

AN INTELLIGENT INTRUSION DETECTION AND RECOVERY SYSTEM

BY

ABDULAZIZ KHALID ALJOHANI

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

ELECTRICAL ENGINEERING

JANUARY, 2023

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN- 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **Abdulaziz K. Aljohani** under the direction of his thesis advisor and approved by his thesis committee, has been presented and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN ELECTRICAL ENGINEERING**.

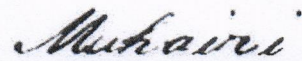


Dr. Abdallah Alahmari
Chairman of Electrical Engineering
Department



Dr. Suliman Alhomidan
Dean of Graduate Studies

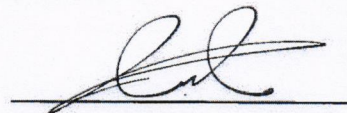
Date



Dr. Mohammad Almuahini
(Advisor)



Dr. Mohammad Abido
(Member)



Dr. Maad Alowaifeer
(Member)



© Abdulaziz Aljohani

2023

This work is dedicated to my family

ACKNOWLEDGMENTS

I would like to acknowledge the support, guidance and help provided by my advisor Dr. Mohammad Almuhaini. Many thanks are also due to my thesis committee members Dr. Mohammad Abido and Dr. Maad Alowaifeer for spending their valuable time in providing useful feedback and comments.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	V
TABLE OF CONTENTS	VI
LIST OF TABLES	VIII
LIST OF FIGURES	X
LIST OF ABBREVIATIONS	XII
ABSTRACT	XIV
ملخص الرسالة	XV
CHAPTER 1 INTRODUCTION	1
1.1 Background	1
1.2 Motivation.....	2
1.3 Thesis Objectives.....	3
1.4 Thesis Organization	3
CHAPTER 2 LITERATURE REVIEW	5
2.1 False Data Injection Detection	5
2.2 False Data Injection Location	9

2.3	False Data Injection Recovery	11
2.4	Literature Gap and Thesis Contributions	13
 CHAPTER 3 PROPOSED INTRUSION DETECTION AND RECOVERY SYSTEM		15
3.1	IEEE 13 Bus system Model	16
3.2	Electrical Fault Model	21
3.3	False Data Injection Model	25
3.4	Deep Learning Neural Network Model.....	28
3.5	Long Short-Term Memory Model.....	32
 CHAPTER 4 RESULTS AND DISCUSSIONS		35
4.1	False Data Injection Detection Results.....	36
4.2	False Data Injection Classification Results.....	39
4.3	False Data Injection Location Results.....	43
4.4	False Data Injection Measurement Recovery Results	58
 CHAPTER 5 CONCLUSION AND FUTURE RECOMMENDATIONS		63
 REFERENCES.....		65
 VITAE		78

LIST OF TABLES

Table 3.1. IEEE 13 Bus System Line Data.....	17
Table 3.2. IEEE 13 Bus System Capacitor Data	17
Table 3.3. IEEE 13 Bus System Transformer Data	18
Table 3.4. IEEE 13 Bus system Load Data	18
Table 3.5. Breakdown of Coordinated Attacking Scenarios	27
Table 3.6. Average Activation Function Experimental Accuracy for the Proposed Problem	31
Table 3.7. Average Optimizer Accuracy for the Proposed Problem	32
Table 4.1. Confusion Matrix of The Trained Detection DLNN Using the Training Dataset	39
Table 4.2. Confusion Matrix of The Trained Detection DLNN Using the Testing Dataset.....	39
Table 4.3. Confusion Matrix of The Trained Classification DLNN Using the Training Dataset.....	42
Table 4.4. Confusion Matrix of The Trained Classification DLNN Using the Testing Dataset	43
Table 4.5. Confusion Matrix of The DLNN Using The Training Dataset.....	45
Table 4.6. Confusion Matrix of The DLNN Using The Testing Dataset	46
Table 4.7. Confusion Matrix of Double FDIA DLNN Using The Training Dataset.....	48
Table 4.8. Confusion Matrix of Double FDIA DLNN Using The Testing Dataset	49

Table 4.9. Confusion Matrix of Triple FDIA DLNN Using The Training Dataset.....	52
Table 4.10. Confusion Matrix of Triple FDIA DLNN Using The Testing Dataset	53
Table 4.11. Confusion Matrix of Quadruple FDIA DLNN Using The Training Dataset.....	56
Table 4.12. Confusion Matrix Quadruple FDIA DLNN Using The Testing Dataset.....	57

LIST OF FIGURES

Figure 3.1. IDRS algorithm flowchart	16
Figure 3.2. Modified IEEE 13 Bus System with Distributed Loads	19
Figure 3.3. Electrical Fault Locations	22
Figure 3.4. Overall System Readings During an ABCG Fault at Node 650	24
Figure 3.5. DLNN Model.....	29
Figure 3.6. ReLU Activation Function.....	30
Figure 3.7. Long short-Term Memory Network Model	33
Figure 4.1. DLNN Training Performance for The Classification Problem	42
Figure 4.2. DLNN Training Performance for the Single IED FDIA Location Problem.....	45
Figure 4.3. DLNN Training Performance for the Double IED FDIA Location Problem	47
Figure 4.4. DLNN Training Performance for the Triple IED FDIA Location Problem	51
Figure 4.5. DLNN Training Performance for the Quadruple IED FDIA Location Problem	55
Figure 4.6. LSTM NN Training Performance in Predicting Single FDIA IED Measurements	60
Figure 4.7. Actual Vs. Predicted IED 650 Current Waveform	60
Figure 4.8. Actual Vs. Predicted IED 633 Current Waveform	61

Figure 4.9. Actual Vs. Predicted IED 671 Current Waveform.....	61
Figure 4.10. Actual Vs. Predicted IED 671_2 Current Waveform.....	62
Figure 4.11. Actual Vs. Predicted IED 675 Current Waveform.....	62

|

LIST OF ABBREVIATIONS

DoS	:	Denial of Service
FDIA	:	False Data Injection Attack
CIC	:	Canadian Institute of Cybersecurity
RF	:	Random Forest
SVM	:	Support Vector Machine
MMS	:	Manufacturing Messaging Specification
KVL	:	Kirchhoff Voltage Law
KCL	:	Kirchhoff Current Law
DRFSA	:	Dynamic Recursive Feature Selection Algorithm
GOOSE	:	Generic Object Oriented Substation Event
KNN	:	K-Nearest-Neighbor
SCADA	:	Supervisory Control and Data Acquisition
XGBoost	:	Extreme Gradient Boosting
LSTM	:	Long Short-Term Memory
ANN	:	Artificial Neural Network
ANFIS	:	Adaptive Neuro Fuzzy Inference System

SMT	:	Satisfiability Modulo Theory
SSDAT	:	Semi-Supervised Domain-Adversarial Training
IDS	:	Intrusion Detection System
LDCR	:	Line Current Differential Relays
RFN	:	Residual Function
VRI	:	Virtual Range Increment
WTM	:	Weight Trust Method
SDN	:	Software-Defined Networking
ERLC	:	Ensemble Representation Learning Classifier
PMU	:	Phasor Measurement Unit
MILP	:	Mixed Integer Linear Programming
RMPC	:	Recovery-Based Model Predictive Control Methodology
IED	:	Intelligent Electronic Device
DLNN	:	Deep Learning Neural Network
IDRS	:	Intrusion Detection and Recovery System

ABSTRACT

Full Name : Abdulaziz Khalid Aljohani

Thesis Title : AN INTELLIGENT INTRUSION DETECTION AND RECOVERY
SYSTEM FOR SMART GRIDS

Major Field : Electrical Engineering

Date of Degree : January,2023

The emergence of power system digitalization initiatives revolutionized the way electricity grids are monitored and protected. However, the integration of cyber and physical electrical infrastructures led to an increase in risk of cyber intrusions. Attackers can gain access to the smart grid and inject falsified data leading the protection schemes to activate unnecessary power outage actions. Such outages can be devastating to the end users. In this research, an IDRS is proposed using DLNN to detect, classify and locate intrusions in smart grids. Once the disturbance is located, the IDRS is designed to isolate the contaminated IED and predict its current waveform utilizing LSTM neural network to maintain the power system observability. The proposed IDRS performs the required diagnosis on the modified simulated IEEE 13 bus system. Simulation results demonstrated high accuracy in the proposed detection, classification, location and prediction approach.

ملخص الرسالة

الاسم الكامل: عبدالعزيز خالد الجهني

عنوان الرسالة: نظام ذكي للوقاية والكشف عن الاختراقات الأمنية للشبكات الذكية

التخصص: الهندسة الكهربائية

تاريخ الدرجة العلمية: رجب / ١٤٤٤ هجري

أحدثت مبادرات التحول الرقمي لشبكات الطاقة ثورة في مجال مراقبة وحماية خطوط النقل. إلا ان ذلك أدى إلى زيادة مخاطر الاختراقات السيبرانية للبنية التحتية الرقمية والمادية للكهرباء. فيمكن للمخترقين الوصول إلى الشبكة الذكية وحقن البيانات المزيفة بهدف إحداث انقطاعات تدميرية للتيار الكهربائي. لذلك فقد تم إنشاء نظام اكتشاف الاختراقات واسترداد القراءات في هذه الرسالة باستخدام الشبكة العصبية للتعلم العميق. يقوم النظام المصمم باكتشاف الاقتحامات في الشبكات الذكية وتصنيفها وتحديد موقعها. و بمجرد تحديد الاضطراب، يقوم النظام بعزل أجهزة التحكم والمراقبة المستهدفة والتنبيه بشكل الموجات الجيبية باستخدام الشبكة العصبية ذات الذاكرة قصيرة المدى للحفاظ على إمكانية مراقبة نظام الطاقة. أظهرت نتائج المحاكاة دقة عالية في كشف وتصنيف وتحديد موقع الاختراق بالإضافة إلى التنبيه بشكل الموجات الجيبية.

CHAPTER 1

INTRODUCTION

1.1 Background

A grid can be defined as the network of generators, lines, transformers and substations that deliver electricity to commercial and industrial customers. However, in recent years, information systems such as energy management centers were integrated for efficient distribution of energy, quicker restoration after disturbances and reduced operational costs. Such initiatives signify the differences between a grid and a smart grid. Moreover, the integrity of cyber-physical systems is crucial for the availability of energy supply across the electrical distribution grids. In recent years, the trend towards incorporating digitized solutions to monitor, control and diagnose electrical equipment was adopted by power system providers [1], [2]. Such an approach was possible mainly due to the existence of IEC-61850 [3]–[6] standard which revolutionized the communication protocol within electrical substations.

With a wider digitalization of electrical cyber-physical systems, many security vulnerabilities emerged, many of these threats can be classified as:

1. Replay attack [7], [8] which is a malicious behavior conducted by the attacker to resend previously sent messages after a delay and without alteration. Such an attack

can lead to catastrophic consequences if the command to “close breaker” was resent during a maintenance activity where the system is isolated.

2. DoS attack [9], [10] which can be defined as the interruption and disturbance of existing communication channels between the user and the machine. This attacking method leaves the user in a state of paralysis with no ability to control the system.
3. FDIA [11], [12] by an intruder into the digital system to produce falsified outputs from sensors and prompt the control system to take extreme actions that destabilize the power system.

The latter of the aforementioned classifications can have the most potential devastating outcome to the reliability of power supply. Therefore, a comprehensive IDRS is needed to maintain the availability of electricity supply to the customer [1].

1.2 Motivation

The transformation towards digitalized grid monitoring and operation led to the emergence of cyber vulnerabilities allowing the attacker to maliciously control the system. The subject attacks extend their threat capabilities onto the physical part of the Cyber-Physical power systems and may result in undesirable operation of substation components or a loss of control. Therefore, a need for developing a diagnosis tool that can detect, classify and locate FDIAs had emerged to maintain the grid’s operation. In addition, after the identification of an intrusion, the system’s observability shall be maintained using a predictive scheme that produces alternative temporary readings while the repair activities are on-going.

1.3 Thesis Objectives

The main target of this thesis work is to develop an intrusion diagnosis tool to detect, classify and locate FDIAs. An important set of features is extracted from the current sinusoidal waveforms to improve the accuracy of classification and prediction. The developed system will provide sufficient warnings to the power system operator and take corrective recovery actions without a need of human intervention. The objectives of this thesis are summarized as follows:

1. Propose a DLNN based technique to detect, classify and locate cyber-attacks in smart grids.
2. Propose an LSTM based technique to recover the system's observability.
3. Validate the effectiveness of proposed algorithm using a set of testing data.

1.4 Thesis Organization

Besides the introduction, this thesis contains the following chapters. Chapter two provides a comprehensive literature survey covering the existing methods developed by researchers in the field of cyber intrusion diagnosis. The methodology of proposed approach is detailed in chapter three. A modified version of the IEEE 13 bus system is simulated in MATLAB Simulink. The algorithm constantly monitors the current sinusoidal signals through the distributed IEDs throughout the grid. Once an increase in the current amplitude is detected, the IDRS algorithm would perform the necessary diagnosis. Chapter four introduces a detailed discussion on the results of the proposed research approach in distinguishing

between injected current signals and disturbances caused by a short circuit, classification of the FDIA into one of the following categories: an attack targeting one IED, two IEDs, three IEDs, four IEDs or all IEDs in the grid, location and isolation of the contaminated IEDs from the grid and Prediction the signals of the isolated IEDs to maintain the system observability. And finally, Chapter five present the conclusion and future work recommendations.

CHAPTER 2

LITERATURE REVIEW

In literature, many scholars have attempted to solve the cyber-attack intrusion detection problem [13]–[18]. For example, A combination of classifiers were used to evaluate the most effective intrusion detection approach utilizing CIC dataset named CIC-IDS2018 [19]. The approach utilized several machine learning classifiers such as RF, Naive Bayes, XGBoost and SVM to validate the proposed Boruta Feature Selection and Recursive Feature Elimination methods. Although the results of accuracy are satisfactory, an analysis in smart grid specific attacks is required to substantiate the efficacy of the approach for power systems.

2.1 False Data Injection Detection

The detection of falsified inserted measurement in MMS messages was attempted by [20]. The algorithm verified the entered measurement against Ohm's law, KVL and KCL. If any violation is detected, then the algorithm will flag the falsified measurement. However, such approach relies heavily on special set of rules that were not tested against coordinated attacks. Also, the implementation of the proposed approach requires high knowledge of the system specifications (Current and Voltage instrumental transformers) to consider tolerance rates in measurements.

A rule based on analyses traffic data algorithm was proposed by [21]. The methodology generated rules based on packet time threshold, payload, and incorrect checksum to detect

intrusions targeting the grid's control network. However, the method was not assessed against coordinated cyber-attacks.

In [22], Nancy et al. Presented an integration between Convolutional Neural Networks and decision trees. DRFSA was deployed to improve the classifier accuracy. The accuracy of the model was tested using KDD CUP 99 dataset. However, coordinated cyber-attacks scenarios were not considered.

Real-time IEC 61850 based detection of infected GOOSE messages was attempted by [23], [24]. The method highlighted the abnormality in GOOSE messages aiming to relay the power system status and categorized them into three main classes: event, stop/reconfiguration or normal operation. Later on, a security analysis was conducted to classify the message into the aforementioned categories, an alarm is raised if the analysis fails to classify the event into an appropriate category. The method provides acceptable results. However, a diagnoses of the FDIA was not presented.

A hybridization between correlation-based feature selection (CFS) [25] and KNN algorithm [26] was utilized by [27] for intrusion detection in SCADA systems. The imported datasets were processed through CFS for feature extraction. Later on, the training of KNNs was conducted to detect cyber-attacks. The methodology presented was effective with a reduced computational burden. However, the localization problem was not discussed.

Song et al. [28] proposed an XGBoost [29] and LSTM [30] classifier based algorithms optimized by Bayesian method. The method accuracy outperformed other techniques in

literature. However, the utilization of various classifiers will require heavy computational effort to achieve desired results.

Autoencoders (AEs) were implemented to dynamically optimize the set of features used in the training of RF [31] classifiers as demonstrated by [32]. The introduced AE utilized an ANN to compress the original statistics of data and reconstruct the output. However, the trained RF classifier was only able to achieve 91.78% in testing accuracy.

Bedoya et. al. [33] proposed an ANFIS based approach to detect cyber-intrusions. The algorithm identifies the grid's component status such as: Voltage, Current, Power and breaker switching position and evaluates them against the predicted system condition. Although the accuracy of detection is satisfactory, the proposed ANFIS method requires modification in case of a change in system architecture.

A state estimation model developed using SMT [34] was introduced by the authors of [35]. The model estimates the unknown system parameters and evaluates if an FDIA has occurred without the knowledge of system operator. The presented accuracy of results are acceptable. However, the model evaluation time significantly increases in larger grids.

SVM [36] were used by the authors of [37] to analyze and detect DoS attacks on smart grids. The research utilized the KDDCup99 training dataset to identify and detect DoS attacks applying SVM algorithms. The reported detection results are satisfactory in comparison to other detection approaches. However, the authors did not tackle the localization problem.

Hybrid Decision Tree was proposed as an intrusion detection algorithm by [38]. The authors modeled a configuration of various decision trees to solve the classification

problem. One decision tree builds its model based on examining the complete dataset of the training phase. The tree is later assessed with the same training set. If the tree fails to classify the set accurately, the model will proceed towards the second and third trees.

SSDAT framework was utilized by [39] in an attempt to detect FDIAs targeting smart grids. The utilized latest domain-adversarial learning technique [40] was designed to extract useful statistical features and improve the accuracy of the intrusion detection. The authors explored both balanced and imbalanced loading conditions. However, the scenario of coordinated FDIA was not considered.

The utilization of physical power system data alongside the network data produce the hybridized IDS proposed in [41]. The method studied the effect of FDIAs and Insider Threats on the power system behavior to create alarms in case of operational abnormalities. However, the method's ability to distinguish between disturbances caused by system failures or cyber-attacks was not proven.

Ameli et. al. [42] introduced a new IDS method of LDCRs. In the subject research, the variance between the measured and approximated local voltage is calculated and used as a tool for distinguishing whether the disturbance is of a faulty equipment or a cyber intrusion. Such variable was referred to as the RFN. Hence, the large value of the RFN during a disturbance would indicate a cyber-attack. The effectiveness of this approach was demonstrated on the IEEE 39-bus system [43]. However, the method is only limited to intrusion in LDCRs and was not examined for overall smart grid intrusion localization.

Based on voltages stability of the power system, the authors of [44] proposed a rule-based IDS for FDIA detection. The work presenting shows promising results in using stability

parameters of the power system. However, extensive work is required to improve the detection accuracy.

2.2 False Data Injection Location

The intrusion location problem presents a challenge for the resilience against cyber-attacks. Identifying the compromised network components is crucial for maintaining a reliable operation of the power system. WTM hybridized with VRI was proposed by [45]. The methodology focused on locating wireless sensor node-based intrusion attacks by analyzing the inputs from all sensors in the grid. The detection speed of the proposed method was highlighted as a novelty. However, the problem of coordinated attacks was not considered in this research.

Bayesian game-Theoretic hypervisor dynamic system was researched by [46] to prevent the DoS attacks exploiting SDN grids. The modeled system distributes its available resources optimally monitor intruder point of attack. the method's results proofed to be satisfactory. However, coordinated attack scenarios were not considered.

A GOOSE based IDS for IEDs was presented and discussed by the authors of [47]. The analysis of GOSSE messages allowed for the detection and localization of cyber-attacks in digital substations. However, the paper's algorithm cannot be centralized and requires the implementation of a distributed IDS scheme. Moreover, the simultaneous cyber-attack detection was not studied.

A differential sequence variance IDS design was proposed by [48]. The attributes of stochastic and burst traffic in the process layer of digital substations was predicted to detect

and locate anomalies in the smart grid. Although the method provided satisfactory results, the dependency on modeled burst data accuracy was highlighted as a shortcoming by the authors.

An analysis of multiple network futures was attempted by [49] to develop a behavior-based IDS. In this approach, the static and dynamic features of an IEC 61850 based network traffic is monitored to identify if any packet is in misalignment with the required protocol sequence. As a result, the method would detect and identify the compromised IED. however, integrated recovery was not attempted.

The problem of intrusion localization in the physical layer of the system was attempted in [50]. ERLC [51] was trained to classify and locate FDIA attacks. The method accuracy was found to be satisfactory. However, larger systems with varying topologies must be tested to map the full extent of such approach.

A data-driven attempt was proposed by [52] detection and location of silent FDIA attacks in smart grids. In the suggested approach, a machine-learning based detector was deployed for each sub-area of the power system. The detectors were designed to freely communicate with neighboring areas. An iterative distributed state estimation algorithm was deployed to estimate the local state of the system and then forward the data to the local intrusion detector. Accuracy of location and detection are satisfactory. However, authors did not consider coordinated attacks.

2.3 False Data Injection Recovery

Power grids in recent years transformed into a framework for exchange energy and information. Such a development increases the risk of cyber-attacks [53]. Therefore, the need for a recovery system in case these attacks succeed is crucial for the continuity of power supply [12]. Deep reinforced learning was utilized by the authors of [54], the method was aiming to identify the optimal reclosing time for transmission line breakers and minimize the power system outage time. The method was successful in the proposed 9-bus system. However, a study on larger system is needed.

The authors of [55], [56] proposed an algorithm for data recovery by exploring the intrinsic low-dimensional structures in high-dimensional spatial-temporal blocks of Phasor Measurement Unit (PMU) dataset. The method collected PMU data from multiple locations and instances to form a matrix. Later on, the low-rank matrix completion method was deployed to correct bad measurements resulting from FDIAs. The results reported were satisfactory. However, a consideration of coordinated FDIAs is necessary.

A study was presented by [57] to control the selection between human or automated system recovery approaches after a cyber-attack. The method analyzed the probability of successful recovery, recovery action cost and successful attack cost to determine the most suitable healing approach with the least potential cost and highest probability of success. The method can be further applied on larger power systems to test its effectiveness.

A recovery approach for IEC 61850 substations was developed by the authors of [58]. The method identified and isolated the affected IEDs from the local network through a dynamic network reconfiguration. Afterwards, the back-up IED was deployed to take part in the

monitoring and control of the power system. While the approach was tested in a SDN based substation, an expansion of the algorithm is required for validation across a larger distribution system.

Recovering the observability of the smart grids was the key objective in [59], [60], A MILP problem was constructed to maximize the observability of the network after a cyber-attack. The method focused on rapid recovery of PMUs and communication infrastructure of a modeled IEEE 57-bus system. Although the results provided are satisfactory, no effort was made to integrate such a recovery approach into an intrusion detection system.

An intelligent SDN controller with technical features that can support self-healing schemes in smart grids was proposed by [61]. When an attack occurs, the controller would detect and isolate the affected relays from the network. Afterwards, the algorithm would establish new uncompromised paths for communicating to maintain the power system integrity. However, the subject controllers must be wisely configured to avert errors and assure network availability.

Zhang et al [62] proposed a sequential node recovery strategy for power grids based on Q-learning. The method identifies the optimal method for sequential restoration of the power flow in an IEEE 300 bus test system. However, an extension of the proposed work on cyber-physical systems can be explored.

A self-healing mechanism was proposed by the authors of [63] to isolate the compromised PMUs and prevent cascading failures in power delivery. The approach was tested on the IEEE-30 and IEEE 118 bus systems with acceptable results. However, the stability of the system was not considered as a constraint.

A recovery based model was discussed in [64] to predict the system state after the occurrence of a cyber-attack and maintain the observability of the grid. The subject RMPC utilized the DC power flow model to predict the correct system states masked by an FDIA. However, the authors did not explore the potential of using distributed grid sensors in improving the accuracy of state estimation.

In the field of data recovery, [65] presented a linear algebra and graph theory based method for information recovery post cyber-physical attacks on smart grids. The algorithm showed promising results, however, a larger scale application is required to fully illustrate the capability of the approach.

2.4 Literature Gap and Thesis Contributions

In literature, many researchers attempted to introduce IDSs for smart grids. It was clearly demonstrated that there are many areas of concern the cyber-physical protection systems such as:

1. Existing methods rarely address the security against coordinated cyber-attacks that inject malicious measurements into the protection system to force unwanted system behavior.
2. The classification and localization of attacks are necessary to be used as basis for outage recovery.
3. Cyber-attacks targeting the grid measurements reduce the overall system observability without a strategy in place to predict the system state.

The IDRS proposed in this research is able to accurately detect, classify and locate cyber intrusions in smart grids. In addition, the algorithm provides an accurate estimation of current measuring as a strategy to recover the system's observability. The contributions of this thesis are as follows:

1. Proposing a new distributed DLNN based method to detect, classify and locate coordinated FDIAs.
2. Introducing an LSTM based approach for system recovery after the isolation of an FDIA.

CHAPTER 3

PROPOSED INTRUSION DETECTION AND RECOVERY SYSTEM

The method presented in this research aims to provide an IDRS for smart grids to minimize customer power supply interruption. To test and validate the proposed approach, a modified version of the IEEE 13 bus system is simulated in MATLAB Simulink. The IDRS constantly monitors the current sinusoidal signals through the distributed IEDs throughout the grid. As shown in Figure 3.1, Once an increase in the current amplitude is detected, the IDRS algorithm would perform a DLNN based analysis to identify whether the disturbance is caused by an electrical fault or a FDIA. If the analysis output determined that the disturbance is caused by an electrical fault, a signal will be sent to open the closest breaker and isolate the faulty segment. On the other hand, if the analysis resulted in identifying an FDIA present in the system, the IDRS would initiate the classification procedure to categorize the FDIA into one of the following classes: FDIA targeting a single IED, FDIA targeting two IEDs simultaneously, FDIA targeting three IEDs simultaneously, FDIA targeting four IEDs simultaneously or FDIA targeting all five IEDs in the virtual grid. Once the classification part is completed, the algorithm will initiate the recovery approach. The system locates the affected IEDs based on historical patterns. The contaminated devices are afterwards isolated from the grid and a LSTM based recurrent neural network is

deployed to forecast the current sinusoidal readings of the isolated IEDs and maintain the system observability during a cyber-attack.

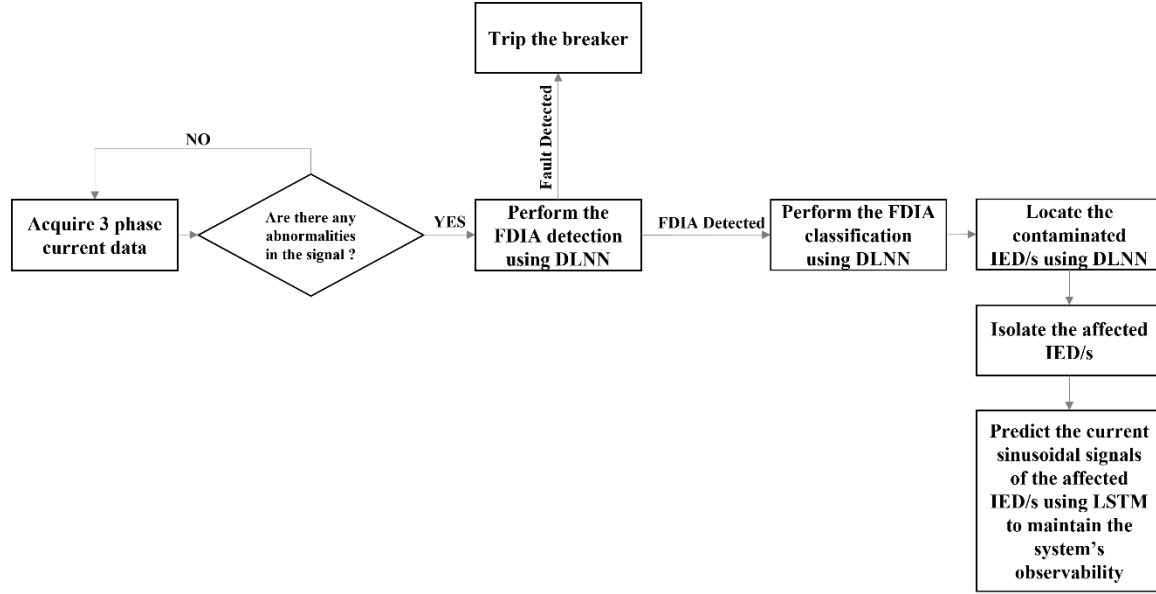


Figure 3.1. IDRS algorithm flowchart

3.1 IEEE 13 Bus system Model

A smart grid is an electricity network that uses digital communications and control technologies to monitor and manage the exchange of electricity from all generation sources to meet the varying electricity demands of end users. Its objective is to coordinate the needs and capabilities of all generators, grid operators, end users and electricity market stakeholders to operate all parts of the system as efficiently as possible, minimizing costs and environmental impacts while maximizing system reliability, resilience and stability. This research adopted the IEEE 13 bus system presented in [66]. The subject distribution model is ideal for the objectives of this research since it exhibits the following properties:

1. Relatively high load is drawn from the 4.16 kV generation source.
1. A variety of overhead and underground distribution lines.
2. Presence of non-linear shunt capacitor banks.
3. Existence of in-line power transformers.
4. Randomly unbalanced and distributed loading across the model.

The line parameters used in modeling the IEEE 13 bus system are displayed in Table 3.1.

The model clearly provides a variety of line types such as overhead or underground, phasing sequences and sizes. Moreover, the Capacitor data are shown in Table 3.2, Transformer data are shown in Table 3.3 And finally, the loading configuration is detailed in Table 3.4. To add an additional layer of complexity, this model was modified to randomly vary the loads across the distribution feeder with a factor ranging from 50% to 100% of the original rated value to represent different consumer behaviors.

Table 3.1. IEEE 13 Bus System Line Data

From Node	To Node	Length (m)	Line Type	Phasing	Size (AWG)	
					Phase	Natural
632	645	152.4	Overhead	C B N	4/0	4/0
632	633	152.4	Overhead	C A B N	4/0	4/0
645	646	91.44	Overhead	C B N	4/0	4/0
650	632	609.6	Overhead	B A C N	556	4/0
684	652	243.84	Underground	A N	1/0	1/0
632	671	609.6	Overhead	C B N	4/0	4/0
671	684	91.44	Overhead	A C N	1/0	1/0
671	680	304.8	Overhead	C B N	4/0	4/0
684	611	91.44	Overhead	C N	1/0	1/0
692	675	152.4	Underground	A B C N	250,000	None

Table 3.2. IEEE 13 Bus System Capacitor Data

Node	Phase A kVar	Phase B kVar	Phase C kVar
675	200	200	200
611	0	0	100

Table 3.3. IEEE 13 Bus System Transformer Data

From Node	To Node	Capacity (KVA)	High Voltage Rating	Low Voltage Rating	R %	X %
633	634	500	4.16 kV	0.48 kV	1.1	2

Table 3.4. IEEE 13 Bus system Load Data

Node	Configuration	Phase A		Phase B		Phase C		Load Randomization Factor
		kW	kVAr	kW	kVAr	kW	kVAr	
634	Wye - PQ	160	110	120	90	120	90	50% - 100%
645	Wye - PQ	0	0	170	125	0	0	
646	Delta - Z	0	0	230	132	0	0	
652	Wye - Z	128	86	0	0	0	0	
671	Delta - PQ	385	220	385	220	385	220	
675	Wye - PQ	485	190	68	60	290	212	
692	Delta	0	0	0	0	170	151	
611	Wye	0	0	0	0	170	80	
632-671	Wye - PQ	17	10	66	38	117	68	
Total		1175	616	1039	665	1252	821	

The original IEEE 13 bus system requires additional modifications to accurately represent a modern smart grid. Namely, monitoring and digital communication equipment based on IEC 61850 protocol [67]. The transformation towards a smart grid started by incorporating distributed IEDs designed to protect and control the grid as show in Figure 3.2. The IEDs were strategically placed to cover all three-phase loads with it designated protection zones. As a result of this placement, each IED will be able to monitor a specific area of the smart grid and perform the necessary protection actions in case of an electrical fault.

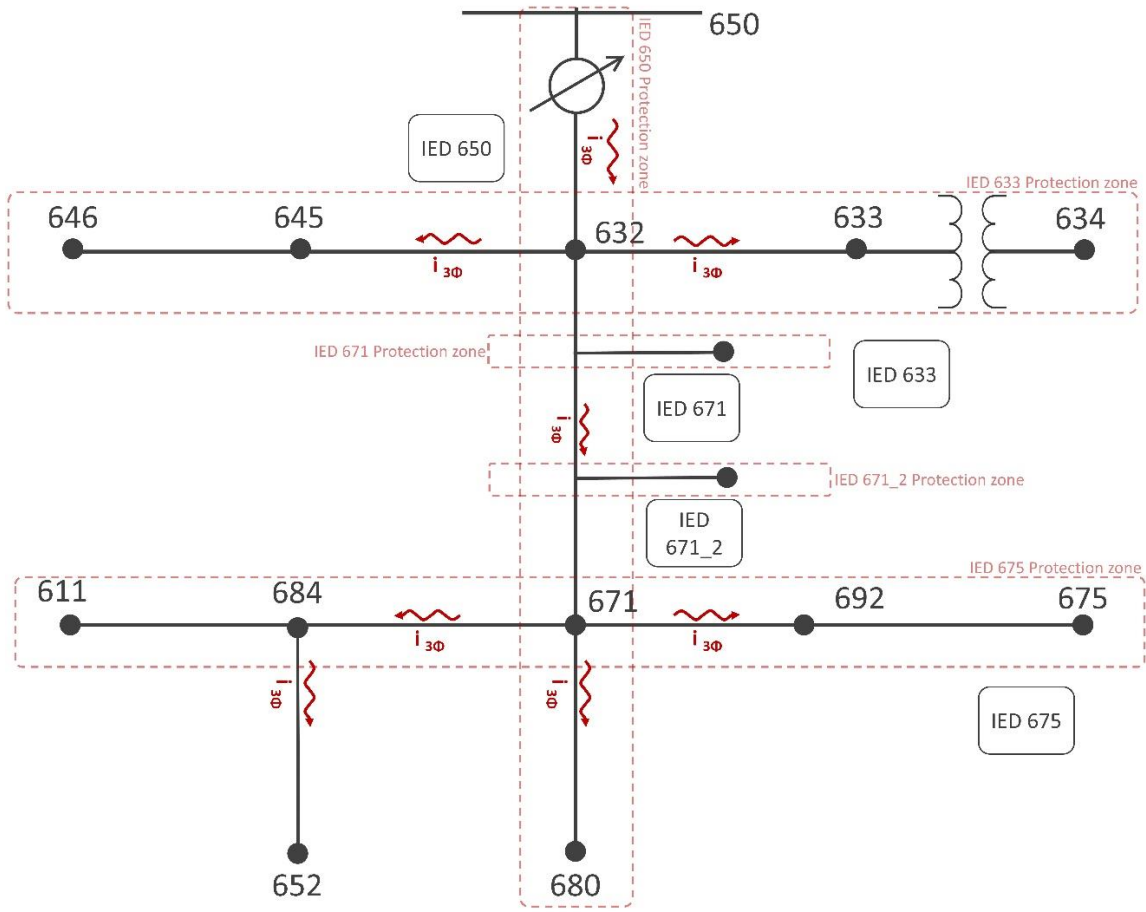


Figure 3.2. Modified IEEE 13 Bus System with Distributed Loads

To develop the data set required for achieving Intrusion detection, classification, location and recovery, this thesis focused on current sinusoidal wave forms as the main input type for training the neural networks. Current waveforms carry over harmonic components that can be distinguished easily by pattern recognition approaches and are considered the key measurement parameter in power system protection schemes [68]–[71]. Simulating the data set and extracting the current waveforms for each case requires an accurate calculation

of the system power flow at the modeled loading conditions. The Newton-Raphson method [72] is utilized in this research. The method defines the real and reactive powers as follows:

$$P_k = \sum_{n=1}^m |V_k| |V_n| |Y_{kn}| \cos(\theta_{kn} - \delta_k + \delta_n) \quad (3.1)$$

$$Q_k = - \sum_{n=1}^m |V_k| |V_n| |Y_{kn}| \sin(\theta_{kn} - \delta_k + \delta_n) \quad (3.2)$$

Where k and n represent the buses, V represents the voltage, Y indicates the line admittance, θ outlines the admittance phase angles in radian and δ defines the voltage phase angles in radian.

As a result, the estimates for the bus voltage magnitude and angle are:

$$\delta_k^{(q+1)} = \delta_k^{(q)} + \Delta \delta_k^{(q)} \quad (3.3)$$

$$|V_k^{(q+1)}| = |V_k^{(q)}| + \Delta |V_k^{(q)}| \quad (3.4)$$

The iterative approach is set to terminate when the change in residuals is less than $\epsilon = 0.0001$. Once the voltages are calculated, the method utilizes the following equation to determine the current:

$$I_{kn} = \frac{V_n - V_k}{R_{kn}} \quad (3.5)$$

The system frequency was selected as 60 hz. The current sinusoidal waveforms are calculated at each branch of the grid to create the needed database. Each sample collected is limited to a 2-cycle measurement with a sampling rate of 1 sample every 0.0165 ms.

3.2 Electrical Fault Model

An electrical fault represents a critical event that occurs in any power system component due to insulation damage or internal malfunction. Such disturbances can be classified into two main types: Active and passive. The latter of which occurs in underground conductor insulation deterioration over a period of time [73], and the other occurs when an overhead conductor breaks and touches a resistive ground creating an immediate transient arc [74], [75]. During its undetected state, an electrical fault is a risk to the public safety since a downed conductor can create hazardous shock, fire or life-threatening injuries through unintentional human contact [76]–[79]. Equipment damages due to the presence of faults are also considered as a threat to the facility's assets and may cause irreparable damage [80], [81]. As a result, the industry focused on developing protection schemes such as differential and overcurrent functions [82]–[89] to act instantly and isolate the faulty component from the grid. However, such action can initiate a series of events that will lead to complete power outage. Therefore, with the introduction of smart grids, the vulnerability of the power grid greatly increased as the attackers can inject falsified measurements into the IEDs to trigger nuisance protection functions and disturb the power flow.

This research aims to simulate all possible three classes of electrical faults namely: three phase to ground, double phase to ground (ABG, ACB and BCG) and single phase to ground (AG, BG and CG) at the distributed locations shown in Figure 3.3. The faults were strategically placed to capture the occurrence of such disturbance in both overhead and underground lines.

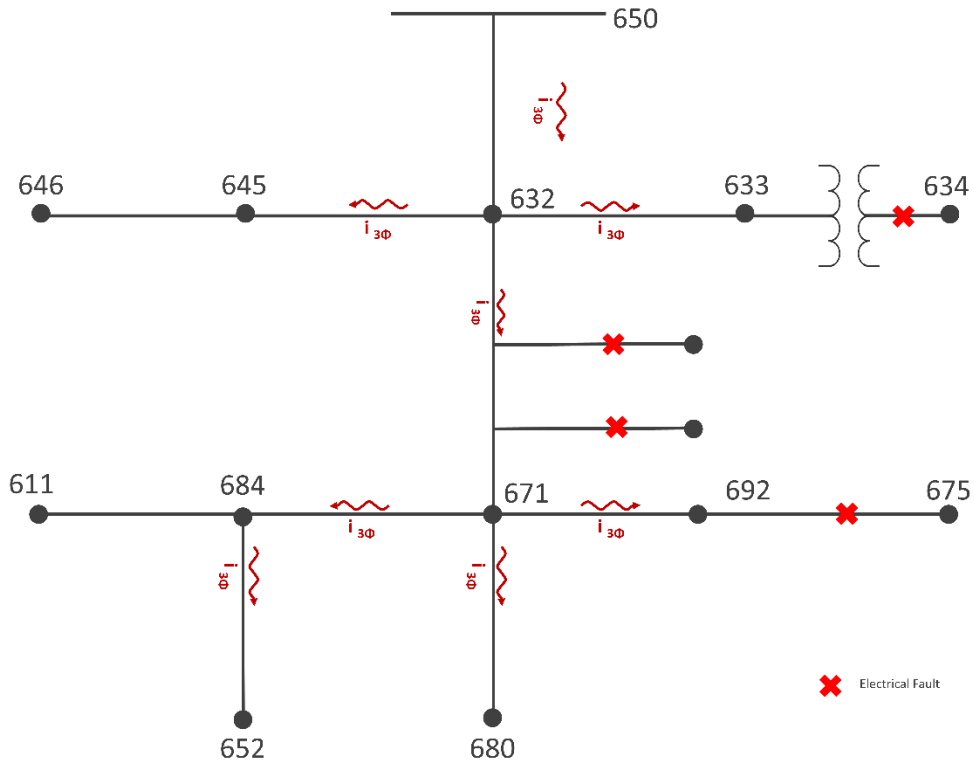


Figure 3.3. Electrical Fault Locations

Obtaining the Thevenin equivalent impedance [90] at the fault location is key for calculation three phase to ground faults. Parallel impedance equivalents are calculated as follows:

$$Z_{th}^{Parallel} = \frac{Z_k Z_n}{Z_k + Z_n} \text{ for any bus } k \text{ or } n \quad (3.6)$$

And series impedance is calculated as follows:

$$Z_{th}^{series} = Z_k + Z_n \text{ for any bus } k \text{ or } n \quad (3.7)$$

Once the Thevenin equivalent impedance is determined, the following equation is used to obtain the fault current:

$$I_k = \frac{V_k}{Z_{th} + Z_f} \quad (3.8)$$

Where Z_f is the fault impedance. Figure 3.4 shows the complete system readings during the occurrence of a three phase to ground fault near node 634. It can be observed that the sharp increase in current amplitude is only observed at IEDs 650 and 633.

Double line to ground faults are considered asymmetrical. Therefore, a representation of the system in sequence components [91] is needed for accurate calculations of fault current. Therefore, the symmetrical components of the current can be calculated as follows:

$$I_a^{+-0} = A^{-1} I^{abc} \quad (3.9)$$

And the symmetrical components of the voltage can be calculated as follows:

$$V_a^{+-0} = A^{-1} V^{abc} \quad (3.10)$$

Assuming that i, j and k would represent any combination of the phases a, b and c where $i \neq j \neq k$, then the double line to ground fault between phases i and j can lead to the following:

$$V_i = V_j = Z_f(I_i + I_j) \quad (3.11)$$

Where the fault current can be obtained from:

$$I_f = I_i + I_j = I_k^0 + a^2 I_k^+ + a I_k^- + I_k^0 + a I_k^+ + a^2 I_k^- = 3I_k^0 \quad (3.12)$$

On the other hand, a single line to ground fault at bus i will result in the following:

$$V_i = Z_f I_i \quad (3.13)$$

$$I_j = I_k = 0 \quad (3.14)$$

By substituting (27) into (22), the fault current can be calculated as follows:

$$I_f = 3I_i^0 \quad (3.15)$$

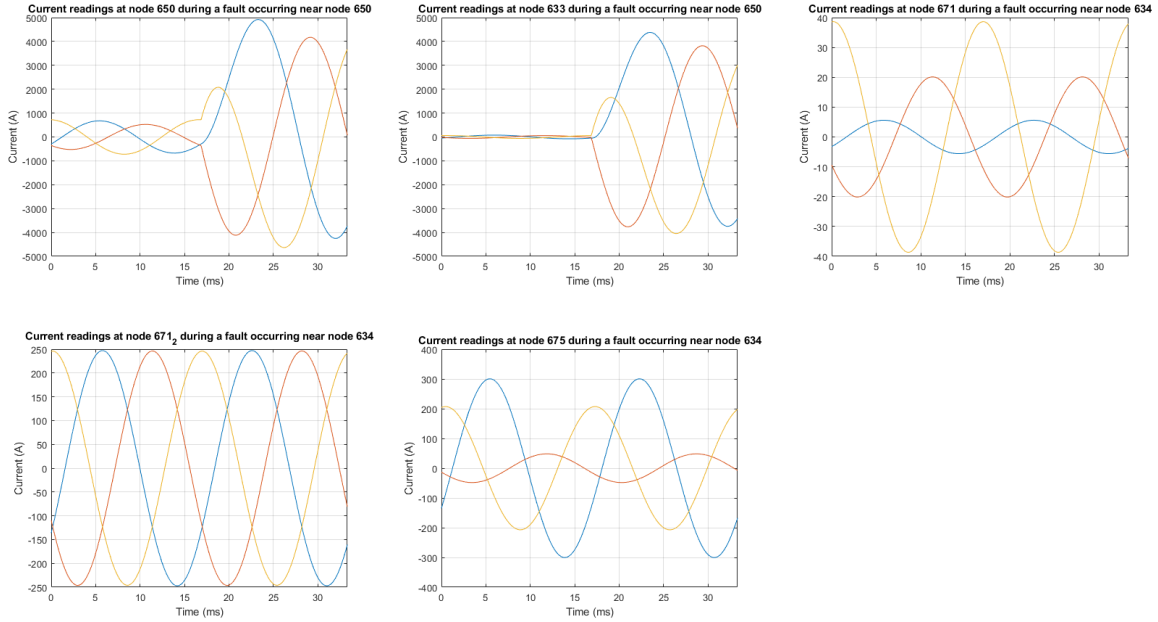


Figure 3.4. Overall System Readings During an ABCG Fault at Node 650

3.3 False Data Injection Model

An FDI attack occurs when the attacker injects a misleading set of measurements in place of the IED field sensors. As a result, the attacker can trigger catastrophic actions taken by the automated protection algorithms that can lead to power supply loss. Several objectives can be achieved by the attacker while targeting a power system such as:

1. Earning financial benefits.
2. Gaining reputation in the hacker's community.
3. Disturbing the power flow in the grid without being detected.

The latter of the aforementioned motives will be the focus of this research while modeling the attacking scenarios. This research considers the following capabilities of the attacker targeting the proposed modified IEEE 13 bus system:

1. Only lines feeding 3-phase loads are protected by IEDs. Hence the focus of the intruder is limited.
2. The intruder can mask the local measurements of the grid via the network to inject a sudden high current measurement similar to the short circuit cases presented in 3.2.
3. System parameters including loads, distribution, generation are available for the attacker.

Taking into account the capabilities of the attacker, the injected false current measurements are calculated based on equation (14):

$$I_{FDI} = \frac{V_n - V_k}{R_{kn}} \times F_{factor} \quad (3.16)$$

Where F_{factor} represents a random value between [6,8] to accurately simulate current readings similar in behavior to an actual short circuit fault with varying fault resistance value. The range is selected based on the maximum available short circuit in the modeled system.

The simulated FDIA scenarios are classified into two main categories: Single IED FDIA scenario is caused by an infiltration of one out of the 5 IEDs impeded in the system. The attack is designed to falsely emulate an overcurrent measurement to the protection system at a single point. As a result, the protection scheme would automatically trigger an alarm and send a trip signal to the breaker. This research simulated single FDI attacks distributed among 5 different measurement points.

On the other hand, coordinated FDI attacks targeting multiple IEDs are further classified depending on the number of targeted IEDs. A breakdown of all simulated scenarios is provided in Table 3.5. Double IED FDI attacks target all possible 10 combinations of two IEDs distributed in the system. Triple IED FDI attacks are another class of the coordinated assaults on the smart grid. The class of quadruple IED FDI attacks considers 5 scenarios.

Table 3.5. Breakdown of Coordinated Attacking Scenarios

Attack Classification	Scenario Number	Tragetted IED				
		IED 650	IED 633	IED 671	IED 671_2	IED 675
Double IED	Scenario 1	x	x			
	Scenario 2	x		x		
	Scenario 3	x			x	
	Scenario 4	x				x
	Scenario 5		x	x		
	Scenario 6		x		x	
	Scenario 7		x			x
	Scenario 8			x	x	
	Scenario 9			x		x
	Scenario 10				x	x
Triple IED	Scenario 11	x	x	x		
	Scenario 12	x	x		x	
	Scenario 13	x	x			x
	Scenario 14	x		x	x	
	Scenario 15	x		x		x
	Scenario 16	x			x	x
	Scenario 17		x	x	x	
	Scenario 18		x	x		x
	Scenario 19		x		x	x
	Scenario 20			x	x	x
Quadruple IED	Scenario 21	x	x	x	x	
	Scenario 22	x	x	x		x
	Scenario 23	x	x		x	x
	Scenario 24	x		x	x	x
	Scenario 25		x	x	x	x
All Out Attack	Scenario 26	x	x	x	x	x

3.4 Deep Learning Neural Network Model

A DLNN is an interconnection of several processing nodes performing a series of mathematical operations governed by the network's internodal strength, or weight, influenced by an external input referred to as bias attained by a set of historical patterns through the process of adaptation [92]–[94]. The presences of an additional layer between the input and output layers as well as the pre-processing stage of a DLNN is the distinguishing factor from the classical Multi-Layer Perceptron Neural Network (MLPNN). Such layer is often referred to as a hidden layer due to its invisibility from the prospective of both input and output layers [95]. The addition of such a hidden layer provides an extra computational width to the DLNN via extracting larger numbers of distinguishing features from the system's inputs [96].

The DLNN model tailored for this approach is shown in Figure 3.5, the method begins by performing normalization to reduce the sensitivity to initial values, this function rescales all inputs to the DLNN to a range from 0 to 1 and as a result, the network model can efficiently classify cases independent of the system loading condition or fault resistance. Subsequently, the Standard score (z-score) is calculated as follows:

$$Z_{score} = \frac{x - \mu}{\sigma} \quad (3.17)$$

Where x represents the current sample, μ is the mean of the sample set and σ is the standard deviation of the sample set. The z-score is critical for showcasing the trends in the raw signal as it highlights the numerical differences between the sample and mean.

The pre-processed data set is transmitted afterwards into the input layer, the numerical values are scaled by the network's weights and biases and inputted into the hidden layer.

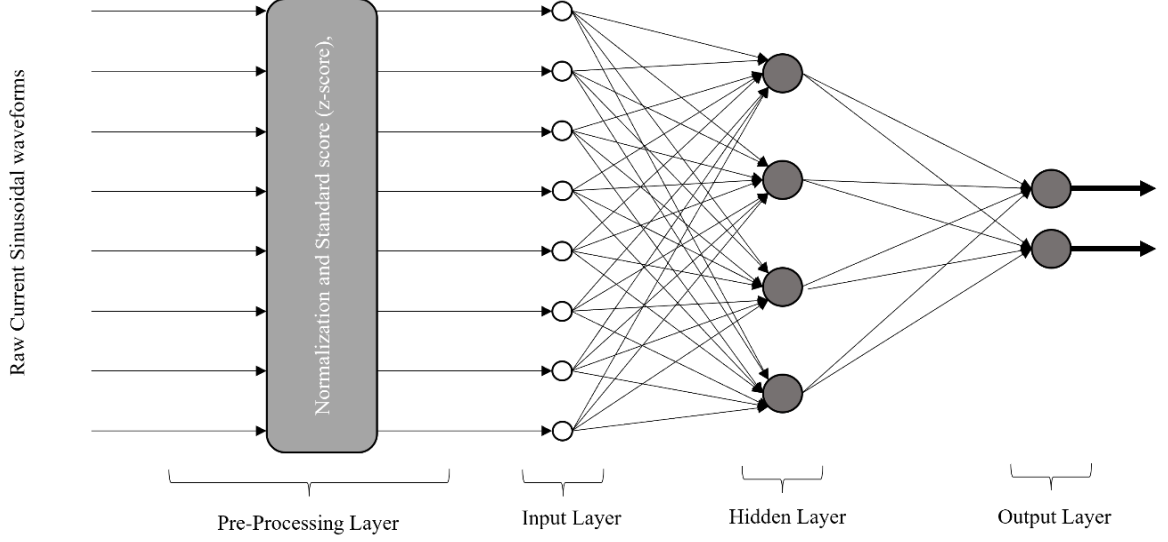


Figure 3.5. DLNN Model

In the hidden layer, the Rectified Linear Units (ReLU) activation function is utilized as governed by the following equation:

$$Output(y) = \begin{cases} 0, & x < 0 \\ x, & x \geq 0 \end{cases} \quad (3.18)$$

As shown in Figure 3.6, ReLU is a less computationally expensive function in comparison with hyperbolic tangent and sigmoid functions [97]. Moreover, gradient-based learning methods updates the weights and biases of a neural network in an iterative approach. In some cases, the gradient calculated will be numerically small and will stop the training process. However, ReLU functions voids the vanishing gradient problem [98].

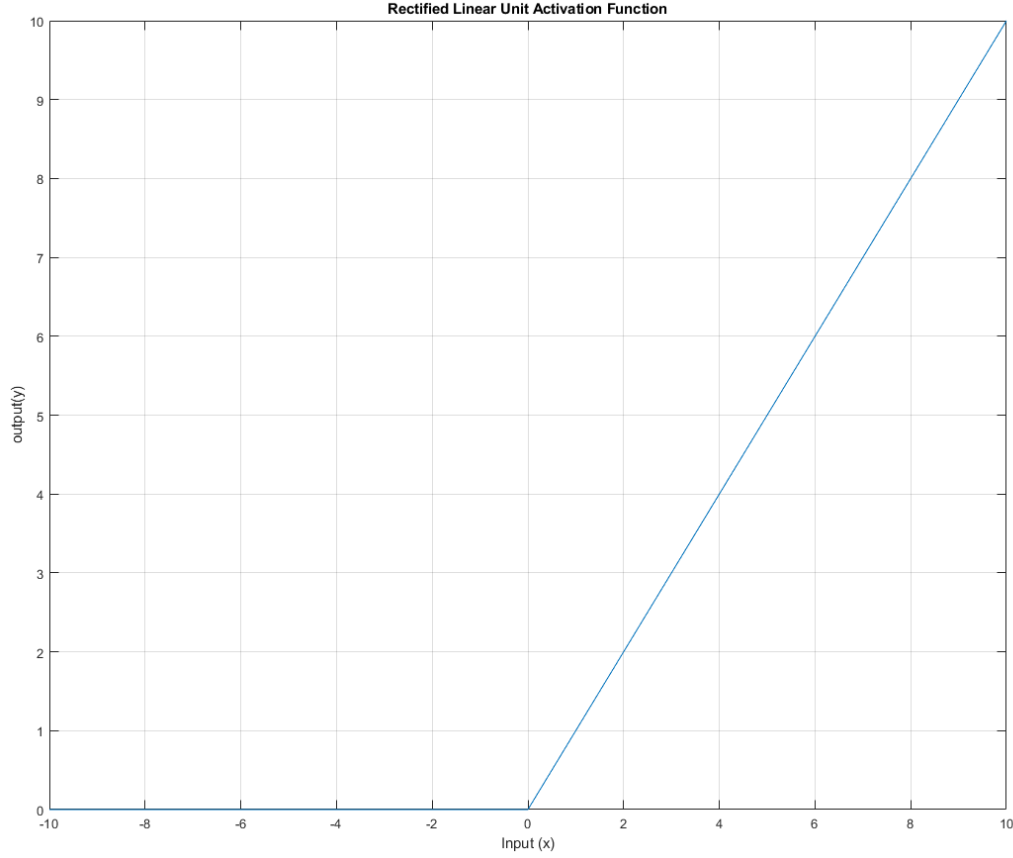


Figure 3.6. ReLU Activation Function

The output layer in the modeled DLNN deploys the Softmax activation function, the algorithm transforms a vector of numerical value into a vector that sums to 1. As a result, each input can be interpreted as a probability [99]. The Softmax function can be calculated as follows:

$$\sigma(\vec{x})_i = \frac{e^{x_i}}{\sum_{j=1}^K e^{x_j}} \quad (3.19)$$

Where $\vec{x}$ represents the input vector and K is the number of classes. The processed data set is converted into a probability distribution, as a result, the DLNN can distinguish between a spike the in the current signal due to a short circuit or an FDIA.

The selection of the Softmax and ReLU functions was based on several experimentation to obtain the selection most suitable for the data set used in this research. It can be observed from Table 3.6 that the functions provide greater accuracy probabilities.

Table 3.6. Average Activation Function Experimental Accuracy for the Proposed Problem

Activation Function	Average Experimental Accuracy
scaling Function	32%
quadratic Function	24%
dropout Function	40%
softmax Function	95%
sigmoid Function	61%
ReLU Function	98%
elu Function	25%
softplus Function	13%

To determine the weights and biases that corollate the output to the input for each of the described detection, classification and location problems, the Adam [100] optimization method is used. The algorithm capitalizes on the Adaptive gradient and Root Mean Square Propagation to calculate an exponential learning rate. Moreover, individual learning rate are calculated for each parameter which results in higher computational efficiency for large data problems. The Adam optimizer utilizes the following update equations:

$$w_i = \beta_1 w_{i-1} + (1 - \beta_1) \nabla E(\theta_i) \quad (3.20)$$

$$b_i = \beta_2 b_{i-1} + (1 - \beta_2) (\nabla E(\theta_i))^2 \quad (3.21)$$

Where the decay rates β_1 and β_2 are specified by the user, θ_i is the loss function, w_i represents the weight and b_i embodies the bias.

Table 3.7 demonstrates the performance of the Adam optimizer in comparison to other techniques such as Stochastic Gradient Descent with Momentum and Root Mean Square Propagation that are widely used in data classification problems. The method clearly demonstrates high average accuracy rates in the provided data set.

Table 3.7. Average Optimizer Accuracy for the Proposed Problem

Optimizer	Average Accuracy
Stochastic Gradient Descent with Momentum	54%
Root Mean Square Propagation	21%
Adam	90%

The proposed DLNN model is trained to achieve the following objectives:

1. Accurately distinguish between FDI attacks and various short circuit faults.
2. Classify the detected attack into one of the following categorize:
 - a. FDIA targeting a Single IED.
 - b. FDIA targeting two IEDs.
 - c. FDIA targeting three IEDs.
 - d. FDIA targeting four IEDs.
 - e. FDIA targeting all five IEDs.
3. Pinpoint the intrusion location and alarm the operator.

3.5 Long Short-Term Memory Model

To accurately estimate the current sinusoidal signal of the isolated IED after a cyber-attack the Long Short-Term Memory (LSTM) model introduced in this section is used as shown in Figure 3.7. The model consists of the hidden state (H) and the cell state (C). The hidden

state at time step t contains the output of the LSTM layer for this time step. The cell state contains information learned from the previous time steps. At each time step, the layer adds information to or removes information from the cell state.

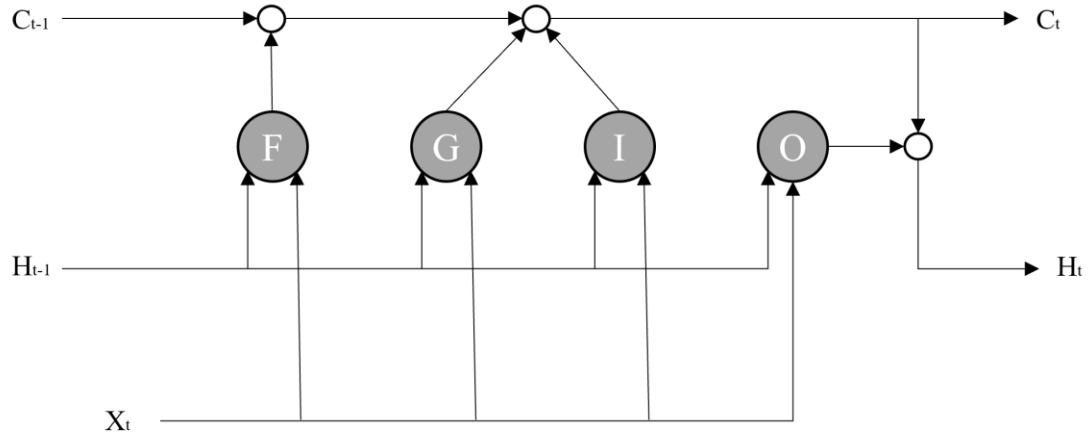


Figure 3.7. Long short-Term Memory Network Model

In the aforementioned model, the input gate **I** controls the cell state update, **F** gate is used to control what information is forgotten in order to avoid the long-term dependency on old data, **G** gate provide information to the cell state and the output gate **O** controls the flow of information provided to the hidden state.

The weights **W**, recurrent weights **R** and bias **b** can be represented as follows:

$$W = \begin{bmatrix} W_i \\ W_f \\ W_g \\ W_o \end{bmatrix}, R = \begin{bmatrix} R_i \\ R_f \\ R_g \\ R_o \end{bmatrix} \text{ and } b = \begin{bmatrix} b_i \\ b_f \\ b_g \\ b_o \end{bmatrix} \quad (3.22)$$

As a result, the input gate, forget gate, cell candidate and output gate formulas can be described as follows [101], [102]:

$$I_t = \sigma(W_i X_t + R_i H_{t-1}) + b_i \quad (3.23)$$

$$F_t = \sigma(W_f X_t + R_f H_{t-1}) + b_f \quad (3.24)$$

$$G_t = \sigma(W_g X_t + R_g H_{t-1}) + b_g \quad (3.25)$$

$$O_t = \sigma(W_o X_t + R_o H_{t-1}) + b_o \quad (3.26)$$

The cell state at time t is given by:

$$C_t = F_t \cdot C_{t-1} + I_t \cdot G_t \quad (3.27)$$

And the hidden state at time t is given by:

$$H_t = O_t \cdot \sigma(C_t) \quad (3.28)$$

Where the gate activation function σ is defined as:

$$\sigma(x) = (1 + e^{-x})^{-1} \quad (3.29)$$

The proposed LSTM model utilizes the Adam optimizer to achieve the best set of weights, recurrent weights and biases and estimate the current sinusoidal signals. The model aims to provide accurate estimate of the current sinusoidal signal of a single IED FDIA.

CHAPTER 4

RESULTS AND DISCUSSIONS

To achieve the required continuity of power supply during an FDI attack, an IDRS for smart grids is developed using DLNN and LSTM. The proposed DLNN architecture is utilized at the first stage to distinguish between system faults and falsified injected signals by the intruder. To accomplish this objective, a set of training data is created out of all possible combinations of FDI attacks as well as short circuit faults. This set is categorized and fed into the DLNN training model to detect FDIAs in the grid. Later on, a new DLNN model is trained to classify the detected intrusion into one of the five possible types of FDI attacks, namely an attack targeting one, two, three, four or all IEDs in the grid. Once the classification endeavor is complete, five new sets of DLNNs are trained. Each of the aforementioned networks specializes in identifying the targeted IED or IEDs depending on the intrusion class. The algorithm is designed to isolate the compromised IEDs and alert the power system operator to the presence of an intrusion. Finally, the LSTM network is trained for each of the identified intrusion classifications to predict the readings of the isolated IEDs and maintain the observability of the network.

This section aims to detail the steps taken and results obtained while training the proposed DLNN and LSTM networks in achieving the following objectives:

1. Detect FDI attacks and distinguish between injected current signals and disturbances caused by a short circuit.

2. Classify the FDI attack into one of the following categories: an attack targeting one IED, two IEDs, three IEDs, four IEDs or all IEDs in the grid.
3. Locate and isolate the contaminated IEDs from the grid and send an alarm to the operator.
4. Predict the signals of the isolated IEDs to maintain the system observability.

4.1 False Data Injection Detection Results

Solving the FDIA identification problem is the most crucial stage for the proposed IDRS approach. In theory, the FDIA and faults exhibit similar current amplitudes. However, the proposed features will highlight the presence of the noise due to the fault arc and improve the accuracy of detection. In this attempt, the proposed DLNN is trained to accurately distinguish between an FDIA with high current spikes and a real system fault. However, to accomplish this desired objective, a set of fault data, occurring in the proposed IEEE 13 bus system, is created using MATLAB Simulink. The faults are distributed across four different locations in the system within both underground cable and overhead distribution lines. Moreover, electrical faults are simulated to cover all possible configurations such as three phase to ground, double phase to ground (ABG, ACB and BCG) and single phase to ground (AG, BG and CG). And finally, the faults are simulated under one-thousand different loading conditions and combinations to model the consumer's random behavior in electricity consumption. As a result, the total number of simulated cases is calculated as follows:

$$4 \text{ locations} \times 7 \text{ types} \times 1000 \text{ load conditions} = 28,000 \text{ cases}$$

Out of the 28,000 cases, 19,600 (70%) are used for the DLNN training procedures and the remaining 8,400 (30%) are used as testing cases. The selection of training and testing case is uniformly distributed and randomized to correctly train the deep learning model.

On the other hand, the FDI attacks are simulated in accordance to the following five scenarios: an attack targeting one IED, two IEDs, three IEDs, four IEDs or all IEDs in the grid. For each scenario, the FDIA is simulated using one of the seven possible phase combinations, namely ABCG, ABG, ACB, BCG, AG, BG and CG, and under 4,000 different current amplitudes ranging from 600% to 800% of the normal values. As a result, the total number of simulated FDI attacks is calculated as follows:

$$\begin{aligned} & 5 \text{ Scenarios} \times 7 \text{ Phase combinations} \times 4000 \text{ amplitude conditions} \\ & = 140,000 \text{ cases} \end{aligned}$$

However, only 28,000 cases were selected to achieve the required equality in input type dimensions to the DLNN. Therefore, for the FDIA data set, 19,600 (70%) cases are used in training procedures and the remaining 8,400 (30%) cases are used for testing purposes.

The procedure used in training the DLNN as per the proposed model is detailed in Algorithm 1. The program starts by loading the training dataset for the faulty and FDIA classes. Subsequently, the two-class target matrix is formed for the network to categorize each case of the presented dataset to its appropriate class. Afterwards, the preprocessing Z-score layer is calculated and activation functions ReLU and Softmax are impeded into the model. Finally, the adam optimizer is selected and the training program is activated to find the optimal set of weights and biases.

Algorithm 1. DLNN training procedure for FDIA detection

Step 1:	Load ('Fault Dataset'); Load ('FDIA Dataset')
Step 2:	Create the target matrix as follows: Targets (1:size('Fault Dataset'))=1; Targets (size('Fault Dataset')+1: size('FDIA Dataset') + size('Fault Dataset'))=2;
Step 3:	Form the required layers for the DLNN training as follows: Layers=[featureInputLayer('Normalization', 'zscore') fullyConnectedLayer(70 hidden neurons) reluLayer softmaxLayer classificationLayer]
Step 4:	Select the optimizer: Optimizer='adam'
Step 5:	Train the network: Detection_DLNN=trainNetwork(Training Data, Targets, Layers, Optimizer);

The training was set to terminate at a maximum of 30 epochs, each epoch is composed of 2,450 iterations updating at a learning rate set to be equal to 0.001. The average accuracy of training was exponentially increasing during the subsequent training epoch and achieving an average of 98.73% during the final epoch. In addition, the computed value of the loss function sharply detreated into an average of 0.14 during the final epoch.

The training data set was reintroduced into the training DLNN as a verification step, the results of the inputted cases are demonstrated in Table 4.1. It is clearly demonstrated by the shown overall accuracy in detection that the training objective was complete. Therefore, the unseen testing dataset is introduced to the trained network to gauge the accuracy of FDIA detection as shown in Table 4.2. As expected, the number of cases falsely identified has slightly increased. However, the network maintains a satisfactory overall accuracy score.

Table 4.1. Confusion Matrix of The Trained Detection DLNN Using the Training Dataset

Data Type	Class	Fault	FDIA	Accuracy
Training Data	Fault	19,595	5	99.9%
	FDIA	3	19,597	99.9%
Overall Accuracy				99.9%

Table 4.2. Confusion Matrix of The Trained Detection DLNN Using the Testing Dataset

Data Type	Class	Fault	FDIA	Accuracy
Testing Data	Fault	8,301	99	98.8%
	FDIA	28	8,372	99.6%
Overall Accuracy				99.2%

4.2 False Data Injection Classification Results

The classification of FDI attack types is the baseline for any further diagnosis or recovery attempt as it demonstrates the nature of the FDI attack to the power system operator. The objective of this algorithm is to identify the type of FDIA subjected into the grid. To accomplish this objective, a set of data is simulated for all of the five FDIA classes. In the single IED FDIA class, five scenarios were considered. Namely, an attack targeting IED 650, an attack targeting IED 633, an attack targeting IED 671, an attack targeting IED 671_2 and an attack targeting IED 675. For each of the aforementioned scenarios, all possible seven phase combinations are simulated under 400 different amplitudes. As a result, the total number of Single IED FDI attack cases can be calculated as follows:

$$\begin{aligned}
 &5 \text{ Scenarios} \times 7 \text{ Phase combinations} \times 400 \text{ amplitude conditions} \\
 &= 14,000 \text{ cases}
 \end{aligned}$$

The total number of Double IED FDI attack cases can be calculated as follows:

$$\begin{aligned} &10 \text{ Scenarios} \times 7 \text{ Phase combinations} \times 200 \text{ amplitude conditions} \\ &= 14,000 \text{ cases} \end{aligned}$$

The total number of Triple IED FDI attack cases can be calculated as follows:

$$\begin{aligned} &10 \text{ Scenarios} \times 7 \text{ Phase combinations} \times 200 \text{ amplitude conditions} \\ &= 14,000 \text{ cases} \end{aligned}$$

The total number of Quadrable IED FDI attack cases can be calculated as follows:

$$\begin{aligned} &5 \text{ Scenarios} \times 7 \text{ Phase combinations} \times 400 \text{ amplitude conditions} \\ &= 14,000 \text{ cases} \end{aligned}$$

And the total number of All out IED FDI attack cases can be calculated as follows:

$$7 \text{ Phase combinations} \times 2,000 \text{ amplitude conditions} = 14,000 \text{ cases}$$

The cases are totaling at 70,000. 70% (49,000) of the total cases are used in the DLNN training process, and the remaining 30% (21,000) is used for testing purposes.

As demonstrated in Algorithm 2, the program starts by loading all data sets. Afterwards, the target matrix is formed with a similar number of rows to the total cases. Since the five classes are defined to the network, Z-score is calculated as well as the activation functions ReLU and Softmax. Finally, the adam optimizer is selected and the training program is activated to find the optimal set of weights and biases.

Algorithm 2. DLNN training procedure for FDIA classification

Step 1:	Load ('Single FDIA Dataset'); Load ('Double FDIA Dataset'); Load ('Triple FDIA Dataset'); Load ('Quadrable FDIA Dataset'); Load ('All out FDIA Dataset');
Step 2:	Create the target matrix as follows: Targets size = 1 X all rows of training data Targets = 1; for rows corresponding to Single FDIA data Targets = 2; for rows corresponding to Double FDIA data Targets = 3; for rows corresponding to Triple FDIA data Targets = 4; for rows corresponding to Quadrable FDIA data Targets = 5; for rows corresponding to All out FDIA data
Step 3:	Form the required layers for the DLNN training as follows: Layers=[featureInputLayer('Normalization', 'zscore') fullyConnectedLayer(50 hidden neurons) reluLayer softmaxLayer classificationLayer]
Step 4:	Select the optimizer: Optimizer='adam'
Step 5:	Train the network: Classification_DLNN=trainNetwork(Training Data, Targets, Layers, Optimizer);

100 epochs were set as training termination limit due to the high number of classes in comparison to the detection problem, each epoch is composed of 98 iterations updating at a learning rate set to be equal to 0.001. As shown in Figure 4.1 , the losses calculated were decaying throughout the training process. And in contrast, the accuracy of classification was exponentially increasing up until an average of 95% in the las epoch which demonstrated the success in training the DLNN.

To validate the effectiveness of the proposed approach, the training data set was entered into the trained DLNN demonstrating the accuracy results shown in Table 4.3. The results show an overall satisfactory average accuracy of 98.98%. However, it can be observed that the algorithm is performing better in classifying Single, Quadrable and All out FDI attacks in comparison to Double and Triple FDI attacks. The same observation can be seen in the

attempt to test the trained network using a new set of data. As shown in Table 4.4, the algorithm maintains a similar accuracy average with a variance of -0.09%. This further proves the efficacy of the proposed DLNN algorithm in classifying the FDI attack types.

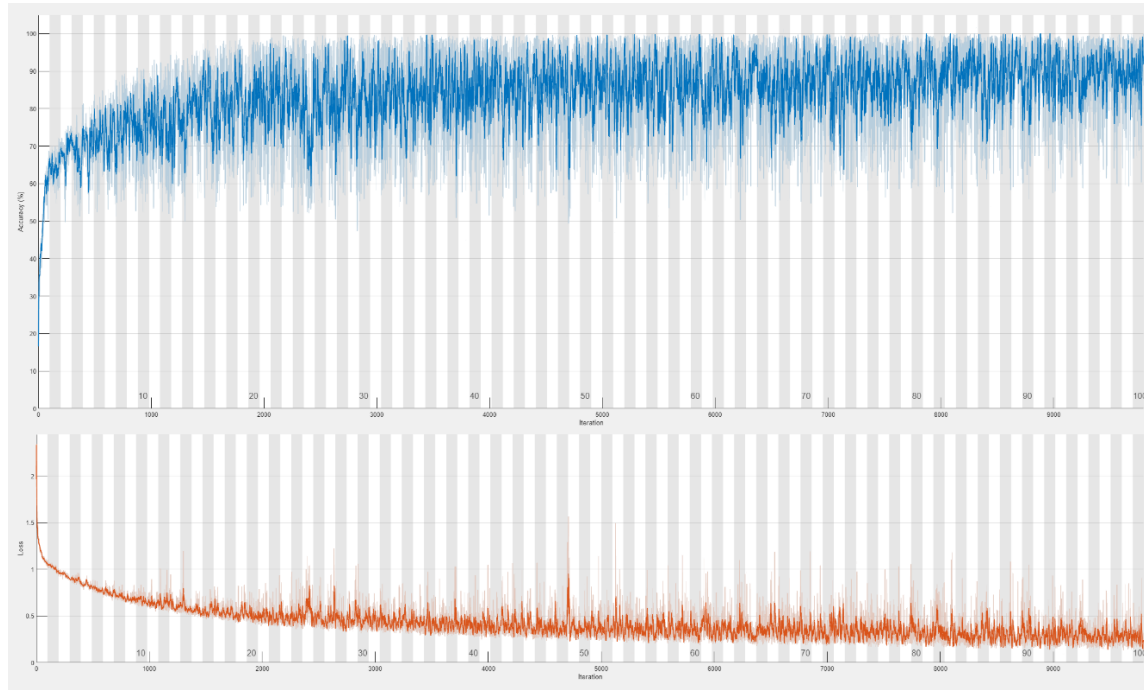


Figure 4.1. DLNN Training Performance for The Classification Problem

Table 4.3. Confusion Matrix of The Trained Classification DLNN Using the Training Dataset

Data Type	Class	Single IED FDIA	Double IED FDIA	Triple IED FDIA	Quadrable IED FDIA	All out IED FDIA	Accuracy
Training Data	Single IED FDIA	9,769	5	9	8	9	99.68%
	Double IED FDIA	97	9,533	32	92	46	97.27 %
	Triple IED FDIA	42	31	9,618	73	36	98.14%
	Quadrable IED FDIA	0	20	0	9,780	0	99.79%
	All out IED FDIA	0	0	0	0	9,800	100%
Overall Accuracy							98.98%

Table 4.4. Confusion Matrix of The Trained Classification DLNN Using the Testing Dataset

Data Type	Class	Single IED FDIA	Double IED FDIA	Triple IED FDIA	Quadrable IED FDIA	All out IED FDIA	Accuracy
Testing Data	Single IED FDIA	4,190	2	1	4	3	99.76%
	Double IED FDIA	39	4,087	21	19	34	97.31%
	Triple IED FDIA	11	26	4,100	18	19	97.62%
	Quadrable IED FDIA	0	10	0	4,190	0	99.76%
	All out IED FDIA	0	0	0	0	4,200	100%
Overall Accuracy							98.89%

4.3 False Data Injection Location Results

The next stage of the proposed IDRS approach consists of locating the point of intrusion. This step is essential to quickly recover the grid's functionality. To achieve successful intrusion location, Algorithm 3 is deployed. The program loads the data set utilized for training. Afterwards, the target matrix is created to assign a categorical value for each intrusion location class. Finally, the network is trained with the preprocessing Z-score layer, ReLU and Softmax activation functions and adam optimizer.

Algorithm 3. DLNN training procedure for FDIA location

Step 1:	Load training dataset
Step 2:	Create the target matrix and assign a categorical value for each class.
Step 3:	Form the required layers for the DLNN training as follows: Layers=[featureInputLayer('Normalization', 'zscore') fullyConnectedLayer(60 hidden neurons) reluLayer softmaxLayer classificationLayer]
Step 4:	Select the optimizer: Optimizer='adam'

Step 5: Train the network:
location_DLNN=trainNetwork(Training Data, Targets, Layers, Optimizer);

For each of the simulated FDIA scenarios. Namely, an attack targeting one IED, two IEDs, three IEDs, four IEDs or all IEDs in the grid, a separate network is trained to identify the contaminated IEDs. This procedure will effectively improve the accuracy of locating the intrusion points in the smart grid.

In the Single IED FDIA scenario, 7 phase combinations (phase A to ground, Phase B to ground, Phase C to ground, phases A and B to ground, Phases A and C to ground, phases B and C to ground and Phases A, B and C to ground) are simulated at 5 different intrusion points (IED 650, IED 633, IED 671 IED 671_2 and IED 675) and at 2,000 different amplitude conditions. As a result, the total number of cases simulated for the Single IED FDIA scenario is:

$$\begin{aligned} & 5 \text{ Intrusion Points} \times 7 \text{ Phase Combinations} \times 2,000 \text{ Amplitude Conditions} \\ & = 70,000 \text{ cases} \end{aligned}$$

Only 49,000 cases (70%) are used in the DLNN training process, while the remaining 21,000 (30%) are kept apart for testing purposes.

The proposed DLNN approach was successful in training the location network for Single FDIA IED intrusions. As shown in Figure 4.2, the network was trained using a learning rate equal to 0.001. The number of epochs was set to 20 with 3,062 iterations per epoch. The algorithm's accuracy was sharply increasing in each sequential epoch. On the other hand, the loss function output was observed to be nearing zero in the latest epochs.

The approach for locating Single IED FDIA intrusions was validated using the training data set. As shown in Table 4.5, the proposed DLNN approach was able to successfully locate the intrusion points maintain an accuracy rate of 100%. Moreover, an identical average accuracy of location was also observed while using the testing data set as shown in Table 4.6. This proves that the proposed DLNN approach is highly effective in locating the intrusion points during Single IED FDIA scenario.

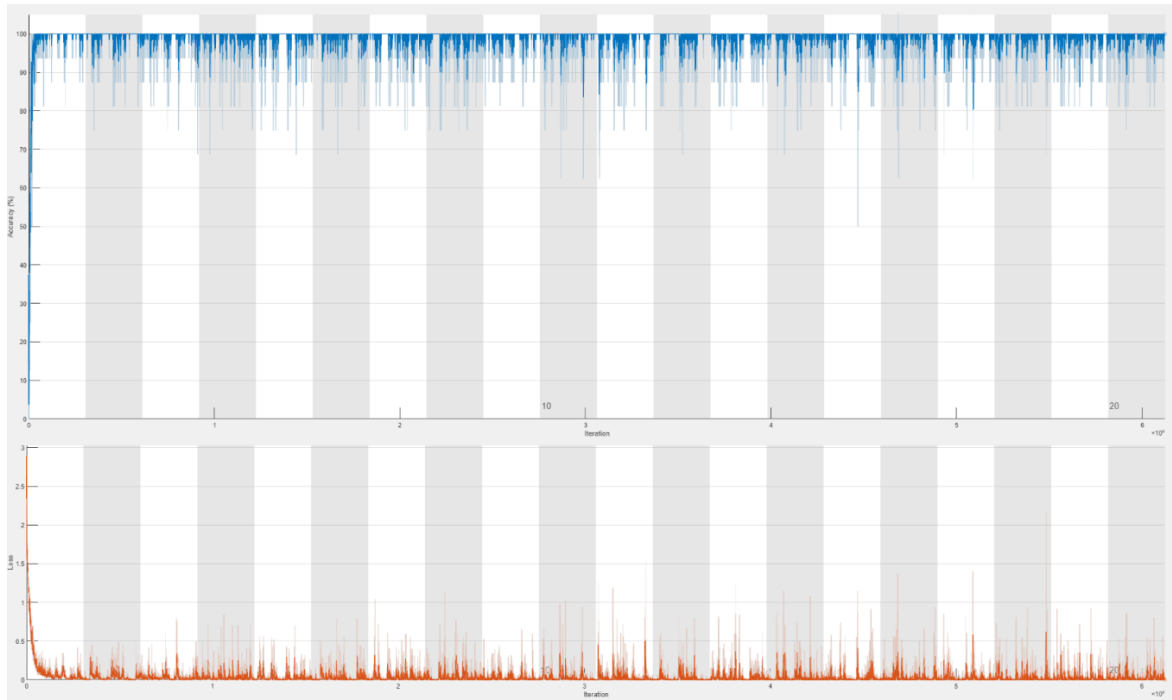


Figure 4.2. DLNN Training Performance for the Single IED FDIA Location Problem

Table 4.5. Confusion Matrix of The DLNN Using The Training Dataset

Data Type	Location	IED 650	IED 633	IED 671	IED 671_2	IED 675	Accuracy
Training Data	IED 650	9,800	0	0	0	0	100%
	IED 633	0	9,800	0	0	0	100%
	IED 671	0	0	9,800	0	0	100%
	IED 671_2	0	0	0	9,800	0	100%
	IED 675	0	0	0	0	9,800	100%
Overall Accuracy							100%

Table 4.6. Confusion Matrix of The DLNN Using The Testing Dataset

Data Type	Location	IED 650	IED 633	IED 671	IED 671_2	IED 675	Accuracy
Testing Data	IED 650	4,200	0	0	0	0	100%
	IED 633	0	4,200	0	0	0	100%
	IED 671	0	0	4,200	0	0	100%
	IED 671_2	0	0	0	4,200	0	100%
	IED 675	0	0	0	0	4,200	100%
Overall Accuracy							100%

The double IED FDIA scenario intrusion location problem extends the complications presented earlier as the framework of this scenario includes a coordinated scheme to disturb the power distribution through an unwanted protection action. The 10 combinations simulated in this approach include IEDs 650 & 633, IEDs 650 & 671, IEDs 650 & 671_2, IEDs 650 & 675, IEDs 633 & 671, IEDs 633 & 671_2, IEDs 633 & 675, IEDs 671 & 671_2, IEDs 671 & 675 and IEDs 671_2 & 675. As a result, the total cases used:

$$\begin{aligned}
 &10 \text{ Intrusion Points} \times 7 \text{ Phase Combinations} \times 2,000 \text{ Amplitude Conditions} \\
 &= 140,000 \text{ cases}
 \end{aligned}$$

Only 98,000 cases (70%) are used in the DLNN training process, while the remaining 42,000 (30%) cases are kept aside for testing purposes.

The proposed DLNN approach was successful in training the location network for Double FDIA IED intrusions. As shown in Figure 4.3, the network was trained using a learning rate equal to 0.001. the number of epochs was set to 10 with 6125 iterations per epoch. The algorithm's loss function output was approaching zero in the latest epochs. Additionally, the accuracy was greatly increasing in each sequential epoch.

The utilized training dataset was validated with the trained network as shown in Table 4.7. It can be observed that the validation process resulted in a 100% accuracy in location as expected. On the other hand, the overall location accuracy slightly dropped while utilizing the testing data set as shown in Table 4.8. Although the accuracy of location utilizing the testing data slightly dropped to 99.61%, the trained network proved to be reliable in location the intrusion points during several coordinated attacking scenarios targeting any two combinations of IEDs.

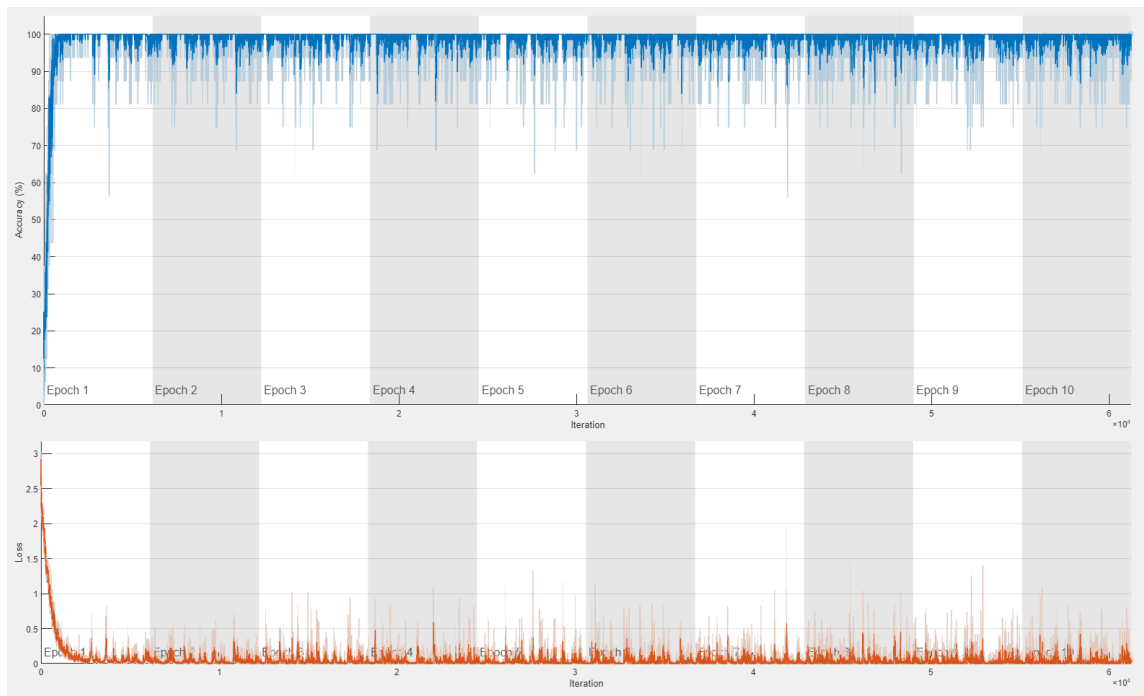


Figure 4.3. DLNN Training Performance for the Double IED FDIA Location Problem

Table 4.7. Confusion Matrix of Double FDIA DLNN Using The Training Dataset

Location	IED 650 and IED 633	IED 650 and IED 671_2	IED 671_2 and IED 675	IED 650 and IED 671	IED 650 and IED 675	IED 633 and IED 671_2	IED 633 and IED 671	IED 633 and IED 675	IED 671 and IED 671_2	IED 671 and IED 675	Accuracy
IED 650 and IED 633	9,800	0	0	0	0	0	0	0	0	0	100%
IED 650 and IED 671_2	0	9,800	0	0	0	0	0	0	0	0	100%
IED 671_2 and IED 675	0	0	9,800	0	0	0	0	0	0	0	100%
IED 650 and IED 671	0	0	0	9,800	0	0	0	0	0	0	100%
IED 650 and IED 675	0	0	0	0	9,800	0	0	0	0	0	100%
IED 633 and IED 671_2	0	0	0	0	0	9,800	0	0	0	0	100%
IED 633 and IED 671	0	0	0	0	0	0	9,800	0	0	0	100%
IED 633 and IED 675	0	0	0	0	0	0	0	9,800	0	0	100%
IED 671 and IED 671_2	0	0	0	0	0	0	0	0	9,800	0	100%
IED 671 and IED 675	0	0	0	0	0	0	0	0	0	9,800	100%
Overall Accuracy											100%

Table 4.8. Confusion Matrix of Double FDIA DLNN Using The Testing Dataset

Location	IED 650 and IED 633	IED 650 and IED 671_2	IED 671_2 and IED 675	IED 650 and IED 671	IED 650 and IED 675	IED 633 and IED 671_2	IED 633 and IED 671	IED 633 and IED 675	IED 671 and IED 671_2	IED 671 and IED 675	Accuracy
IED 650 and IED 633	4,194	0	0	6	0	0	0	0	0	0	99.85%
IED 650 and IED 671_2	0	4,198	0	0	0	2	0	0	5	0	99.95%
IED 671_2 and IED 675	0	0	4,191	0	9	0	0	0	0	0	99.78%
IED 650 and IED 671	6	0	0	4,194	0	0	0	0	0	0	99.88%
IED 650 and IED 675	0	0	9	0	4,189	0	0	0	0	2	99.73%
IED 633 and IED 671_2	0	2	0	0	0	4,177	0	21	0	0	99.45%
IED 633 and IED 671	0	0	0	0	0	0	4,159	0	41	0	99.78%
IED 633 and IED 675	0	0	0	0	0	9	0	4,191	0	0	99.02%
IED 671 and IED 671_2	0	0	0	0	0	0	41	0	4,159	0	99.02%
IED 671 and IED 675	0	0	0	0	0	15	0	0	0	4,185	99.64%
Overall Accuracy											99.61%

The triple IED FDIA intrusion location problem presents another possibility for the attacker to lead the protection systems of the electricity grid into taking an unwanted outage action. The 10 combinations simulated in this approach include IEDs 650 & 633 & 671, IEDs 650 & 633 & 671_2, IEDs 650 & 633 & 675, IEDs 650 & 671 & 671_2, IEDs 650 & 671 & 675, IEDs 650 & 671_2 & 675, IEDs 633 & 671 & 671_2, IEDs 633 & 671 & 675, IEDs 633 & 671_2 & 675 and IEDs 671 & 671_2 & 675. As a result, the total cases used:

$$\begin{aligned} &10 \text{ Intrusion Points} \times 7 \text{ Phase Combinations} \times 2,000 \text{ Amplitude Conditions} \\ &= 140,000 \text{ cases} \end{aligned}$$

70% of the cases (98,000) are used in the DLNN training process, while the remaining 30% (42,000) of cases are kept aside for testing purposes. As shown in Figure 4.4 the DLNN approach was successful in acquiring the optimal weights and biases for the triple IED FDIA location problem. The network was trained using a learning rate equal to 0.001. the number of epochs was set to 10 with 6125 iterations per epoch. The training accuracy was ranging from 84% to 100% in the last epoch. Moreover, the calculated function loss exponentially decreased below the 0.5 mark. The training set was reintroduced into the trained network as demonstrated in Table 4.9. It can be observed that the algorithm maintained an acceptable average accuracy of 99.87%. However, the accuracy of location was slightly decreased with the introduction of the training dataset as shown in Table 4.10. The accuracies calculated further solidifies the efficacy of the proposed DLNN approach in location the intrusion points of a triple IED FDI attack.

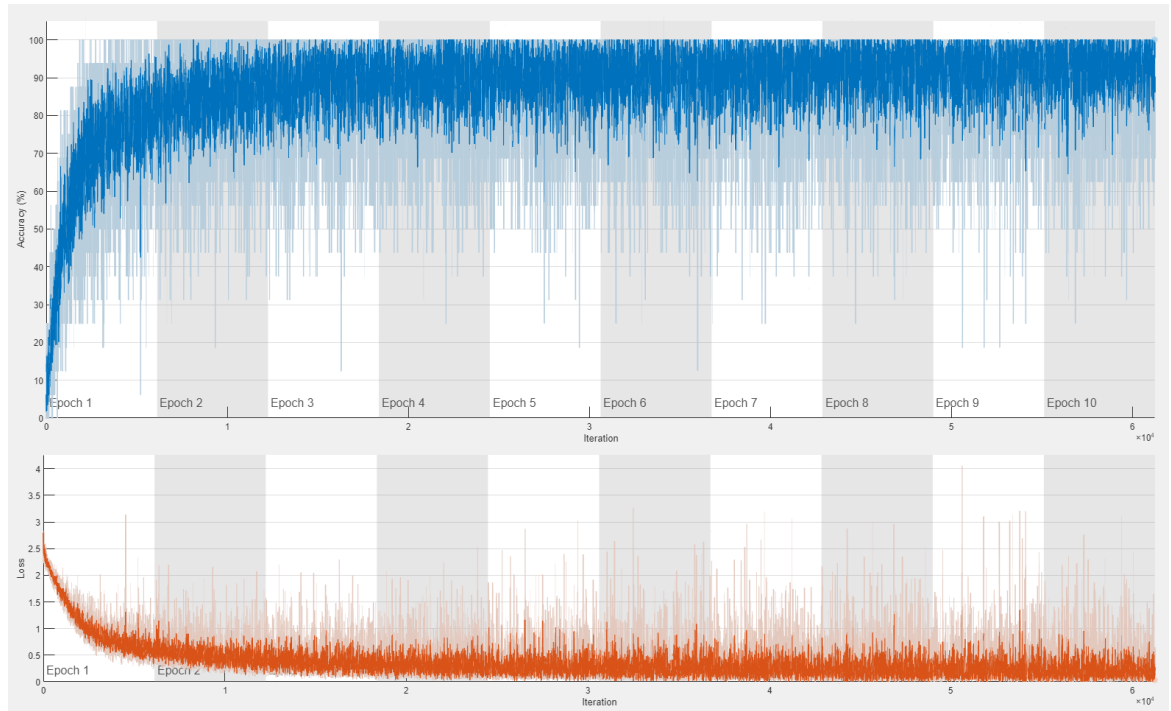


Figure 4.4. DLNN Training Performance for the Triple IED FDIA Location Problem

Table 4.9. Confusion Matrix of Triple FDIA DLNN Using The Training Dataset

Location	IED 632, IED671_2 and IED 675	IED 633, IED 671_2 and IED 675	IED 671, IED 671_2 and IED 675	IED 632, IED 633 and IED 671	IED 632, IED 633 and IED 675	IED 632, IED 671 and IED 671_2	IED 632, IED 671 and IED 675	IED 633, IED 671 and IED 671_2	IED 633, IED 671 and IED 675	IED 632, IED 633 and IED 671_2	Accuracy
IED 632, IED671_2 and IED 675	9,795	0	0	5	0	0	0	0	0	0	99.94 %
IED 633, IED 671_2 and IED 675	0	9,792	0	0	0	0	0	0	8	0	99.91 %
IED 671, IED 671_2 and IED 675	0	0	9,725	0	0	0	0	0	65	10	99.23 %
IED 632, IED 633 and IED 671	5	0	0	9,793	3	0	0	0	0	0	99.92 %
IED 632, IED 633 and IED 675	0	0	0	3	9,796	0	1	0	0	0	99.95 %
IED 632, IED 671 and IED 671_2	0	0	0	0	0	9,797	3	0	0	0	99.96 %
IED 632, IED 671 and IED 675	0	0	0	0	1	3	9,796	0	0	0	99.95 %
IED 633, IED 671 and IED 671_2	0	0	0	0	0	0	0	9,800	0	0	100%
IED 633, IED 671 and IED 675	0	0	0	0	0	0	0	0	9,794	0	99.93%
IED 632, IED 633 and IED 671_2	0	0	10	0	0	0	0	0	0	9,790	99.89%
Overall Accuracy											99.87%

Table 4.10. Confusion Matrix of Triple FDIA DLNN Using The Testing Dataset

Location	IED 632, IED671_2 and IED 675	IED 633, IED 671_2 and IED 675	IED 671, IED 671_2 and IED 675	IED 632, IED 633 and IED 671	IED 632, IED 633 and IED 675	IED 632, IED 671 and IED 671_2	IED 632, IED 671 and IED 675	IED 633, IED 671 and IED 671_2	IED 633, IED 671 and IED 675	IED 632, IED 633 and IED 671_2	Accuracy
IED 632, IED671_2 and IED 675	4,188	0	0	12	0	0	0	0	0	0	99.71%
IED 633, IED 671_2 and IED 675	0	4,192	0	0	0	0	0	0	8	0	99.80%
IED 671, IED 671_2 and IED 675	0	0	4,170	0	0	0	0	0	20	10	99.28 %
IED 632, IED 633 and IED 671	3	0	0	4,197	0	0	0	0	0	0	99.92 %
IED 632, IED 633 and IED 675	0	0	0	3	4,192	0	1	4	0	0	99.80 %
IED 632, IED 671 and IED 671_2	0	0	0	0	0	4,186	3	7	4	0	99.66 %
IED 632, IED 671 and IED 675	0	0	0	0	1	3	4,181	10	9	0	99.54 %
IED 633, IED 671 and IED 671_2	0	0	0	0	0	0	2	4,198	0	0	99.95 %
IED 633, IED 671 and IED 675	0	0	0	0	0	0	7	0	4,193	0	99.83 %
IED 632, IED 633 and IED 671_2	0	0	4	0	0	0	0	0	0	4,196	99.90 %
Overall Accuracy											99.74%

The final scenario considered in the coordinated FDI attack location problem refers to the quadrable IED FDIA. This methodology of attack is designed to severely affect the measurement systems and send the grid into a critical state resulting in the loss of power supply. Five combinations are considered in this scenario as follows: an attack targeting IEDs 650 & 633 & 671 & 671_2, IEDs 650 & 633 & 671 & 675, IEDs 650 & 633 & 671_2 & 675, IEDs 650 & 671 & 671_2 & 675, IEDs 633 & 671 & 671_2 & 675. As a result, the total cases used:

$$\begin{aligned} & 5 \text{ Intrusion Points} \times 7 \text{ Phase Combinations} \times 2,000 \text{ Amplitude Conditions} \\ & = 70,000 \text{ cases} \end{aligned}$$

Only 70% of the cases (49,000) are used in the DLNN training process, while the remaining 30% (21,000) of cases are kept aside for testing purposes. As shown in Figure 4.5, the DLNN approach was successful in acquiring the optimal weights and biases for the quadruple IED FDIA location problem. The network was trained using a learning rate equal to 0.001. The number of epochs was set to 7 with 3062 iterations per epoch. The training accuracy was ranging from 88% to 100% in the last epoch. Moreover, the calculated loss function exponentially decreased below the 0.4 mark. The training dataset was used to validate the trained network performance as shown in Table 4.11. It was observed that the accuracy performance of locating intrusions occurring at IED 650, IED 671, IED 671_2 and IED 675 simultaneously is slightly less distinguishable from the intrusions occurring at IED 633, IED 671, IED 671_2 and IED 675 due to the close proximity of IEDs 650 and 633. A similar behavior was also observed in the testing cases as shown in Table 4.12. However, the high average overall accuracy of 94.35% was accomplished, which proves the effectiveness of the proposed approach.

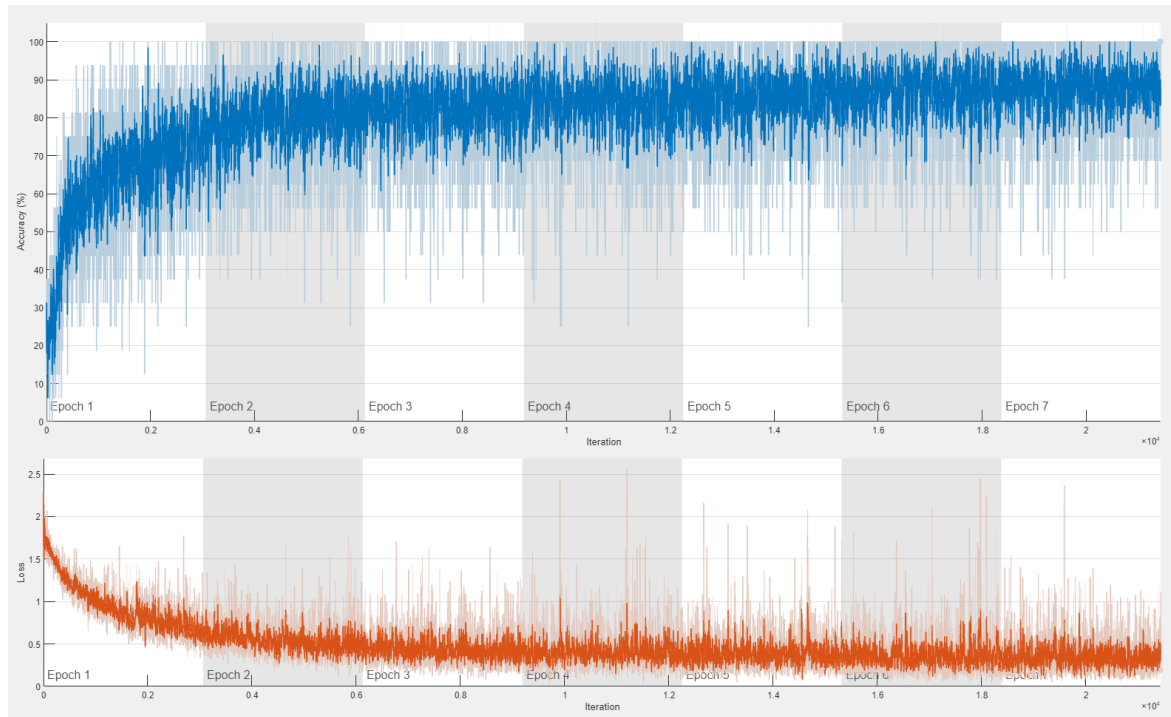


Figure 4.5. DLNN Training Performance for the Quadruple IED FDIA Location Problem

Table 4.11. Confusion Matrix of Quadruple FDIA DLNN Using The Training Dataset

Location	IED 650, IED 633, IED 671_2 and IED 675	IED 650, IED 671, IED 671_2 and IED 675	IED 633, IED 671, IED 671_2 and IED 675	IED 650, IED 633, IED 671 and IED 671_2	IED 650, IED 633, IED 671 and IED 675	Accuracy
IED 650, IED 633, IED 671_2 and IED 675	9,744	14	20	14	8	99.42 %
IED 650, IED 671, IED 671_2 and IED 675	0	8,528	1,272	0	0	87.02 %
IED 633, IED 671, IED 671_2 and IED 675	0	1,341	8,459	0	0	86.31 %
IED 650, IED 633, IED 671 and IED 671_2	6	0	0	9,794	0	99.93 %
IED 650, IED 633, IED 671 and IED 675	0	0	0	0	9,800	100%
Accuracy						94.54%

Table 4.12. Confusion Matrix Quadruple FDIA DLNN Using The Testing Dataset

Location	IED 650, IED 633, IED 671_2 and IED 675	IED 650, IED 671, IED 671_2 and IED 675	IED 633, IED 671, IED 671_2 and IED 675	IED 650, IED 633, IED 671 and IED 671_2	IED 650, IED 633, IED 671 and IED 675	Accuracy
IED 650, IED 633, IED 671_2 and IED 675	4,167	0	0	33	0	99.21 %
IED 650 IED 671, IED 671_2 and IED 675	0	3,680	520	0	0	87.61 %
IED 633, IED 671, IED 671_2 and IED 675	0	599	3,601	0	0	85.73 %
IED 650, IED 633, IED 671 and IED 671_2	33	0	0	4,167	0	99.21 %
IED 650, IED 633, IED 671 and IED 675	0	0	0	0	4,200	100%
Accuracy						94.35%

4.4 False Data Injection Measurement Recovery Results

Once an FDIA threat is identified, classified, located and isolated from the system, a further step is required to mitigate the consequences of such incident. The isolation of IEDs will limit the operator's observability. Therefore, the proposed IDRS implements an LSTM based approach to predict the current sinusoidal waveforms of the isolated IEDs. As detailed in Algorithm 4, the system begins by loading the dataset. This set is further segregated where the target signal to be predicted is isolated from the input signals. For example, if the attack was identified to be a single FDIA targeting IED 650, then the algorithm will use the signals of IEDs 633, 671, 671_2 and 675 as inputs, and the signals of IED 650 as the predicted output. Moreover, the layers are defined in the next step based on the number of phases to be predicted, the adam optimizer is selected and finally, the network is trained based on the input and selected options.

Algorithm 4. LSTM training procedure for signal prediction

Step 1:	Load training dataset
Step 2:	Define the number of channels (phases)
Step 2:	Form the required layers for the LSTM NN as follows: Layers=[sequenceInputLayer(numChannels) lstmLayer(128) fullyConnectedLayer(numChannels) regressionLayer];
Step 3:	Select the optimizer: Optimizer='adam'
Step 4:	Train the network: Prediction_LSTM=trainNetwork(Training Data,, Layers, Optimizer);

In the Single FDIA IED measurement recovery problem, the proposed approach sought to predict the measurement of isolated IEDs in the flowing scenarios: an attack targeting IED 650, IED 633, IED 671, IED 671_2 or IED 675. For each case, the signals from the other healthy IEDs are used as inputs to the LSTM network to predict the waveform of the isolated IED. The network was trained for a cycle of 200 epochs as shown in Figure 4.6. The Root Mean Square Error (RMSE) settled at a value of 0.14 in the last iteration. While the calculated loss function approaches zero at later simulation times.

The predicted current waveforms of IEDs 650 and 633 are shown in Figure 4.7 and Figure 4.8 respectively. The performance of the proposed method proved to be ideal in predicting the waveforms of the isolated IEDs. The similarity in accuracy is also contributed to the fact that both IEDs are close in proximity. On the other hand, the predicted current waveform of IED 671 exhibits a slight shift in phase A. However, the amplitude and frequency of the signal was accurately predicted as shown in Figure 4.9. The prediction of IED 671_2 waveforms result in a shifted pattern in phases A and B similar to the prediction results observed earlier in IED 671 as shown in Figure 4.10. Finally, the prediction of IED 675 exhibits various discrepancies as shown in Figure 4.11. The predicted signal in phases A and C endure a slight phase shift. Moreover, a slight difference in amplitude value between the actual and predicted phase B waveforms can be clearly observed.

Despite the minor errors shown in predicting the measurement of IED 675, the overall RMSE in testing was found to be 0.14 which is satisfactory to maintain the grid's observability and mitigate the consequences of an FDI attack.

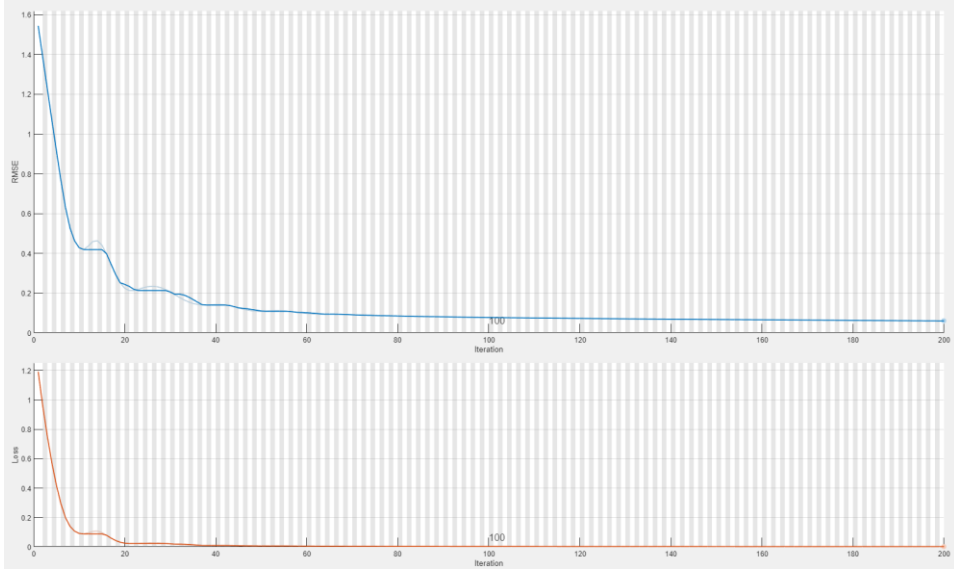


Figure 4.6. LSTM NN Training Performance in Predicting Single FDIA IED Measurements

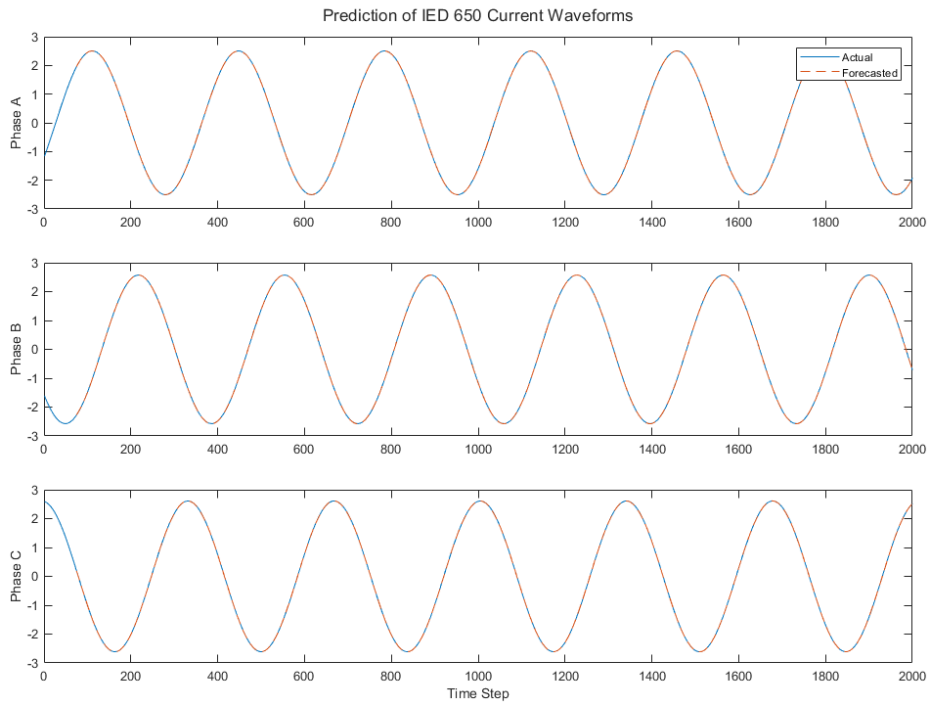


Figure 4.7. Actual Vs. Predicted IED 650 Current Waveform

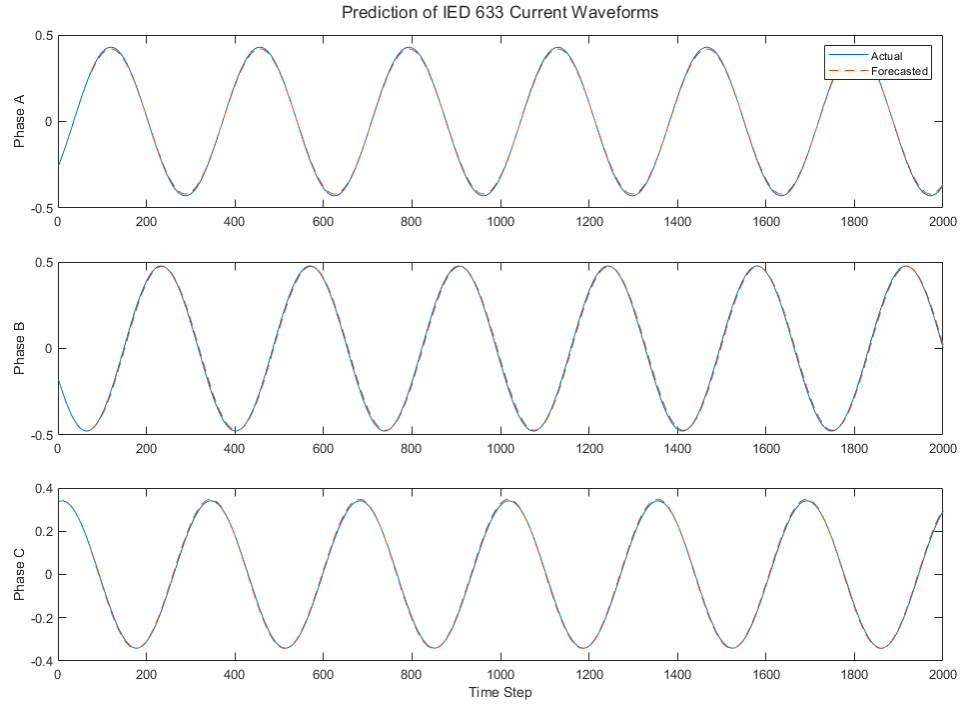


Figure 4.8. Actual Vs. Predicted IED 633 Current Waveform

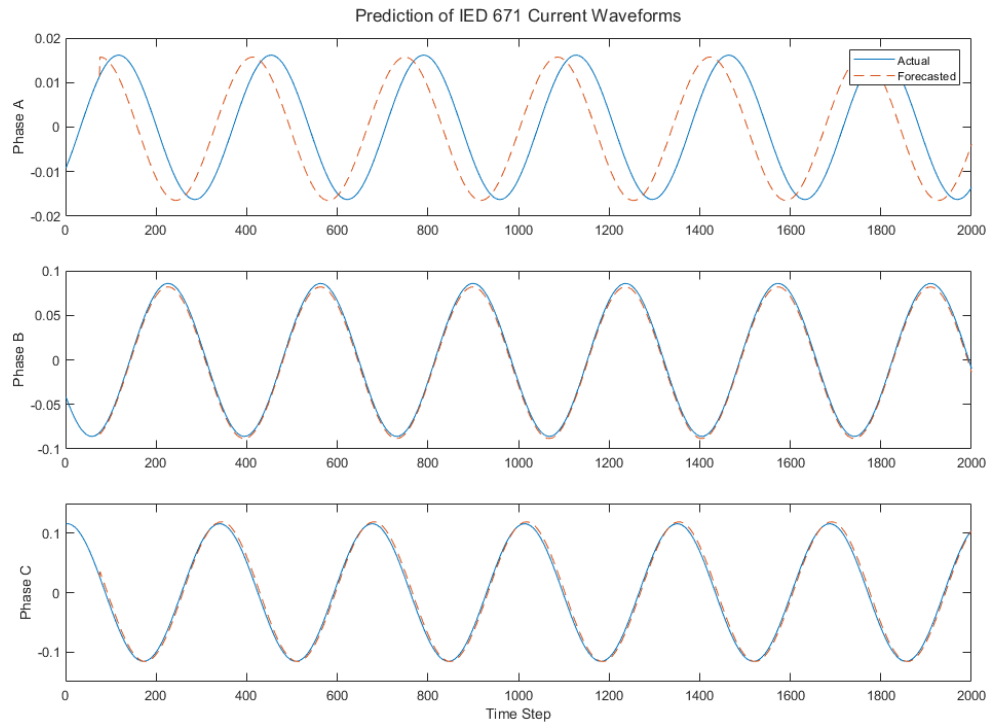


Figure 4.9. Actual Vs. Predicted IED 671 Current Waveform

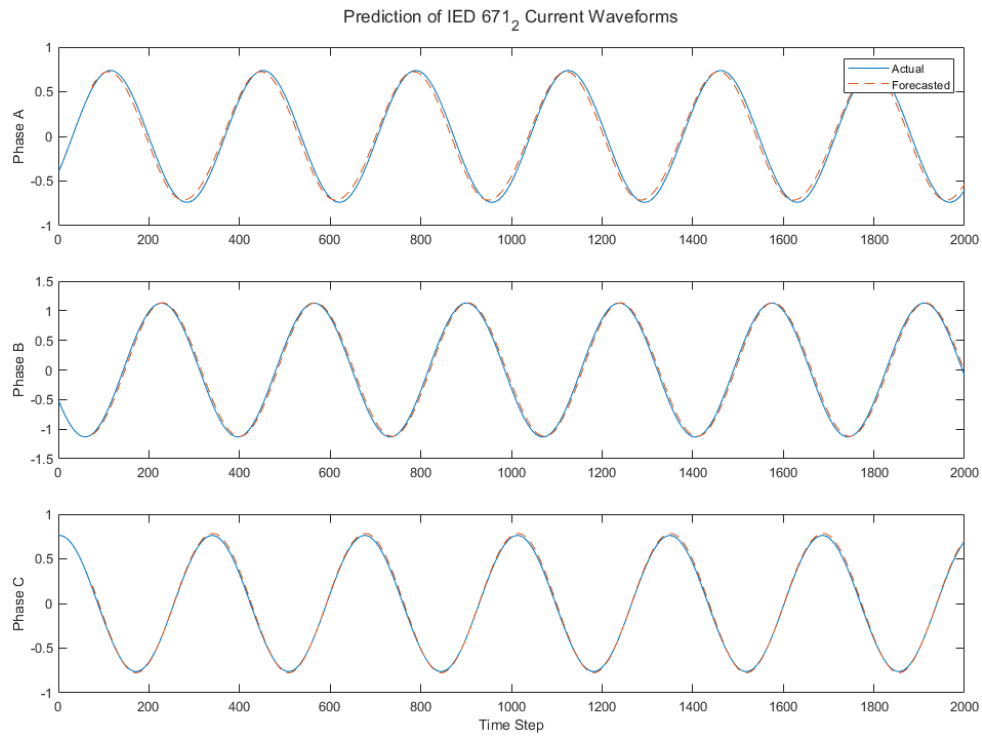


Figure 4.10. Actual Vs. Predicted IED 671₂ Current Waveform

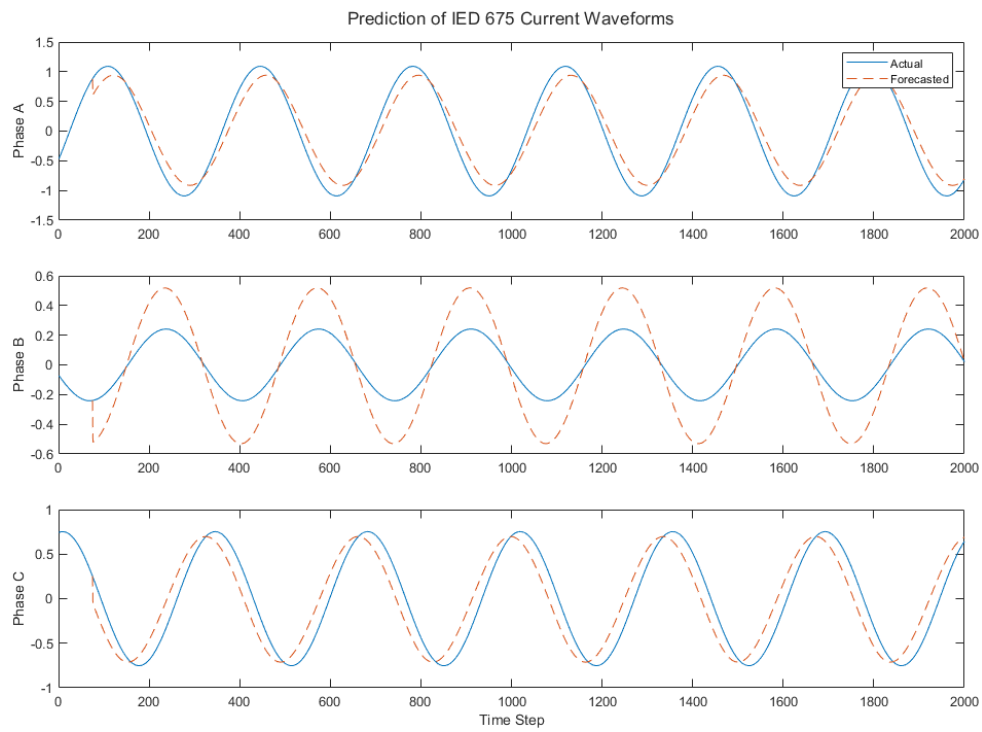


Figure 4.11. Actual Vs. Predicted IED 675 Current Waveform

CHAPTER 5

CONCLUSION AND FUTURE RECOMMENDATIONS

In recent years, the adaptation of digitalized monitoring and protection equipment was evident in electricity grids, which led to the emergence of the term known as “Smart Grid”. In this research, the smart grid was defined to be an interconnection of equipment aiming to exchange energy and data. Therefore, the IEEE 13 bus system was adopted and modified via the inclusion of distributed Intelligent Electronic Devices (IEDs). These IEDs are designed to constantly monitor the current sinusoidal waveforms and isolate the transmission lines in case of an electrical fault. However, the digitalization of power grids introduces additional vulnerabilities to the grid such as FDIAs that can fool the protection system into taking an unwanted outage action. In this research, a database was created containing the following:

1. Electrical fault data simulated in different locations of the grid, at distinctive loading conditions and with all possible phase combinations.
2. FDIAs with several coordinated scenarios.

The aforementioned data sets were used to train the DLNN in detecting, classifying and locating FDI attacks. The approach demonstrated the efficiency of Z-score pre-processing layer, ReLU and softmax activation functions and the adam optimizer in training the network for the research objectives. The network was tested later on using a new data set unseen by the network which resulted in an average overall accuracy of 98.63%.

Moreover, this research also introduces a Long Short Term Memory (LSTM) based approach for predicting the isolated IED readings after the detection of a cyber intrusion. The proposed method was successful in predicting the current waveforms with an average mean square error of 0.14. The average execution time for the proposed algorithm is measured to be 39.8 ms per incidents. In comparison, the typical IED protected medium voltage breaker will require 83.33 ms [104] to clear the fault. Therefore, the proposed approach can easily diagnose the case and provide the needed analysis prior to the protection action time.

The contributions of this work can be summarized as follows:

1. Proposing a new distributed DLNN based method to detect, classify and locate coordinated FDIAs.
2. Introducing an LSTM based approach for system recovery after the isolation of an FDIA.

In future work, the proposed methodology can be tested using noisy measurements and on power grids with distributed generation schemes. In addition, the IEEE 13 bus system can be further modified to include distributed generation. And finally, an optimization of execution time can be further investigated while using the forward-backward method in load flow analysis.

REFERENCES

- [1] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, “A survey on intrusion detection and Recovery systems in digital substations,” *Comput. Networks*, vol. 184, no. September 2020, p. 107679, 2021, doi: 10.1016/j.comnet.2020.107679.
- [2] C. C. Sun, A. Hahn, and C. C. Liu, “Cyber security of a power grid: State-of-the-art,” *International Journal of Electrical Power and Energy Systems*, vol. 99, Elsevier Ltd, pp. 45–56, Jul. 01, 2018, doi: 10.1016/j.ijepes.2017.12.020.
- [3] A. Elgargouri, R. Virrankoski, and M. Elmusrati, “IEC 61850 based smart grid security,” *Proc. IEEE Int. Conf. Ind. Technol.*, vol. 2015-June, no. June, pp. 2461–2465, Jun. 2015, doi: 10.1109/ICIT.2015.7125460.
- [4] M. Girdhar, J. Hong, R. Karnati, S. Lee, and S. Choi, “Cybersecurity of process bus network in digital substations,” *2021 Int. Conf. Electron. Information, Commun. ICEIC 2021*, Jan. 2021, doi: 10.1109/ICEIC51217.2021.9369743.
- [5] W. S. Hokama and J. S. De Souza, “Cybersecurity for smart substation,” *2020 IEEE PES Transm. Distrib. Conf. Exhib. - Lat. Am. T D LA 2020*, Sep. 2020, doi: 10.1109/TDLA47668.2020.9326174.
- [6] D. T. Dantas, H. Li, T. Charton, L. Chen, and R. Zhang, “Machine learning based anomaly-based intrusion detection system in a full digital substation,” *IET Conf. Publ.*, vol. 2020, no. CP771, 2020, doi: 10.1049/CP.2020.0049.
- [7] J. Noce, Y. Lopes, N. C. Fernandes, C. V. N. Albuquerque, and D. C. Muchaluat-Saade, “Identifying vulnerabilities in smart gric communication networks of electrical substations using GEESE 2.0,” *IEEE Int. Symp. Ind. Electron.*, pp. 111–116, Aug. 2017, doi: 10.1109/ISIE.2017.8001232.
- [8] S. Sengan, S. V, I. V, P. Velayutham, and L. Ravi, “Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning,” *Comput. Electr. Eng.*, vol. 93, p. 107211, Jul. 2021, doi:

10.1016/j.compeleceng.2021.107211.

- [9] M. Amin, F. F. M. El-Sousy, G. A. A. Aziz, K. Gaber, and O. A. Mohammed, “CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review,” *IEEE Access*, vol. 9, pp. 38571–38601, 2021, doi: 10.1109/ACCESS.2021.3063229.
- [10] Q. Liu, V. Hagenmeyer, and H. B. Keller, “A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids,” *IEEE Access*, vol. 9, pp. 57542–57564, 2021, doi: 10.1109/ACCESS.2021.3071263.
- [11] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, “On Feasibility and Limitations of Detecting False Data Injection Attacks on Power Grid State Estimation Using D-FACTS Devices,” *IEEE Trans. Ind. Informatics*, vol. 16, no. 2, pp. 854–864, Feb. 2020, doi: 10.1109/TII.2019.2922215.
- [12] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Comput. Networks*, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
- [13] X. Y. Li, R. Tang, and W. Song, “Intrusion Detection System Using Improved Convolution Neural Network,” *Proc. - 2022 11th Int. Conf. Inf. Commun. Technol. ICTech 2022*, pp. 97–100, 2022, doi: 10.1109/ICTECH55460.2022.00028.
- [14] A. Khan, M. B. Shadmand, and S. K. Mazumder, “Intrusion Detection System for Multilayer-Controlled Power Electronics-Dominated Grid,” *IEEE Access*, vol. 10, pp. 98329–98347, Sep. 2022, doi: 10.1109/ACCESS.2022.3206025.
- [15] J. R. F. Martínez and M. C. Fernández, “Cyber security intrusion detection for electrical stations in power networks,” pp. 11–14, Jul. 2022, doi: 10.1049/ICP.2022.0651.
- [16] Y. Sun, L. Hou, Z. Lv, and D. Peng, “Informer-based Intrusion Detection Method for Network Attack of Integrated Energy System,” *IEEE J. Radio Freq. Identif.*, 2022, doi: 10.1109/JRFID.2022.3215599.

- [17] S. B. Rakas, V. Timcenko, M. Kabovic, and A. Kabovic, "Intrusion Detection Systems in Smart Grid," *2022 21st Int. Symp. INFOTEH-JAHORINA, INFOTEH 2022 - Proc.*, 2022, doi: 10.1109/INFOTEH53737.2022.9751302.
- [18] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, and R. Kinta, "Review of Recent Intrusion Detection Systems and Intrusion Recovery Systems in IoT Networks," *2022 Int. Conf. Software, Telecommun. Comput. Networks*, pp. 1–6, Sep. 2022, doi: 10.23919/SOFTCOM55329.2022.9911401.
- [19] D. Das Roy and D. Shin, "Network Intrusion Detection in Smart Grids for Imbalanced Attack Types Using Machine Learning Models," *ICTC 2019 - 10th Int. Conf. ICT Converg. ICT Converg. Lead. Auton. Futur.*, pp. 576–581, 2019, doi: 10.1109/ICTC46691.2019.8939744.
- [20] R. Zhu, C. C. Liu, J. Hong, and J. Wang, "Intrusion Detection against MMS-Based Measurement Attacks at Digital Substations," *IEEE Access*, vol. 9, pp. 1240–1249, 2021, doi: 10.1109/ACCESS.2020.3047341.
- [21] M. Sathya Narayana, R. Gelli, and G. Manimaran, "Distributed Intrusion Detection System using Semantic-based Rules for SCADA in Smart Grid," 2020, doi: 10.1109/TD39804.2020.9299960.
- [22] P. Nancy, S. Muthurajkumar, S. Ganapathy, S. V. N. Santhosh Kumar, M. Selvi, and K. Arputharaj, "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks; Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks," 2020, doi: 10.1049/iet-com.2019.0172.
- [23] L. E. da Silva and D. V. Coury, "A new methodology for real-time detection of attacks in IEC 61850-based systems," *Electr. Power Syst. Res.*, vol. 143, pp. 825–833, Feb. 2017, doi: 10.1016/J.EPSR.2016.08.022.
- [24] J. Yang, L. Zhou, L. Wang, S. Li, Z. Lin, and Z. Gu, "A Multi-step Attack Detection Framework for the Power System Network," pp. 1–8, Sep. 2022, doi: 10.1109/DSC55868.2022.00008.

- [25] A. C. Siregar and B. Ceasar Octariadi, "Feature Selection for Sambas Traditional Fabric 'Kain Lunggi' Using Correlation-Based Featured Selection (CFS)," *Proc. 2019 Int. Conf. Data Softw. Eng. ICoDSE 2019*, Nov. 2019, doi: 10.1109/ICODSE48700.2019.9092731.
- [26] P. Wang, Y. Zhang, and W. Jiang, "Application of K-Nearest Neighbor (KNN) Algorithm for Human Action Recognition," *IMCEC 2021 - IEEE 4th Adv. Inf. Manag. Commun. Electron. Autom. Control Conf.*, pp. 492–496, Jun. 2021, doi: 10.1109/IMCEC51613.2021.9482165.
- [27] A. Gumaï *et al.*, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," *Appl. Soft Comput.*, vol. 96, p. 106658, Nov. 2020, doi: 10.1016/J.ASOC.2020.106658.
- [28] C. Song, Y. Sun, G. Han, and J. J. P. C. Rodrigues, "Intrusion detection based on hybrid classifiers for smart grid," *Comput. Electr. Eng.*, vol. 93, p. 107212, Jul. 2021, doi: 10.1016/J.COMPELECENG.2021.107212.
- [29] I. L. Cherif and A. Kortebi, "On using eXtreme Gradient Boosting (XGBoost) Machine Learning algorithm for Home Network Traffic Classification," *IFIP Wirel. Days*, vol. 2019-April, Apr. 2019, doi: 10.1109/WD.2019.8734193.
- [30] A. Tongta and K. Chooruang, "Long Short-Term Memory (LSTM) Neural Networks Applied to Energy Disaggregation," *2020 8th Int. Electr. Eng. Congr. iEECON 2020*, Mar. 2020, doi: 10.1109/IEECON48109.2020.229559.
- [31] N. Kurniawati, D. N. N. Putri, and Y. K. Ningsih, "Random Forest Regression for Predicting Metamaterial Antenna Parameters," *Proceeding - 2020 2nd Int. Conf. Ind. Electr. Electron. ICIEE 2020*, pp. 174–178, Oct. 2020, doi: 10.1109/ICIEE49813.2020.9276899.
- [32] C. Hu, J. Yan, and X. Liu, "Adaptive feature boosting of multi-sourced deep autoencoders for smart grid intrusion detection," *IEEE Power Energy Soc. Gen. Meet.*, vol. 2020-Augus, 2020, doi: 10.1109/PESGM41954.2020.9281934.

- [33] J. C. Bedoya, C. C. Liu, and J. Xie, “Adaptive Neuro Fuzzy Inference System for Cyber-Intrusion Detection in a Smart Grid,” *2019 20th Int. Conf. Intell. Syst. Appl. to Power Syst. ISAP 2019*, 2019, doi: 10.1109/ISAP48318.2019.9065956.
- [34] T. Lyu, J. O. Blech, and V. Vyatkin, “SMT-based deployment calculation for IEC 61499 control applications,” *Proc. - 2021 4th IEEE Int. Conf. Ind. Cyber-Physical Syst. ICPS 2021*, pp. 172–178, May 2021, doi: 10.1109/ICPS49255.2021.9468194.
- [35] M. A. Majeed, N. K. Singh, L. Tak, and V. Mahajan, “Detection of stealthy cyber intrusion in smart electric grid using advanced state estimation,” *Proc. Conflu. 2021 11th Int. Conf. Cloud Comput. Data Sci. Eng.*, pp. 660–665, 2021, doi: 10.1109/Confluence51648.2021.9377067.
- [36] L. Mohan, J. Pant, P. Suyal, and A. Kumar, “Support Vector Machine Accuracy Improvement with Classification,” *Proc. - 2020 12th Int. Conf. Comput. Intell. Commun. Networks, CICN 2020*, pp. 477–481, Sep. 2020, doi: 10.1109/CICN49253.2020.9242572.
- [37] Z. Wang, W. Cheng, and C. Li, “DoS attack detection model of smart grid based on machine learning method,” *Proc. 2020 IEEE Int. Conf. Power, Intell. Comput. Syst. ICPICS 2020*, pp. 735–738, 2020, doi: 10.1109/ICPICS50287.2020.9202401.
- [38] S. M. Taghavinejad, M. Taghavinejad, L. Shahmiri, M. Zavvar, and M. H. Zavvar, “Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree,” *2020 6th Int. Conf. Web Res. ICWR 2020*, pp. 152–156, 2020, doi: 10.1109/ICWR49608.2020.9122320.
- [39] Y. Zhang and J. Yan, “Semi-Supervised Domain-Adversarial Training for Intrusion Detection against False Data Injection in the Smart Grid,” *Proc. Int. Jt. Conf. Neural Networks*, 2020, doi: 10.1109/IJCNN48605.2020.9207525.
- [40] F. L. Y. Ganin, E. Ustinova, H. Ajakan, P. Germain, H. Larochelle and V. L. M. Marchand, “Domain-adversarial training of neural networks,” *J. Mach. Learn. Res.*, vol. 17, pp. 2096–2030, 2016.

- [41] A. Chavez *et al.*, “Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems,” *2019 IEEE CyberPELS, CyberPELS 2019*, 2019, doi: 10.1109/CyberPELS.2019.8925064.
- [42] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, “An Intrusion Detection Method for Line Current Differential Relays,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 329–344, 2020, doi: 10.1109/TIFS.2019.2916331.
- [43] “IEEE 39-Bus System.” <https://electricgrids.engr.tamu.edu/electric-grid-test-cases/ieee-39-bus-system/> (accessed May 07, 2021).
- [44] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi, and J. Yan, “Detection and Mitigation of Cyber Attacks on Voltage Stability Monitoring of Smart Grids,” *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5227–5238, 2020, doi: 10.1109/TSG.2020.3004303.
- [45] N. Kumar Singh and V. Mahajan, “Cyber Attack Detection in Smart Grid Substation Using Virtual Range Increment and Trust Weight,” *2019 8th Int. Conf. Power Syst. Transit. Towar. Sustain. Smart Flex. Grids, ICPS 2019*, 2019, doi: 10.1109/ICPS48983.2019.9067396.
- [46] R. A. Niazi and Y. Faheem, “A Bayesian Game-Theoretic Intrusion Detection System for Hypervisor-Based Software Defined Networks in Smart Grids,” *IEEE Access*, vol. 7, pp. 88656–88672, 2019, doi: 10.1109/ACCESS.2019.2924968.
- [47] J. Hong and C. C. Liu, “Intelligent Electronic Devices with Collaborative Intrusion Detection Systems,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, 2019, doi: 10.1109/TSG.2017.2737826.
- [48] C. Yang, J. Zhang, K. Li, J. Zhang, N. Jin, and X. Wang, “CP Fusion based Abnormal Traffic Dedection for Process Layer Network in Digital Substation,” *iSPEC 2019 - 2019 IEEE Sustain. Power Energy Conf. Grid Mod. Energy Revolution, Proc.*, pp. 1801–1806, Nov. 2019, doi: 10.1109/ISPEC48194.2019.8975306.

- [49] Y. J. Kwon, H. K. Kim, Y. H. Lim, and J. I. Lim, "A behavior-based intrusion detection technique for smart grid infrastructure," *2015 IEEE Eindhoven PowerTech, PowerTech 2015*, 2015, doi: 10.1109/PTC.2015.7232339.
- [50] J. Sakhnini, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "Physical layer attack identification and localization in cyber-physical grid: An ensemble deep learning based approach," *Phys. Commun.*, vol. 47, p. 101394, Aug. 2021, doi: 10.1016/j.phycom.2021.101394.
- [51] K. Zhou, Y. Yang, Y. Qiao, and T. Xiang, "Domain Adaptive Ensemble Learning," *IEEE Trans. Image Process.*, vol. 30, pp. 8008–8018, 2021, doi: 10.1109/TIP.2021.3112012.
- [52] J. Shi, S. Liu, B. Chen, and L. Yu, "Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 68, no. 3, pp. 993–997, 2021, doi: 10.1109/TCSII.2020.3020139.
- [53] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019, doi: 10.1109/TSG.2018.2817387.
- [54] F. Wei, Z. Wan, and H. He, "Cyber-Attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2476–2486, May 2020, doi: 10.1109/TSG.2019.2956161.
- [55] M. Wang *et al.*, "A low-rank framework of PMU data recovery and event identification," *2019 Int. Conf. Smart Grid Synchronized Meas. Anal. SGSMA 2019*, May 2019, doi: 10.1109/SGSMA.2019.8784541.
- [56] Z. S. Khalafi, M. Dehghani, A. Khalili, A. Sami, N. Vafamand, and T. Dragicevic, "Intrusion Detection, Measurement Correction, and Attack Localization of PMU Networks," *IEEE Trans. Ind. Electron.*, vol. 69, no. 5, pp. 4697–4706, May 2022, doi: 10.1109/TIE.2021.3080212.

- [57] D. L. Van Bossuyt and B. M. O'Halloran, "A Method to Choose Between Automation and Human Operators for Recovery Actions During a Cyber Attack," *Procedia Comput. Sci.*, vol. 153, pp. 352–360, Jan. 2019, doi: 10.1016/J.PROCS.2019.05.089.
- [58] R. Zhu, J. Hong, C. C. Liu, and J. Wang, "Cyber system recovery for IEC 61850 substations," *2021 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2021*, Feb. 2021, doi: 10.1109/ISGT49243.2021.9372195.
- [59] S. N. Edib, Y. Lin, V. Vokkarane, F. Qiu, R. Yao, and D. Zhao, "PMU and communication infrastructure restoration for post-attack observability recovery of power grids," *2020 IEEE Int. Conf. Commun. Control. Comput. Technol. Smart Grids, SmartGridComm 2020*, Nov. 2020, doi: 10.1109/SMARTGRIDCOMM47815.2020.9303014.
- [60] S. N. Edib, Y. Lin, V. M. Vokkarane, F. Qiu, R. Yao, and D. Zhao, "Optimal PMU Restoration for Power System Observability Recovery after Massive Attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1565–1576, Mar. 2021, doi: 10.1109/TSG.2020.3028761.
- [61] S. Al-Rubaye, J. Rodriguez, A. Al-Dulaimi, S. Mumtaz, and J. J. P. C. Rodrigues, "Enabling digital grid for industrial revolution: Self-healing cyber resilient platform," *IEEE Netw.*, vol. 33, no. 5, pp. 219–225, Sep. 2019, doi: 10.1109/MNET.2019.1800312.
- [62] Y. Zhang, L. Wu, Z. Chen, Y. Huang, and Z. Zheng, "Sequential node/link recovery strategy of power grids based on Q-learning approach," *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2019-May, 2019, doi: 10.1109/ISCAS.2019.8702107.
- [63] H. Lin *et al.*, "Self-healing attack-resilient PMU network for power system operation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1551–1565, May 2018, doi: 10.1109/TSG.2016.2593021.
- [64] R. Ma, S. Basumallik, S. Eftekharijrad, and F. Kong, "Recovery-based model predictive control for cascade mitigation under cyber-physical attacks," *2020 IEEE*

- Texas Power Energy Conf. TPEC 2020*, Feb. 2020, doi: 10.1109/TPEC48276.2020.9042584.
- [65] S. Soltan, M. Yannakakis, and G. Zussman, “Power Grid State Estimation Following a Joint Cyber and Physical Attack,” *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 499–512, Mar. 2018, doi: 10.1109/TCNS.2016.2620807.
 - [66] IEEE Distribution Planning Working Group Report, “Radial Distribution Test Feeders,” *IEEE Trans. Power Syst.*, vol. 6, no. 3, pp. 975–985, 1991.
 - [67] *IEEE Recommended Practice for Conducting Load-Flow Studies and Analysis of Industrial and Commercial Power Systems - IEEE Standard*. IEEE, 2018.
 - [68] A. Aljohani and I. Habiballah, “High-Impedance Fault Diagnosis: A Review,” *Energies 2020, Vol. 13, Page 6447*, vol. 13, no. 23, p. 6447, Dec. 2020, doi: 10.3390/EN13236447.
 - [69] A. Aljohani, T. Sheikhoon, A. Fataa, M. Shafiullah, and M. A. Abido, “Design and Implementation of an Intelligent Single Line to Ground Fault Locator for Distribution Feeders,” in *2019 International Conference on Control, Automation and Diagnosis (ICCAD)*, Mar. 2020, pp. 1–6, doi: 10.1109/iccad46983.2019.9037950.
 - [70] A. Aljohani, A. Aljurbua, M. Shafiullah, and M. A. Abido, “Smart fault detection and classification for distribution grid hybridizing ST and MLP-NN,” *2018 15th Int. Multi-Conference Syst. Signals Devices, SSD 2018*, pp. 94–98, 2018, doi: 10.1109/SSD.2018.8570582.
 - [71] A. Aljohani, “Centralized Fault Detection and Classification for Motor Power Distribution Centers Utilizing MLP-NN and Stockwell Transform,” in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, Oct. 2020, pp. 222–226, doi: 10.1109/ISGT-Europe47291.2020.9248886.
 - [72] H. W. Dommel and W. F. Tinney, “Optimal Power Flow Solutions,” *IEEE Trans. Power Appar. Syst.*, vol. PAS-87, no. 10, pp. 1866–1876, 1968, doi:

10.1109/TPAS.1968.292150.

- [73] J. C. Chen, B. T. Phung, H. W. Wu, D. M. Zhang, and T. Blackburn, "Detection of high impedance faults using wavelet transform," Nov. 2014, doi: 10.1109/AUPEC.2014.6966629.
- [74] J. Vico, M. Adamiak, C. Wester, and A. Kulshrestha, "High impedance fault detection on rural electric distribution systems," 2010, doi: 10.1109/REPCON.2010.5476205.
- [75] M. Sarlak and S. M. Shahrtash, "High-impedance faulted branch identification using magnetic-field signature analysis," *IEEE Trans. Power Deliv.*, vol. 28, no. 1, pp. 67–74, 2013, doi: 10.1109/TPWRD.2012.2222056.
- [76] T. A. Kawady, A. E. M. I. Taalab, and M. Z. Elgeziry, "Experimental investigation of high impedance faults in low voltage distribution networks," 2009, doi: 10.1109/PES.2009.5275248.
- [77] V. Torres G. and H. F. Ruiz P., "High impedance fault detection using discrete wavelet transform," in *Proceedings - 2011 IEEE Electronics, Robotics and Automotive Mechanics Conference, CERMA 2011*, 2011, pp. 325–329, doi: 10.1109/CERMA.2011.60.
- [78] S. M. Shahrtash and M. Sarlak, "High impedance fault detection using harmonics energy decision tree algorithm," 2006, doi: 10.1109/ICPST.2006.321441.
- [79] Y. Sheng and S. M. Rovnyak, "Decision tree-based methodology for high impedance fault detection," *IEEE Trans. Power Deliv.*, vol. 19, no. 2, pp. 533–536, Apr. 2004, doi: 10.1109/TPWRD.2003.820418.
- [80] C. D. Prasad, N. Srinivasu, D. J. V. Prasad, and M. Saiveerraju, "Reliability of different fault detection algorithms under high impedance faults," Oct. 2014, doi: 10.1109/ICACCS.2013.6938708.
- [81] A. Siadatan, H. Kazemi Karegar, and V. Najmi, "New high impedance fault detection," in *PECon2010 - 2010 IEEE International Conference on Power and*

Energy, 2010, pp. 573–576, doi: 10.1109/PECON.2010.5697647.

- [82] T. M. Lai, L. A. Snider, E. Lo, and D. Sutanto, “High-impedance fault detection using discrete wavelet transform and frequency range and RMS conversion,” *IEEE Trans. Power Deliv.*, vol. 20, no. 1, pp. 397–407, 2005, doi: 10.1109/TPWRD.2004.837836.
- [83] A. Thakallapelli, R. Mehra, and H. A. Mangalvedekar, “Differentiation of faults from power swings and detection of high impedance faults by distance relays,” in *2013 IEEE 1st International Conference on Condition Assessment Techniques in Electrical Systems, IEEE CATCON 2013 - Proceedings*, 2013, pp. 374–377, doi: 10.1109/CATCON.2013.6737530.
- [84] M. Michalik, W. Rebizant, M. R. Lukowicz, S. J. Lee, and S. H. Kang, “High-impedance fault detection in distribution networks with use of wavelet-based algorithm,” *IEEE Trans. Power Deliv.*, vol. 21, no. 4, pp. 1793–1802, Oct. 2006, doi: 10.1109/TPWRD.2006.874581.
- [85] A. N. Milioudis, G. T. Andreou, and D. P. Labridis, “Detection and location of high impedance faults in multiconductor overhead distribution lines using power line communication devices,” *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 894–902, Mar. 2015, doi: 10.1109/TSG.2014.2365855.
- [86] M. S. Ali, A. H. Abu Bakar, H. Mokhlis, H. Aroff, H. A. Illias, and M. M. Aman, “High impedance fault localization in a distribution network using the discrete wavelet transform,” in *2012 IEEE International Power Engineering and Optimization Conference, PEOCO 2012 - Conference Proceedings*, 2012, pp. 349–354, doi: 10.1109/PEOCO.2012.6230888.
- [87] I. Baqui, I. Zamora, J. Mazón, and G. Buigues, “High impedance fault detection methodology using wavelet transform and artificial neural networks,” *Electr. Power Syst. Res.*, vol. 81, no. 7, pp. 1325–1333, Jul. 2011, doi: 10.1016/j.epsr.2011.01.022.
- [88] A. H. A. Bakar, M. S. Ali, C. Tan, H. Mokhlis, H. Arof, and H. A. Illias, “High impedance fault location in 11 kV underground distribution systems using wavelet

- transforms,” *Int. J. Electr. Power Energy Syst.*, vol. 55, pp. 723–730, Feb. 2014, doi: 10.1016/j.ijepes.2013.10.003.
- [89] A. Mahari and H. Seyedi, “High impedance fault protection in transmission lines using a WPT-based algorithm,” *Int. J. Electr. Power Energy Syst.*, vol. 67, pp. 537–545, May 2015, doi: 10.1016/j.ijepes.2014.12.022.
- [90] G. H. Gabriels, D. T. O. Oyedokun, and S. Ruggeri, “Realtime thévenin equivalent impedance at a PCC in the Italian power grid,” *2020 Int. SAUPEC/RobMech/PRASA Conf. SAUPEC/RobMech/PRASA 2020*, Jan. 2020, doi: 10.1109/SAUPEC/ROBMECH/PRASA48453.2020.9040924.
- [91] J. L. Blackburn and T. J. Domin, “Protective Relaying : Principles and Applications, Third Edition,” *Prot. Relaying*, Dec. 2006, doi: 10.1201/9781420017847.
- [92] K. Gurney, *AN INTRODUCTION TO NEURAL NETWORKS*. 1997.
- [93] M. Nielsen, *Neural Networks and Deep Learning*. 2018.
- [94] G. I. Belfast, K. W. Reading, and K. H. Berlin, Eds., *Neural Network Applications in Control*. London: Institution of Electrical Engineers, 1995.
- [95] S. Haykin, *Neural Networks and Learning Machines*, Third., vol. 127. Hamilton, Ontario, Canada: Perason, 2009.
- [96] P. S. Churchland and T. J. Sejnowski, *The Computational Brain* . 1992.
- [97] X. Glorot, A. Bordes, and Y. Bengio, “Deep Sparse Rectifier Neural Networks,” 2011.
- [98] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2016-December, pp. 770–778, Dec. 2016, doi: 10.1109/CVPR.2016.90.
- [99] C. Yang, S. K. Oh, W. Pedrycz, Z. Fu, and B. Yang, “Design of Reinforced Fuzzy Radial Basis Function Neural Network Classifier Driven with the Aid of Iterative Learning Techniques and Support Vector-Based Clustering,” *IEEE Trans. Fuzzy*

Syst., vol. 29, no. 9, pp. 2506–2520, Sep. 2021, doi: 10.1109/TFUZZ.2020.3001740.

- [100] Z. Zhang, “Improved Adam Optimizer for Deep Neural Networks,” *2018 IEEE/ACM 26th Int. Symp. Qual. Serv. IWQoS 2018*, Jan. 2019, doi: 10.1109/IWQOS.2018.8624183.
- [101] H. R. Wilson and J. D. Cowan, “Excitatory and Inhibitory Interactions in Localized Populations of Model Neurons,” *Biophys. J.*, vol. 12, no. 1, pp. 1–24, Jan. 1972, doi: 10.1016/S0006-3495(72)86068-5.
- [102] P. Dayan and L. F. Abbott, *Theoretical Neuroscience: Computational and Mathematical Modeling of Neural ... - Peter Dayan, L. F. Abbott - Google Books*. 2001.
- [103] Z. El Mrabet, H. El Ghazi, and N. Kaabouch, “A performance comparison of data mining algorithms based intrusion detection system for smart grid,” *IEEE Int. Conf. Electro Inf. Technol.*, vol. 2019-May, pp. 298–303, 2019, doi: 10.1109/EIT.2019.8834255.
- [104] NFPA, *NFPA 70e*. 2019.

Vitae

Name : Abdulaziz K. Aljohani

Nationality : Saudi

Date of Birth : 23/05/1994

Email : abdulazizkaljohani@gmail.com

Address : 8140 Al Maliki - Al Jisr Dist. AL KHOBAR 34714, KSA

Academic Background : Abdulaziz Aljohani received his M.S and B.S degrees in Electrical Engineering from King Fahd University of Petroleum and Minerals (KFUPM) 2023 and 2018 respectively. Abdulaziz is a lead electrical projects engineer working with Saudi Aramco on the development of South Ghawar Unconventional Field. His research interests include Security and Resiliency of Smart Grids, cyber-physical systems and fault diagnosis.