CHALLENGES AND APPLICATION OF WIRELESS MULTIMEDIA SENSOR NETWORKS TO TELEMEDICINE

A Thesis Submitted

to the

Department of Electrical and Electronic Engineering

by

Mugumya Twarik Harouna	Student No. 123416
Rammah Mohammed	Student No. 123421
Nafiu Salele	Student No. 123436

In partial fulfillment of the requirements

for the Degree of Bachelor of Science in Technical Education

in Electrical and Electronic Engineering

Islamic University of Technology

Dhaka,Bangladesh

October 2013

CERTIFICATE OF RESEARCH

This is to certify that the thesis titled

CHALLENGES AND APPLICATION OF WIRELESS MULTIMEDIA SENSOR NETWORKS TO TELEMEDICINE

has been approved and accepted for the degree of Bachelor of science in Technical Education in Electrical and Electronic Engineering.

Supervisor:

.....

Mr. Nafiz Imtiaz Bin Hamid

Assistant Professor

Department of EEE

Signature of Head of the Department

.....

Prof. Dr. Md. Shahid Ullah

Head

Department of Electrical and Electronic Engineering,IUT

DECLARATION

This is to declare that the work presented in this thesis is the result of our own investigation carried out under the supervision of Mr. Nafiz Imtiaz Bin Hamid, in the Department Of Electrical And Electronic Engineering.
It has not already been accepted for any degree or diploma, and is also not being concurrently submitted for any other degree or diploma.

Authors:

.....	.....	.....
Mugumya Twarik Harouna	Rammah Mohammed	Nafiu Salele
Student No. 123416	Student No. 123421	Student No. 123436

Date:_____

Supervisor:

.....

Mr. Nafiz Imtiaz Bin Hamid

Assistant Professor

Department of Electrical and Electronic Engineering,IUT

ACKNOWLEDGEMENTS

All praise and thanks are due to Allah who has enabled us to accomplish this piece of work and may His peace and blessings be upon the last prophet Muhammad(SAW).

This thesis is a result of research of one year. Early in the process of completing our thesis, it became quite clear to us that a researcher cannot complete his thesis alone. Although the list of individuals we wish to thank extends beyond the limits of this format, we would like to thank the following people for their dedication and support:

First and foremost, we would like to acknowledge with gratitude the continuous support and guidance rendered to us by our supervisor Mr. Nafiz Imtiaz Bin Hamid, Assistant Professor, Department of Electrical and Electronic Engineering, IUT . Without his scholarly guidance, timely supervision, constructive criticism and valuable advices, We would not have been able to complete this thesis with such level of professionalism. We have been fortunate to enter the world of research and publications at an Undergraduate level, which will definitely be helpful in our future lives and careers. We have also benefited a lot from his professional training on how to conduct top-notch research.

We wish to take this opportunity to express our sincerest gratitude and heartiest thanks to our dear parents and family members for being such delightful people and the inspiration for our effort. Without their prayers, continued encouragement, moral and financial support, it would not have been easy for us to accomplish this work, indeed their reward is with the Almighty Allah.

Last but not the least, we would like thank all our friends, colleagues and whoever has given us encouragement in the course of our work and our write-up.

DEDICATION

We dedicate this work to our Parents for their endless love and support

Contents

List of Figures

List of Tables

LIST OF ACRONYMS

Abbreviation	**Meaning**
MEMS	Micro Electro-Mechanical Systems
CMOS	Complementary Metal Oxide Semiconductor
WMSN	Wireless Multimedia Sensor Networks
WSN	Wireless Sensor Networks
PM	Physiological Monitors
RP	Relay Points
UWB	Ultra-Wide Band
IATV	Interactive Television
MASN	Medical Ad hoc Sensor Network
DOS	Denial Of Service
MEDiSN	Medical Emergency Detection in Sensor Networks
GUI	graphical user interface
ECG	electrocardiograph
PDA	personal data assistant
SRP	secure remote password
AES	advanced encryption system
BSN	body sensor network
SK	session keys

Abstract

The increasing need for better healthcare is one of the fiercest challenges faced by both developed and developing countries. The aging population has led to shortage of specialists in the medical field, depriving remote and underprivileged areas of better healthcare. The advances in information and communication technologies offer hope of technologies that have a great potential to reduce mortality and morbidity while improving the healthcare service delivery. Telemedicine is a magnificent tool that bridges the gap between the specialists and patients, bringing specialty care to the location of the patient in life time. This thesis discusses the application wireless multimedia sensor networks (WMSNs) to telemedicine, a WMSN enabled telemedicine architecture integrated with a 4G wireless cellular network is proposed. It is followed by potential solutions for some ongoing challenges like the high bandwidth demand, security and energy consumption. Finally an energy-efficient routing algorithm is proposed.

Chapter 1

Introduction

1.1 Background

Recent Advances in wireless communications and Micro Electro-Mechanical Systems (MEMS) have motivated the development of extremely small, low-power, inexpensive devices such as Complementary Metal Oxide Semiconductor (CMOS) cameras, which possess sensing, signal processing and wireless communication capabilities. These sensors can be deployed as wirelessly interconnected devices, namely Wireless Multimedia Sensor Networks (WMSNs).

WMSNs are emerging Wireless Sensor Networks (WSNs) with the capability of retrieving multimedia data from place to place. They are rapidly gaining interest of researchers due to the great success of WSNs in solving real-world problems. WSNs were initially developed for military application but currently they are being utilized for civil purposes, a number of applications have been developed. On the other hand, WMSNs, step up to support and enable many new applications ranging for Traffic Avoidance, Enforcement, and Control Systems, Advanced Health Care Delivery, Environmental and Structural Monitoring, Industrial Process Control, and Multimedia Surveillance Sensor Networks among others

1.2 Problem Statement

Wireless Multimedia Sensor Networks have led to the emergence of new applications such Advanced health care delivery as well as challenges. The multimedia rich data transmitted results into higher resources requirements being placed on to the network. Collection, processing, and dissemination of multimedia data are processing intensive operations, that demand higher processing power, large memory, and high bandwidth, with that being said, numerous threat are being invented to create barriers to the privacy and hinder the performance of the networks, the wireless nature of the of the WMSN medium, causes the network to be very much susceptible to threats and attacks.

1.3 Objectives

The objectives of this thesis were:

1.3.1 General Objective

To propose solutions to the different challenges of WMSN and its application to Telemedicine

1.3.2 Specific Objectives

- Understand basics of Wireless Multimedia sensor networks
- Understand application of Wireless Multimedia sensor networks to Telemedicine
- Explore the different challenges of WMSN and propose solutions
- To propose an Algorithm for energy efficient consumption

1.4 Scope of the Study

The scope of our study will focus its discussion around the application of Wireless Multimedia sensor networks to telemedicine and the various challenges faced by the networks.

1.5 Significance of the study

It provides a WMSN enabled telemedicine architecture that helps in establishing a wide area WMSN based telemedicine system integrated with a 4G wireless cellular network. Also this study will help in overcoming the different challenges faced in the application of Wireless Multimedia Sensor network to telemedicine.

1.6 Organization of the Thesis

The remainder of this thesis is organized as follows.

In chapter 2, we present an overview of wireless multimedia sensor networks, we introduce the network architecture followed by applications, In chapter 3, an overview of telemedicine application is presented in details, discussing the application of wireless multimedia sensor networks to Telemedicine and a proposition an architecture for the application with distinctive features. Chapter 4 tackles the different design challenges experienced and application challenges of WMSN based Telemedicine application. Simulation of the proposed algorithm for energy efficient routing is presented in Chapter 5.

Finally, in Chapter 6, we draw the main conclusions and an outline of the future research direction.

Chapter 2

Wireless Multimedia sensor Networks

2.1 Introduction

The advances in wireless communication, networking and sensing technologies have developed and they are merging to provide new and evolving technologies for example Wireless Multimedia Sensor Networks (WMSNs). A WMSN is a network of wirelessly interconnected devices that are able to ubiquitously retrieve multimedia content such as video and audio streams, still images and scalar data from the environment.

Still images are used usually in the transmission of event triggered observations during short periods of time, while multimedia streaming requires the transmission of large amounts of real time traffic over longer periods of time. The resources needed, in general, by multimedia traffic in terms of buffering, bandwidth, battery consumption, and processing are higher than the resources required in Wireless Scalar Sensor Networks (WSSNs). Multimedia data requires sensor platforms that provide higher data rates. Moreover, WMSNs are designed for real-time applications as well as non-real time applications.

2.2 Network Architecture

A Wireless Multimedia Sensor Network can be in different architectures composed of several different devices. A recent survey on WMSN [1] shows that there are three different reference architectures for WMSNs namely:

a) single-tier flat, homogeneous sensors, distributed processing, centralized storage;

b) single-tier clustered, heterogeneous sensors, centralized processing, centralized storage;

c) multitier, heterogeneous sensors, distributed processing, distributed storage. Examples of the above WMSN architectures are shown in Figure 2.1:

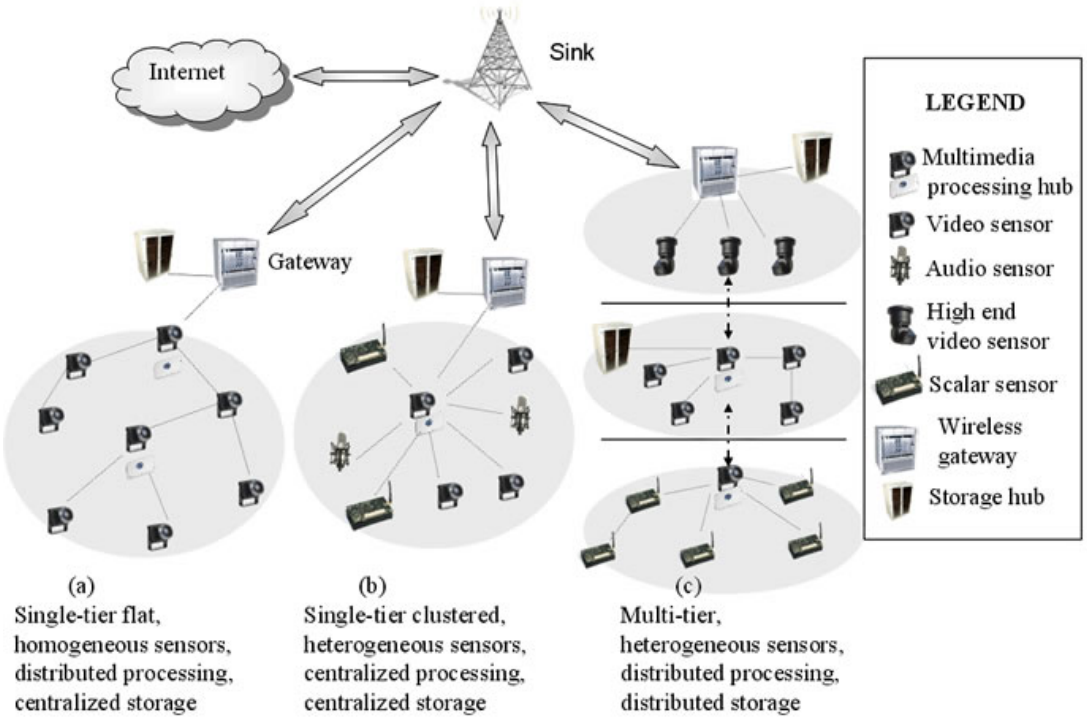

Figure 2.1: Wireless multimedia sensor network and its sub-classifications

A wireless multimedia sensor network is made of various network components,which include but not limited to video and audio sensors, scalar sensors, multimedia processing hubs, storage hubs, sink and a gateway.

- Standard Video and Audio sensors

  They are used to capture still and moving images of sensed events

- Scalar sensors

  They are used to sense scalar data and physical attributes e.g. Temperature, pressure, humidity, heart beat, location of object and report measured values to the cluster head

- Multimedia processing hubs

  Reduce both the dimensionality and the volume of data conveyed to the sink and storage hubs

- Storage hubs

  Allow data-mining & feature extraction algorithm to identify the important characteristics of the event, even before the data is sent to the end user.

- Sink

  Packaging high level user queries to network directives and returning filtered portions of the multimedia stream back to the user.

- Gateway

  Last mile connectivity by bridging the sink to the internet and is also the only IP addressable component of the WMSN

- User

  Users run applications and send queries to the network to perform monitoring tasks. Results are obtained via the returning replies.

2.3 Applications of WMSNs

Wireless Multimedia Sensor Network steps up to support and enable many new applications:

2.3.1 Multimedia Surveillance Sensor Networks

Existing surveillance systems can be improved with multimedia content using computer vision techniques. This technology enables a crime or a terrorist attack to be prevented using detection systems considering suspicious behaviors. Furthermore identifying criminals, locating missing persons and recording events like thefts, murders, violations will be possible with this technology.

2.3.2 Traffic Avoidance, Enforcement, & Control Systems.

car traffic in big cities or on highways is monitored and controlled, routing suggestions can be advised preventing congestion in the roads. Recording car accidents will result in better fault identification and by monitoring traffic violations traffic enforcement may become stronger. In addition, smart parking advice systems based on WMSNs detect available parking spaces and provide drivers with automated parking advice.

2.3.3 Advanced Health Care Delivery

Health care services can be advanced by some remote medical centers that can monitor the condition of the patients. In this system medical sensors will be carried by the patients and important parameters like body temperature, breathing activity, blood pressure and so on can be recorded. By this way early diagnosis of diseases can be done, and in an emergency situation early medical intervention may save many lives.

2.3.4 Environmental and Structural Monitoring.

Besides measuring the physical phenomena, capturing multimedia content is enabled via audio and video sensors. Forests, oceans can be monitored and researchers may interpret the observed data attracting their attention. Arrays of video sensors already are used by oceanographers to determine the evolution of

sandbars using image processing techniques. Video and imaging sensors also are used to monitor the structural health of bridges or other civil structures.

2.3.5 Industrial Process Control

Multimedia content such as imaging, temperature, or pressure, are used for time-critical, industrial, process control. In automated manufacturing processes, the integration of machine vision systems with WMSNs simplifies and adds flexibility to systems for visual inspections and automated actions.

Chapter 3

Telemedicine

3.1 Introduction

Telemedicine is a growing application of WMSN, it is neither a technology nor a separate medical specialty, but an application. The World Health Organization has adopted the description of Telemedicine as "The delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities" [2].

$$Telemedicine = Telecommunications + Technology + Medicine$$

Telemedicine is sometimes referred to as telehealth and telecare.
Telemedicine can be mainly classified into three categories:

- Store and forward telemedicine,
- remote monitoring telemedicine
- real-time (live) telemedicine [3]

In store and forward telemedicine, medical data and images are retrieved from the patient using medical sensors, and then sent through a secure connection to a medical specialist who examines the data and gives the recommendation[3]. Medical data may include EEG, ECG, EMG, EOG and ERG signals, heart beat rate, and blood pressure, and the medical images may include CT, SPECT, MRI and PET. Store and forward telemedicine is very important in many medical situations, for example in reading a pediatric EEG, this EEG is complex, due to the uniqueness of the electrical signals from the baby's brain and it requires a specialist to interpret it, who may not be available locally.

In Remote monitoring telemedicine, medical data is collected periodically and continuously from the patient and integrated automatically into the patient care record. It allows long-term care and trend analysis by monitoring vital signs of a patient remotely using various technological devices. It's primarily used for monitoring chronic diseases, thus reducing the length of hospital stay.

Live telemedicine involves video-conferencing between the patients and the specialist doctor. This is usually facilitated by a two way interactive television (IATV)[3].

3.2 Advantages of Telemedicine

- Saves lives and preserves lives
- Assures patients access to care when they need it and when time is critical for diagnosing and treating serious conditions
- Allows specialist physicians to practice more efficiently while supporting communities that don't have specialty care available locally
- Reduces the amount of travel for both physicians and patients
- Makes it possible for adults and children to benefit from the knowledge and experience of specialists no matter where they live.
- Cost effective and resource effective

3.3 Existing Architectures

There are several wireless healthcare researches and projects that have been designed to provide continuous patient monitoring in hospital and during disaster management, real time collection of medical data in-house assisted-living as well as mobile monitoring. This section gives an overview of the existing architectures of wireless medical sensor networks. These include MEDiSN, CodeBlue, MASN, AlarmNet and MobiCare.

3.3.1 MEDiSN

The Medical Emergency Detection in Sensor Networks (MEDiSN)[4] project utilizes a wireless sensor network composed of a network gateway, physiological monitors (PMs), and relay points (RPs), to monitor the health and transmit physiological data of patients. Figure 3.1 provides an illustrative overview of the MEDiSN architecture[5] and how the various components (e.g., PMs, RPs, etc.) operate. The PMs are sensor devices which collect, encrypt and sign patients' physiological data (e.g., blood oxygen level, pulse, ECG, etc.) before transmitting them to a network of relay points that eventually forwards the data to the network gateway. The RPs self organize into a routing tree that facilitates the reliable delivery of periodic data and alerts from the PM to the network gateway, and also from the network gateway to individual PMs. The data received by the network gateway is stored persistently at a backend server, where clients can use a graphical user interface (GUI) to access the data through different queries. Unlike CodeBlue in which the PMs generate and forward data, only the RPs in MEDiSN are responsible for relaying data (i.e., PMs in MEDiSN only generate data and are not involved with data forwarding). As a result, the RPs can use hop-by-hop retransmissions to assure the reliable delivery of bidirectional data traffic that is prone to packet collision and corruption. The designations of RPs as the sole nodes with forwarding capabilities allow PMs to duty cycle their radios and reduce their energy consumption. On the other hand, RPs cannot duty cycle because they are

actively forwarding packets. However, due to the static nature of the RPs, they can utilize the regular power supply from the hospital or use batteries in scenarios with no infrastructure. Another feature that MEDiSN offers is an over-the-air management interface that remotely controls individual PMs using downstream messaging.

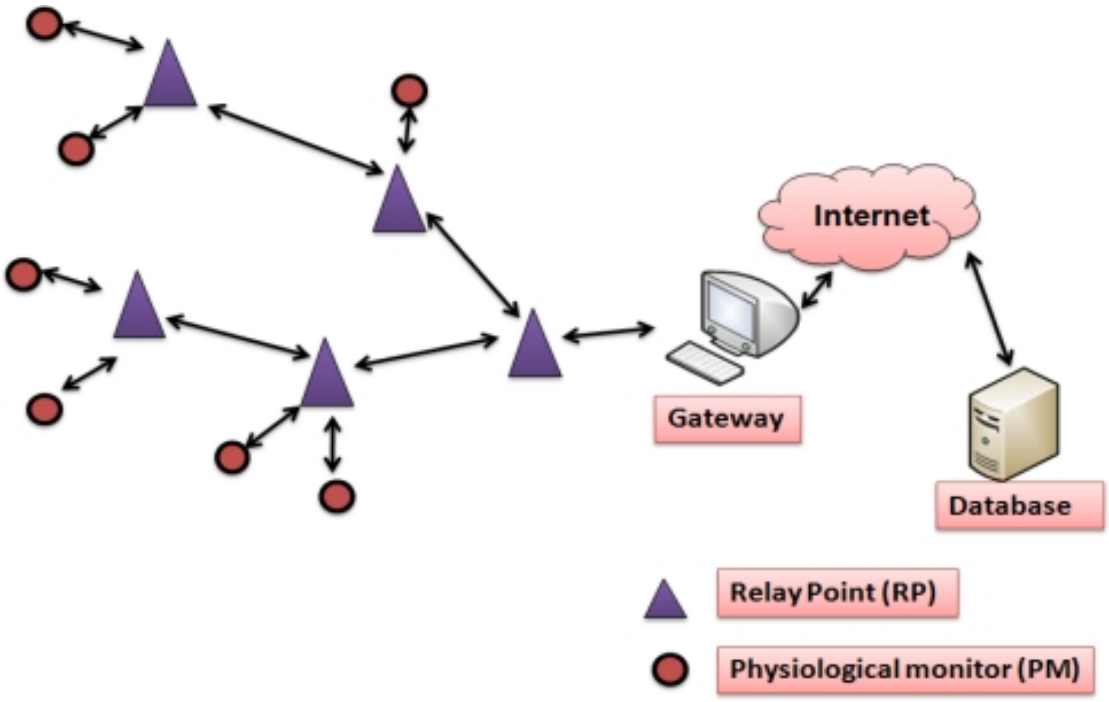

Figure 3.1: MEDiSN architecture

3.3.2 CodeBlue

CodeBlue[6] is a prototype health care wireless sensor network that defines an architecture for hardware and a framework for software. The hardware architecture design allows for the integration of a pulse oximeter, electrocardiograph (ECG), and motion analysis sensor board onto the MicaZ and Telos motes. The software framework provides protocols for device discovery, a publish and subscribe routing layer, and a simple query interface that allows caregivers to request data from groups of patients. Figure 3.2 provides an illustration of the CodeBlue architecture[5] and how it operates.

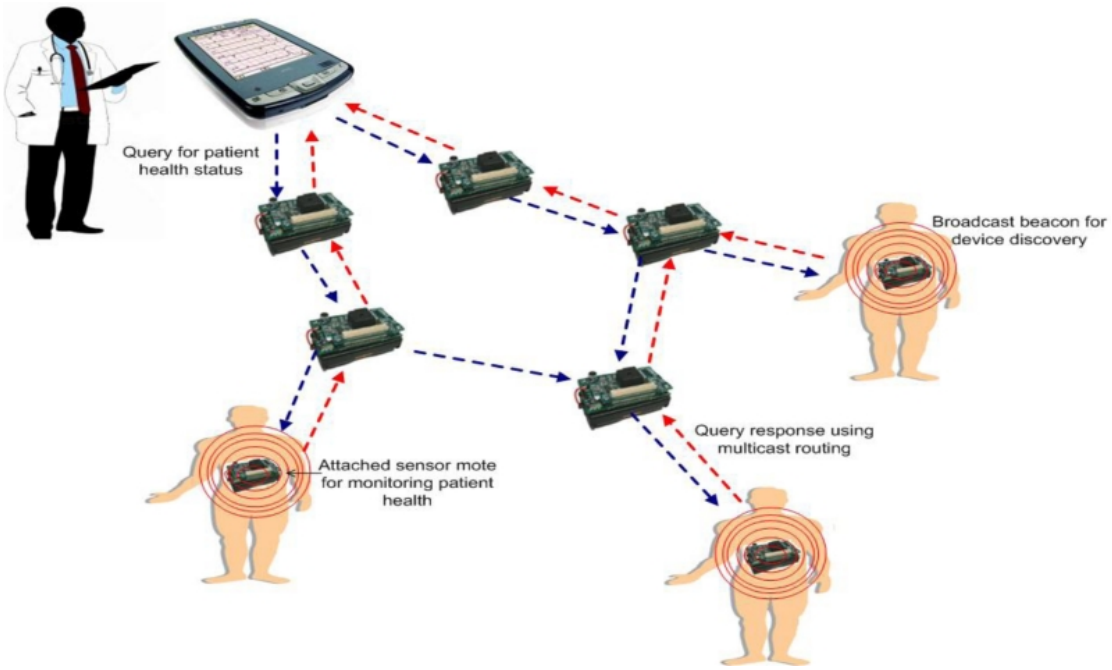

Figure 3.2: CodeBlue architecture

In Figure 3.2, each patient is equipped with a sensor mote that is used to monitor health status. A simple device discovery protocol is employed so that the motes in the network can discover each other. Specifically, each node periodically publishes its node ID and the sensor types it supports to a specific broadcast channel using a broadcast beacon. End-user devices, such as personal data assistant (PDA) devices operated by medical professionals (e.g., doctors or nurses), issue network wide queries to request information of patients that are monitored by a group of sensor motes that possess specific biomedical sensing capabilities. In order to facilitate a query and response communication process, the TinyADMR multicast routing protocol is used to establish multicast routes between the data publishing sensors and the end-user devices that subscribe interest to that data. The main purpose of TinyADMR is to deliver queries and responses under the effect of node mobility, multiple simultaneous paths, and an error-prone communication channel. For the querying mechanism, an interface is designed to allow a receiving device to request data from specific biomedical sensors based on their physical node address, sensor type, and whether or not it meets the requirements

of a specified filter. CodeBlue is also equipped with a RF-based localization system that is used to track the location of patients and caregivers, a capability that is especially valuable in large hospital settings.

3.3.3 MASN

The robust Medical Ad hoc Sensor Network (MASN) is a practical hardware and software platform designed to perform real-time collection of health care data. MASN adopts a reliable cluster-based communication scheme as its routing protocol for transmitting data[7]. The protocol groups wireless sensor nodes in clusters to detect signals for the purpose of prolonging the lifetime of MASN, load balancing, and scalability. The clustering scheme reliably relays collected ECG data to the ECG server (sink) in the form of aggregated packets. As a result, it is able to provide fast and accurate event detection and reliability control capabilities to the area where the event is occurring because the overhead, latency, and packet loss are reduced. Figure 3.3 provides an overview of the MASN architecture and the operation of the different components. As previously mentioned, groups of patients equipped with ECG sensors are organized into clusters. In these clusters, a clusterhead is elected and used as an aggregation point to relay data to the ECG server. After the data is collected, wavelet-based ECG feature extraction and classification techniques are applied to the patient data and characteristic points of interest are extracted. The main benefit of the ECG data mining mechanism is that it provides meaningful information for the diagnosis of possible cardiovascular diseases and also automates the extended recordings of ECG signals, instead of using human processing that is very time consuming and may lead to human errors. To secure the wireless transmission of vital patient data, MASN also employs a low overhead and low complexity encryption and decryption security scheme. The security scheme periodically issues session keys (SK) to cluster heads for secure transmission of data between clusters. Therefore, the security scheme must secure against possible gateway attacks (SKs are issued by the gateway), SK attacks

among cluster heads, patient ECG data corruption, and man-in-the-middle attacks. The security scheme successfully defends against these attacks, but does so by adding up to 20% overhead to data packet transmissions. MASN also features a patient location tracking system that is an enhanced version of the CodeBlue MoteTrack algorithm. Using only radio signal information, MoteTrack can determine the location of a patient with an accuracy of 1 meter. The enhanced version of MoteTrack does not use GPS. Rather, the RF chip on each MASN sensor node broadcasts beacon messages at a range of different transmission power levels that the MoteTrack algorithm uses to perform location estimation of patients' positions.

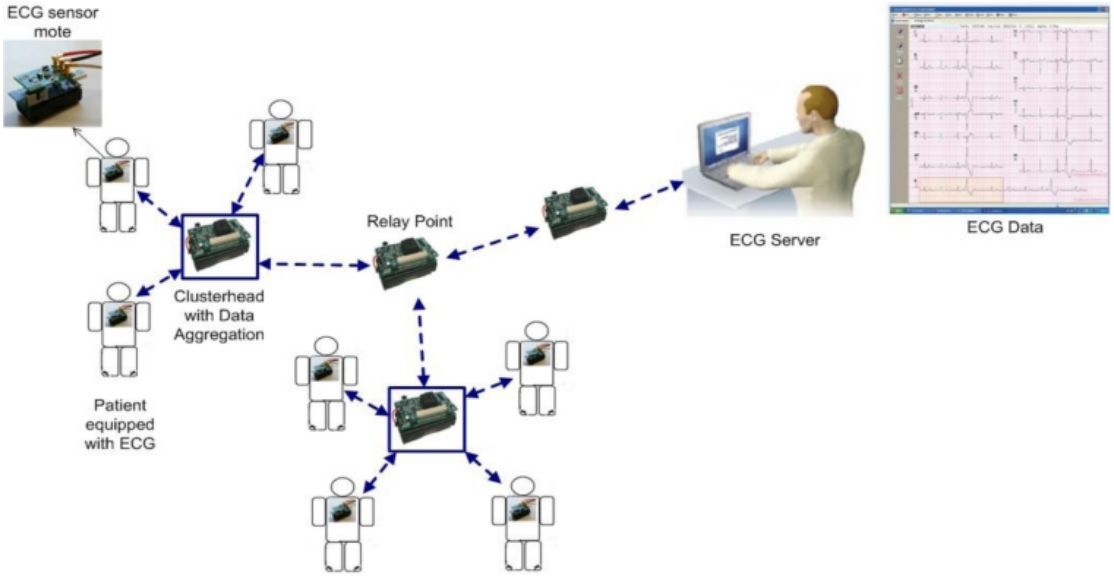

Figure 3.3: MASN architecture

3.3.4 AlarmNet

A heterogeneous network architecture named Alarm-Net was designed at the University of Virginia. The research is specifically designed for patient health monitoring in the assisted-living and home environment. Alarm-net consists of body sensor networks and environmental sensor networks. Three network tiers are applied to the proposed assisted-living and home environment, as shown in Figure 3.4. In the first tier a resident wears body sensor devices such as ECG, accelerom-

eter, SpO_2 (i.e., a MicaZ boards) which sense individual physiological data; and in the second tier environmental sensors such as temperature, dust, motion, light (i.e., MicaZ boards) are deployed in the living space to sense the environmental conditions. In the third tier an internet protocol (IP)-based network is used which is comprised of Stargate gateways called AlarmGate. The idea of Alarm-net is very simple, body sensors broadcast individual physiological data using single-hop to the nearest stationary sensor (i.e., second tier). Thereafter, the stationary emplaced sensor nodes forward the body data using multi- hop communication (i.e., shortest-path-first routing protocol) to the AlramGate. The AlarmGate is a gateway between the wireless sensor and IP networks, and is also connected to a back-end server.

Any real-time data queries about physiological or environmental data are originated by the user that contains the source address, ID, and sensor type. For a single-shot query, the sensors sample the requested data and respond a single report to the query originator, and hence complete the query. In addition, authors have developed a circadian activity rhythms program to aid context- aware power management and privacy policies.

Further Alarm-Net facilitates network and data security for physiological, environmental, behavioral parameters about the residents. Only authenticated users can access the Alarm-Net and can query the sensor networks. The IP-network is secured by secure remote password (SRP) protocol for user authentication. The wireless sensor networks are enabled with Link-layer security suites. Sensors (i.e., MicaZ and Telos) use built-in cryptosystems, i.e., an advanced encryption system (AES) for cryptographic operations. AES security modes supported are: none, CBC-MAC authentication-only, CTR mode encryption-only, and CMM combines with authentication and encryption. The major drawback of the built-in cryptosystem is that it does not offer AES-based decryption, by which means the encrypted data cannot be accessed by an intermediary node during communication, if needed. Further, hardware based built-in cryptosystem makes the application

highly platform dependent.

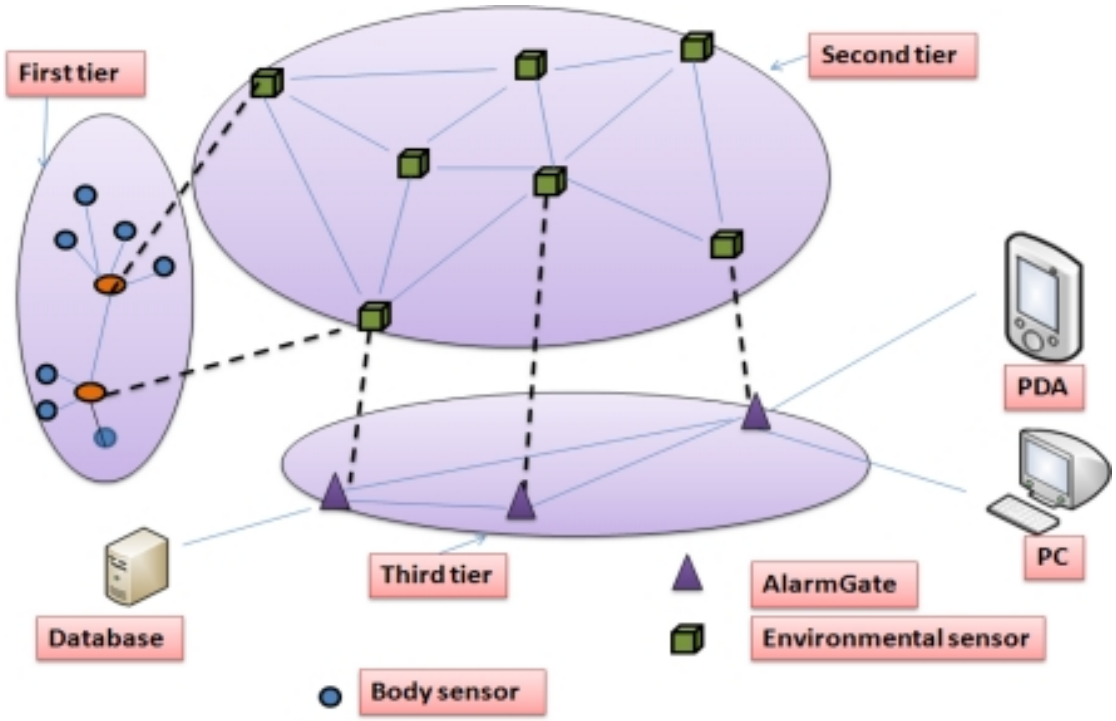

Figure 3.4: AlarmNet architecture

3.3.5 MobiCare

In 2006, Chakravorty designed a mobile healthcare project called MobiCare[9]. MobiCare provides a wide-area mobile patient monitoring system that facilitates continuous and timely monitoring of patients physiological status. It potentially improves the quality-of-patient care and saving many lives. As shown in the Figure 3.5, the proposed system comprises of body sensor network (BSN) having wearable sensors (e.g., ECG, SpO2, and blood oxygen); a BSN manager called "MobiCare client that is an IBM wristwatch"; and a back-end infrastructure (i.e., MobiCare server). The medical sensors timely sense the patient's body data and broadcast it to the MobiCare client. The MobiCare client aggregates the body data and sends them using GPRS/UMTS or CDMA cellular link to the MobiCare server. In this research, MobiCare client makes use of application layer standard HTTP POST

protocol for sending BSN data to the server. The MobiCare server supports to the medical staffs for offline physiological analysis, and for patient care.

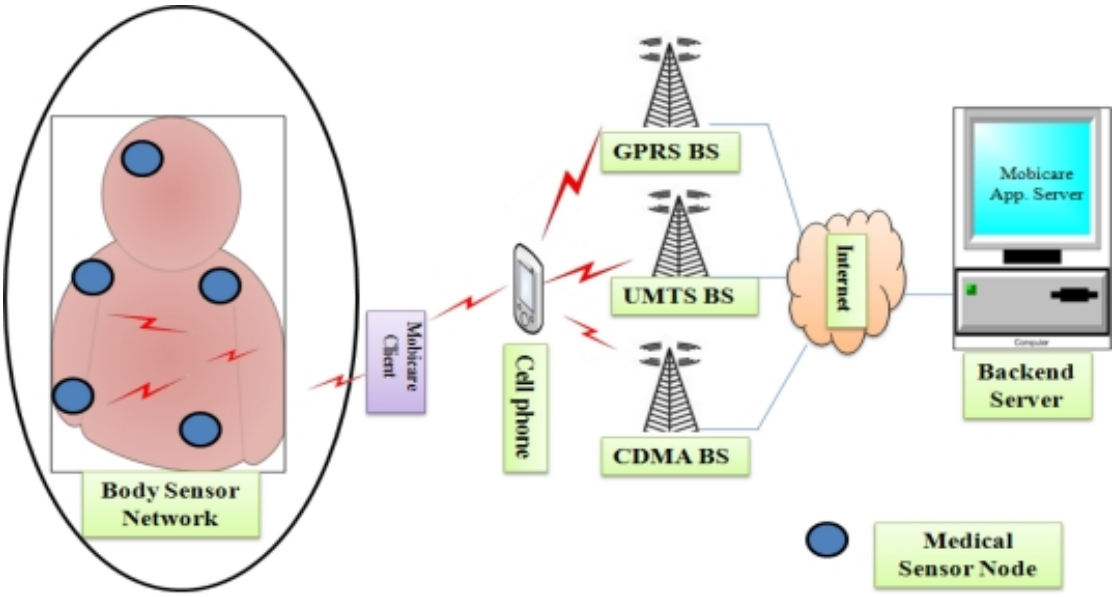

Figure 3.5: MobiCare architecture

3.3.6 Comparison of existing telemedicine architectures

The following tables give a comparison of the various exiting architectures of wireless medical sensor networks discussed above. The comparison is based on six parameters; namely Operational Environment Supported Application, Reliability Mechanism, Scheme for Energy Efficiency, Routing Methodology, Techniques for Mobility Support.

MEDiSN	**CodeBlue**	**MASN**	**AlarmNet**	**MobiCare**
constitutes a Dedicated Wireless Sensor Network in Hospital Deployment with RPs and PMs	The prototype was validated on 30 Node Ad Hoc Sensor Network Test-Bed, demonstrating its scalability and robustness	Medical Ad Hoc Sensor Network deployed in Nursing homes	Scalable and heterogeneous architecture integrating ESs and PMs in assisted-living and home environment	A remote wireless patient monitoring consisting of BSN, MobiClient and MobiCare Server.

Table 3.1: Architectural comparison based on Operational Environment

MEDiSN	**CodeBlue**	**MASN**	**AlarmNet**	**MobiCare**
Applied in Medical Emergency Detection for patient monitoring in hospitals and disaster scenes.	It was applied in Medical Care and Disaster management	Real-time remote cardiac patient monitoring and collection of ECG Data	Patient health monitoring in the assisted-living and home environment	Wide-Area Mobile patient monitoring

Table 3.2: Architectural comparison based on Supported Application

MEDiSN	**CodeBlue**	**MASN**	**AlarmNet**	**MobiCare**
Message oriented Middleware (MOM), which was JMS-based has been selected to run on the Gateway. While the back-end server is responsible for storing, routing, and Retransmitting messages.	CodeBlue was designed to provide for reliable transmission of critical data through content-specific prioritization and dynamic scaling of transmission power.	Enhanced cluster-based, energy-aware data transmission has been proposed, where the ECG data are reliably relayed to the sink in the form of aggregated data packets.	Three-Tier Architecture with Mobile Body network, Emplaced Sensor Network and IP Network	MobiCare designed a secure reliable dynamic code update functionality that is implemented as part of each MobiCare client and sensor device

Table 3.3: Architectural comparison based on Reliability Mechanism

MEDiSN	CodeBlue	MASN	AlarmNet	MobiCare
The division of functionality between acquiring and relaying data enables PMs to achieve low energy consumption, through duty cycling their radios	CodeBlue uses Berkeley Mica2 sensor nodes which include a low-power, single-chip radio with batteries that will last for up to a week of continuous running. Employing duty-cycling, the device can drop to a very low power sleep state of 10μA	MASN Proposed an Energy-aware cluster formation scheme using event triggered energy level determination of sensor nodes	Context-aware and Open Power Management Scheme (COPM) module was designed, where some nodes are plugged into the wall and others operate on batteries	Propose the use of low-power, low-frequency wireless sensor developed at Harvard University using (using the Berkeley MICA2 mote)

Table 3.4: Architectural comparison based on Scheme for Energy Efficiency

Parameter	MEDiSN	CodeBlue	MASN	AlarmNet	MobiCare
Routing Methodology	Many-to-one and one-to-one communication between PMs and RPs. Collection Tree Protocol (CTP) was also used by the RPs	Based on the Adaptive Demand-Driven Multicast Routing (ADMR) protocol in which sensors publish relevant data to a specific channel and end-user devices subscribe to channels of interest	Used Intra-Cluster and Inter-Cluster Data Relay routing scheme	Single hope at the first Tier, multi-hop at the second tier (i.e., Shortest-path-first routing protocol)	Application layer standard HTTP POST protocol
Techniques for Mobility Support	During mobility PM sends its data to the stationed RP that shares the best link with it	A tracking system named MoteTrack which operates in an entirely decentralized, robust fashion, provide good location accuracy	MASN cannot achieve real-time data collection (delay $>$ 10 s) if the users move quickly such as at 30 mph	Emplaced Sensors (ES) maintain connections with mobile body as they move through the living space	Used always-on wide-area cellular wireless communication interface

Table 3.5: Architectural comparison based on Routing Methodology and Techniques for Mobility Support

3.4 Proposed Architecture

The structure of our proposed architecture shown in Figure 3.6 is created by integrating a WMSN with a 4G cellular network. The WMSN provides a platform for acquiring medical data from the patients and sends it through a 4G based wireless cellular network to the specialist for analysis and diagnosis. The architecture is made up of cameras, speakers, interactive television, different biomedical sensors (handheld and wearable devices), local storage server and a gateway. Biomedical sensors include digital stethoscope for measuring the heartbeat, ophthalmoscope and others. It provides real-time consultation and continuous monitoring of the patients physiological data regardless of location provided the location has a 4G wireless network coverage needed for the multimedia streaming for transmitting the required data to the specialist at a distant location. The 4G cellular network provides the long range telemedicine facilities between the specialist and patient's healthcare center, thus providing global services.

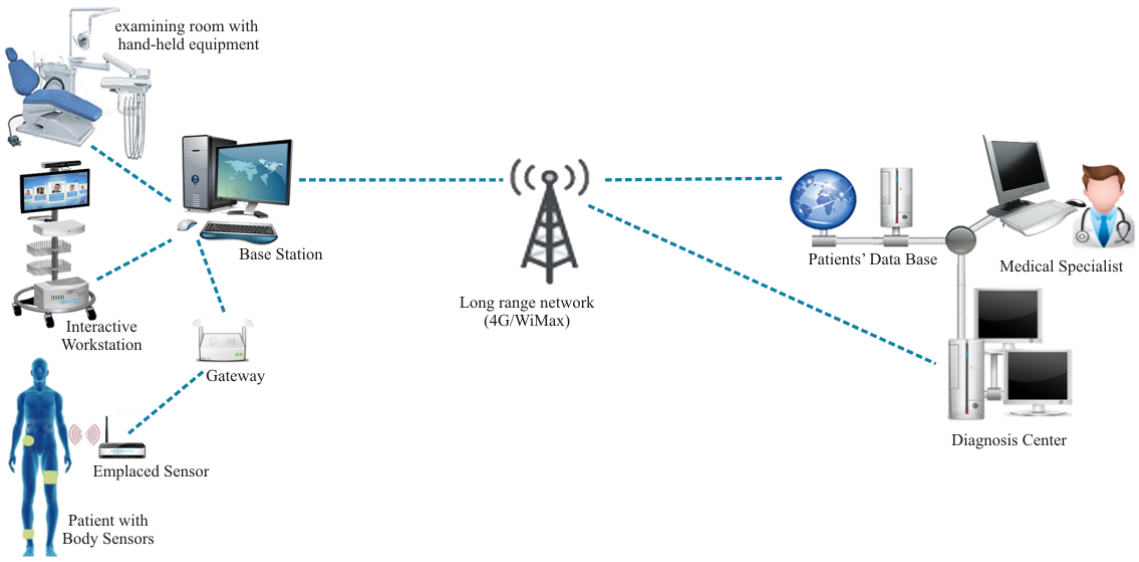

Figure 3.6: Architecture of the proposed network

3.4.1 How it works

The proposed architecture supports heterogeneous networking. Using UWB network, it forms an island of sensors (WMSN), and these different sensors collect the required data from the patient depending on the telemedicine type (i.e. live, store and forward, monitoring telemedicine). The medical data is processed (compressed, encrypted, etc) and then it is sent to the gateway (the only IP addressable component of the WMSN) and it's also stored locally in the storage server. The gateway provides the connectivity and integration with the WiMAX network. The WiMAX network transmits the data over a long communication range to the specialist in another area. The data is received at the specialist side, the data is checked if it's valid and then after it can be processed (decrypted, decompressed), Then the data can be analyzed and then used for diagnosis and treatment.

3.4.2 Distinctive Features

The architecture offers an automatic process for accomplishing tasks.

- The first feature is the monitoring; vital signs of a patient with a chronic disease are collected periodically, processed and saved into the patient's medical record locally. For some special cases, for example a stroke patient, a camera is also used in monitoring. If the readings recorded deviates from the safety margin, an alert will be sent to the doctor. A biometric scheme will also be used to identify the patient and authentic data.
- The second feature of the system is the live telemedicine; Face to face consultation is carried out using the interactive workstation, the physiological data of the patient is measured on real-time from the patient for analysis using wireless hand held devices like digital otoscope, digital stethoscopes, ophthalmoscope, laryngoscope, nasolaryngoscope then the appropriate treatment can be recommended by the specialist.

Chapter 4

Challenges

There are several challenges faced by WMSN applications, they include: QoS requirements, scalable and flexible architectures and protocols to support heterogeneous applications, localized processing and data fusion, energy efficiency design, reliability and fault tolerance, multimedia coverage, high bandwidth demand, and more [15].

4.1 High Bandwidth

The real-time video conferencing in the live telemedicine makes telemedicine application a high bandwidth hungry application of WMSN. High bandwidth requirement is a big challenge to the network. This section discusses the most promising solution for bandwidth hungry WMSN enabled telemedicine applications.

4.1.1 Ultra-wide band

Ultra-wide band (UWB) [1] is a recently approved low power and high speed, short-range wireless communication standard based on IEEE 802.15.3, oriented to high-

[1]The FCC defines UWB as a signal with either a fractional bandwidth of 20% of the center frequency or 500 MHz (when the center frequency is above 6 GHz). The FCC calculates the fractional bandwidth as $2(f_H - f_L)/(f_H + f_L)$ where f_H represents the upper frequency of the -10 dB emission limit and f_L represents the lower frequency limit of the -10 dB emission limit[11]

bandwidth multimedia links [10]. UWB signals have been used for several decades in the radar community. Since 2002, UWB inspired a renewed flourish of research and development efforts in both academy and industry [12], this is due to its characteristics that make it a viable candidate for wireless communications in dense multi-path environments and high bandwidth applications.
There exist two main variants of UWB, namely MultiCarrier UWB (MC-UWB) and Time- Hopping Impulse Radio UWB (TH-IR-UWB).

MultiCarrier UWB (MC-UWB), is based on Orthogonal Frequency Division Multiplexing (OFDM) and uses multiple simultaneous carriers. MC-UWB is particularly well-suited for avoiding interference because its carrier frequencies can be precisely chosen to avoid narrowband interference to or from narrowband systems. However, implementing a MC-UWB front-end power amplifier can be challenging due to the continuous variations in power over a very wide bandwidth. Moreover, when OFDM is used, high-speed FFT processing is necessary, which requires significant processing power and leads to complex transceivers.

A different approach, known as Time-Hopping Impulse Radio UWB (TH-IR-UWB)is based on sending very short duration pulses (in the order of hundreds of picoseconds) to convey information. Time is divided into frames, each of which is composed of several chips of very short duration. Each sender transmits one pulse in a chip per frame only, and multiuser access is provided by pseudo-random time hopping sequences (THS) that determine in which chip each user should transmit. TH-IR-UWB signals require fast switching times for the transmitter and receiver and highly precise synchronization. Transient properties become important in the design of the radio and antenna. The high instantaneous power during the brief interval of the pulse helps to overcome interference to UWB systems, but increases the possibility of interference from UWB to narrowband systems. The RF front-end of a TH-IR-UWB system may resemble a digital circuit, thus circumventing many of the problems associated with mixed-signal integrated circuits. Simple TH-IR-UWB systems can be very inexpensive to construct.

Although no sound analytical or experimental comparison between the two technologies is available to our knowledge, we believe that TH-IR-UWB is particularly appealing for WMSNs for the following reasons:

- It enables high data rate, very low power wireless communications, on simple-design, low-cost radios (carrierless, baseband communications)
- Its fine delay resolution properties are appropriate for wireless communications in dense multipath environment, by exploiting more resolvable paths
- Provides large processing gain in presence of interference
- Provides flexibility, as data rate can be traded for power spectral density and multipath performance
- It naturally allows for integrated MAC/PHY solutions;
- The large instantaneous bandwidth enables fine time resolution for accurate position estimation and for network time distribution (synchronization);

Telemedicine application involves real-time video conferencing between the patient and the specialist to allow proper diagnosis, the video conferencing requires a high bandwidth for multimedia streaming, and this demand can be met by UWB technology. Among the features of UWB that make it viable for telemedicine application is its low electromagnetic radiation due to the low radio power pulse less than -41dB in indoor environment which has proved to be harmless to human body, even in the short distance and also low influence on the environment [13], makes it suitable for health care applications. At the same time UWB can coexist with other wireless technologies due to its low power spectral density which prevents interference other wireless services. A Comparison between UWB and Zigbee, another promising technology for wireless sensor network applications is presented in the Table 4.1.

Parameter	**UWB**	**Zigbee**
IEEE Specification	802.15.3	802.15.4
Typical Range (Meters)	10	10
Power Consumption	Very little	Low
Spectrum (GHz)	3.1 - 10.6	2.4
Bandwidth	High	Low
Data rate	110-480 Mbps	20 - 240 Kbps
Channel bandwidth	500MHz	0.3MHz-2MHz
Energy efficiency	Very High	Low
Data protection	32-bit cyclic redundancy check	16-bit cyclic redundancy check
Typical Applications	Industrial control and monitoring, sensor networks, etc.	Streaming video, home entertainment applications

Table 4.1: Comparison of UWB and Zigbee technology

As seen in Table 4.1, the data rate of UWB is 2000 times higher than that of Zigbee. To maintain acceptable QoS, Zigbee cannot support many devices due to the low data rate, for example in [14], 24Kbps was taken as the required data rate for ECG monitoring application, but Zigbee can at best provide 240Kbps, implying that a maximum of 10 devices could be connected, also, at least 640Kbps is required to allow high quality diagnostic video stream (MPEG-4 format) and a minimum 768 kbps for Normal diagnostic video(MPEG-2 format)[14], these data rates cannot be provided by Zigbee devices, UWB can support many devices using the "peer to peer" mechanism [15] while utilizing the available data rates. This makes UWB a viable solution for high bandwidth demand in live telemedicine application.

4.2 Security Threats

The emergence of new applications such health care delivery which are time critical and at times involve real time transmission is likely to be hindered by threats which include denial of service that consume the required bandwidth, denying either the patient or specialist from accessing the other in time critical situations, this calls for devising of means to prevent this situation before it may put the system to halt. There are a number of vulnerabilities in WMSN, and they are due to a number of reasons but not limited to

1) wireless channel, which make the network susceptible to eavesdropping, unauthorized access, spoofing, replay and denial-of-service (DoS) attacks. [22],

2) Most current standard security protocols were designed for two-party settings and do not scale to a large number of participants,

3) conventional security solutions do not fit into sensor network system.

With the emergence of new applications for WMSNs, these networks are suffering from new threats; such threats aim at gaining unauthorized access to data, denial of service, denial of sleep, or shut down of entire network. Recent attacks made on networks by these threats have led to huge financial crisis and loss of vital data. This section discusses the vulnerabilities and potential attacks on WMSNs. The major concern is put on denial of service attacks, how they are done, how to prevent them at the different layers of the network.

4.2.1 Denial Of Service Attacks

Denial-of-service (DoS) is an event that diminishes or eliminates a network's capacity to perform its expected function [21], through hardware failures, software bugs, resource exhaustion, malicious broadcasting of high energy signals, environmental conditions, or any complicated interaction between these factors. As the name states denial of service is a network threat manifested in many ways but whose ultimate objective is to deny or degrade a user's ability to legitimately access network or services [17].With Expansion of WMSN applications to accommodate

applications like Medical monitoring highlights the need for better security to ensure privacy of the data. However new threats are being created at a higher rate. The Denial of service attack in WMSN is similar to that of the attack against traditional sensor, but it becomes severe with presence of multimedia data, thus calling for new techniques of mitigation. DoS attacks can be grouped into three scenarios; those attack scenario that target energy resources, those that targets Storage and Processing Resources and those target, targets bandwidth. These target points are some of the vital constraint put by the multimedia data on the network [18]. Denial of service attack happens in a number of ways, but the general concept behind it the bombardment of a sensor node with high traffic useless request and commands and data, to deny it from being used for the for the transmission to the next node. DoS attacks can occur in one of the following ways:

- Consumption of scarce, limited, or non-renewable resources
- Destruction or alteration of configuration information
- Physical destruction or alteration of network resources

Attacks at the various layers

Sensor networks are usually divided into layers, and this layered architecture makes WMSNs vulnerable to DoS attacks as DoS attacks may occur in any layer of a sensor network.

- Physical layer
- Link/MAC layer
- Network layer
- Transport layer
- Application layer

We Analyze each layer for attacks and potential defenses A number of techniques are used for DOS at the different network layers and they are discussed in section.

This section discusses the existing Denial of service attacks at the application, transport, network, link, and physical layers of the communication stack, respectively, with the corresponding of countermeasures to reduce the risk of DOS at the various network layers.

4.2.2 Physical Layer Attacks

Jamming attack Jamming is a type of attack which interferes with the radio frequencies that networks nodes are using.

Defense

- Frequency hopping: is a method of transmitting signals by rapidly switching a carrier among many frequency channels using a pseudo random sequence known to both transmitter and receiver.
- Code spreading: Is another jamming attack defence technique and most common in mobile networks. However, it requires greater design complexity and energy restricting in its use in WMSNs.

Tampering: Is the Physical attack on the node itself.

Defense Tamper-proof packaging; It obstructs attacks and could prevent wear and tear due to environmental factors. There by increasing the overall life of the node assuming sufficient power is available.

4.2.3 Link Layer Attacks

Collision: A collision occurs when two nodes attempt to transmit on the same frequency simultaneously

Defense: use of error correcting codes; However, most codes work best with low levels of collisions such as those caused by probabilistic errors. While it is possible to detect these malicious collisions, no complete defence against them are known.

Exhaustion: Exhaustion of network resources by inducing repeated retransmission attempts.

Defense:

- To apply rate limits to the MAC admission control such that the network can ignore excessive requests preventing the energy drain caused by repeated transmissions
- To use time-division multiplexing where each node is allocated in a time slot in which it can transmit. This eliminates the need of arbitration for each frame and can solve the indefinite postonement problem in a back-off algorithm. However, it is susceptible to collisions.

Unfairness: Unfairness is considered a weeak form of a DOS attack and can be performed by attacker attempt to degrade the network performance instead of completely preventing access to a service.
Defense: use of small frames lessens the effect of such attacks by reducing the amount of time an attacker can capture the communication channel. However, this technique often reduces efficiency and is suceptible to further unfairness such as an attacker trying to retransmit quickly instead of radom delaying.
Interrogation This makes use of the interaction that takes place between two nodes prior to data transmission.
Defense A node can limit itself in accepting connections from same identity or use anti replay protection and strong link-layer authentication.

4.2.4 Network Layer Attacks

Spoofed, altered or replayed routing information The straightest attack against a routing protocol in any network is to target the routing information itself as it is exchanged between nodes.
Defense to append a MAC (Message Authentication Code) after the message. By adding a MAC to the message, the receivers can verify whether the messages have been spoofed or altered.
Selective forwarding: A specific form of this attack is the black hole attack

in which a node drops all messages it receives as if the node doesn't exist at all. An attacker may perform another form of attack by selectively forwarding only certain messages and simply dropping others which is denoted by grey holes.

Defense

- Using multiple paths to send data
- To detect the malicious node or assume it has failed and seek an alternative route
- To use implicit acknowledgments, which ensure that packets are forwarded as they were sent

Sinkhole an attacker makes a compromised node look more attractive to nearby nodes by forging routing information. The end effect is that surrounding nodes will choose the compromised node as the next node to route their data through.

Defense Using Geo-routing protocols, these routing protocol groups are resistant to sinkhole attacks, because the topology is built using only localized information, and traffic is naturally routed based on the physical location of the sink node, which makes it difficult to lure it elsewhere to create a sinkhole.

Sybil A single node presents a variety of identities to all other nodes in the WMSN. This may mislead other nodes, and hence routes believed to be disjoint with respect to node can have the same adversary node.

Defense Using a unique shared symmetric key for each node with the base station

Wormholes An adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. This is usually done with the coordination of two adversary nodes, where the nodes try to understate their distance from each other, by broadcasting packets along an out-of-bound channel available only to the attacker.

Defense the traffic is routed to the base station along a path, which is always geographically shortest or use very tight time synchronization among the nodes, which is infeasible in practical environments.

Hello flood attacks This attack exploits Hello packets that are used in many

protocols to declare nodes to their neighbors. A node receiving such packets may believe that it is in radio range of the sender.

Defense Authentication is the key solution to such attacks. Such attacks can easily be avoided by verifying bi-directionality of a link before taking action based on the information received over that link

Acknowledgement spoofing Routing algorithms used in sensor networks sometimes require acknowledgements to be used. An attacking node can spoof the acknowledgements of overheard packets destined for neighboring nodes in order to afford false information to those neighboring nodes.

Defense Authentication via encryption of all sent packets and also packet headers.

4.2.5 Transport Layer Attacks

Flooding: An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. A very common form of DoS attacks involves sending a large number of common packets aimed at a single destination.

Defense: To require that each connecting client demonstrate its commitment to the connection via solving of a puzzle. A connecting client will not needlessly waste its resources creating unnecessary connections.

De-synchronization De-synchronization refers to the disruption of an existing connection. An attacker may, for example, repeatedly spoof messages to an end host causing that host to request the retransmission of missed frames.

Defense Packet authentication

4.2.6 Application Layer Attacks

Overwhelm attack An attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

Defense: Carefully tuning sensors so that only the specifically desired stimulus,

such as vehicular movement, as opposed to any movement, triggers them.

Path-based DOS attack It involves injecting spurious or replayed packets into the network at leaf nodes. This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station.

Defense Combining packet authentication and anti replay protection.

Deluge (reprogram) attack Network-programming system lets you remotely reprogram nodes in deployed networks. If the reprogramming process isnŠt secure, an intruder can hijack this process and take control of large portions of a network.

Defense use of authentication streams to secure the reprogramming process.

LAYER	**THREAT**	**DEFENCE**
Physical	Jamming	Frequency hopping
		Code Spreading
	Tampering	Tamper- proof Packaging
MAC / Link	Collisions	Error correcting codes
	Exhaustion	Apply Rate limits to the MAC admission control
		Time-division multiplexing
	Unfairness	Use of small frames
	Interrogation	Anti replay protection
		Strong link-layer authentication.

Table 4.2: Summary of DOS Attacks & Defences at the Physical and MAC / Link Layers

LAYER	THREAT	DEFENCE
Network	Spoofed or replayed routing information	Append a MAC after the message.
	Selective forwarding	Using multiple paths to send data
		Detect the malicious node
		Implicit acknowledgments
	Sinkhole	Geo-routing protocols
	Sybil	Unique shared symmetric key
	Wormholes	Shortest path traffic routing
	Hello flood attacks	Authentication
	Acknowledgement spoofing	Authentication via encryption of all sent packets
Transport	Flooding	Connection via solving of a puzzle
	De-synchronization	Packet authentication
Application	Overwhelm attack	Carefully tuning sensors
	Path-based DOS attack	Combining packet authentication and anti replay protection
	Deluge (reprogram) attack	Use of authentication streams

Table 4.3: Summary of DOS Attacks & Defences at the Network, Transport and Application Layers

4.3 Energy consumption

Energy consumption is an important concern in wireless multimedia sensor networks. In traditional sensor networks, sensors are powered by batteries. Therefore, saving energy is a primary goal in network protocol design. The design of protocols and applications for wireless Multimedia sensor networks has to be energy aware in order to prolong the lifetime of the network, because the replacement of the embedded batteries is a very difficult process once these nodes have been deployed.

Classical approaches like Direct Transmission and Minimum Transmission Energy do not guarantee well balanced distribution of the energy load among nodes of the sensor network. Using Direct Transmission (DT), sensor nodes transmit directly to the sink, as a result nodes that are far away from the sink would die first. On the other hand, using Minimum Transmission Energy (MTE), data is routed over minimum-cost routes, where cost reflects the transmission power expended. Under MTE, nodes that are near the sink act as relays with higher probability than nodes that are far from the sink. Thus nodes near the sink tend to die fast.

Under both DT and MTE, a part of the field will not be monitored for a significant part of the lifetime of the network, and as a result the sensing process of the field will be biased. A solution proposed in LEACH, guarantees that the energy load is well distributed by dynamically created clusters, using cluster heads dynamically elected according to a priori optimal probability. Cluster heads aggregate reports from their cluster members before forwarding them to the sink. By rotating the cluster-head role uniformly among all nodes, each node tends to expend the same energy over time. Most of the analytical results for LEACH schemes are obtained assuming that the nodes of the sensor network are equipped with the same amount of energy. Hence this is the case of homogeneous sensor network which is not feasible in telemedicine with heterogeneous sensors network.

Another scheme Stable Election Protocol (SEP) was proposed with the assumption that a percentage of the node population is equipped with more energy than the rest of the nodes in the same network, this is the case of heterogeneous sensor networks.

In the following chapter, we propose Dijkstra's algorithm as the solution for energy consumption It find the shortest path between sender node and receiver node, as the shortest path is found, the nodes in the other paths can be put in sleep mode, thus ensuring efficient energy routing and utilizing the available energy.

Chapter 5

Simulations

5.1 Energy-Efficient Routing Algorithm

The data routing in wireless multimedia sensor network is realized on the links comparison base. The considered links between a sender and a receiver can be compared in terms of the length, link quality or residual energy of the node pairs. Nevertheless, the path with the smallest investigated value is selected as the route for the data delivery. For the discovering of the optimal route between two nodes in the graph data structure, a Matlab implementation of ***Dijkstra's*** algorithm can be used. The ***Dijkstra's*** algorithm is implemented within a *grShortPath* function that is included in *grTheory* Matlab toolbox.

$$[\text{dsp, sp}_{i,j}] = \text{grShortPath(E, ID}_i\text{, ID}_j\text{);}$$

The *grShortPath* function takes a E matrix of neighbors, source i and destination j node as an input arguments. It returns a dSP matrix with the shortest path between all node pairs in the network. Furthermore, it returns an sp vectors with the nodes constituting the shortest path between nodes i, j. The E matrix must have an exact form for the correct *grShortPath* algorithm processing. It contains three columns, where the first two columns contains the all nodes in the network that are neighbors of each other and third column contains the Euclidean distance

in meters between them. The E matrix can be created during the network layout printing, see Table 5.1. As was mentioned before, the link lengths between all node pairs are compared with the uniform radio range R and if the condition $d_{i;j}$ < R is accomplished the link is displayed. The E matrix is created within this condition since all required parameters such as IDs of two neighbors and their distance d is known and condition of lengths is accomplished. The context of the E matrix is visualized also in Table 5.2. If the link quality or residual energy are to be used instead of the distance between nodes for the route establishment, the information in the third column of E matrix can be substituted by the required information. Then the path between two nodes is selected as the path with the highest quality or path with the maximum energy. Fig. **??** shows results of the described functions

Algorithm: **E=createNbrTable**
1 : $row = 1$;
2: for all node pairs
3 : x =abs$(x_i - x_j)$;
4 : y =abs$(y_i - y_j)$;
5 : $dist$ =sqrt$(x^2 + y^2)$;
6 : if $dist_{i,j} < R$;
7 : plot$([x_i, x_j], [y_i, y_j])$; %draw edge
8 : $E(row, 1) = ID_i$;
9 : $E(row, 2) = ID_j$;
10 : $E(row, 3) = dist_{i,j}$;
11 : $row++$;

Table 5.1: Pseudocosde of layout visualization and matrix definition.

ID_i	ID_j	$dist_{i,j}$
1	2	15.65
1	3	9.21
1	8	21.54
2	1	15.65
2	8	11.12
.	.	.
.	.	.
.	.	.

Table 5.2: E-matrix Example.

Parameter	**Value**
Network size (N)	500 x 500m
Source node location (L_s)	Random
Number of sources (C_s)	1
Number of sensor nodes (C_n)	100, 300, 500, 700, 1000

Table 5.3: Simulation Parameters

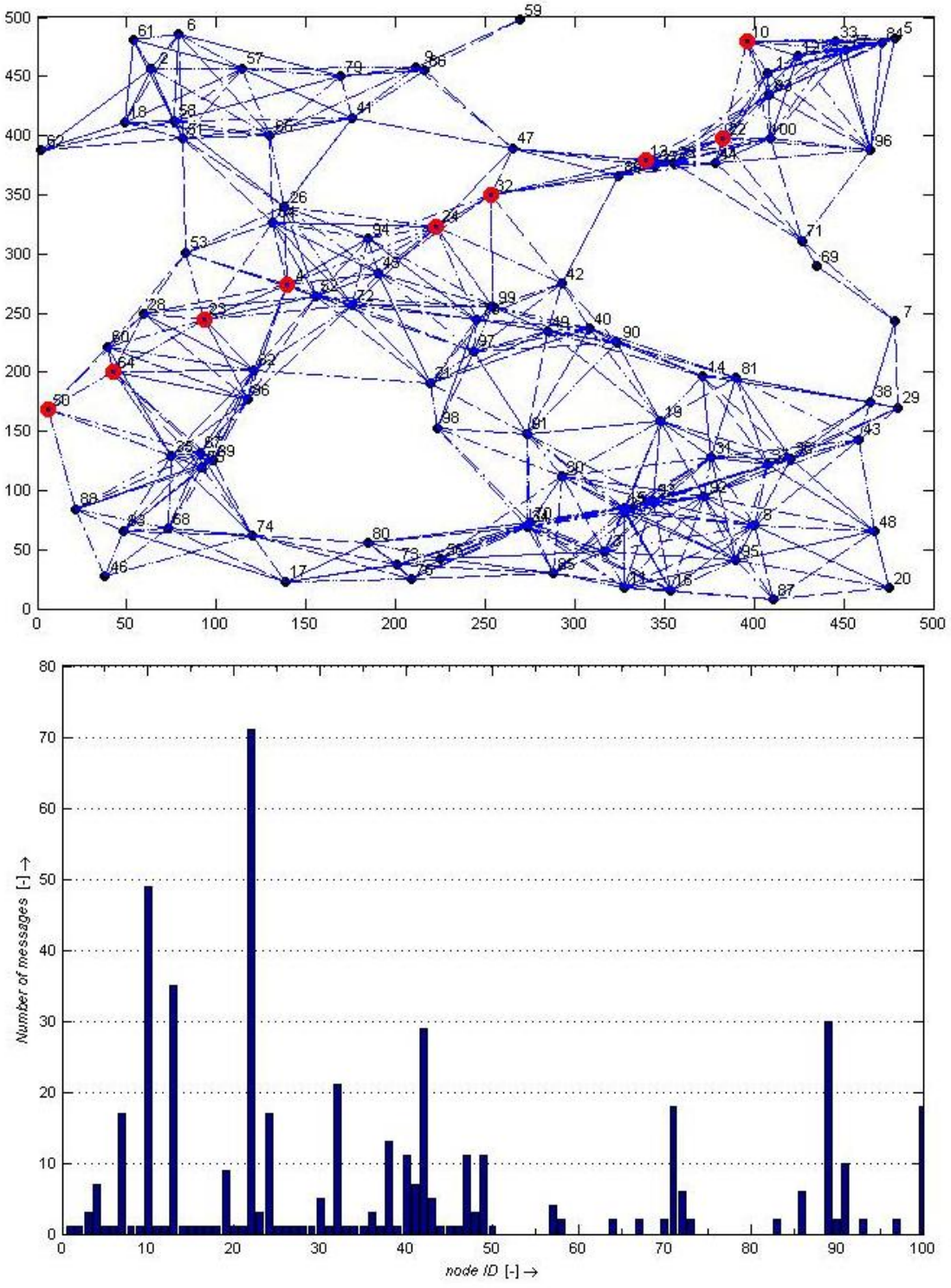

Figure 5.1: 100 Sensor Nodes

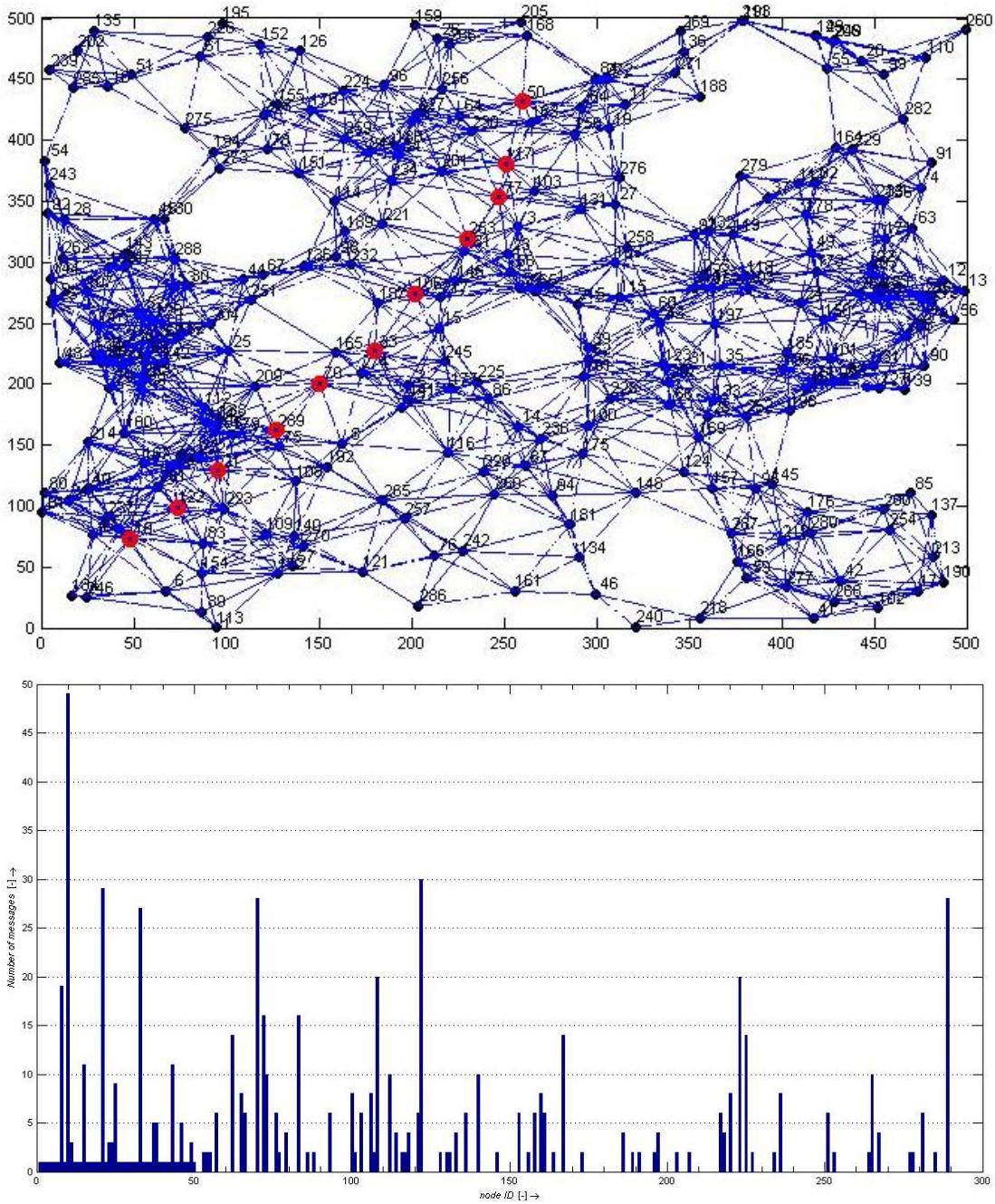

Figure 5.2: 300 Sensor Nodes

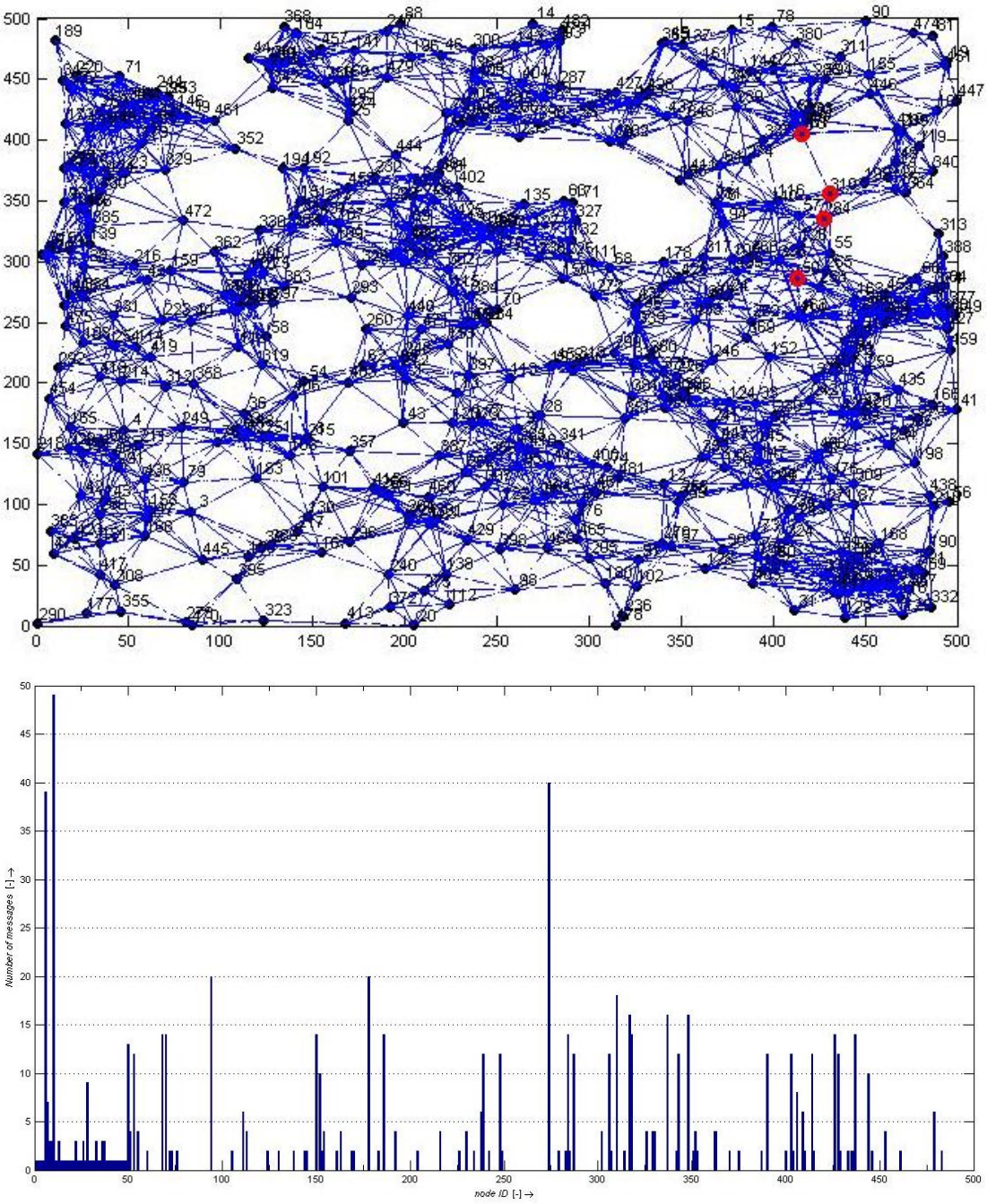

Figure 5.3: 500 Sensor Nodes

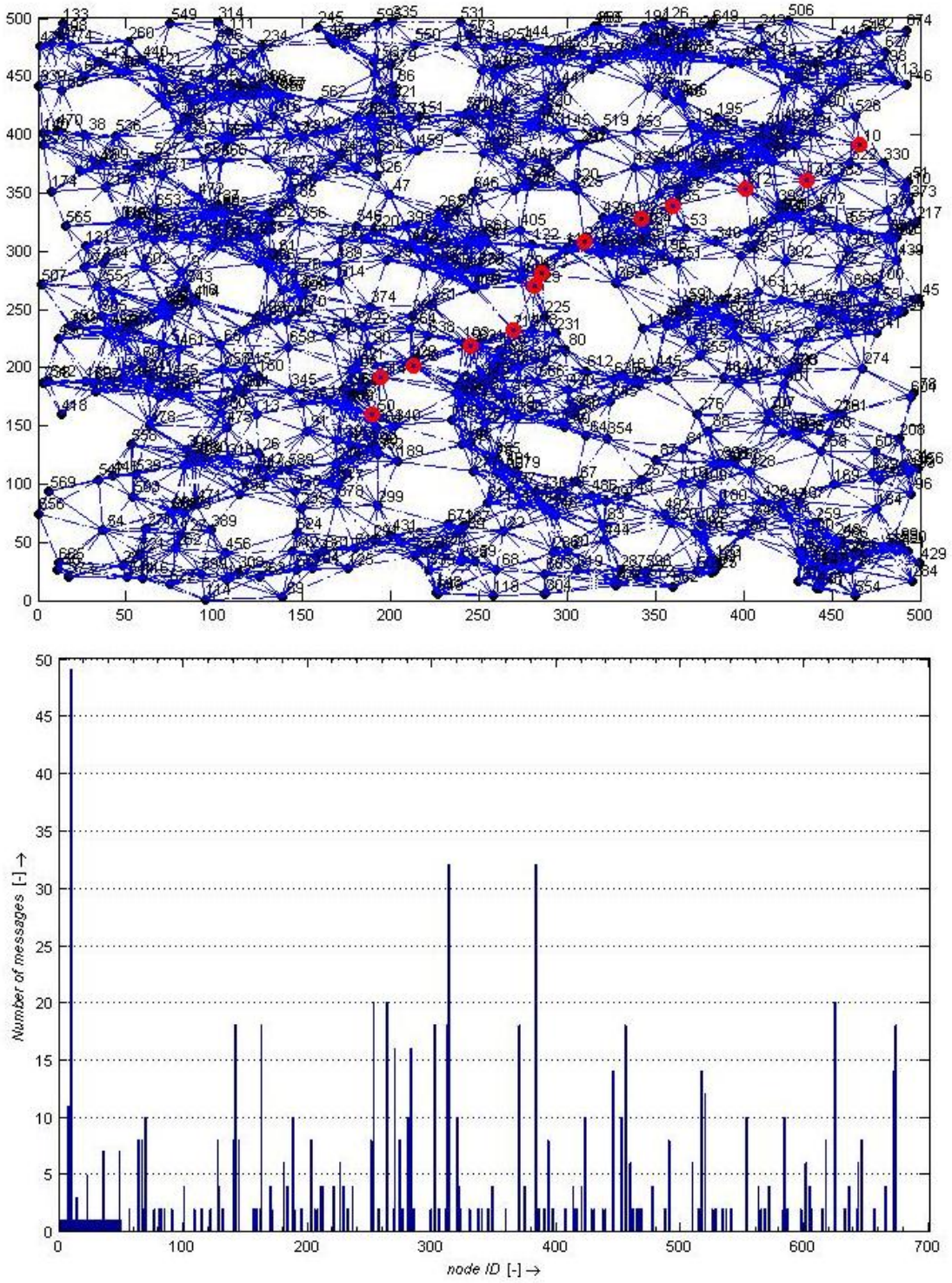

Figure 5.4: 700 Sensor Nodes

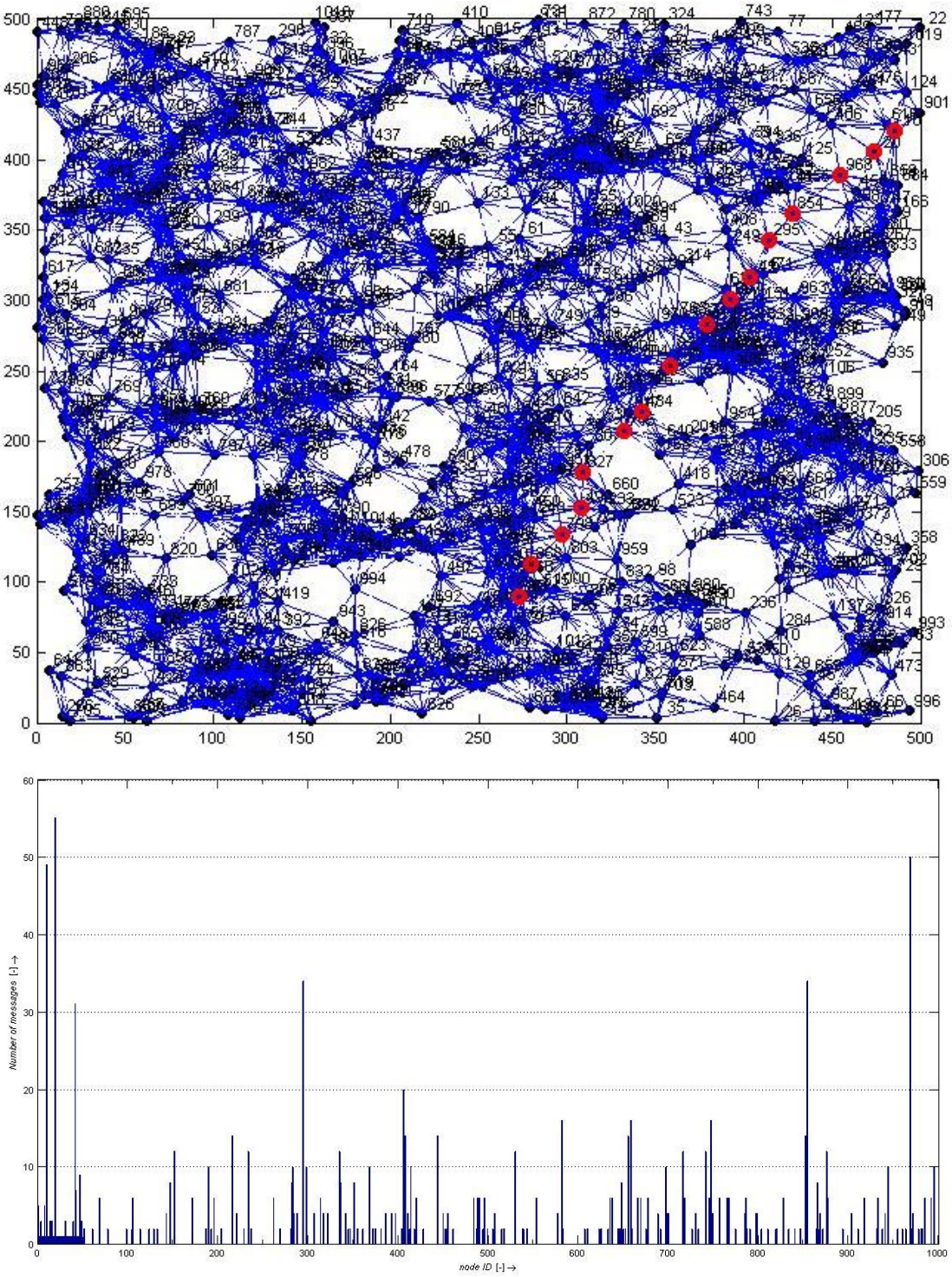

Figure 5.5: 1000 Sensor Nodes

Using 500 square meters as a test bed, the network was initially simulated for 100 sensor nodes, followed by 300, 500, 700 and 1000 sensor nodes as shown in figure 5.1, 5.2, 5.3, 5.4 and 5.5 respectively. In each case the shortest path was established between the sender node and receiver. From the figures, the sensor nodes that are involved in establishing the rout are highlighted with red colour. The bar charts also indicate the number of messages processed by each node during the simulation. Nodes with higher number of processed messages tend to be more proximate to the sender and receiver.

However as the number of sensor nodes are increased, the time taken to establish the path also increased. This may consequently lead to latency in data transmission which will hence be considered as limitation.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

We have investigated the current status of WMSN, we proposed an architecture to be utilized while applying WMSN to telemedicine; we also explored various challenges experienced during the design as well as application, these included high bandwidth demand, security focusing on the Denial of Service aspects and energy consumption.

Finally we proposed Dijkstra's algorithm as an energy efficient scheme in the routing, by finding the shortest path, we simulated the Algorithm using grTheory Matlab toolbox. However, during the simulation we experienced one challenge; as we increased the number of sensor nodes, the simulation time increase and this may bring about latency in the transmission.

6.2 Future Work

In the future, we intend to extend our study and broadly address the other challenges experienced by wireless multimedia senor networks, which include latency, multimedia in network processing and more.

References

[1] I.F. Akyildiz, T. Melodia, and K.R.Chowdhury, 2007. A Survey on wireless multimedia sensor networks, Computer Networks (Elsevier) J., vol. 51, pp. 921-960.

[2] World Health Organization (WHO). 2010. Report on the second global survey on eHealth. TELEMEDICINE Opportunities and developments in Member States. Global Observatory for eHealth series - Volume 2.

[3] Adnan .I. Al Rabea. 2012. Using Wireless Sensor Networks for Managing Telemedicine. Applications. International Conference on System Engineering and Modeling (ICSEM 2012) IACSIT Press, Singapore.

[4] Ko J., Lim J.H., Chen Y., Musaloiu-E. R., Terzis A., Masson G.M. MEDiSN: Medical Emergency Detection in Sensor Networks. ACM Trans. Embed. Comput. Syst. 2010; $10 : 1 - 29$.

[5] Pardeep K., Hoon-Jae L: Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. MDPI Sensors (ISSN 1424-8220; CODEN: SENSC9), 2012; 12(1): $55 - 91$. 22 December 2011

[6] Lorincz K., Malan D.J., Fulford-Jones T.R.F., Nawoj A., Clavel A., Shayder V., Mainland G., Welsh M. Sensor Networks for Emergency Response: Challenges and Opportunities. , IEEE Pervasive Computing, vol. 3, no. 4, pp. 16-23, Oct.-Dec. 2004, doi:10.1109/MPRV.2004.18

[7] Hu F, Jiang M, Celentano L, Xiao Y. Robust medical ad hoc sensor networks (MASN) with wavelet-based ECG data mining. Ad Hoc. 2008; 6 : 9861012.

[8] Wood A., Virone G., Doan T., Cao Q., Selavo L., Wu Y., Fang L., He Z., Lin S., Stankovic J. ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring. Department of Computer Science, University of Virginia; Charlottesville, VA, USA: 2006. Technical Report CS-2006-01;

[9] Chakravorty R. A Programmable Service Architecture for Mobile Medical Care. Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW'06); Pisa, Italy. 131 March 2006.

[10] Wimedia Alliance, www.wimedia.org/

[11] Reed, J., Introduction to Ultra Wideband Communication Systems. Englewood Cliffs, New Jersey: Prentice Hall, June 2005.

[12] "Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems." First note and Order, Federal Communications Commission, ETDocket 98-153, Adopted February 14, 2002, released April 22, 2002.

[13] Jianli Pan, Prof. Raj jain. 2008. Survey paper. Medical applications of UWB. http://www.cse.wustl.edu/ jain/cse574-08/ftp/uwb/index.html. Last accessed 2013.

[14] D. Niyato, E. Hossain, and J. Diamond, "IEEE 802.16/WiMAX-based broadband wireless access and its application for telemedicine/e-health services [Accepted from Open Call]," Wireless Communications, IEEE [see also IEEE Personal Communications], vol. 14, pp. 72-83, 2007.

[15] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. 2007. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON).

[16] Yuechun Chu and Aura Ganz. 2006. Mobile Telemedicine Systems Using 3G Wireless Networks. Report. University of Massachusetts.

[17] Adrian Brindley November 1, 2002 “Denial of Service attacks and the emergence of Intrusion Prevention Systems”

[18] Mieso K. Denko “Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme” systemics, cybernetics and informatics, volume 3 - number 4

[19] Tom Anderson, Timothy Roscoe, David Wetherall, Preventing Internet Denial-of-Service with Capabilities

[20] Manel Guerrero-Zapata, Ruken Zilan, José M. Barceló-Ordinas, Kemal Bicakci, Bulent Tavli, December 2009, “The future of security in Wireless Multimedia Sensor Networks” Springer.

[21] A. D.Wood, J. A Stankovic, “Denial of Service in Sensor Networks”, IEEE Computer., vol. 35, no. 10, October 2002, pp. 54-62.

[22] P. Ning, A. Liu, and WL Du, “Mitigating DoS attacks against broadcast authentication in wireless sensor networks, ACM Transactions on Sensor Networks, vol. 4, no. 1, pp.35, Jan, 2008.

[23] E. Shi, and A. Perrig, “Designing secure sensor networks, Journal of IEEE Wireless Communications”, vol. 11, issue 6, Dec. 2004, pp. 38-43.