REMOTE MEDICAL EMERGENCY RESPONSE

THROUGH NEAR-ME AREA NETWORK

By

SWETHA NANDIRAJU

Bachelor of Science in Information Technology

Jawaharlal Technological University

Hyderabad, Andhra Pradesh

2010

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
May, 2015

REMOTE MEDICAL EMERGENCY RESPONSE

THROUGH NEAR-ME AREA NETWORK

Thesis Approved:

Ting Ting Chen

Thesis Adviser

David Cline

Christopher Crick

ACKNOWLEDGEMENTS

I would like to thank Dr Ting Ting Chen for guiding me patiently and for all her support without which this work would not have been possible. For her instructions were valuable and are the reasons for this great achievement.
I would also like to thank Dr David Cline for all his time and dedication towards the document and suggesting appropriate changes wherever he found a scope for betterment.
I would like to take this opportunity to thank Computer Science department at Oklahoma State University for providing me with resources that were really helpful in conducting the experiments.
A big thanks and love to my mom, Mrs N Jayalakshmi, who was responsible for encouraging me to pursue masters at an international level.

Acknowledgements reflect the views of the author and are not endorsed by committee members or Oklahoma State University.

Name: SWETHA NANDIRAJU

Date of Degree: MAY, 2015

Title of Study: REMOTE MEDICAL EMERGENCY RESPONSE THROUGH NEAR-ME AREA NEETWORK

Major Field: COMPUTER SCIENCE

Abstract:

With the advancement in technology, there have been found ways in which even Healthcare can be made readily available. Technologies involving Body Sensor Networks, Wireless Communications and Security in wireless media, have helped to a great extent to make it possible. With this project, we are trying to make remote healthcare readily and quickly available. The secure automatic emergency response system that we develop helps in attending to patients quickly by propagating a help signal to potential healthcare provider. The signal propagates from sensors on a patient till it reaches the nearest Healthcare node and alerts it informing an authentic Healthcare provider near the patient, in case of emergency. For this kind of propagation, we take the help of a Networking technology called the "Near-me Area Network". A Near-me Area Network helps in full duplex communication between nodes in spatial proximity, precisely, sending the readings pulled from Body Sensor on the patient and receiving appropriate help from the healthcare provider. This avoids the need for human intervention from the side of patient in getting help for the health ailment.

Given that communication is wireless, and several intermediate nodes are involved in the transmission process, security is an issue. We take care of securing the location and vitals information of the patient by encrypting all the data that is being transmitted. We also try to eliminate duplicate and unauthentic signals by posing a few constraints on the initial signal generation.

Our simulation results show that the system determines the presence of a potential Healthcare Provider within 2 minutes and if the presence is positive, healthcare is provided to the patient readily by the identified health official.

TABLE OF CONTENTS

Chapter Page

I. INTRODUCTION 1

1.1 Overview 1
1.2 Background 2

II. REVIEW OF LITERATURE 4

2.1 Near-me Area Network 4
2.1.1 Communication in NAN 7
2.1.2 Application Scenarios of NAN 8
2.1.3 Advantages and Disadvantages 8
2.2 Scattered Network 9
2.3 Scattered NAN 9
2.4 Security in Wireless Communication, NAN and Healthcare 10
2.5 Public Key Infrastructure 12
2.6 Existing Technologies and Challenges 13

III. PROBLEM STATEMENT 15

IV. SYSTEM DESIGN AND IMPLEMENTATION 17

4.1 Design 17
4.1.1 Broadcast and Discover Module 19
4.1.2 Listen Module 22
4.1.3 Secure Communication Module 24
4.2 Simulation 25
4.2.1 Simulation Environment 25
4.2.2 System Requirements 26

V. SIMULATION RESULTS 27

5.1 Single Hop 29
5.2 Two Hops 31
5.3 Isolated Location 33
5.4 Performance 33

VI. CONCLUSION 35

REFERENCES 36

LIST OF FIGURES

Figure Page

1 Near-Me Area Network Architecture 7

2 Packet Traversal Between Two nodes in NAN……8

3 Scatternet…….....10

4 Scattered NAN……10

5 Overall System Design……...18

6 Overall Functional Design……..19

7 Broadcast and Discover Design……..20

8 Broadcast and Discover Flowchart…….22

9 Listener Module at Patient Node……....24

10 Secure Communication module……25

11 Single Hop at Patient Node……...…31

12 Single Hop at Healthcare Node……...…..31

13 Two hops at Patient Node……...…..32

14 Two Hops, Intermediate Node……...…...33

15 Two Hops, Healthcare Node……...…..33

16 Isolated Location, Patient Node……...….34

17 Performance……...…...35

CHAPTER I

INTRODUCTION

Health Informatics, a field of research and development, is a combination of two different fields with same area of focus [1]. Specifically, both Healthcare and Informatics have in common, the goal to efficiently store healthcare data, information and process it wisely for solving problems and taking decisions. This chapter discusses about the evolution of Healthcare to the current m-Health and how it has been used for developing the current system and the technologies that form its backbone.

1.1 Overview:

America spends about 17% of its GDP on healthcare [2], usage of technology in the field of healthcare has hence been researched into and remote healthcare, which could help in delivering services to patients without actually needing patient's presence in a hospital, has been identified to be a useful contribution to the field of healthcare. It has considerably impacted the number of deaths that occur due to lack of help during emergencies. The continuous and rapid development in information and communication technologies has directly or indirectly affected every field of the generation previous to it. Healthcare is one of them.

During initial days of its emergence, the Healthcare departments wanted to make the health information of their patients to be easily accessible and shared with other professionals for their

opinions. This demanded that the data be electronic and hence evolved the e-Health. E-Health is a modern healthcare practice that includes electronic storage, processing and communication of health information between institutions and professionals [3]. Later, it was noticed that, patients made use of electronic communication devices to interact with the healthcare professional, a process named Interactive Health Communication (IHC) [4] was booming rapidly.

Later, with mobile phones becoming ubiquitous, mobile apps are becoming more and more popular among customers who look into their mobiles for more than mere communication. Telemedicine, one of the early remote healthcare technologies, has considerably impacted the availability of healthcare and the costs involved in it by taking even rural areas into consideration. The services offered by Telemedicine include full-duplex communication between the patient and the registered healthcare provider through audio or video on his mobile phone.

These trending technologies made us realize the huge potential in areas of information technology and mobile telecommunications for developing meaningful and useful services.

1.2 Background:

The ubiquitous use of mobile phones made the scientists and developers turn their focus onto the technologies like Telemedicine, and its companion e-Health. A recent survey found about 40,000 mobile health applications across multiple platforms, with Apple alone having about 12,000 of them available in Apple Store [5]. These facts help us understand the public's interest in using app-based services.

With sensitive information being stored in the cloud, it would be definitely tempting for evil minds to snatch the information for personal gains, and Telemedicine and its successors are no exceptions. There are multiple reasons why the data or information that is being accessed in the healthcare field needs to be safeguarded. First, the information about the vitals of a person must not be tampered with, as it could lead to a wrong diagnosis and treatment. Second, the data could

be used to commit crimes and discriminate against the patient. For example, patients with HIV or other diseases may not wish to reveal their ailment to others. Compared to the traditional file method of storing data, wireless transmission is much more vulnerable to security and privacy threats. This justifies the requirement for security and privacy, both, while accessing and transmitting data [6].

The system we designed in this work is a combination of three fields of interest, namely Mobile Telecommunications, Networking and its Security, and Health Informatics. It uses patient's mobile device as a network initiator that helps him connect to the healthcare provider. We make use of one of the Mobile Telecommunications Standards that allows patient's node to provide certain services relevant to the situation.

The link to Networking from Telecommunications comes from the idea that mobile's ability can be expanded hugely by providing it with access to the Internet. By applying this idea, we were able to create a new network namely Near-me Area Network. It determines the presence and helps receive attention and/or response to the situation of a medical official even when at a location other than a hospital or clinic.

As the communication is required to be highly confidential and private, there appeared to be a need for sound security protocols. Each of the security attributes has been attended to individually in order for our system to deliver secure and reliable services.

The system we developed comprises the following aspects apart from monitoring the health status of a patient (1) Identifies if there are any nodes in the patient's close proximity that are willing to help the source; (2) Creates a network; (3) Connects the patient to the nearest Healthcare provider; (4) Initiates a secure two-way communication.

CHAPTER II

REVIEW OF LITERATURE

In this chapter, we discuss how various technologies could be correlated and the resultant could be made use of in solving difficult problems and/or making decisions. We particularly introduce a novel network architecture called the Near-me Area Network and explain how we can collaborate it with the Scatternet(a concept in Bluetooth for expanding a network) to obtain a resultant Scattered NAN that can be used in various disciplines of research and development. We also discuss the security and privacy aspects that have been most bothered-about issues when it comes to making healthcare an electronic dependant. It is because of the native roots of interception, alteration and disruption kind of threats in wireless means of communication ,that we need to pay special attention towards this aspect especially in Healthcare.

Later in this chapter, we discuss similar research problems and existing solutions and provide the basic knowledge required to understand the current problem.

2.1 Near-me Area Network

Services tend to be classified based on the segment of the population that might use them. For example, an app with compass to show directions, or a maps app is useful for people who travel a

lot. Gaming apps are meant for people who fancy playing them. In both these cases, people are categorized depending on their interests. Similarly, a few apps require categorizing people based on the distance between each other. For example, a person who wants to sell away his concert tickets might find another one looking to purchase, just around him. This kind of scenario requires a network to be formed among all the people in a certain radius of area. Such services are called the Location Based Services.

A few examples of location-based services are location-based advertisements – nearest theater to me, Traffic Monitoring and Points of Interest [7]. These systems involve static information stored in a server and when the user's mobile tries to query the app, server responds with the results.

Near-me Area Network is one such logical network that is formed based on the latitudinal and longitudinal values of all people's mobile phones in a certain area and offers location based services to them. A typical communication link in NAN goes from the mobile's LAN to Internet to the receiver's LAN and then to the receiver's mobile phone. It is not a "Querying Server" kind of architecture. The mobile phones are assumed to be possessing GPS (Global Positioning System) and Internet Connectivity. NAN is a dynamic network that is formed when there is a health emergency situation with a patient who is using the service.

Figure 1 explains that the mobile phones, which are communicating with their respective mobile carriers before getting connected to a near by device that is identified through the Internet.

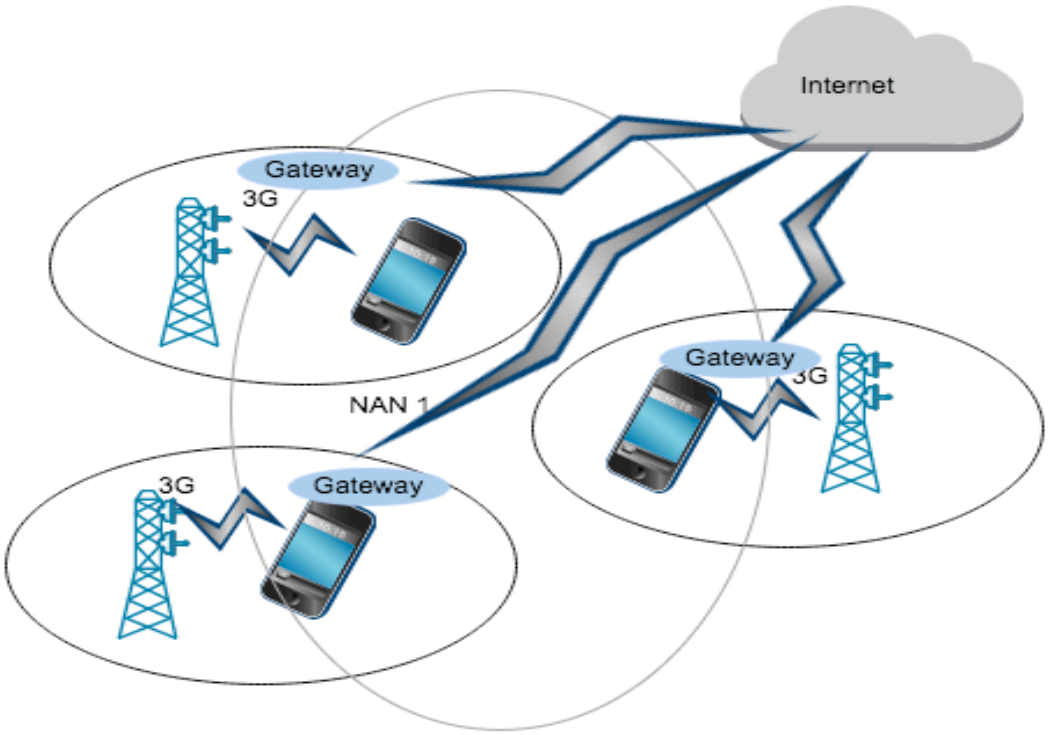

Figure 1: Near-Me Area Network Architecture

The architecture [8] explains that a logical network is formed from a physical network i.e., the Internet. It's based on the radius of NAN that these nodes, which fall inside the radius, are considered a part of it. Therefore, any broadcasted communication that is being carried out could reach all the nodes within the network. A typical data packet's traversal is explained in the **Figure 2** below as well as in the steps following it.

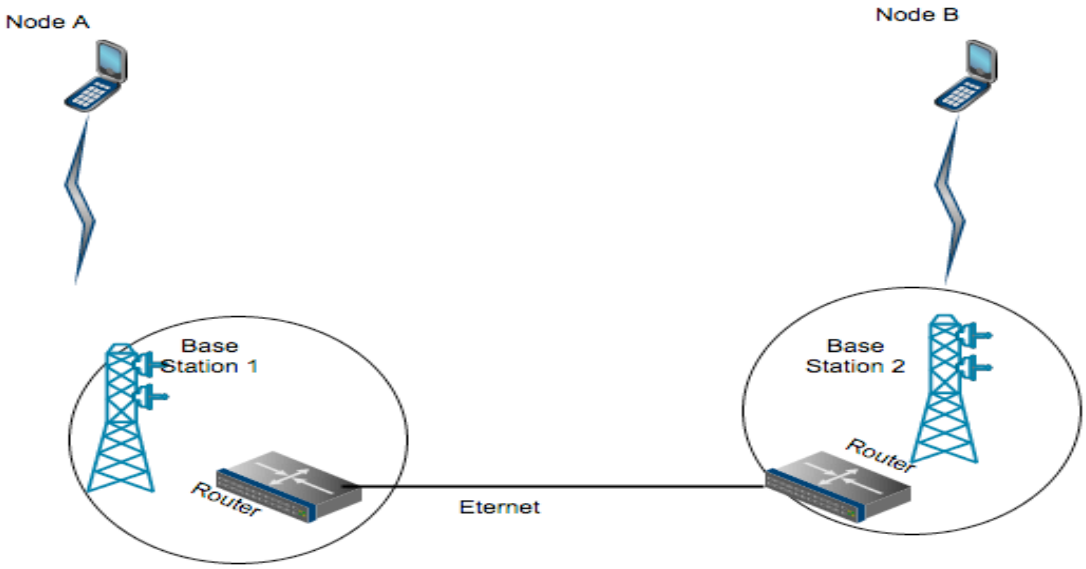

Figure 2: Packet traversal between two nodes in NAN

2.1.1 Communication in NAN

Steps followed by any packet in NAN is as follows:

1. Sender's mobile communicates with its carrier base station.

2. Base Station transmits packet across to the other base station through gateway(router) which connects to the destination gateway through Internet.

3. Receiver's gateway, which is at the receiver's carrier base station, sends packet to the receiver's mobile.

2.1.2 Application Scenarios of NAN

1. **WhosHere:** It's a mobile app that helps users meet people nearby with similar interests. It lets users create a profile and looks for a matching profile around them.

2. **Loopt:** Loopt is a mobile service that allows users to share their location and other details with a group of selective other users. It helps users to update their location to the server; view their friends' locations by querying the server.

Various other apps that offer location based services are, in a way, using NAN technology.

2.1.3 Advantages and Disadvantages

Satellites that are typically required in Global Positioning Systems do not often work indoors. Near-me Area Network can be advantageous in this aspect. For example, within a shopping mall, information about a product can be exchanged between people using NAN services. This avoids satellites tracking each of the users and then transmitting advertisement messages individually.

On the negative side, making location easily available to others might become a threat to privacy of the user. Therefore, NAN applications must be built in such a way that they allow users to choose different levels of location information, i.e., exact location or neighborhood or city, etc. There could even be threat to authentication and confidentiality attributes of security in NAN applications; Section 2.4 discusses security aspects in NAN in detail.

2.2 Scattered Network

A scattered network is an extended network that is formed when two or more piconets are combined using one or more bridge nodes. Scatternet [9] has been proposed for networks utilizing low range radio frequency like Bluetooth. **Figure 3** below depicts how a network of limited nodes in it can be extended using bridge nodes. A bridge node is the one, which belongs to two piconets at the same time.

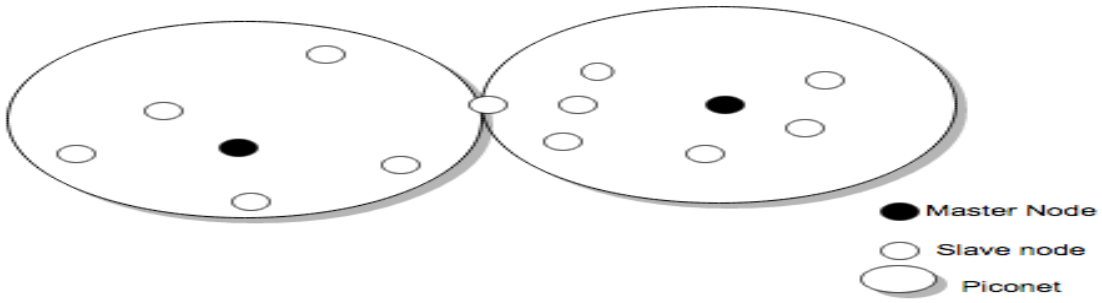

Figure 3 : Scatternet

2.3 Scattered NAN

Many meaningful applications can be developed by using this simple architecture, which saves bandwidth by just broadcasting to nodes that would contribute to the purpose of the network. A scattered network expands gradually to a wider, meaningful area. Especially in Healthcare domain, where the locality of a Healthcare provider is important to the patient, this type of network expands its search area gradually and makes sure that the nearby places that could be useful are not neglected.

Figure 4: Scattered NAN

Unnecessary transmission of data packets to the nodes that do not or cannot contribute to the healthcare of the patient can be avoided by this simple calculation of distance and forming a virtual network.

2.4 Security in Wireless Communication, NAN and Healthcare

Security is as core to the Remote Healthcare domain as treating a patient is. Transmission of patient's healthcare information over a wireless medium increases the vulnerability of the data due to characteristics of wireless medium, in which the risk of interference and interception is greater than in wired networks. Also, reliability, security and range have been indentified as the disadvantages of using a wireless network [10]. Among these, security and reliability come hand in hand. Securing the identity and location of the communication parties, mainly, have been the two vital aspects that need to be looked into, in this kind of insecure (wireless) environments [11].

One of the disadvantages of Near-me Area Network is that it poses threat to location privacy of the user it is serving. Even though the essence of NAN is to make the location information available to the user on the other end of the communication line (to Healthcare provider in current project), masquerading is possible type of attack where the receiver could be disguised as an authentic message receiver. Masquerading type of attack can cause several problems that are typical to a Healthcare System and these are discussed below. Confidentiality is another attribute that needs attention in networking. In Near-me Area Network, limiting information access to authorized people and preventing access to unauthorized ones, needs to be implemented in order to address the confidentiality aspect of Security.

The main purpose of using technology in various fields is to make life easier. Remote Healthcare especially, has a meaningful purpose as the name suggests. It has the goal of saving lives rather than making them easier; an even more meaningful purpose. A few reasons as to why patient's data needs to be secured are: reputation damage and image harm. Data integrity is also important because if the data, during its traversal, gets tampered with, this results in wrong diagnosis. Giving control of sensitive information transmission to the patient himself wins the confidence of the patient over the system he is using. There have been many policies and procedures that were followed to safeguard patient's personal information. For example, patient consent forms are required before giving away the information to other authorized officials [12]. But, once the data is on the transmission line or on the transmission media, this problem of safeguarding data is no more with the Health institute. Instead, it is with the computing professionals that develop the system.

Encrypting the communication between these parties solves the problems of data tampering. The encryption schemes that mainly used keys, performed great when it came to disguising the messages before putting it onto the transmission medium. The trick lies in the one-way function

that can compute public, private key pair. Hence, we determined that Public Key Infrastructure (PKI) is one solution for protecting patient's data's integrity.

2.5 Public Key Infrastructure

In this section, we discuss how PKI contributes to secure information exchange in Near-me Area Network. The security features of PKI include Authentication, Privacy and Non-Repudiation, which combined, promise a secure information exchange environment [13].

2.5.1 Entities in PKI:

1. Digital Certificate: Digital identities, issued by the trusted third parties, act as a proof that the entity bearing it is trust worthy and could be further considered for information and/or data transactions.

2. Public and Private Keys: These two mathematically related entities forma a strong foundation for secure communication that is required in any kind of network that uses PKI.

3. Certificate Authority: This entity is a trusted third party (i.e., not a member of network), that issues Digital Certificates to the parties whom it feels are authentic. Therefore, when a Digital Certificate is looked in order to authenticate its bearer, we are authenticating not only the bearer but also the Certificate Authority that issued it.

2.5.2 Advantages of PKI:

1. Public Key Infrastructure provides to its user, a choice of choosing their Certificate Authority and does not restrict the options to a limited set.

2. PKI is highly scalable. Any number of members can be issued Digital Certificate and hence be made to participate in various network communications.

3. PKI is flexible. This means that a member who has a Digital Certificate by other authentic Certificate Authority does not need to sign up with the system but can authenticate with the server instantly.

These features and advantages offered by PKI, made it suitable for the current system in terms of conducting secure information exchange between various wireless nodes.

2.6 Existing Technologies and Challenges

Remote Healthcare has received attention from technologists and scientists ever since Internet transitioned into the smarter Internet of Things (IoT) [14]. Internet of Things is a network of physical "things" embedded with electronics, software, sensors and connectivity, that work with each other in order to obtain solutions to existing real-time problems in varied fields [15]. 'Remote Patient Monitoring' has been one such field that used IoT in order to monitor patients with chronic illnesses and send information using the Internet to the registered Healthcare official.

Telemedicine, a better approach, came into the limelight where assistance has been offered to patients by voice or video communication [16]. Then evolved m-Health, collaboration of mobile computing, medical sensor and communications technologies for Healthcare [17].

By far, healthcare through remote patient monitoring has been the solution to the current research question, where, the assistance is made available either in text, voice or video. Our attempt is to make healthcare available to the patient, which might as well involve physical presence of the nearest Healthcare representative, which is an ideal thing to do during critical situations when waiting for more than a minute cannot be afforded by the victim.

The system takes into account physical proximity and makes use of the near me feature to contribute to the Remote Healthcare field.

CHAPTER III

PROBLEM STATEMENT

Personal Emergency Health Response Systems, which typically are Hardware devices that detect certain kinds of signals, coming from their partner hardware, in order to alert the emergency response team, have been observed to fail due to various reasons. Few of the reasons are rebooting of their base system, signal attenuation due to increase in distance between the transmitter and the receiver and/or the response team taking more than the anticipated time to reach the patient's location.

This called for an attention towards developing a system that is reliable and is sensitive to distance to replace those that deceived user about their healthy operation [18] because there is no way for the user to determine when the above mentioned failures occur.

There have also been many cases that have been observed where patient could not receive appropriate treatment due to

a) time lag in the response from the healthcare provider. For example, Emergency Response Systems [19], have been observed to take an average of 30 minutes before they reached the hospital after picking up the patient which is clearly not a time efficient way of handling patients.

b) inability of the healthcare providers to respond to the healthcare emergency situations remotely. As most of the current services like Telemedicine [20], Personal Emergency Reporting Systems [18], use e-Health technology either to monitor patient's health. remotely or offer audio/video help that would require presence of a person by the patient or health education through digital media.

Reasons a) and b) seem to affect about 3 million patients all around the world [21] and indirectly called for a system that is sensitive to time and urgency that helps avoid the loopholes. The current study contributes to Emergency Remote Healthcare by solving the problems discussed above which are posed by the current technologies.

CHAPTER IV

SYSTEM DESIGN AND IMPLEMENTATION

This chapter explains the design of the Emergency Response System we are developing, and goes over its modules and their functionalities in detail. Based on problem analysis, we determined that the important phases required for the efficient functioning of the system are Discovery Phase(Start point), Listening and Communication(Loop point) and Termination(End point). These three phases are discussed thoroughly through out this chapter.

Later in the implementation section, the modules in design are given real tasks to do in order to contribute to the functioning of the system. These tasks are explained in the flow charts.

4.1 Design:

The Emergency response system aims to get a patient connected to the nearest Healthcare provider. It can be used at any location where patient's, participant's and healthcare provider's nodes are connected to the internet. The proposed system needs access to the Internet to determine the physical proximity of the nodes that are ready to contribute to the Scattered Near-

me Area Network. Also the nodes need to get their digital certificate from an authorized certification authority. **Figure 5** below shows system design of the proposed emergency response system using NAN.

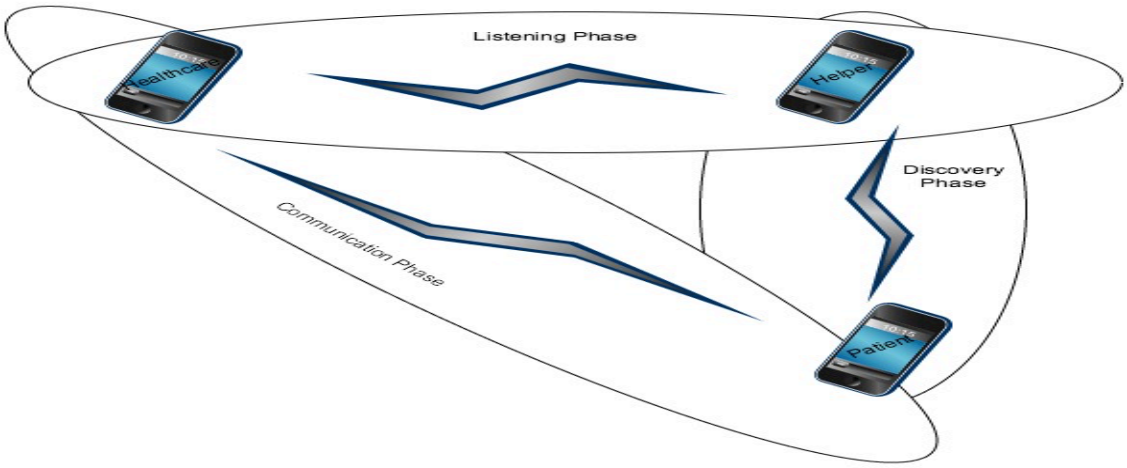

Figure 5: Overall System Design

Like a typical m-Health architecture, the current system has three technologies core to its functionality [13]. They are:

1. Wearable and Sensors, which create a data stream of vital health measures from a patient,
2. Information and Communication Systems such as mobile phones to provide continuous internet access , and
3. Computing and Internet technologies, which helps set up Near-me area Networks on top of the global net.

Each of the above acts as a functional module. They collaborate and communicate with each other, which can be seen in terms of messages as shown in **Figure 6 below.**

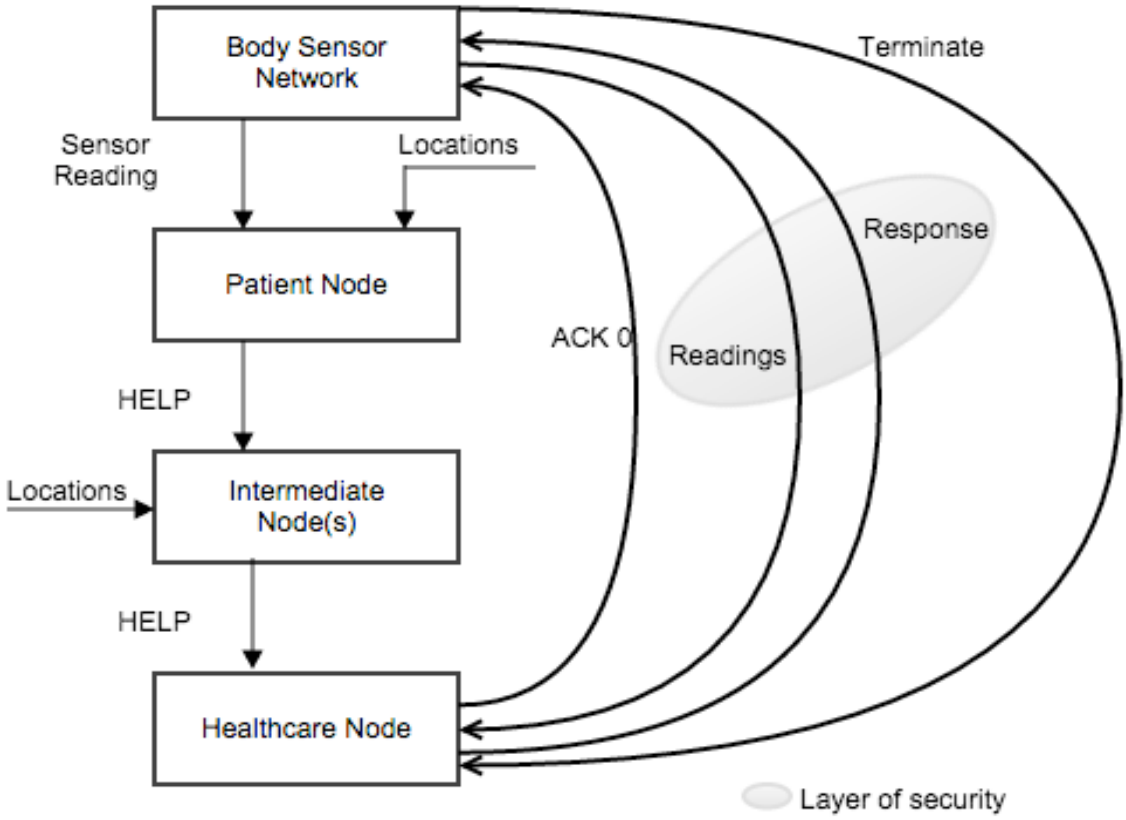

Figure 6: Overall Functional Design

4.1.1 Broadcast and Discover Module:

The design of the Broadcast and Discover module is shown in the **Figure 7** shows what triggers the system and how the NAN network is formed. As demonstrated in the figure, there might be a few nodes that are nearby the Patient node but do not want to participate in the network. The network can still form without them, however.

Figure 7: Broadcast and Discover Design

The flow of events that take place during Broadcast and Discover Phase is shown in the flowchart in **Figure 8**. It explains about the actions carried out by the Network initiator (the patient node). The Patient node initially broadcasts HELP message to other nodes, which are ideally listening continuously. This module includes broadcasting and socket timeout period which determines if there are no helper ready for forming the network. The Patient node also listens for acknowledgement for a certain period of time after which a pre-determined action will take place, like calling emergency services. Also, a database that has the current location of the helper nodes is accessed through the Internet to determine the distance between each acknowledging node and

the patient node. Nodes that are within a predetermined distance from that of patient's are shortlisted for further communication.

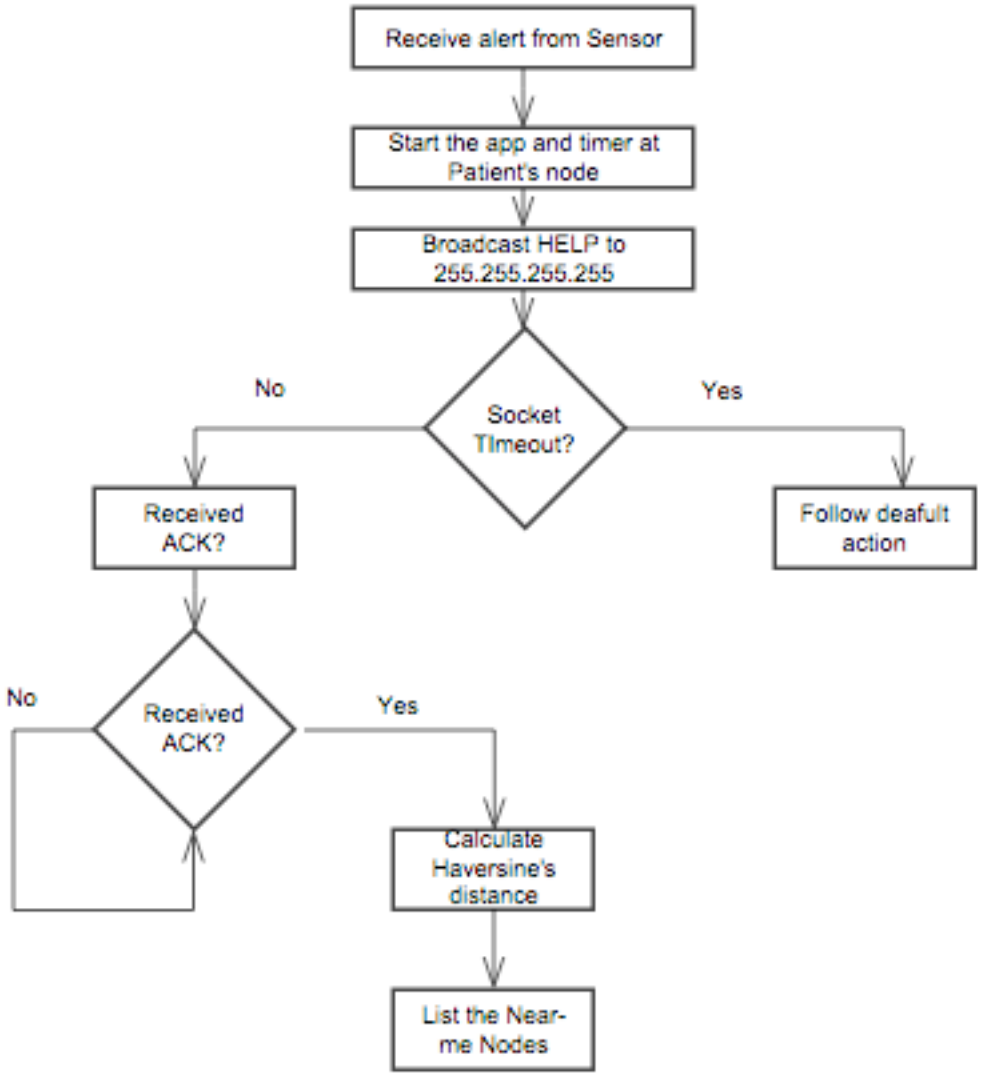

Figure 8: Broadcast and Discover Flowchart

4.1.2 Listen Module:

At this stage, the patient node keeps listening at a particular port that only a Healthcare is supposed to be sending to his ACK at. Listening at this port takes place for a certain amount of time after which it times out. This is to make sure that the process doesn't delay calling the registered emergency service any longer than a patient can afford. While the patient node is listening for a Healthcare's ACK, the intermediate helper nodes, which already received the HELP message from patient, follow the 'Broadcast and Determine' process to identify their Near-me nodes and propagate the message.

If the timer times out before receiving an ACK from a healthcare provider, a call to a standard emergency service such as 911 is dialed from the phone.

When the Healthcare node receives the packet from the intermediate node, it decodes the IP address contained in the packet and binds the IP address to the port number that has previously selected. Flow chart of listener module that is running on the patient is shown in the **Figure 9** below.

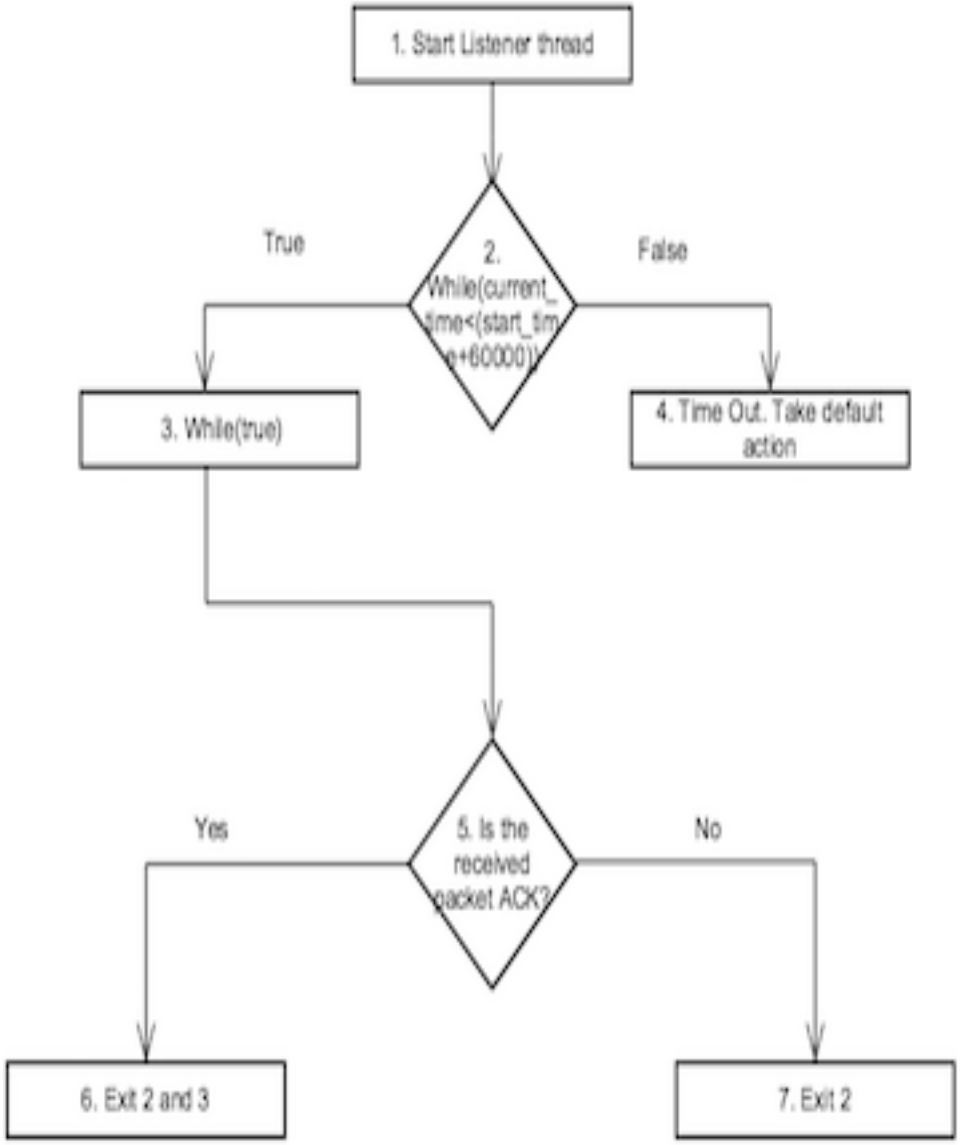

Figure 9: Listener Module at Patient's node.

4.1.3 Secure Communication Module:

As soon as a Healthcare Node receives the IP of the patient, it binds its Socket with patient's IP address, sends an ACK and listens to it. After the patient receives an ACK from the healthcare node, a direct communication channel is formed between the Healthcare Provider and the Patient The flow chart below explains these steps in detail.

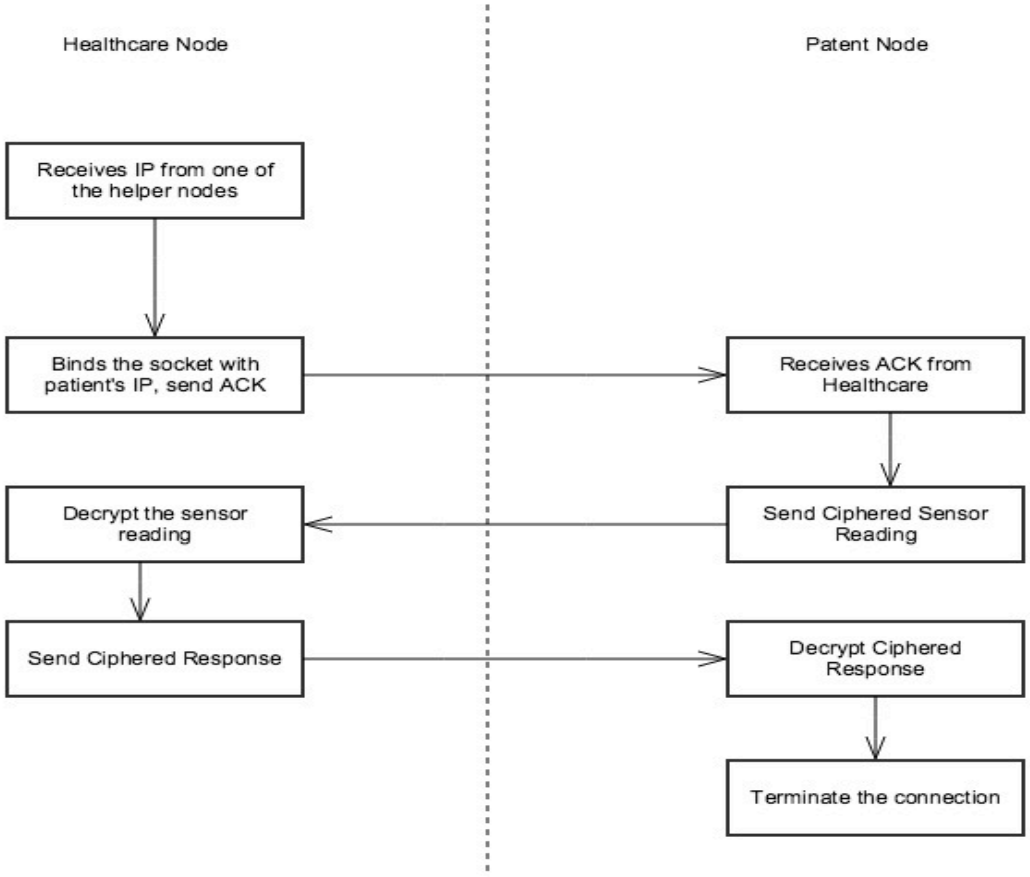

Figure 10: Secure communication Module

All the communication that takes place between healthcare and patient nodes can be displayed on each other's mobile screens.

4.2 Simulation:

4.2.1 Simulation Environment

To test our simulation design, we carried out simulations of the communication setup for the emergency response system. The system simulation program runs in three modes which simulate the three different mode types in our system. The majority of the functionality resides at the Patient node, which has to remain active till the healthcare emergency is resolved. Intermediate mode inherits a few functions from patient node such as, broadcasting and determining the near-me nodes. Healthcare mode keeps passively listening for a data packet and then comes into action of communicating directly with the patient through Internet until patient wants to terminate the connection.

Simulation requires access to two external files that stand in for real world data. The patient and intermediate modes of the system ideally require access to the Internet in order to determine how far the helper node is situated from it. This information is stored in a file that has latitude and longitude values of any node. The second file contains the public and private keys of patient and healthcare nodes. This allows us to simulate Public Key Infrastructure [22] where public keys are attached to a node's Digital Certificate. The Patient node picks a public key while encrypting the sensor reading and Healthcare node picks its corresponding private key and decrypts it. The opposite happens while the Healthcare node sends response.

Another requirement is that the Healthcare and patient node are notified about each other's port number that they are listening to, beforehand. This makes sure that the broadcasted packets do not return to the sender themselves through out the simulation process.

4.2.2 System Requirements

In order to run our system, we need Internet connectivity at all the participating nodes through out the simulation duration. The file, which contains location specifics of all the participating nodes should be accessible. Another file that acts as a Certificate Authority needs to be accessible only by the patient and Healthcare node. In order to make this file inaccessible by the helper nodes, the functionality that would access the file is simply not included in Intermediate node's design and implementation.

CHAPTER V

SIMULATION RESULTS

The System here developed has been executed taking into consideration a variable number of hops a patient's HELP packet must travel through. The System has been tested for one hop with two nodes (computers), each running the patient and healthcare programs. Split time stamps have been recorded. Times to find nearby nodes, to send requests once the Healthcare node is found and to receive responses together contribute to the turn around time of a single request. These split timings have also been recorded. We followed a similar procedure for two hops. This time three different computers were used and the locations file was updated to calculate the distance less than the parameter that was programmed into the Patient node.

For more than two hops, which now require more than three physical systems, we conducted experiments in multiple consoles on a single machine. There underlies an assumption in this case that all the intermediate helper nodes fall within the radius that has been chosen as a parameter for our Near-me System. Every intermediate node program runs taking the destination's port number as input which is different from where it has received the packet from the previous hop. Hence the packet sent by helper node in hop 2 does not reach back to the helper from hop 1 even though the distance between them is the same. In the end, our experiments encompassed upto 4 hops. Timestamps have been recorded and graph has been plotted (Figure 17) with distance against the turnaround time to determine the timeliness and efficiency of the system.

Later in this chapter, we provide simulation results for each of the above scenarios and discuss what they indicate and how they obtain an answer to the current research question.

Results at patient's node comprises the following information:

1. Text messages which could be one of 'HELP', 'ACK 0'(Acknowledgement from an Healthcare provider node), 'ACK 1'(Acknowledgement from an Intermediate node),

2. Requests – which is numeric sensor data,

3. Encrypted Request – Numeric data that is obtained after encrypting the sensor raw data,

4. Received Encrypted response – A text/ numeric data

5. Decrypted response

Results at an Intermediate node comprises the following information:

1. Text message which is typically 'HELP' message coming from either patient or one of its near-me nodes.

2. IP address of the patient – his information needs to be forwarded further in the network for a Healthcare provider to know whom it needs to bind itself to.

Results at a Healthcare Provider node comprises the following information:

1. Text message with 'HELP' message and 'IP' of the patient – which is sent either by one of the intermediate nodes or the patient itself,

2. IP address of the sender,

3. Cipher of the sensor data - sent by patient,

4. Plaintext of the sensor data,

5. Response to be sent.

5.1 Single Hop:

The experiment for single hop has a Healthcare node available within the near-me radius of the patient. The Healthcare node receives the HELP message datagram packet that is coming form patient, binds its socket with the IP address of the patient and communication is carried out. **Figure 11** and **Figure 12** show our system's performance at Patient and Intermediate nodes respectively, in the Single Hop scenario.

Figure 11: Timestamps for Single Hop at Patient Node

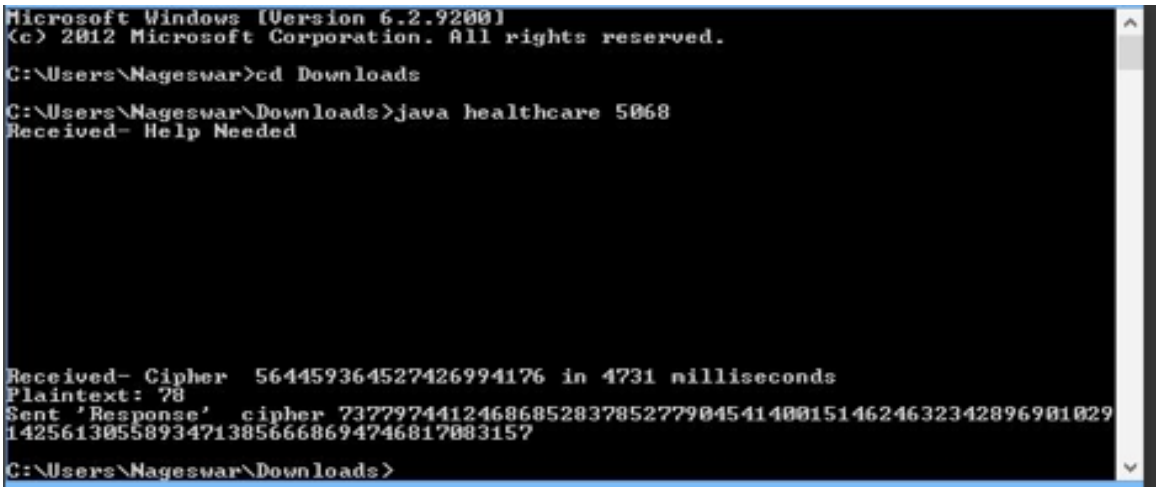

Figure 12: Timestamps for Single Hop at Healthcare Node

The Figures depict that within the radius of 50 Units, the response takes as less as 6868 milliseconds. However, this time depends on how prepared the Healthcare node is in responding to the query that the Patient node is going to send.

5.2 Two Hops:

The system's performance with one intermediate node helping connect patient node with Healthcare node is shown in **Figures 13, 14 and 15** below. In order to differentiate the ACK received by the patient node, we assign number 1 for an ACK coming from a helper node and a 0 for an ACK coming from a Healthcare node. After receiving ACK 0, the thread responsible for listening to an ACK stops and control is handed either to the user to enter the sensor reading or to an automated system that is responsible for inducing sensor data into the communication line with Healthcare node.

```
Swethas-MacBook-Pro:~ swethanandiraju$ java patient 5051 5050
Received :Ack 1 from IP /192.168.1.6 in 1799 milliseconds
Time Out
Swethas-MacBook-Pro:~ swethanandiraju$ java patient 5051 5050
Received :Ack 1 from IP /192.168.1.6 in 18151 milliseconds
Received :Ack 0 from IP /192.168.1.11 in 27339 milliseconds
Found Healthcare
Distance identified as 5.28655275183125
Enter the sensor reading
45
Plaintext: 45
Cipher in bigInteger 426427118248139353125
Sent cipher text in 45088 milliseconds
Received 56 in 45089 milliseconds
Swethas-MacBook-Pro:~ swethanandiraju$
```

Figure 13: Timestamps for Two Hops at Patient Node

Figure 14 shows packet received at the Intermediate Node is being forwarded to its near-me nodes.

Figure 14: Activity for Two Hops at Intermediate Node

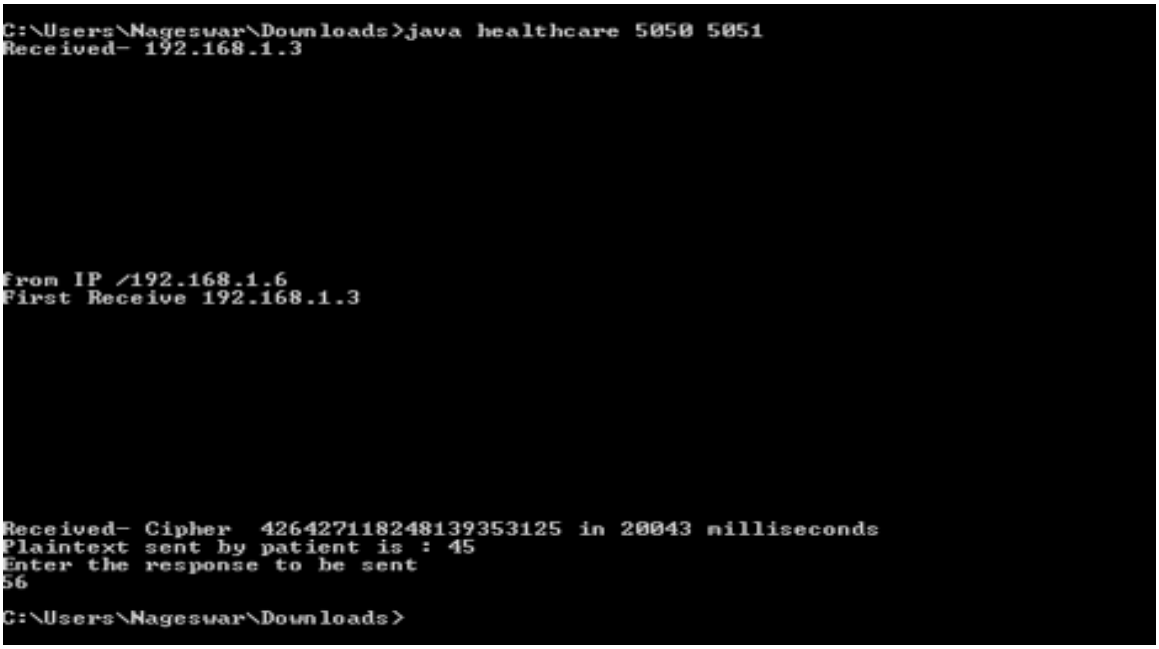

Figure 15: Timestamps for Two Hops at Healthcare Node

It takes 45009 Milliseconds in order for the patient to receive response from the nearest and authentic Healthcare official when the registered Healthcare is unavailable. Hence our system outperforms the traditional emergency response systems, which have the 30 minutes time window to take patients to their registered Healthcare providers. The identified Healthcare node could be as far as 100 Units away from patient node i.e., twice the Near-me distance.

A similar experiment with 4 hops returned 67386 milliseconds of round trip time for a single request and response between Patient and Healthcare nodes.

5.3 Isolated location:

When the Patient node has broadcast the HELP message and there are no nodes in its "Near-me" radius, an Isolated Location situation occurs. It is handled by the SocketTimeOut property of the patient node which detects if the Receive(DatagramPacket) at receiver's end has not been called even once during the timer period. The Socket timer period needs to be decided beforehand. In our system, we use time out period of 30 seconds. After the socket times out, the registered Healthcare or a 911 is dialed automatically from the user's phone.

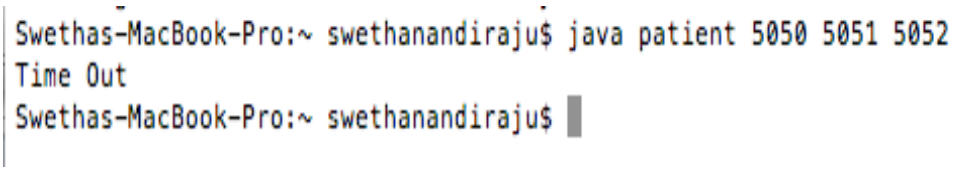

Figure 16: Activity at Patient Node in case of Isolated Location

5.4 Performance

After plotting these results on a graph with area versus the turn around time (in milliseconds), **Figure 17** is obtained which demonstrates that our system can usually determine if there is a help available around the patient within one minute.

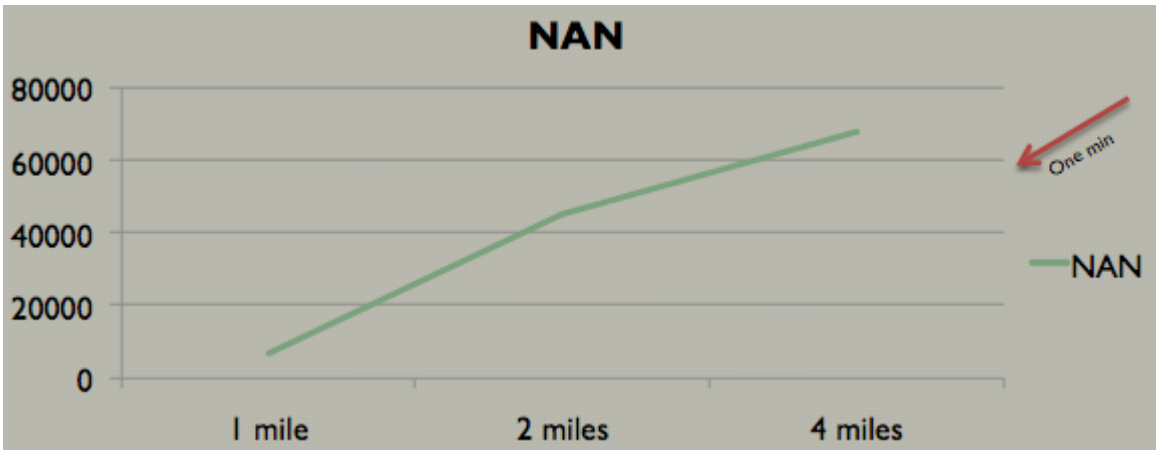

Figure 17: Performance graph

The resultant effect of the graph is essentially the discovery time that the patient node and other intermediate nodes take to identify a potential Healthcare Provider node.

CHAPTER VI

CONCLUSION

This thesis developed a system that provides secure transmission of data over a novel ad-hoc network named Near-me Area Network(NAN). A NAN is an ad-hoc network that takes into account the physical proximity of network nodes. The simulated results show that, patients can get connected to the nearest Healthcare Provider in less than two minutes; We feel that there is a great potential in this technology to make efficient use of secured adhoc wireless networks in diverse fields.

REFERENCES

[1] Prudence W. Dalrymple (June/July 2011), *Data, Information, Knowledge: The Emerging Field of Health Informatics*. The Association for Information Science and Technology (ASIS&T)

[2] The Economist(Sep 2014), *America's health-care system remains dysfunctional, but it could be made better*

[3] Peggy Bresnick Kendler, *Trend in e-Health.* The Healthcare Information and Management Systems Society

[4] Thomas R. Eng, David H. Gustafson(Jan 2008), *Wired for Health and well being. The emergence of Interactive Health Communication.* Science Panel on Interactive Communication and Health (SciPICH)

[5] West, Darrell. *How mobile devices are transforming healthcare*. Issues in technology innovation 18.1 (2012): 1-11.

[6] Xiao, Yang, and Hui Chen, eds. *Mobile telemedicine: a computing and networking perspective*. CRC Press, 2008.

[7] Vicente, Carmen Ruiz. *Location-Based Services, Applications and Privacy.*

[8] Wong, Angus KY, *The near-me area network*.IEEE internet computing 14.2 (2010): 74-77.

[9] Sato, Tadashi, and Kenichi Mase. *A scatternet operation protocol for bluetooth ad hoc networks.* Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on. Vol. 1. IEEE, 2002.

[10] Choi, Min-kyu, et al. *Wireless network security: Vulnerabilities, threats and countermeasures*. International journal of Multimedia and Ubiquitous Engineering 3.3 (2008).

[11] Kärpijoki, Vesa. *Security in ad hoc networks*. Seminar on Network Security. 2000.

[12] Protecting Patient Privacy: Strategies for regulating electronic Health records exchange NYCLU

[13] Oracle9i Security Overview *The Public Key Infrastructure Approach to Security;*

[14] Boric-Lubecke, Olga, et al. *E-healthcare: Remote monitoring, privacy, and security*. Microwave Symposium (IMS), 2014 IEEE MTT-S International. IEEE, 2014.

[15] Chui, Michael, Markus Löffler, and Roger Roberts. *The internet of things*. McKinsey Quarterly 2.2010 (2010): 1-9.

[16] Eron, Lawrence. *Telemedicine: the future of outpatient therapy?.* Clinical Infectious Diseases 51.Supplement 2 (2010): S224-S230.

[17] Istepanaian, Robert SH, and Y-T. Zhang. *Guest editorial introduction to the special section: 4G health—the long-term evolution of m-health*. Information Technology in Biomedicine, IEEE Transactions on 16.1 (2012): 1-5.

[18] United States Costumer Product Safety Commission , *Linear-Expands-Recall-of-Personal-Emergency-Reporting-System-Transmitters*

[19] EMS data from National EMS Information System (NEMSIS Data).

[20] American Telemedicine Association. *What is Telemedicine?*

[21] Medicate news - *Business of Innovation in Healthcare*

[22] Albarqi, Aysha, et al. *Public Key Infrastructure: A Survey*. Journal of Information Security 6.01 (2014): 31.

VITA

Swetha Nandiraju

Candidate for the Degree of

Master of Science

Thesis: REMOTE MEDICAL EMERGENCY RESPONSE THROUGH NEAR-ME AREA NETWORK

Major Field: Computer Science

Biographical:

Education:

Completed the requirements for the Master of Science in Computer Science at Oklahoma State University, Stillwater, Oklahoma in May, 2015.

Completed the requirements for the Bachelor of Science in Information Technology at Jawaharlal Nehru Technological University, Hyderabad, India in 2010.

Experience:

Professional Memberships: