ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

AFRICAN RAILWAY CENTER OF EXCELLENCE

Artificial Neural Network Based Cryptography for Secure Operation of Ethio-Djibouti Railway using Wireless Sensor Networks

A Thesis in Electrical Engineering for Railway Systems

By TEMESGEN GETNET

September 2019

Addis Ababa

A Thesis

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science

The undersigned have examined the thesis entitled '**Wireless Sensor Networks for Secure Operation of Ethio-Djibouti Railway Line**' presented by **TEMESGEN GETNET**, a candidate for the degree of **Master of Science** and hereby certify that it is worthy of acceptance.

YALEMZEWD NEGASH (PhD)	_____	_____
Advisor	Signature	Date
	_____	_____
Internal Examiner	Signature	Date
	_____	_____
External Examiner	Signature	Date
_____	_____	_____
Chair person	Signature	Date

UNDERTAKING

I certify that research work titled "**Artificial Neural Network Based Cryptography for Secure Operation of Ethio-Djibouti Railway Using Wireless Sensor Networks**" is my own work. The work has not been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged / referred.

Signature of Student

Temesgen Getnet

Abstract

Railway transportation is a reasonable choice to transport an enormous volume of passengers and cargos. But guaranteeing the safety and reliability of transport is the main issue. In this research reliability and security issues will be discussed along with types of attacks and measures to be taken. Unreliable communication which is a result of unreliable transfer, conflicts and latency and unattended operation which is due to exposure to physical attacks, remote management and lack of central management point is used to describe reliability.

Secure operation is a combined effect of data confidentiality, data integrity, data freshness, availability, self-organization, time synchronization, secure localization and authentication. The attacks against this security metrics includes: Denial of service attacks, the Sybil attack, traffic analysis attack, node replication attacks, attacks against privacy (i.e. this includes monitor and eavesdropping, traffic analysis and camouflage) and physical attacks.

There are some efficient and effective measures that are discussed briefly such as: measures against DoS attacks, secure broadcasting and multicasting. Encryption using Artificial Neural Network is used to communicate the nodes in a secure and reliable manner. 6 hidden layers are used to update the weight functions. And it is simulated using MATLAB simulation Software.

Acknowledgments

Above all I would like to thank GOD for the success of this paper. Foremost, I acknowledge, with my sincere gratitude, my advisor Dr. Yalemzewd Negash for his continuous support, advice, inspiration, and foresight.

Besides my advisor, I would like to thank my wife and classmate Mrs. Edom Tsegaye for her immense knowledge, encouragements and insightful comments.

Table of Contents

List of Tables

List of Figures

List of Acronyms

ABS	Automatic Block Signaling
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ANN	Artificial Neural Network
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
ETCS	European Train Control System
ERA	European Railway Agency
ERC	Ethiopian Railway Corporation
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FA	Functional Addressing
GSA	Gravitational Search Algorithm
GSM	Global System for Mobile Communication
GSM-R	GSM-Railways
HLR	Home Location Register
HSPA	High Speed Packet Access
HSS	Home Subscriber Register
ICI	Inter-Carrier Interference
LDA	Location Dependent Addressing
LTE	Long Term Evolution
LTE-R	LTE-Railways
QoS	Quality of Service
WiMAX	Worldwide Interoperability for Microwave Access
WSN	Wireless Sensor Networks

CHAPTER 1 INTRODUCTION

1.1 Background of the Study

Railway system is one of the important transport facilities that is needed in the achievement of effective development and provides an efficient, cost-effective and environmental friendly transport system which can quickly haul large volumes of goods and passengers which are not easily convoyed through other motor vehicles for long distances. It is safe and cost effective relative to some other transportation systems. It is also one of the supporting mechanisms in eliminating poverty and initiating sustainable development.

Emerging need to carry bulk commodities in large quantities coal, iron, stone, cotton, food, and fuel for large cities. Building cost of canals and turnpikes monopoly charges by canal and road owners who do not operate Inefficiency of horse and cart/ cost of turnpike roads: Adam smith said the feed for one horse is enough to nourish 8 workers Corn Laws of 1815 do not allow import of corn high local cost. Long journey times when using canals and road transport increases interest on investment in machinery and raw materials. Perishable products and live stocks have to reach consumer as fast as possible. Loss of interest on funds invested in finished goods Pollution caused by large numbers of horses Poorer people have to travel to work and need cheap food, etc.

Addis Ababa-Djibouti route is the fundamental gate of our country; 75% of the total import and export goods are conveyed through this route. This route will also serves as passenger transportation. About 20,000,000 people lives across the path. It covers about 661.245km distance, and it comprises tunnels, bridges and level crossings [1].

Safe and reliable transportation system is crucial for economic, social and political development of a country. Since train is moving in a guided path and running through many interlocking and level crossings, it needs appropriate protection of collision and derailment hazards. Thereby we have to use latecomer's advantage of technology development without needing to start from the beginning i.e. we have to use the latest Wireless Sensor Networks technology in railway system. However, security is the

drawback of these technologies. This research tries to solve security problems of wireless sensor networks by using cryptography based on artificial neural network.

Work on artificial neural network has been motivated right from its inception by the recognition that the human brain computes in an entirely different way from the conventional digital computer. The brain is a highly complex, nonlinear and parallel information processing system. It has the capability to organize its structural constituents, known as neurons, so as to perform certain computations many times faster than the fastest digital computer in existence today. The interest to biological neural networks is motivated by the capability of the human brain to solve in a short time very different and complex problems, despite the "data" transmission velocity is very low (order of milliseconds). A neural network is a machine that is designed to model the way in which the brain performs a particular task. The network is implemented by using electronic components or is simulated in software on a digital computer. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for use [32]. In this research, application of artificial neural network with sequential machine method is used to perform encryption and decryption of messages transmitted between wireless sensor nodes. The output of the sequential machine depends on the state of the machine as well as the input given to the sequential machine. The state of the sequential machine is used as the key and then uses the data as an input to the sequential machine. The relationship between different output and states can be any random but unique sequence providing security to the encryption. As a sequential machine can be implemented by using a neural network, therefore a neural network can be used to encrypt data and another to decrypt data. In this case the starting state of the sequential machine can act as a key.

1.2 Statement of the Problem

Now a day wireless sensor networks become more advanced and simple but more effective technologies in the world so that the use of these technologies in a transportation system is a wise choice. Sensors became cheaper and cheaper ever since. The recent development in wireless technologies is the main factor to this contribution. Wireless Sensor networks can be used for implementation of signaling and

communication of railway system. Ethio Djibuti railway line uses GSM network for communication and signaling. It is prone to much amount of cost and the system is very complex for maintenance and some other issues hence using wireless sensor networks will solve such problems. But the big problem is the security and reliability issue raised on wireless sensor networks due to their vulnerability for different types of attacks.

Using cryptography at the time of data transmission is one of the measures to solve such problems of security and reliability. Even though there are some commonly known methods of cryptography like Elliptic Curve Cryptography, it is difficult to apply them in wireless sensor networks for their complexity and need for bulky size microprocessors. Hence, this research studies cryptography based on artificial neural network for secure operation of Ethio-Djibuti railway line.

1.3 Objective

1.3.1 General Objective

The main objective of this research is to introduce a secure and reliable operation system for the Ethio-Djibouti Railway Line using Wireless Sensor Networks.

1.3.2 Specific Objectives

- Conducting a survey on security and reliability of Railway systems
- Deep study of Wireless Sensor Networks and their operation
- Study and model Artificial Neural Network for encryption of messages to be sent and received
- Matlab Simulation of Encryption using Artificial Neural Network is done at the end.

1.4 Methods, Processes and Materials

1.4.1 General Procedure

The current state of the art in detecting immediate and long-term railway track problems involves both inspectors walking the track lines and train cars instrumented with accelerometers and ultrasonic sensors that are capable of detecting failures. Additionally,

a widespread practice of sensing rail continuity by using the tracks to complete simple circuits is in place.

In this research, a fundamentally different approach to improve the security and reliability practices in railway operations using wireless sensor network (WSN) is introduced. The primary technical and scientific objectives of the system introduced in this research are to generate innovative solutions for a number of the issues facing the railroad community through the development of a system based on WSN. The objectives from a railroad perspective include finding new approaches to reduce the occurrence rate of failures by prevention and improving the efficiency of railroad maintenance activities.

This research will insure a fail-safe and uninterrupted service while a problem occurred at some point in the system. It tastes the proposed method of cryptography using artificial neural network using MATLAB simulation software.

1.4.2 Processes and Materials

The current state of the art in signaling and communication are using track circuit and axle counters and GSM or LTE networks. This research studies a fundamentally different approach for signaling and communication in a railway system that is application of wireless sensor networks for communication and signaling.

In this research, it is tried to solve the security and reliability problems of wireless sensor networks using cryptographic methods by artificial neural networks. The primary goal of this research is to develop a secured and reliable means of communication for Ethio-Djibuti railway line.

This research will insure a fail-safe and uninterrupted service while a problem occurred at some point in the system. It tastes the proposed method of cryptography using artificial neural network using MATLAB simulation software.

1.4.3 Processes and Materials

WSN system provides:

- Fast and immediate data communication and no intervention of human operators manually;

- Increased use of data monitoring since there is no need of human operators at the field and easy way of data management due to central processing;
- Suitable for crosschecking of data since it is found from a number of sensors;
- Enable to use different analyzing algorisms centrally;
- Ability to store data as an information for further processing;
- Also allow data to compare with international standards so as to follow the conditions and status of different systems and machinery.

In general Wireless sensor networks are used to:

1. Reduce failure time;
2. Check safeness and working of machines and systems;
3. Eradicate system failure and save money;
4. Maintain process tolerances;
5. Inspect maintenance needs;
6. Request prevention maintenance before failures occur.

The data produced by sensors might be erroneous since sensors are sensitive to environmental conditions. So it must be managed carefully. A railway system is very complex in nature and it needs maximum safety and security. Therefore it is crucial to consider in the wellbeing of sensors in implementing wireless sensor networks for signalling and communication of railways. There has to be a method to prevent such extremely important sensors from internal and external attacks.

Ethio Djibuti line is a corridor with variety of topography and environmental conditions. Hence it must be bearded in mind while designing wireless sensor network system for this corridor.

The kind of sensors must be selected so as to increase the quality of data acquisition and the number of sensors must be reduce to decrease energy usage which in turn saves expenditure. Sensor nodes include sensors, power supply and micro controllers. The size of these sensor nodes must be as small as possible. So this needs a careful analysis and design of the system.

Hence, the study will incorporate the following major procedures in the proper order of precedence

I. Discusses the Use of WSN according to Security and reliability
II. Study key encryption technologies for the best result in fail-safe system
III. Examines future work in the area of secure and reliable railway operation.

1.5 Scope of the Study

The topic of Wireless Sensor Networks is vast and needs a thorough study and planning. However, considering the time limit, this research discusses and carefully models the cryptography based on artificial neural network for the secure operation of Ethio-Djibouti railway line. It only demonstrates the secured communication between two sensor nodes.

1.6 Review of Related Works

In [17] four main aspects of wireless sensor network security issues are studied: obstacles, requirements, attacks, and defenses. Within each of these divisions the authors sub divided the topics of routing, trust, denial of service, and so on. Aiming to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the relevant literature can be completed by the interested researcher. Authors deduct that as wireless sensor networks stay to grow and become more common, further outlooks of security will be essential of these wireless sensor network applications.

In particular, the addition of public key cryptography and the addition of public-key based key management described in [17] will likely make strong security a more realistic expectation in the future. It's also expected that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas. As the authors dictate, the increase demand of wireless sensor networks brought the increase demand of security solutions for the networks. As they might be interacted with sensitive data sources their security must be tightly protected.

As authors' conclusion, there is currently massive research potential in the field of wireless sensor network security. Thus, familiarity with the current research in this field will benefit researchers greatly. Bearing this in mind, they went through the key topics in

wireless sensor network security, and present the difficulties and the necessities in the sensor security, categorize many of the current attacks, and finally list their equivalent defensive actions.

In [19] a summary of the applications of WSNs and different attacks and their countermeasures are presented. Types of attacks on WSNs comprising wormhole attack, Sybil attack, selective forwarding, and impersonation attack are fleetingly discussed.

They defined that now a day, there has been a vertical development in research in the area of wireless sensor networks (WSNs). In WSNs, communication takes place with the assistance of spatially dispersed, autonomous sensor nodes equipped to sense specific information. WSN found in a number of government and civil applications in the world. For instance, they are used to detect enemy intrusion in the battle, patient treatment, fire extinguishing and so on. Sensor networks are becoming highly potential technology for the future in wireless communication development.

However, [19] indicate that challenges remained to be addressed in issues relating to coverage and deployment, scalability, quality-of-service, size, computational power, energy efficiency and security. [19] Presents an outline of the diverse uses of the wireless sensor networks and numerous security associated issues in WSNs.

The authors of [20] showed their worries about accidents happening in railway transportation systems. As their explanation, railway transportation is the means of lots of death and body injury for human beings. This has to get a solution in which case Wireless sensor networks get highly demanded to eradicate this problem. The can be used to detect abnormalities in railway tracks.

Based on their model, sensor nodes are furnished with sensors that can sense the vibration in the railway track due a coming train. The geographical positioning sensors are located on the trains. These sensors send the train’s geographic position. The total system must be immediate and real time. Optimization of the communication protocol and real time working network with minimum interval in multi-hop routing from the nodes to the train using a static base station is required, so that the decision making can be done and the decision is sent to the train without any delay.

As they state in their study, the railways have become a major means of transportation remaining to their capacity, speed, and reliability. Even a minor upgrading in performance of railways has substantial economic paybacks to rail industry. Thus, an appropriate maintenance approach is essential to manage optimization of checkup frequency and/or advance in ability and competence. Calamities happening due to track flouting have been a big delinquent for railways for life security and timely management of facilities. This rupture needs to be recognized in real time before a train actually comes close to the cracked track and get exposed to an accident. In this research, diverse kinds of rail faults checkup and maintenance methods are designated and a basic procedure is readdressed that makes use of wireless acoustic sensors for sensing cracks and fractures in the railway tracks.

1.7 Thesis Outline

This thesis is organized in six chapters.

Chapter 1: includes introduction which provides clear information about the background of the thesis work, problem statement, objective, methods, processes and materials, review of related works.

Chapter 2: is about the Ethio Djibuti Railway route: the topography, the station distribution, the current GSM-R architecture, and the GSM-R network requirements.

Chapter 3: is about the overview of WSNs, the introduction about WSNs, application of WSNs and operations of WSNs, the security and reliability concerns in WSNs

Chapter 4: is about attacks in WSNs: that includes DoS attacks, the Sybil Attack, traffic analysis attack, node replication attacks, attacks against privacy, and physical attack

Chapter 5: is about measures against the attacks that have been previously stated.

Chapter 6: is about MATLAB simulation results, recommendation and conclusion. Here, the work is concluded based on the result obtained. Further recommendation for the Development of new model or improvement of the result in this thesis is suggested.

CHAPTER 2 ETHIO-DJIBOUTI ROUTE

Figure 2-1: Ethio-Djibouti Railway line overview [21]

Ethio-Djibouti railway line is found in the mount areas between the central highlands of Ethiopia and Djibouti plateau. The line is an electrified railway intended for transportation of both passengers and freights. The design speed for passenger trains equals or is less than 120km/h and that of freight trains equals or is less than 80km/h. The section from Sebeta (Addis)-Adama is double track railway, and the section from Adama - Nagad is single track railway. Ethiopia sets up a railway company in Addis Ababa (Labu) to manage the operation of Sebeta-Dewele (included) section and coordination with Djibouti railway. The line includes cities starting westward from Sebeta at southwest of Addis Ababa, and runs eastward through Labu, Indode, Gelan, Dukem, Bishoftu, Mojo, Adama, Welenchiti, Metehara, Awash, Asebot, Mieso, Mulu, Afdem, Bike, Bota, Dire Dawa to Dewele, reaches Djibouti, then passes Guelile and Holhol, and finally ends at Nagad. The total length is 743.245km. Djibouti sets up a railway company to manage the operation of Dewele (excluded) - Nagad section and railway inside the port area [1].

2.1 Topography of the Route

2.1.1 Sebeta-Mieso Section

The area includes the geographical platform common in Ethiopia. It consists of hills, mountains and plateaus. It also comprises a river in flowing in the area. The elevation of road surface is about 850-2300m, the relative elevation difference is scores of meters, and the traffic condition is relatively poor. Because of continuing scouring and damaging of seasonal flood, the surface-incised dry gullies can be seen, which has a width of 2-5m, depth of 3-12m and length of hundreds kilometers. Both sides of the channel wall are almost vertical sidewalls and the bottom of the trench is largely sandy soil [1].

2.1.2 Mieso-Dewele Section

This section of the line fit in to the Ethiopian plateau platform and shallow hill landform. Part of the zone has Low Mountain and river valley landform, the ground is wide and the geographical relief is not good, the slope of road surface is about 700-1200m, and the relative elevation difference is scores of meters. The climate is hot and the surface tropical plant is scarce with coverage of approximately 10% to 30%. There is dry riverbed. Bulk Gobi phenomenon can be seen with few roads and poor traffic conditions.

2.2 Overview of Station Distribution

The whole Ethio Djibuti railway line is 743.245kms long. The section from Sebetta - Adama (included) is double track railway, with a length of 113.836km, 7 stations, and an average distance between two stations 16.26km. The section from Adama (excluded) - Mieso (included) is single track railway, with a length of 213.418km, 12 stations, and an average distance between two stations 17.78km. The section from Mieso (excluded) ~ Dewele (included) is single track railway, with a length of 334.014km, 21 stations, and an average distance between two stations 15.91km. The section from Dewele (included)- Nagad (included) in single track railway, with a length of 81.977km, 5 stations, and an average distance between two stations 16.4km [1].

In the study of ERC Lebu station is taken as the center station for Addis Ababa city to satisfy the needs of passengers in the city as the initial station for passenger trains. It is

far from the center of the city to make it free from traffic density. Indode station is taken as the center station for freight transport. It is used for demarshaling service.

The stations Sebeta, Labu, Bishoftu, Mojo, Adama, Awash, Mieso, Dire Dawa, Dewele, Alisabieh, Holhol, and Nagad have a passenger transport service. The other stations can choose to start freight transportation as appropriate based on the increase of transportation demand.

In the first stage the stations which will start freight service are Feto, Metehara, Awash, Sirba Kunkur, and Bike. The other five stations can start the service based on the demand to the service.

Terms/Stages	Sections	Pairs of trains (Train/Day)				Required passing capacity
		Passenger Trains	Freight Trains	Pick up and Drop Trains	Sub Total	
Initial Stage	Sebeta-Adama	5	5	1	11	17
	Adama-Awash	2	5	1	8	11
	Awash-Dire Dawa	2	5	1	8	11
	Dire Dawa-Nagad	1	5	1	7	10
Short Term Stage	Sebeta-Adama	6	7	1	14	21
	Adama-Awash	2	8	1	11	15
	Awash-Dire Dawa	2	9	1	12	16
	Dire Dawa-Nagad	1	9	1	11	15
Long Term Stage	Sebeta-Adama	10	16	1	27	38
	Adama-Awash	3	17	1	21	27
	Awash-Dire Dawa	3	19	1	23	30
	Dire Dawa-Nagad	2	19	1	22	28
Total		39	124	12	175	239

Table 2-1: Total train traffic of the line [1]

There are about 60 trains among which 38 are used as freight trains and 2 are pick up trains whereas the remaining 20 trains are for passenger transport.

Ethiopian railway corporation (ERC) made the management and operation center for passenger and freight transport at the Lebu station depot.

The whole number of personnel hired for the whole section of the line is found in the table below. Some variation may take place due to some other duties stated in the table.

Department	Quantity
Company Management Staff	76
Rolling stock depot in Addis Ababa (Lebu)	54
Personnel of all stations in total	403
Dispatching center staff (Lebu)	63
Total	536

Table 2-2: Total personnel of the whole line [1]

2.3 Current GSM-R Architecture of Addis Ababa- Djibouti Line

2.3.1 GSM-R Introduction

The GSM-R network architecture is shown below. Its blocks and components are described briefly.

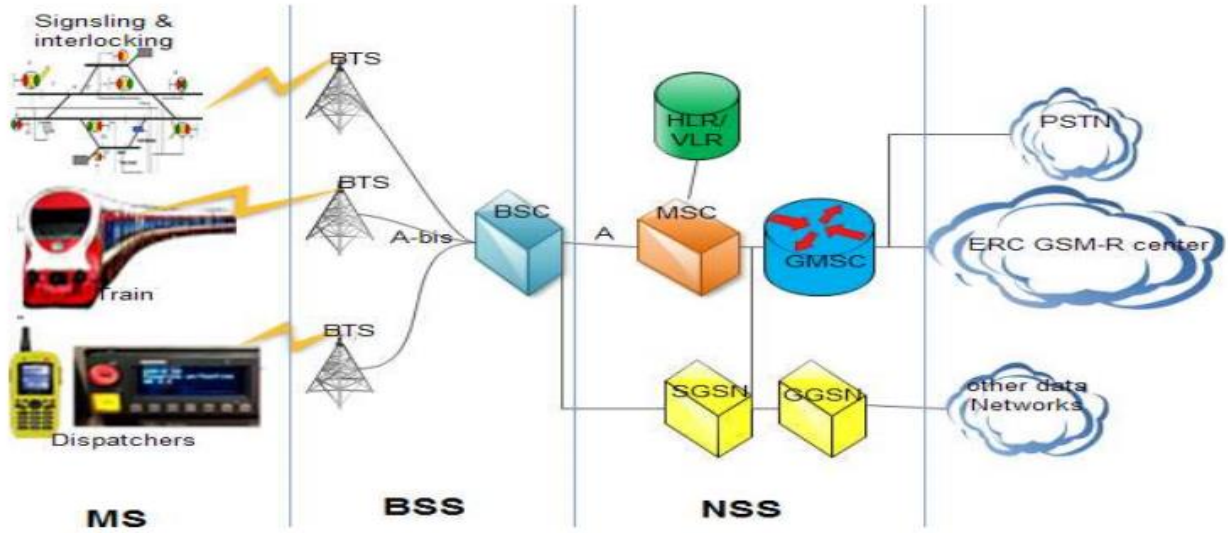

Figure 2-2: End to end GSM-R Radio Network [5]

GSM-R network is derived from GSM (2G) network and it is a special application for railways. The network is followed a path of the railway line. It is built on the proven GSM standard. This means all sorts of existing hardware can be easily modified by vendors and manufactures in order to work on GSM-R platform [5]. GSM-R is a widely used method of communication for railways. It is used as a means of communication between the train, the driver and control center. It can help to identify the position of the train the speed of the train and the signaling system. It can support voice and data communication. It is advantageous in saving the cost of maintenance for cables and other connectors in that of wired communication.

GSM-R network is applicable for a speed up to 500Km/hr. Above this due to Doppler effect it cannot be used. GSM-R helps in carrying signaling information for the driver and control center with other methods of automatic train controlling systems. GSM-R is also helpful for communication between drivers, shunting men, dispatchers and station control personnel. Moreover, it enables fast communication in case of emergency relative to cable networks. It eliminates the problem of stealing network equipment like cables, it also evades infrastructure for radio patching covering disruptions in cable. Although GSM-R is emerged from GSM communication it has also other features of communication unique to itself such as broadcasting call and group call, location-based

connections, and call pre-emption in case of an emergency which are vital for railway environment. This will enhance activities such as cargo tracking, video surveillance in trains and at stations. So the following parameters should be taken into consideration in GSM-R design [5]:

- Fast fading of signals caused by fast-moving trains
- Frequency shift
- Coverage in tunnel and valleys
- Handover times

End to End communication of GSM-R system is shown in the above figure and the briefs of each subsystem are explained below.

The section in which CAB radio signaling, dispatcher portable mobiles and other signaling & interlocking systems are included is called Mobile Station. The mode of communication between all systems and base transceiver station is wireless network. BSS includes Base transceiver station (BTS) and base station controller (BSC) subsystems. BTS is a system of equipment that is used for wireless communication between user equipment (UE) and the network. The tasks to be performed by BTS include Radio interface control, diversity control, channel encryption and media access control. BSC is the main component of GSM network and it controls the all the BTSs. Radio Network management, BTS handover and call set ups are the main tasks which are controlled by BSC [6, 1]. Network switching system (NSS) includes many subsystems. Calls between base station subsystem and other networks like PSTN are controlled by Mobile switching center (MSC). MSC is enabled by Gateway MSC (GMSC) to interrogate an HLR to route a mobile terminating call. It performs gateway functionalities for MSC. Home location register (HLR) is a database that contains the permanent address and information of subscribers. Visitor Location Register (VLR) is a database which consists of the temporary address of a subscriber based on the current BTS location where the subscriber is found on. There is always one VLR per MSC. All packet switched data within the network is handled by Serving GPRS Support Node (SGSN) which is the main component of GPRS. Gateway GPRS Support Node (GGSN)

is responsible for internetworking GSM-R based ATP design for Addis Ababa-Djibouti route. The interface between user equipment and BTS is Um interface with TDMA media access control and the interface between BTS and the BSC is A-bis, which can channeled by DS-1, E1 or T1 data network carriers. A-interface is used to carry signal and traffic data between BSC and MSC subsystems. To determine the number of BTS we need to know the cell radius and the coverage area of a single base station. This scheme enables us to determine the number of BTS required for the given area. The coverage area of a base station is determined based on the number of sectors in the base station. Tri-sector, bi-sector and Omni-directional sectors are the three types of sectoring in cellular networks. Frequency reuse schemes help to reduce inter cell interference.

2.4 GSM-R Network parameters

Technical specifications of GSM-R network system include the bandwidth includes 4 different operation frequencies which are 850 MHz, 900 MHz, 1800 MHz and 1900 MHz. 124 carrier frequency channels each with a space of 200 KHz apart are included in a 25 MHz bandwidth. It needs a transmission power of 2W in 850/900 and 1W in 1800/1900 MHz operating frequencies. The modulation scheme is a Gaussian Minimum Shift Keying (GMSK) which helps to reduce cross channel interference. It offers 8 full rate or 16 half rate speech channels per radio by applying a time division multiplexing technique. Among the drawbacks, digital signals can bring dropouts rather than static noises. The others include loss of tones in voice and limited amount of data in control channel. One of the challenges is that it needs frequency planning to expand the network. GSM-R is a network depending on the 2^{nd} Generation network system and its operating frequency band is the same range defined for GSM network. GSM-R is a very robust standard since it is defined for very high blocking performance, and wide dynamic range. Such qualities are the key to deliver a reliable communication, especially in terms of resistance to blocking interference, or in terms of required carrier over interference ratio which is very low and thus profitable for frequency reuse pattern.

Finally GMSK modulation defined for GSM/GSM-R is very robust to system linearity and this allows wide receiver dynamic range. GSM-R networks have to fulfill tight availability and performance requirements of the railway radio services. The special conditions and requirements of a railway communication system such as linear train

movement along the tracks are laid down in EIRENE SRS V15 specification. Both line oriented GSM-R network and ERTMS requires a very high quality of service [8, 1].

Especially ETCS application needs a permanent connection with a traffic load of 1 ERLANG per rain and a permanent radio link availability of 100% in a time. These requirements of GSM-R and ETCS for continuous radio link availability are in accordance with the UIC/EC/EIRENE definitions [8, 1]. There are many factors limiting the power signal path loss in GSM-R radio networking. These factors are described in the following paragraphs.

Shortcomings of GSM-R

- GSM-R system uses circuit switched data transmission technique. This in turn has an effect of constant bandwidth but data transmission is variable in nature. So it ends up with underutilization of channel resource.
- GSM-R network capacity is insufficient; a typical cell can provide a total of 23 traffic channels [1]. ETCS connection provides all the trains to have a dedicated channel for a CSD call established. Based on this principle a cell can provide a channel for up to 23 trains only. But in reality since some channels must be allocated for voice communication and handover process the cell can only support for 20 trains only.
- In some places where the train density is relatively high like depots, shunting yards and the like, there is a shortage of free channels to be allocated for every train which is also the shortcoming of GSM-R system. There are three sources of this problem: an inflexible radio interface, circuit-switched based transmission and limited frequency spectrum assigned to railways [12].
- GSM-R is an obsolete technology that is no longer able to meet the communication need of the future railways since railway communication demand (especially data transmission capacity) is expected to increase. The evolution of the commercial mobile network, undertaken by the telecommunication industry in order to address the shortcomings of the GSM technology, shows how outdated the GSM-R technology is [12].

In general, we can conclude that GSM-R communication system is taken as old technology and the currently many companies are shifting towards the LTE. GSM-R,

as mentioned above, operates in a dedicated frequency band, which is prone to an interference issues caused by nearby frequency bands. Due to all the shortcomings stated above in addition to the smaller capacity of the GSM-R technology, we need a new railway communication system. Here comes the necessity of latest technologies like wireless sensor networks. In the consecutive chapters wireless sensor networks are explored to some extent.

CHAPTER 3 OVERVIEW OF WIRELESS SENSOR NETWORKS

3.1 Introduction

A wireless sensor network (WSN) is among the communication technology which comprises of spatially distributed devices which can sense and measure some parameters of environmental processes. A given WSN system includes the sensor nodes containing a sensor, a power unit, and microcontroller which are combined with routers and gateway. In case of railway systems these nodes communicate with each other wirelessly and transmit their messages to the train and control center. The control centers collecting the data from wireless sensors will analyze and pass control information for train protection.

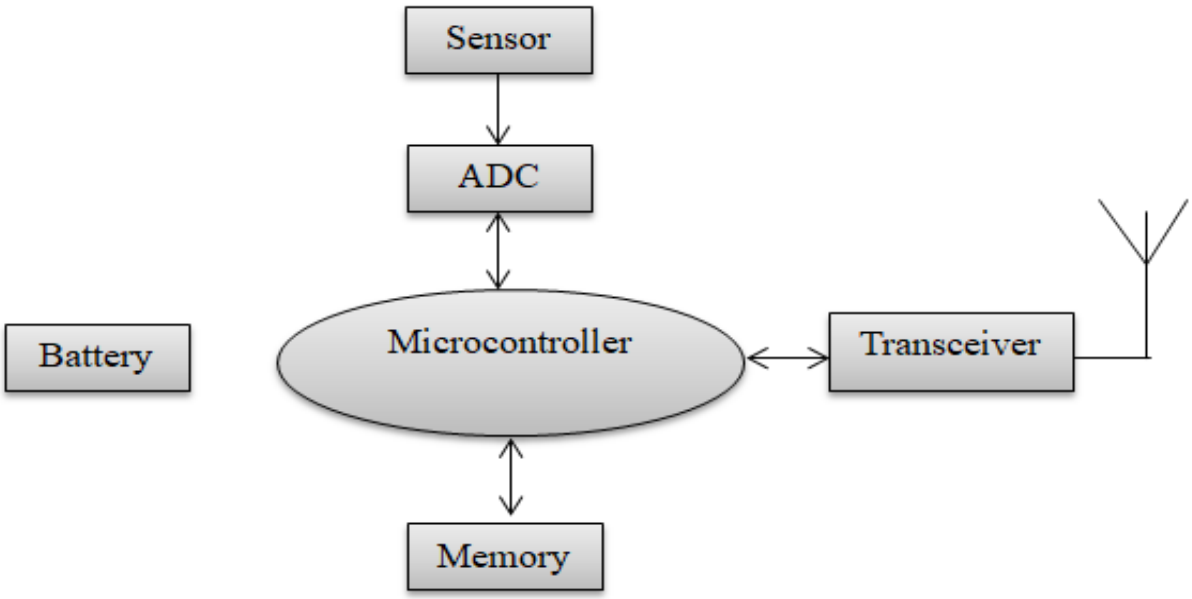

Figure 3-1: Representation of a Sensor Node

Routers might be interfaces between end nodes and control centers. The train can in some conditions get direct information from track side sensor nodes wirelessly through onboard sensor nodes communicating through wireless scheme. In general, looking the accelerated rate of deployment of wireless sensor networks for variety of applications one can deduce that after 3 decades the world will become under the colony of wireless sensor networks. It is clear that the importance of these sensor networks is extended to a

number of fields like health surveillance, battle field surveillance, environmental monitoring, coverage, routing, location service, target tracking, education, agriculture, transportation, large scale industries, telecommunication, and so on. As these systems have numerous prone they also do have their own drawbacks among which the reliability and security issues are at the front because of wireless networks are vulnerable to external attacks. The other challenges included in WSNs coverage and deployment, scalability, quality- of- service, size, computational power, and energy efficiency. In designing WSNs, one of the main issues is limited energy source for each sensor node. Hence, offering ways to optimize energy consumption in WSNs which eventually increases the network lifetime is strongly felt [3].

The lack of security monitoring system related to the railway track introduces high vulnerability to possible terrorist threats. Conventional wired sensor networks could possibly be used but the large length of existing track in the U.S. will introduce implementation problems. On the contrary the use of wireless sensor networks presents a very attractive and feasible alternative [2].

3.2 Applications of Wireless Sensor Networks

WSNs are implemented for different areas in which some are stated below.

Military Surveillance Applications:

WSN are used in military battles of field for the purpose of communication and surveillance of vehicles of enemy and soldiers. Most of the time, they are used to enhance the safe keeping of borders from intrusion of enemy or illegal migrants by sending a message for guards and keepers.

Environmental Applications:

Environmental applications include detecting earthquake, land slide, volcano and other changes and also the level of lakes and rivers weather and so on. They can be also applied to track the movements of insects, birds, animals or any other in their region of operation. WSNs can be the part of solutions by communicating with the controlling mechanisms to overcome environmental problems happened in relation to the above conditions.

Health Care Applications:

Now a day, diseases like diabetes and stroke are among the killers of human beings. Patients may repeatedly fall due to such type of diseases. If they do not get immediate support and travel to health centers they might passed away. For such reasons it is a good trend to have a monitoring mechanism for such type of patients to save their lives. In this case wireless sensor network fits in well into this application.

Home Automation

Wireless sensor networks can be used in home applications to control electrical and electronic devices and to exchange status information between the devices and further to the resident. For instance, the air conditioning process can be controlled automatically through monitoring of wireless sensor networks.

Industrial Control:

In industry, wireless sensor networks can be applied to monitor and process controls. In this manner they are used to reduce the need of man power. For instance, in a bottling company they might be implemented to sense the bottle with a defect so that it will be removed and reused after modification.

3.3 Application of Wireless Sensor Networks in the Railway Industry

Wireless sensor networks can be applied in railway systems for signaling and communication purposes and also they can be served to monitor the conditions of rail tracks and tunnels and used to control security in stations and overall infrastructure through video surveillance. These applications are briefly described as follows:

WSN for Railway Security Enhancement On-line surveillance is one of the most important applications of WSN. The surveillance can be taken into effect in different areas of a railway system. In stations and depots there has to be a video surveillance mechanism to ensure security, for instance, by using Closed Circuit Television (CCTV) system. In addition to this system spatial distribution of sensor nodes in this area enhances the controlling of security. In this way, before security problem has occurred, these systems help the operator to detect and take the measures by himself or inform the

right authority to take an action. Besides stations WSNs might be used to detect the entrance of animals, cars or any other objects into the level crossings and send information to control center and the train in that area so that the operators can take actions to reduce accidents.

The other application of WSNs in railway systems is in the form of smart metering. One of the keys of innovation for the future of the railway is the enhancement of the energy efficiency. This objective can be reached by using methods of smart metering. Smart metering relies on a distributed energy resource management system, which aims to manage the different energy flows of the entire railway system [3].

WSNs are used for safe and secure railway operations by monitoring infrastructures and detecting obstacles. Failures in infrastructure or intrusion of obstacle into the track may bring derailment, train collision or any other accidents. And such types of train accidents are means of potential loss of human lives and wealth. So, if we incorporate WSNs in such areas we can save lives and loss of wealth from such accidents. In [3] a WSN is deployed along the track side and they transmit data to the control center or sink node. Sink nodes are connected through wire lined connection and sensor nodes scattered across railway tracks. Each of these sensor nodes is capable of collecting necessary data and forwarding the data to the sink node. Then the data is forwarded to the monitoring system through network connections between the different sink nodes.

3.4 Reliability and Security

A wireless sensor network is a special network which has many constraint compared to a traditional computer network. The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes [28]. Wireless sensor networks are getting a potentially higher demand due to their low cost expenditure during installation and time of operation. This enables them to be installed in a wide area as a collection of sensor arrays.

In the case of wireless sensor networks, we might assume that all of the sensors are working securely and reliably but in real case it might not be as the assumption; there must be a mechanism to check the security of each sensor nodes frequently. Because

there are a number of risks which a node may be suffer in. Traditional and professional attacks are among these dangerous attacks.

Similarly because of wireless nature, sensor nodes are more vulnerable to attacks. The typical attacks in WSNs include replay attack, data forwarding attack, and sinkhole attacks. Unfortunately, the current complex security algorithms are inadmissible for WSN in view of the limited capacities of minimal power of node. Trust administration is central to recognize danger, selfish, and unauthorized nodes. Trust in MWSN is the level of a conviction about the behavior of different nodes [27].

The security issue in WSN system for railway industries must be considered at the early time of design of the system since a railway needs a high level of safety. Almost all of the systems in railway environment are considered to be fail-safe. The wireless sensor networks need a more special attention due to their involvement to a much sensitive data and they are implemented in a challenging environment which is not suitable to test and observe simply. However, still having given the special attention starting from the time of design we might face our sensor network security being failed because of different attacks.

But we also have some remedies stated as the following for attacks on WSNs [19]:

- Powerful cryptography can be applied to eradicate data reply attacks, data modification and eavesdropping.
- Pushback, complex authentication, and network identification are among the methods to defend denial of service attacks.
- A correct Authentication is a good solution to withstand a Sybil attack. Nodes are authenticated to trust each other while transmitting data from one to the other by a trusted server or a base station. That means every node is given a secret word or text that is used by the central station or a server. If a single network key is used, compromise of any node in the WSN would defeat all authentications [29].

3.4.1 Reliability

A railway system is always evaluated in terms of RAMS(S) or reliability, accessibility, maintainability, safety and security. Among these, reliability and security of wireless sensor networks are concerns of this research. Most of the time there are standards

defining these parameters for international companies and suppliers working on railway industries. Due to these standards inter-operability can be performed within two different railway lines. The important function of railway systems is the safest transportation of passengers and freights. For this to be true reliability of equipment and operational staff is required. Equipment includes switches, interlocking machines, signaling systems and so on. Staff includes drivers, shunting men, controllers and security officials. Reliability can be defined as the probability of that system can do a given job under some constraints within the given amount of time. Reliability of a given system can be measured by failure rate. The reliability of communication and signalling systems decides the speed and safeness of transportation of goods and passengers. The failure of these systems can lead to train collision, derailment or delay. So it is an essential task to study the security and reliability of wireless sensor networks. To design and decide the feasibility of a given wireless network system there need to be the knowledge of the reliability of a system [19].

For wireless sensor networks unreliable communication is the big challenge. For the whole network to be considered as a reliable system the communication between each node and that of the control center must be reliable. This should have a mechanism to assure the reliability of these communications. Unreliable communication can be viewed in different manners such as [19]:

- The first case is due to the wireless nature of sensor networks there might be packets damaged or lost over the channel. This can be arising due to the lack of error handling mechanism of the channel and the congestion of data at sensor nodes. In this case the communication channel or the sensor network system cannot be described as reliable.
- The second case is while the communication channel is reliable but when there is a collision between packets at the channel. That means the wireless sensor nodes may transfer data at the same instant. In that case, packets may get collide in halfway the channel. This will result in damage or failure of data transmission. So, in this case also the network cannot be taken as a reliable system.
- The other issue is that unless properly managed synchronization problem inhibits the safeness of the sensor networks. That means the network due to congestion and other problems packets may have delays while they reach the required

destination. Hence, they need time synchronizing techniques to understand each other properly. Otherwise, those networks can be taken as unreliable systems.

3.4.2 Security

Sometimes we observe that some people used the terms safety and security interchangeably. But, the two terms have a considerable difference with each other. Safety can be defined as the functional wellness of a system against dangerous moments due to un-anonymous errors and technical failures, whereas, security is the prevention of loss from dangerous moments caused by illegal actions.

A wireless sensor network, to be considered as a secured network, needs different requirements to be effective regarding to its nature. Some of the important aspects are discussed below.

Information Privacy

In a wireless sensor network information privacy is a parameter which needs a primary attention. When we say information privacy it involves keeping the secret data to one's self only. There must not be information leaking to another sensor node which do not deserve to read the message [18].

In railway transport system sensors are involved in very crucial information. If this information is not kept confidential there will be high probability to be attacked by hijackers. Therefore, the data must be encrypted as well as send only to the targeted sensor or system.

Information Reliability

Information privacy is a good parameter to be considered for sensor networks but it is not enough condition for a sensor network to be taken as secured [19]. The information must also be reliable; that means, it should be delivered to the required place. Due to channel error, congestion and other factors the data might be damaged or dropped at the journey which will result in information loss. This information may include a secret key for encryption which will affect the security highly.

Information Newness

In addition to information privacy and reliability its newness is an important factor for security [17]. Otherwise, it might be vulnerable for message replay attacks. For example,

if we consider a public key cryptography where the keys are changed frequently and broadcasted accordingly, there must be a mechanism for the nodes to know the new keys at the same instant. But, if there is a delay of the new key, the node may consider the previous key as the new one. Hence the attackers may use this weakness as an opportunity.

Accessibility

Using some method of cryptography may strengthen the security of a network system. But, the cryptography needs a dedicated channel or the same channel of communication but, still, with additional computational complexity [5]. This complexity will need more energy which may cause the sensor node to run out of its energy and cease its functionality. This will lead into the problem of accessibility and end up with security problem for the whole network.

Synchronization

Sensor nodes need some form of synchronization to understand the chronology of a message. It is difficult to read the information in their order of release since they might lose their order of release due to the congestion problem [28]. For this reason, we need to have some mechanism to handle this problem. Time synchronization is also used to properly apply key updating principle. That means, when we use public key cryptography the secrete keys might be broadcasted at the same time and updated simultaneously. But, if congestion occurs somewhere, the updated key may not reach the sensor node at the required time. But, if there is a time synchronization mechanism the sensor node will understand that the correct secrete key is yet to come and wait for it until it reaches which will help it to understand the information incorrectly.

Proper Placement

A proper placement of sensor nodes is necessary for wireless sensor network which helps to get complete information about the overall system [2]. Since sensors are cheaper devices it is not hard to deploy as much number of sensors in a dense manner. But, energy and controlling factors will not allow implementing this idea. Therefore, it needs optimization of these parameters which makes it a hot area of research currently.

CHAPTER 4 ATTACKS AND MEASURES IN WIRELESS SENSOR NETWORKS

4.1 Attacks

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Denial of service attacks on wireless sensor networks can range from simply jamming the sensor's communication channel to more sophisticated attacks designed to violate the 802.11 MAC protocol or any other layer of the wireless sensor network.

Due to the potential asymmetry in power and computational constraints, guarding against a well-orchestrated denial of service attack on a wireless sensor network can be nearly impossible. A more powerful node can easily jam a sensor node and effectively prevent the sensor network from performing its intended duty. We note that attacks on wireless sensor networks are not limited to simply denial of service attacks, but rather encompass a variety of techniques including node takeovers, attacks on the routing protocols, and attacks on a node's physical security. First some common denial of service attacks and then additional attacking will be addressed, including those on the routing protocols as well as an identity based attack known as the Sybil attack.

Certainly, denial of service attacks is not a new phenomenon. In fact, there are several standard techniques used in traditional computing to cope with some of the more common denial of service techniques, although this is still an open problem to the network security community. Unfortunately, wireless sensor networks cannot afford the computational overhead necessary in implementing many of the typical defensive strategies. What makes the prospect of denial of service attacks even more alarming is the projected use of sensor networks in highly critical and sensitive applications. For example, a sensor network designed to alert building occupants in the event of a fire could be highly susceptible to a denial of service attack. Even worse, such an attack could result in the deaths of building occupants due to the non-operational fire detection network.

Other possible uses for wireless sensors include the monitoring of traffic flows which may include the control of traffic lights, and so forth. A denial of service attack on such a sensor network could prove very costly, especially on major roads. For this reason, researchers have spent a great deal of time both identifying the various types of denial of service attacks and devising strategies to subvert such attacks. Some of the major types of denial of service attacks are described below [28].

4.1.1 Denial of Service Attack

A standard attack on wireless sensor networks is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received.

If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently. This too can have a detrimental impact on the sensor network as the messages being exchanged between nodes may be time sensitive. Attacks can also be made on the link layer itself. One possibility is that an attacker may simply intentionally violate the communication protocol e.g., ZigBee or IEEE 801.11b (Wi-Fi) protocol, and continually transmit messages in an attempt to generate collisions. Such collisions would require the retransmission of any packet affected by the collision. Using this technique it would be possible for an attacker to simply deplete a sensor node's power supply by forcing too many retransmissions.

At the routing layer, a node may take advantage of a multi-hop network by simply refusing to route messages. This could be done intermittently or constantly with the net result being that any neighbor who routes through the malicious node will be unable to exchange messages with, at least, part of the network. Extensions to this technique include intentionally routing messages to incorrect nodes (misdirection). The transport layer is also susceptible to attack, as in the case of flooding. Flooding can be as simple as sending many connection requests to a susceptible node. In this case, resources must be allocated to handle the connection request. Eventually a node's resources will be exhausted, thus rendering the node useless [28].

4.1.2 The Sybil attack

Sybil attack is simply defined as “malicious device illegitimately taking on multiple identities”. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection.

Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional “votes.” Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node [28].

4.1.3 Traffic Analysis Attacks

Wireless sensor networks are typically composed of many low-power sensors communicating with a few relatively robust and powerful base stations. It is not unusual, therefore, for data to be gathered by the individual nodes where it is ultimately routed to the base station. Often, for an adversary to effectively render the network useless, the attacker can simply disable the base station. To make matters worse, demonstrate two attacks that can identify the base station in a network (with high probability) without even understanding the contents of the packets (if the packets are themselves encrypted).

A rate monitoring attack simply makes use of the idea that nodes closest to the base station tend to forward more packets than those farther away from the base station. An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets. In a time correlation attack, an adversary simply generates events and monitors to whom a node sends its packets. To generate an event, the adversary could simply generate a physical event that would be monitored by the sensor(s) in the area (turning on a light, for instance) [28].

4.1.4 Node Replication Attacks

Conceptually, a node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor

node. A node replicated in this fashion can severely disrupt a sensor network's performance: packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc.

If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor and can also insert the replicated node into strategic points in the network. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether [28].

4.1.5 Physical Attacks

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions.

Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker. Recent work has shown that standard sensor nodes, such as the MICA2 motes, can be compromised in less than one minute. While these results are not surprising given that the MICA2 lacks tamper resistant hardware protection, they provide a cautionary note about the speed of a well-trained attacker. If an adversary compromises a sensor node, then the code inside the physical node may be modified [28].

4.2 Measures

Now it is a position to describe the measures for satisfying security requirements, and protecting the sensor network from attacks. We start with key establishment in wireless sensor networks, which lays the foundation for the security in a wireless sensor network, followed by defending against DoS attacks, secure broadcasting and multicasting, defending against attacks on routing protocols, combating traffic analysis attacks,

defending against attacks on sensor privacy, intrusion detection, secure data aggregation, defending against physical attacks, and trust management [30].

4.2.1 Measures against DoS Attacks

Since denials of service attacks are so common, effective defenses must be available to combat them. One strategy in defending against the classic jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion.

In this case, a sending node can send the message along multiple paths in an effort to increase the likelihood that the message will ultimately arrive at its destination. This has the advantage of effectively dealing with nodes that may not be malicious, but rather may have simply failed as it does not rely on a single node to route its messages.

To overcome the transport layer flooding denial of service attack, enforcing to discern a node's commitment and making the connection by utilizing some of their own resources. This strategy would likely be effective as long as the client has computational resources comparable to those of the server [30].

4.2.2 Secure Broadcasting and Multicasting

The research community of wireless sensor networks has progressively reached a consensus that the major communication pattern of wireless sensor networks is broadcasting and multicasting, e.g., 1-to-N, N-to-1, and M-to-N, instead of the traditional point-to-point communication on the Interne [30]. Next we examine the current state of research in secure broadcasting and multicasting.

As we might see, in wireless sensor networks, a great deal of the security derives from ensuring that only members of the broadcast or multicast group possess the required keys in order to decrypt the broadcast or multicast messages. Schemes that have been specifically designed to support broadcasting and multicasting in wireless sensor networks are addressed below [30]:

4.2.2.1 Secure Multicasting

Describe a directed diffusion based multicast technique for use in wireless sensor networks that also takes advantage of a logical key hierarchy. In a standard logical key hierarchy a central key distribution center is responsible for disbursing the keys

throughout the network. Then key distribution center, therefore, is the root of the key hierarchy while individual nodes make up the leaves. The internal nodes of the key hierarchy contain keys that are used in the re-keying process.

Directed diffusion is a data-centric, energy efficient dissemination technique that has been designed for use in wireless sensor networks. In directed diffusion, a query is transformed into an interest (due to the data-centric nature of the network). The interest is then diffused throughout the network and the network begins collecting data based on that interest. The dissemination technique also sets up certain gradients designed to draw events toward the interest. Data collected as a result of the interest can then be sent back along the reverse path of the interest propagation.

Using the above mentioned directed diffusion technique; one can enhance the logical key hierarchy to create a directed diffusion based logical key hierarchy. The logical key hierarchy technique provides mechanisms for nodes joining and leaving groups where the key hierarchy is used to effectively re-key all nodes within the leaving node's hierarchy. The directed diffusion is also used in node joining and leaving. When a node declares intent to join, for example, a join "interest" is generated which travels down the gradient of "interest about interest to join". When a node joins, a key set is generated for the new node based on keys within the key hierarchy. In this case, nodes are grouped based on locality and attach to a security tree. However, they assume that nodes within the mobile network are somewhat more powerful than a traditional sensor in a wireless sensor network.

4.2.2.2 Secure Broadcasting

Some authors used a routing-aware based tree where the leaf nodes are assigned keys based on all relay nodes above them. They argue that their technique, which takes advantage of routing information, is more energy efficient than routing schemes that arbitrarily arrange nodes into the routing tree. It is a greedy routing-aware key distribution algorithm.

Others use geographic location information (e.g., GPS) rather than routing information. In this case, however, nodes (with the help of the geographic location system) are grouped into clusters with the observation that nodes within a cluster will be able to

reach one another with a single broadcast. Using the cluster information, a key hierarchy will then be constructed.

4.2.3 Cryptography

Introduction

Many institutions and systems need to be secured for safe operation. To make this security tight their communication systems must not be open for all individuals. The problem, here, is most of the time the channel to be used is common resource. Therefore, it becomes impossible to make our communication inaccessible by others. But there is a means to make the messages transmitted secret by using keys. This method of encryption and decryption is called cryptography. In railway industry security is a big issue in which every system must have a bench mark. We have discussed the essentials of wireless sensor networks for the industry. Moreover, we try to understand that there are different types of attacks which can make wireless sensor networks more hazardous if they are not treated with cryptography. In general there are three types of encryption algorithms. They are secret key (symmetric), public key (asymmetric) and one way cryptography. All these are described in the following diagram [32].

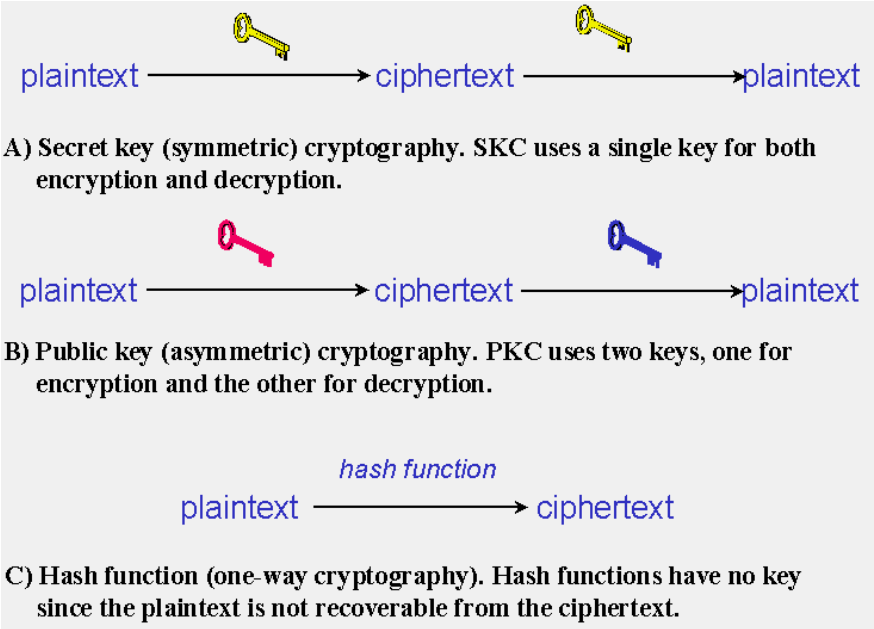

Figure 4-1 Different Encryption Algorithms [32]

Elliptic Curve Cryptography

Elliptic Curves are a type of algebraic curve with a general form described by the Diophantine equation [29]:

$$y^2 = ax^3 + bx^2 + cx + d \quad \text{..... (7.1)}$$

The elliptic curve can be defined over many fields, ranging from the complex numbers C and the rational numbers Q to the real numbers IR and integers modulo p. For any field K we can in general find a group (E(K),⊞). The ⊞ operator that acts upon the elements of the group remains the same algebraically for each field, though the procedure for calculating it may vary slightly [29].

The Diffie-Hellman key exchange method can be used for wireless sensor networks key exchange method. It enables two sensor nodes to transfer keys for each other. This can be an example for symmetric encryption method. This technique can be seen as the effective cryptographic method but it needs a processor with higher speed and capacity. Different authors perform the Matlab implementation of Elliptic Curve Cryptography in different ways. But the necessary elements are more or less similar for all of them. These elements include modular exponentiation, multiplicative inverse over finite fields, modular square roots, addition over elliptic curve, multiplication over elliptic curve and elliptic curve point multiplication [29]. In elliptic curve cryptography a 160-bit key provides the same security as compared to the traditional crypto system RSA with a 1024-bit key, thus lowers the computer power [28]. The use of elliptic curve in cryptography was proposed by Miller and Koblitz. Elliptic curve cryptography is not easy to understand by attacker. So, it is not easy to break. The choice of the type of elliptic curve is dependent on its domain parameters, the finite field representation, elliptic curve algorithms for field arithmetic as well as elliptic curve arithmetic. The optimum selection of these parameters also depends on the security conditions under consideration [28]. Security is critical to sensor networks deployed in hostile environments, such as military battlefield, railway transport and security monitoring. A number of literatures have studied security issues in homogeneous sensor networks. Key management is an essential cryptographic primitive upon which other security primitives are built. Due to resource constraints, achieving such key agreement in wireless sensor networks is non-trivial [28]. Even though elliptic curve cryptography techniques have such important features it is hard to implement them with a simple microprocessor built

in the sensor nodes deployed for railway industry. For this reason we need another robust and simple algorithm which can use for cryptographic application and implemented on simple microprocessor chips built in sensor nodes.

4.2.4 Artificial Neural Network

Introduction

A human brain solves very complicated problems in a short period of time. This process attracts the researcher's attitude towards this complex system of biological neural networks. And this is the reason for the design of artificial neural network system. ANNs allow to learn mappings from a given input space to a desired output space. The life of a typical ANN (neural net) is characterized by two phases: training phase and prediction phase. Though Neural Net is very complex in its pattern it is very effective in solving capacity. It may take relatively longer time to indicate the output due to its computational complexity.

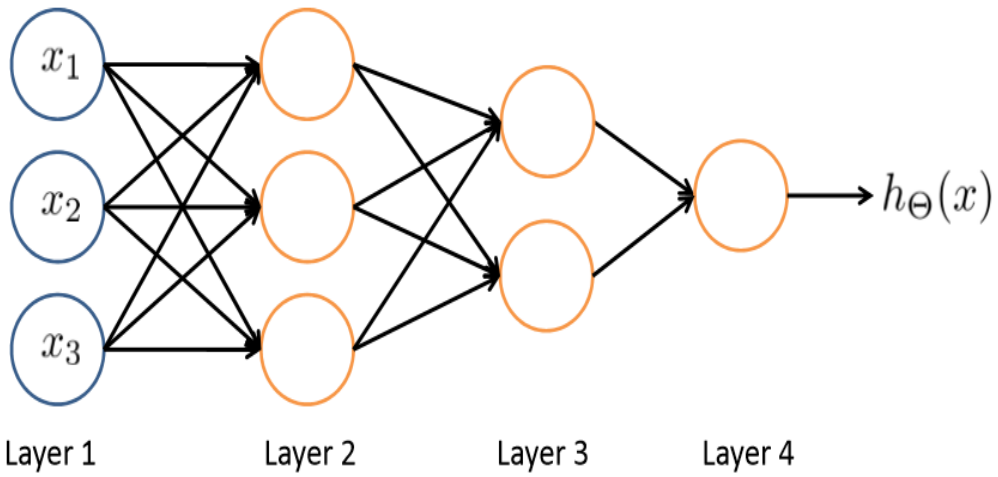

Figure 4-2: Representation of an Artificial Neural Network [34]

An ANN is a system representing the input process and output with analogy to a biological neural network. The first layer in the above diagram represents the inputs and the next layers represent a hidden layer whereas the last layers are representing the output layers. The arrows indicate the direction of flow of data.

ANN, as its name indicates, is a system developed to imitate human nervous system functionality. For instance, if we want the machine to learn classifying the numbers from different handwriting, it is difficult for the computer to identify the handwritings of every person. Since, it only determines what has been programed unless it is trained to classify by having a special training algorisms like neural networks. To determine the number 2 from different handwriting the machine is given variety of hand writing examples for number 2. In this way the machine is looking at the pixels of the number 2 and extracts related features from repeated pictures so that it can learn to differentiate between numbers.

A neural network is implemented to perform computational activity based on the behavior of human brain. It is done using software as well as hardware solutions [32]. Comparison between human brain and computer is difficult. But, one can understand that if a machine is trained to do things in its own we can use the advantage of complex computations in a few milliseconds. The choice of interconnection and activation function decides the capability and performance of the network.

Network Architectures

There are two fundamental different classes of feed forward network architectures [32]:

I. Single-layer feed forward Networks

In an ANN there are layers. The simplest one is a single layer. A single layer contains only the input and the output layers. An input layer is not considered in the number of layers since there is no computation on this layer. It is just only served as a contribution for the next layer. A single layer feed forward network has an output layer which is dependent only on the input layer. But, the output layer does not back contributed to the input layer. As the name indicates the relation is only feeding forward. A diagram representing the general single layer feed forward network is shown below.

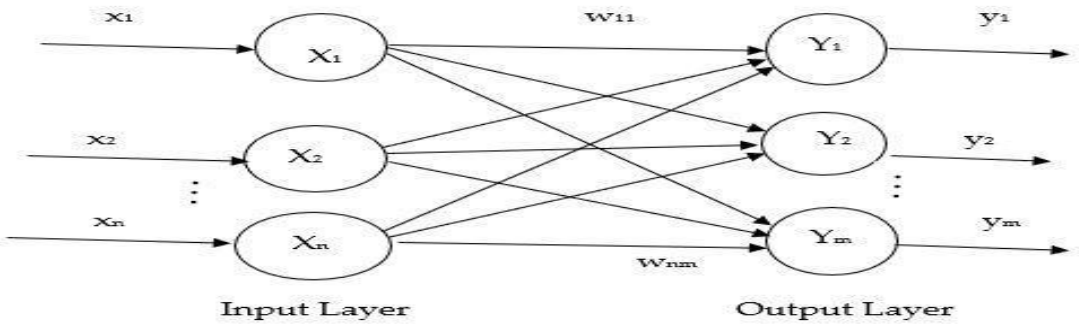

Figure 4-3: Single layer feed-forward network [35]

II. Multilayer feed forward Networks

The multilayer feed forward network is, as the name indicates, the network constructed by two or more layers. That means it contains some additional layers to that of the input and output layers. These additional layers are known as hidden layers. The number of hidden layers is not restricted by standard. Rather, the user decides to limit the number of hidden layers as per his/her interest. But, it is known that as the number of hidden layers gets increased it enables the network to extract more complex features with the cost of slowness.

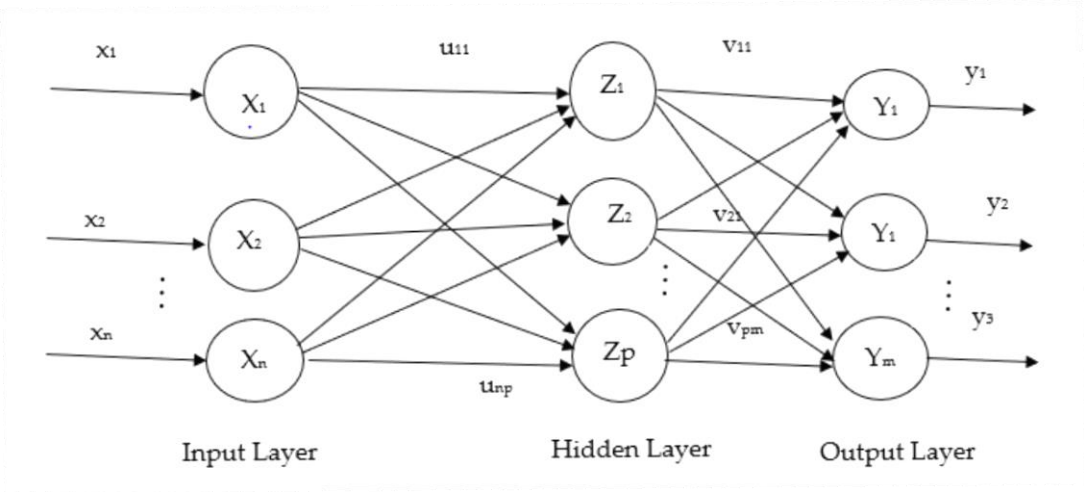

Figure 4-4: Multi-Layer feed-forward network [35]

ANN Structure

A user should first design the topology of the neural network before computation. That means, we need to determine the number of units in the outputs, the number of units in the input and the number of hidden layers and their units. Now the work of the neural

network itself is finding the weights of the connections between the input, the hidden layers and the output which brings good solution which helps in problems requiring prediction or classification.

There is no a standard rule for how to determine the number of hidden layers. Just it is a common practice to try and error until it comes reasonably good result. It is true that the number of hidden layers affects the accuracy of the neural network. And also the initial inputs may affect the accuracy of prediction or classification of the network.

ANN consists of a number of processing units. The units are connected and their relation is determined by weights. These weights are updated with each of iterations based on the activation function. There is also a bias or an external input for each unit. Finally there is rule used to learn or we call it learning rate.

In ANN each units perform activities like receiving information from the preceding unit processing this information and sending the result to the next unit. At the same time the unit performs the work of updating weights. The weights of all the network might be updated simultaneously or one at a time.

For each iteration number n it is designed as the total input to a unit j is the sum of all the multiples of outputs of unit i with the corresponding weights and the bias unit defined by θ_i [26].

$$y_j(n) = \sum_i \omega_{ij}(n) y_i(n) + \theta_j(n) \quad \text{.....} \quad (7.1)$$

Some units may have a contribution of positive result where as some units have negative contribution for the next layer. This depends on the extracted feature. The positive and negative contribution is determining the sign of the weights $\boldsymbol{\omega_{ij}}$. The maximum number of iteration is determined by trial and error as that of the number of hidden layers. Once the cost function converges increasing iteration number will result in better values of weights. There must be also a rule which relates the total input a given unit to its activation which we call an activation function. Mathematically, it can be expressed as [26]:

$$y_j(n+1) = A_j\left(y_j(n)\right) = A_j(\sum_i \omega_{ij}(n) y_i(n) + \theta_j(n)) \quad \text{.....} \quad (7.2)$$

For activation purpose the functions defined by the following curves are commonly used. From those functions sigmoid (logistic) function is most frequently applied for its smoothness. Mathematically, it can be expressed in the following formula [28]:

$$y_j(n+1) = A_j\left(y_j(n)\right) = \frac{1}{1+e^{-y_j(n)}} \quad \text{..... (7.3)}$$

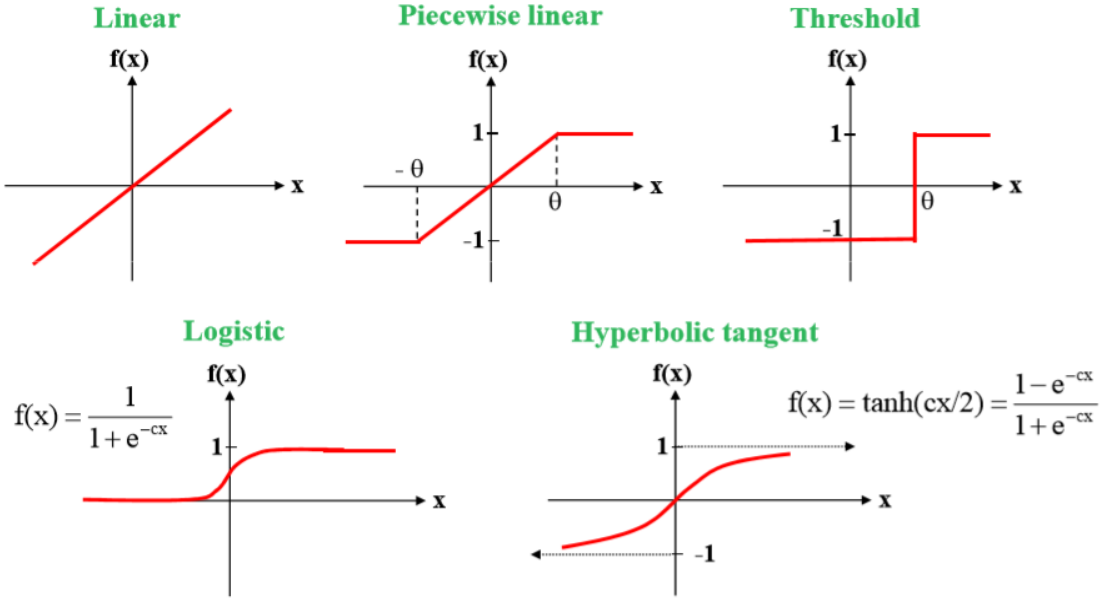

Figure 4-5: Various activation signals for a unit [33]

Training of Artificial Neural Networks

As for all supervised classifiers, one of the most important issues with MLP classifiers is how to train it. Training a multilayer neural net means finding an opportune architecture and the related weight and bias values so that to perform the desired classification task. The highly nonlinear nature of multilayer makes it not trivial to find an analytical solution to the problem [22]. Therefore, one has to resort to numerical optimizers.

Neural network enables the machine to process a computation and learn from the given data. Training of neural network can be performed by adjusting the weights according to some rules. Or sometimes weights can be given explicitly. For a multilayer neural network back propagation rule is widely used to update weights.

Back propagation

A neural network for multilayer feed-forward network is commonly used a back propagation algorithm. Back propagation algorithm learns from the given data set. Using the initial weights, the network is calculating the outputs and the algorithm is comparing the results with the known outputs from the data set [32].

Which connection weights must be modified, and by how much, to perform correctly the desired classification task? To put it another way, how do we know which connection is responsible for the greatest contribution to the error in the output [22]? It is easy to decide the use of proper algorithm which can perform well to update the weights. The most widely used one is the back propagation algorithm.

It is a gradient-based search method which allows finding a (local) minimum of the sum of squared error criterion [29]:

$$E_T = \frac{1}{2}\sum_{i=1}^{N}(y_i - t_i)^2 \quad \text{..... (7.4)}$$

We can use the following equation to find the error for each unit which is used to update the weights [32].

$$\delta_h^p = A' y_h^p \sum_1^N \delta_0^p w_{h0} \quad \text{..... (7.5)}$$

Generally, there are three different phases:

- Forward propagation phase
- Backward propagation phase
- Weight updating phase

Initializing the weights: The weights in the network are initialized to small random numbers (e.g., ranging from −1.0 to 1.0 or −0.5 to 0.5) [22]. Each unit has a bias associated with it, as explained below. The biases are similarly initialized to small random numbers. Each training tuple, X, is processed by the following steps. Propagate the inputs forward: first the input data set is given for the input layer. This data set is fed directly to the output as a buffer, that is, whatever is on the input layer will pass into the output layer. Next, the net input and output of each unit in the hidden and output layers are computed. For any layer in the network to find the values all the connected branches are multiplied by their weights and the resultant is summed with the bias and it will be

assigned for the components in the layer. The bias is used for each unit to vary its result. Having the input all the units implement activation function.

The activation function or logistic function is a nonlinear function which helps neural net to solve classification and prediction problems. With this method we need to compute for all layers including the output layer. Then back propagation follows. The error is propagated backward by updating the weights and biases to reflect the error of the network's prediction. Back propagation learns using a method of gradient descent to search for a set of weights that fits the training data so as to minimize the mean squared distance between the network's class prediction and the known target value of the inputs. The learning rate α helps the algorithm not to be deceived by local extreme values. Rather it will go until it gets the global minima. Biases are updated by the following equations below [29]:

$$\Delta\theta_j = \alpha\delta_j \, , \theta_j = \theta_j + \Delta\theta_j \quad \text{..... (7.6)}$$

4.2.5 Appling of Neural Network for Cryptography

Here, we can use a sequential machine principle to apply neural network for cryptography. Sequential machine based neural network has a bit modification from that of normal neural network structure so that it includes the idea that the output depends on the states of the machine in addition to the given inputs. The output of a machine is fed back into the input to determine the next status of the states [32].

Implementation

To implement a sequential machine based neural network the following diagram is used. The architecture is known as Jordan architecture. In this type of neural network the feedback is given to the input side through the state units which are unique to this network. Once state units are connected to the outputs they will see the values of the output exactly as it is. That means their weights are unity. And back propagation algorism has no effect on these weights.

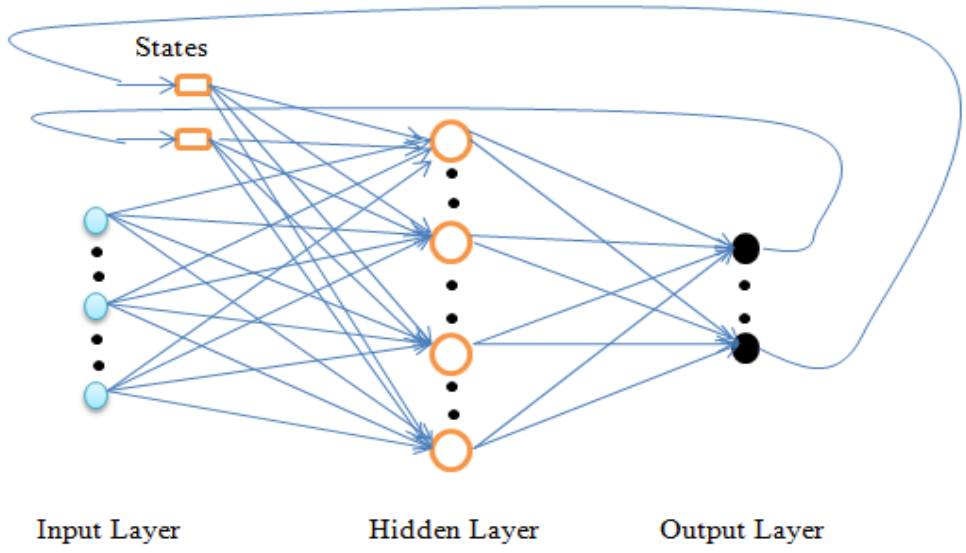

Figure 4-6: Jordan Architecture [34]

As discussed previously the back propagation algorithm is implemented for this network. Every step is the same as normal neural network intuition except the output values are provided as the input via state units. Hence, as usual there is a feed forward propagation in which the output is computed from the current values of inputs and there is a back propagation step in which errors are calculated by comparing outputs and the exact values. And these errors are back propagated through each layer to be used for updating the weights. In general the weights for each unit are to be updated in the following process [32]:

In the feed forward step the inputs to each unit is going to be calculated by multiplying each input connected to the unit by its weight and adding a bias value as follows:

$$y_j = \sum_i \omega_{ij}(n) y_i(n) + \theta_j(n) \quad \text{..... (7.7)}$$

Each unit taking the above input applies an activation function; in our case sigmoid function. Mathematically, it is expressed as:

$$y_{j0} = A_j(y_j) = \frac{1}{1+e^{-y_j}} \quad \text{..... (7.8)}$$

In the back propagation stage the first task is to calculate the errors from the prediction of the network. For a unit j in the output layer it is calculated as follows:

$$\delta_j = (O_j - y_{jo}) A'(y_j) \quad \text{..... (7.9)}$$

From equation 7.8 it can be shown that

$$A'(y_j) = y_{j0}(1 - y_{j0}) \quad \text{..... (7.10)}$$

Substituting equation 7.10 into 7.9 we will find the equation for the error as follows:

$$\delta_j = \mathrm{y_{j0}}(1 - \mathrm{y_{j0}})\,(O_j - y_{jo}) \quad \text{(7.11)}$$

To find the error of a unit in the hidden layer j we can use the following equation [29]:

$$\delta_j = \mathrm{y_{j0}}(1 - \mathrm{y_{j0}}) \sum_k \delta_k w_{jk} \quad \text{(7.12)}$$

In the above equation, δ_k is the error in k and w_{jk} is the weight from unit j to k.

Finally, the weights can be updated using the following equations:

$$\Delta w_{ij} = \alpha \delta_j y_i \quad \text{(7.13)}$$

$$w_{ij} = w_{ij} + \Delta w_{ij} \quad \text{(7.14)}$$

CHAPTER 5 RESULTS AND CONCLUSION

5.1 Result

The neural network based cryptography was successfully built and tried to demonstrate while two nodes are communicating by encrypting and decrypting keys. The neural network based sequential machine is given a word to be encrypted. It first checks the starting state and if the starting state is 1 it changes the first letter of the given word with a letter 2 steps ahead alphabetically. Otherwise if the starting state is 0 it reverts the first letter one step ahead alphabetically. Then the state will be changed to the next state. That is if the state was 0 and the letter was E it will change the letter to F and the state to 1. Then if the next letter was D it will change to F. In this way an encryption takes place. The node wanting to decrypt the word must know and apply this scheme to retrieve the original message. The following figures show the Matlab simulation results.

Figure 5.1 shows the error function versus number of iterations plot. From the plot it can be seen that the error function is decreasing as the number of iteration increases. For the 3000th iteration it results the error value of 0.1132.

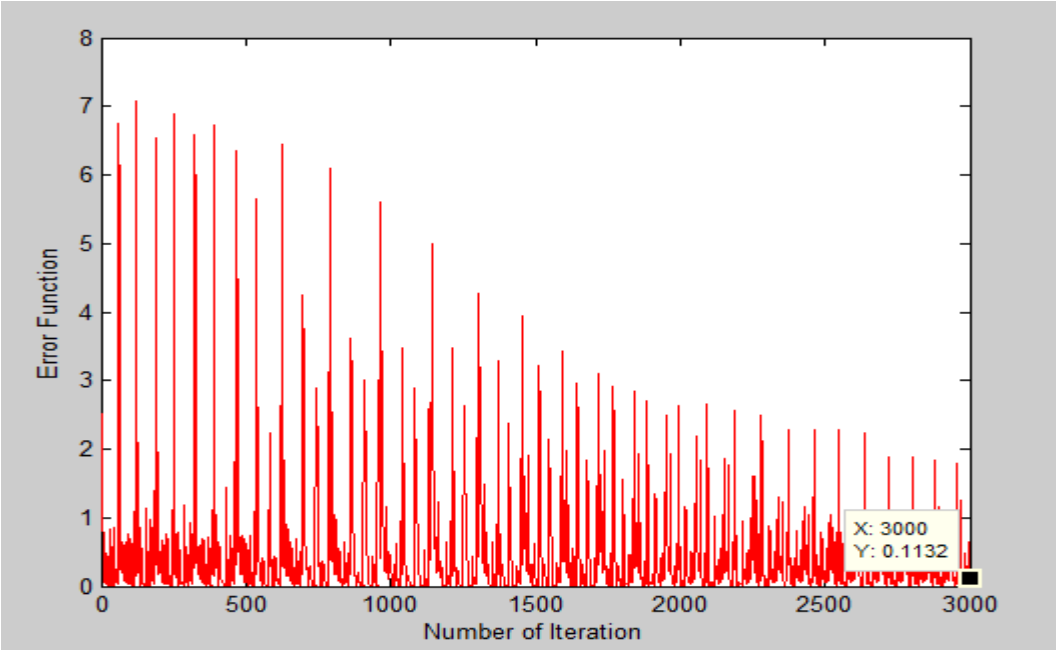

Figure 5-1: Result 1

From Figure 5.2 as the iteration is increased to 5000 the error is decreased to 0.979.

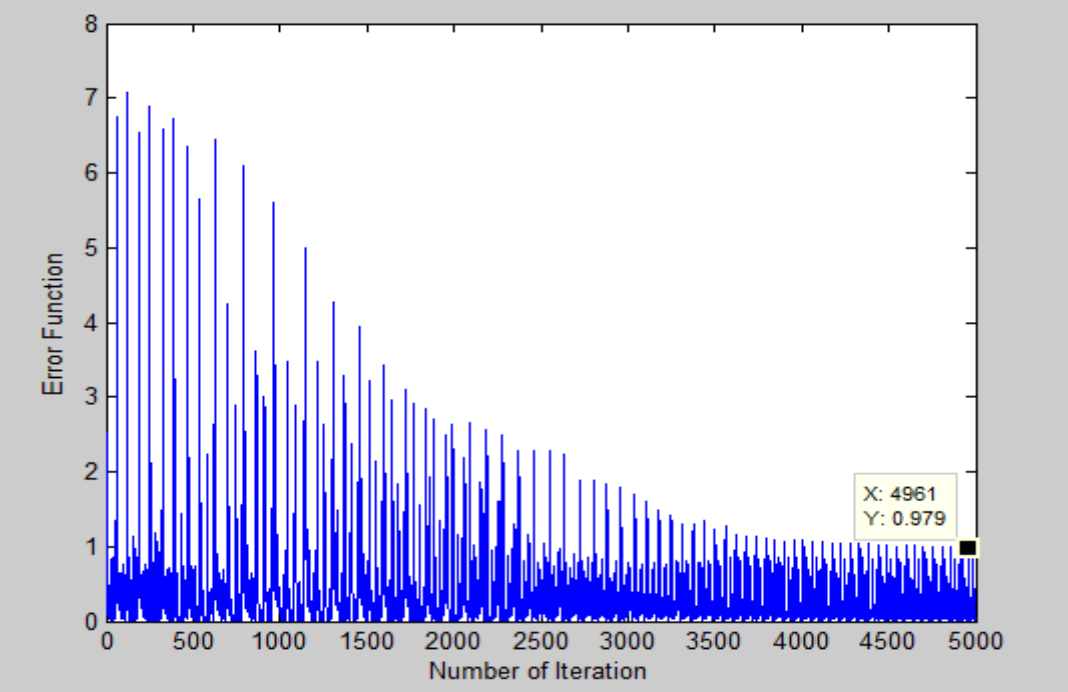

Figure 5-2: Result 2

From figure 5.3 it can be read that at the iteration of 10,000 the error is dropped to 0.01105.

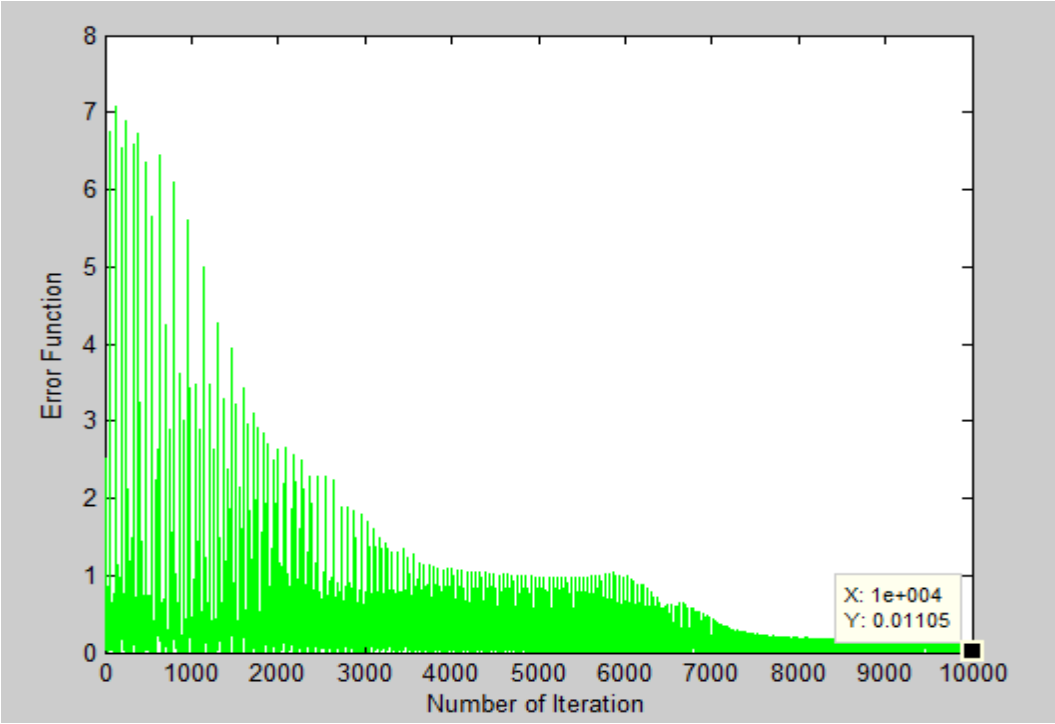

Figure 5-3: Result 3

Generally, the error tends to go to null as the number of iteration increased. But, this cannot be applicable in real case since it needs a processing time. So the optimum value of iteration and tolerated error depends up on the type of processor we used and how fast to be the response required.

The following figure shows that node x is sending a message and another node can read the message after verifying the encryption and decryption keys. In this case, the starting state of the machine is 0 so if the plain text is given as ABCD A will shift one step so it will be B and the state is changed to 1 hence B will be shifted 2 steps to D and the next state is 0, C is shifted to D and D is shifted to F. Therefore, ABCD is decrypted by BDDF. Otherwise, the message cannot be delivered.

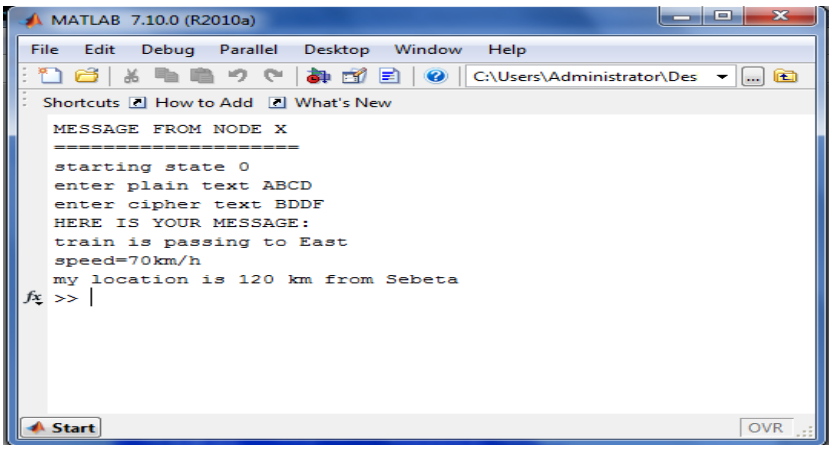

Figure 5-4: Result of State 0

The following figure shows when the starting state of the sequential machine is 1. It follows the same procedure as the above except it starts by shifting the first letter by 2 steps. Hence, ABCD is decrypted by CCEE.

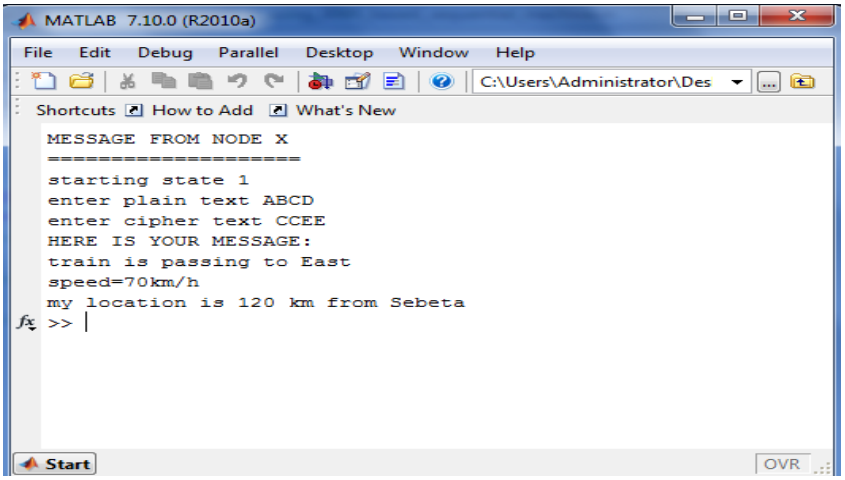

Figure 5-5: Result of State 1

5.2 Conclusion

Wireless sensor nodes are in big endanger of security attacks because of unguided nature of wireless channel. Attacks may force sensor networks to transmit erroneous messages or totally missed the communication. There has to be a method to solve this problem if we need to implement them in cautious industries like railways. Using cryptography for data transmission enhances the reliability and security of a railway system. That is why I intended to do on cryptography based on Artificial Neural Network. Artificial Neural Network is a simple yet powerful technique which has the ability to perform a complex and vast amount of work in a short period of time. It can be used to implement much complex combinational as well as sequential circuits. In this research, I have used this technique to build simple sequential machine using back-propagation algorithm. In general, since data security is a prime concern in security of wireless sensor networks, the use of ANN in the field of Cryptography sequential machine based method for encryption of data is designed. Finally the simulation result indicates that the sensor nodes can communicate securely using secret keys. Better results can be achieved by improvement of code or by use of better training algorithms.

5.3 Recommendation

The field of wireless sensor networks is latest technology. If it is implemented properly it will help railway industries in many aspects such as reduction of cost, low energy consumption and less complexity of circuits. However, they are highly vulnerable for security problems. So, improving security of wireless networks is an open area of research. In this research it is tried to solve security problem by using cryptography based on artificial neural network for its simplicity and suitability. A better result can be found by improving the code or using other training algorithms. Furthermore, anyone who is interested in this field of research can try other methods of cryptography. Despite its complexity, Elliptic Curve Cryptography is the commonly used method in related fields of studies.

REFERENCES

[1] Teklebrhan Aregawi Weldegebreal*," GSM-R Network Design for ATP System of Addis Ababa-Djibouti route",* April, 2015/2007

[2] M. Grudén, A. Westman, J. Platbardis, P. Hallbjorner, and A. Rydberg, "*Reliability experiments for wireless sensor networks in train environment*," in *Proc. Eur. Wireless Technol. Conf.*, 2009, pp. 37–40.

[3] M. Palo, "*Condition monitoring of railway vehicles: a study on wheel condition for heavy haul rolling stock*," M.S. thesis, Luleâ Univ. Technology, Luleâ, Sweden, 2012.

[4] Victoria J. Hodge, Simon O'Keefe, Michael Weeks, and Anthony Moulds," *Wireless Sensor Networks for Condition Monitoring in the Railway Industry: A Survey*, IEEE transactions on intelligent transportation systems, vol. 16, no. 3, June 2015

[5] Ethiopian Railways Corporation, *"Ethiopia/ Sebeta-Djibouti/Nagad Railway; Feasibility Study, Transportation Organization*" Executive Edition, Part III, September 2012, pp.3-12.

[6] http://www.techopedia.com/definition/24191/base-station-controller-bsc(14-May 2015)

[7] http://en.wikipedia.org/wiki/Noise_(electronics)(14-May-2015)

[8] Montegrotto Terme, "*Practical Mechanism to Improve the Compatibility between GSM-R and Public Mobile Networks and Guidance on Practical Coordination,"* ECC report 162, May 2012, p.9-31.

[9] file:///H:/newdata/Receiver_Sensitivity-Learning-Center_Digi-International.htm (06-May- 2015)

[10] file://H:/newdata/noisefigure-Wikipedia,thefreeencyclopedia.htm (17-May-2015)

[11] En.wikipedia.org/wiki/noise-figure (16-May-2015)

[12] http://www.teletopix.org/4g-lte/calculation-for-body-loss-and-feeder-loss-for-lte/ (14-May-2015)

[13] http://wiki.yatebts.com/index.php/Radio_Performance_Concepts(14-May-2015)

[14] http://en.wikipedia.org/wiki/Antenna_gain(14-May-2015)

[15] http://www.l-com.com/content/Article.aspx?Type=N&ID=9475(14-May-2015)

[16] Alireza Shirvani, Bruce A.Wooley, (2003), *"Design and control of RF power Amplifier, "*

[17] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, *"Wireless Sensor Network Security: A Survey"*

[18] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen and David E. Culler, "*SPINS: Security Protocols for Sensor Networks*",

[19] S.Prasanna, Srinivasa Rao, "*An Overview of Wireless Sensor Networks Applications and Security*", May 2012

[20] Kalpana Sharma, Jagdish Kumawat, Saurabh Maheshwari, Neeti Jain," *Railway Security System based on Wireless Sensor Networks: State of the Art*", International Journal of Computer Applications (0975 – 8887) Volume 96– No.25, June 2014

[21] Ethiopian Railways Corporation, "*Ethiopia/Sebeta-Djibouti/Nagad Railway Feasibility Study, Communication*," Executive Edition, Volume II, September 2012.

[22] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: *security protocols for sensor networks*. Wireless Networking, 8(5):521–534, 2002.

[23] Ben Martin. "*Elliptic curve cryptography*," Math 409 Notes, University of Canterbury, 2006.

[24] F. Vercauteren. "Elliptic curve discrete logarithm problem." Lecture Slides, Katholieke Universiteit Leuven, 2005.

[25] Joseph H. Silverman. "*Elliptic curves and cryptography*." In Paul Garrett and Daniel Lieman, editors, *Public Key Cryptography*. American Mathematical Society, 2005.

[26] Culler, D. E and Hong, W., "*Wireless Sensor Networks*", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[27] Adrian Perrig, John Stankovic, David Wagner, "*Security in Wireless Sensor Networks"* Communications of the ACM, Page53-57, year 2004.

[28] J. P. Walters, Z. Q. Lian, W. S. Shi et al., "*Wireless sensor network security: a survey*," in Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, Boca Raton, Fla, USA, 2006.

[29] H. Chan, A. Perrig, and D. Song, "*Random key predistribution schemes for sensor networks*," in Proceedings of the IEEE Symposium on Security and Privacy, pp. 197–213, Washington, DC, USA, May 2003.

[30] R. Watro, D. Kong, S.-F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "*TinyPK: securing sensor networks with public key technology*," in Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 59–64, Washington, DC, USA, October 2004.

[31] K. Piotrowski, P. Langendoerfer, and S. Peter, "*How public key cryptography influences wireless sensor node life-time*," in Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 169–176, 2006.

[32] Vikas Gujral and Satish Kumar Pradhan." *Cryptography using Artificial Neural Networks*", Department of Electronics and Communication Engineering National Institute of Technology *Rourkela*-769008, Orissa, January 2009

[33] Haykin, Simon. *Neural Networks, A Comprehensive Foundation*. MacMillin College Publishing CO, New York. 1994.

[34] Ben Krose, Patrick van der Smagt, "An *Introduction to Neural network*" Eighth Edition , November 1996.

[35] Asmelash Tesfay*,'' Neural Network based 3G Mobile Sites Fault Prediction: A Case Study in Addis Ababa, Ethiopia'',* November, 2018

APPENDIX A

Matlab Code for Neural network based Cryptography:

```
clc;
clear all;
close all;

fprintf('MESSAGE FROM NODE X\n')
fprintf('====================\n')
ix=3;     %---------------------bits
ox=3;
sx=2; %---------------%states

% ---------------------%

for temp=1:100
if 2^temp >=sx
st=temp;
break
end
end
hid=6;    %hidden%layer

% --------------------------  %weights%
wt1=rand(hid,(ix+st+1));
wt2= rand( ( ox+st ) , hid+1 );
Q=1;
l=1;
sx=0;
p=[];

setx=[];
setx=[0000;0010;0100;0110;1000;1010;1100;1110;0001;0011;0101;0111;1001;
1011;1101;1111];

outx=[0011;0101;0111;1001;1011;1101;1111;0001;0100;0110;1000;1010;1100;
1110;0000;0010];

for x=1:10000

   set=setx(l,:);
   out=outx(l,:);
% ---------------------------output%hidden%layer
    inpu=[1 set];
    sumh=(wt1*(inpu)')';
    outh=1./(1+exp(-sumh));

% ---------------------------output%layer
    inph=[1 outh];
    sumout=(w2*(inph)')';
    outt=1./(1+exp(-sumout));

% ---------------------------  %delta
    delout=(outt.*(1-outt)).*(out - outt);

    delh=(delout*wt2).*inph.*(1-inph);
```

```
     %update%of%weight -------------------------

 %output%layer ---------------------------------

    for t=1:(ox+st)
        wt2(t,:) = wt2(t,:) + Q*delout(t)*inph;
    end

 %hidden%layer ---------------------------------

     for t=1:hid
         wt1(t,:) = wt1(t,:) + Q*delh(t+1)*inpu;
     end


    for t=1:(ox+st)

        if outt(t)>=0.7
             outt1(t)=1;
        elseif outt(t)<=0.2
            outt1(t)=0;
        else outt1(t)=outt(t);
        end
 end
   r=[r sum(outt-out)];

    if outt1==out
        l=l+1;
        ssx=ssx+1;
    end

    if l > ((2^inpx)*stx)
        l=l-((2^inpx)*stx);
    end

end
plot(r.*r);

%testing%the%program

stx=input('starting state ');

    io = input('enter plain text ','s');
    fip=[];
    for i=1:length(io)
    b=io(i);
        switch b
        case('A')
            set=[000];
        case('B')
            set=[001];
        case('C')
            set=[010];
        case('D')
            set=[011];
        case('E')
```

```
            set=[100];
        case('F')
            set=[101];
        case('G')
            set=[110];
        case('H')
            set=[111];
        end
    iox=[set stx];
    inpp=[1 iox];
    sumh=(wt1*(inpp)')';
    oh=1./(1+exp(-sumh));

    % %output%layer ----------------------------
    inph=[1 oh];
    sumout=(wt2*(inph)')';
    outt=1./(1+exp(-sumout));

    for t=1:(st+ox)

        if outt(t)>=0.7
             outt1(t)=1;
        elseif outt(t)<=0.2
            outt1(t)=0;
        else outt1(t)=outt(t);
        end
end
  fip=[fip;outt1];
  temph=[];

  stx=outt1( (ox + 1):(ox+st));

end
outz=[''];
for f=1:length(io)
    temph=fip(f,:);
    temph=temph(1:3);

    if temph==[000]
        outz=[outz 'A'];
    end
    if temph==[001]
        outz=[outz 'B'];
    end
    if temph==[010]
        outz=[outz 'C'];
    end
    if temph==[011]
        outz=[outz 'D'];
    end
    if temph==[100]
        outz=[outz 'E'];
    end
    if temph==[101]
        outz=[outz 'F'];
    end
    if temph==[110]
        outz=[outz 'G'];
    end
```

```
    if temph==[111]
        outz=[outz 'H'];
    end
end
io2 = input('enter cipher text ','s');
if outz==io2
    fprintf ('HERE IS YOUR MESSAGE:\n')
    fprintf ('train is passing to East\n')
    fprintf ('speed=70km/h\n')
    fprintf ('my location is 120 km from Sebeta \n')
else
    fprintf ('error!!\n')
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

%%Matlab code for DeffieHellman ECC:

```
clc;
clear all;
close all;
%enter public information
Disp(' ')
ECp=input(' EC parameters [a b c d]= ')
Disp('')
P=input(' prime number p=');
%check primality
If isprime(p)==0
Error('Input is not prime')
End
Disp('')
P=input(' Point p=[px py]=');
Px=p(1);
Py=p(2);
%verify thet point p is on the EC
PECflag=isecptmod(px,py,ECp(1),ECp(2),ECP(3),ECp(4),p);
If PECflag==0
Error('point p does not lie on the specified elliptic curve')
end
disp(' ')
disp('Enter Private Information:')
a=input(' Natural Number a=');
%Perform A=aP calculations
[Ax, Ay]=elcmultmod(a, Px, Py, ECp(1), ECp(2), ECp(3), ECp(4), p);
A=[Ax, Ay];
disp('Send the following EC point to counterpart') fprintf(' A = [%3d
%3d ]\n\n', Ax, Ay)
%Enter Recieved data
disp('Enter EC point recieved from counterpart')
B=input(' Point B = [Bx By] = ');
Bx=B(1);
By=B(2);
%Verify that point B is on the EC
BECflag=isecptmod(Bx, By, ECp(1), ECp(2), ECp(3), ECp(4), p);
while -BECflag
  disp ('Point B does not lie on the specified EC;')
  disp ('Enter new Point B value:')
  B=input (' Point B = [Bx By] = ');
  Bx=B(1);
  By=B(2);
```

```
  BECflag=isecptmod(Bx, By, ECp(1), ECp(2), ECp(3), ECp(4), p);
end
% Calculate Key K
[Kx, Ky]=elcmultmod(a, Bx, By, ECp(1), ECp(2), ECp(3), ECp(4), p);
K=[Kx, Ky];
%Output Key K
fprintf('The    key    is    K    =    [%3d    %3d    ]\n\n',    Kx,    Ky)
disp('>·····>')
```