number of nodes

$T \leftarrow$ Target node

Generator cost coefficients $\leftarrow ai, bi, ci$

$T_i \leftarrow$ Target node

STEP 2: Attack execution

$$\Delta P_{L_i} = P_{L_i}^{max} - P_{L_i}$$

$$C = \begin{cases} ai + bi + ci & \text{if } P_g^1 = P_g^2 \dots = P_g^N \\ \max((ai + bi + ci) * P_g^i + \overline{\Delta P_{L_i}}) & \text{otherwise} \end{cases}$$

$T_i \leftarrow$ Node with highest C value

$$P_d^{From_Node_{T_i}} = P_d^{From_Node_{T_i}} - Attack_intensity$$

$$P_d^{To_Node_{T_i}} = P_d^{To_Node_{T_i}} + Attack_intensity$$

$$\sum_{i=1}^N P_d^i(Before_attack) = \sum_{i=1}^N P_d^i(After_attack)$$

Table 3.3: 6 Bus-system C values calculation

Bus	ai	bi	ci	pg	(ai+bi+ci)pg	$\overline{\Delta P_{L_i}}$	Ci
1	0.005	11.669	213.1	50	11238.72	30	337161.49
2	0.008	10.333	200	88.07	18525.56	33.344	617709.39
3	0.007	10.833	240	71.92	18042.04	39.512	712874.60

Table 3.4: 9 Bus system C values calculation

Bus	ai	bi	ci	pg	(ai+bi+ci) *pg	$\overline{\Delta P_{L_i}}$	Ci
1	0.11	5	150	86.56	13427.01	163.436	2194451.68
2	0.085	1.2	600	134.37	80799.23	384.378	31057414.94
3	0.123	1	335	94.05	31614.97	205.942	6510854.12

Table 3.5: Generation cost increase under minimum effort FDIA(\$hr)

Bus-Systems	Normal systems state	Unbounded effort attack
6-bus systems	3046.413	3129.886 (2.74%)
9-bus systems	5216.026	5246.593 (0.5%)

CHAPTER 4

RULE-BASED DETECTION SYSTEM FOR FDIA

This section presents the detection and prevention system for the FDIA in power systems. We have a primary detection feature and four secondary detection features. Both primary and secondary detection features help in detecting and preventing FDIA in power systems. First, the detection and prevention systems checks the primary detection feature. If the primary detection feature is true, the system proceed to check the secondary detection features.

The primary detection feature is a surge in generation cost that is greater than a threshold value denoted by $C_{threshold}$. The secondary detection features are checked as follows: for the first secondary detection feature, the detection and prevention system checks if there is a change in load demand and the changes is an increase and decrease in load demand in the power systems. This is being done by comparing the present load demand value and the previous load demand value of every node in the power

systems. The first secondary detection feature is donated by $+/-$.

For the second secondary detection feature, the detection and prevention systems checks if the increase in load demands happened on one node and the decrease in load demands happened on another node in the power systems network. This detection feature is donated by T-N which represent the target nodes and it is the second secondary detection feature that helps in determining if the system is under FDIA attacks or not. For the third detection feature, the detection and prevention systems check if the load demand increases and decreases by the same amount on different nodes within the power systems. This secondary detection feature is donated by $\pm P_d$. It is the third detection feature that helps us determine if the power system is under FDIA attacks or not.

Lastly, for the fourth secondary detection feature, the detection and prevention systems checks if the change in load demand, that is increase in load demand on one node and decrease in load demand on another node happened at the same time. This detection feature is donated by δt . As shown in table 4.2 an AND logic operator is used to determine if all the secondary detection features are true. Also, the table present all possible combinations of all secondary detection features.

If all the secondary detection feature are true, the detection and prevention system will trigger an attack alarm and revert the system configuration to the previous normal system configuration. This will prevent the impact of the FDIA on the cost of power generation and the impact on the physical components of the power systems.

To evaluate the performance of the detection and prevention system, we have used accuracy metrics. The accuracy metrics are the True Positive (TP) rate, True Nega-

tive (TN) rate, False Positive (FP) rate, and False Negative (FN) rate. A threshold parameter τ_{pd} is used to control the accuracy metrics of the detection systems.

The accuracy metric TP indicates when there is an attack and our detection system detects that attack. The accuracy metric TN indicates when there is no attack and our detection system did not detect an attack. The accuracy metric FP indicates when there is no attack and our detection system detects an attack in the system. The accuracy metric FN indicates when there is an attack and our detection system detects no attack in the systems. Therefore, both TP and TN shows the good side of our detection systems, while the FP and FN show the bad side of the detection systems.

Throughout our simulation studies, we have found that the value of FP is zero for all the standard bus systems under investigation, this means that our detection systems never indicate the presence of an attack when there no actual attack happening in the system. Therefore, the only important metrics that shows the performance of our detection systems are the TP, TN, and FN.

To determine the sensitivity of the detection system we find the threshold value that minimizes the number of FP. The threshold parameter is donated by τ_{pd} and it is determined by running multiple simulations on the IEEE bus systems. As shown in figure 5.10, 5.13, 5.16, and 5.19 we have found that the rate of FN become very low as the value of load demand threshold τ_{pd} increases. Specifically, in the 6-bus systems the FN rate approaches 0 when $\tau_{pd} > 130MW$. In the 9-bus systems the FN rate approaches 0 when $\tau_{pd} > 300MW$. In the 30-bus systems the FN rate approaches 0 when $\tau_{pd} > 150MW$. In the 118-bus systems the FN rate approaches 0 when

$\tau_{pd} > 1200MW$.

To prevent FDIA, after the system detected there is an attack, the system reverts the power system state and configuration to the previously known normal operation state of the system. This helps in combating the increase in generation costs incurred by the FDIA.

Table 4.1: Truth table of the secondary FDIA detection features

Feature 1 (+/-)	Feature 2 (T-N)	Feature 3 ($\pm P_d$)	Feature 4 (δt)	$(+/-) \wedge (T-N) \wedge (\pm P_d) \wedge (\delta t)$
False	False	False	False	False
False	False	False	True	False
False	False	True	False	False
False	False	True	True	False
False	True	False	False	False
False	True	False	True	False
False	True	True	False	False
False	True	True	True	False
True	False	False	False	False
True	False	False	True	False
True	False	True	False	False
True	False	True	True	False
True	True	False	False	False
True	True	False	True	False
True	True	True	False	False
True	True	True	True	True

CHAPTER 5

RESULTS AND DISCUSSIONS

In this section, we first present the simulation environment and the simulation setup. Next, we present our simulation results of FDIA with minimum and unbounded effort from the attackers' perspective. Next, we present the results of our proposed APT-based FDIA that intends to maximize the power generation cost and the detection mechanism that intends to mitigate such attacks in power systems. Last we compare our results with the previously proposed FDIA from the literature.

5.1 Simulation setup

The impact of FDIA on the power systems is studied using simulation. Specifically, the impact on the cost of power generation and the impact on the operation of the generators in power systems is investigated. Also, the attacks were simulated on the IEEE bus systems using MATPOWER Matlab package [14]. MATPOWER is an open-source and free tool for electric power systems simulations. All simulations are carried out on a 2.3GHz Intel Core i5 CPU and 8GB RAM laptop.

Table 5.1: Simulation parameters

Notation	Value	Notation definition
T_{max}	1000	Maximum temperature
T_{min}	0	Minimum temperature
C	0.99	Cooling rate
P	50	Population size
$\tau - P_d$	N/A	Dynamic false load demand
T_{list}	N/A	Dynamic Tabu list
C_{init}	3046.03	6-bus systems initial cost
C_{init}	5216.03	9-bus systems initial cost
C_{init}	951.62	30-bus systems initial cost
C_{init}	125947.9	118-bus systems initial cost
$C_{threshold}$	N/A	Dynamic cost increase threshold

Table 5.1 present simulation parameters. It include the maximum temperature and cooling rate for the simulated annealing, the population size for the genetic algorithm and particle swarm optimization algorithms, tabu list does not have a specific value because the is dynamic, the initial cost of all the standard IEEE bus systems under investigation. We have chosen a very high temperature and a small cooling rate in order to observe the behaviour of simulated annealing when solving the optimization problem. We have chosen population size of 50, which is enough to observe the behavior of genetic and particle warm optimization algorithms. The initial cost of 3046.03 dollars per hour, 5216.03 dollars per hour, 951.62 dollars per hour, 125947.9 dollars per hour are the normal cost of power generation when the system is under normal operation without FDIA attacks.

$C_{threshold}$ represent the cost increase threshold which is a dynamic value. The $C_{threshold}$ unit is in dollar per hour and it the value the system can afford to lose. This cost increase threshold lead to the relationship between the generation cost of the power system and the accuracy metrics of the detection and prevention system. When the attacker falsify the load demand and the increase in generation cost in less than the $C_{threshold}$ the detection system will not be able to detect this attack because is incur negligible effect on the system. This leads to the occurrence of the FN. That is is an actual attack and the detection system detects no attack in the systems due to the negligible impact of the attack.

In the coming sections, we present the simulation results of our proposed APT-based FDIA strategy using the IEEE 6-Bus, 9-bus, IEEE 30-Bus, and IEEE 118-

Bus. The results are summarized in Table 5.9. We compare our attack model with the attack in [2]. Each simulation is repeated 10 times to get better confidence in determining the maximum increase in generation cost. Tables 5.5, 5.6, and 5.7 presents the maximum, average, and minimum cost increase of the ten (10) simulation runs where we highlighted the highest generation cost increase in bold for the different bus systems.

5.2 APT-based FDIA on IEEE 6 Bus systems

To evaluate the proposed FDIA, the IEEE 6-bus system is used as a test case to investigate the impact of FDIA against OPF in power systems. The system is composed of six buses with three generators at bus numbers 1, 2, and 3. Moreover, eleven transmission lines connect all buses to form a power system network. Figure 5.1 presents the results of attacks on 6-bus systems. From the figures, the attacker is able to achieve an up to 15.6% increase in the cost of power generation when the standard IEEE 6-bus system is attacked. Moreover, to analyze the effect of the FDIA on generators, we have recorded the generator out variation of all generators in the system both before and after the attack execution. Figure 5.2 present the generator output variation. As shown in the figure, the output of the generator at bus number 1 increases from 50 MW to 120.28 MW due to the FDIA attack. Therefore, the attack cause a significant impact on the generator at bus number 1. Moreover, as shown in figures 5.1, 5.3, 5.5, and 5.7 we have observed a fluctuation when solving the optimization problem using simulated annealing. This is because the simulated annealing algorithm is a

single solution based metaheuristics and it combines both the notion of exploring and exploiting. Exploring is the idea of visiting more search space with the hope that the algorithm will get a better solution. However, the notion of exploiting is that the algorithm is always trying to find a global optimum as quickly as possible, this can lead it to stuck at a local optimum. That is, during the hill-climbing, the algorithm always wanted to exploit. Combining the two notions exploring and exploiting manse that the algorithm does not always improve, sometimes the algorithm wander away from the current system state with the hope of finding a better system state in next iteration.

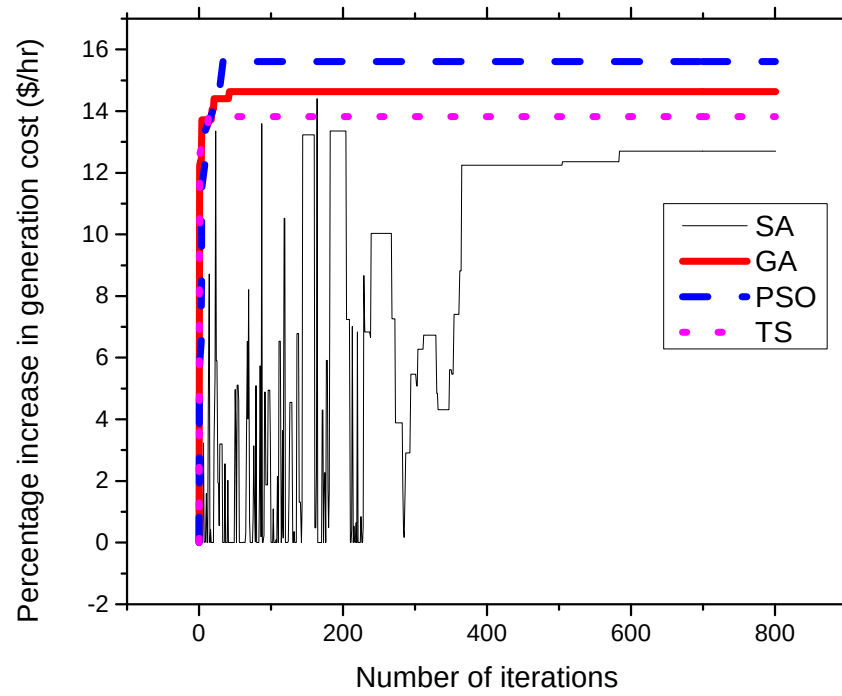


Figure 5.1: 6-Bus systems Percentage increase in generation cost

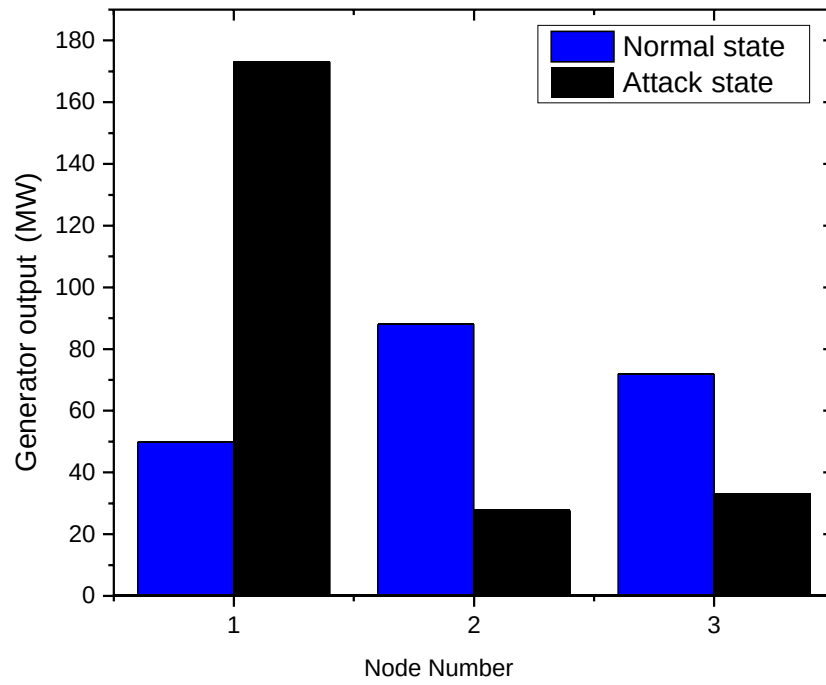


Figure 5.2: 6-bus systems generator output variation

5.3 APT-based FDIA on IEEE 9-bus system

The IEEE 9-bus system consists of nine buses with three generators at bus number 1, bus number 2, and bus number 3. Moreover, nine transmission lines connect all buses in the system to form a power system network. Figure 5.3 presents the results of attacks on 9-bus systems. From the figures, the attacker can achieve an up to 45.1% increase in the cost of power generation when the standard IEEE 9-bus system is attacked. Moreover, as shown in figure 5.4 the attack cause a significant impact on the generator at bus number 2 for the standard 9-bus systems. The output of the generator increases from 134.38 MW to 269.30 MW due to the FDIA attack. This the major factor that leads to an increase in power generation cost.

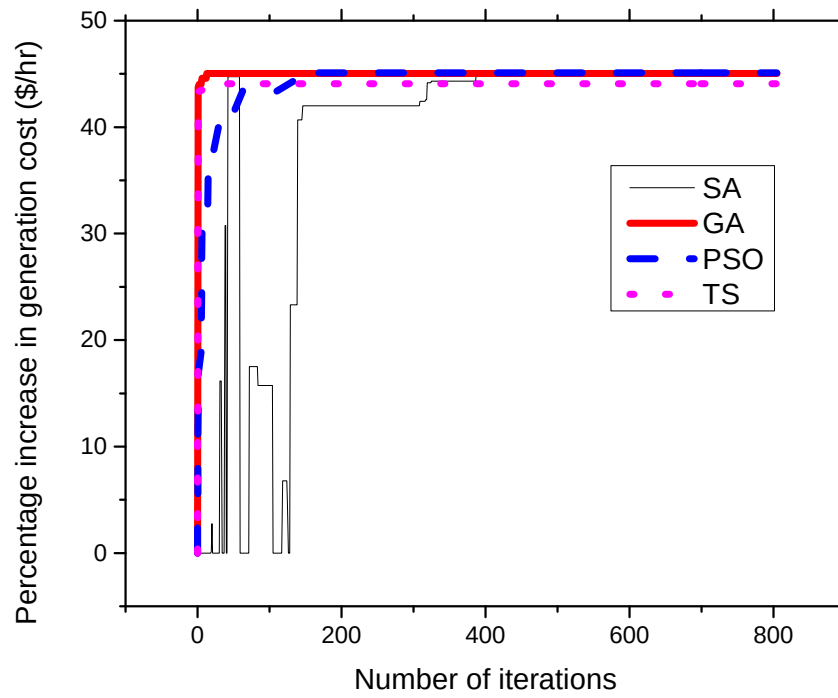


Figure 5.3: 9-Bus systems Percentage increase in generation cost

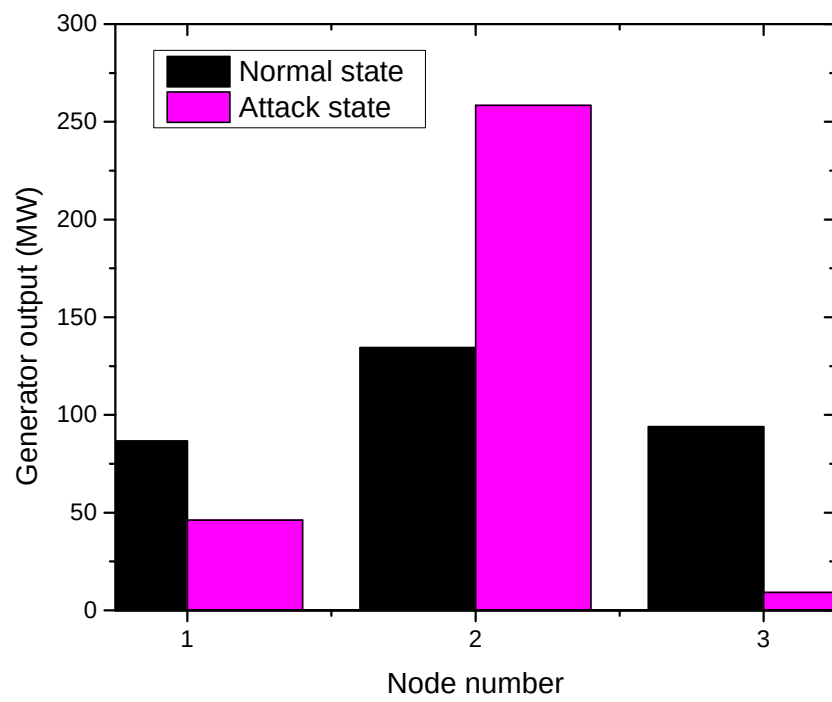


Figure 5.4: 9-bus systems generator output variation

5.4 APT-based FDIA on IEEE 30-bus system

The 30-bus system consists of thirty buses. Moreover, these buses are connected with 41 transmission lines to form the power system network. The system also consists of six generators connected to bus numbers 1, 2, 5, 8, 11, and 13.

Figure 5.5 presents the results of attacks on the 30-bus systems. From the figures, the attacker can achieve an average of up to 57.7% increase in the cost of power generation when the standard IEEE 30-bus systems is attacked. As shown in figure 5.6 The attacks cause a significant impact on the generator at bus number 1. The output of the generator increases by about 70 MW due to the FDIA attack. Consequently, it leads to the increase in the fuel cost.

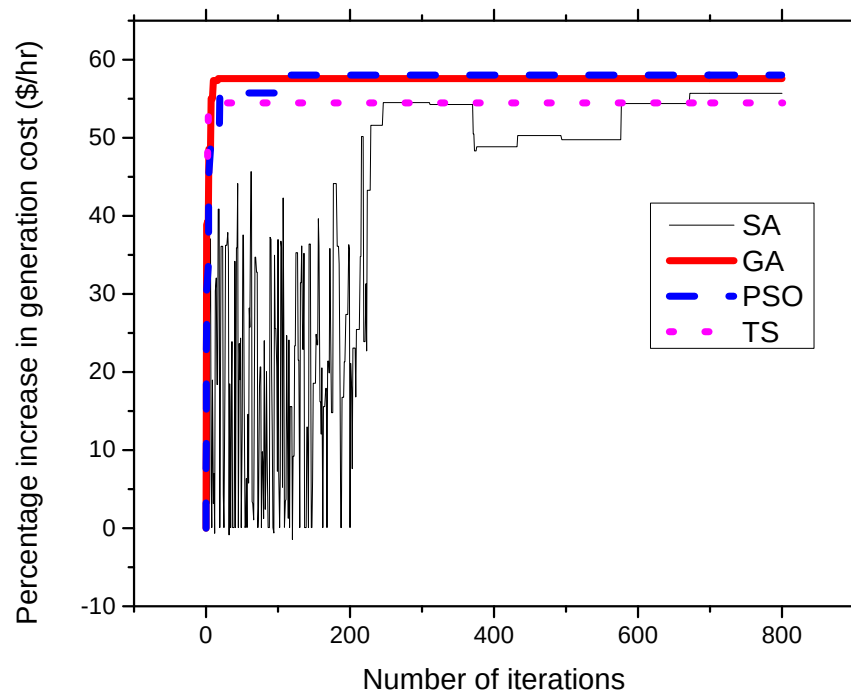


Figure 5.5: 30-Bus systems Percentage increase in generation cost

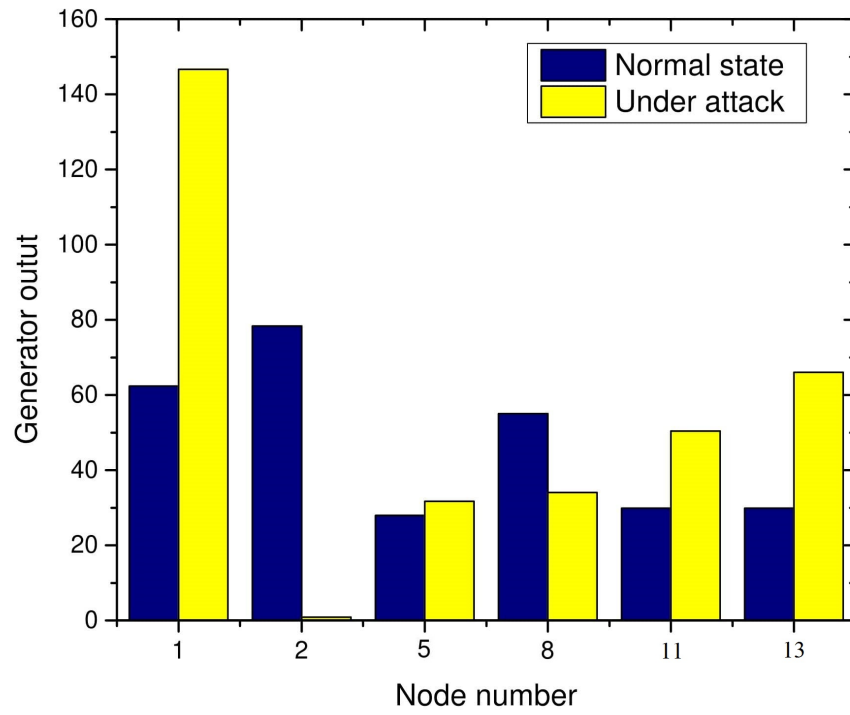


Figure 5.6: 30-Bus systems generator output variation

5.5 APT-based FDIA on IEEE 118-bus system

The 118-bus system consists of 118 buses with 54 generator buses. The buses are connected by 186 transmission lines to form the power system network. Figure 5.7 presents the results of attacks on the 118-bus systems. From the figures, the attacker can achieve an average of up to 71.7% increase in the cost of power generation when the standard IEEE 118-bus system is attacked. As shown in figure 5.8, the attack cause a significant impact on the generator at bus number 69. The output of the generator increases from 500.43 MW to 796.06 MW due to the FDIA attack.

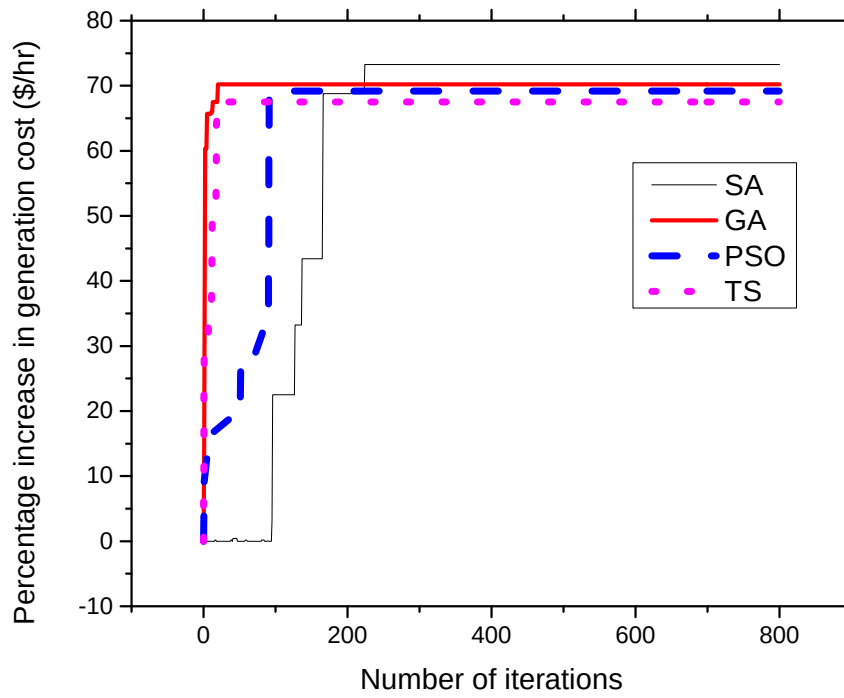


Figure 5.7: 118-Bus systems Percentage increase in generation cost

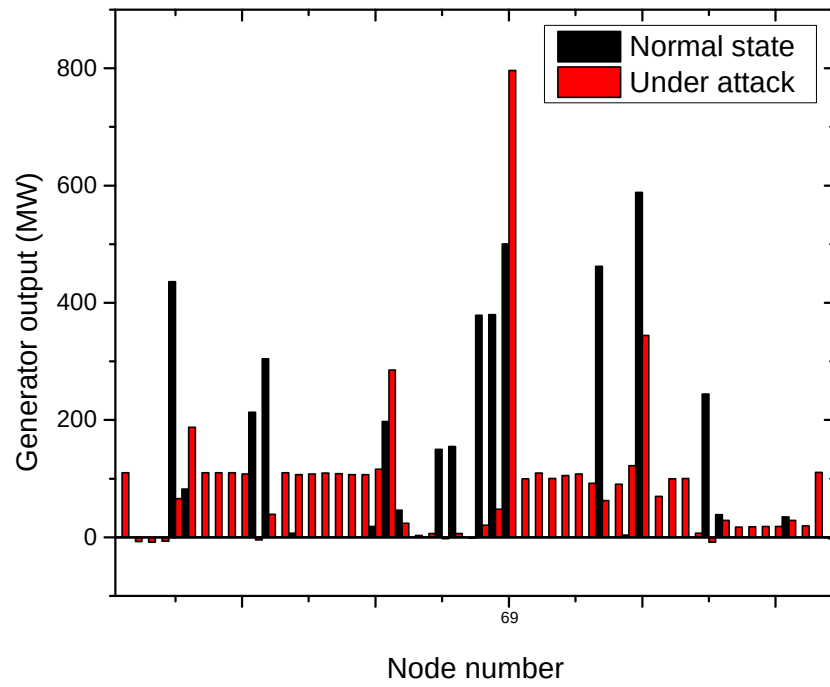


Figure 5.8: 118-Bus systems generator output variation

Table 5.2: Maximum cost increase under attack on different bus systems using SA

Simulation runs	6-Bus (\$/hr)	9-Bus (\$/hr)	30-Bus (\$/hr)	118-Bus (\$/hr)
Simulation run 1	3488.35	7557.44	1485.48	218240.65
Simulation run 2	3491.73	7564.83	1481.58	215867.44
Simulation run 3	3488.35	7564.83	1497.38	215690.66
Simulation run 4	3488.35	7564.83	1513.71	212166.41
Simulation run 5	3484.90	7527.79	1497.38	219180.72
Simulation run 6	3491.73	7550.05	1507.05	217627.96
Simulation run 7	3491.73	7533.40	1517.57	212672.88
Simulation run 8	3491.73	7564.83	1496.63	217456.22
Simulation run 9	3491.73	7564.83	1485.47	215325.55
Simulation run 10	3491.73	7564.83	1517.57	218895.35

Table 5.3: Maximum cost increase under attack on different bus systems using GA

Simulation runs	6-Bus (\$/hr)	9-Bus (\$/hr)	30-Bus (\$/hr)	118-Bus (\$/hr)
Simulation run 1	3491.73	7564.81	1499.44	214387.45
Simulation run 2	3491.72	7564.83	1513.71	212108.16
Simulation run 3	3491.74	7564.82	1494.56	214387.45
Simulation run 4	3491.73	7564.83	1507.05	214387.45
Simulation run 5	3491.74	7564.82	1513.71	214387.45
Simulation run 6	3491.73	7564.81	1517.57	214387.45
Simulation run 7	3491.72	7564.82	1517.57	214387.45
Simulation run 8	3491.72	7564.83	1505.2	212108.16
Simulation run 9	3491.74	7564.82	1513.71	214387.45
Simulation run 10	3491.72	7564.83	1513.71	212108.16

Table 5.4: Maximum cost increase under attack on different bus systems using PSO

Simulation runs	6-Bus (\$/hr)	9-Bus (\$/hr)	30-Bus (\$/hr)	118-Bus (\$/hr)
Simulation run 1	3498.23	7568.70	1503.34	217031.53
Simulation run 2	3494.46	7568.70	1523.75	213059.88
Simulation run 3	3504.41	7538.70	1492.11	218954.18
Simulation run 4	3492.21	7568.70	1511.98	215999.65
Simulation run 5	3504.41	7508.76	1522.49	212977.36
Simulation run 6	3507.06	7478.89	1493.90	215999.65
Simulation run 7	3495.49	7568.70	1507.76	211535.02
Simulation run 8	3492.21	7538.69	1497.49	215786.91
Simulation run 9	3521.65	7508.76	1503.14	218145.06
Simulation run 10	3507.95	7568.70	1503.98	217327.12

Table 5.5: Maximum cost increase under attack on different bus systems using TS

Simulation runs	6-Bus (\$/hr)	9-Bus (\$/hr)	30-Bus (\$/hr)	118-Bus (\$/hr)
Simulation run 1	3467.0	7478.89	1469.0	211000
Simulation run 2	3467.0	7478.89	1470.0	211000
Simulation run 3	3455.64	7478.89	1470.0	212500
Simulation run 4	3467.0	7515.0	1470.0	211000
Simulation run 5	3467.0	7515.0	1470.0	211000
Simulation run 6	3455.64	7515.0	1470.0	212500
Simulation run 7	3455.64	7478.89	1469.0	212500
Simulation run 8	3455.64	7478.89	1469.0	212500
Simulation run 9	3467.64	7515.0	1469.0	212500
Simulation run 10	3467.64	7515.0	1469.0	212500

Table 5.6: Minimum, average, and Maximum cost increase under attack on different bus systems

Bus systems	Metaheuristics	Min. cost (\$/hr)	Avg. cost (\$/hr)	max. cost (\$/hr)
6-Bus System	SA	3484.9	3490.03	3491.73
	GA	3491.72	3491.73	3491.74
	PSO	3492.21	3501.80	3521.65
	TA	3455.64	3462.456	3467
9-Bus System	SA	7527.79	7555.77	7564.83
	GA	7564.81	7564.82	7564.83
	PSO	7478.89	7541.73	7568.70
	TA	7478.89	7496.945	7515
30-Bus System	SA	1481.58	1499.982	1517.57
	GA	1494.56	1509.62	1517.57
	PSO	1492.11	1505.99	1523.75
	TA	1469	1469	1470
118-Bus System	SA	212166.41	216312.38	219180.72
	GA	212108.16	213703.66	214387.45
	PSO	211535.02	215681.64	218954.18
	TA	211000	211900	212500

Table 5.7: Comparison between our work and the work in [2]

Bus systems	Normal	Min. Effort [6]	APT-based
6-bus systems	3046.41	3256.37	3521.65
		(6.89%)	(15.6%)
9-bus systems	5216.03	6652.88	7568.70
		(27.55%)	(45.1%)
30-Bus systems	951.62	1034.49	1523.75
		(8.7%)	(60.12%)
118-bus systems	125947.88	132697.88	219180.72
		(5.36%)	(74.02%)

5.6 FDIA Detection Results

In this section, we present the simulation results of our proposed detection and prevention system using the IEEE 6-Bus, 9-bus, IEEE 30-Bus, and IEEE 118-Bus. Also, the detection and prevention system is simulated using MATPOWER Matlab package [14]. All simulations are carried out on a 2.3GHz Intel Core i5 CPU and 8GB RAM laptop. Figures 5.9, 5.12, 5.15, and 5.18 present the generation cost both before and after deploying our detection and prevention system. The figures show that our detection and prevention system is capable of detecting and blocking the FDIA and take the systems back to the normal operation state. Accuracy metrics are used to evaluate the performance of the developed rule-based FDIA detection and prevention system.

Figures 5.11, 5.14, 5.17, and 5.20 present the percentage occurrence of the accuracy metrics at a specific load demand threshold value. The accuracy metrics are the True Positive (TP) rate, True Negative (TN) rate, False Positive (FP) rate, and False Negative (PN) rate. We have observed that the rate of the accuracy metric True Positive (TP) is greater than 90% for the all the IEEE standard 6,9,30, and 118 bus systems. This shows the good performance of our detection and prevention system. It also shows that the system almost always accurately detect the presence of an attack when there is an actual attack on the power systems. We have conducted several simulations to evaluate the sensitivity of the load demand threshold $\tau - P_d$. In addition, we have observed that the rate of the FP is always zero (0) on all the bus

systems under investigation. This also shows the good performance of our detection and prevention system. This is because, the accuracy metric FP indicates when there is no attack and a detection system detects an attack in the system. Therefore, when the value of FP is zero (0), this means that the detection and prevention never indicate the presence of an attack when there is no actual attack on the system. Also, the reason for the FP becoming zero (0) in our system is because there is no presence of noise during our simulation.

As shown in figure 5.10, 5.13, 5.16, and 5.19 we have found that the False Negatives (FN) rates become significantly low as the value of load demand threshold τ_{pd} increases. Specifically, the FN rates approaches 0 when $\tau_{pd} > 130MW$, $\tau_{pd} > 300MW$, $\tau_{pd} > 150MW$, and $\tau_{pd} > 1200MW$ for the standard IEEE 6-bus, 9-bus, 30-bus, and 118-bus systems respectively.

Figures 5.21 and 5.22 present the comparison of the percentage of occurrence of the accuracy metrics in our proposed detection and prevention system and the detection mechanism in [2] from the literature. From the figure the false positive rates of the detection mechanism proposed in in in [2] becomes significantly low as the value of load active power threshold approaches 40MW on both IEEE 30, and 118 bus systems. This means that their system performs better when the threshold value is greater than 40MW. On the other hand, our proposed detection and prevention system performs better when the threshold values approaches 150MW and 1200MW on the standard IEEE 30, and 118 bus systems respectively.

Finally, table A1-A11 in Appendix A presents the transmission line parameters

and the generator cost coefficients, where r , x , and b represent resistance, reactance, and susceptance respectively in per unit (P.u).

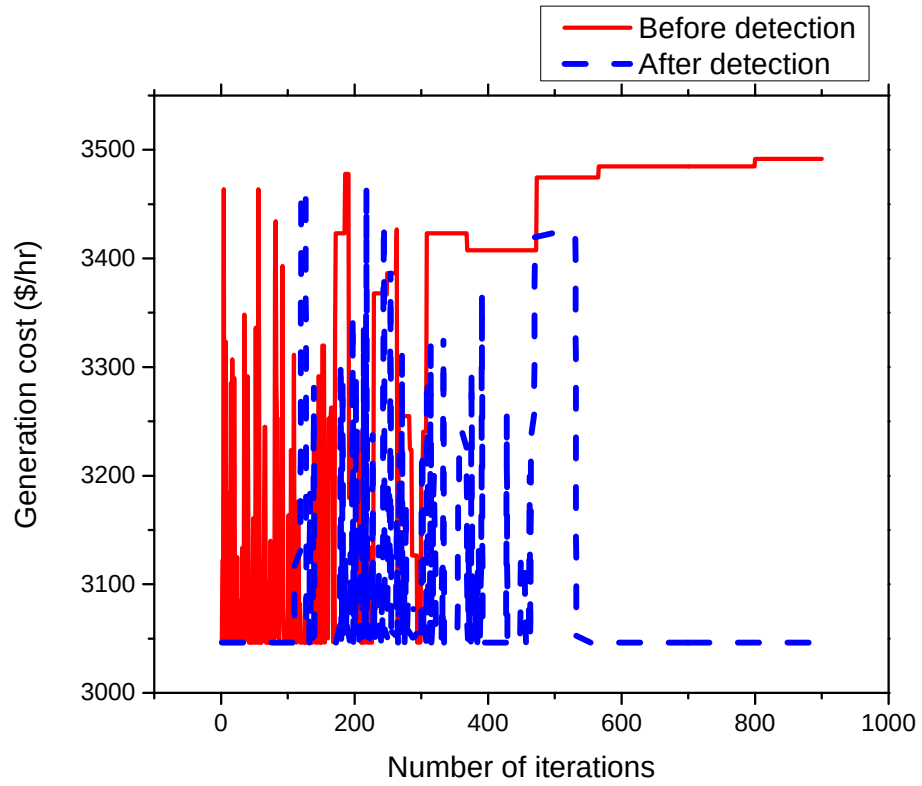


Figure 5.9: 6-bus increase in cost before and after detection and prevention

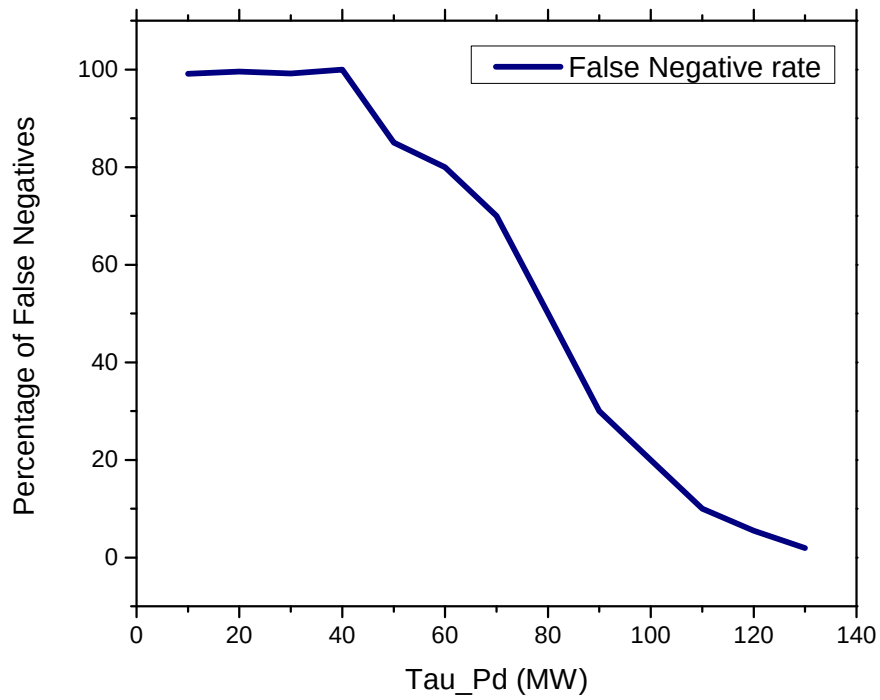


Figure 5.10: 6-bus Percentage of False Negatives (FN) accuracy metric vs Threshold

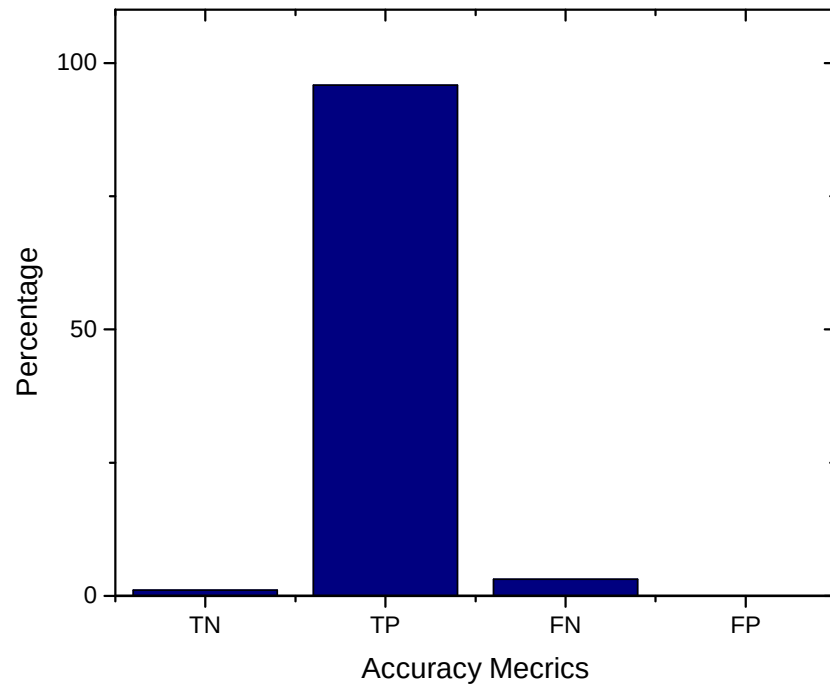


Figure 5.11: 6-bus systems accuracy metrics at $\text{Tau-P}_d = 130$

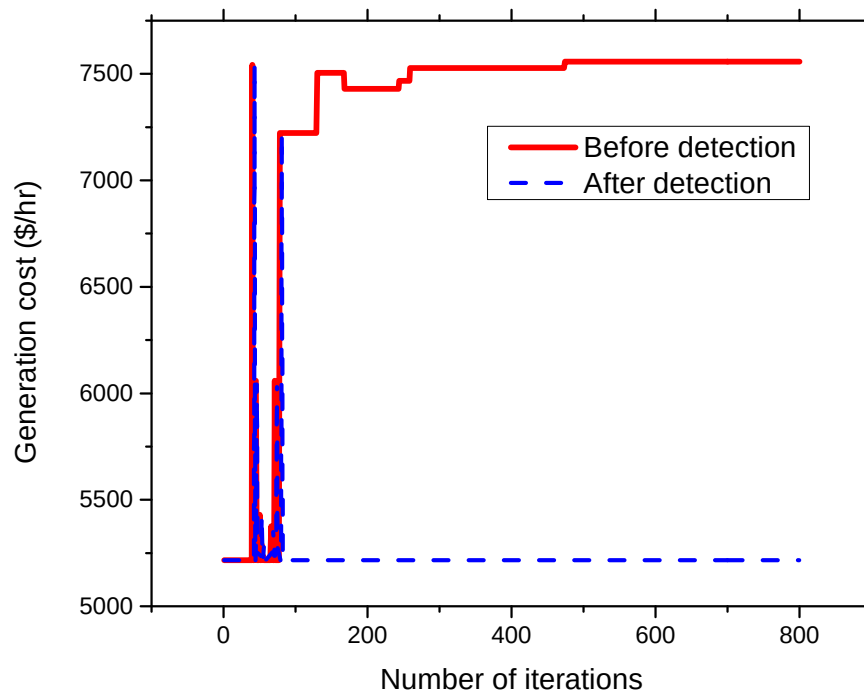


Figure 5.12: 9-bus increase in cost before and after detection and prevention

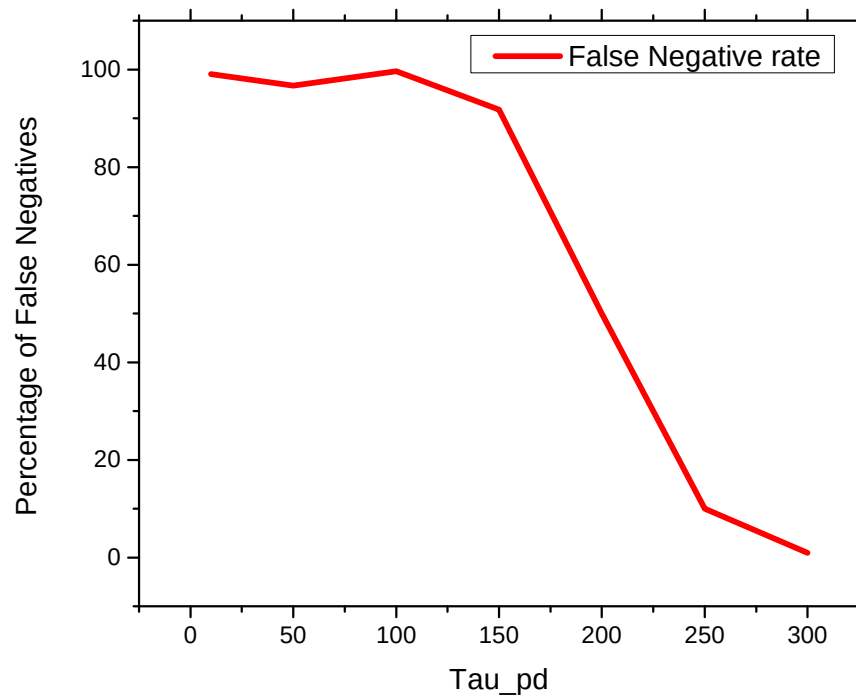


Figure 5.13: 9-bus Percentage of False Negatives (FN) accuracy metric vs Threshold

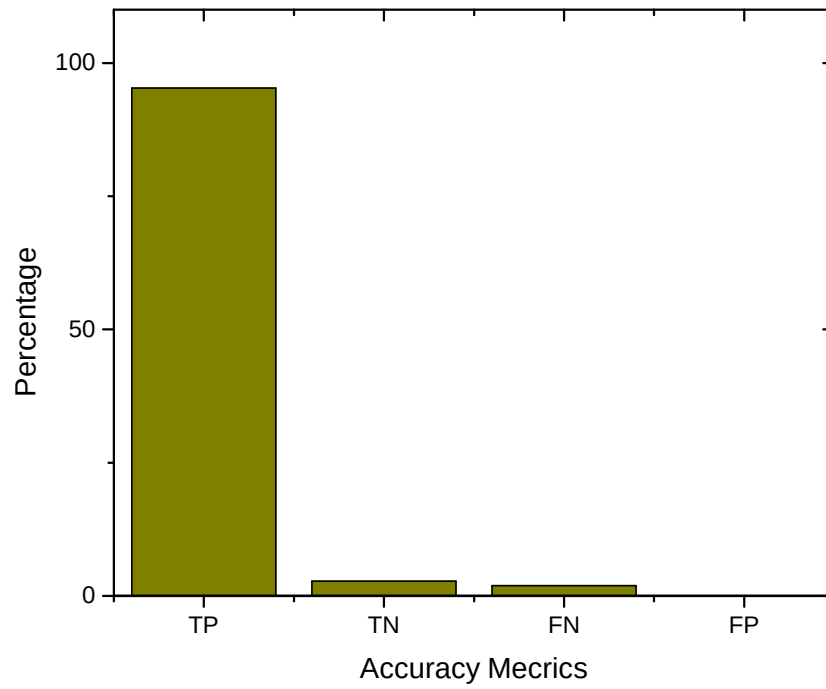


Figure 5.14: 9-bus systems accuracy metrics at $Tau - P_d = 300$

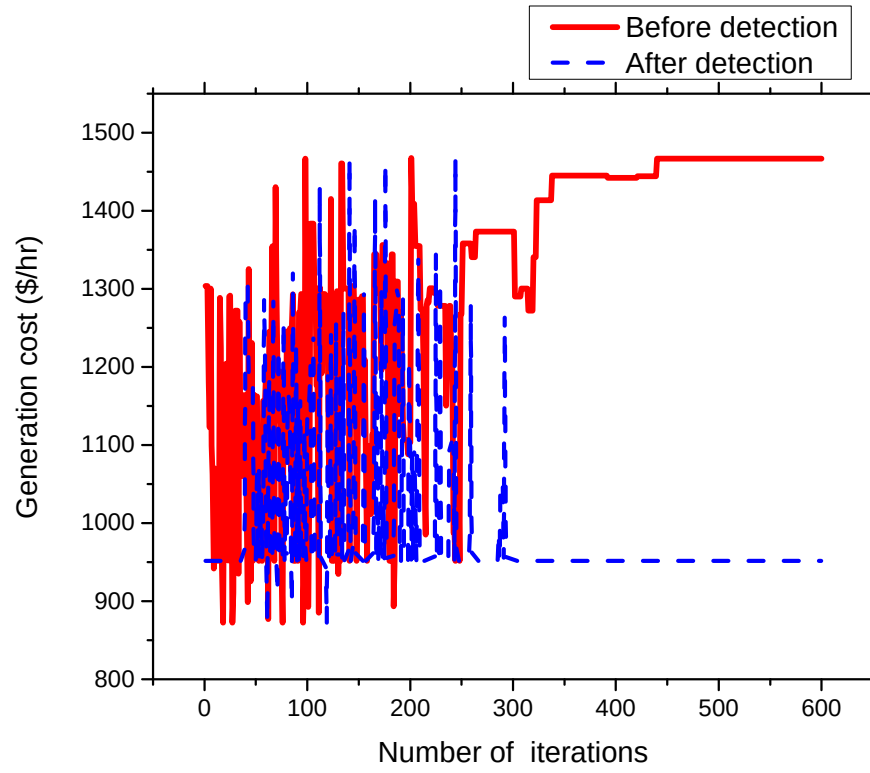


Figure 5.15: 30-bus increase in cost before and after detection and prevention

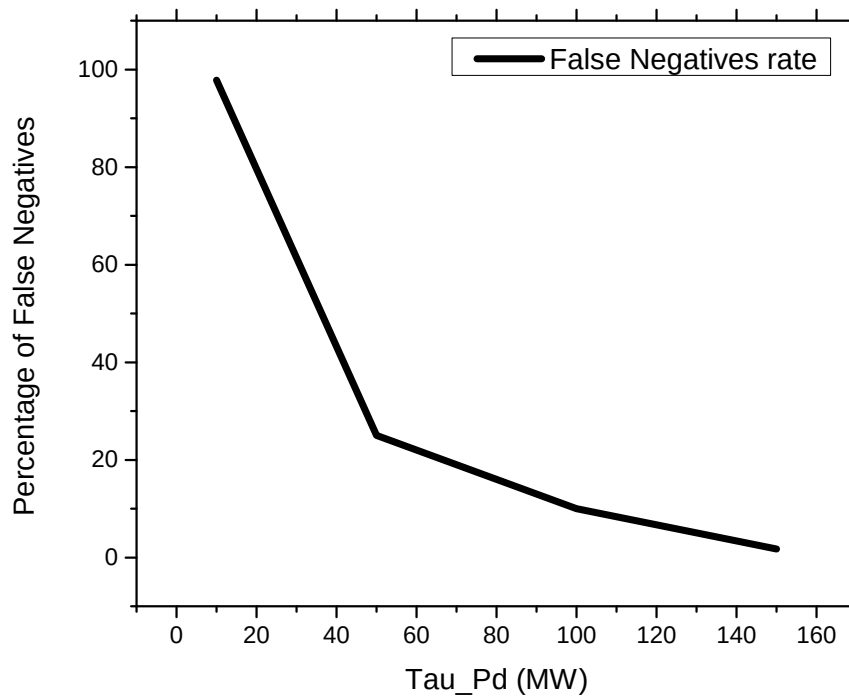


Figure 5.16: 30-bus Percentage of False Negatives (FN) accuracy metric vs Threshold

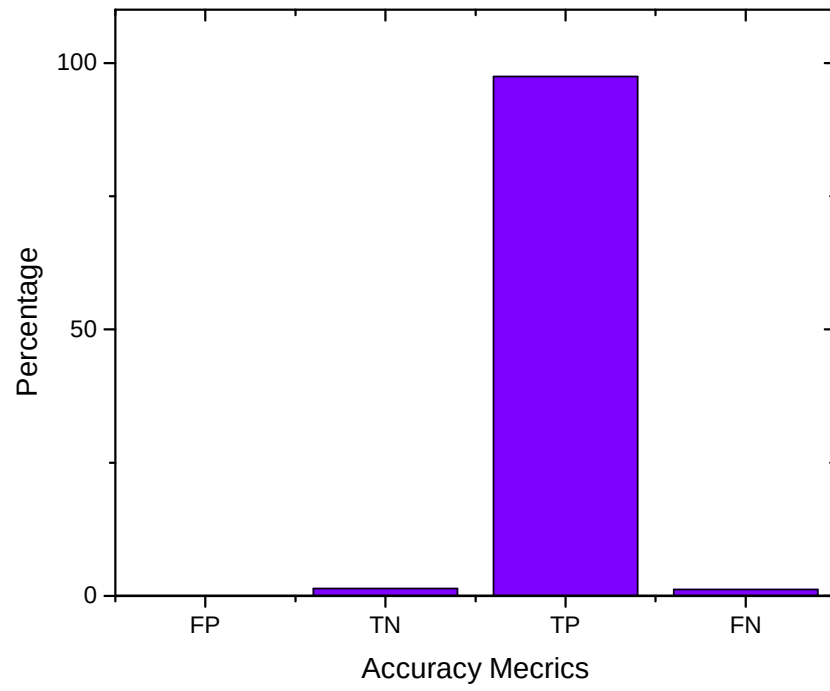


Figure 5.17: 30-bus systems accuracy metrics at $Tau - P_d = 150$

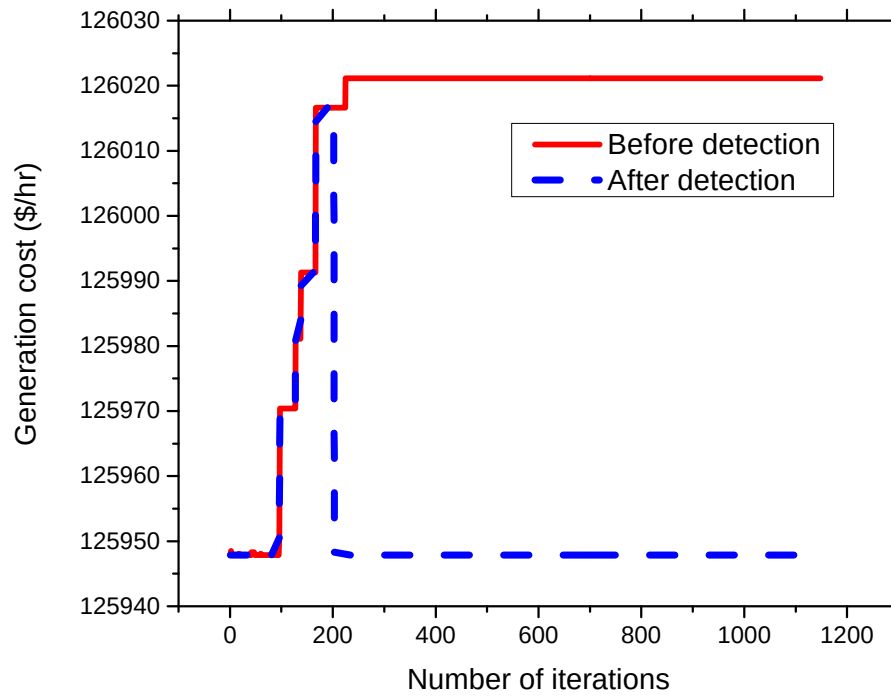


Figure 5.18: 118-Bus systems increase in cost before and after detection and prevention

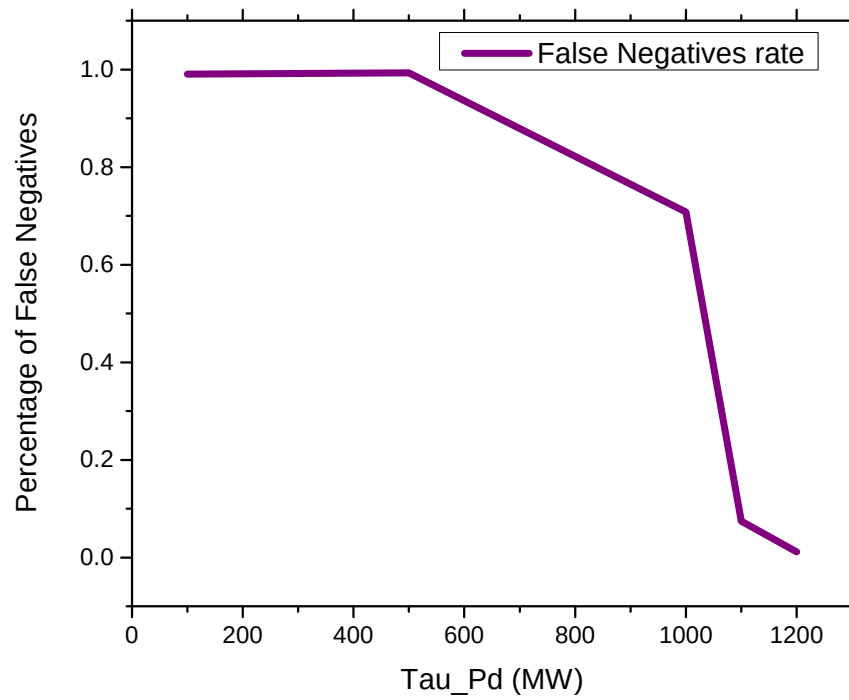


Figure 5.19: 118-bus Percentage of False Negatives (FN) accuracy metric vs Threshold

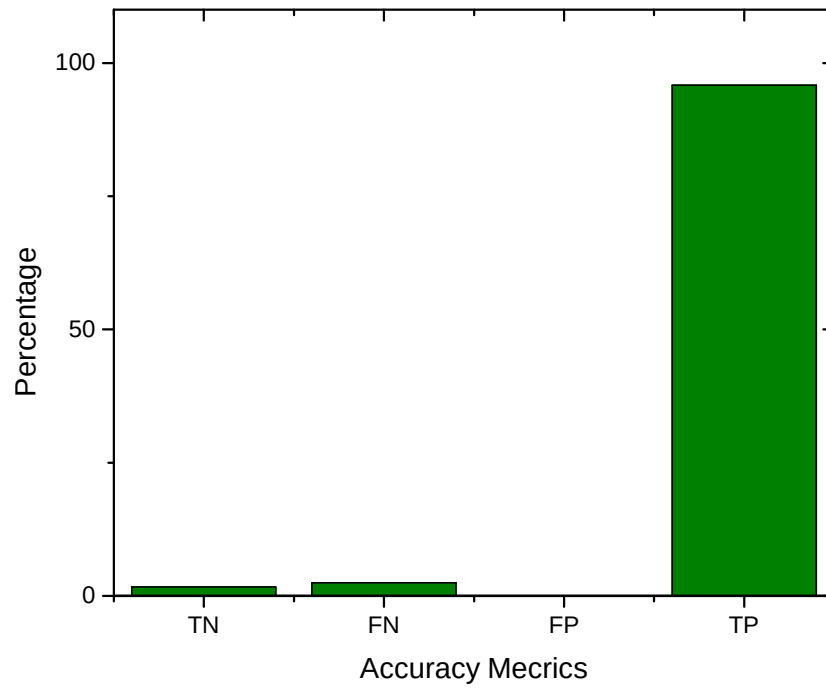


Figure 5.20: 118-bus systems accuracy metrics at $Tau - P_d = 1200$

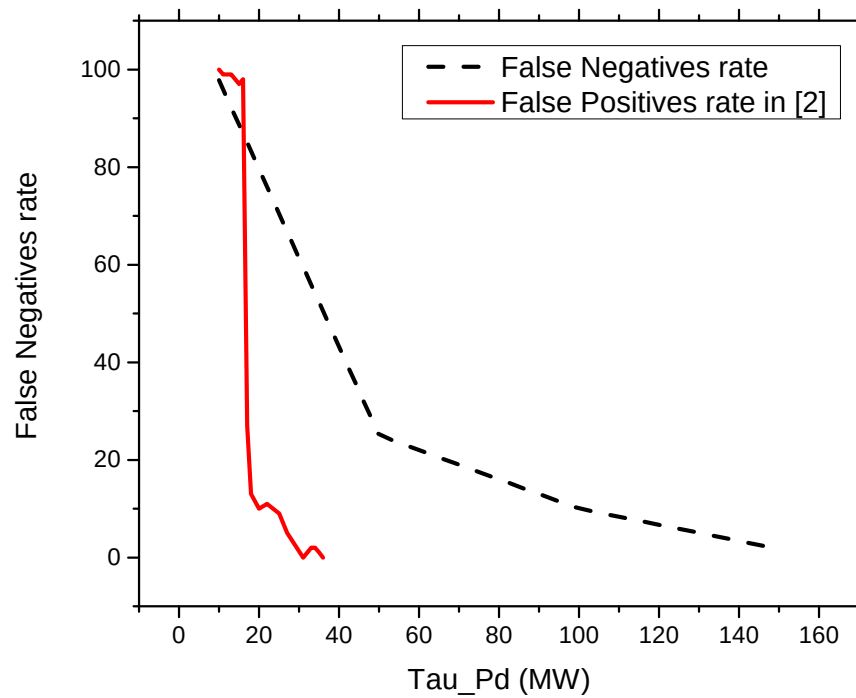


Figure 5.21: Comparison of accuracy metrics rates on 30-bus systems

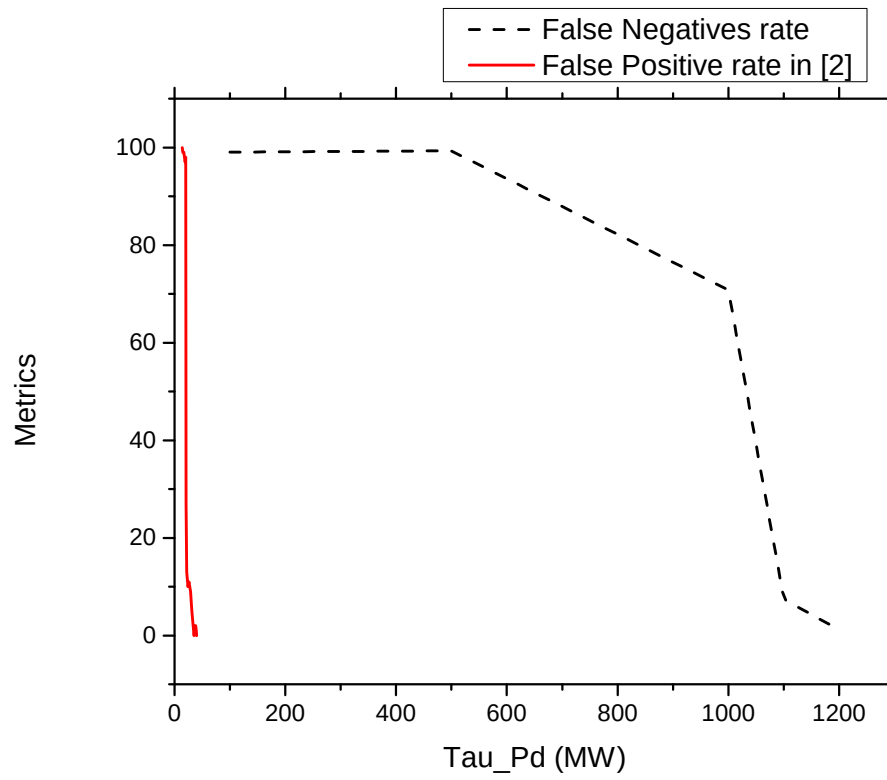


Figure 5.22: Comparison of accuracy metrics rates on 118-bus systems

CHAPTER 6

CONCLUSION AND FUTURE WORK

OPF is one of the most important modules in power systems that ensure the optimal operation of power systems. In this research, we have analyzed the impact of FDIA against OPF in power systems. Then, we have namely simulated annealing, genetic algorithm, and particle swarm optimization OPF is one of the most important modules in power systems that ensure the optimal operation of power systems. In this research, we have introduced a novel APT-based attack strategy with the objective to maximize the operation cost of power generation. We have modeled the attack strategy as an optimization problem. We have used metaheuristic algorithms, namely: Genetic Algorithm (GA), Simulated Annealing (SA) algorithm, Tabu Search (TS), and Particle Swarm Optimization (PSO) to solve the proposed optimization problem and obtain the attack plan. We have conducted several simulation scenarios and observed that our proposed attack strategy can increase the power generation cost by up to 15.6%, 45.1%,

60.12%, and 74.02% on the 6-bus, 9-bus, 30-bus, and 118-bus systems, respectively. Also, we have observed a fluctuation when solving the optimization problem using simulated annealing. This is expected, because the simulated annealing algorithm is a single solution based metaheuristics and it combines both the notion of exploring and exploiting. That is, during the hill-climbing, the algorithm always wanted to exploit. Combining the two notions of exploring and exploiting means that the algorithm does not always improve, sometimes the algorithm wanders away from the current system state with the hope of finding a better system state in next iteration. In addition, the attacks cause significant impact on the generators performance on the bus number 1, 2, and 69 for the 6-bus, 9-bus, 30-bus, and 118-bus systems respectively. We have developed a rule-based FDIA detection and prevention system with primary and secondary detection features. The system is able to detect and Prevent FDIA in power systems. Moreover, accuracy metrics are used to evaluate the performance of the developed rule-based FDIA detection and prevention system. We have found that the False Negatives (FN) rates become significantly low as the value of load demand threshold τ_{pd} increases. Specifically, the FN rates approach 0 when $\tau_{pd} > 130MW$, $\tau_{pd} > 300MW$, $\tau_{pd} > 150MW$, and $\tau_{pd} > 1200MW$ for the standard IEEE 6-bus, 9-bus, 30-bus, and 118-bus systems respectively. In the future we intend to use other metaheuristics algorithms to check the possibility of improving our results.

APPENDIX A

BUS SYSTEMS PARAMETERS

Table A.1: 6 Bus-system Transmission line Parameters

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
1-2	0.1	0.2	0.04	40
2-3	0.05	0.25	0.06	40
1-4	0.05	0.2	0.04	60
2-4	0.05	0.1	0.02	60
3-6	0.02	0.1	0.02	80
4-5	0.2	0.4	0.08	20
4-6	0.07	0.2	0.05	90
3-5	0.12	0.26	0.05	70
2-5	0.1	0.3	0.04	30
1-5	0.08	0.3	0.06	40
5-6	0.1	0.3	0.06	40

Table A.2: 6 Bus-system generator cost coefficients and limitations

Node number	a (\$)	b (\$)	c (\$)	Limit (MW)
1	0.00533	11.669	213.1	200
2	0.00889	10.333	200	150
3	0.00741	10.833	240	180

Table A.3: 9 Bus-system Transmission line Parameters

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
1-4	0	0.0576	0	250
4-5	0.017	0.092	0.158	250
5-6	0.039	0.17	0.358	150
3-6	0	0.0586	0	300
6-7	0.0119	0.1008	0.209	150
7-8	0.0085	0.072	0.149	250
8-2	0	0.0625	0	250
8-9	0.032	0.161	0.306	250
9-4	0.01	0.085	0.176	250

Table A.4: 9 Bus-system generator cost coefficients and limitations

Node number	a (\$)	b (\$)	c (\$)	Limit (MW)
1	0.11	5	150	250
2	0.085	1.2	600	300
3	0.1225	1	335	270

Table A.5: 30 Bus-system Transmission line Parameters

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
1-2	0.02	0.06	0.03	130
1-3	0.05	0.19	0.02	130
2-4	0.06	0.17	0.02	65
3-4	0.01	0.04	0	130
2-5	0.05	0.2	0.02	130
2-6	0.06	0.18	0.02	65
4-6	0.01	0.04	0	90
5-7	0.05	0.12	0.01	70
6-7	0.03	0.08	0.01	130
6-8	0.01	0.04	0	32
6-9	0	0.21	0	65
6-10	0	0.56	0	32
9-11	0	0.21	0	65
9-10	0	0.11	0	65
4-12	0	0.26	0	65
12-13	0	0.14	0	65
12-14	0.12	0.26	0	32
12-15	0.07	0.13	0	32
12-16	0.09	0.2	0	32
14-15	0.22	0.2	0	16
16-17	0.08	0.19	0	16
15-18	0.11	0.22	0	16
18-19	0.06	0.13	0	16
19-20	0.03	0.07	0	32
10-20	0.09	0.21	0	32
10-17	0.03	0.08	0	32
10-21	0.03	0.07	0	32
10-22	0.07	0.15	0	32
21-22	0.01	0.02	0	32
15-23	0.1	0.2	0	16
22-24	0.12	0.18	0	16
23-24	0.13	0.27	0	16
24-25	0.19	0.33	0	16
25-26	0.25	0.38	0	16
25-27	0.11	0.21	0	16
28-27	0	0.4	0	65
27-29	0.22	0.42	0	16
27-30	0.32	0.6	0	16
29-30	0.24	0.45	0	16
8-28	0.06	0.2	0.02	32
6-28	0.02	0.06	0.01	32

Table A.6: 30 Bus-system generator cost coefficients and limitations

Node number	a (\$)	b (\$)	c (\$)	Limit (MW)
1	0.02	2	0	105
2	0.0175	1.75	0	80
5	0.0625	1	0	50
8	0.00834	3.25	0	55
11	0.025	3	0	30
13	0.025	3	0	40

Table A.7: 118 Bus-system Transmission line Parameters I

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
1 -2	0.0303	0.0999	0.0254	220
1 -3	0.0129	0.0424	0.01082	220
4 -5	0.00176	0.00798	0.0021	220
3 -5	0.0241	0.108	0.0284	220
5 -6	0.0119	0.054	0.01426	220
6 -7	0.00459	0.0208	0.0055	220
8 -9	0.00244	0.0305	1.162	1100
8 -5	0	0.0267	0	880
9 -10	0.00258	0.0322	1.23	1100
4 -11	0.0209	0.0688	0.01748	220
5 -11	0.0203	0.0682	0.01738	220
11 -12	0.00595	0.0196	0.00502	220
2 -12	0.0187	0.0616	0.01572	220
3 -12	0.0484	0.16	0.0406	220
7 -12	0.00862	0.034	0.00874	220
11 -13	0.02225	0.0731	0.01876	220
12 -14	0.0215	0.0707	0.01816	220
13 -15	0.0744	0.2444	0.06268	220
14 -15	0.0595	0.195	0.0502	220
12 -16	0.0212	0.0834	0.0214	220
15 -17	0.0132	0.0437	0.0444	440
16 -17	0.0454	0.1801	0.0466	220
17 -18	0.0123	0.0505	0.01298	220
18 -19	0.01119	0.0493	0.01142	220
19 -20	0.0252	0.117	0.0298	220
15 -19	0.012	0.0394	0.0101	220
20 -21	0.0183	0.0849	0.0216	220
21 -22	0.0209	0.097	0.0246	220
22 -23	0.0342	0.159	0.0404	220
23 -24	0.0135	0.0492	0.0498	220
23 -25	0.0156	0.08	0.0864	440
26 -25	0	0.0382	0	220
25 -27	0.0318	0.163	0.1764	440
27 -28	0.01913	0.0855	0.0216	220
28 -29	0.0237	0.0943	0.0238	220
30 -17	0	0.0388	0	660
8 -30	0.00431	0.0504	0.514	220
26 -30	0.00799	0.086	0.908	660
17 -31	0.0474	0.1563	0.0399	220

Table A.8: 118 Bus-system Transmission line Parameters II

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
29 -31	0.0108	0.0331	0.0083	220
23 -32	0.0317	0.1153	0.1173	220
31 -32	0.0298	0.0985	0.0251	220
27 -32	0.0229	0.0755	0.01926	220
15 -33	0.038	0.1244	0.03194	220
19 -34	0.0752	0.247	0.0632	220
35 -36	0.00224	0.0102	0.00268	220
35 -37	0.011	0.0497	0.01318	220
33 -37	0.0415	0.142	0.0366	220
34 -36	0.00871	0.0268	0.00568	220
34 -37	0.00256	0.0094	0.00984	440
38 -37	0	0.0375	0	660
37 -39	0.0321	0.106	0.027	220
37 -40	0.0593	0.168	0.042	220
30 -38	0.00464	0.054	0.422	220
39 -40	0.0184	0.0605	0.01552	220
40 -41	0.0145	0.0487	0.01222	220
40 -42	0.0555	0.183	0.0466	220
41 -42	0.041	0.135	0.0344	220
43 -44	0.0608	0.2454	0.06068	220
34 -43	0.0413	0.1681	0.04226	220
44 -45	0.0224	0.0901	0.0224	220
45 -46	0.04	0.1356	0.0332	220
46 -47	0.038	0.127	0.0316	220
46 -48	0.0601	0.189	0.0472	220
47 -49	0.0191	0.0625	0.01604	220
42 -49	0.0715	0.323	0.086	220
42 -49	0.0715	0.323	0.086	220
45 -49	0.0684	0.186	0.0444	220
48 -49	0.0179	0.0505	0.01258	220
49 -50	0.0267	0.0752	0.01874	220
49 -51	0.0486	0.137	0.0342	220
51 -52	0.0203	0.0588	0.01396	220
52 -53	0.0405	0.1635	0.04058	220
53 -54	0.0263	0.122	0.031	220
49 -54	0.073	0.289	0.0738	220
49 -54	0.0869	0.291	0.073	220
54 -55	0.0169	0.0707	0.0202	220
54 -56	0.00275	0.00955	0.00732	220
55 -56	0.00488	0.0151	0.00374	220
56 -57	0.0343	0.0966	0.0242	220

Table A.9: 118 Bus-system Transmission line Parameters III

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
50 -57	0.0474	0.134	0.0332	220
56 -58	0.0343	0.0966	0.0242	220
51 -58	0.0255	0.0719	0.01788	220
54 -59	0.0503	0.2293	0.0598	220
56 -59	0.0825	0.251	0.0569	220
56 -59	0.0803	0.239	0.0536	220
55 -59	0.04739	0.2158	0.05646	220
59 -60	0.0317	0.145	0.0376	220
59 -61	0.0328	0.15	0.0388	220
60 -61	0.00264	0.0135	0.01456	440
60 -62	0.0123	0.0561	0.01468	220
61 -62	0.00824	0.0376	0.0098	220
63 -59	0	0.0386	0	440
63 -64	0.00172	0.02	0.216	440
64 -61	0	0.0268	0	220
38 -65	0.00901	0.0986	1.046	440
64 -65	0.00269	0.0302	0.38	440
49 -66	0.018	0.0919	0.0248	440
49 -66	0.018	0.0919	0.0248	440
62 -66	0.0482	0.218	0.0578	220
62 -67	0.0258	0.117	0.031	220
65 -66	0	0.037	0	220
66 -67	0.0224	0.1015	0.02682	220
65 -68	0.00138	0.016	0.638	220
47 -69	0.0844	0.2778	0.07092	220
49 -69	0.0985	0.324	0.0828	220
68 -69	0	0.037	0	440
69 -70	0.03	0.127	0.122	440
24 -70	0.00221	0.4115	0.10198	220
70 -71	0.00882	0.0355	0.00878	220
24 -72	0.0488	0.196	0.0488	220
71 -72	0.0446	0.18	0.04444	220
71 -73	0.00866	0.0454	0.01178	220
70 -74	0.0401	0.1323	0.03368	220
70 -75	0.0428	0.141	0.036	220
69 -75	0.0405	0.122	0.124	440
74 -75	0.0123	0.0406	0.01034	220
76 -77	0.0444	0.148	0.0368	220
69 -77	0.0309	0.101	0.1038	220
75 -77	0.0601	0.1999	0.04978	220
77 -78	0.00376	0.0124	0.01264	220

Table A.10: 118 Bus-system Transmission line Parameters IV

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
78 -79	0.00546	0.0244	0.00648	220
77 -80	0.017	0.0485	0.0472	440
77 -80	0.0294	0.105	0.0228	220
79 -80	0.0156	0.0704	0.0187	220
68 -81	0.00175	0.0202	0.808	220
81 -80	0	0.037	0	220
77 -82	0.0298	0.0853	0.08174	220
82 -83	0.0112	0.03665	0.03796	220
83 -84	0.0625	0.132	0.0258	220
83 -85	0.043	0.148	0.0348	220
84 -85	0.0302	0.0641	0.01234	220
85 -86	0.035	0.123	0.0276	220
86 -87	0.02828	0.2074	0.0445	220
85 -88	0.02	0.102	0.0276	220
85 -89	0.0239	0.173	0.047	220
88 -89	0.0139	0.0712	0.01934	440
89 -90	0.0518	0.188	0.0528	660
89 -90	0.0238	0.0997	0.106	660
90 -91	0.0254	0.0836	0.0214	660
89 -92	0.0099	0.0505	0.0548	220
89 -92	0.0393	0.1581	0.0414	220
91 -92	0.0387	0.1272	0.03268	220
92 -93	0.0258	0.0848	0.0218	220
92 -94	0.0481	0.158	0.0406	220
93 -94	0.0223	0.0732	0.01876	220
94 -95	0.0132	0.0434	0.0111	220
80 -96	0.0356	0.182	0.0494	220
82 -96	0.0162	0.053	0.0544	220
94 -96	0.0269	0.0869	0.023	220
80 -97	0.0183	0.0934	0.0254	220
80 -98	0.0238	0.108	0.0286	220
80 -99	0.0454	0.206	0.0546	220
92 -100	0.0648	0.295	0.0472	220
94 -100	0.0178	0.058	0.0604	220
95 -96	0.0171	0.0547	0.01474	220
96 -97	0.0173	0.0885	0.024	220

Table A.11: 118 Bus-system Transmission line Parameters V

Line (From-To)	r(Per Unit)	x (Per Unit)	b(Per Unit)	Limit (MW)
98 -100	0.0397	0.179	0.0476	220
99 -100	0.018	0.0813	0.0216	220
100 -101	0.0277	0.1262	0.0328	220
92 -102	0.0123	0.0559	0.01464	220
101 -102	0.0246	0.112	0.0294	220
100 -103	0.016	0.0525	0.0536	440
100 -104	0.0451	0.204	0.0541	220
103 -104	0.0466	0.1584	0.0407	220
103 -105	0.0535	0.1625	0.0408	220
100 -106	0.0605	0.229	0.062	220
104 -105	0.00994	0.0378	0.00986	220
105 -106	0.014	0.0547	0.01434	220
105 -107	0.053	0.183	0.0472	220
105 -108	0.0261	0.0703	0.01844	220
106 -107	0.053	0.183	0.0472	220
108 -109	0.0105	0.0288	0.0076	220
103 -110	0.03906	0.1813	0.0461	220
109 -110	0.0278	0.0762	0.0202	220
110 -111	0.022	0.0755	0.02	220
110 -112	0.0247	0.064	0.062	220
17 -113	0.00913	0.0301	0.00768	220
32 -113	0.0615	0.203	0.0518	220
32 -114	0.0135	0.0612	0.01628	220
27 -115	0.0164	0.0741	0.01972	220
114 -115	0.0023	0.0104	0.00276	220
68 -116	0.00034	0.00405	0.164	440
12 -117	0.0329	0.14	0.0358	220
75 -118	0.0145	0.0481	0.01198	220
76 -118	0.0164	0.0544	0.01356	220

APPENDIX B

PUBLICATIONS

- Paper Title: Advanced Persistent False Data Injection Attacks Against Optimal Power Flow in Power Systems. (Submitted to the IEEE International Conference on Communications (ICC), Smart Grid Communications Track, Cybersecurity, privacy, and cyber-physical security topic of interest)
- Paper Title: Rule-based detection system for False Data Injection Attacks Against Optimal Power Flow in Power Systems. (To be submitted to Sensors Journal)

REFERENCES

- [1] A. S. Musleh, G. Chen, and Z. Y. Dong, “A survey on the detection algorithms for false data injection attacks in smart grids,” *IEEE Transactions on Smart Grid*, 2019.
- [2] Q. Yang, D. Li, W. Yu, Y. Liu, D. An, X. Yang, and J. Lin, “Toward data integrity attacks against optimal power flow in smart grid,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1726–1738, 2017.
- [3] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber–physical security of a smart grid infrastructure,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.
- [4] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, “Cyber security and privacy issues in smart grids,” *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.
- [5] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

- [6] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013.
- [7] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, “Detecting false data injection attacks on power grid by sparse optimization,” *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.
- [8] R. Ambekar and H. Mangalvedekar, “Power system state estimation by linear programming under false data injection attack and contingency,” in *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE, 2017, pp. 698–703.
- [9] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, “Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation,” *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 6–8, 2015.
- [10] Z. Hu, Y. Wang, X. Tian, X. Yang, D. Meng, and R. Fan, “False data injection attacks identification for smart grids,” in *2015 Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAECE)*. IEEE, 2015, pp. 139–143.
- [11] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures,” in *2010 first IEEE international conference on smart grid communications*. IEEE, 2010, pp. 220–225.

- [12] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 ukraine blackout: Implications for false data injection attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.
- [13] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.
- [14] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, “Matpower: Steady-state operations, planning, and analysis tools for power systems research and education,” *IEEE Transactions on power systems*, vol. 26, no. 1, pp. 12–19, 2010.
- [15] C.-C. Sun, A. Hahn, and C.-C. Liu, “Cyber security of a power grid: State-of-the-art,” *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.
- [16] Y. Lopes, N. C. Fernandes, T. B. de Castro, V. dos Santos Farias, J. D. Noce, J. P. Marques, and D. C. Muchaluat-Saade, “Vulnerabilities and threats in smart grid communication networks,” in *Security Solutions and Applied Cryptography in Smart Grid Communications*. IGI Global, 2017, pp. 1–28.
- [17] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, “Cyber-security in smart grid: Survey and challenges,” *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

- [18] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.
- [19] B. R. Amin, S. Taghizadeh, M. S. Rahman, M. J. Hossain, V. Varadharajan, and Z. Chen, “Cyber attacks in smart grid—dynamic impacts, analyses and recommendations,” *IET Cyber-Physical Systems: Theory & Applications*, 2020.
- [20] F. Aliyu, T. Sheltami, and E. M. Shakshuki, “A detection and prevention technique for man in the middle attack in fog computing,” *Procedia Computer Science*, vol. 141, pp. 24–31, 2018.
- [21] J. S. Foster Jr, E. Gjeldel, W. R. Graham, R. J. Hermann, H. M. Kluepfel, R. L. Lawson, G. K. Soper, L. L. Wood, and J. B. Woodard, “Report of the commission to assess the threat to the united states from electromagnetic pulse (emp) attack: Critical national infrastructures,” ELECTROMAGNETIC PULSE (EMP) COMMISSION MCLEAN VA, Tech. Rep., 2008.
- [22] L. Peng, X. Cao, H. Shi, and C. Sun, “Optimal jamming attack schedule for remote state estimation with two sensors,” *Journal of the Franklin Institute*, vol. 355, no. 14, pp. 6859–6876, 2018.
- [23] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, “Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system,” *Journal of Parallel and Distributed Computing*, vol. 103, pp. 32–41, 2017.

- [24] Y. Ding and J. Liu, “Real-time false data injection attack detection in energy internet using online robust principal component analysis,” in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*. IEEE, 2017, pp. 1–6.
- [25] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, “Signal temporal logic-based attack detection in dc microgrids,” *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, 2018.
- [26] U. Adhikari, T. H. Morris, and S. Pan, “Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection,” *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 3928–3941, 2016.
- [27] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, “Online cyber-attack detection in smart grid: A reinforcement learning approach,” *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5174–5185, 2018.
- [28] B. Li, R. Lu, and G. Xiao, “Hmm-based fast detection of false data injections in advanced metering infrastructure,” in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.
- [29] Y. He, G. J. Mendis, and J. Wei, “Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

- [30] H. Sedghi and E. Jonckheere, “Statistical structure learning of smart grid for detection of false data injection,” in *2013 IEEE Power & Energy Society General Meeting*. IEEE, 2013, pp. 1–5.
- [31] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, “Detecting stealthy false data injection using machine learning in smart grid,” *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2014.
- [32] J. Yan, B. Tang, and H. He, “Detection of false data attacks in smart grid with supervised learning,” in *2016 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2016, pp. 1395–1402.
- [33] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, “Real-time cyber-physical false data attack detection in smart grids using neural networks,” in *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2017, pp. 1–6.
- [34] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, “Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2765–2777, 2019.
- [35] J. Duan, W. Zeng, and M.-Y. Chow, “Resilient distributed dc optimal power flow against data integrity attack,” *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3543–3552, 2016.

- [36] M. A. Rahman, E. Al-Shaer, and R. G. Kavasseri, “A formal model for verifying the impact of stealthy attacks on optimal power flow in power grids,” in *2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2014, pp. 175–186.
- [37] K. Khanna, B. K. Panigrahi, and A. Joshi, “Bi-level modelling of false data injection attacks on security constrained optimal power flow,” *IET Generation, Transmission & Distribution*, vol. 11, no. 14, pp. 3586–3593, 2017.
- [38] A. Abdallah and X. S. Shen, “Efficient prevention technique for false data injection attack in smart grid,” in *2016 IEEE International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.
- [39] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Combating false data injection attacks in smart grid using kalman filter,” in *2014 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2014, pp. 16–20.
- [40] L. Wei, D. Gao, and C. Luo, “False data injection attacks detection with deep belief networks in smart grid,” in *2018 Chinese Automation Congress (CAC)*. IEEE, 2018, pp. 2621–2625.
- [41] T.-Y. Zhang and D. Ye, “False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach,” *Automatica*, vol. 120, p. 109117, 2020.

- [42] A.-Y. Lu and G.-H. Yang, “False data injection attacks against state estimation in the presence of sensor failures,” *Information Sciences*, vol. 508, pp. 92–104, 2020.
- [43] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and C. Konstantinou, “Survey of machine learning methods for detecting false data injection attacks in power systems,” *IET Smart Grid*, 2020.
- [44] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, “Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning,” *Computers & Security*, vol. 97, p. 101994, 2020.
- [45] H. Saadat, *Power System Analysis*, ser. McGraw-Hill series in electrical and computer engineering. WCB/McGraw-Hill, 1999. [Online]. Available: <https://books.google.com.sa/books?id=kia4AAAACAAJ>
- [46] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, “Towards a framework for cyber attack impact analysis of the electric smart grid,” in *2010 First IEEE International Conference on Smart Grid Communications*. IEEE, 2010, pp. 244–249.
- [47] S. Ólafsson, “Metaheuristics,” *Handbooks in operations research and management science*, vol. 13, pp. 633–654, 2006.
- [48] S. Z. Selim and K. Alsultan, “A simulated annealing algorithm for the clustering problem,” *Pattern recognition*, vol. 24, no. 10, pp. 1003–1008, 1991.

- [49] S. Kirkpatrick, “Dg jr., and mp vecchi,” *Optimization by simmulated annealing. science*, vol. 220, no. 4598, pp. 671–680, 1983.
- [50] K. A. Dowsland and J. Thompson, “Simulated annealing,” *Handbook of natural computing*, pp. 1623–1655, 2012.
- [51] O. Kramer, *Genetic algorithm essentials*. Springer, 2017, vol. 679.
- [52] K. P. Ferentinos, K. G. Arvanitis, and N. Sigrimis, “Heuristic optimization methods for motion planning of autonomous agricultural vehicles,” *Journal of Global Optimization*, vol. 23, no. 2, pp. 155–170, 2002.
- [53] M. Elbes, S. Alzubi, T. Kanan, A. Al-Fuqaha, and B. Hawashin, “A survey on particle swarm optimization with emphasis on engineering and network applications,” *Evolutionary Intelligence*, pp. 1–17, 2019.
- [54] R. Poli, J. Kennedy, and T. Blackwell, “Particle swarm optimization,” *Swarm intelligence*, vol. 1, no. 1, pp. 33–57, 2007.
- [55] R. A. Gallego, R. Romero, and A. J. Monticelli, “Tabu search algorithm for network synthesis,” *IEEE Transactions on Power Systems*, vol. 15, no. 2, pp. 490–495, 2000.
- [56] I. Ghafir and V. Prenosil, “Advanced persistent threat attack detection: an overview,” *Int J Adv Comput Netw Secur*, vol. 4, no. 4, p. 5054, 2014.

- [57] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, “Detection of false data injection attacks in smart-grid systems,” *IEEE Communications Magazine*, vol. 53, no. 2, pp. 206–213, 2015.

VITAE

- **Personal Information**

- Name: Sani Umar
- Nationality: Nigerian
- Date of Birth: 15th January, 1994
- Email: *saniumarkadira@gmail.com*
- Permanent Address: TW1 No. 8 Takur Housing Estate, Dutse, Jigawa State.
- Postal Code: 720223

- **Education:**

- 2018-2020: King Fahd University of Petroleum and Minerals
Master of Science in Computer Network (CGPA: 3.53/4.00)
- 2012-2016: Eastern Mediterranean University, Famagusta TRNC
Bachelor of Science (B.S.) program in Information Systems Engineering (CGPA:
3.94/4.00)

- 2009-2011: Science Secondary School, Kafin Hausa, Jigawa State of Nigeria
Senior Secondary Certificate Examination (SSCE)
- 2006-2008: Junior Science Secondary School, Aujara, Jigawa State of Nigeria
Junior Secondary Certificate Examination (JSCE)
- 1999-2005: Jigawa Tsada Special Primary School, Dutse
Primary School Certificate
- **Working Experience:**
- 2016-2017: Kano Electricity Distribution Company Plc
National Youth Service Corps (System Operation and Dispatch)
- 2015: Eastern Mediterranean University Computer Center
Computer Software and Hardware Maintenance (Internship)
- **Honors and Awards:**
- Certified Network Security Specialist (CNSS), International Cybersecurity Institute (ICSI)
- Best student paper presented during the 2nd IEEE Middle East North Africa Communication Conference organized by University of Bahrain, IEEE Communications Society Bahrain Chapter, and Bahrain Society of Engineers. 19-21 Nov. 2019
- Certificate of completion (Python Programming Short course) organized by Student Success Center, King Fahd University of Petroleum and Minerals

- Fully-funded MS scholarship (KFUPM, Ministry of higher Education, Kingdom of Saudi Arabia)
- Certificate of Achievement (Best Graduating student in Information Systems Engineering) 2016.
- Certificate of High Honor Fall 2015-2016 Semester
- Certificate of High Honor Spring 2014-2015 Semester
- Certificate of High Honor Fall 2014-2015 Semester
- Certificate of High Honor Spring 2013-2014 Semester
- Certificate of Attendance “ICT and cyber security conference” organized by school of Computing and Technology, Eastern Mediterranean University.
- Certificate of High Honor Fall 2013-2014 Semester
- Certificate of High Honor Spring 2012-2013 Semester
- Certificate of High Honor Fall 2012-2013 Semester
- Fully-funded Bsc. scholarship (Ministry of Education, Jigawa State Scholarship Board, Nigeria)
- Certificate of Recognition 2011 cowbell national secondary schools mathematics competition (2nd position in senior Category)

- **Computer literacy**

- 2011: Dutse Computer Training Centre, Ministry of Education Science and Technology Jigawa State of Nigeria

Introduction to Windows Operating Systems

Microsoft word

Microsoft Power point

Microsoft Excel

- **Reserch work**

- Aliyu, Farouq, Sani Umar, and Hussain Al-Duwaish. "A survey of applications of artificial neural networks in wireless sensor networks." 2019 8th International Conference on Modeling Simulation and Applied Optimization (ICM-SAO). IEEE, 2019. (Published)

- Farouq Aliyu, Sani Umar, Talal Alkharobi, and Uthman Baroudi "Improving Base Station Anonymity using Data Funneling and PID Controlled Fake Packets." 2019 2nd IEEE Middle East North Africa COMMunications Conference (MENACOMM 2019). (Published)

- Muhammad Tukur, Sani Umar, and Jameleddine Hassine "Requirements engineering challenges in research and practice: a mapping study" (Accepted - Arabian Journal for Science and Engineering)

- **Referees**

- Assit. Prof. Dr. Muhamad Felemban

Computer Engineering Department

King Fahd University of Petroleum and Minerals.

Phone: 2940

Email: mfelemban@kfupm.edu.sa

Website: <http://faculty.kfupm.edu.sa/coe/mfelemban>

- Prof. Dr. Aykut Hocanin

Rector

Eastern Mediterranean University

Tel: +90 (392) 630 1380

Email: aykut.hocanin@emu.edu.tr

Web: <https://staff.emu.edu.tr/aykuthocanin>

- Prof. Dr. Hasan Demirel

Vice Rector, Academic Affairs

Eastern Mediterranean University

Email: hasan.demirel@emu.edu.tr

Tel: +90 (392) 630 1300

Web Page: <http://faraday.ee.emu.edu.tr/hdemirel>