REPUBLIC OF TURKEY
ISTANBUL GELISIM UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

Department of Electrical-Electronic Engineering

DETECTION AND LOCALIZATION OF ENERGY THEFT IN DISTRIBUTION NETWORKS USING ARTIFICIAL INTELLIGENCE NEURAL NETWORKS

Master Thesis

Ali Hawi Mezban MEZBAN

Supervisor

Supervisor: Asst.Prof. Dr. Mahmoud HK ALDABABSA

Co-Supervisor: Asst. Prof. Dr. Khalid O.MOH. YAHYA

Istanbul – 2023

THESIS INTRODUCTION FORM

Name and Surname : Ali Hawi Mezban MEZBAN

Language of the Thesis : English

Name of the Thesis : DETECTION AND LOCALIZATION OF ENERGY THEFT IN DISTRIBUTION NETWORKS USING ARTIFICIAL INTELLIGENCE NEURAL NETWORK

Institute : Istanbul Gelisim University Institute of Graduate Studies

Department : Electrical-Electronic Engineering

Thesis Type : Master

Date of the Thesis : 07.07.2023

Page Number : 93

Thesis Supervisors :

1. Asst. Prof. Dr. MAHMOUD HK. ALDABABSA
2. Asst. Prof. Dr. Khalid O.MOH. YAHYA

Index Terms : Theft Energy, Neural Network, Distribution System, Transformer, theft current, Drop voltage.

Turkish Abstract : Bu çalışma, dağıtım ağlarında yaygın olan teknik olmayan kayıpları, özellikle enerji kaçakçılığını ve hırsızlığı araştırıyor. Yapay zeka nöron ağı ve ileri yayılım yöntemi kullanarak hırsızlık olaylarının doğru tespiti ve lokalizasyonu için yeni bir yaklaşım önermektedir. Akıllı enerji sayaçlarından ve merkezi bir sunucuya bağlı bilgi işlem biriminden oluşan simüle edilmiş bir akıllı ağ kullanılır. Yük verileri, gerilim düşümü ölçümleri ve enerji akışı verilerinin analizi yoluyla teknik kayıplar belirlenir ve optimum gerilim düşümü değerleri hesaplanır. MATLAB'de uygulanan önerilen nöron ağı algoritması, hırsızlık konumlarını belirlemek için ideal ve gerçek voltaj düşüşlerini karşılaştırır.

Endüstri standardı denklem tabanlı algoritmalarla karşılaştırmalı analiz, nöron ağı yaklaşımının üstün algılama doğruluğunu gösterir. Önceden belirlenmiş voltaj düşüş değerlerine dayalı sabit algoritmaların aksine, nöron ağı değişen yük koşullarına uyum sağlayarak sağlam ve güvenilir bir hırsızlık tespit mekanizması sunar. Beklenen verileri kullanarak nöron ağının sürekli eğitimi, optimum performansı sürdürmek için gereklidir. İlgili ağ verilerini ve müşteri yük profillerini içeren düzenli güncellemeler, hırsızlık tespit doğruluğunu ve verimliliğini artırabilir.

Bu çalışmanın bulguları, dağıtım şebekelerinde enerji hırsızlığı ve dolandırıcılıkla mücadelede devam eden çabalara katkıda bulunmaktadır. Önerilen nöron ağı tabanlı metodoloji, enerji sağlayıcılarını teknik olmayan kayıpları etkili bir şekilde azaltma konusunda güçlendirerek, hassas hırsızlık lokalizasyonu için umut verici bir çözüm sunar. Gelecekteki araştırmalar, nöron ağının eğitim sürecini daha da iyileştirmek için yenilikçi teknikleri keşfederek, gelişmiş genel performans ve daha yüksek tespit oranları hedefliyor.

Distribution List : 1. To the Institute of Graduate Studies of Istanbul Gelisim University

2. To the National Thesis Center of YÖK (Higher Education Council)

Signature

Ali MEZBAN

REPUBLIC OF TURKEY
ISTANBUL GELISIM UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

Department of Electrical-Electronic Engineering

DETECTION AND LOCALIZATION OF ENERGY THEFT IN DISTRIBUTION NETWORKS USING ARTIFICIAL INTELLIGENCE NEURAL NETWORKS

Master Thesis

Ali Hawi Mezban MEZBAN

Supervisor

Supervisor: Asst. Prof. Dr. Mahmoud HK. ALDABABSA

Co-Supervisor: Asst. Prof. Dr. Khalid O.MOH. YAHYA

Istanbul – 2023

DECLARATION

I hereby declare that in the preparation of this thesis, scientific ethical rules have been followed, the works of other persons have been referenced in accordance with the scientific norms if used, there is no falsification in the used data, any part of the thesis has not been submitted to this university or any other university as another thesis.

Ali Hawi MEZBAN

…./…./2023

TO ISTANBUL GELISIM UNIVERSITY

THE DIRECTORATE OF SOCIAL SCIENCES INSTITUTE

The thesis study of Energy Theft in Distribution Networks titled Detection and Localization of Energy Theft in Distribution Networks using Artificial Intelligence Neural Networks has been accepted as MASTER THESIS in the Department of Electrical-Electronic Engineering by our jury.

Director	*Prof. DrMahmoud H. K. ALDABABSA* (Supervisor)
Member	*Prof. Dr. Yusuf Gürcan ŞAHİN*
Member	*Assoc. Prof. Dr. Mohammed SALEM*

APPROVAL

I approve that the signatures above signatures belong to the aforementioned faculty members.

… / …. / 2023

Signature

Prof. Dr. Izzet GUMUS

Director of the Institute

SUMMARY

This study investigates the pervasive issue of non-technical losses, specifically energy fraud, and theft, in distribution networks. It proposes a new approach for the accurate detection and localization of theft incidents using an artificial intelligence neuron network and the forward propagation method. A simulated smart network is utilized, comprising smart energy meters and a central server-connected information processing unit. Technical losses are determined and optimal voltage drop values are calculated through analysis of load data, voltage drop measurements, and energy flow data. The proposed neuron network algorithm in MATLAB compares ideal and actual voltage dips to identify theft locations.

Comparative analysis with industry-standard equation-based algorithms demonstrates the superior detection accuracy of the neuron network approach. Unlike fixed algorithms based on predetermined voltage drop values, the neuron network exhibits adaptability to changing load conditions, offering a robust and reliable theft detection mechanism. Continuous training of the neuron network using anticipated data is essential for sustaining optimal performance. Regular updates incorporating relevant network data and customer load profiles can enhance theft detection accuracy and efficiency.

The findings of this study contribute to the ongoing efforts in combating energy theft and fraud in distribution networks. The proposed neuron network-based methodology provides a promising solution for precise theft localization, empowering energy providers to effectively mitigate non-technical losses. Future research can explore innovative techniques to further improve the neuron network's training process, aiming for enhanced overall performance and higher detection rates.

Keywords: Theft Energy, Neural Network, Distribution System, Transformer, theft current, Drop voltage.

ÖZET

Bu çalışma, dağıtım ağlarında yaygın olan teknik olmayan kayıpları, özellikle enerji kaçakçılığını ve hırsızlığı araştırıyor. Yapay zeka nöron ağı ve ileri yayılım yöntemi kullanarak hırsızlık olaylarının doğru tespiti ve lokalizasyonu için yeni bir yaklaşım önermektedir. Akıllı enerji sayaçlarından ve merkezi bir sunucuya bağlı bilgi işlem biriminden oluşan simüle edilmiş bir akıllı ağ kullanılır. Yük verileri, gerilim düşümü ölçümleri ve enerji akışı verilerinin analizi yoluyla teknik kayıplar belirlenir ve optimum gerilim düşümü değerleri hesaplanır. MATLAB'de uygulanan önerilen nöron ağı algoritması, hırsızlık konumlarını belirlemek için ideal ve gerçek voltaj düşüşlerini karşılaştırır.

Endüstri standardı denklem tabanlı algoritmalarla karşılaştırmalı analiz, nöron ağı yaklaşımının üstün algılama doğruluğunu gösterir. Önceden belirlenmiş voltaj düşüş değerlerine dayalı sabit algoritmaların aksine, nöron ağı değişen yük koşullarına uyum sağlayarak sağlam ve güvenilir bir hırsızlık tespit mekanizması sunar. Beklenen verileri kullanarak nöron ağının sürekli eğitimi, optimum performansı sürdürmek için gereklidir. İlgili ağ verilerini ve müşteri yük profillerini içeren düzenli güncellemeler, hırsızlık tespit doğruluğunu ve verimliliğini artırabilir.

Bu çalışmanın bulguları, dağıtım şebekelerinde enerji hırsızlığı ve dolandırıcılıkla mücadelede devam eden çabalara katkıda bulunmaktadır. Önerilen nöron ağı tabanlı metodoloji, enerji sağlayıcılarını teknik olmayan kayıpları etkili bir şekilde azaltma konusunda güçlendirerek, hassas hırsızlık lokalizasyonu için umut verici bir çözüm sunar. Gelecekteki araştırmalar, nöron ağının eğitim sürecini daha da iyileştirmek için yenilikçi teknikleri keşfederek, gelişmiş genel performans ve daha yüksek tespit oranları hedefliyor.

anahtar kelimeler: Hırsızlık Enerjisi, Sinir Ağı, Dağıtım Sistemi, Trafo, kaçak akım, Düşme gerilimi.

TABLE OF CONTENTS

CHAPTER ONE

PURPOSE OF THE THESIS

CHAPTER TWO

LOSSES AND METERS ELECTRICAL ENERGY

CHAPTER THREE

THEFT AND FRAUD IN DISTRIBUTION NETWORK

CHAPTER FOUR

SYSTEM SIMULATION

CHAPTER FIVE

RESULTS AND COMPARISON

CHAPTER SIX

CONCLUSIONS AND REFERENCE

ABBREDIVATIONS

AMI	**:**	Advanced Measurement Infrastructure
IOT	**:**	Internet of Things
SVM	**:**	Support Voctor machines
OPF	**:**	Optimum-Path Forest
KPCA	**:**	Harmony Search
GMM	**:**	Gaussian Matrix Mixtury
LSTM	**:**	Long Short Term Momroy
MLP	**:**	Multi Layer Percptrons
LT	**:**	Line Transmission
NTL	**:**	NON Technical Losses
DG	**:**	Distributed Generators
Kwh	**:**	Kilo Watt Hour
AMR	**:**	Automatic Meter Reading
LM	**:**	Levenberg-Marquardt
FFNN	**:**	Feed-Forword Neural Network
GN	**:**	Gauss Newten
BFGN	**:**	Broyden Fletcher Goldfarb Shanno
NBN	**:**	Neuron by Neuron
NN	**:**	Neural Network

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Electric energy is considered one of humanity's most essential and greatest innovations in the field of technology, as it has become an essential part of our lives that we cannot do without. So we have to study how to reduce losses in the sector from generation to transmission and distribution. Electric power has two types of losses, one of which is technical losses, which are divided into fixed losses such as iron losses that can be calculated and determined industrially, and variable losses with an increase in the load current, such as copper losses, which can also be measured and determined according to the amount of the prescribed load current Henriques, H. O (2020). The second type of loss is non-technical loss, which is the consumption of electrical energy without bills by way of energy theft or fraud in the energy meter. Non-technical losses are currently among the most common problems facing the electricity distribution sector. Where the process of identifying and controlling these losses or the possibility of detecting them is one of the difficult and costly matters (Nizar, A. H. et al 2008) – (Nagi, J. et al 2009). Energy theft or fraud in the meters exposes energy companies to large financial losses Ali, S., Yongzhi, M., & Ali, W. (2023), and this matter is not limited to developing countries only but includes most countries of the world, even the most advanced ones. A recently released report shows the number of financial losses for energy companies in the world due to non-technical losses, which amount to $96 billion annually LLC, N. (2017) at the level of distribution networks. These losses also include the side effects of excess electrical loads that are not calculated within the designed capacity of networks and transformers. Distribution, which means that there will be breakdowns, an increase in the cost of maintenance, and the unreliability of the network (Abdulkareem, A. 2016) - (Dike, D. et al 2015) and this will lead to an increase in the cost of bills for legal customers. Therefore, electricity companies usually assign field maintenance teams to detect and address violations of distribution networks and fraud in energy meters. However, the cost of this work is very high and increases significantly with the expansion of the distribution network. Consequently, determining the amount of non-technical losses is both expensive and challenging. This issue is a major concern for electric power companies as it results in a substantial loss of investment returns and poses difficulties in containment.

Recently, progress has been made in the identification and detection of losses through various applications. Nta, E, et al (2022) focused on locating energy theft in a fully measured smart grid by analyzing distribution line information. They conducted a comprehensive network modeling process using Algorithm simulation with MATLAB software, applying it to a radial network. H.O. Henriques et al. (2020) pursued a similar approach, implementing the sweep backward/forward algorithm while also considering the ambient temperature of the conductors and its impact on technical losses. Uvais, M. (2020, February) presented an affordable and practical strategy to control fraud and electricity theft from distribution network lines. They utilized data from consumer energy meters and distribution transformers, employing a system connected to a control unit that received wireless data and sent signals to circuit breakers to prevent electricity supply. If theft persisted after four attempts, the entire system was reconfigured; otherwise, an alert message was sent to the maintenance station in the electricity company for examination and follow-up. This system operated based on measuring the extra voltage drop and current increase, and it successfully passed simulations in the MATLAB Biswas, P. P, et al (2019) program. Most of these studies successfully determined non-technical losses and provided a rough estimation of the theft's location.

This thesis examines the process of using an artificial intelligence neuron network using the forward propagation method to determine non-technical losses in the network. Knowing the location of theft or fraud more accurately in the distribution lines or between the load locations of consumers. Therefore, we will work on simulating a smart network that depends on smart energy meters for consumers and processor Information that is connected near the distribution transformer and one of the means of communication is linked with a server in the main center of the electricity company, where the information processing unit works to collect load information for consumers by means of a smart meter, with determining the amount of voltage drop for each load and the amount of energy coming out of the distribution transformer and sending it to the main unit in the company.

This will take into account the value of technical losses for the distribution network and determine the amount of the ideal voltage drop and adopt the difference with the actual voltage drop in simulations of the network in addition to entering the entire network data into the forward algorithm of neuron network in the MATLAB program to determine the location of the network theft according to the voltage difference between the ideal voltage and the difference Actual effort, and we will compare this study with another that adopts the same principle (finding theft by the voltage drop difference), but by the algorithm method of equations, and we give the results for each method and explain the positives of the neuron method, which represents the point of view of the thesis in determining non-technical losses and the location of the theft. And as a first step, we have to know what we mean by theft and what we mean by fraud in the distribution networks in order to distinguish each of them and ways to detect it.

Energy theft is the process of connecting a feeder to one or more consumers who are not subscribers to the energy distribution network, illegally and without the knowledge of the energy companies to consume energy without paying bills.

Fraud: It is the process of tampering with energy meters by customers connected to the distribution network for the purpose of consuming part or all of the energy consumed without paying bills.

Problem Statement

Energy theft is considered one of the most important problems of the electric power distribution network, which significantly impacted the work of the distribution networks. This led to operational failures in the work of the short- and long-term power distribution system, which led to a rise in maintenance costs, which was reflected in a rise in the prices of electricity bills for legal consumers and negatively affected the financial return on investment for electricity companies. Therefore, an effective way must be found to combat energy theft and fraud in energy meters, by locating theft on the network.

Thesis objectives

1 - Through in-depth study and inspection, look into the nuances of losses that happen throughout the distribution network.

2- Assess the effectiveness of various energy-related methods in spotting cases of fraud and theft in order to discover the most efficient ones

3. Create a remarkably low error rate detection and localization method for non-technical losses within the distribution network using simulated neural networks.

CHAPTER ONE

PURPOSE OF THE THESIS

Literature Survey

In order to ensure the continuation of a fair and reasonable supply of energy, while minimizing economic losses as far as possible (Jiang, R.et al 2014), (Cao, M.et al 2021). In the past methods were adopted to detect the theft of electric power by practicing the pre-determined activities of technicians and workers in electric power companies. The procedure begins with field detection and meter reading on the mains supply and consumption and continues to manually record, classify and perform analyses and calculations. In addition to installing a special watt-hour metering box, with the low-voltage metering outlet side closed, adding an anti-theft function to the watt-hour meter by connecting it with a wire and soldering with lead to control fraud, and the energy meter was an early form of combating energy theft, then the practice of improving the rate of electricity application by using the acquisition system for some operations related to devices that can prevent energy theft. Other hardware-related processes include optimizing the application rate of the electrical acquisition system (McLaughlin, S. et al 2013) – (Jokar, P, et al 2015). The Advanced Measurement Infrastructure (AMI) is an important early example of the Internet of Things (IOT) in the smart grid. As it transmits actual data from smart meters to both consumers and grid operators, thus harnessing the full potential of demand response Jadidbonab, M.et.al (2020), the authors present a strategy for detecting energy theft in smart grids while preserving users' right to privacy regarding their energy use. In particular

Presented Nagi et al. (2008, December) refers to the method of assembling a group of Support Vector Machines (SVM) with an automatic feature of profiles to identify and identify illegal customers. This is done by using previous customer data that was collected and then analyzed and extracting the pattern of each consumer of electric energy through statistics and data Recorded with the assumption that files exposed to fraud will contain anomalies from the mainstream, and (SVM) works to load and classify customer files according to loads to identify suspects in energy theft, but Nagi et al more focused on sudden changes in the loads' pattern to infer theft and fraud activities.

Then Caio C.O et al. (2011) aimed at exploiting the speed of Optimum-Path Forest (OPF) and using it in a new and hybrid algorithm based on Harmony Search, OPF (HS-OPF) to demonstrate its potential within the context of automatic identification of consumer data and identify non-technical losses in distribution networks in a rapid methodology of knowledge and performance. It was to integrate (HS-OPF) is more representative in identifying features by conducting two rounds, the first is to compare OPF with several other classifiers, and the second is to compare the hybrid algorithm (HS-OPF) to the basic algorithm of Particle Swarm Optimization (PSO) to choose the characteristics of (PSO-OPF) Ramos, C. C et al (2011, May) and that both data are derived from the original space of the algorithm to adapt the Principal Analysis (PCA) and the kernel principal component analyzes (KPCA). This study provided a process for identifying non-technical losses at a lower cost than its predecessor.

Leandro Aparecido Passos Júnior et al (2016) used the multivariate Gaussian distribution algorithm, which is used to determine non-technical losses and indicates the presence of theft in the distribution network by classifying a new sample that is not believed to belong to the prevailing pattern in consumer data, then this sample is classified As belonging to an illegal customer, where all samples of the cluster are modeled a Gaussian distribution with its data defined and determined by artificial intelligence techniques. Therefore, identifying the abnormal sample, its data is analyzed from the nearest Gaussian distribution on it, and if it is illegal, its location is determined. In this research used the illegal unsupervised OPF to calculate the Gaussian distributions' parameters. Because the researcher believes that OPF is more accurate than other techniques that can be used to detect non-technical losses, and compares it with some known means (K-means) and Gaussian Matrix Mixture (GMM), and developed this research on what was previously mentioned in the process of detecting energy theft and locating losses Non-technical to illegal consumers This method was tested with a commercial energy company in Brazil.

Then Buzau, M. M, et al (2019) suggested a process for developing the detection and search for non-technical losses using hybrid neurons that require the least amount of input data. This paper is characterized by the use of Analyzed classifiers in addition to previous deep learning of network data. The profile is classified on a daily basis through (LSTM) a long short-term memory by sending non-sequential data over a Multi-layer Perceptron's (MLP) network to adopt the energy consumption in the distribution networks that is recorded in the energy meters, which It is a combination of (LSTM) and (MLP) and significant performance improvements were obtained by training the model on several actual network data in an energy company in Spain. But its reliance on taking an average sample for each actual pregnancy is determined for a period of 365 days by a field inspection team and this matter is inaccurate and expensive

While H.O. Henriques et al (2020) to develop the process of detecting non-technical losses by using sensors to measure the temperature of surrounding for the conductors and wires in the network and to show its effect on increasing the technical losses so that he can later determine a more accurate value for the non-technical losses, which helps to determine the difference in the actual voltage difference And ideal to be used in the Backward/Forward sweep algorithm and with the help of a data recording device that connects near a transformer in the distribution network that works to send all information about the network, temperature and energy recorded in the smart meters to a main server in the center of the electricity company to analyze the data and classify it with the algorithm using a method Energy collection Cespedes, R. G. (1990) Which compares the voltage drop recorded in the energy meters and the ideal voltage drop after determining the exact value of the technical losses to force the calculation of a value close to the non-technical losses and to determine the location of the theft in the distribution network with a very small error.But The study depends on adding temperature sensors to connectors and wires of the network to accurately determine the TL and NTL which is very expensive

And there a practical and affordable method of preventing electricity theft along distribution lines was given by Uvais, M. et al. (2022). A controller-based system is created using information gathered from household energy meters and the line Transmission (LT) side of the distribution transformer. The central control unit is located on the LT side of the distribution transformer and receives data from the energy meter via a wireless link. If theft is detected within four attempts, the controller will reinitialize the entire system; if not, it will send a warning message with the location of the theft to the nearest substation or the electricity provider. The controller sends the signal to the circuit breaker to block the electricity and re-check for theft. This is accomplished by measuring the increased voltage drop and current that the theft has caused in the distribution line. MATLAB has been used to test the suggested system with great success. Another crucial component of this initiative is the use of IoT to transmit theft data to the distribution utility Saad, M. A et al. (2020). Since a network is made up of connected nodes, information gathered by sensors, for instance, may be instantaneously shared across the internet. The main benefit of the proposed system is the elimination of the requirement for external power sources. A novice could use the suggested approach because it is doable, useful, and economical KAMATAGI, A. P et al. (2020, July).

Eric Nta and Kingsley Udofia (2022) suggested simulating a real electrical power distribution network, and the developer program was introduced to store a complete matrix of wire and conductor resistance in the consumer distribution network to be used in the algorithm to identify and find energy theft in the system by comparing the voltage of each pole node present in the system. The network with reference to all the nodes of the network associated with consumers and using the resistances of the conductors recorded and stored in the program. When a difference occurs between the readings, this is evidence of the existence of theft and a difference between the currents recorded in the energy meters and the main measure of the power consumed by the feeder. This method has been simulated in the Matlab program and accurate results were obtained in the detection of up to 92%. The disadvantage of the study is that it needs to have permanent knowledge of the voltages of each node and the legal variation in loads to ensure accurate calculations

Through our study of the previous research papers and what came in them of many different ideas and methods, for one purpose, which is to estimate the value of technical losses and locate the location of energy theft in the distribution network. The whole network and recording deformation or anomaly in the samples is recorded within the Gaussian algorithm and others proposed a complete matrix of the resistance of wires and connectors in the consumer distribution network to be used in the algorithm to identify and find energy theft in the system by comparing the voltage of each pole node present in the network, and others suggested finding the location of the theft by The difference in the values of the actual and ideal voltage drop of the network and the location of the theft by a specific algorithm or By using the simulation of the neurons of the network, and this is what I will adopt in my thesis to demonstrate the possibility of detecting theft and determining its location with an accuracy of up to 99% of the real values in a simulation of an electrical network in the MATLAB program the method it based on a Feed-Forward neural network.

CHAPTER TWO

LOSSES AND METERS ELECTRICAL ENERGY

2. The Losses in Electrical Power Systems

In the vast majority of instances, the losses of electrical energy in distribution networks have not been handled as well as feasible while having a large value in the decompensation of power systems. These losses represent both short-term and long-term distribution operational difficulties for systems that raise internal costs significantly and negatively impact electricity prices and the economies of the companies. In order to study the theft of electrical energy in the distribution networks, we have to start studying the energy losses in those networks, which are divided into technical losses and non-technical losses, and an indication of their drawbacks with the solutions used to reduce them.

2.1-Non-technical losses

Non-technical losses are an intricate issue that has been plaguing the electricity industry for years. These losses are caused by factors outside of the power system, such as theft, inaccurate metering, and unmetered electricity. They are challenging to quantify since system operators frequently fail to account for them, leaving no records of their occurrence. The impact of non-technical losses is felt not only by the power companies but also by the consumers, as they lead to an increase in the cost of electricity.

Theft is a significant contributor to non-technical losses. Theft energy is the energy that is provided to customers but not registered by their energy meters. This can occur due to meter tampering or meter bypass. Thieves can tamper with the meters by installing magnets or other devices that interfere with the meter's functioning. They can also bypass the meter altogether, allowing them to consume electricity without paying for it. Inaccurate metering is another cause of non-technical losses. The discrepancy between the amount of energy that is actually delivered through the meters and the amount that the meters indicate can result in losses. This can occur due to faulty or malfunctioning meters, meter reading errors, or human errors during, the billing process. Unmetered electricity is also a source of non-technical losses. This can happen in situations where the customer is not connected to the grid, but power is still being supplied to them. It can also happen when the meter is not functioning correctly, and electricity is being consumed without being measured.

2.1.1 Forms of Non-Technical losses (NTLs)

Non-technical losses (NTLs) refer to losses that occur outside of the power system or are not accounted for by technical loss estimates. NTLs mostly deal with power theft in one way or another, and the forms of NTLs can be categorized as follows. First, tampering with meters is one of the most common forms of NTLs. Thieves alter the meters to record a lower consumption reading, reducing their bills. Second, technical losses computation errors may result in discrepancies between the quantity of energy that is delivered and the amount that is invoiced. Tapping, or hooking, on low tension lines, is another form of NTLs. This occurs when consumers tap into the distribution network illegally to access electricity. Additionally, arranging false readings by paying meter readers, stealing by evading the meter or making illegal connections, ignoring outstanding debts, faulty energy meters, unmetered supply, inaccuracies and delays in meter reading and invoicing, and consumers who fail to pay are also forms of NTLs.

2.1.2 Financial Impact of Non-Technical Losses

Accurately measuring the financial impact of non-technical losses can be a challenging task, especially if the value of technical losses has not been determined and incorporated into mathematical and algorithmic operations to calculate precise values for each point in the distribution network. However, once non-technical losses have been identified, the estimates reveal a significant impact on the electricity transmission and distribution sector, with an annual global loss estimated to be between 80-100 billion US dollars Carr, D., & Thomson, M. (2022). These financial losses are primarily attributed to electricity theft, highlighting the severity of non-technical losses and their impact on energy companies.

2.1.3 Causes Non-Technical Losses (electrical power theft)

2.1.3.1 Financial Strain of Electricity Costs in Developing Countries

In developing countries, the high cost of electricity in relation to the daily income of citizens presents a significant challenge. For instance, in Nigeria, where over two-thirds of the population earns an average daily income of 3.2 US dollars Available online (accessed on 4 January 2022), operating an electric appliance such as a refrigerator can consume up to 8% of this income Carr, D., & Thomson, M. (2022). Coupled with other household appliances and the cost of night lighting, the electricity bill can be a considerable burden on the financial capacity of consumers. As a result, some consumers resort to stealing electricity, leading to a decrease in financial imports for electricity companies. This problem is prevalent in developing countries and has significant implications for both legal consumers and electricity companies.

2.1.3.2 The Oversight and technical negligence

In countries that face instability in their security or political situation, there are often problems with outdated and poorly maintained electrical networks. Furthermore, if a large portion of the country's income comes from exporting resources such as oil, minerals, or crops, state-owned electricity companies may not receive sufficient funding. Iraq serves as an example of such a country. As a result, the theft of electric power is rampant, And as shown in Fig. (1), Issues related to politics, security, and economics are more important than the electricity sector, exacerbating the problem

Fig (1) Bypassing citizens on the electrical power distribution network

Given these challenges, monitoring and regulating the electricity theft process is often a secondary concern. This can have severe consequences, including exceeding maximum load current, network collapse, and the need for extensive maintenance. Ultimately, such oversights can have a negative impact on the imports of electricity companies and distribution networks Khalel, S. I, et al (2022).

2.2-Technical losses

Technical losses are the energy dissipated in the conductors and equipment of all parts of the electricity sector, especially the distribution network, from power transformers to distribution lines and measurement equipment, where the heat generated due to the passage of current in the network connectors is one of the most important forms of variable technical losses expressed mathematically by I^2R because these losses depend their amount on the amount of current passing through the conductor, which reaches the highest value in times of peak load, and the core losses, which are the magnetic losses In power transformers, which are considered inherent losses that cannot be eliminated in distribution networks, in addition to technical losses related to power factor and inductive loads, or technical losses when the phase is unbalanced.

2.2.1-Technical Losses of transmission lines

Power losses in underground cables and overhead lines are primarily due to load losses ($P_{loss} = I^2R$), As the power losses varies with the square of current, the amount of current flowing in the cable will have the highest impact on the energy losses in cables and overhead lines. Typically, load losses of feeders are calculated under peak demand condition using load flow simulation. Where load losses are calculated according to the equation below Au, M. T., & Tan, C. H. (2013, June).

$$Energy\ Loss = P_{loss} \times Loss\ Factor \times Time \qquad (1)$$

The energy losses over a specified period (one week) is then calculated using Loss Factor estimated as follows:

$$Energy\ Loss = P_{loss} \times Loss\ Factor \times 24 \times 7 \qquad (2)$$

Using the formula, the Loss Factor is computed from Load Factor.

$$Loss\ Factor = \alpha\ \times Load\ Factor + \beta \times Load\ Factor\ ^{2} \quad (3)$$

Where $0 \leq \alpha \leq 0.35$, and α+ β = 1.0

Input energy to the feeder can be calculated as follows,

$$input\ Energy = Peak\ Damand \times \text{Load Factor} \times 24\times 7 \quad (4)$$

$$Technical\ Losses\ of\ the\ Feedr(\%) = (Energy\ Loss \times 100)/\ input\ Energy \quad (5)$$

2.2.2- Distribution transformer losses

The losses of the distribution transformers are calculated based on the energy spent when preparing the accounts for the user and the transformer to estimate the technical losses in the transformer of the distribution network. The manufacturing data of the transformer is taken into account as shown below in table (1) with regard to the inherent and fixed losses and the resistive losses related to the current square, le giving information when loading and unloading, and the tests are Díaz, S. (2021). Specified load-related losses for the measurement test.

Table (1). Transmission and distributing the resistive loss Díaz, S. (2021).

Nominal Power [KVA]	10	15	25	37.5	50
Specified losses [W]	164	262	392	466	895

2.2.3- Influential Factors on Technical Losses

Where the longer the feeder becomes, the more loads it feeds, which means an increase in the flow of current in it, and thus an increase in copper losses in it ($I^{2}R$). This is in addition to an increase in the voltage drop, which means an increase in electricity consumption to provide the required capacity for the work of electrical loads In addition to other losses, such as iron losses in transformers, which increase with their and with the difference in the type of loads, whether they are capacitive or inductive, and their impact directly affects the percentage of technical losses in the distribution network, as shown in the paragraphs below.

1- Feeder length (mesh size)

2- The capacity of the infrastructure relative to the amount of electricity distributed

3- The number of transformers in the network and the number of feeders connected to them (capacity factor)

4- The load factor and the amount of peak demand

5- Design standards for the size of conductors and the amount of load dispersion

2.2.4- Mitigating Technical Losses: Strategies for Reduction

The following methods are usually used in conventional networks to reduce and limit technical losses within distribution networks, and they are shown

1- Placing capacitors within the network

2- Raise the voltage level

3- Monitor the transformer load

4- Reconfiguration

The following table (2) shows the form of estimating the benefit/cost ratio using technical loss reduction methods, as it takes into account the reduction of consumption expenses as much as possible Agüero, J. R. (2012, May).

Table (2) Benefit/cost ratios for various loss reduction strategies Agüero, J. R. (2012).

Measure	Benefit/cost ratio
Reconductive	0.6 to 7
Compensation reactive	2 to 8
Load management transformer	1 to 15
Voltage enhancement	1.5 to 3

Losses in the load of a distribution system are a function of the square of the current. As a result, lowering the line current's absolute value by lowering its reactive component, or enhancing the power factor, is one technique to lower technical losses. Installing fixed and switched capacitor banks will do this. Reactive compensation is the term used to describe this method. Line currents are decreased from the sites of the capacitor bank locations to the generation equipment because capacitors can lower the reactive power demand. This has the following financial advantages: Díaz, S et al (2020, June)

- Release of generation capacity.

- Release of transmission capacity.

- Released distribution substation capacity.

- Less energy is lost.

- Less voltage drop results in improved voltage regulation.

- The capacity of the released feeder and related equipment.

- Capital expenditures that have been postponed because of system expansions or improvements.

- Higher sales thanks to voltage advancements.

Tolerating stepped reactive power correction is possible with conventional switched capacitor banks. Distributed generators (DG) with tools like Static Var Compensator (SVC) and static compensators (STATCOM) can enable more flexible and continuous voltage correction and control (after reactive power charging) (even during dynamic conditions).

There is a lot of work in this field, including continuing research and modifications to the standard, despite the fact that voltage regulation using DG is not often utilized or permitted by some of the existing laws. Thus, it has the potential to spread and become a standard operating procedure for distribution systems.

It should be noted that for the reduction of primary and secondary lines, the distribution load losses are inversely related to the system components' series resistance (R), suggesting that lowering (R) is another method for cutting technical losses. This can be done by installing conductors with a bigger cross-section in place of the current primary and secondary lines. Conducting is the term used most frequently to describe this process. This utility has recorded losses totaling about 2%. This value is significantly lower than the range of 4 to 13% Agüero, J. R. (2012, May) for the majority of utilities in the same area. Depending on the system, reconductoring has a different benefit-to-cost ratio. The voltage profile is improved by reconductoring because the voltage loss along the feeder is decreased, and there is more capacity available for load transfer, either from or to nearby feeders. The latter is also advantageous to system dependability.

2.3- Metrics for Evaluating Technical Loss Reduction

The energy meter used in its different names is the electricity meter, the consumed power meter, or the kilowatt-hour meter. It is a measure of the amount of electrical energy consumed during a certain period of time. Electricity companies usually install energy meters in homes and buildings to bill the spent energy and sometimes to study consumption data. One of the most famous of these meters is the kilowatt-hour (KWh) meter, which depends on reading what is recorded of the amount of consumption by a person every month or any other period of time Kahmann, M (2020) The energy meter has gone through many developmental stages since the invention of the electromechanical DC meter Fig (2) in 1883 by Dr. Hermann Aron (Aniedu, A. N. et al 2016), to the electrochemical meter, then the electromechanical AC meter, and down to the latest findings of the current science with the latest generations of smart meters. With its different types, its function was the same, billing the energy consumed and trying to control the energy theft process.

Fig (2) Herrmann Aron (1845–1913) and the double-pendulum meter which was developed by him and his engineers.

2.3.1 Type of Metrics

2.3.1.1-Electromechanical meter (kWh)

This meter is one of the most common types of counters WI, M. U. (2017), as it depends on its work on magnetic induction, the first coil is connected in a way that produces a magnetic flux proportional to the current, and the other produces a magnetic flux proportional to the voltage. Which lags by an angle of 90 degrees Fleming, S. J. A. (1914) which works to rotate a metal shaft bearing at one end a toothed rotating disk interlocked with several small gears linked to rings numbered from 0 to 9 To measure the spent energy, and its rotation speed depends on the amount of power consumed Ocampo-Vega, R et al (2013, November) Usually, the meter coil consumes a relatively small voltage estimated at 2 watts, which is considered part of the technical

Fig (3) Electromechanical meter (kWh)

losses because it is not billed. To read it and record the amount of energy consumed during it, in order to issue the invoice, in addition to the negative aspects of the ease of fraud and fraud in it Creep, a phenomenon that can negatively impact accuracy in an induction type meter, happens when the load terminals are open circuited and the meter disc rotates constantly with potential applied. A creep test is one that looks for errors brought on by creep Chen, H. C., & Chang, L. Y. (2012).

2.3.1.2-Electronic Meter

This type of the most advanced setting appeared to address some of the defects and problems of the electromechanical (electromagnetic) meter. It had many capabilities in addition to measuring the consumed energy, including measuring the electrical load, the maximum instantaneous rate of usage demands, the voltage value, and the power factor, in addition to the possibility of transferring the meter readings and sending them to remote places Through communications Kotsampopoulos, P, et al (2016) this type of meter also contains a screen (LCD, LED) to show all the data through it, and it also has a backup source of energy and a connection part with the center, in addition to many specifications such as a digital clock for the time of the spent energy with the possibility of infrared communication to detect fraud and fraud to steal energy However, one of the defects of this device is that its data reading is affected by ambient temperatures around it and this main cause of persistent mistakes in the meter, followed by the accuracy of the voltage reference. Both of these change dramatically when meters are used outside depending on the temperature. A significant component of meter design is characterizing and mitigating these. Therefore, the reading differs whether it is inside the building or outdoors Chen, H. C., & Chang, L. Y. (2012). Therefore, part of the error value is compensated for its manufacture of certain atmospheres, with the addition of a temperature sensor to the processing units when taking data.

2.3.1.3-Smart meter

In these smart meters Fig (4), the manufacturers went a step further than the Automatic Meter Reading (AMR) system counters, by adding the ability to indicate the real-time consumption and report when the power is cut off, in addition to monitoring the quality of the energy consumed and determining the prices of energy consumption according to time in peak or low loads with the ability to classify Loads according to the devices used and determining the energy consumption of each of them, which facilitates the process of preparing complete data when studying loads of the distribution network for the purpose of maintenance or development Abdalzaher, M. S (2022).

Single Phase Double(Phase/Neutral) Missing kWh Meter
FGF
000890
SL No. 544912
FGF ELECTRICAL & ELECTRONICS LTD.
4-A

Fig (4) Single-phase smart meter.

2.3.2 Security and fraud

Since the advent of energy meters, start manipulation, and fraud appeared with some consumers with meter readings, and with the negative things that these dishonest characteristics carry, many companies started to research and develop for the purpose of addressing this problem through field inspection or making metrics to report cheat or fraud in the meter, and progress appeared clear In this field after the emergence of electronic meters and then the smart meter to try to eliminate the process of energy theft and the methods used to manipulate the readings of the electromagnetic meter, It is to put a piece of magnet on the outer part of the meter, which works to saturate the magnetic field in the meter coil, which affects the work of the motor part in it and reduces its rotation speed Xia, X., et al (2022). The same trick may be used on power transformers in electronic meters, so the electricity companies secure these meters by providing the possibility of Readings of the reflected load and the surrounding magnetic fields, in addition to setting certain mechanisms and sealed connections to prevent fraud. In the AMR meter, sensors were added to report magnetic anomalies, inverted installation, opening the cover, etc.… But the current that does not pass through the energy meter remained difficult to detect by the previous methods.

CHAPTER THREE

THEFT AND FRAUD IN DISTRIBUTION NETWORK

3. Energy Theft

Many research and scientific studies have recommended the need to adopt scientific and practical methods to combat cases of theft in the electric power distribution network to minimize its negative effects on the distribution system in addition to the economic losses of the electricity companies. Many studies suggested theoretical solutions and methods only, and others presented methods more compatible with distribution networks' practical reality. To detect theft or fraud in energy meters, this thesis proposes to study three methods of detecting and locating theft on the simulation of a circuit that is part of a distribution network in the MATLAB program. In addition to three load sites representing houses or service buildings that consume energy. The resistance of the conductor was obtained from the cable factory data Nta, E., et al (2022) and we will detect theft and fraud by the method of the difference between the voltage drop occurring in the network when any theft occurs that is contrary to the data documented in the main processor In the company, which is taken from the smart meters and the distribution transformer counter, in addition to calculating the values of the technical losses imposed in all the wires and connectors of the network, and when simulating, we will work on taking more than one case of theft for all methods and recording their results, then comparing those results, provided that we study in advance the types of electricity theft in the distribution network So that we can cover it completely when simulating.

3.1 Detection of Theft and Fraud in Electrical Power Systems

By reviewing many studies and research papers to clarify and determine how to detect non-technical losses, as it was found that there is no fixed methodology for detecting theft, most researchers adopted multiple methods without any common methodology, Among the most common of these methods is the method of detection by artificial intelligence, analysis of network data, and detection of anomalies in network data. These methods are classified into three categories (the directed network category, the hybrid network category, and the directed data category) However, the directed data category is distinguished from other categories by using energy network data (network topology or network measurements) from data related to the consumer only from energy consumption and consumer type. As for the hybrid methods, they use both data for the network and the consumer, and the methods directed towards the network or towards the data are divided into other categories according to the main concept to detect energy theft. The researcher can find many applications and algorithms to detect anomalies in fraud Chandola, V., & Banerjee, A. V., K. (2009). Finally, there are cases where labeled samples from both classes are available but their number is too small compared to unlabeled samples. Semi-supervised learning methods Wei, L., & Keogh, E. (2006) that also use unlabeled samples have lately grown in popularity. This strategy has not been sufficiently demonstrated for detecting Non-Technical Losses (NTL) outside of the work. Saboia, P., & Goldenstein, S. (2014) physical rules that hence only supervised and unsupervised methods are discussed here. Since they are focused on network analysis and characterize such systems, network-oriented methods often typically neglect labels. These techniques are divided into groups based on the central idea or algorithm employed, such as state estimation, load flow, or specialized sensors for fraud detection. Concepts from each of the aforementioned areas are combined in hybrid approaches. To identify NTL at the MV/LV transformer level.

3.2 Data Classification Methods for Theft and Fraud Detection

Several classifications of data are adopted in line with the approved methods for detecting theft, as shown below.

1- Category and concept: The category and style to which it belongs, main or subsidiary

2- Data type: Determine the type of data that is used in the detection of the network, the consumer, or both

3- Data size: Where the data size ranges from small to less than 100 consumers, medium data to more than 100 consumers, or large data to more than 1000 consumers.

4- Algorithm: It is based on the algorithm used in detecting theft and fraud Messinis, G. M., & Hatziargyriou, N. D. (2018).

5- Measurements: In it, theft detection depends on the type of energy meter adopted (mechanical or smart, etc...) and its suitability with the approved detection methods and methods.

6- Response time: It depends on determining the time required to detect theft or fraud and obtain the necessary data to locate the theft Angelos, E. W et al (2011).

3.3- Types of Theft and Fraud in Distribution Networks

In order to avoid paying the official price, using electricity illegally is referred to as electricity theft (Adeniran, A. 2018) – (Komolafe, O. M., & Udofia, K. M. 2020). Where energy can be stolen, there are basically four main ways to gain electricity illegally. Electricity through unauthorized deliveries, meter tampering, bypassing meters, and unpaid invoices, can be fraudulently accessed Dike, D. O, et al. (2015).

1- Meter fraud: by altering the meters to make it less than count, tampering with meters in an attempt to reduce the values of energy consumed and recorded in the meter as shown in fig (2) case A.

2-bypassing meters: Connect a By Bus link on the meter to ensure that the consumed current does not pass through the electric energy meter, as shown in Fig (3) case B.

3-creating unauthorized connections: Theft of energy directly from power transmission lines: (illegally connecting the load line to the power transmission line), theft of energy from food distribution contracts near homes as shown in Fig (4) case C.

4- Counter fraud: collaborating with utility company meter reading devices for fabricating consumption Data, or altering the billing section to change the invoice given to clients (Komolafe, O. M., & Udofia, K. M. 2020)-(Abdulkareem, A. 2016).

As shown below, we have three cases of energy theft from three different points in the distribution network, from a direct connection to the distribution line, fraud in the meter, or completely canceling the work of the meter from the package recording the consumed capacity and recording bills, where (I_{Am}, I_{Bm}, I_{Cm}) represents the theft current in each The state of (I_M) represents the current calculated to pay bills.

Case (A): When the phase line at point A is shorted as shone Fig (5), a significant amount of current and power is transferred to the load through the shorting wire, causing I_{A_m} to be greater than I_m $\text{Nta, E., Udofia, K., \& Okpura, N. (2022).}$

The terminal voltage V_{1_2} , is the same as theft
voltage V_t

$$Total\ current,\ I_1 = I_{A\_m} + I_m + I_{1\_1} \tag{6}$$

$$Theft\ current,\ I_{A\_m} = I_1 - I_m + I_{1\_1} \tag{7}$$

$$Theft\ power,\ p_t = I_{A\_m}\left(V_1 - I_{1-2}R_{s1_2}\right)\ or\ I_{A\_m}\,V_{1\_2} \tag{8}$$

$$Voltage\ meter, V_m = V_{1\_2} \tag{9}$$

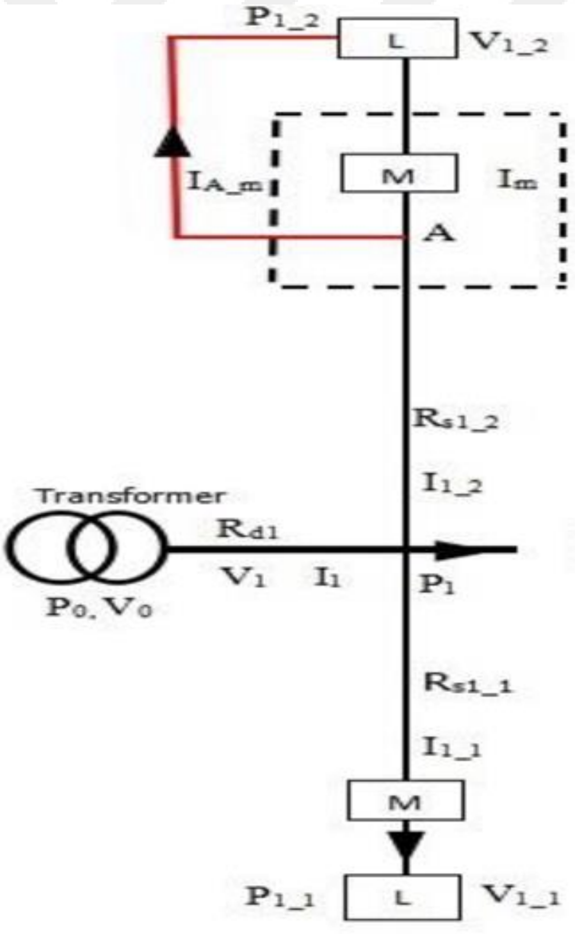


Fig (5) Case (A): When the phase line at point A is shorted Nta, E. Et al (2022).

Case (B): Disconnection of the meter from the consumer loads Fig (6) the analysis is similar, with the exception that since the meter is recording zero current, I_m = 0, consumer current I_{1_2}, is identical to stealing current I_{B_m}. The terminal Nta, E., et al (2022) voltage V_{1_2}, and the theft voltage (V_t) are identical.

$$Total\ current,\ I_1 = I_{B\_m} + I_{1\_1} \tag{10}$$

$$Theft\ current,\ I_{B\_m} = I_1 - I_{1\_1} \tag{11}$$

$$Theft\ power,\ p_t = \ I_{B\_m}\,V_{1\_2} \tag{12}$$

$$Voltage\ meter, V_m = V_{1\_2} \tag{13}$$

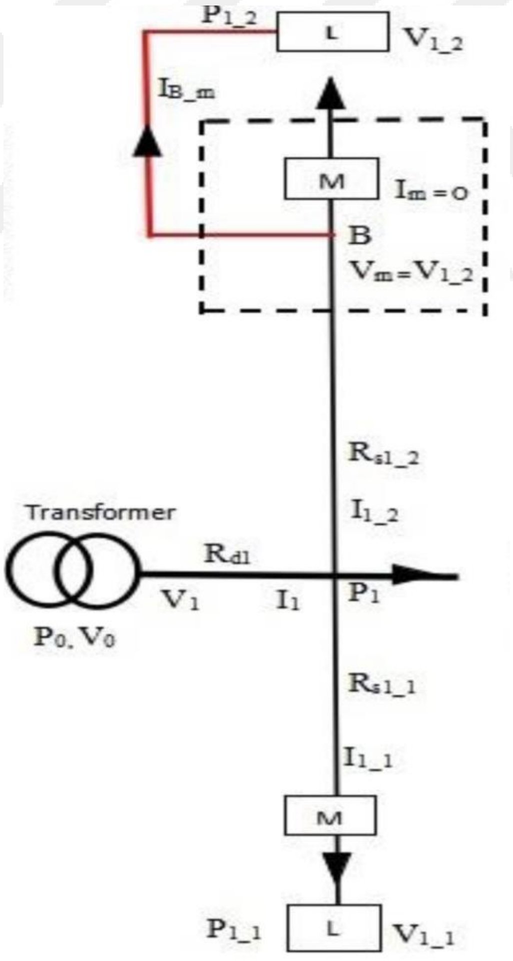


Fig (6) Case B: Disconnection of the meter from the consumer loads Nta, E et al (2022).

Case C: Network overrun illegal wire connection, Consumer load, and supply line are linked directly and fully unplugged from the energy meter Fig (7) Nta, E et al (2022), resulting in zero meter current and voltage across the meter. Energy theft voltage, (V_t) is the real voltage that the consumer actually receives, and theft current,I_{C_m}, is equivalent to consumer branch supply current, I_{1_2} (terminal voltage).

$$Total\ current,\ I_1 = I_{C\_m} + I_{1\_1} \tag{14}$$

$$Theft\ current,\ I_{C\_m} = I_1 - I_{1\_1} \tag{15}$$

$$Theft\ power,\ p_t = I_{C\_m} V_{1\_2} \tag{16}$$

$$Voltage\ meter, V_m = 0 \tag{17}$$

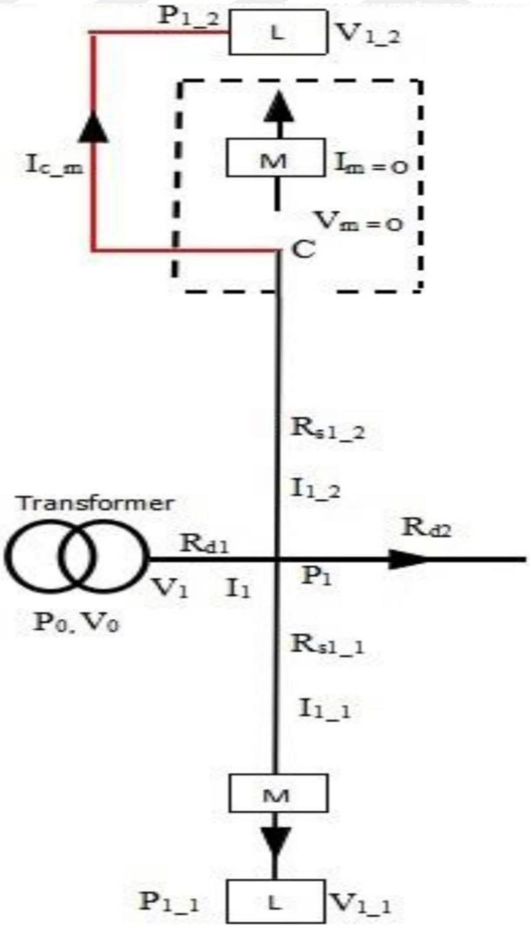


Fig (7) Case C Network overrun illegal wire connection Nta, E, et al (2022).

The previous approach was used in the previous cases (A, B, C) to clarify the types of theft and fraud and the data used to detect them from current, voltage, and capacity in addition to the voltage drop, which will be adopted in the practical side of this thesis to detect theft and fraud in addition to using The data of the design network within a simulation using the MATLAB program for neurons and using the LM, FFNN algorithms and clarifying its results and comparing them relatively to the results of using the method of the equation.

CHAPTER FOUR

SYSTEM SIMULATION

4. Research methodology

4.1 System structure

Depicts the power distribution system employed in this thesis Fig (8). The transmitting side (generation source), distribution transformer (11 KV/220 V, 50 Hz), and various loads (homes) with external tapping make up the single-line diagram, which represents the theft of power. Additionally, the location of power theft may be identified by calculating the voltage drop and additional current flow in the distribution network, by using the equations described later in the theoretical aspect, and by conducting a simulation in the MATLAB program for this case and we record the final results in several cases of theft and in several places to be compared later with the results of the second and third cases, which will simulate the same electrical circuit shown in Table (3), but using the algorithms Levenberg-Marquardt and Feed-Forward of the neurons network.

The controller takes preventative measurements action when the amount of stolen current exceeds the threshold. To prevent unauthorized tapping of distribution lines, the system determines the best course of action based on the theft situation.

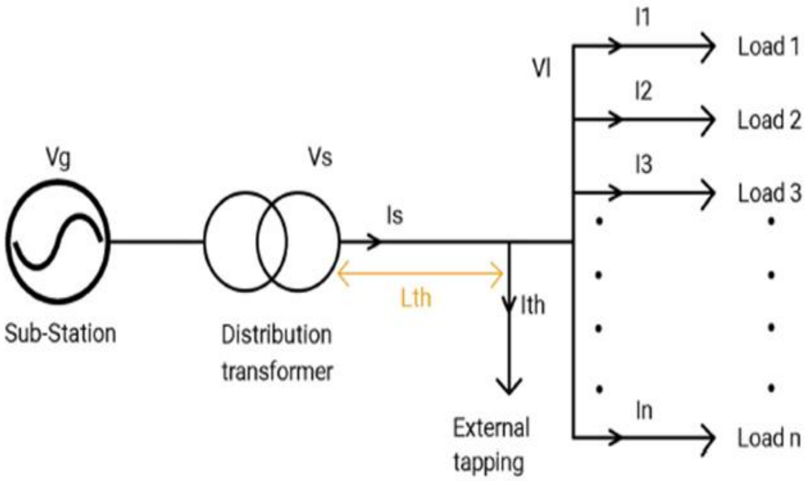


Fig. (8) The diagram circuit used in this thesis Uvais, M. (2020).

Table (3) Network Simulation Specification.

NO:	**Network Simulation Parameters**	
	Network Parameters.	**Network Value.**
1	Distribution Line (Length)	50 m
2	Load home (1)	100 Ω
3	Load home (2)	200 Ω
4	Load home (3)	300 Ω
5	Load for theft energy	100 Ω
6	Power Transformer	75 kVA
7	Input Transformer	11000 V
8	Output Transformer	220 V
9	System Frequency	50 Hz

4.2 Theoretical analysis

4.2.1 Case of Equations

Calculating the source current (I_s), source voltage (V_s), load voltage (V_L), and load current (I_n) are necessary to determine where and how much energy is being stolen. Based on the load currents and the theft (I_{th}) current, the source current can be calculated using the equation (19) below Uvais, M. (2020):

$$I_s = (I_1 + I_2 + \cdots + I_n) + I_{th} \tag{18}$$

Consequently, the theft current could be determined as;

$$I_{th} = I_s - \sum I \tag{19}$$

Because there is no theft current under normal circumstances, the sum of the load currents equals the source current as follows:

$$I_{th} = 0 \quad \Rightarrow \quad I_s = \sum I \tag{20}$$

Therefore, the following equation can be used to determine the drop voltage (ΔV) between the source and the load:

$$\Delta V \; = V_S - V_L \tag{21}$$

Eq. (22) was utilized to determine the impedance of a line (Z):

$$Z = \frac{\Delta V}{I_s} \tag{22}$$

When a theft occurs in the system, the current will not be zero. So the source current can be rewritten as follows:

$$I_{th} \neq 0 \quad \Rightarrow \quad I_s > \sum I \tag{23}$$

On the basis of the updated load voltage, the new drop voltage (ΔV^*) is once more calculated as follows:

$$\Delta V^* = V_S - V_L \tag{24}$$

As a result, using the drop voltage under both normal and abnormal load conditions, the steal voltage (V_{th}) may be computed from Eq. (25).

$$V_{th} = \Delta V^* - \Delta V \tag{25}$$

$$V_{th} = I_{th}.\, Z_{th} = I_{th}\ ((\rho.L_{th})/\ a)$$

Where (ρ) is the resistivity of the material used in the distribution line

and (a) is the cross-sectional area of the conductor.

The following equation can be used to calculate the theft distance from the distribution transformer to the theft site (theft zone) :

$$L_{th} = \frac{V_{th}.\, L}{I_{th}.\, Z} \tag{26}$$

Where (L_{th}) represents the theft distance in meters (m) over the actual length of the distribution line.

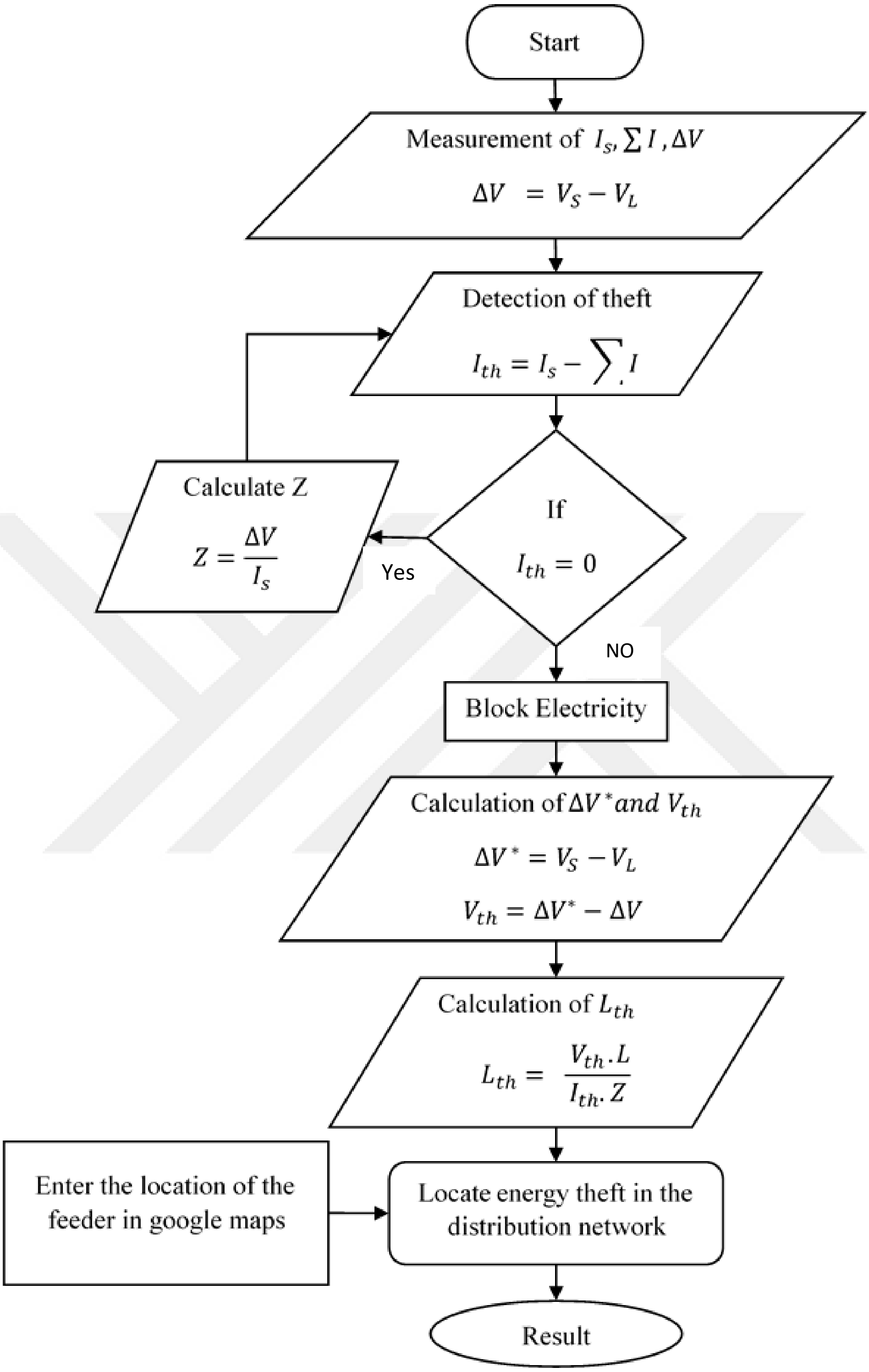

Start
Measurement of $I_s, \sum I, \Delta V$
$\Delta V = V_S - V_L$
Detection of theft
$I_{th} = I_s - \sum I$
If
$I_{th} = 0$
Yes
Calculate Z
$Z = \frac{\Delta V}{I_s}$
NO
Block Electricity
Calculation of ΔV^* and V_{th}
$\Delta V^* = V_S - V_L$
$V_{th} = \Delta V^* - \Delta V$
Calculation of L_{th}
$L_{th} = \frac{V_{th} . L}{I_{th} . Z}$
Enter the location of the feeder in google maps
Locate energy theft in the distribution network
Result

Fig.(9) Flowchart of energy theft detection by used equations.

4.2.1.1 Practical Application: MATLAB Simulation of Case 1 (Equation)

4.2.1.2 without Theft

In this case, is illustrated in Fig (10). When there is no theft or fraud in the meter in the distribution network system, the simulation will clearly show that on the side of the gauges, in the absence of any stolen current, and it will suffice to show the voltage drop in the network resulting only from technical losses (9.27 v).) which is pre-calculated and known to the source, as well as showing the lighting of the detection lamp in the other color to indicate that there is no theft.

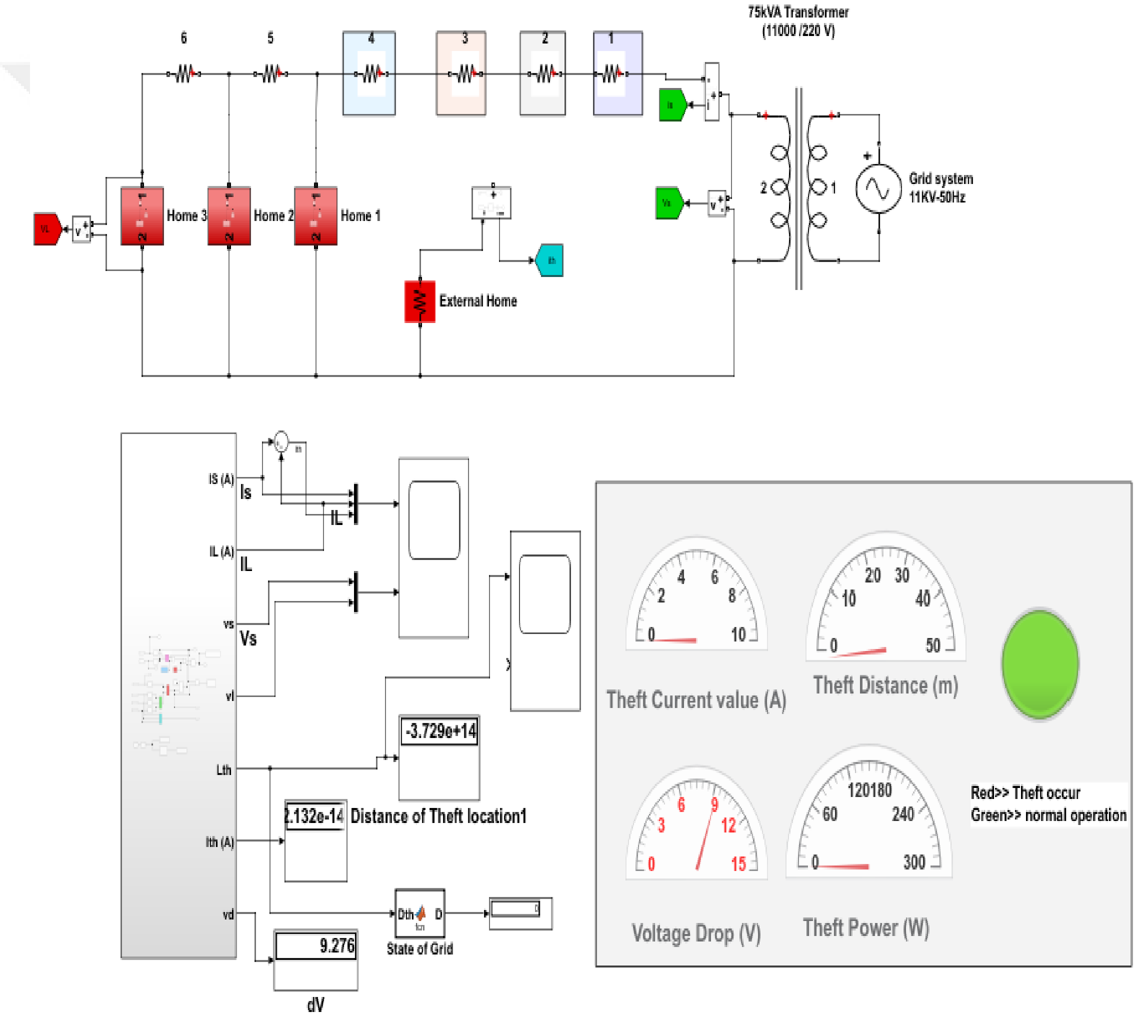


Fig (10) Simulation of theft detection circuit by using equations without theft

4.2.1.3 Description of the Simulation Circuit for the equations.

The simulation circuit of the MATLAB program consists of a distribution circuit similar to the work of the distribution network, the length of which is 50 m. It contains an electrical power transformer of 11000/220 volts and a transmission line represented by resistors (1,2,3,4) representing the technical losses in all transmission and each resistance representing the technical losses of ten Meters and the resistors (5,6) representing the technical losses of the transmission line at homes, while (External energy) represents theft energy and the resistances of Home (1,2,3) house loads.

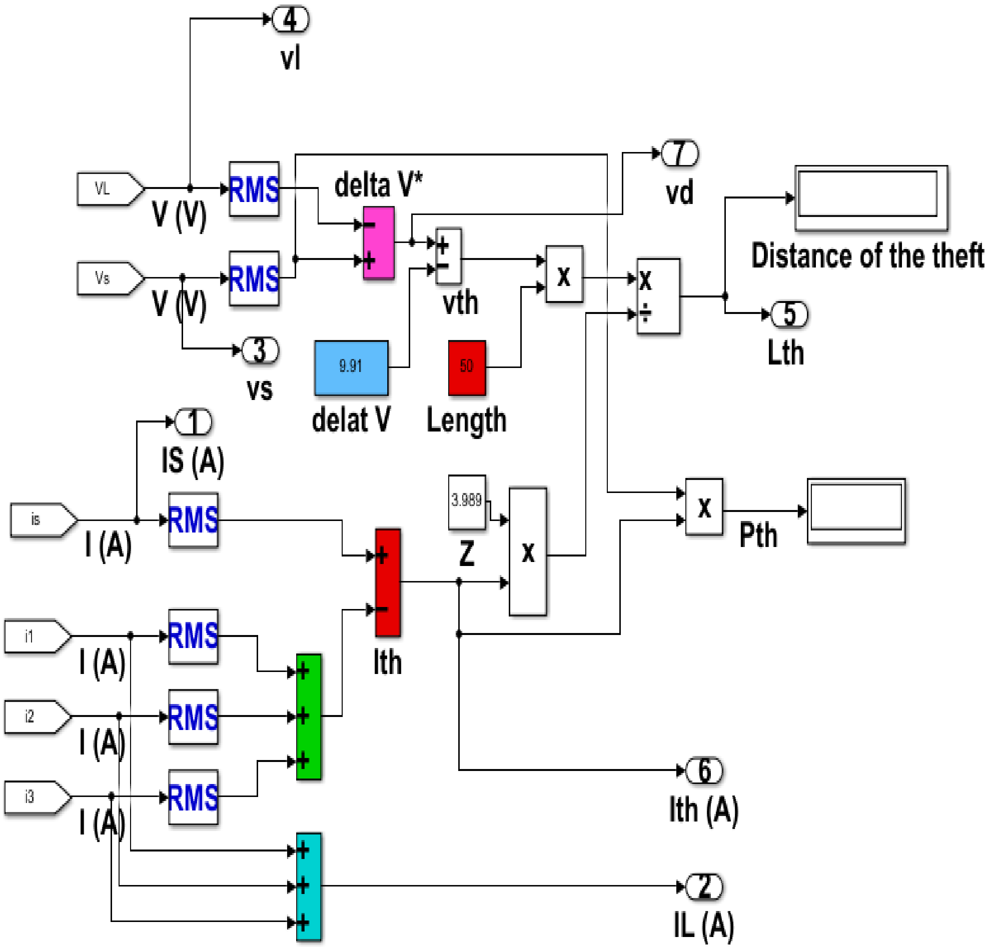


Fig (11). MATLAB/Simulink model subsystem of a theft detection circuit by using equations

4.2.1.4 with Theft

4.2.1.4.1 Theft Detection on the Transmission Line: A Distance of 20m

In this case, Fig (12) shows the presence of theft at a distance equivalent to 20 m from the distance approved for measuring the network from the distribution transformer, but the simulation shows through the measurements used using the case of equations that there is the presence of theft according to what is specified in the distance scale at a distance of 13.44 m from the distribution transformer, It is an imprecise approximation to the real distance, as it indicates that the color of the theft detection lamp has changed to red.

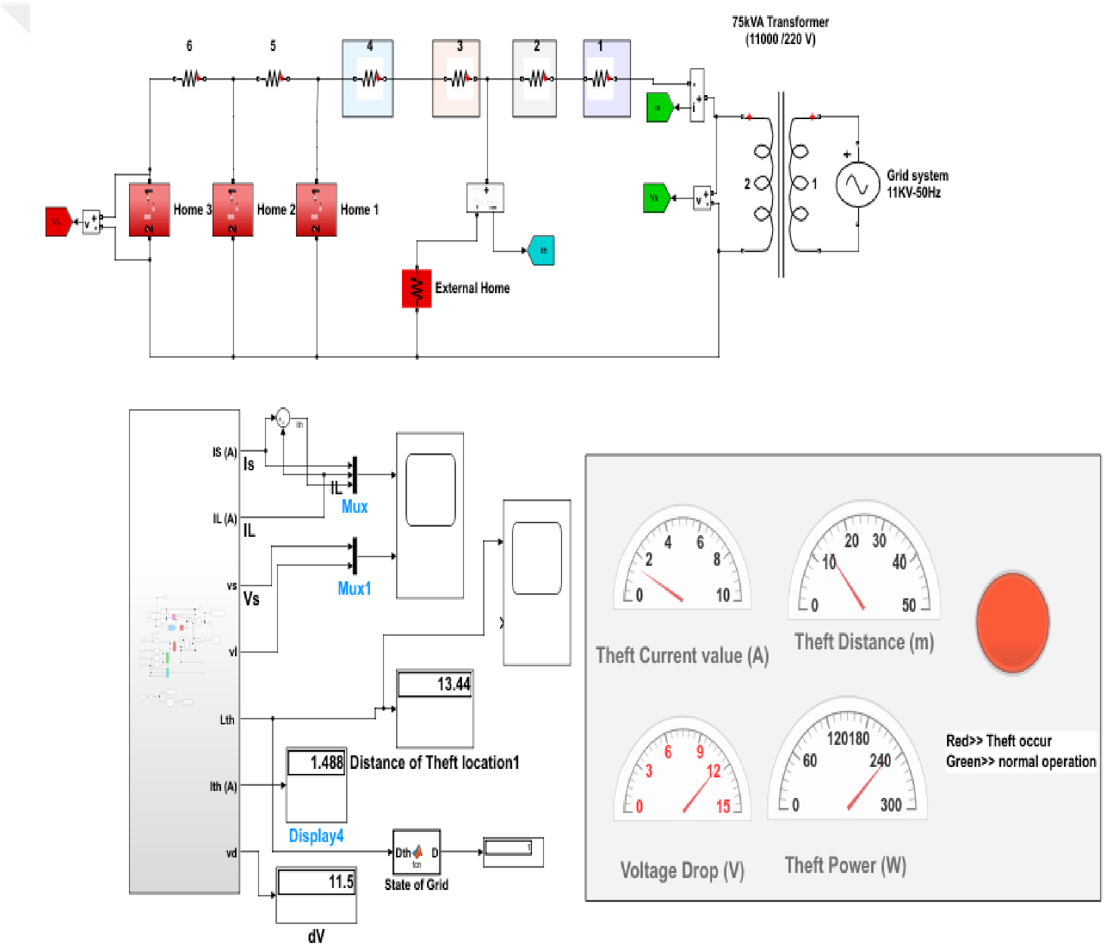


Fig (12) Simulation of a theft detection circuit by using the equations for theft at a distance of 20

4.2.1.4.2 Theft Detection on the Transmission Line: A Distance of 40m

In this case, Fig (13) shows the presence of theft at a distance equivalent to 40 m from the distance approved for measuring the network from the distribution transformer, but the simulation shows through the measurements used using the case of equations that there is the presence of theft according to what is specified in the distance scale at a distance of 32.03 m from the distribution transformer, which is A ratio that is relatively close to the real distance, as it indicates that the color of the theft detection lamp has changed to red.

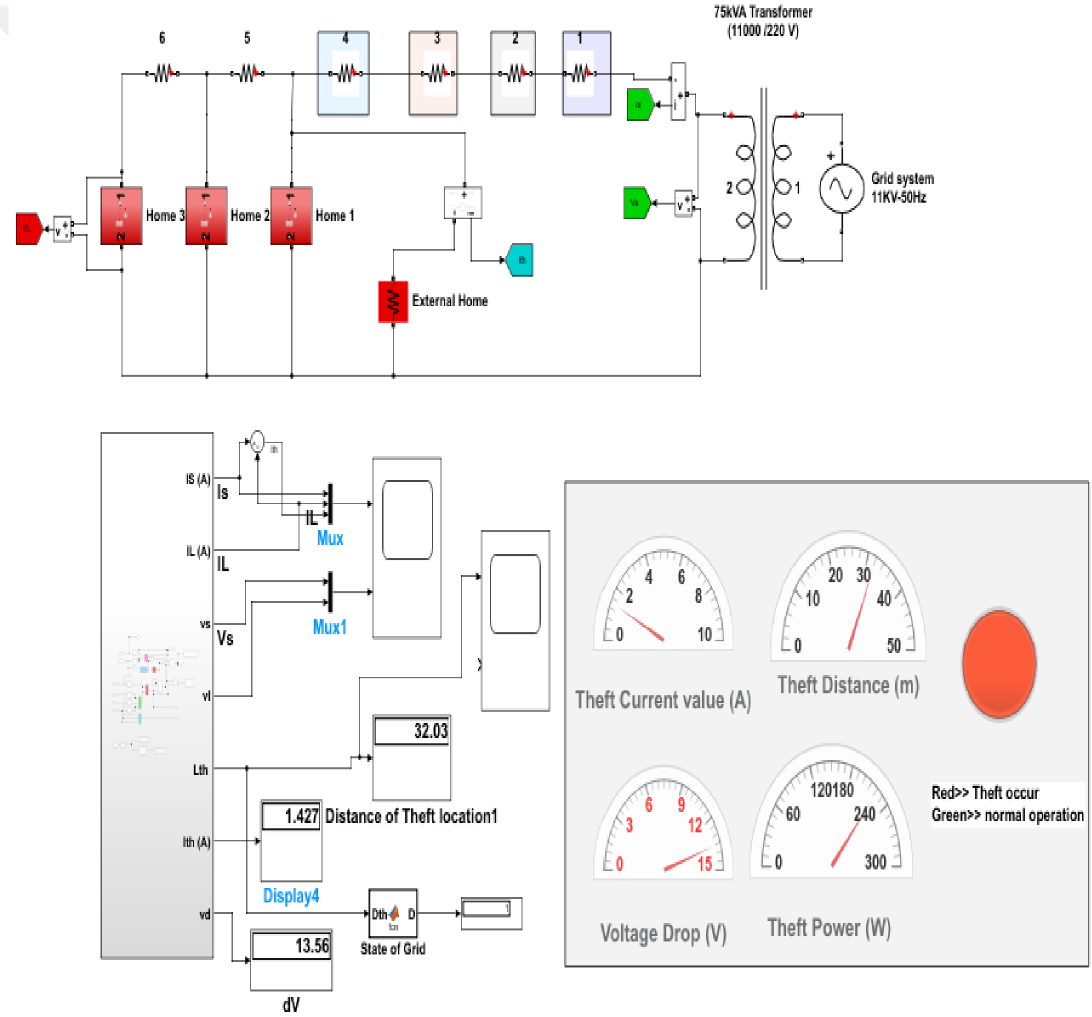


Fig (13) Simulation of a theft detection circuit by using the equations for theft at a distance of 40

4.2.1.4.3 Theft Detection at the Last Load in the Network: 50m Distance from the Transformer

In this case, Fig (14) shows the presence of theft at a distance equivalent to 50 m from the distance approved for measuring the network from the distribution transformer, but the simulation shows through the measurements used using the case of equations that there is the presence of theft according to what is specified in the distance scale at a distance of 51.48 m from the distribution transformer, which is A ratio that is relatively close to the real distance, as it indicates that the color of the theft detection lamp has changed to red.

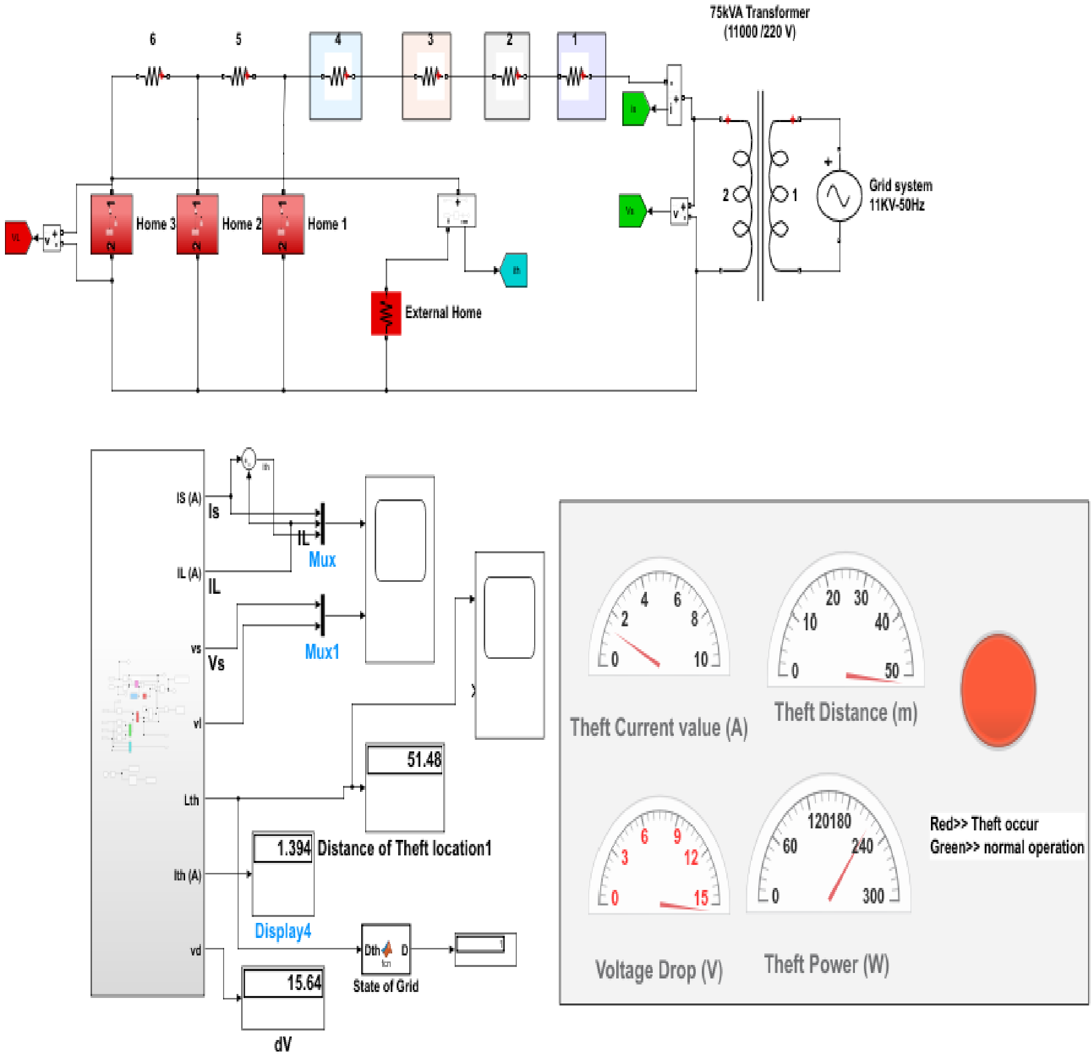


Fig (14) Simulation of a theft detection circuit by using the equations for theft at a distance of 50

Table (4) Determining theft distances in practice using the equation method.

Serial number	Real distance	Distance by algorithm LM
1	0	0
2	10	4,17
3	20	13,44
4	30	22,82
5	40	32,03
6	45	41,69
7	50	51,48

We infer from the above-mentioned simulation results shown in table (4) that the detection method based on the method of using mathematical equations enables us to determine the presence of theft in the distribution system and determines an approximate value of the stolen current, but we were unable to accurately determine the location of the theft, and this matter is considered a major problem In distribution networks, especially large networks that have hundreds of consumers.

4.3- Proposed Neural Network-Based Approach for Power Theft Detection

4.3.1 Neural Network Configuration for Power Theft Detection

The Input, hidden, and output layers are the three different types of NN, and they are all made up of linked artificial neurons see the Fig (14). Each successive layer is made up of many neurons. In general, the weights given to each artificial neuron or link

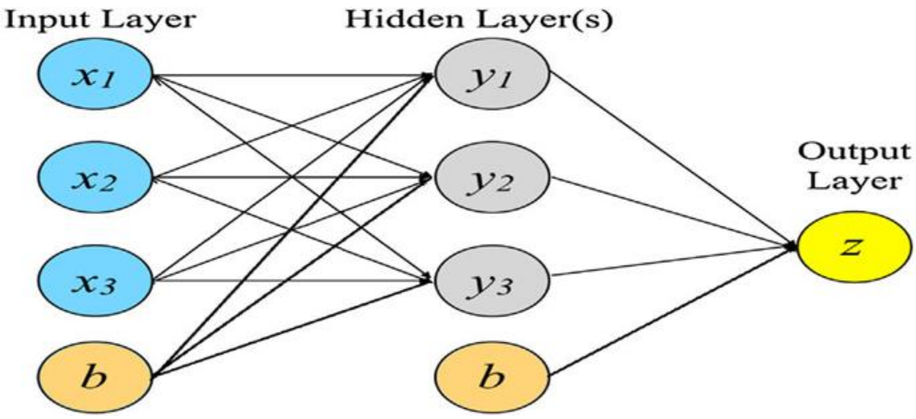


Fig. (15) Configuration of the typical Neural Network (NN) Kannaiyan, M et al (2020).

Directly affect the performance of a NN Kannaiyan, M., & Raghuvaran, J. G. T. (2020) . The train set is used to adjust the weights as learning progresses. How many neurons should be employed in the input and output layers depends on the job size. Nevertheless, try is used to determine the number and size of concealed layers. At the input layer, data is received by the network. The input data is transformed into hidden layers once the biases and weights are applied. The output layer, which is linked to the hidden layers, displays outputs from those layers. In this study, we used the Levenberg-Marquardt (LM) and Feed-Forward Neural Network (FFNN) algorithms learning principles.

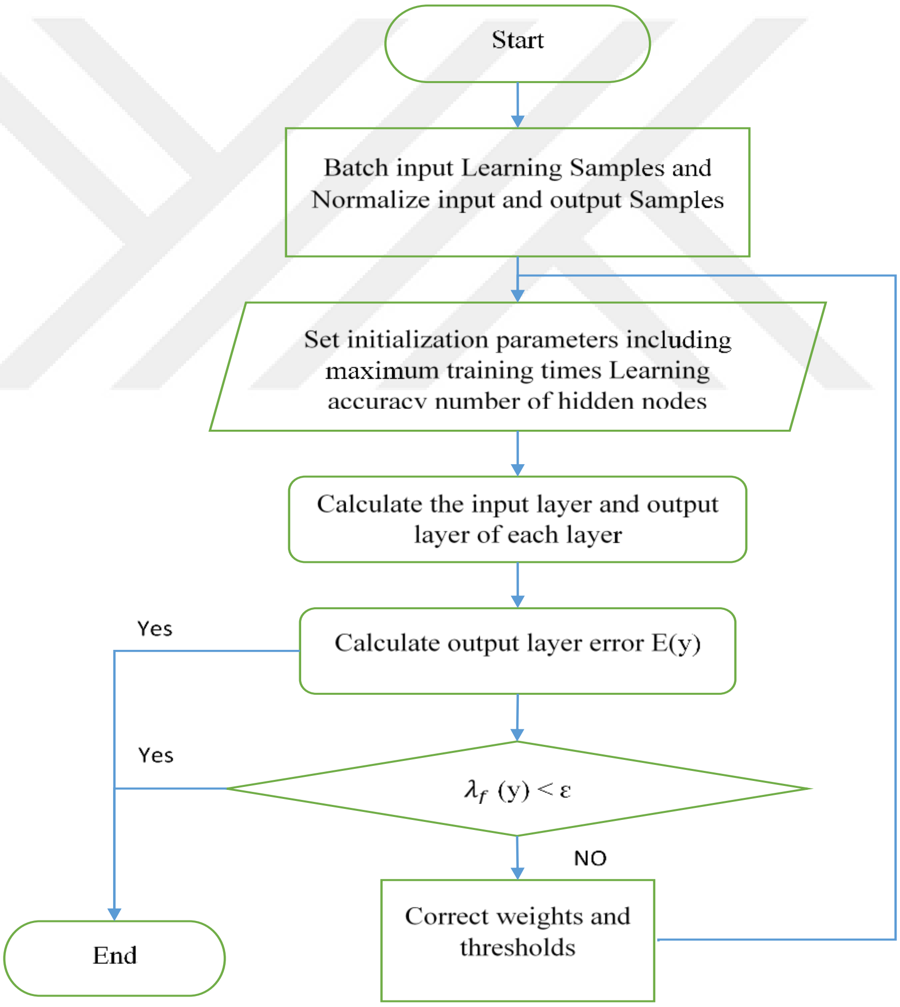

Start
Batch input Learning Samples and Normalize input and output Samples
Set initialization parameters including maximum training times Learning accuracy number of hidden nodes
Calculate the input layer and output layer of each layer
Yes
Calculate output layer error E(y)
Yes
λ_f (y) < ε
NO
End
Correct weights and thresholds

Fig. (15A) flowchart Levenberg-Marquardt backpropagation algorithm Liu, T. Y et al (2020).

4.3.2 Neural Network (NN) Training Algorithm for Power Theft Detection

The pertinent academic literature contains a wide range of NN training techniques. The minimization problem is frequently addressed in NN training utilizing gradient-based methods. They are meant to lessen the amount of lost time brought on by differences between the predictions of the NN model and the actual data Rizk, Y., & Awad, M. (2019). Fig (15) depicts the foundations of how NNs learn. An iterative process of minimizing an error cost function is carried out to obtain the best NN weights for a data set. As a result, a set of adequately trained NN weights is used to create the best possible fit to the measurement data. Gradient-based techniques that are frequently used for NN training include Newton's method, the back-propagation technique (Steepest Descent Method), the conjugate gradient method, the Gauss-Newton (GN) method Ren, Y., & Goldfarb, D. (2019) the Broyden-Fletcher-Goldfarb-Shanno (BFGS) method Egidio, L. N, et al. (2021, July), the Neuron by Neuron (NBN) algorithm Shaheen, B., & Németh, I. (2022), and the Levenberg-Marquardt (LM) algorithm Rizk, Y., & Awad, M. (2019) - Sapna, S, et al (2012), the Feed-Forward Neural Network (FFNN) algorithm.

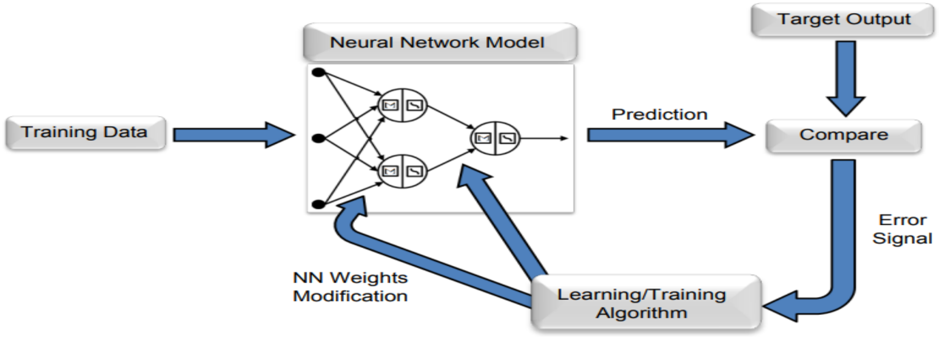


Fig. (16) NN training flowchart process

4.3.3 Theft Detection using the Levenberg-Marquardt (LM) Algorithm.

Backpropagation is used by the LM method as a supervised learning methodology for NNs, training the network with the help of an appropriate iterative method to handle issues involving unrestricted nonlinear optimization. They are used in the NN model's teaching process. In a network using LM backpropagation (LMB), every node serves the same purpose. This method uses the Jacobian matrix (J), a function, to calculate an expected value for the performance being assessed, such as a mean or sum of squared error. The matrix was formatted as follows Rizk, Y., & Awad, M. (2019) for the LMB method:

$$H = J^T J \tag{27}$$

And, the gradient can be calculated as follows:

$$g = J^T e \tag{28}$$

Where e is the error vector.

However, the performance of the LMB can be verified by computing the mean square error (MSE) as presented in Eq (29).

$$MSE = \frac{1}{N}\sum_{i=1}^{N} {e_i}^2 \tag{29}$$

In this study, we use three layers (voltage drop as the input layer, hidden layer and theft distance as the output layer) using 10 neurons-based to build a prediction network for the energy theft location. As seen in Fig. (19) The window of the training LM can be seen in Fig (18). The following is an example of the use of the three-layer LMB backpropagation algorithm:

Step 1: in the first step, the normalizing training data is used to set the starting values for the weights function and bias.

Step 2: in this step, we use the aforementioned equations to calculate the sum total of the hidden layer and output layer (net) neuron outputs Rizk, Y., & Awad, M. (2019).

$$n_i = \sum w_{ij}\, x_i + \theta_i \tag{30}$$

Where w_{ij} is the weight for node j to i and it is computed as follows:

$$w_{ij}\,(n+1) = w_{ij}\,(n) + \alpha\delta_i(n)x_j(n) \tag{31}$$

The parameters of the above equation can be defined as:

- $x_j(n)$ represents the function of the transformation

- α represents the step size of the NN
- δ_i represents the weighted summation of the error
- θ_i is the bias

Step 3: in this step, the weight is updated and the error is calculated.

Step 4: in this step, all weights function are updated, where bias and repeat Steps 2-3 for overall data of training.

Step 5: Repeat steps 2-4 until the error converges and becomes at a good level.

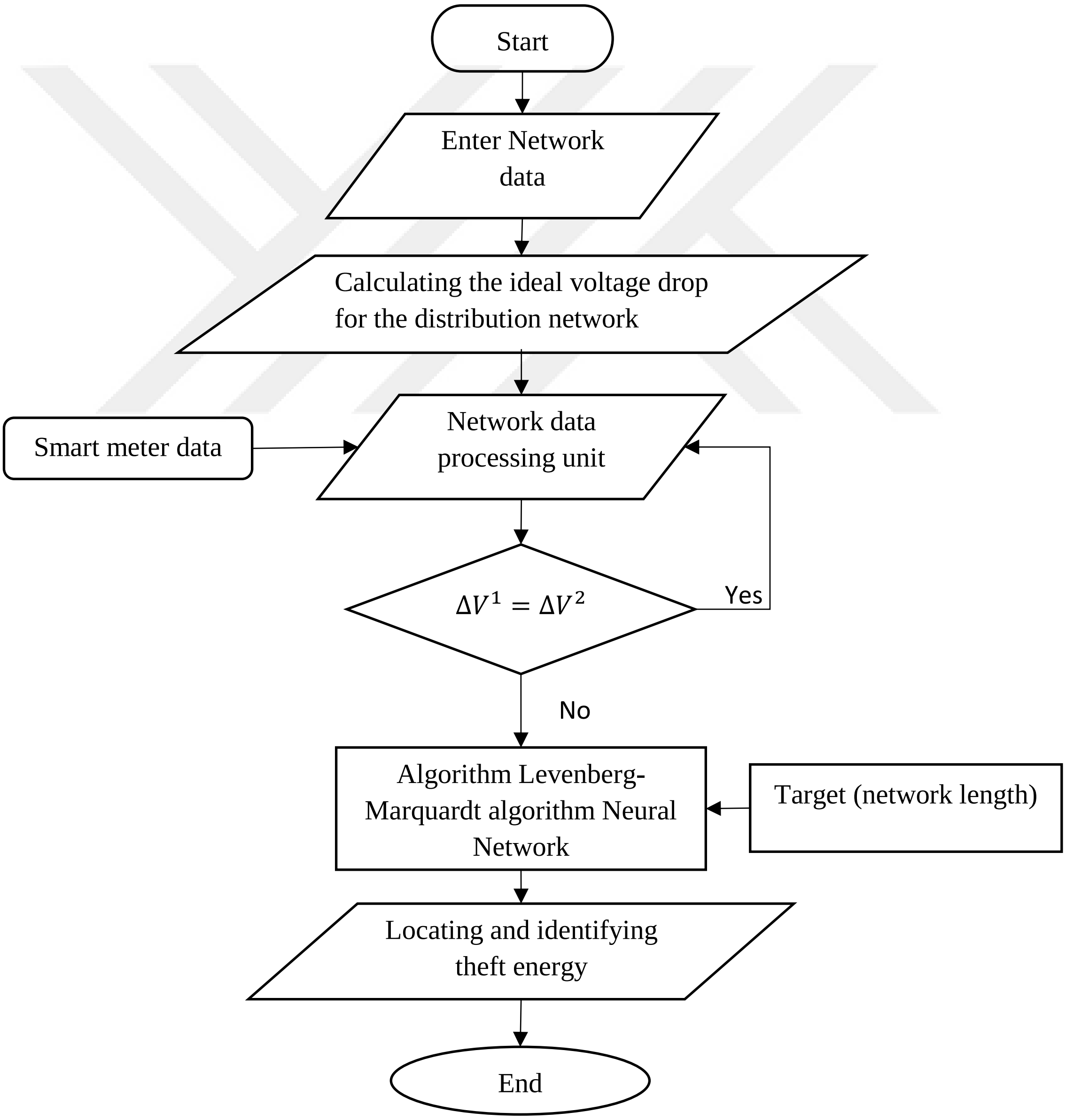
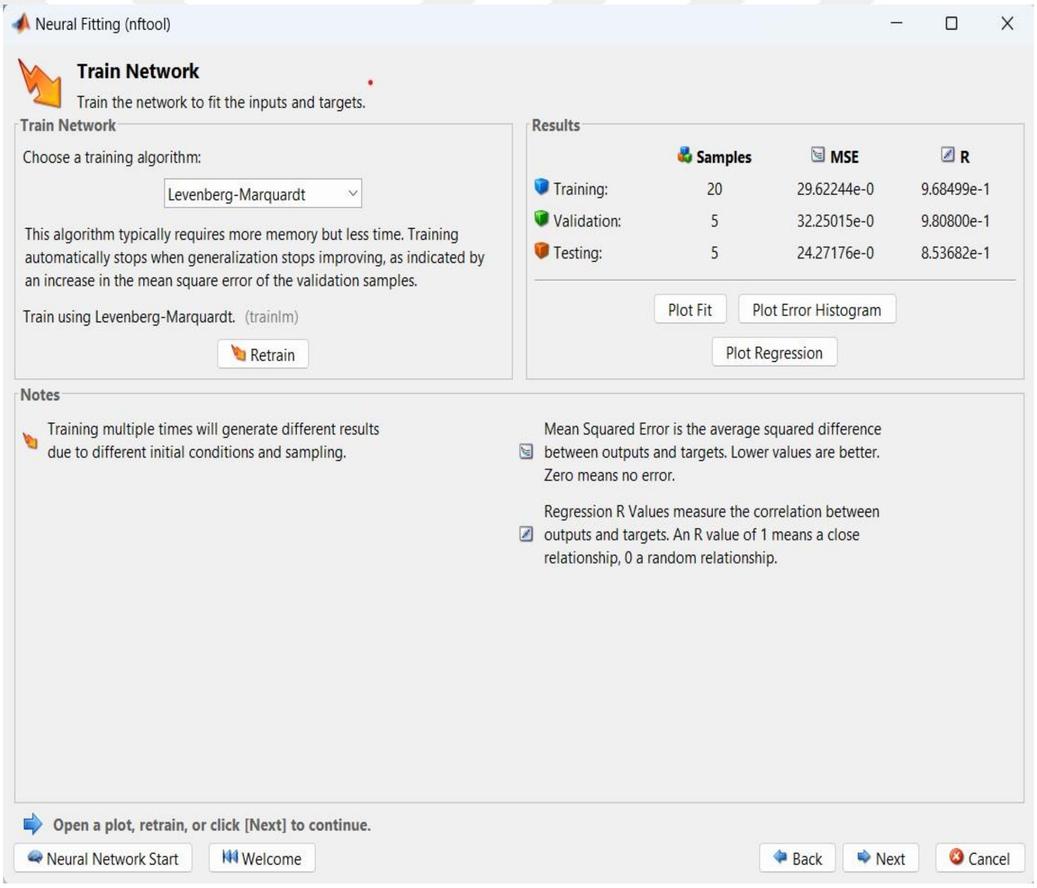

Start
Enter Network data
Calculating the ideal voltage drop for the distribution network
Smart meter data
Network data processing unit
$\Delta V^1 = \Delta V^2$
Yes
No
Algorithm Levenberg-Marquardt algorithm Neural Network
Target (network length)
Locating and identifying theft energy
End

Fig. (17) Flowchart of energy theft detection LM algorithm.

4.3.4 Collected Data for LMB Algorithm in Theft Detection

In this work, the LMB was designed to find the theft location and then classified the theft problem based on the drop voltage value. The voltage drop was calculated during the simulation and the real drop voltage between the source voltage and load voltage at normal conditions and the theft issues are collected and then used as input training data. The theft distance of the network is used as target data for the neural network. Table (5) shows the collected data used in this simulation to test and design the neural. The training samples are 20 samples with 70%, 15 % validation 5 samples, and 15% testing 5 samples as shown in the fig (18).



Train Network

Train the network to fit the inputs and targets.

Train Network

Choose a training algorithm: Levenberg-Marquardt

This algorithm typically requires more memory but less time. Training automatically stops when generalization stops improving, as indicated by an increase in the mean square error of the validation samples.

Train using Levenberg-Marquardt. (trainlm)

Results

	Samples	MSE	R
Training:	20	29.62244e-0	9.68499e-1
Validation:	5	32.25015e-0	9.80800e-1
Testing:	5	24.27176e-0	8.53682e-1

Notes

Training multiple times will generate different results due to different initial conditions and sampling.

Mean Squared Error is the average squared difference between outputs and targets. Lower values are better. Zero means no error.

Regression R Values measure the correlation between outputs and targets. An R value of 1 means a close relationship, 0 a random relationship.

Open a plot, retrain, or click [Next] to continue.

Fig (18). LMB technique used in this work

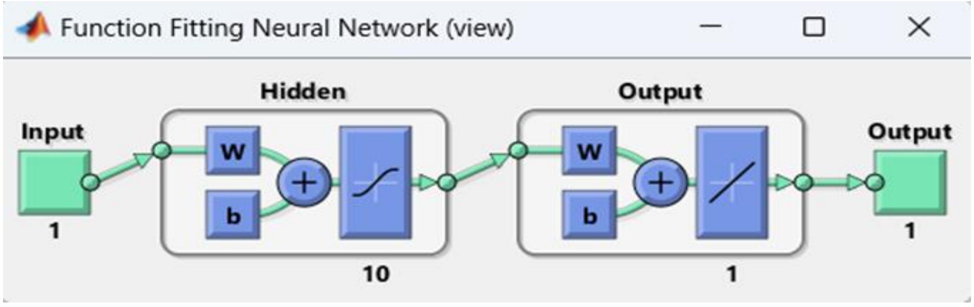


Fig. (19) Proposed LMNN network for theft distance detection.

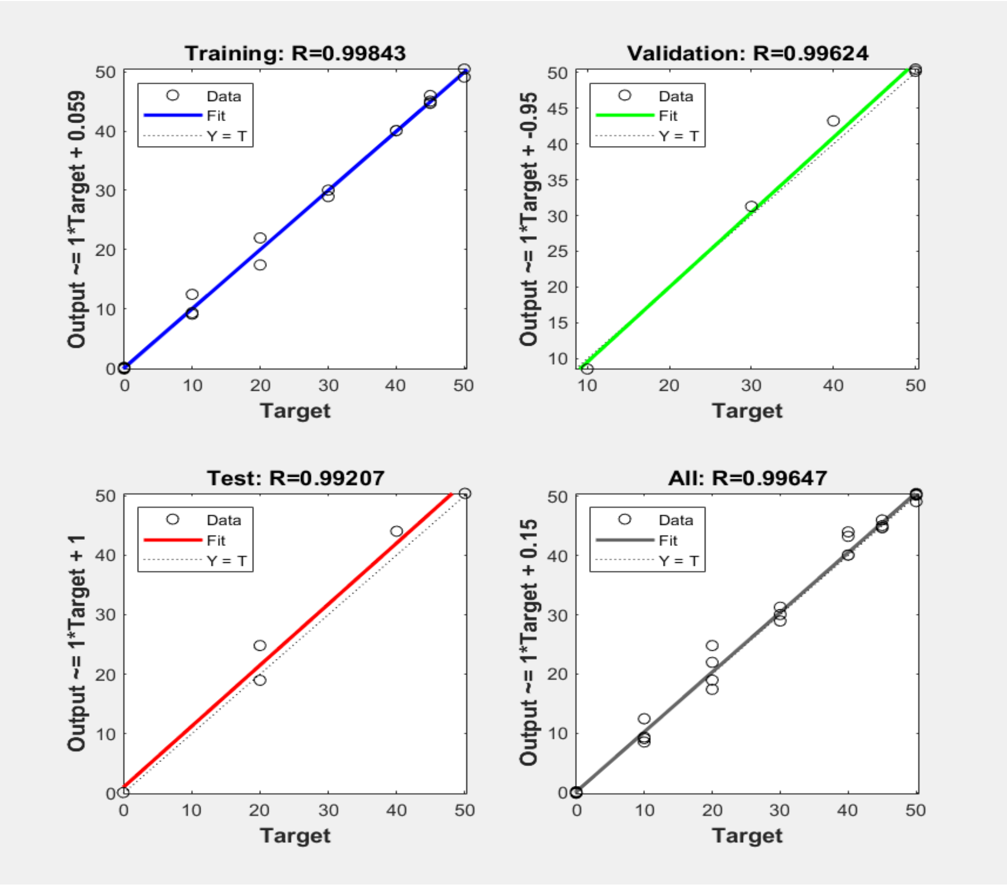


Fig. (20) LMB training regression used in this work

The NN training regression used in this work is shown in Fig. (20) The suggested NN was trained many times under ten epochs in order to reduce error and obtain good values.

Table (5) Collected data when used for the LMB design.

Serial number	input	(Target)	Output of neural
1	8	0	0.9
2	9.5	0	0.94
3	9.7	0	0.25
4	9.9	0	0.24
5	10.3	0	0.004
6	10.8	10	9.6
7	10.99	10	10.5
8	11.4	10	10.7
9	11.5	10	11.3
10	12	20	19.5
11	12.4	20	19.8
12	12.7	20	21.2
13	12.8	20	23.2
14	13	30	28.5
15	13.3	30	30.3
16	13.6	30	30.8
17	14	40	39.7
18	14.2	40	40.5
19	14.5	40	40.7
20	14.7	40	40.7
21	14.8	40	40.8
22	15.1	45	42.5
23	15.2	45	43.3
24	15.5	45	44.5
25	15.7	45	45
26	16	50	48.5
27	16.2	50	49.5
28	16.4	50	50
29	16.7	50	50
30	17	50	50

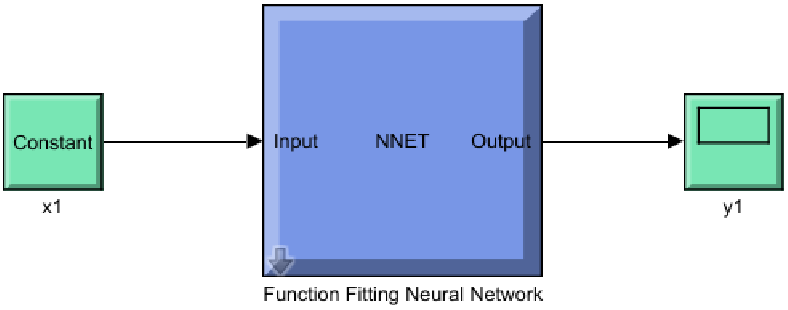


Fig (21) Simulink Levenberg-Marquardt algorithm Neural Network

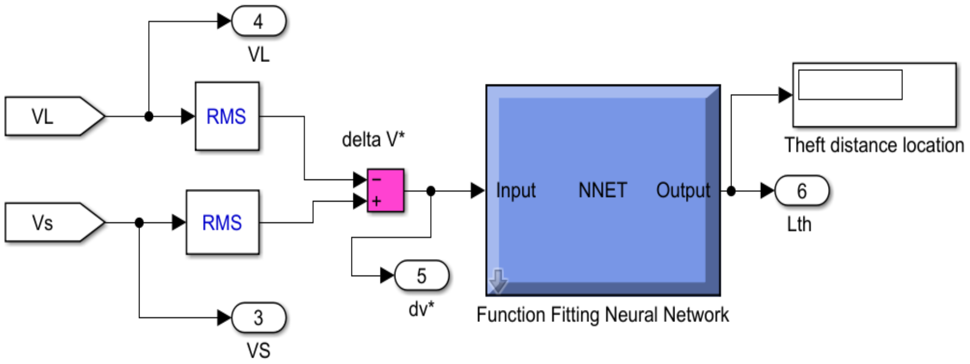


Fig. (21A) Proposed LMNN for theft location.

To validate the suggested Neural Network (NN) approach, the conventional or classical method from reference Uvais, M. (2020, February) was presented. The proposed NN technique was carried out in the MATLAB software using "Nftool," trained using the LMB algorithm Fig (20), and then delivered to Simulink as shown in Fig. (21A). The voltage drop between the Vs and VL serves as the input, and the output of the NN is the distance location. In addition, the fourth theft location is carried out at various zones along the distribution line, and the theft distance, theft current, theft drop voltage, and power of the theft are shown as indicated in Figurers. (23,24,27,28). The first theft occurs 20 m away, the second incident occurs 40 m away, the last theft is 50 m away (at residences in the region), and so on. According to a calculation using the R/L ratio under no-theft conditions, the drop voltage is 9.9 V.

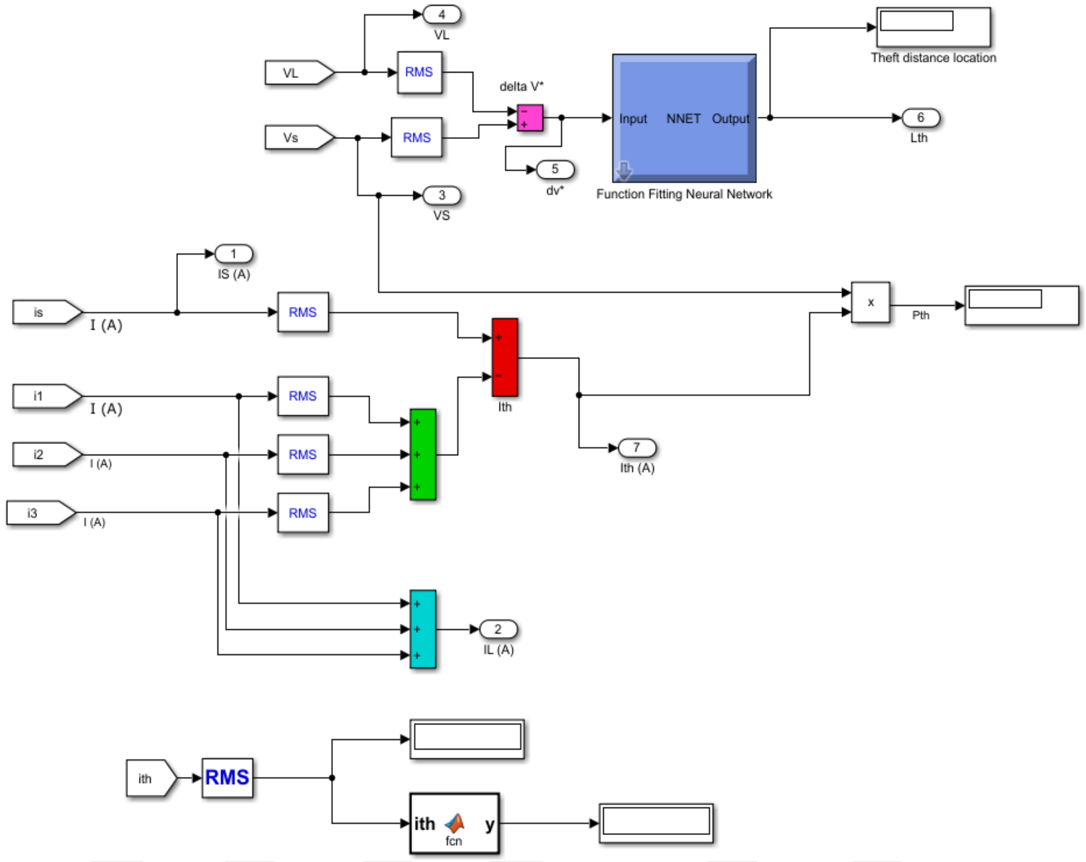


Fig (22) MATLAB/Simulink model subsystem of a theft detection circuit by using the Levenberg-Marquardt algorithm

4.4 Description of the Simulation Circuit for the LMB Algorithm.

The simulation circuit of the MATLAB program consists of a distribution circuit similar to the work of the distribution network, the length of which is 50 m. It contains an electrical power transformer of 11000/220 volts and a transmission line represented by resistors (1, 2 ,3, 4) representing the technical losses in all transmission and each resistance representing the technical losses of ten Meters and the resistors (5,6) representing the technical losses of the transmission line at homes, while (External energy) represents theft energy and the resistances of Home (1,2,3) house loads.

4.4.1 Practical Application: MATLAB Simulation of Case 2 (LM algorithm)

4.4.1.1 without theft

This case is illustrated in Fig (23). When there is no theft or fraud in the meter in the distribution network system, the simulation will clearly show that in the side of the gauges, in the absence of any stolen current, and it will suffice to show the voltage drop in the network resulting only from technical losses (9.9 v).) which is pre-calculated and known to the source, as well as showing the lighting of the detection lamp in the other color to indicate that there is no theft.

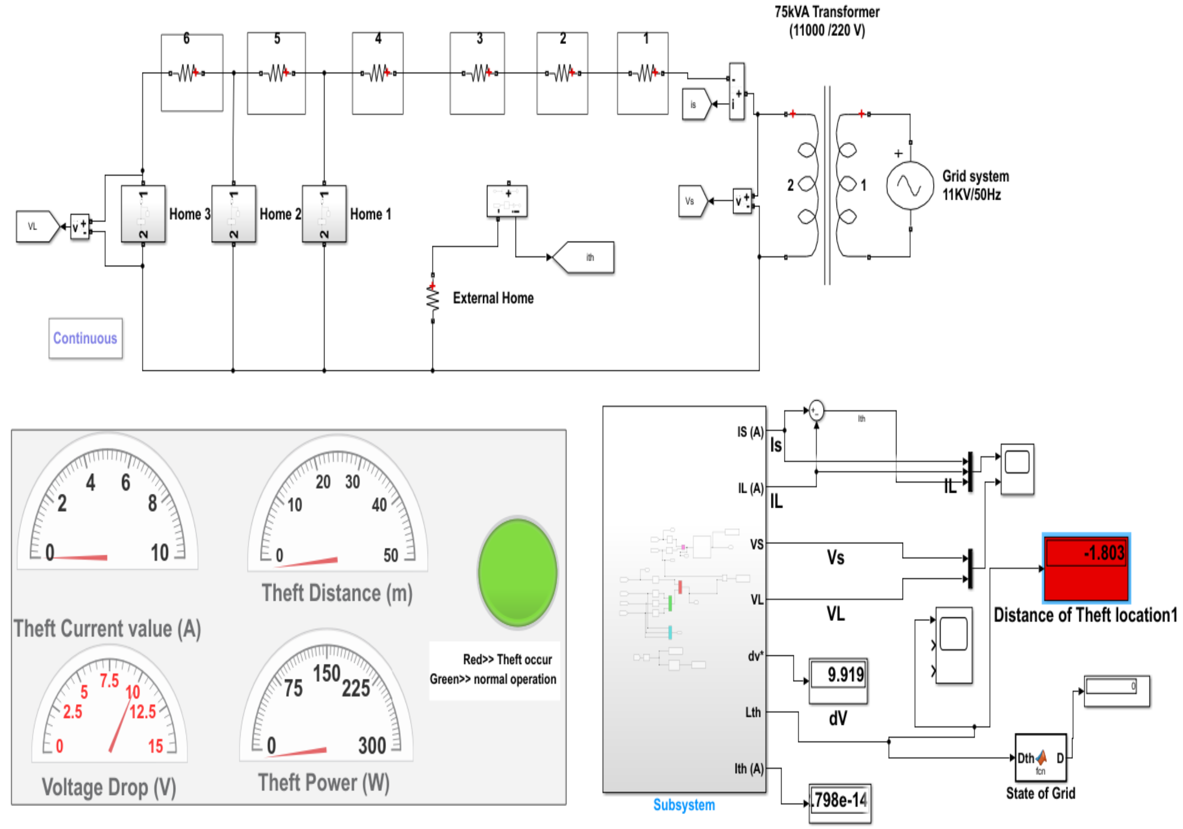


Fig (23) Simulation of a theft detection circuit by using the LM algorithm without theft.

4.4.1.2 with theft

4.4.1.2.1 Theft Detection on the Transmission Line (LM Algorithm): A Distance of 20m

In this case, Fig (24) shows the existence of theft at a distance equivalent to 20 m from the approved distance for measuring the network from the distribution transformer, but the simulation shows through the measures used using case 2 (LM algorithm) the presence of theft according to what is specified in the distance scale at a distance of (21.14m) From the distribution transformer, which is relatively close to the real distance, as it shows the change of the color of the theft detection lamp to red.

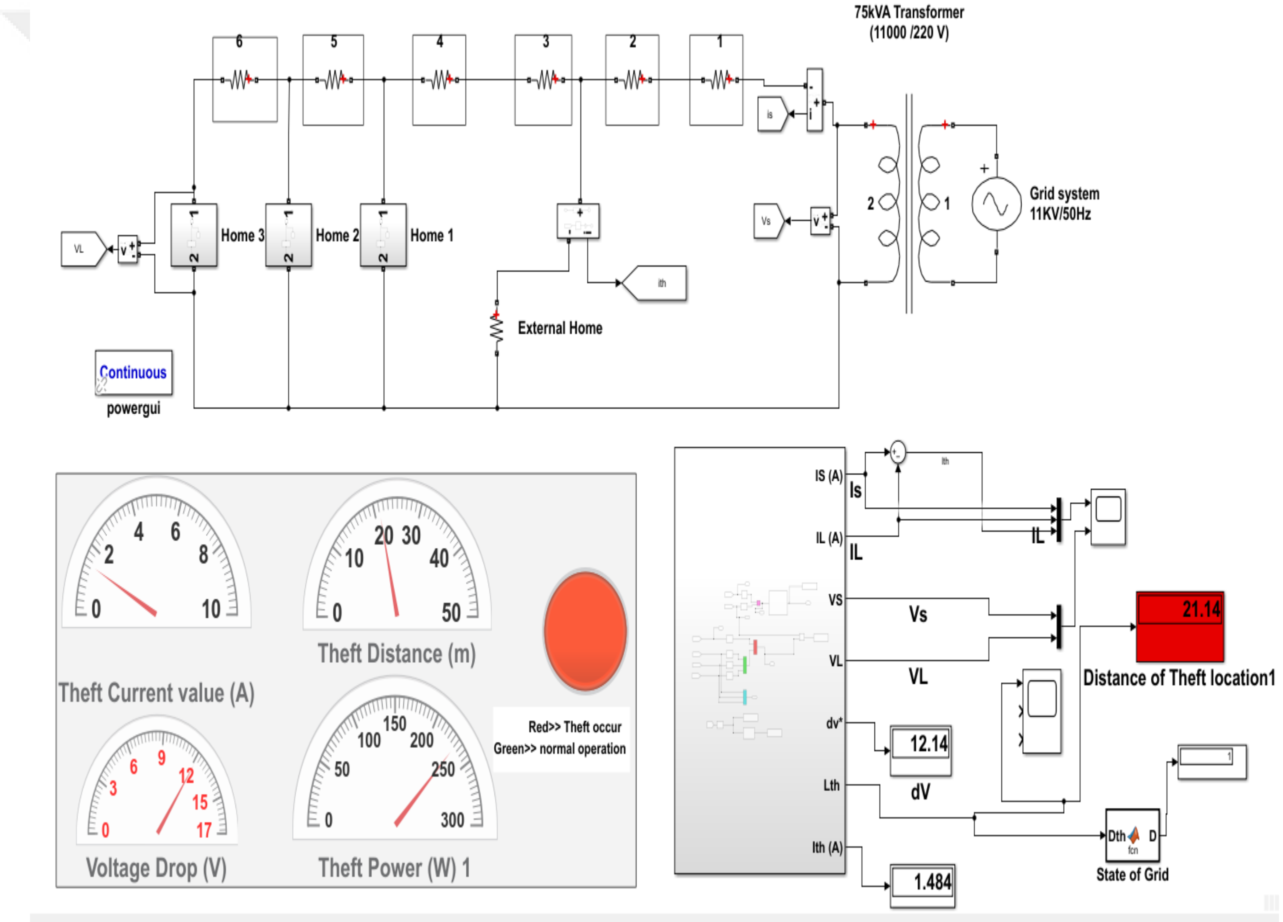


Fig (24) Simulation of theft detection circuit by using LM algorithm at 20m distance.

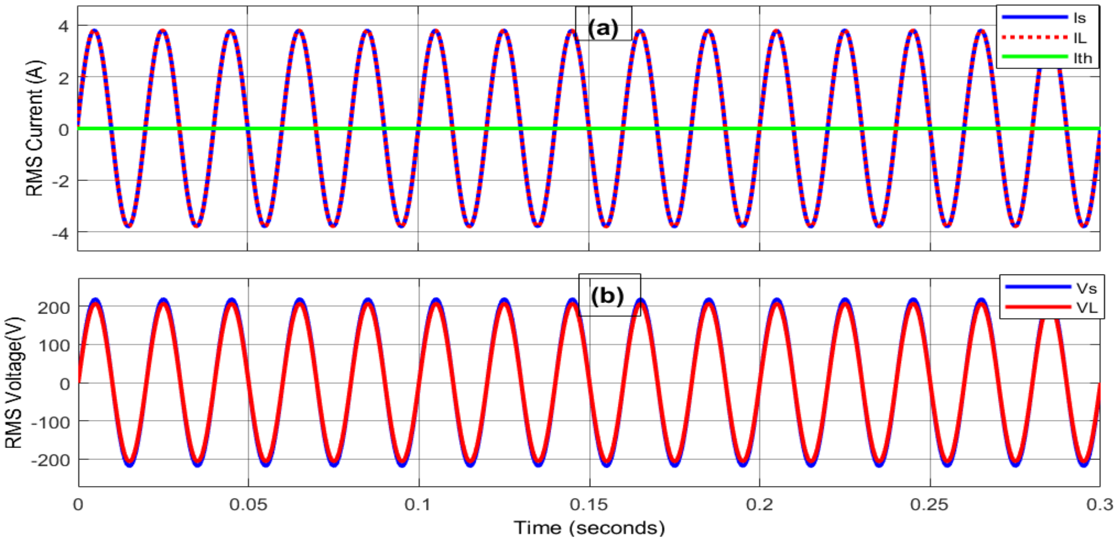


Fig. (25). RMS values of the current and voltage at normal conditions (No theft).

Fig. (25) Shows the source current, total load current, and steal current under typical conditions. The load and supply voltages under typical grid operation are shown also simultaneously. It is evident that the theft current is zero and the source current is equal to the load current at the health distribution line. As illustrated in Fig. (26), when the theft problem occurs, the theft current does not equal zero and instead represents the difference between the load and source currents. At the same time, the drop voltage rises as a result of the fall in load voltage.

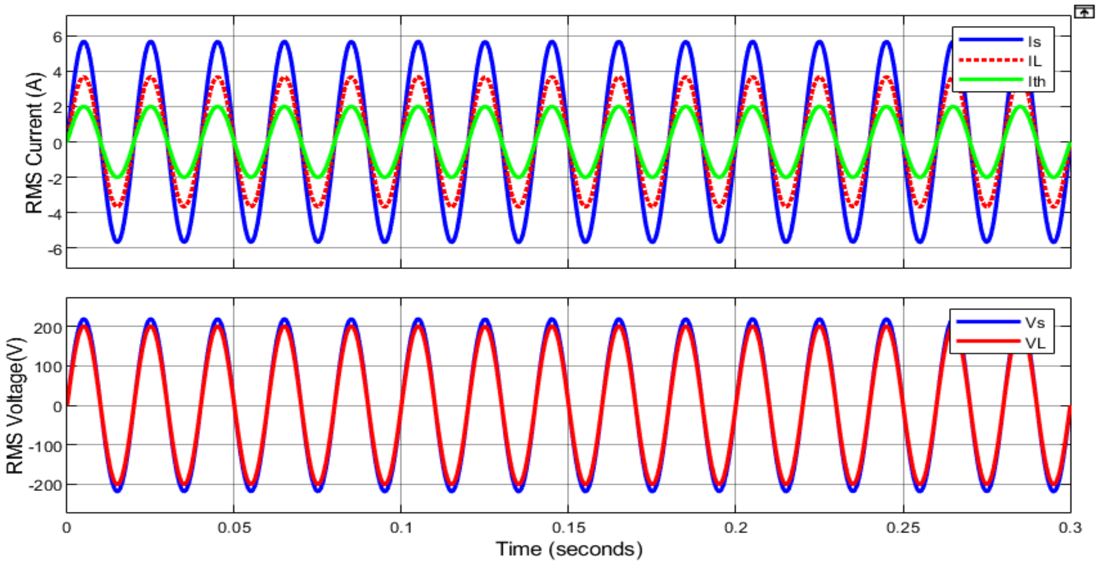


Fig. (26). RMS values of the current and voltage at theft case 2 (LM)

4.4.1.2.2 Theft Detection on the Transmission Line (LM Algorithm): A Distance of 40m.

In this case, Fig (27) shows the presence of theft at a distance equivalent to 40 m from the approved distance for measuring the network from the distribution transformer, but the simulation through the measures used using case 2 (LM algorithm) shows the presence of theft according to what is specified in the distance scale at a distance of (40.61m) From the distribution transformer, which is relatively close to the real distance, as it shows the change of the color of the theft detection lamp to red.

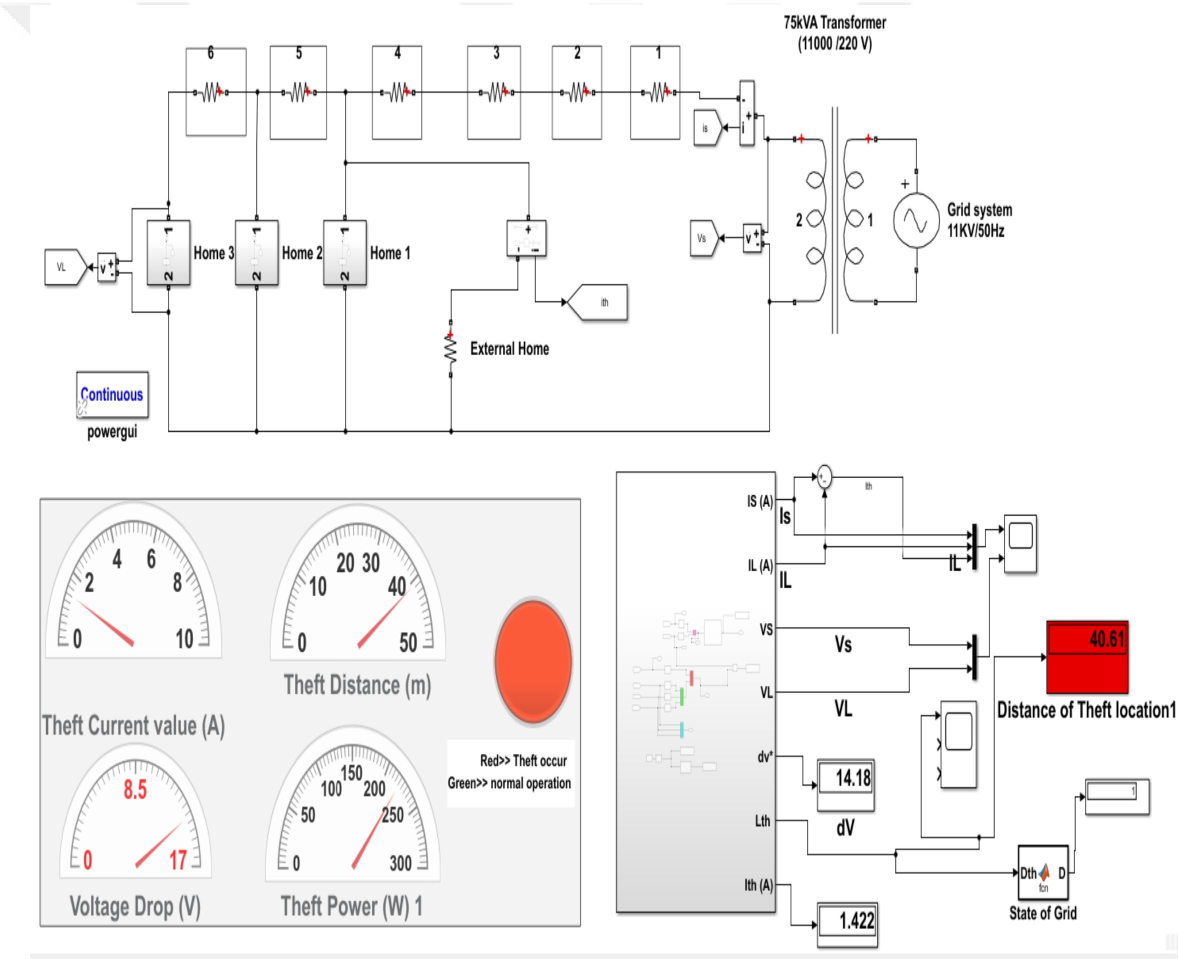


Fig (27) Simulation of theft detection circuit by using LM algorithm at 40m distance.

4.4.1.2.3 Theft Detection at the Last Load in the Network (LM Algorithm): 50m Distance from the Transformer

In this case, Fig (28) shows the presence of theft at a distance equivalent to 50 m from the approved distance for measuring the network from the distribution transformer, but the simulation through the measures used using case 2 (LM algorithm) shows the presence of theft according to what is specified in the distance scale at a distance of (50.33m) From the distribution transformer, which is relatively close to the real distance, as it shows the change of the color of the theft detection lamp to red.

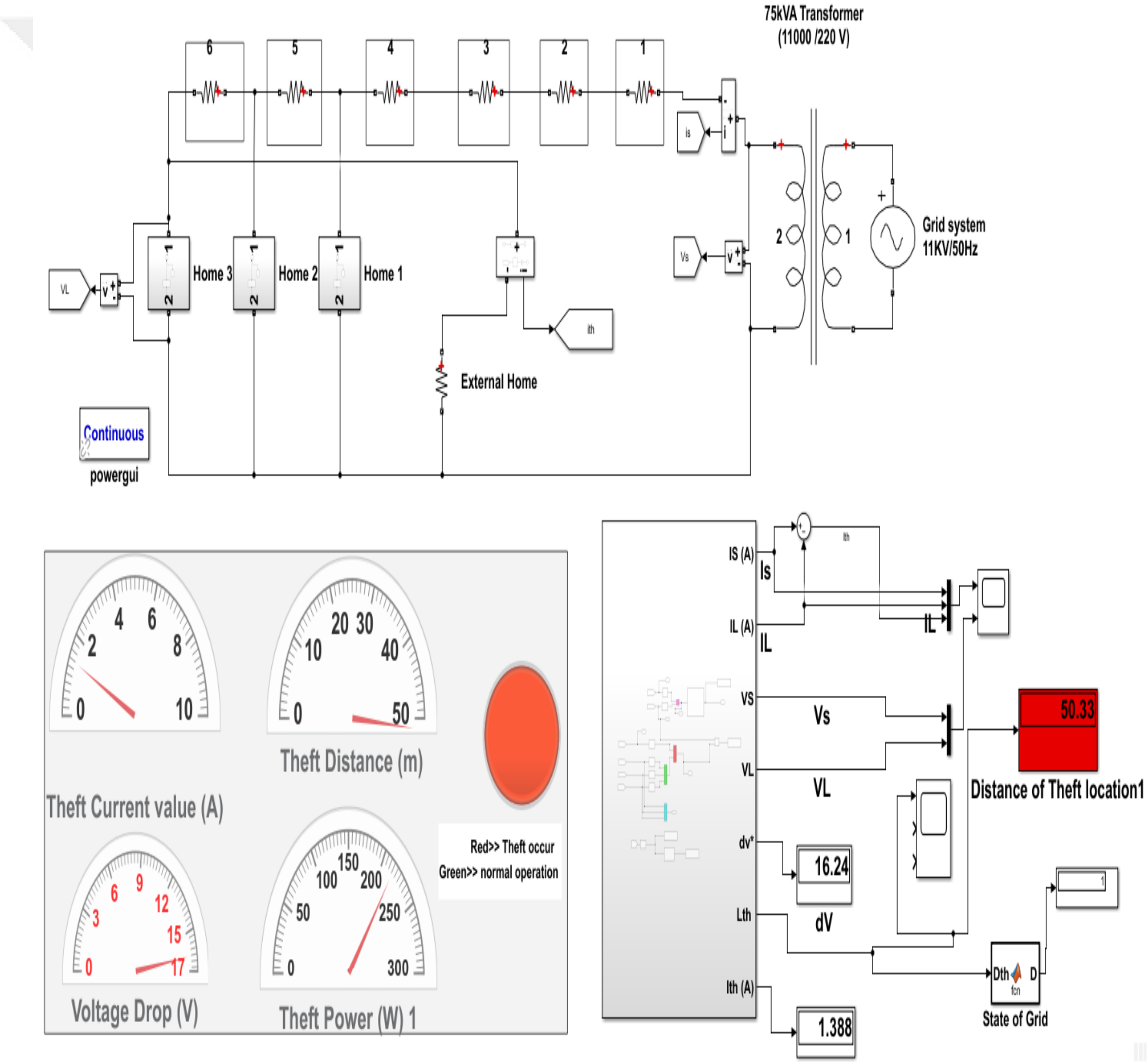


Fig (28) Simulation of theft detection circuit by using LM algorithm at 50m distance

Table (6) Determining theft distances in practice by the LM algorithm.

Serial number	Real distance	Distance by algorithm LM
1	0	0
2	10	9,41
3	20	21,14
4	30	29,6
5	40	40,61
6	45	45,38
7	50	50,33

We see when using the Levenberg-Marquard backpropagation (LMB) algorithm, the results of which are clear through simulation and shown in Table (5), that using this method to detect theft in the power distribution network is more accurate in determining the presence of theft in the power distribution lines and between loads and detecting tampering and cheating in the meters Energy by determining the value of the stolen current, the amount of the actual voltage drop in the network, and the approximate location of the theft in the distribution network.

4.5- Theft Detection using Feed Forward Neural Network (FFNN)

Feed-Forward Neural Networks (FFNN) are the model we use. Only the input nodes, the hidden layers, and finally the output nodes are used to transmit information in a neural network. This suggests that the network's output cannot be returned to the neural network. Compared to other artificial neural networks, the FFNN has a simple structure and functions well in a variety of contexts. Fig. (15) Displays a single hidden layer FFNN model. The hidden layer neurons are identified as $(y_1, y_2, \ldots y_n)$where n is the number of neurons, the inputs are identified as $(x_1, x_2, \ldots x_m)$ where m is the number of input, and the outputs are identified as $(z_1, z_2, \ldots z_k)$ where k is the number of outputs. Each neuron has a certain weight that is connected to every other neuron in the layer below. The weight for the connection from $y_j \; to \; z_k$ is represented by w_{jk}, and the weight for the link from $x_i \; to \; y_j$ is denoted by w_{ij} represents the connection from the input to the hidden layer, while w_{jk} specifies the link between the hidden and output layers.

Applying the activation function (f_1) as described in equation (32) and computing a weighted sum support the movement of input neurons to hidden layer neurons. A weighted sum and an activation function (f_2) are used in equation (33) to depict the change from hidden neurons to output neurons. The neural network model also includes an outside-induced bias, denoted by b. The bias influences increasing or decreasing the activation function net input depending on whether it is positive or negative. Depending on the nature of the issue, the activation function may take different shapes; for multiclass classification issues, softmax activation is used, whereas the sigmoid activation function is used for binary classification Uvais, M. (2020) - Ge, M., Syed, et al. (2021). As illustrated, the proposed model consists of an input layer, ten hidden layer blocks, and an output layer.

$$y_i = f_1(\sum_{i=1}^{m} x_i w_{ij} + b) \qquad (32)$$

$$z_k = f_2(\sum_{j=1}^{n} y_j w_{jk} + b) \qquad (33)$$

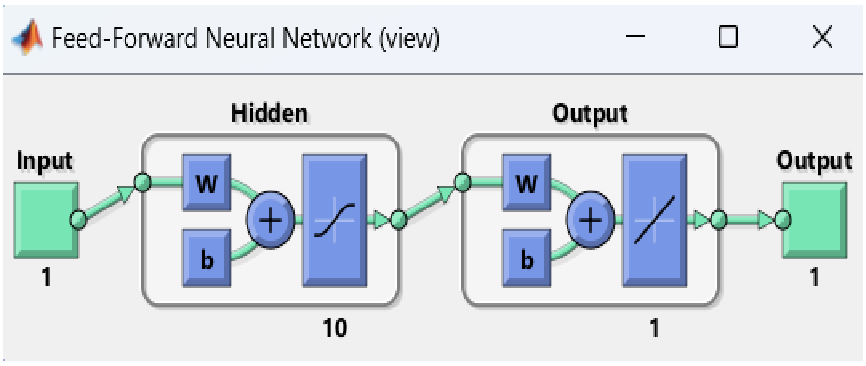


Fig. (29). A Single Hidden Layer FFNN Model

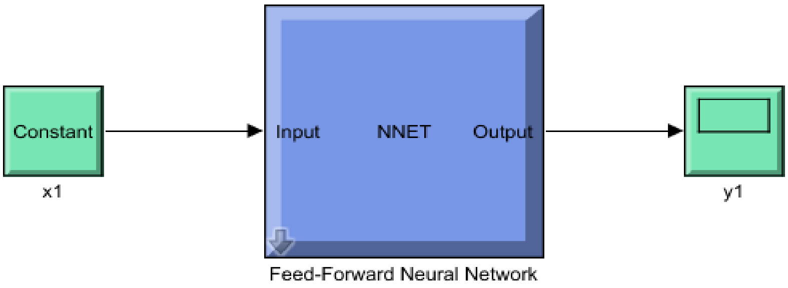


Fig. (30) Simulink Feed-Forward Neural Network

The traditional or classical method used in reference Uvais, M. (2020) is introduced to validate the proposed NN method. The FFNN algorithm was prepared and trained on one hidden layer containing ten neurons as shown in Fig (29) and sent to Simulink to deal with the incoming data to drop the voltage as shown in Fig (30) and locate the theft. After obtaining the best training results.

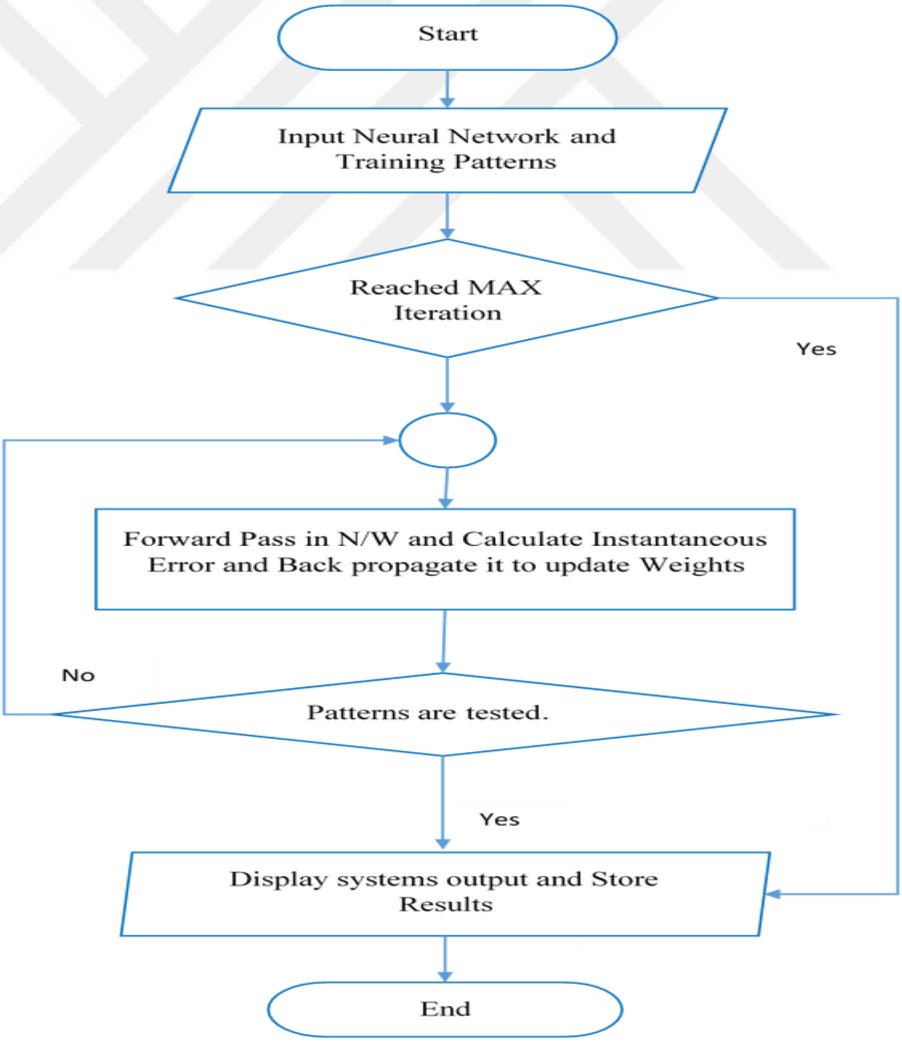

Start
Input Neural Network and Training Patterns
Reached MAX Iteration
Yes
Forward Pass in N/W and Calculate Instantaneous Error and Back propagate it to update Weights
No
Patterns are tested.
Yes
Display systems output and Store Results
End

Fig (31A) Flowchart Feed-Forword neural network Algorithm.

4.5.1 Collected Data for Feed Forward Neural Network (FFNN) in Theft Detection

In this work, the FFNN was designed to find the theft location and then classified the theft problem based on the drop voltage value. The voltage drop was calculated during the simulation and the real voltage drop between the source voltage and load voltage under constant and variable load conditions and theft issues was collected and then used as input training data. The theft distance of the network is used as target data for the NN network. Code MATLAB shows the collected data used in this simulation to test and design the neural.

```
clc
clear all
x1=[2.7421;4.15995;2.2571;3.4502;2.5021;3.21375;2.58281;...

3.11104;4.51989;2.62915;3.81469;2.87267;3.5797;2.95278;...

3.4704;4.8675;2.99265;4.16822;3.234119;3.93519;3.31355;...
     3.82003;5.20236;3.34733;4.5103;3.58621;4.27981;3.6647;...
     4.16553;5.53;3.669;4.854;3.933;4.626;4.011;...
     4.1416;5.50696;3.6748;4.81675;3.91299;4.59124;3.989;...
     4.1303;5.496;3.6633;4.8057;3.90159;4.5756;3.9799];
x=x1';
t1=[0;0;0;0;0;0;0;10;10;10;10;10;10;10;20;20;20;20;20;20;20;30
;30;30;30;30;30;30;40;40;40;40;40;40;40;45;45;45;45;45;45;45;5
0;50;50;50;50;50;50];
t=t1';
net = feedforwardnet([10]);
net.layers{1}.transferFcn = 'tansig';
%  net.layers{2}.transferFcn = 'tansig';
% net.layers{3}.transferFcn = 'tansig';
% net.layers{4}.transferFcn = 'tansig';
net.divideFcn='dividetrain';
net = configure(net,x,t);
net = init(net);
net.trainParam.epochs =150;
net = train(net,x,t);
 view(net)
y = net(x);
perf = perform(net,y,t)
g=gensim(net,-1);
```

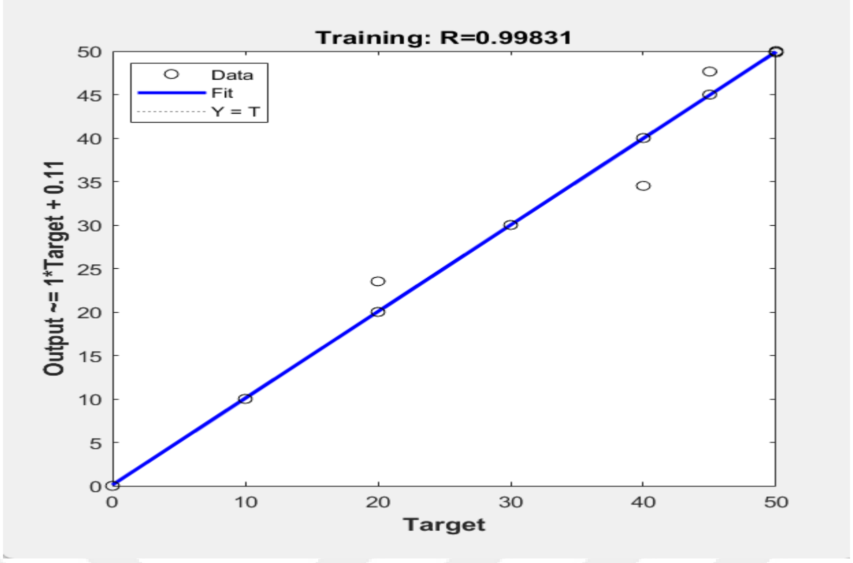


Fig. (31) FFNN training regression used in this work

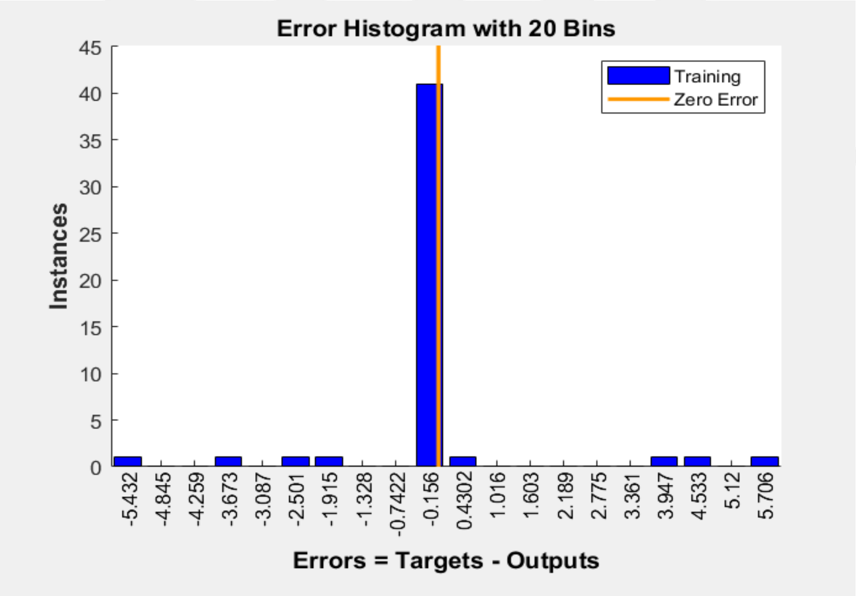


Fig. (32) FFNN Error histogram in this work

Fig (31) shows the regression of the FFNN training used in this work. The proposed NN is trained several times to reduce the error and obtain the best well values. The network fault graph has been shown in Fig (32).

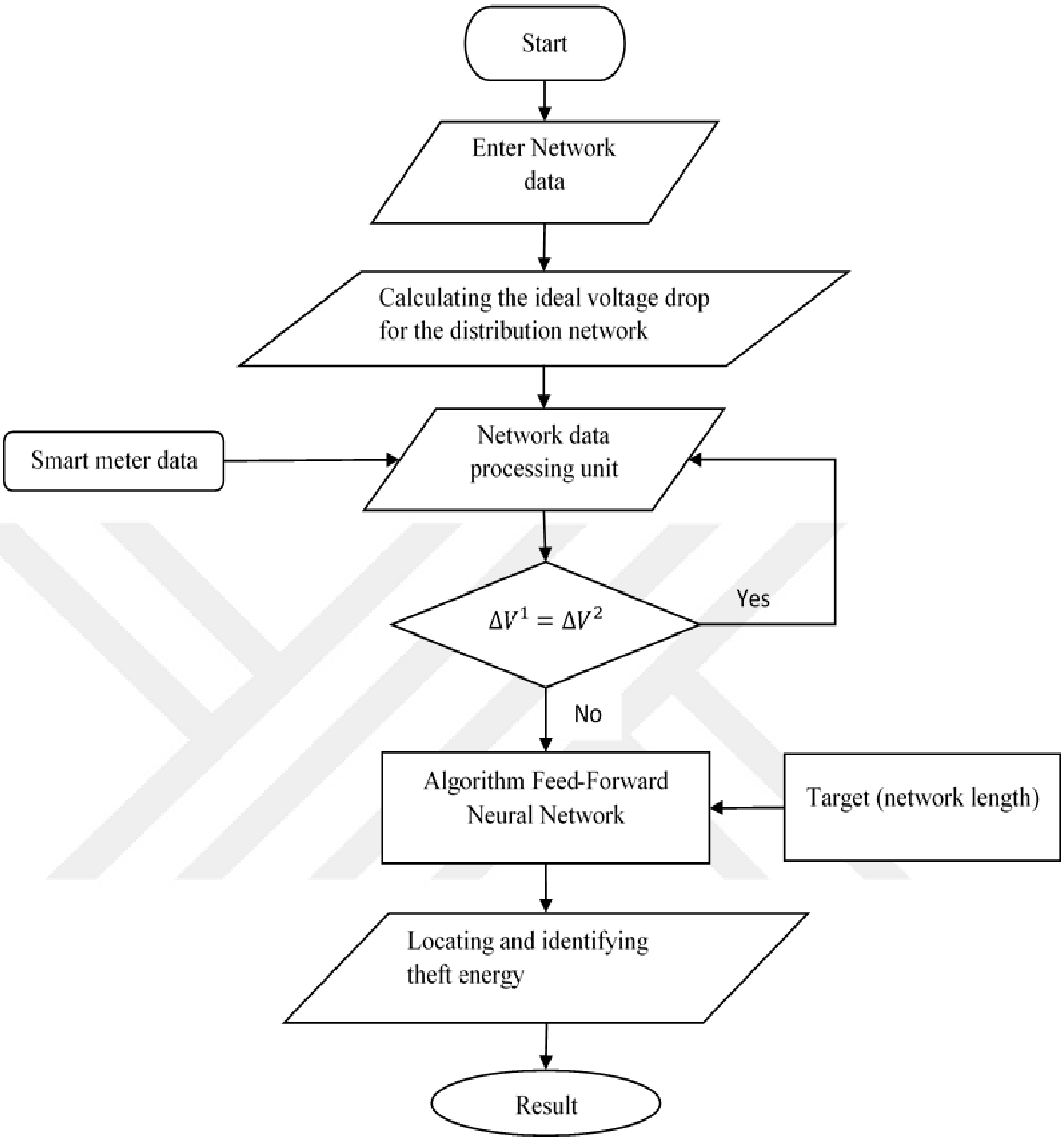

Start
Enter Network data
Calculating the ideal voltage drop for the distribution network
Smart meter data
Network data processing unit
$\Delta V^1 = \Delta V^2$
Yes
No
Algorithm Feed-Forward Neural Network
Target (network length)
Locating and identifying theft energy
Result

Fig. (33) Flowchart of energy theft detection by FFNN algorithm.

4.5.2 Description of the Simulation Circuit for the Feed-Forward Algorithm.

The simulation circuit of the MATLAB program consists of a distribution circuit similar to the work of the distribution network, the length of which is 50 m. It contains an electrical power transformer of 11000/220 volts and a transmission line represented by resistors (1,2,3,4) representing the technical losses in all transmission and each resistance representing the technical losses of ten Meters and the resistors (5,6) representing the technical losses of the transmission line at homes, while (External energy) represents theft energy and the resistances of Home (1,2,3) house loads.

4.5.2 Practical Application Simulation in MATLAB Case 3 (Feed-Forward NN)

4.5.2.1. without theft

This case is illustrated in Fig (34). When there is no theft or fraud in the meter in the distribution network system, the simulation will clearly show that on the side of the gauges, in the absence of any stolen current, and it will suffice to show the voltage drop in the network resulting only from technical losses, which is calculated In advance and known to the source, as shown by the lighting of the detection lamp in the other color to indicate that there is no theft.

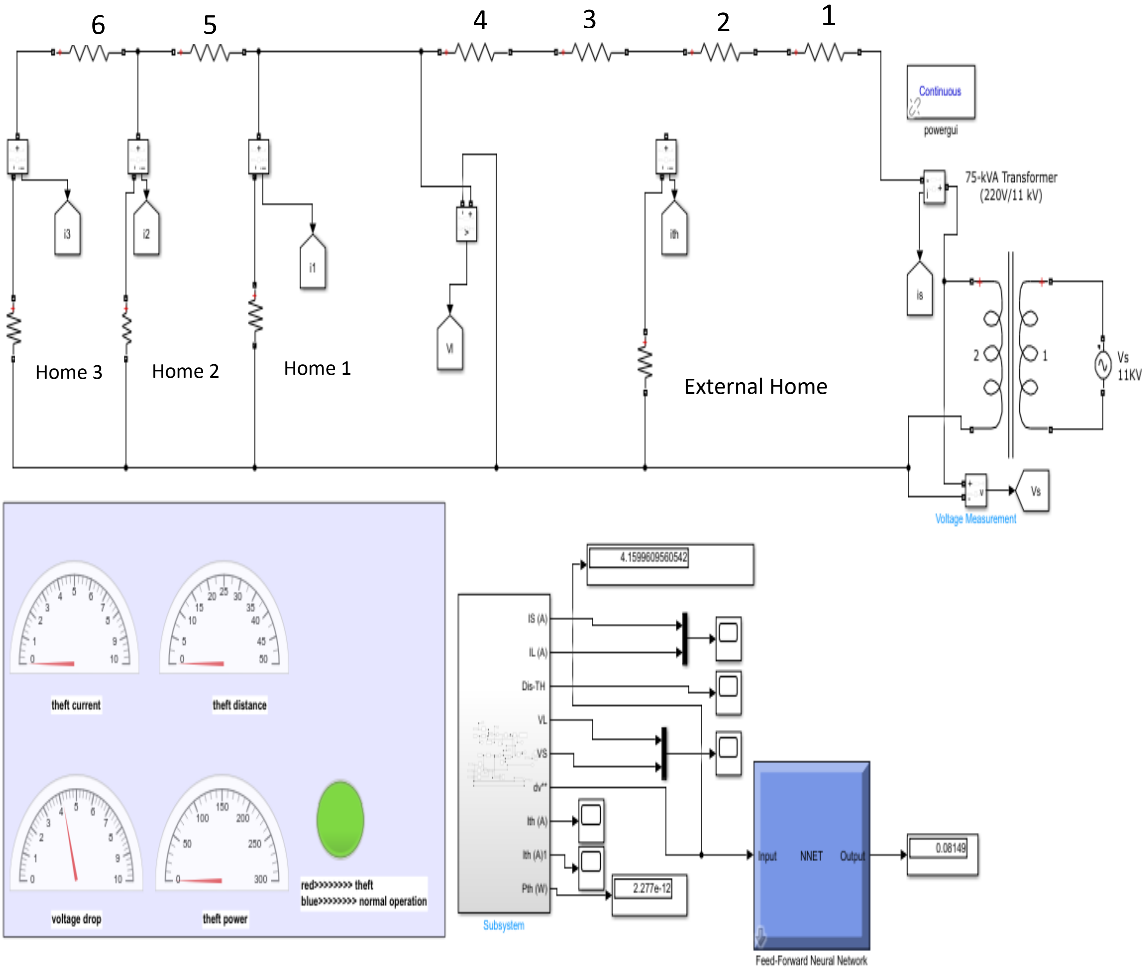


Fig (34) Simulation of a theft detection circuit by using the Feed-Forward algorithm without theft

4.5.2.2. with theft

4.5.2.2.1 Theft Detection on the Transmission Line (FFNN): A Distance of 20m

In this case, Fig (35) shows the presence of theft at a distance equivalent to 20 m from the approved distance for measuring the network from the distribution transformer, but the simulation through the measures used using case 2 (feed-forward algorithm) shows the presence of theft according to what is specified in the distance scale at a distance 19.89 m from the distribution transformer, which is relatively close to the real distance, as it shows the change of the color of the theft detection lamp to red.

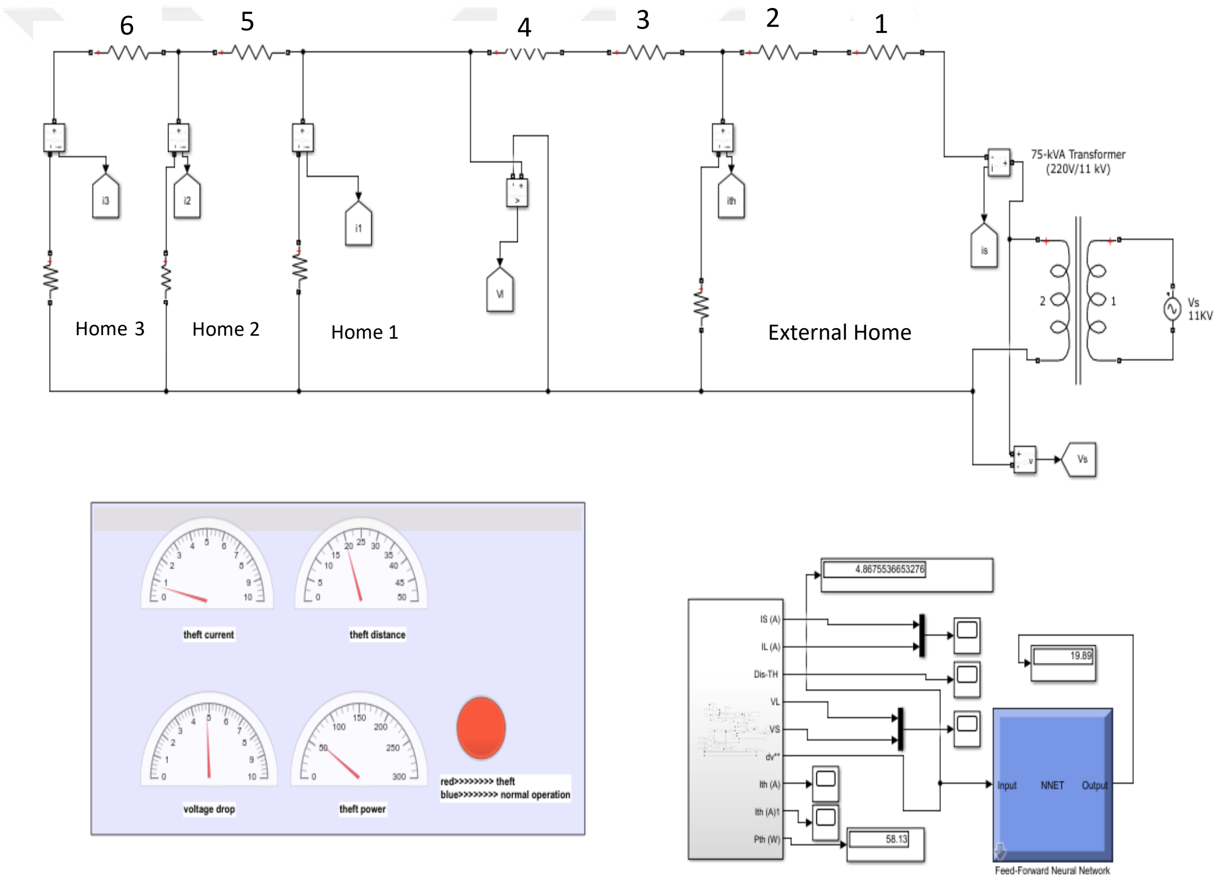


Fig (35) Simulation of theft detection circuit by using Feed-Forward algorithm at 20m distance

4.5.2.2.2 Theft Detection Between the Second and Third Load (FFNN): 45m Distance from the Transformer.

In this case, Fig (36) shows the presence of theft at a distance equivalent to 45 m from the approved distance for measuring the network from the distribution transformer, but the simulation through the measures used using case 3 (feed-forward algorithm) shows the presence of theft according to what is specified in the distance measure at a distance 45 m from the distribution transformer, which is exactly the same ratio as the real distance, as shown by the change of the color of the theft detection lamp to red.

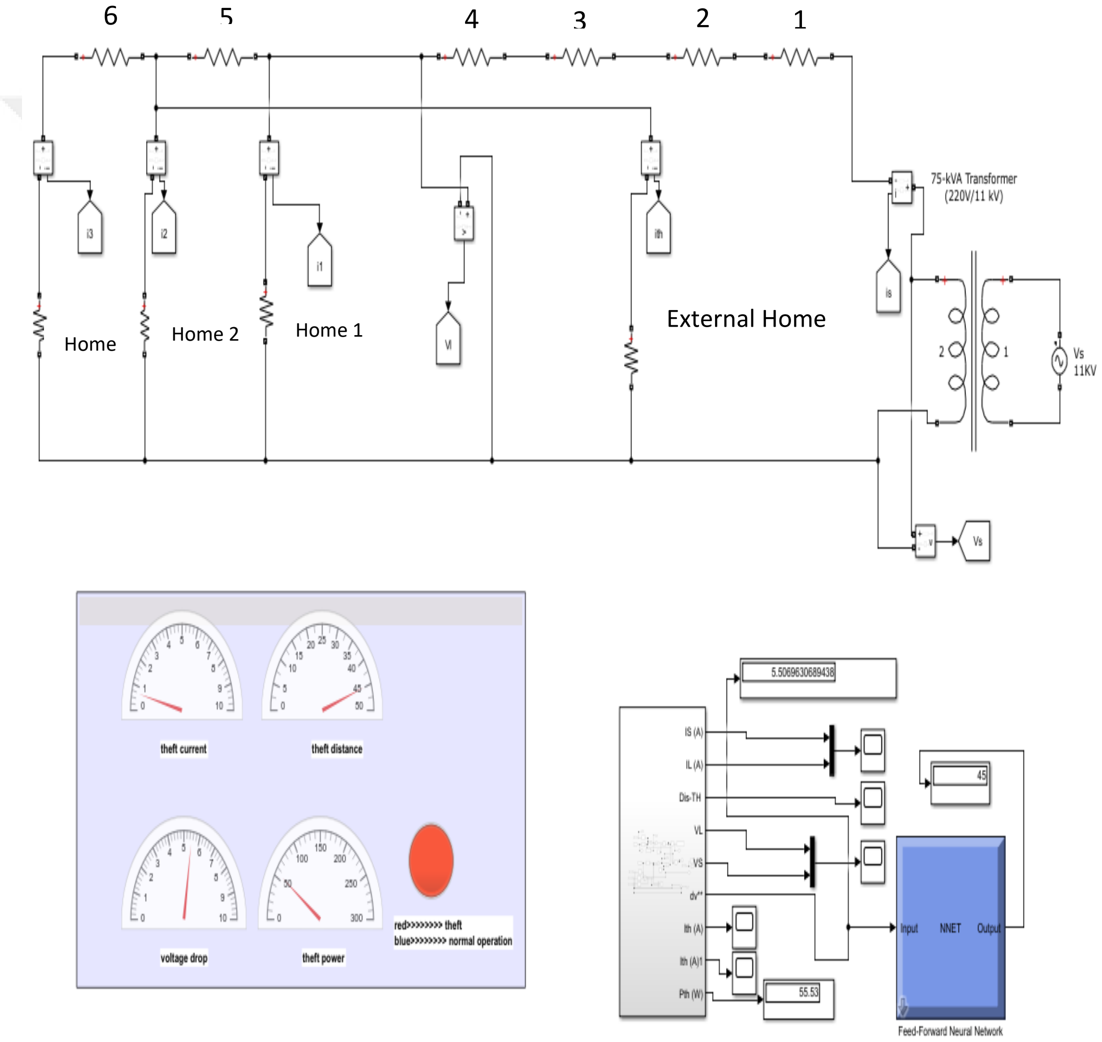


Fig (36) Simulation of theft detection circuit by using Feed-Forward algorithm at 45m distance.

4.5.2.2.3 Theft Detection at the Last Load in the Network (FFNN): 50m Distance from the Transformer

In this case, Fig (37) shows the presence of theft at a distance equivalent to 50 m from the approved distance for measuring the network from the distribution transformer, but the simulation through the measures used using case 3 (feed-forward algorithm) shows the presence of theft according to what is specified in the distance measure at a distance 49.99 m from the distribution transformer, which is relatively close to the real distance, as it shows the change of the color of the theft detection lamp to red.

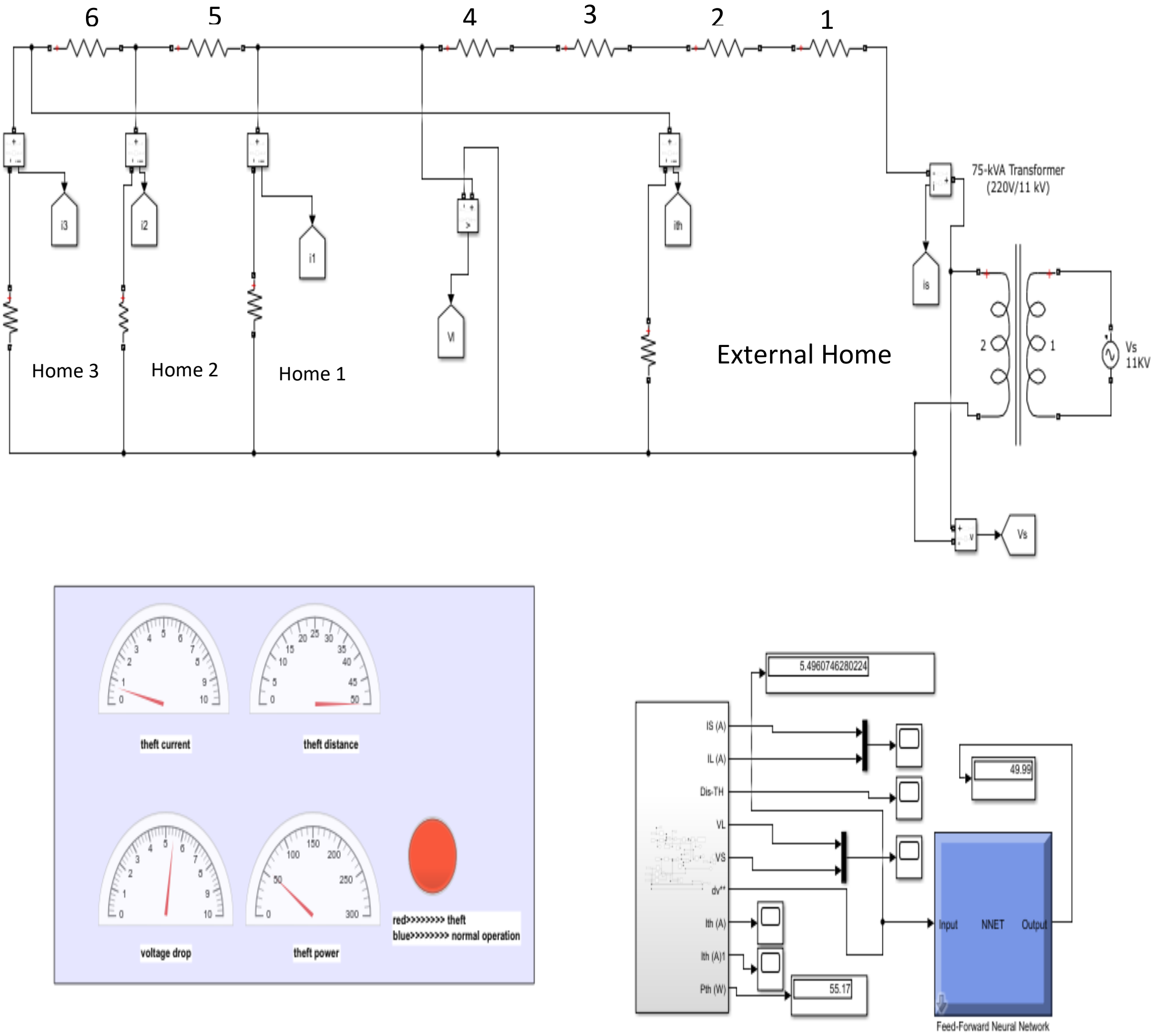


Fig (37) Simulation of theft detection circuit by using Feed-Forward algorithm at 50m distance.

Table (7). Determining theft distances in practice by the Feed-Forward Network

Serial number	Real distance	Distance by algorithm LM
1	0	0
2	10	9,97
3	20	19,89
4	30	30
5	40	40,34
6	45	45
7	50	49,99

It is very clear that the results of the Feed-Forward Neural Network method are accurate in detecting theft from the distribution network and fraud on the energy meter, as shown in Table. (7), with the possibility of determining the value of the stolen current. This is a result of entering integrated data for the distribution network, consumer loads, and repeated training of the algorithm on different expected values of the voltage drop resulting from theft for most parts of the network.

CHAPTER FIVE

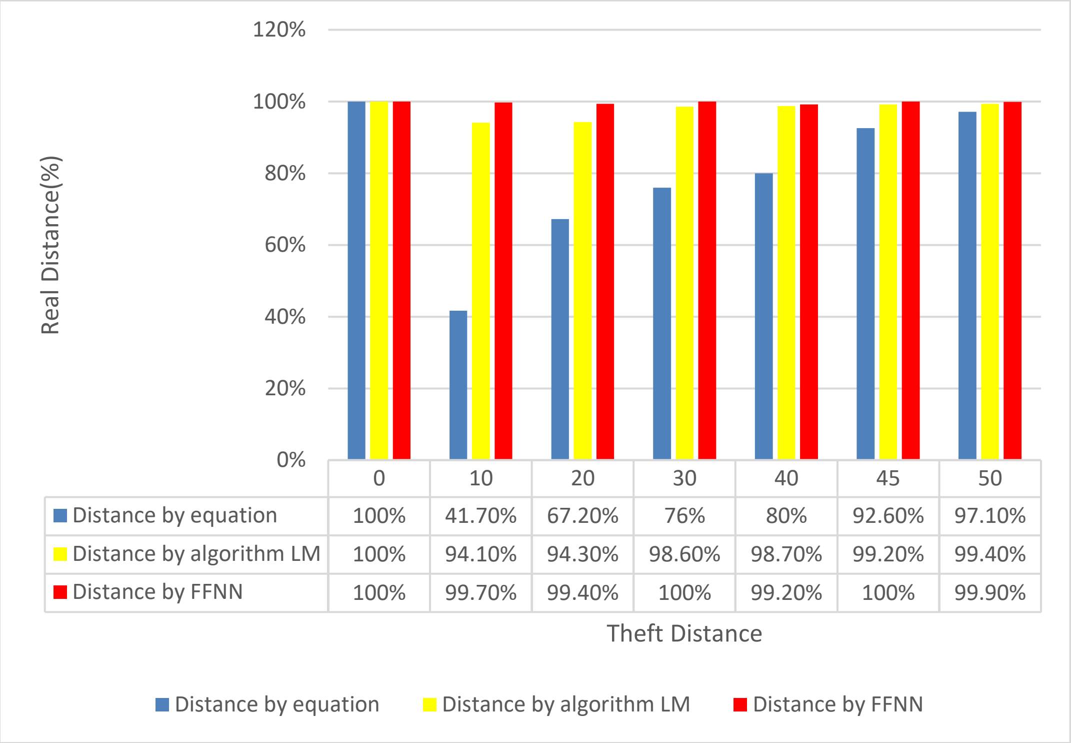
RESULTS AND COMPARISON

5. Results

On the basis of the balanced system Fig (8), the system is designed in MATLAB (Simulink), and a branch impedance value was obtained, which is dedicated to network configuration and operation. The outcome, as shown in Table (8) and Fig (38), shows a very high level of accuracy. The values listed as actual values appear in the form's second vertical field. Other field values, however, are categorized as values discovered through theft detection. The algorithm (calculated values) is being used. And in order to be able to show us which are the best methods that have been studied in this thesis, we make a compare between the results of the detection of the three methods in indicating the sites of theft on the network within the simulation of the MATLAB program to show which methods have the least error rate in them, so that we will later conduct another simulation of the Feed-Forward algorithm method in indicating the sites of theft when load values change.

Table. (8) For actual data and data detected by algorithms.

Serial number	Real distance	Distance by equation		Distance by LM algorithm		Distance by FFNN algorithm	
		value	Matching ratio	value	Matching ratio	value	Matching ratio
1	0	0	100%	0	100%	0	100%
2	10	4.17	41.7%	9.41	94.1%	9.97	99.7%
3	20	13.44	67.2%	21.14	94.3%	19.89	99.4%
4	30	22.82	76%	29.6	98.6%	30	100%
5	40	32.03	80%	40.61	98.7%	40.34	99.2%
6	45	41.69	92.6%	45.38	99.2%	45	100%
7	50	51.48	97.1%	50.33	99.4%	49.99	99.9%
Total Matching ratio			79.2%		97.7%		99.7%



	0	10	20	30	40	45	50
🟦 Distance by equation	100%	41.70%	67.20%	76%	80%	92.60%	97.10%
🟨 Distance by algorithm LM	100%	94.10%	94.30%	98.60%	98.70%	99.20%	99.40%
🟥 Distance by FFNN	100%	99.70%	99.40%	100%	99.20%	100%	99.90%

Fig (38). Compare the results of the detection of the three methods

The system is intended to operate in a steady state in single-phase system. There won't be any unbalanced operations as a result of a failure or short circuit. It was initially initiated with the restriction of no theft. The transformer and smart meter voltage/current data are used as input during the initialization process to compute the pole node voltages, which are then followed to store the resistance data for later use. This process only occurs if there is no theft at start. Then, the simulated theft loads were connected to the various nodes of the network (consumer end, segment line, to identify and identify theft points, theft detection software was used in conjunction with customer service line and column nodes). Different possible sites for theft in the network were taken. The electric power distribution is similar for all three cases to determine the best results, in addition to determining the theft between loads according to the data available from the smart meter, in addition to the network data for the resulting voltage drop due to the technical losses of its conductors to be calculated and to determine the increase in the voltage difference as a result. Theft is to be adopted as data to determine the amount of non-technical losses due to theft and to choose the appropriate case to locate theft on the network. Therefore, these cases are studied in several exercises on the same network. Each effort team has its own accounts. To determine the location of the theft, and it differs when the loads change, it requires training the network for several expected values of the voltage drop to ensure the correct identification of the theft and more training on different values of the voltage drop resulting from technical losses and legal loads, the greater the accuracy of determining the location of the theft. Therefore, the third case (Feed-forward Neural Network) was trained on several different expected values of the voltage drop, which gave this case some possibilities for a more accurate determination, although it required adding more data by training the algorithm in an image wider, This is possible and easy for the electricity companies that have large numbers of cadres that have the ability to extensively train the algorithm within an acceptable time. Accordingly, we find that the third case (FFNN) was the best case in determining the values of non-technical losses and determining their location on the network with constant loads by up to 99.7%, and value less than with variable loads as shown in the table (8).

Table (9) shows the possibility of approximate detection of energy theft with the different changes in load values by the FFNN algorithm.

Real theft distance	Load 1	Load 2	Load 3	Theft distance
10 m away	100	400	200	11.9 m
	125	150	500	9.2 m
	150	200	200	9 m
20 m away	150	150	400	19 m
	100	300	400	19.9 m
	125	200	200	22 m
30 m away	100	400	200	33.9 m
	125	150	500	29.9 m
	150	150	200	36.5 m
40 m away	150	150	200	40 m
	100	300	400	36.5 m
	125	150	500	38.2 m
50 m away	100	200	500	44.7 m
	150	150	200	40 m
	125	150	500	36.7 m

The results are good for detecting thefts in the electric power distribution network, due to the change in the value of the load and its instability. One algorithm enables us to give these results with the quality of multiple values of the voltage drop. And when comparing the final results of the front-feed method used in this research with a research paper that follows the methods of mathematical equations in detecting theft Uvais, M. (2020) , as shown in Table (10), which shows the lowest error rate when using the front-feed method to detect theft with a limit of 0.02%.

Table (10) Comparison of the error rate of the front feed and a research paper based on equations.

Serial number	Real distance	Distance by equation In paper Uvais, M. (2020)		Distance by FFNN	
		value	Matching ratio	value	Matching ratio
1	0	0	0.00%	0	0.00%
2	10	9.52	4.80%	9.97	0.03%
3	20	18.87	5.65%	19.89	0.06%
4	30	28.21	5.97%	30	0.00%
Total Percentage Error			4.1%		0.02%

CHAPTER SIX

CONCLUSIONS AND REFERENCE

6.1 Conclusions

Many families indulge in various forms of electricity theft and illegal tampering with electricity metering devices that lead to problems and malfunctions in the power distribution system as well as loss of revenues for electricity sector companies. This work presents a method for obtaining a method for detecting theft in low-voltage power distribution networks, which includes analyzing the line parameters in order to discover the line voltage, loads, and technical losses, in order to later determine the non-technical losses and detect the locations of energy theft. The main server at the company’s headquarters, which processes the data sent by one of the communication systems, which represents the data of loads and landings at the destination in each distribution node linked to a smart power meter, in addition to the manufacturing network data for technical losses, the most important of which are copper wires associated with the load, as the data processor works on Similar parameters to typical and consumer loads. The network case study and physical structure simulation modeled for consumer loads and theft were also examined. To be able to determine the amount of illegal load and its location on the network. The study also used three methods to detect different cases of theft (equations, lm, and feed-forward). The detection scenario was in several points on the transmission line and between the loads and on the same legal load to be able to detect most of the theft and fraud methods on the energy meter when the loads are proven. The results of the three detection cases differed with the difference in error rates between acceptable, good, and excellent. The possibility of changing the values of the loads when conducting the detection, which is very difficult to change in the basic data. The detection algorithm and the feed-forward algorithm proved good detection rates in this matter, while the case of the equations and the case of the lm algorithm could not keep up with the change in loads to detect theft or fraud because the work questions of these algorithms depend on a fixed algorithm for one specific value of the drop in the natural voltage of the network, which depends on The basis is on the technical losses of the conductors and the load current, so at any change in the load current, we will have a new voltage drop that needs the algorithm to have new training for it, which means the availability of trained algorithms on all expected values of the voltage drop in the network and that the server chooses the appropriate algorithm For the value of the new drop resulting from the smart meter data and the measure of the technical losses of the network connectors and cannot be reduced to the values of all the drop in the expected voltage in the network in one algorithm in the two cases of equations and lm opposite the case of the front feed which showed a good ability to deal with the change in the values of the drop in voltage and the possibility of detecting theft With it in one algorithm, scalable and detectable, with more continuous training of expected data for network data and consumer loads.

6.2 Future work

The following recommendation can be used to develop the research reported in this study.

1- A new technique can be proposed to improve the efficiency of theft detection

With high accuracy and faster detection time

2- The feed-forward algorithm can be developed to detect theft in the distribution network to give better results with changing consumer loads

REFERENCE

Abdalzaher, M. S., Fouda, M. M., & Ibrahem, M. I. (2022). Data privacy preservation and security in smart metering systems. *Energies*, *15*(19), 7419.

Abdulkareem, A. (2016). Evaluation and mitigation of technical losses on power lines: a case study of nigeria 330-kv network. *Covenant University, Nigeria*.

Adeniran, A. (2018). Mitigating Electricity Theft in Nigeria. *Abuja: Centre for Public Policy Alternatives*.

Agüero, J. R. (2012, May). Improving the efficiency of power distribution systems through technical and non-technical losses reduction. In *PES T&D 2012* (pp. 1-8). IEEE.

Ali, S., Yongzhi, M., & Ali, W. (2023). Prevention and Detection of Electricity Theft of Distribution Network. *Sustainability*, *15*(6), 4868.

Angelos, E. W. S., Saavedra, O. R., Cortés, O. A. C., & De Souza, A. N. (2011). Detection and identification of abnormalities in customer consumptions in power distribution systems. *IEEE Transactions on Power Delivery*, *26*(4), 2436-2442.

Aniedu, A. N., Inyiama, H. C., Chukwuneke, C. I., & Asogwa, D. C. (2016). Smart Energy Meter for Load Control using Mobile Communication Technology. *Electroscope Journal*, *8*(8), 23-28.

Au, M. T., & Tan, C. H. (2013, June). Energy flow models for the estimation of technical losses in distribution network. In *IOP Conference Series: Earth and Environmental Science* (Vol. 16, No. 1, p. 012035). IOP Publishing.

Available online: https://www.energyforgrowth.org/memo/for-nigerians-without-affordable-electricity-job-creation-mustcome-first (accessed on 4 January 2022).

Biswas, P. P., Cai, H., Zhou, B., Chen, B., Mashima, D., & Zheng, V. W. (2019). Electricity theft pinpointing through correlation analysis of master and individual meter readings. *IEEE Transactions on Smart Grid*, *11*(4), 3031-3042.

Buzau, M. M., Tejedor-Aguilera, J., Cruz-Romero, P., & Gomez-Exposito, A. (2019). Hybrid deep neural networks for detection of non-technical losses in electricity smart meters. *IEEE Transactions on Power Systems*, *35*(2), 1254-1263.

Cao, M., Zou, J., Wei, L., Zhao, X., Zhang, L., & Li, P. (2021). Detection of Power Theft Behavior of Distribution Network Based on RBF Neural Network. *Journal of Yunnan University*, *49*(23), 178-186.

Carr, D., & Thomson, M. (2022). Non-Technical Electricity Losses. *Energies*, *15*(6), 2218.

Cespedes, R. G. (1990). New method for the analysis of distribution networks. *IEEE Transactions on Power Delivery*, *5*(1), 391-396.

Chandola, V., & Banerjee, A. V., K.(2009). Anomaly detection: A survey. *ACM Computing survey*, *41*.

Chen, H. C., & Chang, L. Y. (2012). Design and implementation of a ZigBee-based wireless automatic meter reading system. *Przegląd Elektrotechniczny (Electrical Review)*, *88*(1b), 64-68.

Díaz, S. (2021). Electric power losses in distribution networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(12), 581-591.

Díaz, S., Nuñez, J., Berdugo, K., & Gomez, K. (2020, June). Study of technologies implemented in the operation of SF6 switches. In *IOP Conference Series: Materials Science and Engineering* (Vol. 872, No. 1, p. 012041). IOP Publishing.

Dike, D. O., Obiora, U. A., Nwokorie, E. C., & Dike, B. C. (2015). Minimizing household electricity theft in Nigeria using GSM based prepaid meter. *American Journal of Engineering Research (AJER) e-ISSN*, *23200847*, 2320-0936.

Dike, D. O., Obiora, U. A., Nwokorie, E. C., & Dike, B. C. (2015). Minimizing household electricity theft in Nigeria using GSM based prepaid meter. *American Journal of Engineering Research (AJER) e-ISSN*, *23200847*, 2320-0936.

Egidio, L. N., Hansson, A., & Wahlberg, B. (2021, July). Learning the step-size policy for the limited-memory broyden-fletcher-goldfarb-shanno algorithm. In *2021 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE.

Fleming, S. J. A. (1914). *Magnets and Electric Currents..*. E. & FN Spon.

Ge, M., Syed, N. F., Fu, X., Baig, Z., & Robles-Kelly, A. (2021). Towards a deep learning-driven intrusion detection approach for Internet of Things. *Computer Networks*, *186*, 107784.

Henriques, H. O., Corrêa, R. L. S., Fortes, M. Z., Borba, B. S. M. C., & Ferreira, V. H. (2020). Monitoring technical losses to improve non-technical losses estimation and detection in LV distribution systems. *Measurement*, *161*, 107840.

Jadidbonab, M., Mohammadi-Ivatloo, B., Marzband, M., & Siano, P. (2020). Short-term self-scheduling of virtual energy hub plant within thermal energy market. *IEEE Transactions on industrial electronics*, *68*(4), 3124-3136.

Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., & Shen, X. (2014). Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, *19*(2), 105-120.

Jokar, P., Arianpoo, N., & Leung, V. C. (2015). Electricity theft detection in AMI using customers' consumption patterns. *IEEE Transactions on Smart Grid*, *7*(1), 216-226.

Júnior, L. A. P., Ramos, C. C. O., Rodrigues, D., Pereira, D. R., de Souza, A. N., da Costa, K. A. P., & Papa, J. P. (2016). Unsupervised non-technical losses identification through optimum-path forest. *Electric Power Systems Research*, *140*, 413-423.

Kahmann, M. The Triumph of Energy Measurement. *Metrology Throughout the Ages*, 3.

Kamatagi, A. P., Umadi, R. B., & Sujith, V. (2020, July). Development of energy meter monitoring system (EMMS) for data acquisition and tampering detection using IoT. In *2020 IEEE international conference on electronics, computing and communication technologies (CONECCT)* (pp. 1-6). IEEE.

Kannaiyan, M., & Raghuvaran, J. G. T. (2020). Prediction of specific wear rate for LM25/ZrO2 composites using Levenberg–Marquardt backpropagation algorithm. *Journal of Materials Research and Technology*, *9*(1), 530-538.

Khalel, S. I., Aziz, N. H., & Al-Flaiyeh, M. A. (2022). Smart grid application in the Iraqi power system: current and future challenges. *Bulletin of Electrical Engineering and Informatics*, *11*(6), 3042-3050.

Komolafe, O. M., & Udofia, K. M. (2020). A technique for electrical energy theft detection and location in low voltage power distribution systems. *Engineering and applied sciences*, *5*(2), 41-49.

Komolafe, O. M., & Udofia, K. M. (2020). Review of electrical energy losses in Nigeria. *Nigerian Journal of Technology*, *39*(1), 246-254.

Kotsampopoulos, P., Rigas, A., Kirchhof, J., Messinis, G., Dimeas, A., Hatziargyriou, N., ... & Andreadis, K. (2016). EMC issues in the interaction between smart meters and power-electronic interfaces. *IEEE Transactions on Power Delivery*, *32*(2), 822-831.

Liu, T. Y., Zhang, P., Wang, J., & Ling, Y. F. (2020). Compressive strength prediction of PVA fiber-reinforced cementitious composites containing nano-SiO2 using BP neural network. Materials, 13(3), 521.

LLC, N. (2017). Electricity Theft and Non-technical Losses Global Markets, Solutions, and Vendors.

McLaughlin, S., Holbert, B., Fawaz, A., Berthier, R., & Zonouz, S. (2013). A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE journal on selected areas in communications*, *31*(7), 1319-1330.

Messinis, G. M., & Hatziargyriou, N. D. (2018). Review of non-technical loss detection methods. *Electric Power Systems Research*, *158*, 250-266.

Nagi, J., Mohammad, A. M., Yap, K. S., Tiong, S. K., & Ahmed, S. K. (2008, December). Non-technical loss analysis for detection of electricity theft using support vector machines. In *2008 IEEE 2nd International Power and Energy Conference* (pp. 907-912). IEEE.

Nagi, J., Yap, K. S., Tiong, S. K., Ahmed, S. K., & Mohamad, M. (2009). Nontechnical loss detection for metered customers in power utility using support vector machines. *IEEE transactions on Power Delivery*, *25*(2), 1162-1171.

Nizar, A. H., Dong, Z. Y., & Wang, Y. (2008). Power utility nontechnical loss analysis with extreme learning machine method. *IEEE Transactions on Power Systems*, *23*(3), 946-955.

Nta, E., Udofia, K., & Okpura, N. (2022). Development of an Energy Theft Detection and location System for Low Voltage Power Distribution Networks. *Development*, *9*(4).

Ocampo-Vega, R., Sanchez-Ante, G., Falcón-Morales, L. E., & Sossa, H. (2013, November). Image processing for automatic reading of electro-mechanical utility meters. In *2013 12th Mexican International Conference on Artificial Intelligence* (pp. 164-170). IEEE.

Ramos, C. C., Papa, J. P., Souza, A. N., Chiachia, G., & Falcão, A. X. (2011, May). What is the importance of selecting features for non-technical losses identification?. In *2011 IEEE International Symposium of Circuits and Systems (ISCAS)* (pp. 1045-1048). Ieee.

Ramos, C. C., Souza, A. N., Chiachia, G., Falcão, A. X., & Papa, J. P. (2011). A novel algorithm for feature selection using harmony search and its application for non-technical losses detection. *Computers & Electrical Engineering*, *37*(6), 886-894.

Ren, Y., & Goldfarb, D. (2019). Efficient subsampled Gauss-Newton and natural gradient methods for training neural networks. *arXiv preprint arXiv:1906.02353*.

Rizk, Y., & Awad, M. (2019). On extreme learning machines in sequential and time series prediction: A non-iterative and approximate training algorithm for recurrent neural networks. *Neurocomputing*, *325*, 1-19.

Saad, M. A., Mustafa, S. T., Ali, M. H., Hashim, M. M., Ismail, M. B., & Ali, A. H. (2020). Spectrum sensing and energy detection in cognitive networks. *Indonesian Journal of Electrical Engineering and Computer Science*, *17*(1), 465-472.

Saboia, P., & Goldenstein, S. (2014). Assessing cross-cut shredded document assembly. In *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications: 19th Iberoamerican Congress, CIARP 2014, Puerto Vallarta, Mexico, November 2-5, 2014. Proceedings 19* (pp. 272-279). Springer International Publishing.

Sapna, S., Tamilarasi, A., & Kumar, M. P. (2012). Backpropagation learning algorithm based on Levenberg Marquardt Algorithm. *Comp Sci Inform Technol (CS and IT)*, *2*, 393-398.

Shaheen, B., & Németh, I. (2022). Machine learning approach for degradation path prediction using different models and architectures of artificial neural networks. *Periodica Polytechnica Mechanical Engineering*, *66*(3), 244-252.

Ullah, I., & Mahmoud, Q. H. (2022, January). An anomaly detection model for IoT networks based on flow and flag features using a feed-forward neural network. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 363-368). IEEE.

Uvais, M. (2020, February). Controller based power theft location detection system. In *2020 international conference on electrical and electronics engineering (ICE3)* (pp. 111-114). IEEE.

Wei, L., & Keogh, E. (2006, August). Semi-supervised time series classification. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 748-753).

WI, M. U. (2017). In Science and Engineerıng.

Xia, X., Xiao, Y., Liang, W., & Cui, J. (2022). Detection methods in smart meters for electricity thefts: A survey. *Proceedings of the IEEE, 110*(2), 273-319.