

Fault Localization Using Neural Networks For Fault Management Based on Alarm Correlation Analysis: The Case of Ethio telecom

BY: Tsion Ketema

ADVISOR: Ephrem Teshale(PhD)

A Thesis submitted to
School of Electrical and Computer Engineering
Addis Ababa Institute of Technology
Addis Ababa University

In partial fulfillment of the requirements for the degree of Master of Science in
Telecommunications Engineering.



Addis Ababa University

Addis Ababa, Ethiopia

November 10, 2021

Declaration

I, the undersigned, declare that the thesis comprises my own work in compliance with internationally accepted practices; I have fully acknowledged and referred all materials used in this thesis work.

Tsion Ketema

Name

Signature



Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

This is to certify that the thesis prepared by **Tsion Ketema**, entitled *Fault localization using neural networks for fault management based on alarm correlation analysis: The Case of Ethio telecom* and submitted in partial fulfillment of the requirements for the degree of Master of Science Telecommunication Engineering complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the Examining Committee:

Internal Examiner(1) Dereje Hailemariam (PhD) Signature _____ Date _____

Internal Examiner(2) Murad Ridwan (PhD) Signature _____ Date _____

Adviser Ephrem Teshale (PhD) Signature _____ Date _____

Dean, School of Electrical and Computer
Engineering

ABSTRACT

Telecommunication sector has considerably large network infrastructure consisting of different network equipment to provide telecom services to the customers. As a service provider, telecom operators have to make sure that customers are getting services without interruption. To do so, they built network operation center to monitor the network status with the help of a fault management system (FMS). When malfunction or error appears on a piece of network equipment, they typically produce an alarm and transmits to the FMS, which is then shown to the monitoring team for trouble ticket creation.

There is also a chance that failures that happened on one network element can cause other network elements to produce alarms as long as the network equipment's are functionally dependent. Thus, during the trouble ticketing, the operators may need to collect further information such as relationship or dependency between alarms to ultimately distinguish the root source of the alarms. But the information on FMS lacks explanation and indication of the causes, forcing monitoring teams to manually figure out the cause and take action, which results in a poor decision making as well as a longer trouble shooting and service outage time.

This study focuses on studying the association between network equipment alarms using a correlation analysis technique called Pearson correlation using history alarm data and studying the feasibility of using artificial neural network to build fault localization model to support the monitoring team with decision making. Fault localization models using one specific neural network architecture are built in different literatures. But in this study two neural network architectures namely, Feed forward neural network (FFNN) and cascade forward neural network (CFNN), are selected to build a model using the data of correlation analysis output, the microwave link topology and the history alarms as an input. Data preparation techniques such as data engineering and feature engineering have been applied to the collected alarm data from the existing fault management system. After building the models, they are evaluated using commonly used performance metrics such as accuracy and error measurement. Python is used as programming tool to perform the correlation analysis as well as to develop and compare the two neural network models. Experimentation results exhibit that CFNN achieves an accuracy of 97.7% while FFNN achieves 95.9% overall accuracy.

keywords: Alarm correlation analysis, Artificial neural network, Fault management system

ACKNOWLEDGMENTS

Above all, I thank the almighty God for giving me the courage to deal with the difficult situations I have encountered while pursuing my studies, as well as for his guidance and support throughout my whole study period.

I am really grateful to my advisor, Ephrem Teshale (PhD), for accepting me as his advisee and allowing me to work on this research. I would want to express my gratitude for his counsel and support throughout the completion of my thesis.

I am also thankful to my thesis examiners, Dereje Hailemariam (PhD) and Murad Ridwan (PhD), who were present during my two seminar presentations for their invaluable feedback and suggestions that allowed me to improve the content and presentation of my thesis. I also want to thank all of the teachers who have contributed to my education over the course of my master's program. Grateful acknowledgments are extended to Addis Ababa University, Addis Ababa Institute of Technology and Ethio telecom for offering the opportunity to pursue this study.

My thanks also goes to Ethio telecom staffs especially for employees of national network operation center section for their cooperation and excellent facilitation during data collection. My warm thanks are extended to my loving family for their unfailing encouragement and unwavering support in the course of the entire work and also during all the study time. Finally, I extend my gratitude and blessings to all of those who helped me in any way throughout the writing of this thesis.

TABLE OF CONTENTS

Abstract	i
Acknowledgments	ii
Table of Content	v
List of Figure	vi
List of Table	vii
Acronyms	viii
1 Introduction	1
1.1 Statement of the problem	2
1.2 Objectives	4
1.2.1 General Objective	4
1.2.2 Specific Objectives	4
1.3 Scope and Limitations	4
1.4 Motivation and Contributions	5
1.5 Literature Review	6
1.6 Methodology	7
1.7 Thesis Organization	8
2 Cellular Network Fault Management	9
2.1 Overview of Cellular Mobile Network	9
2.2 Base Station Outage	11
2.3 Fault Management System	12
3 Artificial Neural Network	14
3.1 Introduction To Neural Network	14
3.2 Architecture Of Neural Network	14
3.2.1 Feed-Forward Neural Network	15
3.2.2 Cascade-Forward Neural Network	16

3.3	The Learning Process	17
4	Correlation Analysis and Fault Localization	19
4.1	Alarm Correlation Analysis	19
4.2	Correlation Analysis Methodology	20
4.2.1	Data Collection	20
4.2.2	Data Preprocessing	21
4.2.3	Pearson Correlation Analysis	22
4.2.4	Visualization and Reporting	22
4.3	Modeling Fault Localization	23
4.3.1	Preparing The Dataset	24
4.3.2	Developing The Supervised ANN Model	25
4.3.3	Training and Testing of ANN	26
4.3.4	Performance Evaluation Metrics	27
5	Experiment Approach	30
5.1	Correlation Analysis Scenario	30
5.1.1	Dataset for Alarm Correlation Analysis	30
5.1.2	Alarm Correlation Analysis	34
5.2	Fault Localization Using Neural Network	35
5.2.1	Dataset for The Neural Network	35
5.2.2	Building a Neural Network Model	37
6	Results and Discussion	39
6.1	Results of Correlation Analysis	39
6.2	Models Performance Analysis	43
7	Conclusion and Recommendations	44
7.1	Concluision	44
7.2	Recommendations	45
	REFERENCES	46

Appendix 50

LIST OF FIGURES

1.1	Steps followed to Perform the study	8
2.1	2G, 3G and 4G network architecture [14]	9
2.2	Interconnection of equipment's in base station sites [14]	12
3.1	Feed-forward neural network architecture	16
3.2	Cascade-forward neural network architecture	17
4.1	Methodology for correlation analysis	20
4.2	Steps to build neural network model	23
4.3	Multi-Class Classification Confusion Matrix	27
5.1	Extraction of original alarm attributes.	31
5.2	Number of alarms per Addis Ababa zones	36
6.1	Correlation between power and BTS alarm	40
6.2	Correlation between Transmission and BTS alarm	41
6.3	Correlation between IP and BTS alarm	42
6.4	Performance Comparison of FFNN and CFNN Model	43

LIST OF TABLES

4.1	Attributes of alarms with their description	21
5.1	Power equipment alarms and their description	32
5.2	Transmission equipment alarms and their description	33
5.3	IP equipment alarms and their description	33
6.1	Performance Comparison of FFNN and CFNN Model	43

ACRONYMS

AI	Artificial Intelligence
ANN	Artificial Neural Network
BTS	Base Transceiver Station
BSC	Base Station Controller
CFNN	Cascade-forward neural network
DG	Diesel Generator
FMS	Fault Management System
FFNN	Feed-forward neural network
FP	False Positive
FN	False Negative
IMSI	Mobile Subscriber Identification
IP	Internet Protocol
MAE	Mean Absolute Error
MSC	Mobile Switching Center
MSE	Mean Square Error
NN	Neural Network
NOC	National operation center
OMC	Operation and Maintenance Center
SLA	Service Level Agreement
TP	True Positive
TN	True Negative

1 INTRODUCTION

Telecommunication networks are made up of different types of network equipment that are operationally dependent on one another in order to complete a telecom task. With the use of various network equipment, telecom operators provides fixed line and internet-based services to their customers [1],[2]. But sometimes a network equipment fails for a variety of causes, including power outage, transmission equipment problem, and connection failures [3],[4]. The failures could result a service outage or interruption. As a result, network equipment should be monitored and managed 24 hours a day, seven days a week, to discover root causes of outages and take corrective action to avoid customer complaints and revenue loss.

Every piece of network equipment is configured to generate an alarm whenever it encounters a fault [5]. A fault is a problem that happens on the installed network equipment's hardware or software. Service failures, severe network degradation, and unplanned disruptive behavior can all be caused by faults [4],[6],[7]. Network equipment generates alarms to describe the faults as stated by the vendor's operators. Telecom operators use a network management system to perform fault management by monitoring the alarms produced by the network equipment. Alarms are displayed on the fault management platform in order for the network monitoring professionals to see the alarms on the fault management platform.

Currently, Ethio telecom has a network monitoring center called national operation center (NOC) consisting of a dedicated network management experts. The operation center is composed of IP, transmission, mobile, and power teams to follow the status of the network equipment in every base transceiver station(BTS) sites using fault management system (FMS). FMS is the alarm presentation master which sort and display the alarm to the specific monitoring team[2],[8],[9]. Each BTS site has its own specific site ID. Whenever a fault happens on the network equipment of a specific BTS site, an alarm will be generated and displayed on the fault management system along with the site in order to let the monitoring team to manage the faults. Fault management is the main function on network management which focuses on diagnosing and

fixing network fault. Fault diagnosing is a process of detecting faults by studying the status of the network equipment and analyzing the root cause[8],[10],[11]. When alarms appear on the FMS along with the site ID, the monitoring team will manage the alarm based on the alarm type or the network equipment by creating a trouble ticket (TT) and assigning it to the operation and maintenance technicians who have direct responsibility. Then the field technicians or the operation and maintenance team receive the trouble ticket and take actions to fix the fault. But mostly it is difficult to manage faults of the network equipment due to large volume of alarms. Because of the fact that the telecommunication network is composed of large number of network equipment's, the produced alarms are too large in number. There is also a chance that one fault could be a cause for the appearance of dozen of alarms. Failures that happened on one network element can cause other network components to produce relevant alarms as long as the network equipment's are functionally dependent[5],[7]. This fault might affect the network critically unless the operation teams take action in a short period of time. Therefore, for telecom service providers, understanding the relationship of the network equipment alarms during fault management is very important to identify and predict the root cause problems in a short period of time.

1.1 STATEMENT OF THE PROBLEM

In the current Ethio telecom situation, network elements from different BTS sites produce a large volume of alarms per day, and the alarms messages appear uncorrelated from the network element to the FMS. The FMS filter and display the generated alarms to let the monitoring team see the alarms and create a trouble ticket and assign it to the corresponding field technicians. The monitoring teams are grouped or formed to monitor the network equipment based on different types of network components in the BTS site. Due to this, they are responsible to monitor the status of specific network equipment types. But the failure of one network equipment might cause problems for different network equipment and this lets different alarms having the same root cause to be detected at the same time by different teams. On the other hand, some alarms might also remain unseen for a long time because of the appearance of dozens of alarms.

The current FMS that is being used by Ethio telecom is based on manual processing and relies on the monitoring team's knowledge. Due to this many efforts are being made by the monitoring team for debugging a BTS outage, especially in the stage of identifying where and what the source is. Some of the existing approach drawbacks are:

- **Redundant trouble tickets:** The experts are expected to diagnose and manage each alarm on time but the appearance of dozens of alarms per second makes them not to cross check the dependency of the alarms. Due to this they just create a different trouble ticket for alarms with similar root cause;
- **Longer troubleshooting time:** It is beyond human's ability to manually find and analyze the root cause of a large number of alarms in a short period of time;
- **Longer Service outage time:** In fact, a Long duration time for fault troubleshooting increase the service outage time and this affects the quality of the service. It affects the network critically unless the operation teams take action in a short period of time. But if they didn't take an action as soon as possible, the duration of the service outage might increase and this will cause the customers not to be able to use the network and get the services and will make the service provider to lose revenue and cause an economic disaster to the telecom company.

To avoid all the efforts that are being made by the monitoring team during fault management, to identify the initial cause of the fault as well as the location of the initial cause, implementing a fault localization system as a decision support system for the monitoring team is very important. In this way, it will minimize, the overload of the operators, redundant trouble ticket creation, and longer troubleshooting and service outage time.

Performing an alarm correlation analysis is very important to diagnose the relationship between alarms and identify the parent and the child alarm before building the fault localization model. Different fault localization approach has been applied with the hope of improving the fault management process in other studies. Some of the approaches are Rule-based approach, Codebook-based approach, and Case-based approach, but the main issue is their performance and suitability. And this paper proposes a fault localization method based on artificial neural network (ANN). There are different types of ANN architectures to build the model. So the purpose of this research will be to perform alarm correlation analysis and build a fault localization model using selected neural network architectures and compare the performance of the model using Performance Metrics.

1.2 OBJECTIVES

1.2.1 GENERAL OBJECTIVE

The main objective of this research work is to perform correlation analysis, build fault localization model using different architectures of ANN and comparing their performance.

1.2.2 SPECIFIC OBJECTIVES

The specific objectives of this research are:

- To identify network equipment alarms impacting on BTS outage status by discovering the dependencies between alarms;
- To build dataset using suitable data preparation techniques;
- To identify and select an effective neural network algorithms to build fault localization model. Since there are so many algorithms few will be selected for this particular research;
- To build fault localization model using the selected algorithms and compare their performance;
- To finally recommend the most accurate fault localization models based on their performance.

1.3 SCOPE AND LIMITATIONS

The scopes of this thesis are:

- Investigating the association between alarms and identifying the root alarm which demonstrate the initial cause of BTS mobile network outage using Pearson correlation analysis technique;
- Building fault localization model using the two selected neural network architectures, feed forward neural network and cascade forward neural network and compare their performance using performance comparison metrics.

The limitations of this thesis are:

- The alarm data are collected from one vendor network equipment which is Huawei. Because the interconnection between BTS and their probable existence of outage might not be the same with other vendor having different equipment;
- Only specific BTS which are under the same microwave link are considered while building the model to reduce the complexity of the neural network architecture.

1.4 MOTIVATION AND CONTRIBUTIONS

The motivation for this research comes from the fact that the existing fault management system that is being used by Ethio telecom has no automated approach to debug and identify where the faults are. Telecom network equipment produces several number of alarms per day to pass information about malfunction location, type, severity, and other relevant information of the mobile network sites. However, the current FMS is based on manual processing and relies on the monitoring team's knowledge. Due to this many efforts are being made by the monitoring team for debugging a BTS outage, especially in the stage of identifying where and what the source is. In addition to that, too much time is being consumed to find the root cause of the alarms and take fast decisions. Thus, the operator needs a decision support system to simplify the fault localization task. Based on these facts two questions are raised as a baseline for this research. The first one is which alarms are correlated to each other. The second one is the uncertainty to explore if, in fact, certain algorithms perform better for a specific kind of problem, which is fault localization. And the other one is a multi classifier algorithm that can perform well regarding performance comparison matrices. So looking for the answer to these questions is the inspiration to do this research.

This thesis makes a number of contributions to the field of fault management. Some of them are listed as follows:

- Examining the basic alarm characteristics using historical alarms from the existing fault management system. The analysis identifies which alarm types are the root alarm for the BTS outage.

- Further, this thesis presents a neural network solution to identify the reason behind the BTS outage plus the exact location in terms of the network site to minimize the overload of the monitoring time as well as to decrease the BTS outage time by reducing the troubleshooting time and the delay during proper maintenance team assignment.
- The model that is built using the neural network is good for the monitoring team to make decisions while creating a trouble ticket to assign a maintenance team by providing the root causes of alarms and the location of the NE which produced the alarm.

1.5 LITERATURE REVIEW

A network elements that make up the telecom network produces daily a number of alarms. The initial cause of one alarm might cause a problem that leads to an effect of other alarms and without alarm correlation network management is very difficult for network operators to analyze alarms and find the root cause of a network failure in short period of time. Alarm correlation can be done in a variety of ways, including rule-based, codebook-based, and case-based. [7][11]. But these approaches rely on manual processing and depend on the knowledge of the operators.

In the Network Operations and Management Symposium (NOMS), Wietgreffe 1997 presented a study that compares and evaluates numerous alarm correlation algorithms for their suitability and performance in global mobile communications networks (GSM). The cascade forward neural network learning approach is compared to rule-based diagnosis, model-based diagnosis, and alarm correlation employing codebooks. The cascade forward neural network performs best [3]. But the performance of other neural network architecture is not include in this study.

Correlating alarms and determining their source is a difficult task in fault management because a single fault in the mobile network initiate a lot of alarms. A. K. Arhouma et al (2013) proposed an ANN model to analyze the alarms, reduce the operator's reaction time and make the decision-making process easier. The feasibility of using ANN technique to solve the problem of fault management in GSM networks is studied by applying the feed forward neural network (FFNN) architecture. But limitation with this paper is that only FFNN architecture is used to study the feasibility of ANN [12].

Among correlation approaches, Bicharra et al. (2012) proposed a hybrid approach by combining AI and rule-based which identifies the root-cause based on event correlation rules and dependency graph. This approach identifies the root cause using a relationship based on network topology information [9]. This reduced the displayed alarm set on the management console of the network operators as a result network operator take action on the alarms by creating trouble ticket in a relatively short amount of time. But it has a limitation when a new combination of alarms occur due to changing network topology, because the rule-based approach cannot handle new and changing data. Plus it requires an excessive amount of expert knowledge when change occurrence.

Another alarm correlation function was also proposed by A. Mehrabinezhad et al. (2001) in iron for SDH network elements based on a data mining technique called rule association [13]. The association rule states that an alarm which has their properties will probably have other properties with respect to their interaction with other alarms. Rule association based alarm correlation algorithm classifies the alarm by the type of network element based on their occurrence time then a decision tree will be built to find the root cause. The proposed algorithm also uses a case-based reasoning technique by taking the stored knowledge as a case to be retrieved, adapted and utilized. In general to refer the solution in stored knowledge for the new occurring problem. The limitation is that in case-based reasoning it is unable to provide the solution for this problem in a relatively short amount of time, if there is no matching case for the new cases that are not yet known.

1.6 METHODOLOGY

This research mainly focuses on how to simplify the task of monitoring and managing the fault that happened on the network equipment of a cellular network to detect and prevent the service disturbance or service outage on time by using a better alarm correlation analysis and modeling a fault localization using neural networks to figure out the location of root Cause alarms in a short period of time. The work will start by collecting base station alarms from the existing FMS and trying to deeply understand the alarm behavior and identifying the network equipment that are associated with the alarms. The next step is figuring out the association between the alarms and identifying the influential alarm for BTS outage with the help of correlation analysis technique. This is followed by modeling a fault localization using selected artificial neural network architectures and finally comparing the model with the help of performance

comparison metrics. In general, the detailed steps followed to perform this study after a literature review are shown in Figure below:

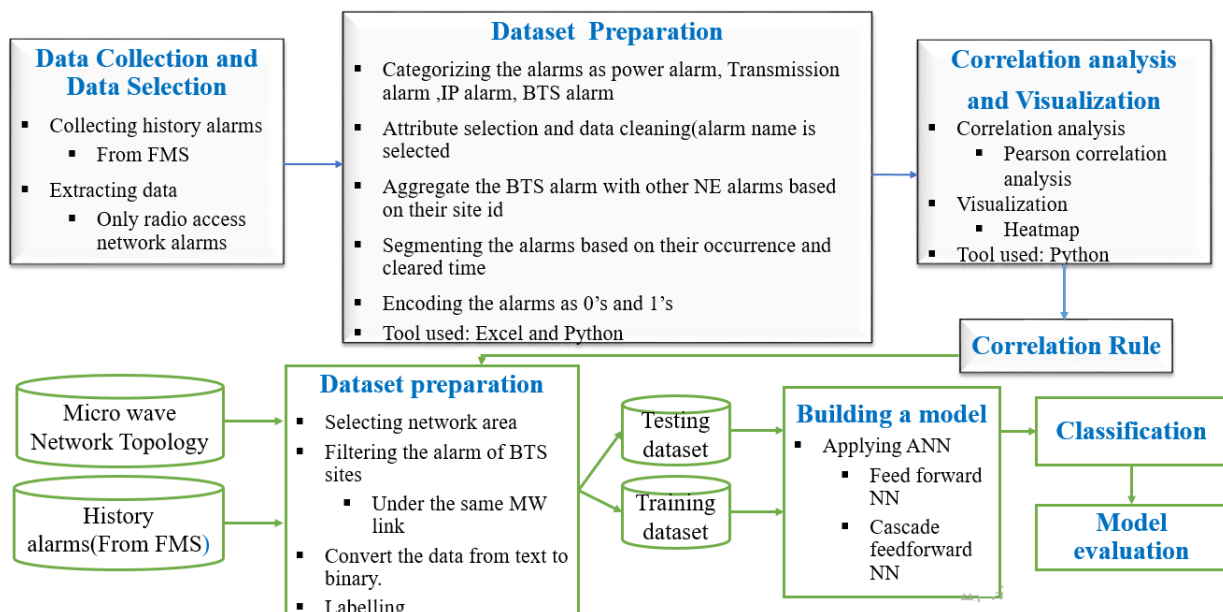


Figure 1.1: Steps followed to Perform the study

1.7 THESIS ORGANIZATION

The remaining part of this paper is organized as follows: Chapter 1 gives a brief introduction to this research giving statement of the problem, thesis objectives, motivation and the main contributions of this work. This is followed by Chapter 2 which consist an overview of cellular mobile network and fault management. Chapter 3 deeply discusses the overview of artificial neural network and working principles of the selected neural network architectures. Chapter 4 covers the various steps that should be carried out to perform correlation analysis and develop a fault localization model using neural networks. It also discusses the performance comparisons metrics that are used in this paper to compare the selected neural network. Chapter 5 explains how data is collected and prepared for the correlation analysis purpose as well as for building a fault localization model in case of ethiotelecom. In Chapter 6 results are shown and discussed in brief and finally, conclusion of the paper is presented in Chapter 7.

2 CELLULAR NETWORK FAULT MANAGEMENT

This section introduces important concepts related to telecommunication cellular networks and fault management.

2.1 OVERVIEW OF CELLULAR MOBILE NETWORK

A cellular network is a mobile network that provides services by using a large number of base stations with limited power, each covering only a limited area [4],[10]. Cellular networks are complex systems offering a wide range of services but for a subscriber a mobile telephone communication is a simple process. In reality though, the call is only possible because of a complex network architecture that comprises of several network elements. The mobile communication network is composed of several functional entities. As shown in Figure 2.1 The network can be divided into mobile station, access network and core network [10],[12].

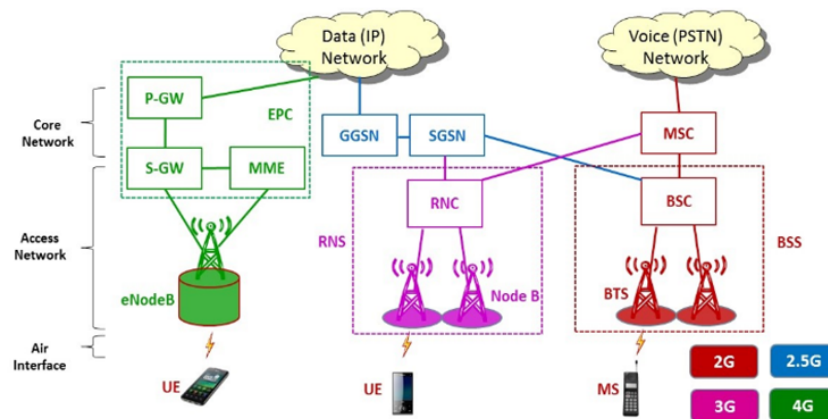


Figure 2.1: 2G, 3G and 4G network architecture [14]

MOBILE STATION

For one person to communicate to another person through a telecommunication network, the very first entity required is a mobile station. The mobile station is also called a cell phone, smart-phone, or terminal. This mobile station has a speaker or microphone, code for digitizing speech, modem for moving one's and zero's around, an antenna and a battery a screen, and a keypad [15] . Another component of a mobile station is a SIM card to store some critical information like international mobile subscriber identification (IMSI).IMSI identifies the mobile subscriber to the network [10],[15]. The SIM card also stores the Location Area identifier. This is a piece of information that the phone learns from the network and identifies which base station the phone or the mobile station has last talked to.

ACCESS NETWORK

The access network is the second component that is required. The access network controls the radio link with the Mobile Station .This access network is made up of BSS (Base station subsystem) and a network subsystem (NSS), which will be managed by NMS or Operations support systems (OSS).

BSS provide a connection between the mobile stations in NSS. NSS forward user signals to other mobile station via BSS and provide the necessary customer data.BSS insures as complete network coverage as possible and includes a large number of structurally organized radio cells.it consists of BTS,BSC and transceiver controller(TC) [4][12][16].

THE CORE NETWORK

Mobile Switching Center (MSC) is the control center for the cellular network, which coordinates the actions of the BSC, provides general control, and acts as a switch and connection to the public telephone network[15],[17]. As a result, it will have a variety of communication links, such as fiber optic links, microwave links, and copper wire cables. These allow it to communicate with the BSC, allowing it to route and control calls as necessary.

2.2 BASE STATION OUTAGE

When there is a mobile network outage, the mobile network operators customers will be unable to use the data, voice and any means of communication functions through mobile. Mobile network outages occur due to various reasons. The main reasons for the outage is due to Base station(BS) faults . A BS is a system in a mobile communication network that houses radio receivers and is used for wireless communication between users and network providers that is under the control of Base Station Controller (BSC) or radio network controller (RNC) and then the exchange. BS is mainly composed of base Transceiver Station (BTS), antennas and physical support for antennas. BTS is the radio and it produces energy in the form of electricity. The electricity is carried up to the second component of the base station which is the antennas, over thick coaxial cables. The antenna is the device that converts the electricity to electromagnetic waves [4],[16].

To make communicate between two or more persons through a telecommunication network, mobile switch makes a connection to the base station. The base station has to be connected back to mobile switch. The mobile switch is capable of keeping truck of users moving around. The connection between base station and mobile switch is called backhaul. If there is a fiber between those two physical locations, they use fiber to connect the BS back to the mobile switch. But if there is no fiber available, point to point radio backhaul will be used. We might have the communications, the backhaul from the BS back to the mobile switch go through multiple different tours with point to point radio systems before we finally get back to a mobile switch[4],[16].

Base station sites are composed of different hardware elements: modems, switching units, cables, cooling elements, energy elements, etc. This elements are interconnected as a result a failure in one element will probably affect a smooth running of the hardware or make it break down. For a example, the failure of the air conditioning system will affect all the hardware installed in the room. The physical interconnection of elements of the mobile base stations shown in the Figure below. In this study the cause for BS outage is generalized as ip equipment failure,power failure,transmission equipment failure.

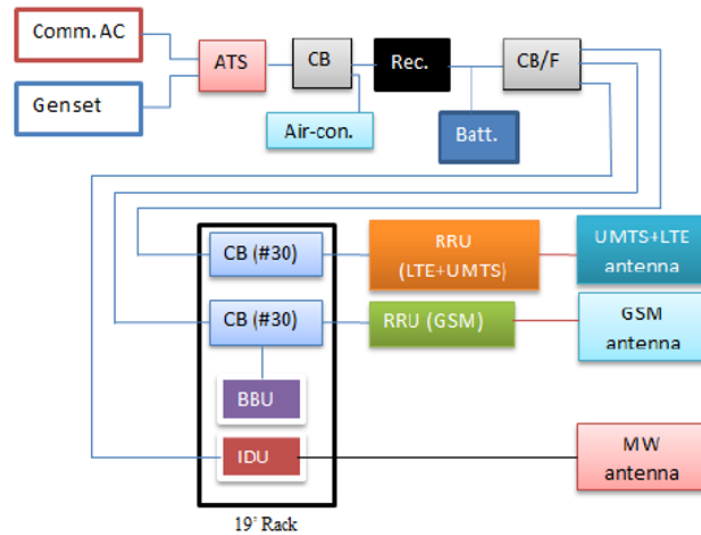


Figure 2.2: Interconnection of equipment's in base station sites [14]

2.3 FAULT MANAGEMENT SYSTEM

A telecommunication network consists of a number of interconnected components like switch, transmission equipment, routers and RNC .These components can produce network alarms to demonstrate sort of abnormal situation [3],[8],[12]. These alarms further help to monitor the status and stability of the network element and the services carried over it using fault management system. Fault management is one part of network management to collect and analyze alarms. The network management is the collection of tasks performed to maximize availability, performance, security and control of a network and its resources[7],[18].fault management mainly deals with remotely controlling or Monitoring the status of network devices to avoid a potential faults.

Fault management systems use network alarms to determine the nature and severity of the faults and to drive the fault resolution. A fault is a malfunction that occurs on a network and may cause errors. A fault can have various consequences such as making a network service unavailable or degrading its performance [7],[8],[19],[12]. These network faults are represented by alarms and the number of produced alarms varies greatly. From a logical point of view fault management system collects network events and filters events which are alarms and group alarms by common fault cause and lastly prioritize the fault resolution [1],[12],[20].

During network fault management, the monitoring team maintain and examine error logs , accept and act upon error detection notifications, trace and identify faults, Carry out sequences of diagnostic tests and finally the fault will be Corrected by the operation and maintenance

team. Managing faults in a telecommunication network can be conceptually divided in three phases [8],[12],[21].

- Detection;
- Fault localization;
- Repairing.

Detection

The fault detection deals with discovering problems that affect performance or data transmission. Usually communication network devices provide indication in the form of alarms when they sense malfunction. Thus, fault detection can be accomplished by using the alarms provided by the network element[12],[22].

Fault localization

Fault localization is also called Fault diagnosis which deals with pinpointing one or more root causes of problems along with their specific location to the point where corrective action can be taken [3],[5]. This is also referred to as fault isolation. This diagnosis can be performed by analyzing and correlating the messages sent by network equipment's as an alarm. Hence it becomes a huge task for a network manager to manually sit and analyze each of these alarms, fault localization model using neural networks is proposed in this paper to segregate them based on their micro wave link topology to make a correct decision and take necessary actions to get rid of the problem.

Currently, fault localization is being performed manually by an expert or a monitoring team experienced in managing communication networks based on network disorder symptoms or alarms displayed on a fault management system. For time critical systems it is required that system must be up and running each and every minute. However, The monitoring team face difficulties in problem management due to the hundreds of alarms issued by network devices. As a result, the technicians are overburdened with thousands of alarms and are unable to investigate them all.

Repairing

Repairing is one operation of fault management performed on the faulty component to avoid the overall impact on the whole telecom network [12].

3 ARTIFICIAL NEURAL NETWORK

This section covers the fundamental concepts underlying the most often used artificial neural network (ANN) for data classification.

3.1 INTRODUCTION TO NEURAL NETWORK

ANN, which is one of the approaches in the field of artificial intelligence, was inspired by the computational mechanism of biological nerve networks. ANN is a computer program that mimics how the human brain does a task. It is composed of a large number of highly interconnected information-processing elements called neurons to solve specific problems. A neuron is a computational element, and is the building block of an ANN [23],[24]. The ANN model consists of three basic elements [24],[25],[26] :

- A set of connecting links, each of which is characterized by a weight;
- An adder for summing the input signals, weighted by the respective weight of the neuron;
- An activation function for limiting the amplitude of the output of a neuron.

The most common type of ANN consists of three layers: input, hidden , and output. The raw data fed into the network is represented by the activity of the input units, and each neuron has a set of inputs. Each link between the input and the hidden layer is represented by synaptic weights. The activities of the input units and the weights on the links between the input and hidden units determine the activity of each hidden unit. The output layer generates output based on the input, hidden unit activity, and hidden/output unit weights[23],[25],[26].

3.2 ARCHITECTURE OF NEURAL NETWORK

The network topology or architecture refers to the way neurons are organised in a neural network. Neural network architectures are roughly divided into feed-forward and feedback architectures [24],[26]. Signals in feed-forward networks flow in one direction only, whereas signals

in feedback networks can flow in both directions. The architecture of ANN used in this study is feed-forward networks and depending on the type of the connections between the neurons, it is further grouped as [23],[27],[28],[29]:

- Feed forward artificial neural network(FFNN)
- Cascade forward artificial neural network (CFNN)

3.2.1 FEED-FORWARD NEURAL NETWORK

FFNN are classified as single layer and Multi-Layer Feed-forward network based on the number of layers [30]. In a multi-layer FFNN, there is at least one layer of hidden neurons between the input and output layers [27],[28],[29]. These architecture allow signals to travel from input to output in one direction only, hence there is no feedback. The signal is carried out from the input layer to the hidden layer in the weighted form. The activation function on the layer processes signals that enter the neurons in the hidden layer [26],[30],[31]. In the hidden layer, the weighted total of each neuron's output is then sent to the output layer. This layer's activation function analyses the incoming signal before sending it to the output layer. Typically, the output layer's activation function is identity mapping, which ensures that the output received in this layer is identical to the incoming signal.

Neural network architectures are trained through various learning algorithms for producing most efficient solutions. There are different types of algorithms to train a neural network. Some of them are gradient descent, newton method, conjugate gradient, quasi newton method and Levenberg-Marquardt . In this paper, ANN model with gradient descent training algorithm is built. To apply gradient descent, back propagation learning algorithm is used. Among many other learning algorithms, back-propagation algorithm is the most popular and the mostly used one for the training of feed-forward neural networks.

Backpropagation is the process of updating the weights of the network in order to reduce the error in prediction as the main intention of training the network is to minimize a cost function [24],[27],[28].

The procedure used to carry out the learning process involves the following steps [23],[29],[30],[32].

1. Initialization: Initialize the weight randomly.
2. Forward computation: Train the model using the training set by propagating the input signals through the network layer by layer.
3. Backpropagation. Compute the error signals corresponding to each neuron.

Figure 3.1 shows the multi-Layer feed-forward neural network with n input neuron, m output neuron and one hidden layer with m neurons.

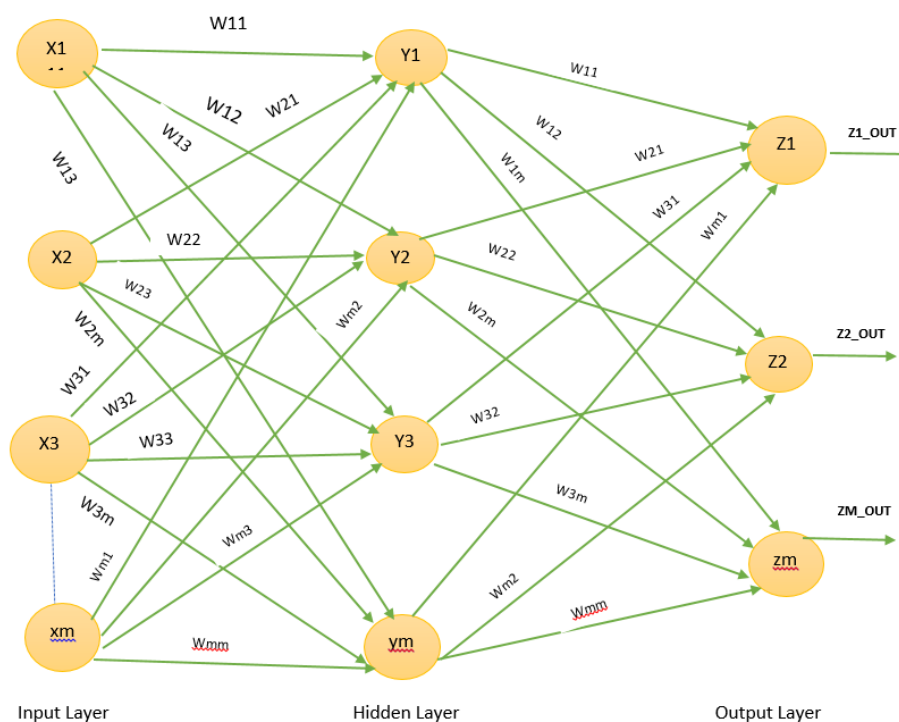


Figure 3.1: Feed-forward neural network architecture

3.2.2 CASCADE-FORWARD NEURAL NETWORK

CFNN is the other classes of the forward neural network. CFNN is almost the same as that of (FFNN). The main difference is that, in case of CFNN, there is direct link between the input layer and the output layer, in addition to the indirect link through the hidden layer as shown in Figure 3.2. In CFNN, each neuron in the input layer is attached to each neuron in the hidden layer as well as each neuron in the output layer [28],[33],[34].

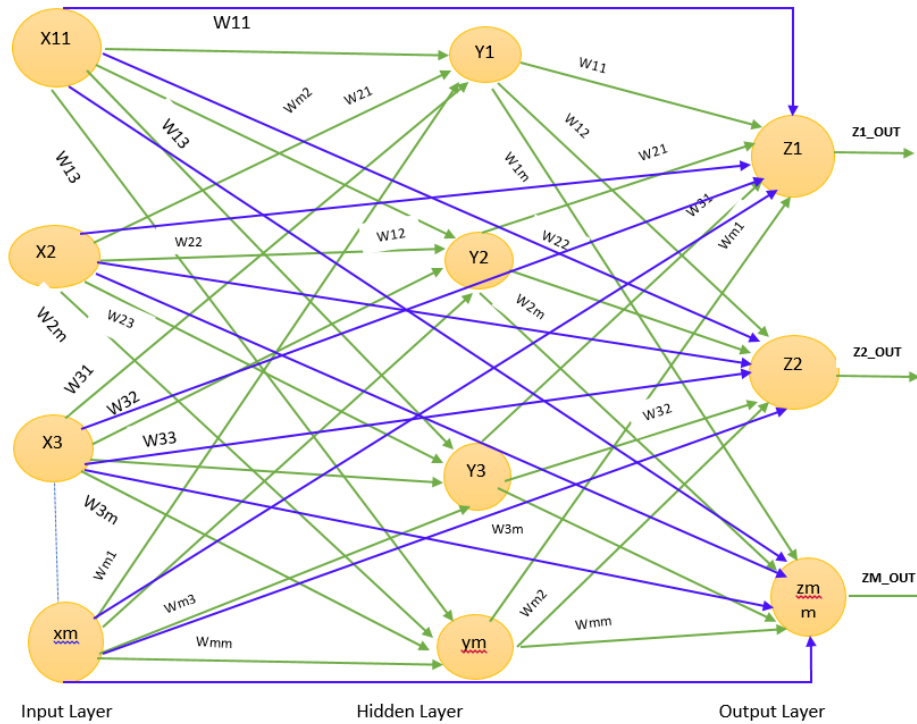


Figure 3.2: Cascade-forward neural network architecture

3.3 THE LEARNING PROCESS

Neural networks have already been shown to be helpful in medical diagnosis, and they could be useful in fault diagnostics by extracting patterns and detecting trends that are too complicated for people or other computer systems to observe.

There are many different algorithms that can be used when training artificial neural networks with their own advantage and disadvantage. As mentioned in the above section gradient descent training algorithm with backpropagation learning is used for this study. The main objective of the learning process is to map the input features to a correct output by altering the network's weights. All learning methods used for neural networks can be classified as Supervised learning and Unsupervised learning [35],[36].

Supervised learning is a technique that uses an external teacher to provide a desired input and output features while training the network. So during the learning process each output unit is told as a response to input signals [36],[29]. An important issue concerning supervised learning is to minimize an error between the desired and computed unit values by updating its weights based on its target output and actual output and make corrections to the network.

There are many different supervised learning algorithms but the most popular one is backpropagation.

Unsupervised learning is also referred to as self-organization, in the sense that the neural network is only given a set of inputs and it's the neural network's responsibility to find some kind of pattern within the inputs provided without any external aid [36],[37].

4 CORRELATION ANALYSIS AND FAULT LOCALIZATION

This research has two sections. One is the alarm correlation analysis part and the other is modeling a fault localization using artificial neural network and identifying a well performing neural network architecture to model fault localization.

4.1 ALARM CORRELATION ANALYSIS

Correlation analysis is a technique that deals with finding the association between two or more variables [38]. The correlation analysis in this study is not performed as one task of data pre-processing rather it is considered as a technique to figure out the association between network equipment alarms. Hence, these portion of the research is mainly performed to identify the association between the alarms and classify the alarms as parent and child alarm. The relationship or the correlation between variables is determined numerically by a decimal value called correlation coefficient[38],[39]. Among many types of correlation coefficients, Pearson correlation coefficient(r) is the one used here to understand and analyze the strength of correlations between alarms as it is the most often used one.

The value of the correlation coefficient varies between +1 and -1 in terms of the strength of the association. Based on the value of the coefficient, the correlation strength can be determined. A value of 1 shows that the two variables are perfectly associated or strongly correlated. As the correlation coefficient value goes towards 0, the relationship between the two variables will be weaker, whereas a negative sign indicates a negative correlation. A correlation coefficient with a higher number value indicates a strong correlation between two variables and a lower value indicates otherwise.

To calculate Pearson's correlation coefficient first, the covariance of the two variables and the standard deviation of each data sample should be calculated and then divided the covariance by the product of standard deviation.

The formula shown in Equation 4.1 is used to compute the Pearson correlation coefficient between two variables X and Y . [38].

$$r = \frac{\text{covariance}(x,y)}{\sigma_x \sigma_y} \quad (4.1)$$

Where r is the correlation coefficient, Covariance(x, y) is the covariance, and σ_x and σ_y are the standard deviations of x and y, respectively. The correlation coefficient can also be calculated using the following formula if the dataset involves more than two set, x_1, x_2, \dots, x_n and y_1, y_2, \dots, y_n .

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 (y_i - \bar{y})^2}} \quad (4.2)$$

Where r is the correlation coefficient, n is the sample size, x_i and y_i are the i^{th} data values, and \bar{x}, \bar{y} are the mean values.

4.2 CORRELATION ANALYSIS METHODOLOGY

In this research, identifying the correlation among alarms of different network equipment in order to identify the strong predictor alarm for BS outage is performed. To get the correlation analysis result the following steps or procedures have been used. The procedure of correlating alarms involves the following tasks as shown in Figure 4.1.

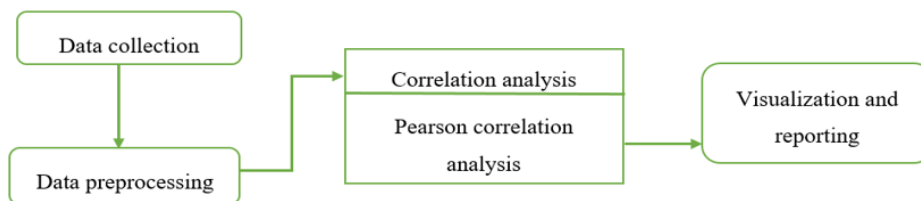


Figure 4.1: Methodology for correlation analysis

4.2.1 DATA COLLECTION

History alarm data is collected from the network management system. A lot of historical alarm data is stored in the database of network alarm. The stored alarms or the kind of network status information and its format depends on many factors, such as configuration, type, and vendor of the nodes and network equipment. But for this research alarms are collected from the Huawei

radio access network sites, more specifically the base station alarms. It includes the fields such as Site Name, Alarm Name, Event Time and Severity as shown in Table 4.1.

Table 4.1: Attributes of alarms with their description

Field	Description
Severity	Priority state of the alarm
Alarm Name	Name identifying the alarm kind
Alarm ID	ID identifying the alarm kind
Site ID	ID identifying Network equipment producing the alarm
Site Name	Name identifying the Network equipment producing the alarm
Region/zoon	The specific location of the NE that produced the alarm. Eg north region, west region, east region, west Addis Ababa zone, etc.
Device Type	The type of the device is categorized as power equipment, transmission, and IP
Location Info	The general information about alarms location alike
Occurred time	The specific time when the alarm occurred on
Cleared On	The specific time when the alarm cleared on
Duration	Calculated time interval between the occurring and cleared time of the alarms

4.2.2 DATA PREPROCESSING

Categorizing alarms

There can be different situations due to which a large amount of alarm message is encounter from different devices. An alarm appear when one or more radio links between network elements in network fail due to failure of a Power equipment, transmission equipment, IP equipment. In order to analyze the association between alarms, the network alarms are grouped based on their network equipment.

Aggregation of Data

The alarm data is aggregated based on their site ID first then to ensure the alarm sequence or time series similarity the alarm data is aggregated using their occurrence time.

Data cleaning and Attributes selection

In order to perform useful alarm correlation, data cleaning is very important because alarm data is either incomplete or contains more redundant information, but it contains some valuable information. The operations of data cleaning include selecting the needed attributes and removing those redundant information. Alarms of specified network element or the specified time period is filtered.

Feature extraction

The other operation of data preprocessing is dealing with data types. Data types can be classified as numeric, categorical and ordinal. The alarm log has a categorical data type as a result the value of the alarm attributes need to be converted into meaningful features to perform a correlation analysis. Therefore the categorical data type of the alarm log has to be converted into a numeric feature by creating dummy features. The alarms are coded in binary data (0's and 1's) according to their occurred and cleared time. In the set of dummy features, 1 indicates that the observation belongs to that category and 0 indicates that the observation doesn't belong to that category.

4.2.3 PEARSON CORRELATION ANALYSIS

After preprocessing the alarm data, identifying the alarm that have strong impacts on BTS outage will take place using a correlation analysis technique. Pearson correlation coefficient is adopted to discover the relationship between alarms. The Pearson correlation coefficient value is used to figure out the strength of the relationship between alarms [39]. Pearson correlation coefficient between two alarms can be calculated using the formula described in equation 4.1.

Python programming language is used in this research to calculate the Pearson's correlation coefficient with a built in function called `pearsonr()`. The result of the calculation or the result of the correlation coefficient can be interpreted to understand the relationship.

4.2.4 VISUALIZATION AND REPORTING

A visualization tool called heatmap is used to interpret and visualize the correlation between alarms. Correlation heatmap is a graphical representation of correlation matrix representing correlation between different variables [40]. Heat maps use colors to communicate numeric data by making tables easier to interpret. The colors are used as a measure of the strength of the associations. The associations are then expressed as a set of rules. Hence, in this research, all alarms from different network equipment are carefully analyzed to extract the parent and child alarms by interpreting the Correlation heatmap using the color rules. A correlation rule is then identified by visualizing the Correlation heatmap to be used in the second part of the research which is fault localization using neural networks.

4.3 MODELING FAULT LOCALIZATION

This part of the research paper concerns with modeling fault localization using artificial neural network processing. The main aim of building this model is to help the monitoring team while making decisions during fault management. In current situation, the monitoring teams are expected to figure out the location of the fault as well as the initial cause for every BTS outage manually and it is very time consuming. So, to get rid of all the consequence that came along with manual processing, modeling a system that support fault localization using neural network is proposed in this paper. The neural network classifies the specific location of the fault along with the problem corresponding to the alarm logs in the specified time period. Power problem, transmission problem and Ip problems are addressed as the main causes for the BTS outage. In this research paper, a model is built following the procedure that is shown in Figure 4.2. A feed-forward neural network and cascade neural network is selected among all the available neural network architectures because they are the most commonly used architectures for classification problems. Their performance will be compared at the end.

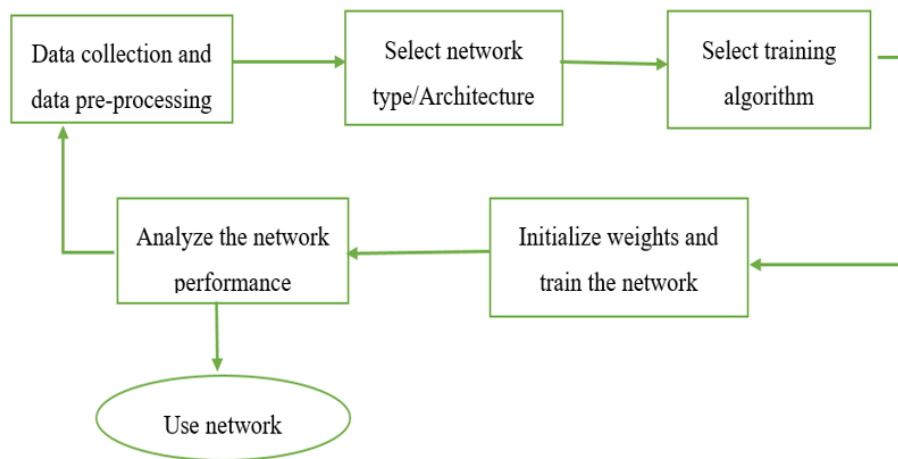


Figure 4.2: Steps to build neural network model

The following specific tasks must be completed in order to attain this goal.

- Preparing the dataset.
- Developing the supervised ANN model.

4.3.1 PREPARING THE DATASET

Data collection

To build a useful fault localization model alarms coming from all the devices forming the network are needed. In addition to alarms, the association between alarms of each equipment as well as topological information or network topology is important. Alarms of the network equipment and topological information are gathered from the existing fault management system database. The existing fault management system includes different database engines coming from different vendors. Three of the main vendors for ethiotelecom are Huawei, ZTE, and Ericson. These vendors use different database engines for the network management system. For this study, only Base station alarms that demonstrate power problem, transmission problem, Ip problem, and BTS are extracted to be used as an input for the proposed model. The correlation rule acquired from the correlation analysis section of this paper is also used as one information while preparing the dataset.

Preprocessing

The preprocessing phase is used to clean and organize the alarm data to prepare the data in a way that is suitable for developing the proposed model. From the perspective of machine learning, Preprocessing step involves both:

- Data engineering;
- Feature engineering.

Data engineering: is the process of converting raw data into prepared data. In order to prepare the data the following tasks are performed in this study.

- **Categorizing alarms:** The collected alarm data is composed of the base station site ID, the alarm name, alarm ID, Network equipment type, Region, occurrence time and cleared time. To prepare the alarm data for the proposed model, the topological data is used. Since base stations are connected to each other via multiplexing transmission system, network elements of base station sites who have topological relationship regarding with their microwave radio transmission link is extracted using their site ID. Then selected alarms of base station sites which are under the same microwave links or who have topological relationships is categorized or gathered in one cluster or group and store them in

a csv file. Number of base station sites under each category is different.in this section alarms of the selected equipment's that has a high correlation with the alarm that shows the BTS outage is used or selected.

- **Aggregation of Data:**once BTS sites are gathered in one group or cluster, alarms of the selected network equipment's will be aggregated based on their occurrence and cleared time. The base station sites which are under the same microwave links and whose occurrence and cleared time fall in the same time interval are merged in one cluster. The time interval is considered as cluster borders. This approach involves identifying patterns of alarms by considering the time interval. That is, the instances to aggregate are defined through temporal window time.
- **Attributes selection:**This step is mainly used to identify and remove redundant and irrelevant information. Therefore, after aggregating the alarm data selecting the useful alarm attributes to identify frequent pattern rules is very important. Even though the alarm has many attributes only the site ID and the alarm name is selected here using filter method. The patterns or rules are extracted for the purpose of identifying the root cause and fault localization.

Feature engineering: is the other task involved in data preprocessing steps and its main purpose is to change the prepared data into suitable format to create the features expected by the machine learning model. This includes changing the data type of the new features into numerical data type to be used by the model during training and testing phase.

4.3.2 DEVELOPING THE SUPERVISED ANN MODEL

This section is concerned with building the neural network model. Due to several possible causes and location of cause's availability, multiclass classier is required. In this study feedforward neural network and cascade neural network is used to process the multiclassification. As discussed in chapter two of this paper, the network topology defines the ways the nodes will be connected and organized. The two artificial neural network models are similar in everything except that in the cascade forward neural network architecture each layer of neurons are connected to all layer of neurons. The architecture can be built from one input layer, one output layer and single or multiple hidden layer.

In this research, the Cascade forward neural network and feed forward neural network is applied for fault localization modeling purpose. Thereby, the neurons in the input layer are the alarm name and the site ID'S, whereas the output is the site ID plus the initial cause of the BTS alarms. The architecture of feed forward neural network and cascade forward neural network is shown in Figure 3.1 and 3.2.

The input layer contains neurons that match with the number of the selected features. The features that are selected in this study are alarm name and site ID. Therefore the number of neuron depends on the number of site ID's that is included in the data set plus the alarm names. The number of alarm names included in the data set are fixed because only alarms that are highly correlated to the BTS outage alarm are taken during the alarm correlation analysis stage.

The neurons in the output layers also depend on the number of class that are considered as a target. In this study the target is the type on the fault or the initial cause (power, IP or transmission problem) and the location of the problem (described using the site id). Therefore the number of neurons in the output layer depends on the number of site ID's that are included in the prepared dataset.

The other layer is the hidden layer which is where the processing part is performed. The hidden layer executes two operational functions. one is summation function and the other is an activation function. The summation function is the first step, and in this part, each input to ANN is multiplied by its respective weight and then, the products is cumulated into the summation function (Σ). A bias value is then added with the weighted sum of the inputs. a bias value is used to regulate the output of the neuron in association with the weighted sum of the inputs. The activation function is the second step; which converts the input signal, received from the summation function module and transform it to an output of a neuron for an ANN model. The number of neuron in the hidden layer of the neural network has nothing to do with The selected features included in the data set, for both feedforward and cascade neural network.

4.3.3 TRAINING AND TESTING OF ANN

After selecting and building the FFNN and CFNN architecture the next step is to train and test the model using the prepared data set. To do so the data set is split into training set and testing set. The training of the ANN is accomplished through a learning process. The procedure used

to carry out the learning process in neural network is called optimization algorithm or optimizer. There are different types of optimizers as described in chapter two. Among all the available training algorithms, for this study, a gradient descent algorithm is selected to train the model. To apply a gradient descent to the neural models backpropagation learning algorithm was used.

4.3.4 PERFORMANCE EVALUATION METRICS

Performance measures are used to select the better model. This section examines the most commonly used performance measures for selecting the best neural network model. Mostly classification accuracy is used to measure the performance of a model. However there are several standard metrics to evaluate classifier models. In this study, the Confusion matrix and some other standard metrics such as Mean Absolute Error (MAE), Mean Square Error (MSE), and Mean Relative Error (MRE) are discussed.

Confusion Matrix : is an $N \times N$ matrix used to visualize and evaluate the performance of a classification model, where N is the number of output or target classes. The number of predictions produced by the model where it classified the classes correctly or erroneously is represented by each entry in a confusion matrix. The matrix compares the actual target values to the model's predictions. This gives us a complete picture of the classification model's performance and the types of errors it makes. Confusion matrix for a multiclass problem depends on the number of target classes [41].

		True class		
		Class1	Class2	Class3
Predicted class	Class1	+ve 1	-ve 2	-ve 3
	Class2	-ve 4	+ve 5	-ve 6
	Class3	-ve 7	-ve 8	+ve 9

Figure 4.3: Multi-Class Classification Confusion Matrix

Unlike binary classification, there are no positive or negative classes. Due to this finding true positive (TP), true negative(TN), false positive(FP), and false negative(FN) may seem tough at first, but it's actually quite simple and for each class it can be calculated by adding the cell values as follows:

Class 1	Class 2	Class 3
TP = cell1	TP = cell5	TP = cell9
FP = cell2 + cell3	FP = cell4 + cell6	FP = cell7 + cell8
TN = cell5 + cell6 + cell8 + cell9	TN = cell1 + cell3 + cell7 + cell9	TN = cell1 + cell2 + cell4 + cell5
FN = cell4 + cell7	FN = cell2 + cell8	FN = cell3 + cell6

Confusion Matrix forms the basis for the other types of metrics. Hence, with the help of TP, TN, FN, and FP, other performance metrics for each class can be calculated.

Accuracy: is a measurement of correctly predicted instances from the total data. It is the ratio of number of correct predictions to the total number of input samples. The accuracy of the model is calculated using Equation (4).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4.3)$$

Precision: It is used to measure the proportion of positive data instances that a model classified as positive. The precision metric takes into account all positive predictions and ignores the capabilities of a model to recognize negative classes. The precision value is calculated using Equation (4.4). The precision value lies between 0 and 1. The higher the precision is, the lower the number of false positive errors committed by the classifier.

$$Precision = \frac{TP}{TP + FP} \quad (4.4)$$

Recall: It is a percentage of positive cases properly predicted by the classifier in a model. It is determined using Equation (4.5), which divides the number of valid positive outcomes by the total number of relevant samples. The lower the number of cases misclassified as negative, the greater the recall value. As a result, a model with no false negatives (FN) has a one-recall value.

$$Recall = \frac{TP}{TP + FN} \quad (4.5)$$

Error measurement: is the other way to evaluate the prediction accuracy of ANN models is to perform error measurement. Mean Absolute Error (MAE) and Mean Square Error (MSE) are employed for comparative evaluation of the performance of each model.

Mean Absolute Error (MAE): is a straightforward method of determining the magnitude of an inaccuracy. It refers to the magnitude of difference between the prediction of an observation and the true value of that observation and takes the average of the absolute differences between the predictions and the observed values. The MAE value ranges from 0 to infinity, with 0 being the best possible value.

$$MAE = \frac{1}{N} \sum_{i=1}^N |Actualvalue - Predictedvalue| \quad (4.6)$$

Where N is the number of data patterns in the independent data set.

Root Mean Square Error (RMSE): measures the quadratic mean of the differences between the predictions made by a model and the actual values. The measure is always positive or 0. Values closer to 0 are better than higher values.

$$RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^N (Predictedvalue - Actualvalue)^2} \quad (4.7)$$

5 EXPERIMENT APPROACH

This study has exploited correlation analysis to identify relevant attributes in the dataset which have a significant impact on the BTS outage and neural network-based fault localization to identify the initial cause and the location of the problem. Hence, the experiment for this research is divided into two parts. The first is the correlation analysis, and the second is the use of neural networks to model faults localization. The correlation analysis is performed first and then modeling the fault localization using the two architectures of neural network is conducted next using the correlation analysis result, the history alarm, and the network topology. The experimental dataset, experimentation Scenarios, and analytical results for the proposed methodologies are described in this chapter.

5.1 CORRELATION ANALYSIS SCENARIO

The steps taken in this research study to perform correlation analysis are discussed in the subsections below.

5.1.1 DATASET FOR ALARM CORRELATION ANALYSIS

This section describes the relevant datasets which are used for correlation analysis. Before applying the correlation analysis approach, relevant dataset is prepared following the preprocessing technique outlined in section 4.2.2 of this paper. This dataset is prepared using historical alarms to undertake alarm correlation analysis in order to mine alarm rules indicating the influential alarms. The original alarm data was first gathered from ethiotelecom's existing fault management system. Currently, ethiotelecom is collaborating with a number of vendors, including ZTE, Huawei, and Ericsson. There are a variety of network management systems available, each of which uses a different database engine coming from this different vendors. Huawei iManager 2000 (for Huawei Technologies' DWDM and SDH nodes), Huawei iManager u2000 (to manage Huawei mobile network elements), ZTE Netnumen u31 (to manage ZTE mobile network elements), Ericsson citrix (to manage Ericsson mobile network elements),

and Huawei iManager NetEco (to manage Huawei mobile network elements) are some of the network management systems (to manage Huawei power equipment). For this study, a total of six hundred Thousand alarm logs or records were collected within 30 days from 441 Huawei BTS sites. The original alarms usually contain different attributes. The following attributes are commonly seen in original alarms: alarm name, alarm ID, equipment name, equipment type, equipment address, severity, occurrence time, cleared time, site ID, subnet, and so forth. Some of the attributes provide similar information. so to start with, we extract the seven important attributes as shown in Figure 5.1.

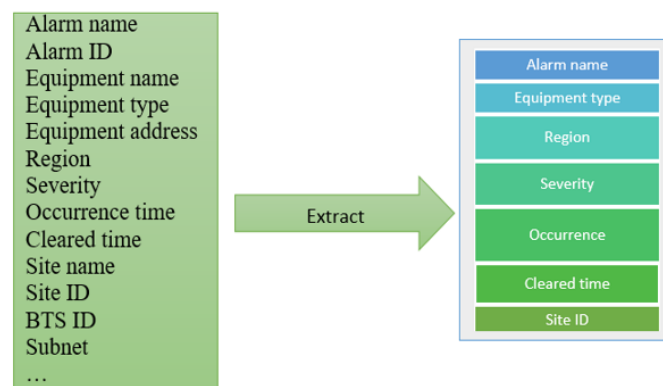


Figure 5.1: Extraction of original alarm attributes.

As a startup, the alarms are categorized based on their equipment type as power alarm, transmission alarm, Ip alarm and BTS alarm to analyze the correlation between alarms that demonstrate the BTS outage and alarms that demonstrate the faulty of other network equipment found within the base station. And finally, distinguish the parent and child alarms. Therefore in this work, three types of datasets have been considered based on the categories of the alarm logs:

- Power equipment alarm dataset for evaluating correlation with BTS alarm.
- IP equipment alarm dataset for evaluating correlation with BTS alarm.
- Transmission equipment alarm dataset for evaluating correlation with BTS alarm.

After categorizing the alarms, only those alarms with critical severity level are filtered and considered for this study specifically .as their severity level indicates, this alarms need very serious attention because they have direct relation for service outage. Whereas, other alarms

which have major or minor severity levels are warnings and has nothing to do with service outage directly. But it doesn't mean alarms with minor or major severity levels doesn't need to be fixed as they have long term effect on the network service. An alarm called NE disconnected is selected from BTS related alarms because this alarm is the one which demonstrate the BTS outage. If the NE disconnected alarm appears on the fault management system, it signifies that the base station site associated with this alarm is neither operational nor delivering service. Hence, the correlation between this alarm and other categories of alarms is the main concern of this study.

Dataset 1: is composed of Power equipment alarm and BTS alarm.

There are many different types of Power equipment in one base station and those equipment's produce several types of alarms which indicate their malfunction, but only alarms with critical severity level are considered and analyzed in this research paper. Severity level is one attribute of an alarm. As described in the above sections alarm name, occurrence time, cleared time, alarm ID, region of the alarm source and the site ID of the alarm are also alarm attributes. Table 5.1, shows Power equipment alarm names along with their description.

Table 5.1: Power equipment alarms and their description

Alarm name	Description
Mains failure	The commercial electricity that powers a system or circuit is gone
Diesel generator startup failure	When the diesel generator fail to start function.
DG Running	The DG is on working mode.
Bus Bar Under voltage	The bus bar voltage is the battery voltage if the battery is connected to the power system. The voltage should be between 43.2 and 57.6 Vdc. More specifically, a low voltage reading of 42Vdc and a high voltage reading of 58Vdc are required.
Air-condition Failure	This means the air conditioner fails to work due to many reasons.
Battery Discharging	Battery loosing voltage or energy.
LLVD	Stands for load low voltage disconnected. Produced when the load connection voltage is below the threshold which is 48V DC in context of Huawei due to AC power failure or loads are manually disconnected.
BLVD	Stands for Battery low voltage disconnected. Produced when the battery connection voltage is below the threshold which is 43V DC-in the context of Huawei due to AC power failure or batteries are disconnected manually.
RADIO_TSL_LOW (635)	The RADIO_TSL_LOW is an alarm indicating that the radio transmit power is very low. This alarm is reported when the detected transmit power is less than the lower power threshold of the RFU/ODU.

Dataset 2: is composed of transmission equipment alarm and BTS alarm.

RTN905, RTN950 and RTN80 are the Transmission equipment's that are found in base station sites. This equipment generates a variety of alarms. Table 5.2 lists the alarm names and descriptions for those alarms with a critical severity level.

Table 5.2: Transmission equipment alarms and their description

Alarm name	Alarm Description
BD.STATUS (119)	The board cannot be detected
ETH_LINK_DOWN (12793)	The link connected to an Ethernet port is interrupted
ETH_LOS (235)	The loss of Ethernet port connection.
MW_LOF (631)	The radio frame is lost.
NE.COMMU_BREAK (1)	The communication between an NE and the NCE is interrupted
NE_NOT_LOGIN (2)	NE is not logged in
R.LOF (8)	Frames are lost on the receive side. This alarm is reported when the OOF state lasts for three milliseconds.
RADIO.RSL_LOW (638)	The radio receive power is very low. This alarm is reported if the detected receive power is equal to or lower than the lower threshold of the RFU/ODU
RADIO.TSL_LOW (635)	The RADIO.TSL_LOW is an alarm indicating that the radio transmits power is very low. This alarm is reported when the detected transmit power is less than the lower power threshold of the RFU/ODU.

Dataset 3: is composed of IP equipment alarm and BTS alarm.

The IP equipment's in the access side of the network are ATN950B and CX600. This equipment produce different type of alarms. IP equipment alarm names with critical severity levels along with their description is shown in Table 5.3.

Table 5.3: IP equipment alarms and their description

Alarm name	Description
Physical Port Down	The physical interface's state has changed to down and due to this traffic forwarding on the physical interface will be affected as a result of this.
Device Offline	The server cannot be connected to the device through ICMP/SNMP.
Optical Invalid	The optical module experienced a complete failure when the input optical power was too low. Due to this Services on the optical module will be affected, and error codes or packets may occur, or services even be interrupted. Thus, a speedy solution is required.
Link Down	The link protocol is Down and due to this the interface cannot forward packets normally.
Board Fail	Board registration failed or Board Fail
Fan Remove	The fan module was not installed in the slot.
Card Invalid	The service logic on the sub-board malfunctions or sub card registration failed
Eth-Trunk Member Down	All of member interface's physical status are down.
LOF(R.LOF)	1. Received signals were attenuated significantly. 2. The peer device sent unframed signals. 3: The local device had a fault on the Rx side.

Once the alarms are categorized, the alarms are then aggregated using their site ID and their occurrence and cleared time. And data cleaning is performed afterward.

After aggregating and cleaning the alarm data, time segmenting is implemented using the occurrence and cleared time of the alarms under the same site ID for each category. Because of the complexity of the network itself and its physical and logical correlation, single fault may lead to a large number of alarms. These alarms triggered by the same failure occur inevitably at the same or similar time. That is to say, the alarms with the similar start time may have relationship, and those with longer time interval may not be caused by the same fault. In the original alarm data, time duration of the alarms are considered as cluster borders. Alarms which demonstrate the BTS outage and alarms which demonstrate one of the network equipment malfunction is considered as one cluster to implement the time segmentation. The time segmentation is performed to visualize the alarm sequence and later to calculate their correlation and identify frequent pattern rules. Even though the alarm has many attributes only the site ID and the alarm name is selected here using filter method. The patterns or rules are extracted for the purpose of identifying the initial cause alarm of the NE disconnected alarm.

Once the alarm of the same site id is segmented based on their time interval the next step to prepare the data set is to deal with the data type of the alarms. Since the alarm logs has a categorical data type it has to be converted into a numeric feature by creating dummy features to perform a correlation analysis. to do so, the alarm names are coded in binary data (0's and 1's) according to their occurred and cleared time. in the set of dummy features, 1 indicates that the alarm name belongs to that time segment and 0 indicates that the alarm name doesn't belongs to that time interval.

5.1.2 ALARM CORRELATION ANALYSIS

Experiments were conducted using the datasets prepared for the correlation analysis purpose to identify interesting relationships in the dataset. These relationships help us realize the relevance of alarms with respect to the target alarm or in other word it helps us identify the parent and child alarm of the base station. Since the intention of the analysis is to identify the root alarm which initiate the alarm that demonstrate the BTS down status, the power equipment alarm ,the transmission equipment alarms and the IP equipment alarms are considered as an independent attributes and the BTS alarm referred as NE disconnected is the dependent attribute. But since there are several alarms that demonstrate the network equipment status Person correlation analysis technique is used to calculate the correlation between those network equipment alarms with BTS alarm. Python program is used to perform the person correlation analysis.

To build the correlation matrix, Pandas .corr () function is used. Pandas is a software library written for the Python programming language for data manipulation and analysis and corr() is a built-in method to calculates the relationship between each column in the data set. The correlation value is visualized using Heatmap. The heatmap help us to analyze the value of the correlation result by representing each value using different shades of color. The Seaborne Python package is used to create Heatmap.

5.2 FAULT LOCALIZATION USING NEURAL NETWORK

The steps taken in this research study to build the fault localization model are discussed in the subsections below.

5.2.1 DATASET FOR THE NEURAL NETWORK

This dataset is created utilizing historical alarm data from Ethio telecom's existing fault management system, the network topology database, and the alarm rules established through correlation analysis in this study. Two procedures are followed to prepare the data in a way that is suitable for developing the model: The two procedures are:

- Data engineering;
- Feature engineering.

Data engineering

As mentioned before this procedure deals with converting raw data into prepared data. to do so, first the base station sites which have a microwave link is extracted using the network topology database. The network topology data shows the microwave link between BTS's of each base stations. The ethio telecom network is divided into different areas regarding with their regional location as north region, west region, south region, east region and Addis Ababa. This areas are again subdivided into different subareas regarding with their micro wave links, each subarea consists of a group of BTS sites and MW links.

Only the Addis Ababa region has been chosen as a research target in this study. Because the other regions networks were not stable due to the country's current situation, most BTS statuses were down due to the same particular reason throughout the data collection time. In reality, collecting various types of alarms proved nearly impossible.

As we continue with the Addis Ababa region, the Addis Ababa region is subdivided into five zones (WAAZ, EAAZ, NAAZ, SAAZ, and CAAZ). To reduce the complexity of the problem, west Addis Ababa zone was selected because large number of alarms were occurred in this specific zone during the data collection period relative to the other Addis Ababa zones as shown in Figure 5.2.

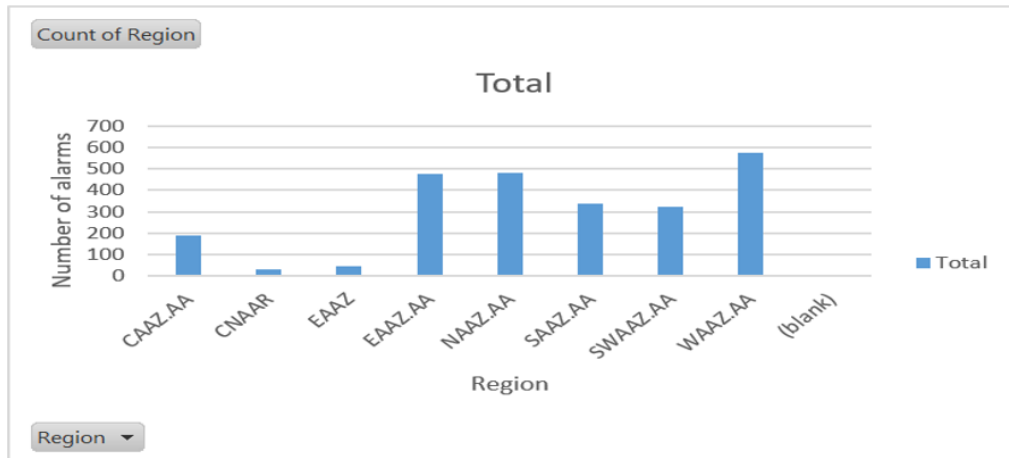


Figure 5.2: Number of alarms per Addis Ababa zones

Since the WAAZ network is divided into different subareas depending on their micro wave link, BTS sites which are under the same micro wave link is selected and represented by one neural network architecture for this experiment or case study. For instance the BTS sites shown in figure share the same microwave link and they are represented by one neural network. This is just for the sake of reducing the complexity of the problem.it is possible to assign more subareas under one neural network but it needs more energy and time to analyze the microwave link between each BTS sites and perform the preprocessing step to prepare the data set .and plus the objective of the research is to evaluate the model performance. The status of the hub site affect the status of the down sites, if they are under the same microwave link topology and this is why the network topology is considered while preparing the dataset.As mentioned in the previous sections, the original alarms usually contain different attributes, but here only important attributes are extracted to prepare the dataset.

The alarms occurrence and cleared time is utilized to aggregate alarms of the selected base station which are categorized under the same group. Aggregating the alarms makes the process of identify patterns of the alarm easy. To prepare the pattern, the site ID and the alarm name attributes are selected. The patterns or rules are extracted for the purpose of identifying the root

cause and fault location as the alarm name indicate the initial cause and the site ID indicates the location of the problem. Hence the output is labeled as power or Ip or transmission problem at that specific site ID. Therefore the model is expected to classify the incoming alarm based on their alarm name and site ID.

Feature engineering

Once the data is prepared the next step is to make the data type of the selected attributes or feature suitable for the model that is going to be developed. Neural network model are comfortable with numerical data types therefore each active alarm name and site ID is represented as 1 value and the inactive alarm name and site ID is then noted as 0 value. On the output or the target site related fault location site ID and the initial cause of the fault are represented as 1 and the rest is represented as 0. The operation ,converting categorical features of the alarm to a numeric representation, is performed using python programming language using a function called Dummy().

5.2.2 BUILDING A NEURAL NETWORK MODEL

Once the data is prepared the next step to build a model using a neural network is selecting a neural network architecture. Among all the available architectures, Feed forward neural network and cascade forward neural network is chosen because in literatures this two are the most commonly used architecture for classification problems. The prepared data is divided into the training and test samples and passed this data to the selected neural network architectures. 80% of the sample is used as training samples and 20% was used as testing sample.

A three layer neural network is considered sufficient for this study and Python program is used for developing neural network model. Python provides necessary functions to quickly create, train and test the neural network. It also provides ready to use training algorithms.

As mentioned before, the west part of Addis Ababa has been chosen to be a case study and this part is divided into different subareas containing different group of BTS sites regarding with their microwave link. The one selected for this study or experiment contains 8 group of BTS sites. A training sample of 104 patterns, each pattern formed by input and output vectors, has been prepared for training.

Both CFNN and FFNN is composed of 14 input nodes, 10 hidden nodes, and 27 output node. The number of input nodes was the number of alarm names and the number of site IDs in the dataset. The number of output nodes was the number of the initial causes (power, IP, and transmission) plus the number of site IDs in the dataset. The number of neurons in the hidden layer is chosen by the model's performance. It was chosen in such a way that the model's training could be completed quickly and accurately. During the training phase, the maximum number of epochs is set to 100, and the network is configured to train until the maximum number of epochs is reached, at which point network performance is evaluated. The network configuration is then modified based on network performance by increasing or decreasing the hidden nodes. The neural network's weights and biases were set using the gradient descent back-propagation algorithm.

6 RESULTS AND DISCUSSION

6.1 RESULTS OF CORRELATION ANALYSIS

This study has exploited correlation analysis approaches to identify relevant alarms of base station network equipment in the dataset which has a significant impact on the BTS down status alarm. By using a `pandas.corr()` function the person correlation coefficient is calculated. The result is then visualized using a heatmap. As mentioned earlier in this paper, a heatmap is a method of graphically representing numerical data where the value of each data point is indicated using colors. A heatmap contains various shades of colors for each value to be plotted. Usually, the darker shades of the chart represent lower values than the lighter shade. Pearson correlation is applied on the three datasets prepared previously on this paper for the correlation analysis purpose. The interpretation of the heatmap for each dataset is discussed separately. Correlation analysis between:

1. POWER EQUIPMENT ALARMS AND BTS ALARM

There are several alarms that demonstrate the power equipment status in base stations. Using dataset1, the association between power equipment alarm and the alarm that demonstrate BTS outage is analyzed. Figure 6.1 presents the heatmap to visualize the correlation between power equipment alarm and BTS alarm. Here the highest correlations are observed between:

- An alarm named with NE is Disconnected looks to be highly correlated with LLVD and BUS BAR undervoltage
- BUS BAR under voltage looks to be highly correlated with LLVD. But based on their functional behavior this two alarms get produced in sequence.
- The rest of alarms have the least correlation with BTS. Hence, it is considered as having no direct impact for the BTS outage.

But here the LLVD alarm is selected as the one which has the highest impact on the BTS

outage.

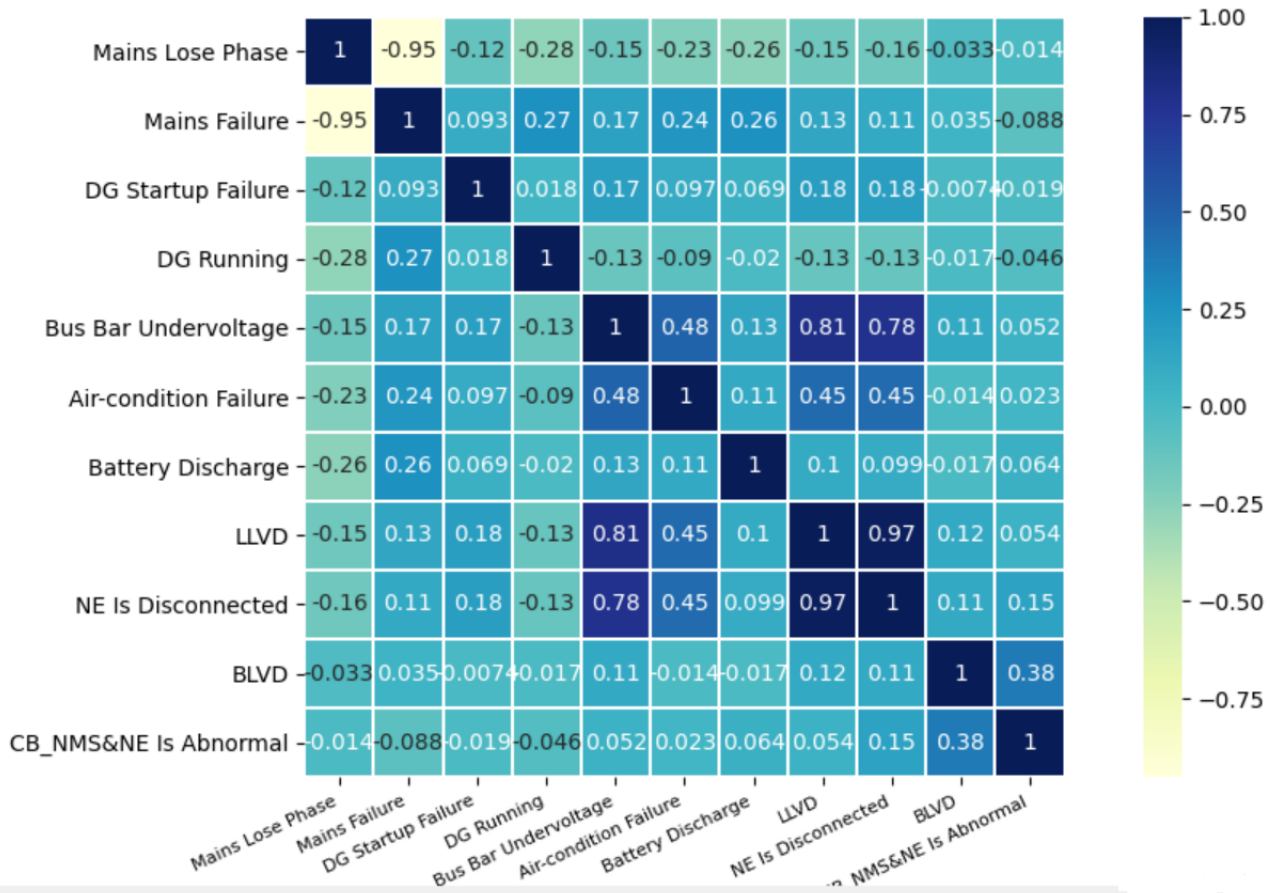


Figure 6.1: Correlation between power and BTS alarm

2. TRANSMISSION EQUIPMENT ALARMS AND BTS ALARM

There are several alarms that demonstrate the transmission equipment status in base stations. Using dataset2, the association between transmission equipment alarm and the BTS alarm that demonstrate BTS outage is analyzed. Figure 6.2 presents the heatmap to visualize the correlation between transmission equipment alarm and BTS alarm. Here, the highest correlations are observed between:

- An alarm named with NE is Disconnected looks to be highly correlated with NE COMMUNICATION BREAK and ETH-LOS.
- The rest of alarms have the least correlation with NE is Disconnected. Hence, it is relatively considered as having no direct impact for the BTS outage.

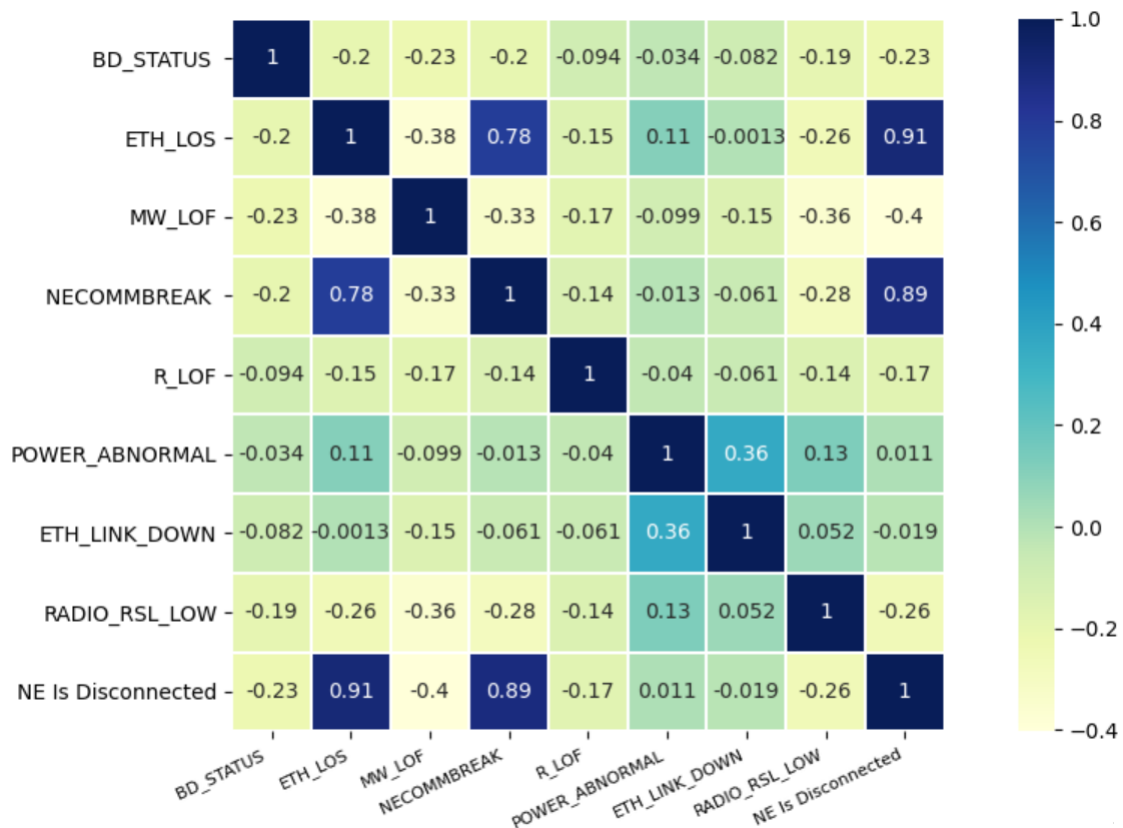


Figure 6.2: Correlation between Transmission and BTS alarm

3. IP EQUIPMENT ALARMS AND BTS ALARM

There are several alarms that demonstrate the IP equipment status in base stations. Using dataset3, the association between IP equipment alarm and a BTS outage alarm is analyzed. Figure 6.3 presents the heatmap to visualize the correlation between IP equipment alarm and BTS alarm. Here the highest correlations are observed between:

- An alarm named with NE is Disconnected looks to be highly correlated with Device Offline and Link Down.
- The rest of alarms have the least correlation with NE is Disconnected. Hence, it is relatively considered as having no direct impact for the BTS outage.

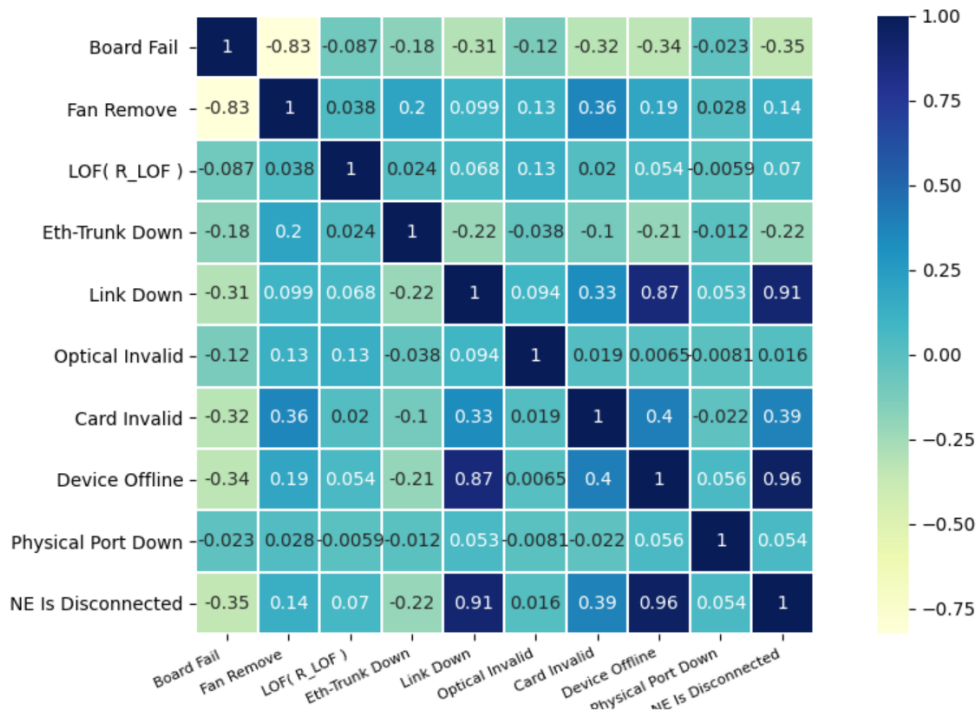


Figure 6.3: Correlation between IP and BTS alarm

6.2 MODELS PERFORMANCE ANALYSIS

A fault localization model using ANN network have been developed using three layers and the performance of the network is evaluated by the performance Metrix such as Accuracy, Mean Square Error (MSE), Mean Absolute Error (MAE), Precision and Recall.

The results were analyzed here on the basis of the output in confusion matrix and time to build the model. Confusion matrix is used in order to evaluate the accuracy of ANN models by allowing to get TP rate, FP rate, precision, recall and F-measure. The detail description of this performance matrix has been discussed in section 4.3.4 of this paper.

Table 6.1: Performance Comparison of FFNN and CFNN Model

Classifier	MSE	MAE	Accuracy	Recall	Precision
FFNN	4.0834	1.843	95.9%	92.25	92.75
CFNN	3.4275	0.634	97.7%	93.05	93.25

The first research question: “which neural network model perform well for fault localization purpose” is answered in the analysis taken. Table 6.1 summarize the performance comparisons of the developed ANN models .

From Table 6.1 it can be observed that cascade forward neural network outperform feed forward neural network. During testing classification using the two neural network architectures , Cascade forward back propagation network shows excellent performance where the MSE and MAE are showing very less error as shown in Figure 6.4. In addition the accuracy shows very good percentage. Feed forward back propagation network shows less performance relative to Cascade forward neural network.

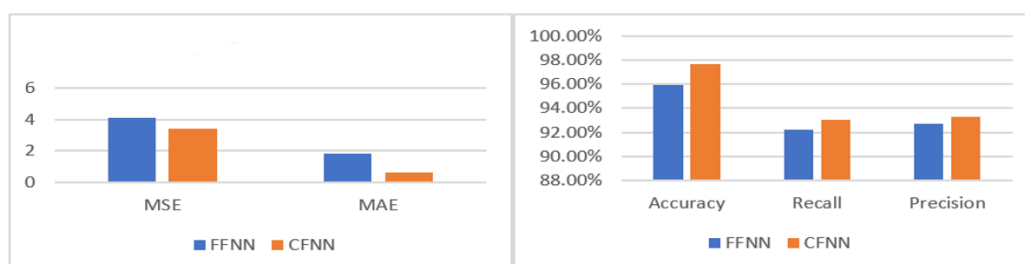


Figure 6.4: Performance Comparison of FFNN and CFNN Model

7 CONCLUSION AND RECOMMENDATIONS

7.1 CONCLUSUION

The thesis work presented an approach for fault management that combines correlation analysis technique and neural networks. The approaches are proposed to automate the existing fault management system process that is being held in Ethio telecom. Automating the fault management system will help the monitoring time while making decisions during trouble ticket creation. Minimizing the service outage time is another benefit of the proposed approach since it helps in fastening the troubleshooting time. The work reported in this paper applied Pearson correlation to find out the possible relations between alarms of the network elements that make up the RAN part of the cellular network. The process of building a fault localization model using two selected neural network architectures as well as the feasibility of using ANN to solve the problem of fault localization is also studied and reported in this paper.

The correlation analysis aimed to analyze the association between network equipment (power equipment, transmission equipment, and IP equipment) malfunction alarms and the BTS outage status alarm. In this study, correlation analysis has been performed using different alarms of the specified network collected from the existing fault management system. In order to perform the correlation analysis, three datasets are prepared and the alarms that are highly connected with a BTS outage alarm are picked based on the correlation results. Heatmap was used as a tool to visualize the correlation analysis. In the first dataset, there are alarms related to power equipment as well as an alarm related to a BTS outage status. Based on the value of the correlation coefficient, power equipment related alarm called LLVD is chosen because it is highly correlated with the NE Disconnected alarm, which represents a BTS outage. In the second dataset, a transmission equipment-related alarm called NECOMMBREAK and ETH Loss is chosen as having the strongest correlation to a BTS outage alarm. From the third dataset, which includes IP equipment and BTS-related alarms, Link Down and Device offline alarms are selected.

In this research, ANN is used to build a fault localization model using alarm names found from the correlation analysis, the microwave link topology data, and the history alarms of the base stations to help the monitoring team during fault management in decision-making process. An experiment was carried out for Ethio telecom RAN. The network was divided into different subareas, each area was represented by one neural network. Two ANN architectures, FFNN and CFNN, are selected for this research. The ANN model incorporated 14 inputs neurons, 29 outputs neurons, and 10 hidden neurons. Each input represented a BTS site and the alarm names selected after correlation analysis and each output represented the initial cause of the fault plus the location of the BTS (site ID).

Python was used as a programming tool to perform the correlation analysis and to build the selected ANN model. It is also used to compare the performance of the two models. NN model's training and testing accuracy have been compared. CFNN, with an accuracy of 97.7% is significantly better than FFNN that has an accuracy of 95.9% as obtained from the ten-fold experimentation technique. CFNN is the best performer model as it is also observed in all performance metrics.

7.2 RECOMMENDATIONS

The developed ANN models could be of great importance to Ethio telecom in simplifying the fault management system by decreasing the burden of the monitoring team and troubleshooting time. The following are some of the recommendations to Ethio telecom and future researchers:

- The correlation analysis results will help Ethio telecom in identifying which network alarms are affecting the BTS.
- The proposed models, if implemented will be more practical solutions to figure out the root cause of the BTS outage along with the location of the fault in terms of BTS site ID.
- This research work is limited to alarms of access part of the neural network, future works may include alarms of other part of cellular network.
- Only two ANN architectures are used and compared in this research but more accurate models could be obtained by trying other machine learning algorithms.

REFERENCES

- [1] S. Wallin and L. Landen, “Telecom alarm prioritization using neural networks,” *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, pp. 1468–1473, 2008.
- [2] M. Nouioua, P. Fournier-Viger, G. He, F. Nouioua, and Z. Min, “A Survey of Machine Learning for Network Fault Management,” *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics*, pp. 1–27, 2021.
- [3] H. Wietgreffe, K.-d. Tuchs, K. Jobmann, G. Carls, P. Fröhlich, W. Nejdil, and S. Steinfeld, “Using Neural Networks for Alarm Correlation in Cellular Phone Networks,” *n Proc. International Workshop on Applications of Neural Networks in Telecommunications*, pp. 1–10, 1997.
- [4] O. P. and J. I., “Automation of Cellular Network Faults,” *Cellular Networks - Positioning, Performance Analysis, Reliability*, no. May 2014, 2011.
- [5] E. Marilly, A. Aghasaryan, S. Betgé-Brezetz, O. Martinot, and G. Delègue, “Alarm correlation for complex telecommunication networks using neural networks and signal processing,” *2002 IEEE Workshop on IP Operations and Management, IPOM 2002*, no. February, pp. 3–7, 2002.
- [6] C. P. Chiba, “Design and Implementation of a Fault Management Service for Heterogeneous Networks using the TINA Network Resource Architecture,” no. December, 2001.
- [7] P. D. Souza, “Advanced Correlation Engine for Fault Identification and Analysis in Network,” vol. 6, no. June, pp. 422–425, 2015.
- [8] S. A. Gutierrez Betancur, “Fault management in TELCO platforms using autonomic computing and mobile agents ,” p. 57, 2011. [Online]. Available: <http://www.bdigital.unal.edu.co/5464/>
- [9] A. C. B. García, L. A. Portes, F. Pinto, and N. Sanchez-Pi, “Real-time alarm management system for emergency situations,” *Studies in Computational Intelligence*, vol. 431, pp. 9–18, 2012.

- [10] P. Froehlich, W. Nejdil, K. Jobmann, and H. Wietgreffe, "Model-based alarm correlation in cellular phone networks," *IEEE International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems - Proceedings*, pp. 197–204, 1997.
- [11] D. S. Kim, H. Shinbo, and H. Yokota, "An alarm correlation algorithm for network management based on root cause analysis," *International Conference on Advanced Communication Technology, ICACT*, pp. 1233–1238, 2011.
- [12] A. K. Arhouma and S. M. Amaitik, "Decision Support System for Alarm Correlation in GSM Networks Based on Artificial Neural Networks," *Conference Papers in Engineering*, vol. 2013, pp. 1–7, 2013.
- [13] A. Mehrabinezhad, D. Dastan, M. R. Shirazi, and H. Pedram, "Rule association based alarm correlation in telecommunication management network (TMN)," *Management Information Systems*, vol. 6, pp. 205–213, 2002.
- [14] A. K. Jagannatham, "Cellular network architecture," <https://www.coai.com/indian-telecom-infocentre/telecom-infrastructurenetworks>, Feb. 2017.
- [15] A. Elouafiq, "Authentication and Encryption in GSM and 3G/UMTS An Emphasis on Protocols and Algorithms," vol. 124, no. 1595, p. 29, 2009.
- [16] M. Vaezi, "Radio Access Network Evolution," no. November, 2019.
- [17] A. Ghayas, "What is a mobile core network?" <https://commsbrief.com/what-is-a-mobile-core-network/>, Feb. 2021.
- [18] O. Jukic and I. Hedi, "Service monitoring and alarm correlations," *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, pp. 317–321, 2012.
- [19] A.T.Boulotos, S.calo and A.finkel, "23 Alarm correlation and fault identification in communication network.pdf."
- [20] D. Mulvey, C. H. Foh, M. A. Imran, and R. Tafazolli, "Cell fault management using machine learning techniques," *IEEE Access*, vol. 7, pp. 124 514–124 539, 2019.

- [21] V. K. Gurbani, D. Kushnir, V. Mendiratta, C. Phadke, E. Falk, and R. State, “Detecting and predicting outages in mobile networks with log data,” *IEEE International Conference on Communications*, 2017.
- [22] A. T. Bouloutas, S. Calo, and A. Finkel, “Alarm Correlation and Fault Identification in Communication Networks,” *IEEE Transactions on Communications*, vol. 42, no. 234, pp. 523–533, 1994.
- [23] R. Harper, “The Application of Neural Networks to Predicting the Root Cause of Service Failures,” pp. 31–35, 2017.
- [24] M. N. Vrahatis, G. D. Magoulas, and K. Parsopoulos, “Introduction to Artificial Neural Networks Training and Applications,” no. October, 2000.
- [25] S. L. Pinjare and E. H. Kumar, “Implementation of Artificial Neural Network Architecture for Image Compression Using CSD Multiplier Implementation of Artificial Neural Network Architecture for Image Compression Using CSD Multiplier,” no. August 2013, 2014.
- [26] K. I. Ahamed, “A Study on Neural Network Architectures,” pp. 1–7, 2016.
- [27] F. G. Furat and T. İbrikçi, “Application of Feed Forward Backpropagation and Cascade Forward Backpropagation Neural Network Algorithms to Detect Pulsar Stars Application of Feed Forward Backpropagation and Cascade Forward Backpropagation Neural Network Algorithms to Detect Pulsar Stars,” no. November 2017, 2019.
- [28] D. S. Badde, A. Gupta, and V. K. Patki, “Cascade and Feed Forward Back propagation Artificial Neural Network Models for Prediction of Compressive Strength of Ready Mix Concrete,” pp. 1–6.
- [29] Y. Zhang, Z. Lin, Y. Kang, R. Ning, and Y. Meng, “A Feed-Forward Neural Network Model For The Accurate Prediction Of Diabetes Mellitus,” vol. 7, no. 8, pp. 151–155, 2018.
- [30] M. H. SAZLI, “A brief review of feed-forward neural networks,” *Communications, Faculty Of Science, University of Ankara*, no. May, pp. 11–17, 2006.

- [31] M. Al-Zewairi, S. Almajali, and A. Awajan, "Experimental evaluation of a multi-layer feed-forward artificial neural network classifier for network intrusion detection system," *Proceedings - 2017 International Conference on New Trends in Computing Sciences, ICTCS 2017*, vol. 2018-January, no. October, pp. 167–172, 2017.
- [32] E. Culurciello, "Learning neural network architectures," <https://towardsdatascience.com/learning-neural-network-architectures-6109cb133caf>, Oct. 2018.
- [33] B. Warsito, R. Santoso, Suparti, and H. Yasin, "Cascade Forward Neural Network for Time Series Prediction," *Journal of Physics: Conference Series*, vol. 1025, no. 1, 2018.
- [34] M. Thilagavathi and S. Abirami, "Cascade-Forward Neural Network in Identification of Plant Species of Desert Based on Wild Flowers," *2018 IEEE International Conference on System, Computation, Automation and Networking, ICSCA 2018*, pp. 1–7, 2018.
- [35] H. Sildir, E. Aydin, and T. Kavzoglu, "Design of feedforward neural networks in the classification of hyperspectral imagery using superstructural optimization," *Remote Sensing*, vol. 12, no. 6, 2020.
- [36] A. Zayegh and N. Al Bassam, "Provisional chapter Neural Network Principles and Applications," 2018. [Online]. Available: www.intechopen.com
- [37] E. Oja, "Unsupervised learning in neural computation," *Theoretical Computer Science*, vol. 287, no. 1, pp. 187–207, 2002.
- [38] S. Kumar and I. Chong, "Correlation analysis to identify the effective data in machine learning: Prediction of depressive disorder and emotion states," *International Journal of Environmental Research and Public Health*, vol. 15, no. 12, 2018.
- [39] P. Schober and L. A. Schwarte, "Correlation coefficients: Appropriate use and interpretation," *Anesthesia and Analgesia*, vol. 126, no. 5, pp. 1763–1768, 2018.
- [40] W. F. Kuhfeld, "Heat Maps : Graphically Displaying Big Data and Small Tables," pp. 1–20, 2017.
- [41] J. M. Twomey and A. E. Smith, "Performance measures, consistency, and power for artificial neural network models," *Mathematical and Computer Modelling*, vol. 21, no. 1-2, pp. 243–258, 1995.

Fault Localization Using Neural Networks for Fault Management Based on Alarm Correlation Analysis: The Case of Ethio telecom

Tsion Ketema

*Department of Electrical and Computer Engineering
Addis Ababa Institute of Technology
Addis Ababa, Ethiopia
ketema33@gmail.com*

Abstract—When malfunction or error appears on a piece of telecom network equipment, they typically produce an alarm and transmits to the FMS, which is then shown to the monitoring team for trouble ticket creation. During the trouble ticketing, the operators may need to collect further information such as relationship or dependency between alarms to ultimately distinguish the root source. But the information on FMS lacks explanation and indication of the root causes, forcing the monitoring teams to manually figure out the root cause and take action, which results in a poor decision making as well as a longer trouble shooting and service outage time. This study focus on studying the association between the network equipment alarms using a correlation analysis technique called Pearson correlation using history alarm data and studying the feasibility of using artificial neural network to build fault localization model to support the monitoring team with decision making. Fault localization models using one specific neural network architecture are built in different literatures. But in this study two neural network architectures, Feed forward neural network (FFNN) and cascade forward neural network (CFNN), are selected to build a model using the data of correlation analysis output, the microwave link topology and the history alarms as an input. Data preparation techniques such as data engineering and feature engineering have been applied to the collected data. After building the models, they are evaluated using commonly used performance metrics such as accuracy and error measurement. Python is used as programming tool to perform the correlation analysis as well as to develop and compare the two neural network models. Experimentation results exhibit that CFNN with an accuracy of 97.7%, is the best model while FFNN achieve 95.9% overall accuracy.

keywords: Alarm correlation analysis, Artificial neural network, Fault management system

I. INTRODUCTION

Telecommunication networks are made up of different types of network equipment that are operationally dependent on one another in order to complete a telecom task. With the use of various network equipment, telecom operators provides fixed line and internet-based services to their customers [1], [2]. But

sometimes a network equipment fails for a variety of causes, including power outage, transmission equipment problem, and connection failures [3], [4]. The failures could result a service outage or interruption. As a result, network equipment should be monitored and managed 24 hours a day, seven days a week, to discover root causes of outages and take corrective action to avoid customer complaints and revenue loss.

Every piece of network equipment is configured to generate an alarm whenever it encounters a fault [5]. A fault is a problem that happens on the installed network equipment's hardware or software. Service failures, severe network degradation, and unplanned disruptive behavior can all be caused by faults [4], [6], [7]. Network equipment generates alarms to describe the faults as stated by the vendor's operators. Telecom operators use a network management system to perform fault management by monitoring the alarms produced by the network equipment. Alarms are displayed on the fault management platform in order for the network monitoring professionals to see the alarms on the fault management platform.

II. PROBLEM DESCRIPTION

In the current Ethio telecom situation, network elements from different BTS sites produce a large volume of alarms per day, and the alarms messages appear uncorrelated from the network element to the FMS. The FMS filter and display the generated alarms to let the monitoring team see the alarms and create a trouble ticket and assign it to the corresponding field technicians. The monitoring teams are grouped or formed to monitor the network equipment based on different types of network components in the BTS site. Due to this, they are responsible to monitor the status of specific network equipment types. But the failure of one network equipment might cause problems for different network equipment and this lets different alarms having the same root cause to be detected at the same time by different teams. On the other hand,

APPENDIX

some alarms might also remain unseen for a long time because of the appearance of dozens of alarms.

The current FMS that is being used by Ethio telecom is based on manual processing and relies on the monitoring team's knowledge. Due to this many efforts are being made by the monitoring team for debugging a BTS outage, especially in the stage of identifying where and what the source is. Some of the existing approach drawbacks are redundant trouble tickets, longer troubleshooting time and longer service outage time.

Therefore, to overcome the mentioned problem building a fault localization model is one solution. To build the model there are different approaches but the main issue is their performance and this paper proposes a fault localization method based on artificial neural network (ANN). Performing an alarm correlation analysis is very important to diagnose the relationship between alarms and identify the parent and the child alarm before building the fault localization model.

There are different types of ANN architectures to build the model. So the purpose of this research will be to perform alarm correlation analysis and build a fault localization model using selected neural network architectures and compare the performance of the model using Performance Metrics.

III. CELLULAR NETWORK FAULT MANAGEMENT

A. Base station outage

A base station is a system in a mobile communication network that houses radio receivers and is used for wireless communication between users and network providers that is under the control of BSC or radio network controller (RNC) and then the exchange. Base station is mainly composed of BTS, antennas and physical support for antennas. BTS is the radio and it produces energy in the form of electricity. The electricity is carried up to the second component of the base station which is the antennas, over thick coaxial cables. The antenna is the device that converts the electricity to electromagnetic waves [4], [8].

To make communication between two or more persons through a telecommunication network, mobile switch makes a connection to the base station. The base station has to be connected back to mobile switch. The mobile switch is capable of keeping track of users moving around. The connection between base station and mobile switch is called backhaul. If there is a fiber between those two physical locations, they use fiber to connect the BS back to the mobile switch. But if there is no fiber available, point to point radio backhaul will be used. We might have the communications, the backhaul from the BS back to the mobile switch go through multiple different towers with point to point radio systems before we finally get back to a mobile switch [4], [8].

Base station sites are composed of different hardware elements: modems, switching units, cables, cooling elements, energy elements, etc. These elements are interconnected as a result a failure in one element will probably affect a smooth running of the hardware or make it break down. For example, the failure of the air conditioning system will affect all the hardware installed in the room. In this study cause of base station outage is generalized as IP equipment failure, power failure, transmission equipment failure.

Mobile network outages occur due to various reasons. The main reasons for the outage is due to Base station faults. When there is a mobile network outage, the mobile network operators' customers will be unable to use the data, voice and any means of communication functions through mobile.

B. Fault Management System

A telecommunication network consists of a number of interconnected components like switch, transmission equipment, routers and RNC. These components can produce network alarms to demonstrate sort of abnormal situation [3], [9], [10]. These alarms further help to monitor the status and stability of the network element and the services carried over it using fault management system (FMS). Fault management is one part of network management to collect and analyze alarms. The network management is the collection of tasks performed to maximize availability, performance, security and control of a network and its resources [7], [11]. Fault management mainly deals with remotely controlling or monitoring the status of network devices to avoid a potential fault.

Fault management systems use network alarms to determine the nature and severity of the faults and to drive the fault resolution. A fault is a malfunction that occurs on a network and may cause errors. A fault can have various consequences such as making a network service unavailable or degrading its performance [7], [9], [12], [10]. These network faults are represented by alarms and the number of produced alarms varies greatly. From a logical point of view fault management system collects network events and filters events which are alarms and group alarms by common fault cause and lastly prioritize the fault resolution [1], [10], [13]. During network fault management, the monitoring team maintains and examines error logs, accepts and acts upon error detection notifications, traces and identifies faults, carries out sequences of diagnostic tests and finally the fault will be corrected by the operation and maintenance team. Managing faults in a telecommunication network can be conceptually divided into three phases [9], [10], [14].

- Detection;
- Fault localization;
- Repairing.

APPENDIX

IV. CORRELATION ANALYSIS AND FAULT LOCALIZATION

This research paper has proposed a combination of two approaches to simplify the Process of fault management. One is the alarm correlation analysis part and the other is modeling a fault localization using artificial neural network and identifying a well performing neural

A. Alarm Correlation Analysis

Correlation analysis is a technique that deals with finding the association between two or more variables [15]. The correlation analysis in this study is not performed as one task of data preprocessing rather it is considered as a technique to figure out the association between network equipment alarms. Hence, these portion of the research is mainly performed to identify the association between the alarms and classify the alarms as parent and child alarm. The relationship or the correlation between variables is determined numerically by a decimal value called correlation coefficient [15], [16]. Among many types of correlation coefficients, Pearson correlation coefficient(r) is the one used here to understand and analyze the strength of correlations between alarms as it is the most often used one.

The value of the correlation coefficient varies between +1 and -1 in terms of the strength of the association. Based on the value of the coefficient, the correlation strength can be determined. A value of 1 shows that the two variables are perfectly associated or strongly correlated. As the correlation coefficient value goes towards 0, the relationship between the two variables will be weaker, whereas a negative sign indicates a negative correlation. A correlation coefficient with a higher number value indicates a strong correlation between two variables and a lower value indicates otherwise.

To calculate Pearson's correlation coefficient first, the covariance of the two variables and the standard deviation of each data sample should be calculated and then divided the covariance by the product of standard deviation.

The formula shown in equation 1 is used to compute the Pearson correlation coefficient between two variables X and Y . [15]. In order to perform correlation analysis, the following specific tasks have been accomplished.

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 (y_i - \bar{y})^2}} \quad (1)$$

Where r is the correlation coefficient, n is the sample size, x_i and y_i are the i^{th} data values, and \bar{x}, \bar{y} are the mean values.

1) *Data Collection:* History alarm data is collected from the Huawei radio access network sites network management system. The data includes the fields such as Site Name, Alarm Name, Event Time and Severity

2) *Data Preprocessing:* The preprocessing phase is used to clean and organize the alarm data to prepare the data in any way that is suitable to perform correlation analysis. Categorizing alarms, aggregation of data, data cleaning and attributes selection and feature extraction are the tasks used to preprocess the alarm data.

3) *Correlation Analysis:* After preprocessing the alarm data, identifying the alarm that have strong impacts on BTS outage will take place using a correlation analysis technique. Pearson correlation coefficient is adopted to discover the relationship between alarms. The Pearson correlation coefficient value is used to figure out the strength of the relationship between alarms [16].

Python programming language is used in this research to calculate the Pearson's correlation coefficient with a built in function called `pearsonr()`. The result of the calculation or the result of the correlation coefficient can be interpreted to understand the relationship.

B. Fault localization

Fault localization is also called Fault diagnosis which deals with pinpointing one or more causes of problems along with their specific location to the point where corrective action can be taken [3], [5]. This is also referred to as fault isolation. This diagnosis can be performed by analyzing and correlating the messages sent by network equipment's as an alarm. Hence it becomes a huge task for a network manager to manually sit and analyze each of these alarms, fault localization model using neural networks is proposed in this paper to segregate them based on their micro wave link topology to make a correct decision and take necessary actions to get rid of the problem.

Currently, fault localization is being performed manually by an expert or a monitoring team experienced in managing communication networks based on network disorder symptoms or alarms displayed on a fault management system. For time critical systems it is required that system must be up and running each and every minute. However, The monitoring team face difficulties in problem management due to the hundreds of alarms issued by network devices. As a result, the technicians are overburdened with thousands of alarms and are unable to investigate them all.

V. PROPOSED ARTIFICIAL NEURAL NETWORK MODEL

Artificial neural network(ANN) is one of the approaches in the field of artificial intelligence. It was inspired by the computational mechanism of biological nerve networks. ANN is a computer program that mimics how the human brain does a task. It is composed of a large number of highly interconnected information-processing elements called neurons to solve specific problems. A neuron is a computational element, and is the building block of an ANN [17], [18]. The ANN model consists of three basic elements [18], [19], [20] :

APPENDIX

- A set of connecting links, each of which is characterized by a weight;
- An adder for summing the input signals, weighted by the respective weight of the neuron;
- An activation function for limiting the amplitude of the output of a neuron.

The most common type of ANN consists of three layers: input, hidden, and output. The raw data fed into the network is represented by the activity of the input units, and each neuron has a set of inputs. Each link between the input and the hidden layer is represented by synaptic weights. The activities of the input units and the weights on the links between the input and hidden units determine the activity of each hidden unit. The output layer generates output based on the input, hidden unit activity, and hidden/output unit weights [17], [19], [20].

The way neurons are organized in a neural network is referred to as network topology or architecture. Neural network architectures are roughly divided into feed-forward and feedback architectures [18], [20]. Signals in feed-forward networks flow in one direction only, whereas signals in feedback networks can flow in both directions. The architecture of ANN used in this study is feed-forward networks and depending on the type of the connections between the neurons, it is further grouped as [17], [21], [22], [23]:

- Feed forward artificial neural network (FFNN).
- Cascade forward artificial neural network (CFNN).

A. Feed-Forward Neural Network

FFNN are classified as single layer and Multi-Layer Feed-forward network based on the number of layers [24]. In a multi-layer FFNN, there is at least one layer of hidden neurons between the input and output layers [21], [22], [23]. These architectures allow signals to travel from input to output in one direction only, hence there is no feedback. The signal is carried out from the input layer to the hidden layer in the weighted form. The activation function on the layer processes signals that enter the neurons in the hidden layer [20], [24], [25]. In the hidden layer, the weighted total of each neuron's output is then sent to the output layer. This layer's activation function analyses the incoming signal before sending it to the output layer. Typically, the output layer's activation function is identity mapping, which ensures that the output received in this layer is identical to the incoming signal.

Neural network architectures are trained through various learning algorithms for producing most efficient solutions. There are different types of algorithms to train a neural network. Some of them are gradient descent, newton method, conjugate gradient, quasi newton method and Levenberg-Marquardt. In this paper, ANN model with gradient descent training algorithm is built. To apply gradient descent, back propagation learning algorithm is used. Among many

other learning algorithms, back-propagation algorithm is the most popular and the mostly used one for the training of feed-forward neural networks.

Backpropagation is the process of updating the weights of the network in order to reduce the error in prediction as the main intention of training the network is to minimize a cost function [18], [21], [22]. The procedure used to carry out the learning process involves the following steps [17], [23], [24], [26].

- 1) Initialization: Initialize the weight randomly.
- 2) Forward computation: Train the model using the training set by propagating the input signals through the network layer by layer.
- 3) Backpropagation. Compute the error signals corresponding to each neuron.

B. Cascade-Forward Neural Network

CFNN is the other classes of the forward neural network. CFNN is almost the same as that of (FFNN). The main difference is that, in case of CFNN, there is direct link between the input layer and the output layer, in addition to the indirect link through the hidden layer as shown in Figure 3.2. In CFNN, each neuron in the input layer is attached to each neuron in the hidden layer as well as each neuron in the output layer [22], [27], [28].

The developed ANN model will be used as decision support system to find the cause of the alarms and the location of the alarms in terms of the BTS site ID. In order to achieve this goal, the following specific tasks have been accomplished.

1) *Preparing The Dataset:* To build a useful fault localization model alarms coming from all the devices forming the network are needed. In addition to alarms, the association between alarms of each equipment as well as topological information or network topology is important. Alarms of the network equipment and topological information are gathered from the existing fault management system database. For this study, only Base station alarms that demonstrate power problem, transmission problem, Ip problem, and BTS are extracted to be used as an input for the proposed model. Preprocessing the data in a way that is suitable for developing the proposed model involves both: topsep=0ex

- Data engineering;
- Feature engineering.

Data engineering: is the process of converting raw data into prepared data. In order to prepare the data the following tasks are performed in this study. topsep=0ex

- **Categorizing alarms:** The collected alarm data is composed of the base station site ID, the alarm name, alarm ID, Network equipment type, Region, occurrence time and cleared time. To prepare the alarm data for the proposed model, the topological data is used. Since base stations are connected to each other via multiplexing transmission system. Network elements of base

APPENDIX

station sites who have topological relationship regarding with their microwave radio transmission link is extracted using their site ID. Then selected alarms of base station sites which are under the same microwave links or who have topological relationships is categorized or gathered in one cluster or group.

- **Aggregation of Data:** once BTS sites are gathered in one group or cluster, alarms of the selected network equipment's will be aggregated based on their occurrence and cleared time. The base station sites which are under the same microwave links and whose occurrence and cleared time fall in the same time interval are merged in one cluster. The time interval is considered as cluster borders. This approach involves identifying patterns of alarms by considering the time interval. That is, the instances to aggregate are defined through temporal window time.
- **Attributes selection:** This step is mainly used to identify and remove redundant and irrelevant information. Therefore, after aggregating the alarm data selecting the useful alarm attributes to identify frequent pattern rules is very important. Even though the alarm has many attributes only the site ID and the alarm name is selected here using filter method. The patterns or rules are extracted for the purpose of identifying the root cause and fault localization.

Feature engineering: is the other task involved in data preprocessing steps and its main purpose is to change the prepared data into suitable format to create the features expected by the machine learning model. This includes changing the data type of the new features into numerical data type to be used by the model during training and testing phase.

2) *Developing The Supervised ANN Model:* Among all the available architectures, Feed forward neural network and cascade forward neural network is chosen because in literatures this two are the most commonly used architecture for classification problems. The prepared data is divided into the training and test samples and passed this data to the selected neural network architectures. 80% of the sample is used as training samples and 20% was used as testing sample.

A three layer neural network is considered sufficient for this study and Python program is used for developing neural network model. Python provides necessary functions to quickly create, train and test the neural network. It also provides ready to use training algorithms.

As mentioned before, the west part of Addis Ababa has been chosen to be a case study and this part is divided into different subareas containing different group of BTS sites regarding with their microwave link. The one selected for this study or experiment contains 8 group of BTS sites. A training sample of 104 patterns, each pattern formed by input and output

vectors, has been prepared for training.

Both CFNN and FFNN is composed of 14 input nodes, 10 hidden nodes, and 27 output node. The number of input nodes was the number of alarm names and the number of site IDs in the dataset. The number of output nodes was the number of the initial causes (power, IP, and transmission) plus the number of site IDs in the dataset. The number of neurons in the hidden layer is chosen by the model's performance. It was chosen in such a way that the model's training could be completed quickly and accurately. During the training phase, the maximum number of epochs is set to 100, and the network is configured to train until the maximum number of epochs is reached, at which point network performance is evaluated. The network configuration is then modified based on network performance by increasing or decreasing the hidden nodes. The neural network's weights and biases were set using the gradient descent back-propagation algorithm.

VI. RESULTS AND DISCUSSION

A. Results of Correlation Analysis

The study has exploited correlation analysis approaches to identify relevant alarms of base station network equipment in the dataset which has a significant impact on the BTS down status alarm. `pandas.corr()` function is used to calculate person correlation coefficient. The result is then visualized using a heatmap. heatmap is a method of graphically representing numerical data where the value of each data point is indicated using colors. A heatmap contains various shades of colors for each value to be plotted. Usually, the darker shades of the chart represent lower values than the lighter shade. Pearson correlation is applied on the three datasets prepared previously on this paper for the correlation analysis purpose. The interpretation of the heatmap for each dataset is discussed separately. Correlation analysis between:

1) POWER EQUIPMENT ALARMS AND BTS ALARM

There are several alarms that demonstrate the power equipment status in base stations. Using dataset1(power equipment alarms and bts alarm), the association between power equipment alarm and the alarm that demonstrate BTS outage is analyzed. Using heatmap to visualize the correlation between power equipment alarm and BTS alarm, the highest correlations are observed between:

- An alarm named with NE is Disconnected looks to be highly correlated with LLVD and BUS BAR undervoltage
- BUS BAR under voltage looks to be highly correlated with LLVD. But based on their functional behavior this two alarms get produced in sequence.

APPENDIX

- The rest of alarms have the least correlation with BTS. Hence, it is considered as having no direct impact for the BTS outage.

But here the LLVD alarm is selected as the one which has the highest impact on the BTS outage.

2) TRANSMISSION EQUIPMENT ALARMS AND BTS ALARM

There are several alarms that demonstrate the transmission equipment status in base stations. Using dataset2, the association between transmission equipment alarm and the BTS alarm that demonstrate BTS outage is analyzed. Using heatmap to visualize the correlation between transmission equipment alarm and BTS alarm, the highest correlations are observed between:

- An alarm named with NE is Disconnected looks to be highly correlated with NE COMMUNICATION BREAK and ETH-LOS.
- The rest of alarms have the least correlation with NE is Disconnected. Hence, it is relatively considered as having no direct impact for the BTS outage.

3) IP EQUIPMENT ALARMS AND BTS ALARM

There are several alarms that demonstrate the IP equipment status in base stations. Using dataset3, the association between IP equipment alarm and a BTS outage alarm is analyzed. Using heatmap to visualize the correlation between IP equipment alarm and BTS alarm, the highest correlations are observed between:

- An alarm named with NE is Disconnected looks to be highly correlated with Device Offline and Link Down.
- The rest of alarms have the least correlation with NE is Disconnected. Hence, it is relatively considered as having no direct impact for the BTS outage.

B. Models Performance Analysis

A fault localization model using ANN network have been developed using three layers and the performance of the network is evaluated by the performance Matrix such as Accuracy, Mean Square Error (MSE), Mean Absolute Error (MAE), Precision and Recall.

The results were analyzed here on the basis of the output in confusion matrix and time to build the model. Confusion matrix is used in order to evaluate the accuracy of ANN models by allowing to get TP (True positive) rate, FP (False positive) rate, precision, recall and F-measure.

TABLE I
PERFORMANCE COMPARISON OF FFNN AND CFNN MODEL

Classifier	MSE	MAE	Accuracy	Recall	Precision
FFNN	4.0834	1.843	95.9%	92.25	92.75
CFNN	3.4275	0.634	97.7%	93.05	93.25

“which neural network model perform well for fault localization purpose” is answered in the analysis made in this study. Table 1 summarize the performance comparisons of the developed ANN models .

From Table 1 it can be observed that cascade forward neural network outperform feed forward neural network. During testing classification using the two neural network architectures , Cascade forward back propagation network shows excellent performance where the MSE and MAE are showing very less error as shown in Figure 1. In addition the accuracy shows very good percentage. Feed forward back propagation network shows less performance relative to Cascade forward neural network.

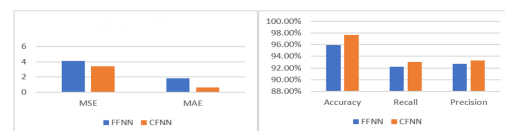


Fig. 1. Performance Comparison of FFNN and CFNN Model

REFERENCES

- [1] S. Wallin and L. Landen, “Telecom alarm prioritization using neural networks,” *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, pp. 1468–1473, 2008.
- [2] M. Nouioua, P. Fournier-Viger, G. He, F. Nouioua, and Z. Min, “A Survey of Machine Learning for Network Fault Management,” *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics*, pp. 1–27, 2021.
- [3] H. Wietgreffe, K.-d. Tuchs, K. Jobmann, G. Carls, P. Fröhlich, W. Nejd, and S. Steinfeld, “Using Neural Networks for Alarm Correlation in Cellular Phone Networks,” *n Proc. International Workshop on Applications of Neural Networks in Telecommunications*, pp. 1–10, 1997.
- [4] O. P. and J. I., “Automation of Cellular Network Faults,” *Cellular Networks - Positioning, Performance Analysis, Reliability*, no. May 2014, 2011.
- [5] E. Marilly, A. Aghasaryan, S. Betgé-Brezetz, O. Martinot, and G. Delègue, “Alarm correlation for complex telecommunication networks using neural networks and signal processing,” *2002 IEEE Workshop on IP Operations and Management, IPOM 2002*, no. February, pp. 3–7, 2002.
- [6] C. P. Chiba, “Design and Implementation of a Fault Management Service for Heterogeneous Networks using the TINA Network Resource Architecture,” no. December, 2001.
- [7] P. D. Souza, “Advanced Correlation Engine for Fault Identification and Analysis in Network,” vol. 6, no. June, pp. 422–425, 2015.
- [8] M. Vaezi, “Radio Access Network Evolution,” no. November, 2019.
- [9] S. A. Gutierrez Betancur, “Fault management in TELCO platforms using autonomic computing and mobile agents ,” p. 57, 2011. [Online]. Available: <http://www.bdigital.unal.edu.co/5464/>

APPENDIX

- [10] A. K. Arhouma and S. M. Amaitik, "Decision Support System for Alarm Correlation in GSM Networks Based on Artificial Neural Networks," *Conference Papers in Engineering*, vol. 2013, pp. 1–7, 2013.
- [11] O. Jukic and I. Hedi, "Service monitoring and alarm correlations," *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, pp. 317–321, 2012.
- [12] A.T.Boulotos, S.calo and A.finkel, "23 Alarm correlation and fault identification in communication network.pdf."
- [13] D. Mulvey, C. H. Foh, M. A. Imran, and R. Tafazolli, "Cell fault management using machine learning techniques," *IEEE Access*, vol. 7, pp. 124 514–124 539, 2019.
- [14] V. K. Gurbani, D. Kushnir, V. Mendiratta, C. Phadke, E. Falk, and R. State, "Detecting and predicting outages in mobile networks with log data," *IEEE International Conference on Communications*, 2017.
- [15] S. Kumar and I. Chong, "Correlation analysis to identify the effective data in machine learning: Prediction of depressive disorder and emotion states," *International Journal of Environmental Research and Public Health*, vol. 15, no. 12, 2018.
- [16] P. Schober and L. A. Schwarte, "Correlation coefficients: Appropriate use and interpretation," *Anesthesia and Analgesia*, vol. 126, no. 5, pp. 1763–1768, 2018.
- [17] R. Harper, "The Application of Neural Networks to Predicting the Root Cause of Service Failures," pp. 31–35, 2017.
- [18] M. N. Vrahatis, G. D. Magoulas, and K. Parsopoulos, "Introduction to Artificial Neural Networks Training and Applications," no. October, 2000.
- [19] S. L. Pinjare and E. H. Kumar, "Implementation of Artificial Neural Network Architecture for Image Compression Using CSD Multiplier Implementation of Artificial Neural Network Architecture for Image Compression Using CSD Multiplier," no. August 2013, 2014.
- [20] K. I. Ahamed, "A Study on Neural Network Architectures," pp. 1–7, 2016.
- [21] F. G. Furat and T. Ibrıkçi, "Application of Feed Forward Backpropagation and Cascade Forward Backpropagation Neural Network Algorithms to Detect Pulsar Stars Application of Feed Forward Backpropagation and Cascade Forward Backpropagation Neural Network Algorithms to Detect Pulsar Stars," no. November 2017, 2019.
- [22] D. S. Badde, A. Gupta, and V. K. Patki, "Cascade and Feed Forward Back propagation Artificial Neural Network Models for Prediction of Compressive Strength of Ready Mix Concrete," pp. 1–6.
- [23] Y. Zhang, Z. Lin, Y. Kang, R. Ning, and Y. Meng, "A Feed-Forward Neural Network Model For The Accurate Prediction Of Diabetes Mellitus," vol. 7, no. 8, pp. 151–155, 2018.
- [24] M. H. SAZLI, "A brief review of feed-forward neural networks," *Communications, Faculty Of Science, University of Ankara*, no. May, pp. 11–17, 2006.
- [25] M. Al-Zewairi, S. Almajali, and A. Awajan, "Experimental evaluation of a multi-layer feed-forward artificial neural network classifier for network intrusion detection system," *Proceedings - 2017 International Conference on New Trends in Computing Sciences, ICTCS 2017*, vol. 2018-January, no. October, pp. 167–172, 2017.
- [26] E. Culuiello, "Learning neural network architectures," <https://towardsdatascience.com/learning-neural-network-architectures-6109cb133caf>, Oct. 2018.
- [27] B. Warsito, R. Santoso, Suparti, and H. Yasin, "Cascade Forward Neural Network for Time Series Prediction," *Journal of Physics: Conference Series*, vol. 1025, no. 1, 2018.
- [28] M. Thilagavathi and S. Abirami, "Cascade-Forward Neural Network in Identification of Plant Species of Desert Based on Wild Flowers," *2018 IEEE International Conference on System, Computation, Automation and Networking, ICSCA 2018*, pp. 1–7, 2018.